Middle East Technical University
Informatics Institute

Process, Technology and Human Aspects of a Security Operations Center

Advisor Name:
Aybar Can ACAR
(METU)

Student Name:
Cem ERDIVAN
Department of Cyber Security

January 2024

TECHNICAL REPORT
METU/II-TR-2024-

Orta Doğu Teknik Üniversitesi
Enformatik Enstitüsü

Bir Güvenlik Operasyonları Merkezinin Süreç, Teknoloji ve İnsan Boyutları

Danışman Adı:
Aybar Can ACAR
(ODTÜ)

Öğrenci Adı:
Cem ERDİVAN
Siber Güvenlik Bölümü

Ocak 2024

TEKNİK RAPOR
ODTÜ/II-TR-2024-

REPORT DOCUMENTATION PAGE

1. AGENCY USE ONLY (Internal Use)	**2. REPORT DATE** 24.01.2024
3. TITLE AND SUBTITLE **PROCESS, TECHNOLOGY AND HUMAN ASPECTS OF A SECURITY OPERATION CENTER**	
4. AUTHOR Cem ERDIVAN	**5. REPORT NUMBER (Internal Use)** METU/II-TR-2024-
6. SPONSORING/ MONITORING AGENCY NAME(S) AND SIGNATURE(S) Cyber Security Master's Programme, Department of Cyber Security, Informatics Institute, METU Advisor: Aybar Can ACAR Signature:	
7. SUPPLEMENTARY NOTES	

8. ABSTRACT (MAXIMUM 200 WORDS)

This report presents the high level aspects of any security operations center and tries to define a baseline for SOC processes, technologies to be used and roles to be assigned for an effective and efficient service. This work takes international standards and guideline as reference as they are highly mature documents with wide adoption rate. This report can be used as benchmark tool for initial stages of gap assessments or even present a roadmap for those who need it.

9. SUBJECT TERMS	**10. NUMBER OF PAGES** **91**

TABLE OF CONTENTS

TABLE OF CONTENTS ..... *IV*

LIST OF TABLES ..... *V*

LIST OF FIGURES ..... *VI*

INTRODUCTION *1*

WHAT IS A SOC? 1

SOC BENEFITS 1

TYPES OF SOCs 2

PROCESS ASPECT *4*

LOG MANAGEMENT 4

SECURITY MONITORING 5

CYBER THREAT INTELLIGENCE 5

INCIDENT RESPONSE 6

VULNERABILITY AND PATCH MANAGEMENT 7

CRYPTOGRAPHIC KEY MANAGEMENT 8

IT CONTINGENCY PLANNING 9

SECURE DEVELOPMENT SUPPORT 9

IT RISK MANAGEMENT 10

SECURITY AWARENESS TRAINING 11

ORGANIZATIONAL CAPABILITY DEVELOPMENT (SECURITY TRAINING) 12

TECHNOLOGY ASPECT *13*

SIEM 13

XDR 15

FIREWALL 16

IDS/IPS 17

EDR 18

ANTIMALWARE SOLUTIONS 19

GRC TOOLS 20

HSM 21

DLP 22

DATA CLASSIFICATION TOOLS 23

VULNERABILITY SCANNER 23

NETWORK SCANNER 25

HUMAN ASPECT *27*

SOC GOVERNANCE *33*

PERFORMANCE MEASUREMENT AND KPIS 33

INTERNAL AUDIT 33

VERIFICATION OF RESULTS AND OUTPUTS 34

REFERENCES *36*

APPENDIX *37*

LIST OF TABLES

Table 1 SFIA Security Leadership, Strategy and Management 28
Table 2 SFIA Security Operations 28
Table 3 SFIA Security Risk Management, Audit and Compliance 29
Table 4 SFIA Incident Management Practitioners 29

LIST OF FIGURES

Figure 1 NICE Framework Building Blocks 27
Figure 2 ECSF Role Profiles 30

INTRODUCTION

WHAT IS A SOC?

A Security Operations Center (SOC) is a centralized unit within an organization dedicated to monitoring, detecting, responding to, and mitigating cybersecurity threats. Its primary objective is to safeguard the organization's information systems, networks, and data from a spectrum of cyber threats, including malware, phishing attacks, and unauthorized access.

Equipped with advanced technologies and skilled cybersecurity professionals, a SOC continuously analyzes and correlates vast amounts of security data generated by network devices, applications, and endpoints. The SOC employs Security Information and Event Management (SIEM) tools, intrusion detection systems, and other technologies to identify anomalies and potential security incidents.

In the event of a security incident, the SOC's expert analysts coordinate incident response efforts, employing predefined playbooks and response plans. The SOC's role extends beyond mere incident detection; it actively works to mitigate and remediate security threats, minimizing potential damage and ensuring the organization's resilience against cyberattacks. Regularly updating its methodologies, technologies, and response strategies, a SOC plays a pivotal role in maintaining a proactive and adaptive cybersecurity posture in the face of evolving cyber threats.

SOC BENEFITS

A Security Operations Center (SOC) is a critical component of modern cybersecurity strategies, playing a pivotal role in safeguarding organizations against a myriad of cyber threats. Its importance is multifaceted, addressing the dynamic nature of the digital landscape and the evolving tactics employed by malicious actors.

Central to a SOC's significance is its ability to provide early threat detection. By continuously monitoring network activities and leveraging advanced technologies such as Security Information and Event Management (SIEM) systems, intrusion detection systems, and endpoint protection tools, a SOC can identify anomalies and potential security incidents in real-time. This early detection is instrumental in preventing cyber threats from escalating into major breaches.

The SOC's capability for rapid incident response is equally crucial. In the event of a security incident, the SOC's dedicated incident response teams can execute predefined playbooks and response plans. This agility minimizes the impact of security breaches, mitigates risks swiftly, and prevents the spread of malicious activities. Continuous monitoring is a cornerstone of a SOC's operation. This ensures vigilant oversight of an organization's digital assets, allowing security professionals to respond promptly to emerging threats, unauthorized access attempts, and abnormal activities within the network. Integration of threat intelligence feeds enhances a SOC's proactive defense capabilities. By staying informed about the latest cyber threats and attack vectors, the SOC can adapt its security measures, fortifying the organization against evolving risks.

A SOC's efficient use of security technologies is instrumental in creating a layered defense mechanism. From SIEM systems that aggregate and analyze security data to intrusion detection systems that identify malicious activities, these technologies work collaboratively to bolster the overall security posture of an organization. Beyond immediate incident response, a SOC conducts thorough incident investigations and forensic analyses. This post-incident analysis not only aids in understanding the root causes of security events but also informs proactive measures to prevent similar occurrences in the future. A SOC's role extends to ensuring compliance with industry standards and regulatory requirements. By adhering to specific cybersecurity standards, organizations can avoid legal and financial repercussions, fostering a secure and trusted operational environment.

In promoting operational resilience, a SOC minimizes downtime and disruptions caused by cyber incidents. Rapid response and recovery strategies are essential for maintaining business continuity and preventing significant operational disruptions. Additionally, a SOC often plays a role in promoting cybersecurity awareness and training within organizations. Educating users about potential threats and best practices enhances the human element of cybersecurity, creating an additional layer of defense against social engineering attacks and other security threats. A well-functioning SOC is a cornerstone of an organization's cybersecurity strategy. Its continuous monitoring, early threat detection, rapid incident response, integration of threat intelligence, and contribution to compliance efforts collectively contribute to an organization's ability to adapt, respond, and thrive in the face of an ever-evolving cyber threat landscape.

TYPES OF SOCs

On-Prem

An on-premises Security Operations Center (SOC) refers to a cybersecurity facility physically located within an organization's premises, emphasizing a tangible, in-house approach to cybersecurity. In this model, the organization owns and manages the entire SOC infrastructure, including servers, network devices, and security appliances. This on-prem SOC allows for direct control and customization of security measures, making it particularly suitable for industries with sensitive data and stringent compliance requirements.

The physical presence of an on-prem SOC enhances network visibility, enabling security analysts to closely monitor internal activities and respond promptly to security incidents. This model offers a higher degree of customization and integration with existing IT systems, aligning security measures more precisely with organizational goals. Additionally, the on-prem SOC provides a level of compliance control, facilitating adherence to industry standards and regulatory frameworks. While it offers benefits in terms of control and customization, organizations should weigh the associated challenges, including infrastructure costs and resource allocation, when opting for an on-prem SOC strategy.

Cloud SOC

A Cloud Security Operations Center (SOC) is a cybersecurity model that operates in cloud environments, offering organizations the ability to monitor, detect, and respond to security threats within cloud-based infrastructure. In contrast to traditional on-premises SOCs, a Cloud SOC is specifically designed to secure assets and data hosted in cloud platforms.

Key features of a Cloud SOC include the ability to monitor virtual machines, containers, and cloud-native services, providing comprehensive visibility into the dynamic and distributed nature of cloud environments. Leveraging cloud-native security technologies, such as Cloud Security Information and Event Management (Cloud SIEM) systems, a Cloud SOC is adept at handling the unique challenges posed by cloud platforms.

Cloud SOCs facilitate the centralization of security operations for organizations utilizing cloud services, offering advantages like scalability, flexibility, and the ability to adapt to the rapid pace of cloud technology evolution. This model allows businesses to harness the benefits of the cloud while ensuring that their digital assets are protected against a wide range of cyber threats. Security professionals in a Cloud SOC employ cloud-native tools and practices to proactively defend against emerging threats and safeguard critical data and applications in the cloud.

M-SOC

A Managed Security Operations Center (SOC) is a cybersecurity service model designed to enhance an organization's security posture by outsourcing the management of its security operations to a specialized provider known as a Managed Security Service Provider (MSSP). In this arrangement, the MSSP assumes the responsibility of monitoring, detecting, and responding to security threats on behalf of the client organization.

Key components of a Managed SOC include continuous monitoring of the organization's digital infrastructure, proactive threat detection, and timely incident response. The MSSP employs advanced technologies, such as Security Information and Event Management (SIEM) systems, intrusion detection systems, and other cybersecurity tools, to analyze and correlate security data. This analysis is conducted by experienced security analysts and experts who can interpret complex threat landscapes.

Managed SOCs offer several advantages to organizations, particularly those with resource constraints or a need for specialized cybersecurity expertise. One of the primary benefits is cost-effectiveness, as outsourcing security operations eliminates the need for significant upfront investments in technology, infrastructure, and skilled personnel. This model allows organizations to leverage the MSSP's expertise, advanced tools, and established processes without the burden of managing these aspects internally. Moreover, a Managed SOC provides scalability, allowing organizations to adjust their level of security services based on their evolving needs. MSSPs are equipped to handle a wide range of security tasks, including incident response, vulnerability management, and compliance monitoring.

The MSSP's role extends beyond monitoring, encompassing incident response and mitigation. When a security incident occurs, the Managed SOC initiates predefined response plans and coordinates with the client to minimize the impact of the incident. This collaborative approach ensures a swift and effective response to security threats. A Managed SOC is a strategic cybersecurity partnership where organizations entrust the management of their security operations to external experts. This model provides a cost-effective, scalable, and expert-driven solution for organizations seeking to bolster their cybersecurity defenses while focusing on their core business objectives.

PROCESS ASPECT

By definition: process is a set of activities that transform inputs into outputs. This section explains which processes any SOC should establish to perform its duties. These processes are tightly integrated with the technologies and people, and require significant strategic planning. Selection of processes to be established is really what defines the SOC's service portfolio. Without carefully crafting portfolio services, and thus processes, it is impossible to come up with the right investment plan for products and talent.

For the processes described below, corresponding NIST standards have been selected as reference. Also, the inherent need for creating policies and procedures, defining roles and responsibilities, and assigning employees to the roles have been omitted for all the processes listed here.

LOG MANAGEMENT

Logs are like records of what happens in a company's computer systems, especially when it comes to security. They're made by things like antivirus software, operating systems, and apps. But handling these logs properly is a big task. Log management includes making, sending, storing, looking at, and getting rid of these security logs. Regularly checking logs is important for catching security problems, rule-breaking, and other issues. It helps with audits, investigations, and compliance. This project uses NIST SP 800-92 Guide to Computer Security Log Management [1] document as a reference.

The challenge is dealing with lots of log sources, different content, formats, and too much data. It's tough because there's only so much we can do with limited resources. Managing logs also means keeping them safe and making sure they're always available when needed. The guide for federal departments and agencies gives tips on how to handle these challenges. It probably suggests ways to use resources better, make log formats more consistent, and ensure that administrators regularly check logs properly. In a nutshell, the guide talks about how important it is to manage logs well for keeping computer systems safe and gives advice on how to do that for government departments.

Common log sources that can be found in a typical organization:

- Security software
- Operating systems
- Application software and APIs

Log Life Cycle

NIST SP 800-92 describes the functions of a log management process as follows:

- Log parsing is extracting data from a log so that the parsed values can be used as input for another logging process.
- Event filtering is the suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
- Event aggregation means, similar entries are consolidated into a single entry containing a count of the number of occurrences of the event.
- Log rotation is closing a log file and opening a new log file when the first file is considered to be complete.
- Log archival is retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.
- Log compression is storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents.
- Log reduction is removing unneeded entries from a log to create a new log that is smaller.

- Log conversion is parsing a log in one format and storing its entries in a second format.
- In log normalization, each log data field is converted to a particular data representation and categorized consistently.
- Log file integrity checking involves calculating a message digest for each file and storing the message digest securely to ensure that changes to archived logs are detected.
- Event correlation is finding relationships between two or more log entries.
- Log viewing is displaying log entries in a human-readable format.
- Log reporting is displaying the results of log analysis. Log reporting is displaying the results of log analysis.
- Log clearing is removing all entries from a log that precede a certain date and time.

SECURITY MONITORING

NIST Special Publication 800-137 [2], titled "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," provides guidelines for implementing continuous monitoring practices to enhance the security of information systems within federal agencies. In simpler terms, it's like a rulebook for keeping an eye on computer systems all the time to make sure they stay safe. Continuous monitoring is crucial because it helps in detecting and responding to security threats promptly, ensuring that computer systems are protected around the clock. The document outlines a step-by-step approach to establish and maintain effective continuous monitoring processes.

The first step is to set up a baseline, which is like creating a standard for normal behavior in the computer system. This baseline helps in identifying when something unusual or potentially harmful happens.

Next, the publication emphasizes the importance of selecting the right security controls. Think of security controls as safety measures for the computer system. The guide suggests choosing controls based on the specific risks and needs of the organization.

Once the controls are in place, continuous monitoring involves regularly checking and analyzing what's happening in the system. It's like having a watchful eye on the computer activities to make sure everything is running as it should.

The publication recommends using automated tools for monitoring whenever possible. These tools can quickly spot unusual activities and potential threats, acting like smart assistants that help keep the system safe. Additionally, it advises creating a plan for responding to incidents. This plan is like a set of instructions for what to do if something goes wrong. Having a well-thought-out plan ensures a quick and effective response to security issues.

Regular training for the people managing the computer systems is also highlighted in the guide. It's like making sure the guardians of the system are well-prepared and know what to look for to keep everything secure. Furthermore, the document stresses the importance of reviewing and updating security measures regularly. This is like giving the computer system a regular check-up to ensure it's protected against the latest threats.

In simpler terms, NIST SP 800-137 is a guide that helps federal agencies keep their computer systems safe by constantly watching over them. It suggests creating a standard behavior, choosing the right safety measures, regularly checking the system, using smart tools, having a plan for emergencies, training the system guardians, and keeping everything up to date. By following these steps, organizations can significantly enhance the security of their information systems and better protect sensitive data.

CYBER THREAT INTELLIGENCE

The selected guide, NIST Special Publication 800-150 [3], titled the "Guide to Cyber Threat Information Sharing," serves as a practical manual for organizations to enhance their collective cybersecurity efforts through effective information sharing. It can be likened to a user-friendly guidebook that facilitates

collaboration within the cybersecurity community, enabling proactive measures against evolving online threats.

The guide underscores the critical importance of sharing information about cyber threats. Similar to neighbors sharing insights about suspicious activities to ensure the safety of the entire community, information sharing in the digital realm is key to collective defense. It recommends the creation of a plan or framework for sharing information. This can be compared to setting up a structured system that enables everyone involved to understand how to share details about cyber threats without causing confusion or inefficiency. The guide assists organizations in determining what type of information is relevant to share. Much like neighbors deciding what specific details about a potentially threatening individual to share, the aim is to enhance collective awareness and protection.

Emphasis is placed on protecting privacy and security while engaging in information sharing. This parallels the real-world practice of ensuring that shared details do not compromise anyone's safety or exacerbate existing security challenges. The guide advocates for the use of common standards and practices in information sharing. This is akin to agreeing on a common language or set of rules to facilitate clear communication and effective collaboration within the cybersecurity community.

Building trust among participating organizations is highlighted. Trust is a cornerstone for effective collaboration in addressing cyber threats, analogous to the trust within a neighborhood watch program where community members rely on each other for collective security. The document encourages a wider array of organizations to actively participate in information sharing. This is comparable to inviting more neighbors to join a community watch, fostering a sense of shared responsibility and contributing to a stronger collective defense against cyber threats.

NIST SP 800-150 provides user-friendly guidance for organizations to collaborate in sharing information about cyber threats. By offering insights on creating a plan, determining what to share, safeguarding privacy, standardizing practices, fostering trust, and encouraging broader participation, the guide enhances the collective capacity of the cybersecurity community to stay informed and collectively protect against evolving cyber threats.

INCIDENT RESPONSE

NIST Special Publication 800-61 Revision 2 (SP 800-61r2) [4], titled "Computer Security Incident Handling Guide," is a comprehensive resource providing guidance on how organizations can effectively handle and respond to computer security incidents. In simpler terms, it's like a guidebook that helps organizations deal with and bounce back from cyber-attacks and security issues.

The guide starts by explaining what computer security incidents are. These are like alarms that go off when something goes wrong in the digital world, such as a cyber-attack or a security breach. It emphasizes the need for organizations to have a plan in place for dealing with incidents. Think of it like having a fire evacuation plan - being prepared for emergencies helps to minimize damage and respond more effectively. The guide suggests preparing for incidents in advance. This involves training staff, setting up tools to monitor for unusual activities, and having a clear understanding of the organization's digital environment. It's like practicing fire drills so that everyone knows what to do if a fire breaks out. It explains how to spot and analyze incidents. This is akin to investigating the cause of a fire - understanding how it started and what's affected helps in developing a targeted response. The guide details steps to contain the incident (limiting its impact), eradicating the threat (getting rid of the cause), and recovering (getting things back to normal). It's similar to putting out a fire, making sure it won't reignite, and then rebuilding what was damaged. After dealing with an incident, the guide recommends analyzing what happened and how it was handled. This is like reviewing a fire response to see what worked well and what could be improved for the future. The importance of coordinating and communicating during incidents is highlighted. It's like making sure everyone involved in handling a fire is on the same page, sharing information to address the situation effectively. The guide stresses the need for continuous improvement. It's like learning from each fire drill and incident to enhance the organization's overall security measures.

NIST SP 800-61r2 is a user-friendly guide that helps organizations prepare for, respond to, and learn from computer security incidents. It provides practical advice, much like a manual for handling digital emergencies, ensuring that organizations can effectively protect their digital assets and recover from cyber-attacks.

VULNERABILITY AND PATCH MANAGEMENT

NIST SP 800-40r4 [5] emphasizes the importance of maintaining and patching software in the face of evolving cybersecurity threats. It discusses how traditional perimeter-based security models are no longer sufficient, given the direct exposure of most technologies to the internet. The shift towards zero trust architectures is highlighted, focusing on securing individual assets rather than entire networks. The text stresses the necessity of enterprise patch management as a critical aspect of reducing risks and maintaining the trust status of assets. It addresses concerns about productivity and downtime, suggesting that patching should be considered a standard cost of doing business. The publication recommends a collaborative approach involving leadership, business/mission owners, and security/technology management to create an effective and streamlined enterprise patch management strategy.

Vulnerability management is a crucial aspect of cybersecurity, focused on identifying, evaluating, and mitigating potential security risks within an organization's systems and networks. A well-structured vulnerability management process helps safeguard against cyber threats and ensures the overall resilience of an organization's IT infrastructure. The following steps outline a comprehensive vulnerability management approach:

- Asset Inventory and Categorization: Begin by creating an inventory of all assets, including hardware, software, and network components. Categorize these assets based on their criticality and importance to the organization. Understanding the asset landscape is essential for prioritizing vulnerability assessments.
- Vulnerability Scanning: Employ automated vulnerability scanning tools to regularly scan the entire IT environment for potential weaknesses. These tools identify known vulnerabilities in software, configurations, and systems. Scheduled scans help maintain an up-to-date view of the organization's security posture.
- Risk Prioritization: Once vulnerabilities are identified, prioritize them based on factors such as severity, potential impact, and exploitability. This allows organizations to focus on addressing the most critical vulnerabilities first, maximizing the impact of remediation efforts.
- Patch Management: Develop and implement a robust patch management process to address identified vulnerabilities promptly. This involves applying security patches and updates to software and systems. Automated patching tools can streamline this process, ensuring timely and effective vulnerability remediation.
- Vulnerability Remediation: Formulate a clear plan for addressing vulnerabilities, which may include applying patches, reconfiguring systems, or implementing compensating controls. Establish accountability and timelines for remediation efforts to ensure a proactive and efficient response.
- Continuous Monitoring: Implement continuous monitoring mechanisms to detect and respond to new vulnerabilities as they emerge. This involves staying informed about the latest threat intelligence, monitoring system logs, and using intrusion detection systems to identify potential security incidents.
- Security Awareness Training: Educate employees about security best practices, common attack vectors, and the importance of reporting potential security issues. A well-informed workforce contributes to a more secure environment by reducing the likelihood of human-related vulnerabilities.
- Incident Response Integration: Integrate vulnerability management with the organization's incident response plan. Establish clear communication channels and protocols for addressing vulnerabilities that may be exploited in a security incident. This ensures a coordinated and effective response to potential threats.

- Documentation and Reporting: Maintain detailed records of vulnerability assessments, remediation efforts, and their outcomes. Regularly report on the organization's security posture to key stakeholders, providing insights into the effectiveness of vulnerability management activities.
- Continuous Improvement: Periodically review and update the vulnerability management process to adapt to evolving threats and technology changes. Conduct post-remediation assessments to identify areas for improvement and refine the overall security strategy.

Patch management and vulnerability management are closely intertwined processes within cybersecurity. Vulnerability management encompasses the identification and prioritization of weaknesses in an organization's IT environment, including software vulnerabilities and configuration issues. Patch management, as a subset of vulnerability management, specifically deals with the remediation aspect by focusing on applying security patches and updates to eliminate or mitigate identified vulnerabilities in software and applications. The two processes work collaboratively, with vulnerability management providing the broader context of security weaknesses and their prioritization, and patch management executing the targeted application of patches to address those vulnerabilities promptly. Automation, continuous monitoring, documentation, and integration with broader security processes are key elements shared by both practices, ensuring a comprehensive approach to reducing security risks and enhancing the overall resilience of the organization's systems and networks.

CRYPTOGRAPHIC KEY MANAGEMENT

NIST SP 800-57 Part-1 Revision 5 [6] explains cryptographic key management, which is a fundamental aspect of modern cybersecurity, ensuring the secure generation, distribution, storage, and disposal of cryptographic keys used in encryption algorithms. Cryptographic keys are essential for safeguarding sensitive information and maintaining the confidentiality and integrity of data. The key management process involves various stages, each critical for maintaining a robust security posture.

- Key Generation and Distribution: The key generation phase involves creating strong and random cryptographic keys that are resistant to attacks. This process often employs specialized algorithms and random number generators. Keys must be of sufficient length to resist brute-force attacks. Once generated, keys need to be securely distributed to authorized parties. This may involve using key exchange protocols, secure channels, or trusted key distribution centers. The challenge lies in ensuring that keys are only accessible to authorized entities, minimizing the risk of interception or compromise during distribution. Automated key distribution systems can enhance efficiency and reduce the risk associated with manual processes, ensuring that keys reach their intended recipients securely.
- Key Storage and Lifecycle Management: Securing cryptographic keys throughout their lifecycle is crucial to maintaining the overall security of cryptographic systems. Key storage mechanisms must be resistant to both physical and digital attacks. Hardware security modules (HSMs) are often used to provide a secure environment for key storage, offering tamper-resistant hardware that safeguards keys from unauthorized access. Additionally, effective key lifecycle management involves defining policies for key rotation, expiration, and revocation. Regularly updating keys helps mitigate the risk associated with compromised or outdated keys. Organizations must establish clear procedures for key archival and recovery, ensuring that encrypted data can still be accessed in the event of key loss. Key management systems often include audit trails to track key usage and changes, aiding in compliance efforts and facilitating the investigation of security incidents.
- Key Deletion and Disposal: When cryptographic keys reach the end of their useful life or are compromised, secure deletion and disposal processes are critical to prevent unauthorized access to sensitive information. Proper key disposal ensures that even if keys are recovered from storage media, they cannot be used to compromise encrypted data. Organizations must implement secure key erasure mechanisms, often involving overwriting key material or rendering it irrecoverable. Furthermore, key disposal procedures should align with regulatory requirements and industry best practices. Regular audits and assessments of key management practices help identify vulnerabilities or deviations from security policies, enabling organizations to continuously improve their cryptographic key management processes and adapt to evolving threats.

IT CONTINGENCY PLANNING

NIST Special Publication 800-34 [7] is a helpful guidebook, providing clear steps for preparing and responding to unexpected events that could affect their computer systems. It's essentially a playbook to ensure the availability and safety of crucial information, even in challenging situations.

The guide underscores the importance of having a contingency plan in place, akin to having a backup strategy for a road trip to handle unexpected detours or disruptions. It breaks down the planning process into key components, starting with a risk assessment to identify potential issues. Agencies are encouraged to create a detailed plan, similar to having a step-by-step guide for various scenarios. Regular testing of the contingency plan is emphasized, ensuring that it functions smoothly, much like practicing a backup plan for a smooth journey.

The document introduces a lifecycle approach to contingency planning, starting with preparation, where risks are identified and plans are made. In the activation phase, the plan is put into action, resembling the use of a backup plan during unexpected road closures. Regular maintenance of the plan is highlighted, drawing a parallel to maintaining a vehicle for a trouble-free journey. When the plan is no longer needed, it should be properly disposed of, similar to safely discarding an old map.

Roles and responsibilities are outlined, ensuring that everyone involved has a specific task, much like assigned roles during a road trip where someone navigates, and someone drives. Real-world examples and case studies are provided to illustrate successful strategies, offering practical insights for agencies in their planning, similar to sharing stories of successful journeys to inspire others. The guide emphasizes that contingency planning is not a one-size-fits-all approach. Instead, it must consider the unique characteristics and needs of each information system. This customization is comparable to tailoring travel plans based on the type of vehicle and specific destinations.

In essence, NIST SP 800-34 serves as a practical and adaptable guide for federal agencies, offering a systematic approach to contingency planning. By following the outlined steps and considering real-world examples, agencies can develop effective plans to navigate through unexpected events, ensuring the security and availability of critical information systems.

SECURE DEVELOPMENT SUPPORT

NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1 [8] specifically focuses on addressing cybersecurity considerations in the context of full-time virtualization technologies. Virtualization involves the creation of virtual instances of computing resources, such as servers, storage, or networks, allowing multiple operating systems or applications to run on a single physical machine.

In the dynamic landscape of cybersecurity, collaboration between Security Operations Centers (SOCs) and developers is pivotal for enhancing the overall security posture of an organization. This essay explores the various ways in which a SOC can provide crucial support to developers, fostering a symbiotic relationship that bolsters the resilience of applications and systems.

One of the primary ways in which a SOC supports developers is by sharing timely and relevant threat intelligence. By providing insights into emerging threats, attack trends, and vulnerabilities, SOC teams empower developers with the knowledge needed to proactively address potential security risks in their code. This collaborative approach ensures that developers stay abreast of the rapidly evolving threat landscape, enabling them to make informed decisions in crafting secure applications.

Additionally, SOC professionals play a vital role in conducting security training sessions and awareness programs tailored for developers. These programs educate developers on secure coding practices, common vulnerabilities, and the latest cybersecurity threats. Armed with this knowledge, developers are better

equipped to write code with security in mind, minimizing the likelihood of introducing vulnerabilities that could be exploited by malicious actors.

In the event of a security incident or suspicious activity, SOC teams provide immediate support to developers through incident response guidance. This assistance includes helping developers understand the nature and potential impact of an incident, as well as collaborating on effective mitigation strategies. The SOC's expertise ensures a coordinated and efficient response, minimizing the impact of security incidents on the organization.

Vulnerability management is another critical area where SOC teams collaborate with developers. By working closely together, they identify and prioritize vulnerabilities, offering guidance on remediation strategies. SOC teams ensure that patches or mitigations are applied promptly, contributing to a more secure application landscape. This collaborative effort aligns vulnerability management with the broader security strategy of the organization.

Continuous monitoring of network and system activities is a core responsibility of SOC teams. Leveraging security information and event management (SIEM) solutions, they can detect anomalies or suspicious behavior that might indicate a security threat. Sharing this information with developers enables them to investigate and address potential security incidents in their applications, fostering a proactive stance against emerging threats.

SOC professionals can also collaborate with developers to integrate security tooling directly into the development pipeline. This involves incorporating automated security testing tools, static code analysis, and other security measures into the continuous integration/continuous deployment (CI/CD) pipeline. By identifying and addressing security issues early in the development lifecycle, developers can ensure the resilience and robustness of their systems. Furthermore, SOC teams provide valuable guidance on security architecture. Collaborating with developers, they ensure that security best practices are integrated into the overall design of applications. This proactive approach helps create resilient and robust systems that are better equipped to withstand cyber threats.

In conclusion, the collaboration between SOC teams and developers is essential for creating a holistic and proactive approach to cybersecurity. By fostering this partnership, organizations can integrate security considerations seamlessly into the development lifecycle, leading to the creation of more secure applications and systems. The synergy between SOC professionals and developers is a cornerstone in the collective effort to mitigate cyber threats and safeguard digital assets.

IT RISK MANAGEMENT

The NIST Risk Management Framework (RMF) [9] is a structured and comprehensive approach designed by the National Institute of Standards and Technology (NIST) to manage cybersecurity risk in information systems effectively. This framework is widely adopted by government agencies and organizations to safeguard their digital assets.

The primary purpose of NIST RMF is to provide organizations with a systematic and flexible process for managing and mitigating cybersecurity risks. It guides them in identifying, assessing, and responding to potential threats and vulnerabilities in their information systems. NIST RMF follows a seven-step process, offering a structured approach to risk management. These steps are:

1. Prepare: Establish the context and priorities for managing risk.
2. Categorize: Classify information systems based on impact levels.
3. Select: Choose and implement security controls based on system categorization.
4. Implement: Put security controls into practice within the information system.
5. Assess: Evaluate the effectiveness of security controls.
6. Authorize: Grant approval for the system to operate based on the assessment.
7. Monitor: Continuously oversee and monitor security controls and the overall risk posture.

One of the strengths of NIST RMF is its adaptability. Organizations can tailor the framework to suit their specific needs, considering factors like system complexity, risk tolerance, and unique operational environments. NIST RMF emphasizes collaboration and communication among different stakeholders within an organization. This involves coordination between security teams, IT personnel, and management to ensure a comprehensive understanding of risks and effective implementation of security measures. The framework promotes a culture of continuous improvement. After implementation, organizations are encouraged to learn from experiences, identify areas for enhancement, and update their security measures accordingly. This iterative process helps organizations stay proactive against evolving cyber threats. NIST RMF is designed to adapt to changes in technology and evolving threats. It acknowledges that the cybersecurity landscape is dynamic, and systems need to be resilient to new challenges. This adaptability ensures that security measures remain effective over time. NIST RMF aligns with established cybersecurity standards, providing a baseline for organizations to meet recognized benchmarks. This alignment ensures that organizations adhere to industry best practices and regulatory requirements, contributing to a robust cybersecurity posture.

The framework assists organizations in prioritizing security controls based on the level of risk. It helps organizations allocate resources efficiently by focusing on controls that address the most critical vulnerabilities and threats. NIST RMF adopts a holistic approach, considering not only technological aspects but also people and processes. This comprehensive perspective ensures that cybersecurity measures are well-rounded, addressing all facets of an organization's security posture. NIST RMF provides a structured and adaptable framework for organizations to effectively manage cybersecurity risks. By following its systematic process, organizations can enhance their resilience to cyber threats, continuously improve their security measures, and ensure the protection of their valuable digital assets in an ever-evolving digital landscape.

SECURITY AWARENESS TRAINING

NIST Special Publication 800-50 [10], titled "Building An Information Technology Security Awareness and Training Program," provides guidance on establishing and maintaining effective security awareness and training programs for information technology within organizations. Please note that updates or new versions may have been released since then. NIST SP 800-50 serves as a guide for organizations looking to establish comprehensive security awareness and training programs. The document recognizes the crucial role of human factors in information security and aims to equip organizations with the tools to enhance the security awareness of their workforce. Acknowledging that humans play a significant role in cybersecurity, the guide emphasizes the importance of educating and raising awareness among employees. It recognizes that well-informed individuals are essential components of a robust cybersecurity posture.

The publication provides a framework for developing a structured awareness and training program. This framework includes assessing needs, designing programs, implementing initiatives, and evaluating their effectiveness. It's like creating a curriculum for cybersecurity education within the organization. NIST recommends clearly defining roles and responsibilities for individuals involved in the awareness and training programs. This involves assigning tasks such as program management, content development, and delivery. This structured approach ensures that everyone knows their part in promoting cybersecurity awareness. Recognizing that one size does not fit all, the guide emphasizes tailoring awareness and training programs to meet the specific needs and characteristics of the organization. It's like customizing educational materials to resonate with the organization's culture and workforce.

NIST SP 800-50 explores various delivery methods and materials for training, considering factors such as content relevance, audience engagement, and accessibility. This could involve using diverse resources, from online modules to interactive workshops, to cater to different learning styles. An essential aspect of the guide is the emphasis on measuring the effectiveness of awareness and training efforts. Organizations are encouraged to assess the impact of their programs regularly and use feedback to continuously improve. It's like evaluating the success of educational initiatives and refining them for better results. NIST recommends integrating the awareness and training program with the organization's overall security program. This ensures alignment with broader security goals and objectives. It's akin to ensuring that cybersecurity education aligns seamlessly with the organization's overarching security strategy. Effective communication

and collaboration are highlighted as crucial elements. Ensuring that information flows seamlessly between different departments and stakeholders contributes to the success of awareness and training initiatives. It's like fostering an environment where everyone is on the same page regarding cybersecurity practices. The guide acknowledges the importance of addressing compliance and legal considerations in the development of awareness and training programs. It ensures that programs align with relevant regulations and legal requirements. NIST SP 800-50 provides a comprehensive guide for organizations to establish, maintain, and continuously improve information technology security awareness and training programs. By following the framework and considering the diverse aspects outlined in the document, organizations can cultivate a cybersecurity-aware workforce, ultimately enhancing the overall security posture of the organization.

ORGANIZATIONAL CAPABILITY DEVELOPMENT (SECURITY TRAINING)

NIST Special Publication 800-16 [11], titled "Information Technology Security Training Requirements: A Role- and Performance-Based Model," provides guidance on developing effective information technology security training programs within organizations. Please note that updates or new versions may have been released since then. NIST SP 800-16 introduces a role- and performance-based model for information technology security training. It emphasizes moving beyond traditional, generic training methods to focus on the specific roles and responsibilities of individuals within an organization.

The publication recognizes that different roles within an organization require specific knowledge and skills related to information technology security. It highlights the importance of tailoring training programs to address the unique requirements of each role, ensuring that individuals receive the training necessary for their specific responsibilities. NIST SP 800-16 outlines a model that integrates role-based training with job performance requirements. This model involves identifying roles, determining the necessary skills and knowledge for each role, and aligning training programs with these role-specific requirements. It's like customizing educational content to match the job functions of individuals within the organization. The guide provides guidance on developing training programs that are both role-specific and performance-based. This involves creating content that directly relates to the tasks and responsibilities associated with each role. Training should be practical and applicable to real-world scenarios, ensuring that individuals can apply their knowledge in their daily work. NIST emphasizes the importance of assessing the training needs of individuals based on their roles. This involves understanding the skills and knowledge required for each role and identifying any gaps that need to be addressed through training. It's akin to conducting a skills assessment to tailor education to specific job requirements.

The guide recommends mapping training programs to job performance requirements. This ensures that the content directly aligns with the tasks individuals are expected to perform in their roles. It's like creating a roadmap that connects training objectives with actual job responsibilities. NIST SP 800-16 encourages a continuous improvement mindset for training programs. Organizations should regularly assess the effectiveness of training, gather feedback, and make adjustments as needed. This iterative process ensures that training remains relevant and impactful over time. Effective collaboration and communication are highlighted as crucial elements in implementing role- and performance-based training. Stakeholders, including training developers, managers, and employees, need to work together to ensure the success of the training initiatives. It's like fostering an environment where all parties are actively involved in the training process. The guide emphasizes the integration of role- and performance-based training with the organization's overall security program. This alignment ensures that training efforts support broader security goals and objectives. It's like ensuring that education seamlessly fits into the organization's overarching security strategy. NIST SP 800-16 acknowledges the importance of considering legal and ethical considerations in training programs. This involves ensuring that training content aligns with legal requirements and ethical standards relevant to the organization's industry.

NIST SP 800-16 provides valuable guidance for organizations seeking to implement role- and performance-based training for information technology security. By tailoring training programs to specific roles, aligning them with job performance requirements, and fostering continuous improvement, organizations can enhance the effectiveness of their training initiatives and strengthen the overall cybersecurity posture.

TECHNOLOGY ASPECT

Selecting the right technologies and products for a Security Operations Center (SOC) is paramount for establishing a robust and effective cybersecurity infrastructure. The importance of this decision encompasses various factors that directly impact the SOC's ability to detect, respond to, and mitigate security threats in a dynamic and evolving threat landscape.

Firstly, the chosen technologies form the foundation of the SOC's capabilities. Security Information and Event Management (SIEM) systems, intrusion detection and prevention systems, endpoint protection solutions, and threat intelligence platforms are among the key components. These technologies should seamlessly integrate to provide comprehensive visibility into the organization's IT environment. The careful selection of technologies ensures that the SOC can monitor network traffic, analyze logs, and detect anomalies effectively.

Interoperability is crucial for optimizing workflows and response times. The right technologies facilitate seamless integration, allowing the SOC to correlate data from various sources and respond rapidly to security incidents. A well-integrated ecosystem enhances the efficiency of incident detection, investigation, and response processes.

Scalability is another critical consideration. The chosen technologies must be scalable to accommodate the organization's growth and evolving security needs. This ensures that the SOC can adapt to changes in the threat landscape and effectively handle an increasing volume of security events without compromising performance.

Automation and orchestration capabilities are integral for efficiency. Technologies that support automation of routine tasks, incident response workflows, and playbooks enhance the SOC's ability to respond swiftly to threats. Automation not only reduces response times but also minimizes the risk of human error.

Integration of threat intelligence feeds is essential for staying ahead of emerging threats. The selected technologies should support the ingestion and analysis of threat intelligence, enabling the SOC to proactively defend against evolving cyber threats.

The right technologies also contribute to compliance efforts. Many industries have specific regulatory requirements, and the SOC's technologies should facilitate adherence to these standards. This includes capabilities for generating reports, logging, and auditing to demonstrate compliance to regulatory bodies.

Additionally, user-friendly interfaces and effective visualization tools are vital for SOC analysts. Technologies that provide clear dashboards, intuitive interfaces, and meaningful insights empower analysts to make informed decisions rapidly, especially during high-pressure situations.

In summary, selecting the right technologies for a SOC is foundational to its success. The chosen technologies shape the SOC's capabilities, influence interoperability and scalability, enable automation and orchestration, support threat intelligence integration, contribute to compliance efforts, and enhance the overall user experience for SOC analysts. A well-curated technology stack equips the SOC to effectively address cybersecurity challenges, mitigate risks, and safeguard the organization's digital assets in a rapidly evolving threat landscape.

SIEM

Security Information and Event Management (SIEM) is a comprehensive approach to managing an organization's information security. It involves the collection, aggregation, and analysis of security data from various sources within an organization, such as network devices, servers, and applications. The primary goals of SIEM are to provide real-time analysis of security alerts generated by applications and network hardware and to store and correlate the data for historical analysis and compliance reporting.

Key Components of SIEM:

- Data Collection: SIEM systems collect data from various log sources, including firewalls, antivirus software, intrusion detection/prevention systems, and more.
- Normalization and Correlation: The collected data is normalized to a common format, and correlations are established to identify patterns or anomalies that may indicate security threats.
- Alerting and Notification: SIEM systems generate real-time alerts when suspicious activities are detected. These alerts are often prioritized based on the severity of the threat.
- Incident Response: SIEM facilitates rapid response to security incidents by providing detailed information about the nature of the threat, enabling quicker mitigation.
- Forensic Analysis: Historical data stored by SIEM allows for forensic analysis, helping organizations understand the timeline and details of security incidents for post-incident investigations.
- Compliance Reporting: SIEM helps organizations meet regulatory compliance requirements by providing comprehensive reports on security events and measures taken for compliance purposes.
- User Activity Monitoring: SIEM systems often include user activity monitoring to detect unauthorized access or abnormal behavior by users within the network.

SIEM is a crucial tool for organizations to enhance their cybersecurity posture by providing real-time threat detection, incident response capabilities, and compliance reporting through the centralized analysis of security events and information.

Main Benefits of SIEM:

- Centralized Log Management: SIEM solutions aggregate and centralize logs and security-related data from various sources across the organization, including network devices, servers, applications, and endpoints. This centralized log management provides a holistic view of the organization's security posture.
- Real-Time Event Correlation: SIEM systems analyze and correlate events in real-time, identifying patterns and relationships that may indicate a security incident. This correlation allows for the detection of complex and sophisticated attacks that may involve multiple stages or vectors.
- Early Threat Detection: By continuously monitoring and analyzing logs and events, SIEM systems enable early detection of potential security threats. This early warning system allows security teams to respond proactively, preventing or minimizing the impact of security incidents.
- Incident Response and Investigation: SIEM solutions streamline the incident response process by providing tools for rapid investigation and analysis. Security teams can quickly drill down into specific events, trace the timeline of incidents, and gather the necessary information to understand the nature of a security event.
- Automated Alerts and Notifications: SIEM systems generate automated alerts and notifications when predefined security thresholds or anomalies are detected. This ensures that security teams are promptly informed of potential issues, allowing them to take swift action to address security incidents.
- Compliance Management: SIEM plays a crucial role in helping organizations meet regulatory compliance requirements. By providing centralized visibility and reporting capabilities, SIEM facilitates the monitoring and documentation of security events, which is essential for compliance audits.
- User and Entity Behavior Analytics (UEBA): SIEM systems often incorporate UEBA, which focuses on analyzing the behavior of users and entities within the network. This helps identify abnormal activities that may indicate insider threats or compromised accounts.
- Integration with Security Technologies: SIEM solutions can integrate with a wide range of security technologies, such as firewalls, antivirus solutions, and intrusion detection systems. This integration enhances the overall effectiveness of the security infrastructure by providing a centralized platform for monitoring and managing diverse security tools.

- Threat Intelligence Integration: SIEM systems can be integrated with threat intelligence feeds to enhance their ability to detect and respond to known threats. This integration ensures that organizations have access to up-to-date information about emerging threats and vulnerabilities.
- Forensic Analysis: SIEM solutions support forensic analysis by retaining historical data and logs. This capability is valuable for post-incident investigations, helping organizations understand the root cause of security incidents and improve their overall security posture.
- Scalability: SIEM solutions are scalable, allowing organizations to adapt to changes in their infrastructure size and complexity. Whether an organization grows or undergoes changes in its technology stack, SIEM can scale to meet evolving security needs.

In summary, SIEM solutions provide a comprehensive and centralized approach to managing security information and events, offering organizations enhanced visibility, rapid incident response, and improved overall cybersecurity posture. The benefits of SIEM extend across various sectors, making it a critical tool in the ongoing battle against cyber threats.

Agent-Based SIEM:

Agent-based SIEM systems use software agents installed on individual devices or endpoints within the network. These agents are responsible for collecting and forwarding security-related information to the central SIEM platform.

Advantages:

- Granular Visibility: Agents provide granular visibility into the security events and activities on individual devices.
- Real-Time Monitoring: Agents can facilitate real-time monitoring and immediate response to security incidents.
- Reduced Network Traffic: Since agents filter and forward only relevant data, they can help reduce network traffic associated with event data.

Agentless SIEM:

Agentless SIEM solutions collect security event data without requiring the installation of dedicated software agents on individual devices. Instead, they leverage existing protocols and mechanisms to gather information.

Advantages:

- Simplified Deployment: Agentless solutions often have simpler deployment processes as they don't require software installations on each device.
- Lower Resource Impact: Since there are no agents consuming resources on devices, there is no additional impact on system performance.

XDR

Extended Detection and Response (XDR) is a comprehensive cybersecurity concept designed to enhance organizations' ability to detect, investigate, and respond to sophisticated cyber threats. In the rapidly evolving landscape of cyber threats, traditional security measures like antivirus software and firewalls are no longer sufficient. XDR represents a strategic evolution beyond traditional endpoint detection and response (EDR) solutions by extending its scope across multiple security layers.

At its core, XDR integrates data from various security sources, including endpoints, networks, and cloud environments, to provide a holistic and contextualized view of potential threats. By aggregating and correlating data from different security tools, XDR enhances the ability to detect complex attacks that may span multiple vectors and stages of the cyber kill chain.

XDR typically includes capabilities such as endpoint detection and response (EDR), network traffic analysis (NTA), user and entity behavior analytics (UEBA), and threat intelligence. This convergence of technologies allows security teams to analyze and respond to incidents more efficiently and with greater precision. The continuous monitoring of endpoints and networks, coupled with advanced analytics, helps identify abnormal patterns or behaviors that may indicate a security incident.

One of the key advantages of XDR is its focus on automation and orchestration. By automating routine tasks and response actions, XDR empowers security teams to prioritize and address threats more rapidly, reducing the dwell time of malicious actors within an environment. Automated responses can include isolating compromised endpoints, blocking malicious network traffic, or even initiating incident response workflows.

Furthermore, XDR emphasizes the importance of context in threat analysis. By correlating data across different security domains, it provides a more accurate understanding of the relationships between various events, helping security analysts make informed decisions. This contextual awareness is crucial in distinguishing between legitimate activities and potential security incidents.

As cyber threats become increasingly sophisticated and multifaceted, XDR represents a proactive approach to cybersecurity, providing organizations with a unified and streamlined defense mechanism. By integrating diverse security technologies and promoting collaboration across security domains, XDR aims to bolster the resilience of organizations against the evolving threat landscape. Implementing XDR can significantly enhance the overall security posture, enabling organizations to respond effectively to the challenges posed by modern cyber threats.

FIREWALL

A firewall is a fundamental component of network security, acting as a barrier between a private internal network and external networks, such as the internet. It functions as a protective shield by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a barrier that prevents unauthorized access and protects the integrity and confidentiality of the information within a network.

Firewalls operate at the network level and, in some cases, at the application level, enforcing a set of predefined rules to filter and manage data packets. These rules dictate which traffic is allowed, denied, or flagged for further inspection. The two main types of firewalls are hardware firewalls, which are dedicated physical devices, and software firewalls, which are software applications running on servers or network devices.

Stateful inspection is a key feature of modern firewalls. It involves monitoring the state of active connections and making decisions based on the context of the traffic. Unlike simple packet filtering, which evaluates each packet in isolation, stateful inspection considers the entire communication session. This approach enhances the firewall's ability to discern legitimate communication from potential security threats.

Firewalls use a variety of methods to control and secure network traffic. Packet filtering examines data packets and makes decisions based on factors like source and destination addresses, port numbers, and the protocol used. Proxy firewalls act as intermediaries between internal and external systems, forwarding requests on behalf of clients to ensure that direct connections between the two are avoided. Network Address Translation (NAT) is often used to mask internal IP addresses, enhancing privacy and security.

Application-layer firewalls, also known as proxy firewalls, operate at the application layer of the OSI model, providing more granular control over specific applications or services. These firewalls can inspect and filter traffic based on the content of the data payload, allowing for more sophisticated threat detection.

Firewalls are an essential component of a comprehensive cybersecurity strategy, forming the first line of defense against unauthorized access and cyber threats. They play a crucial role in preventing malicious activities such as unauthorized access, data exfiltration, and denial-of-service attacks. As networks continue

to evolve, firewalls remain a critical element in safeguarding digital assets and maintaining the confidentiality and integrity of sensitive information.

IDS/IPS

In the realm of cybersecurity, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are crucial components designed to identify and respond to potential security threats within a network. These systems play pivotal roles in proactively safeguarding digital assets, ensuring the integrity and confidentiality of data, and mitigating the risks associated with cyberattacks.

Intrusion Detection Systems (IDS):

An IDS is a monitoring tool that scrutinizes network and/or system activities to detect and alert on suspicious or anomalous behavior. The primary objective is to identify potential security incidents by analyzing patterns and deviations from established baselines. IDS operates in two main modes: signature-based and anomaly-based detection.

- Signature-Based Detection: This approach involves comparing observed activities against a database of known attack signatures or patterns. If a match is found, the IDS raises an alert. Signature-based detection is effective against known threats but may struggle with new or sophisticated attacks that lack predefined signatures.

- Anomaly-Based Detection: Anomaly-based IDS focuses on defining a baseline of normal network behavior and alerting on deviations from that baseline. This method is more adept at detecting novel or previously unseen attacks but may generate false positives if the baseline is not accurately calibrated.

IDS can be network-based, monitoring network traffic, or host-based, inspecting activities on individual devices. Deployment of IDS contributes to early threat detection, aiding security teams in investigating and responding to potential incidents promptly. However, IDS does not actively block or prevent malicious activities; it solely serves to raise alarms for further investigation.

Intrusion Prevention Systems (IPS):

IPS, on the other hand, builds upon the capabilities of IDS by not only detecting but also actively preventing or blocking malicious activities. An IPS operates inline with network traffic and can take immediate action to thwart potential threats. It combines the detection mechanisms of IDS with the ability to enforce security policies and respond in real-time.

- Signature-Based Prevention: Similar to IDS, IPS utilizes signature-based detection to identify known threats and employs predefined rules to block or allow traffic accordingly. This method is effective against recognized attack patterns but may be less adaptive to new or evolving threats.

- Anomaly-Based Prevention: IPS may also incorporate anomaly-based detection to identify deviations from normal behavior and block traffic that exhibits suspicious patterns. This helps in preventing previously unseen attacks but requires a robust baseline for accurate detection.

The integration of both IDS and IPS into a comprehensive cybersecurity strategy enhances an organization's ability to detect and respond to security incidents. IDS provides early warning by identifying potential threats, while IPS actively blocks or mitigates these threats in real-time. Together, they create a layered defense mechanism, fortifying networks against a broad spectrum of cyber threats, including viruses, malware, and various forms of cyberattacks.

However, it's important to note that while these systems are powerful tools, they should be part of a broader cybersecurity framework that includes regular updates, threat intelligence, and other proactive measures to

stay ahead of the evolving threat landscape. Additionally, the configuration of IDS and IPS requires careful tuning to minimize false positives and negatives, ensuring effective and accurate threat detection and prevention.

EDR

Endpoint Detection and Response (EDR) is a cybersecurity solution focused on identifying and mitigating security threats at the endpoint level, such as individual devices like computers, servers, and mobile devices. In the ever-evolving landscape of cyber threats, traditional security measures often fall short in detecting and responding to sophisticated attacks. EDR addresses this gap by providing advanced capabilities for monitoring, analyzing, and responding to suspicious activities on endpoints.

Key Components and Capabilities of EDR:

- Continuous Monitoring: EDR solutions continually monitor endpoint activities in real-time. This includes file and process executions, registry changes, network connections, and user behavior. The constant surveillance allows for the early detection of anomalies and potential security incidents.
- Behavioral Analysis: EDR employs behavioral analysis to establish a baseline of normal behavior for each endpoint. Deviations from this baseline can be indicative of malicious activity. By understanding the typical actions of users and applications, EDR can identify anomalies that may signify a security threat.
- Threat Intelligence Integration: EDR systems are often integrated with threat intelligence feeds, incorporating up-to-date information about known malware, attack patterns, and indicators of compromise. This integration enhances the system's ability to identify and respond to emerging threats.
- Incident Investigation and Response: When a potential threat is detected, EDR provides tools for detailed investigation. Security analysts can review historical endpoint data, track the progression of an incident, and understand the scope and impact. Additionally, EDR allows for response actions, such as isolating an infected endpoint or blocking malicious processes.
- Endpoint Isolation: EDR solutions can isolate compromised endpoints to prevent the lateral movement of threats within a network. This containment capability helps minimize the potential impact of an attack by restricting the compromised system's communication with other network resources.
- Forensic Analysis: EDR tools often include forensic capabilities, enabling security teams to conduct in-depth analyses of security incidents. This involves examining artifacts left by malicious activities, understanding the attack vectors, and gathering evidence for post-incident investigations.
- Integration with SIEM: EDR solutions can be integrated with SIEM systems, creating a synergistic relationship between endpoint data and broader network security information. This integration provides a comprehensive view of the organization's security posture.
- Automation and Orchestration: To cope with the speed and volume of modern cyber threats, EDR often incorporates automation and orchestration. Automated responses can include isolating endpoints, blocking malicious activities, and even initiating predefined incident response workflows.

Benefits of EDR:

- Early Threat Detection: EDR provides early detection of potential security incidents by monitoring endpoint activities in real-time and identifying anomalous behavior.
- Effective Incident Response: With detailed visibility into endpoint activities, EDR facilitates swift and effective incident response. Security teams can quickly investigate and mitigate threats, minimizing the impact of security incidents.
- Adaptability to Evolving Threats: EDR's behavioral analysis and threat intelligence integration make it adaptable to new and evolving threats. It can detect and respond to previously unseen attack techniques.

- Endpoint Isolation for Containment: The ability to isolate compromised endpoints helps prevent the lateral spread of threats within a network, limiting the potential damage caused by a security incident.
- Forensic Capabilities: EDR supports forensic analysis, allowing organizations to conduct in-depth investigations, understand the root cause of incidents, and gather evidence for post-incident analysis or legal purposes.

In conclusion, EDR plays a critical role in modern cybersecurity strategies, providing organizations with the tools needed to detect, respond to, and mitigate threats at the endpoint level. As cyber threats continue to evolve, EDR's capabilities are essential for maintaining a robust and adaptive defense against a wide range of security risks.

ANTIMALWARE SOLUTIONS

Antimalware solutions, also known as antivirus, are essential components of cybersecurity designed to detect, prevent, and remove malicious software, commonly referred to as malware. Malware encompasses a wide range of harmful software, including viruses, worms, Trojans, spyware, adware, ransomware, and other types of malicious code. Antimalware solutions play a crucial role in protecting computer systems and networks from these threats.

Key Features and Functionalities of Antimalware Solutions:

- Signature-Based Detection: Traditional antimalware solutions often use signature-based detection. They maintain a database of known malware signatures, which are unique characteristics or patterns associated with specific malicious programs. When scanning files or processes, the software compares them to these signatures to identify and quarantine known threats.
- Heuristic Analysis: In addition to signature-based detection, many antimalware solutions use heuristic analysis to identify potential threats based on behavior or characteristics that may indicate malicious intent. This allows the software to detect and respond to new or previously unknown malware by recognizing suspicious patterns.
- Behavioral Monitoring: Antimalware solutions monitor the behavior of programs and processes in real-time. If a program behaves in a way consistent with malware (e.g., attempting to modify critical system files or accessing sensitive data), the antimalware software can take action to prevent further malicious activity.
- Real-Time Protection: Antimalware solutions provide real-time protection by actively scanning files, downloads, and system activities as they occur. This proactive approach helps prevent malware from executing and causing harm before it can compromise the system.
- Automatic Updates: To stay effective against new and evolving threats, antimalware solutions regularly receive updates to their databases of malware signatures and heuristic algorithms. Automatic updates ensure that the software remains current and capable of identifying the latest threats.
- Quarantine and Removal: When a potential threat is detected, antimalware solutions often quarantine the affected files or isolate the malicious code to prevent it from spreading. Users are then alerted, and they can choose to remove or further investigate the quarantined items.
- Scanning Options: Antimalware solutions typically offer various scanning options, including full system scans, quick scans, and custom scans. Full system scans check all files and processes on the computer, while quick scans focus on critical areas, providing a balance between thoroughness and speed.
- Email and Web Protection: Many antimalware solutions extend their protection to email and web activities. They scan email attachments, links, and web pages for potential threats, helping to block malicious content before it reaches the user's device.
- Firewall Integration: Some antimalware solutions integrate with firewalls to enhance overall security. The firewall component can monitor and control network traffic, providing an additional layer of protection against external threats.

- Multi-Platform Support: Antimalware solutions are designed to work across various platforms, including Windows, macOS, and Linux. Additionally, many providers offer mobile versions to protect smartphones and tablets from mobile-specific threats.
- Centralized Management: In enterprise environments, antimalware solutions often provide centralized management consoles. This allows administrators to monitor the security status of multiple devices, configure settings, and respond to security incidents from a central location.
- Behavioral Analytics: Advanced antimalware solutions may incorporate behavioral analytics, which involves analyzing the behavior of programs and users over time to identify deviations that may indicate a security threat. This adds an extra layer of sophistication to threat detection.

Antimalware solutions are a fundamental aspect of cybersecurity, serving as a first line of defense against the myriad threats posed by malicious software. It's important for users and organizations to regularly update their antimalware software, practice safe computing habits, and complement these solutions with a comprehensive cybersecurity strategy that includes firewalls, regular backups, and user education.

GRC TOOLS

Governance, Risk, and Compliance (GRC) tools are software solutions designed to help organizations manage their governance, risk management, and compliance activities in an integrated and efficient manner. These tools provide a centralized platform for organizations to streamline processes, ensure regulatory compliance, and make informed decisions related to risk and governance.

Common Categories of GRC Tools:

- Enterprise Risk Management (ERM) Tools: ERM tools assist organizations in identifying, assessing, and managing risks across the entire enterprise. These tools typically provide risk assessment frameworks, risk registers, and risk reporting functionalities. They help organizations prioritize risks, implement risk mitigation strategies, and monitor risk exposure over time.
- Policy Management Tools: Policy management tools enable organizations to create, communicate, and enforce policies and procedures. These tools often include features for policy documentation, version control, distribution, and acknowledgment tracking. They help ensure that employees are aware of and comply with organizational policies.
- Audit Management Tools: Audit management tools facilitate the planning, execution, and tracking of internal and external audits. These tools help organizations manage audit schedules, document findings, track remediation activities, and ensure compliance with regulatory requirements and internal policies.
- Compliance Management Tools: Compliance management tools focus on helping organizations adhere to industry regulations, legal requirements, and internal policies. They provide features for mapping regulations to internal controls, tracking compliance status, and generating compliance reports. These tools are particularly valuable in highly regulated industries.
- Incident Management Tools: Incident management tools assist organizations in recording, tracking, and responding to various incidents, including security incidents, data breaches, and compliance violations. They often include workflows for incident reporting, investigation, and resolution.
- IT GRC Tools: IT Governance, Risk, and Compliance (IT GRC) tools specifically address the challenges related to information technology governance and risk management. These tools help organizations align IT activities with business objectives, manage IT risks, and ensure compliance with IT-related regulations.
- Vendor Risk Management Tools: Vendor risk management tools help organizations assess and manage the risks associated with third-party vendors and suppliers. These tools typically include features for vendor risk assessments, due diligence, and ongoing monitoring of vendor compliance and performance.
- Business Continuity Management (BCM) Tools: BCM tools assist organizations in developing and maintaining business continuity plans. These plans outline strategies for ensuring business operations can continue in the face of disruptions, such as natural disasters, cybersecurity incidents, or other emergencies.

- Data Governance Tools: Data governance tools focus on managing and ensuring the quality, integrity, and security of an organization's data. They often include features for data classification, data lineage tracking, and enforcing data access and usage policies.
- Regulatory Change Management Tools: Regulatory change management tools assist organizations in tracking and managing changes in regulations and legal requirements that may impact their operations. These tools help organizations stay informed about regulatory updates and adjust their compliance efforts accordingly.

It's important to note that GRC tools vary in their features and capabilities, and organizations may choose a combination of tools based on their specific needs, industry requirements, and regulatory environment. Integrating GRC tools into an organization's overall risk management and governance strategy can enhance efficiency, transparency, and the ability to adapt to a rapidly changing business landscape.

HSM

Hardware Security Module (HSM) is a specialized hardware device designed to provide a secure and tamper-resistant environment for cryptographic operations and key management. HSMs play a critical role in enhancing the security of sensitive data and cryptographic processes within various applications and industries.

Key Characteristics and Functions of HSM:

- Secure Key Storage: One of the primary functions of an HSM is to securely store cryptographic keys used for encryption, decryption, digital signatures, and other cryptographic operations. HSMs are designed with robust physical and logical security mechanisms to protect these keys from unauthorized access and tampering.
- Cryptographic Operations: HSMs perform various cryptographic operations, including encryption and decryption using symmetric and asymmetric algorithms, digital signatures, and random number generation. These operations are executed within the secure confines of the HSM, preventing exposure of sensitive key material.
- Key Generation and Management: HSMs often include functionality for generating and managing cryptographic keys securely. Key generation processes within an HSM are typically conducted using a true random number generator, ensuring the unpredictability and strength of the keys.
- Secure Execution Environment: HSMs provide a secure and isolated execution environment for cryptographic operations. This protection is crucial to prevent attacks such as side-channel attacks or attempts to extract cryptographic keys through various means.
- Hardware-based Random Number Generation: HSMs incorporate hardware-based random number generators to ensure the generation of high-quality random numbers. These random numbers are critical for cryptographic protocols and applications requiring unpredictability.
- Secure Communication: HSMs often support secure communication protocols to allow external systems or applications to interact with the HSM securely. This ensures that cryptographic operations and key management activities are conducted in a protected and authenticated manner.
- Compliance with Standards: HSMs are designed to comply with industry standards and regulations governing cryptographic operations and key management. Compliance with standards such as FIPS 140-2 (Federal Information Processing Standard) is common for HSMs used in government and sensitive industries.
- Tokenization: Some HSMs support tokenization, a technique used to replace sensitive data with a non-sensitive equivalent (token). This helps protect sensitive information, such as credit card numbers, by ensuring that the actual data is stored securely within the HSM.

HSM Use Cases:

- Financial Services: HSMs are extensively used in the financial industry to secure transactions, manage cryptographic keys for securing sensitive financial data, and ensure compliance with regulatory requirements.

- Payment Processing: Payment systems and point-of-sale (POS) terminals leverage HSMs to secure transactions, encrypt payment information, and protect cryptographic keys associated with payment processing.
- Cloud Services: Cloud service providers use HSMs to secure and manage cryptographic keys for encrypting data at rest, securing communication between cloud services, and ensuring the integrity of cryptographic operations in a cloud environment.
- Government and Defense: Government agencies and defense organizations deploy HSMs to secure sensitive communications, protect classified information, and ensure the integrity of cryptographic systems.
- Healthcare: In the healthcare industry, HSMs are used to secure electronic health records (EHRs), protect patient data, and ensure the confidentiality and integrity of healthcare-related information.
- Manufacturing and IoT: Industries involved in manufacturing and the Internet of Things (IoT) use HSMs to secure communication between devices, authenticate devices, and protect sensitive information in connected environments.
- HSMs are a fundamental component in building a secure infrastructure for cryptographic operations, ensuring the confidentiality, integrity, and availability of sensitive information in a wide range of applications and industries.

DLP

DLP stands for Data Loss Prevention, which is a comprehensive approach to protecting sensitive information from unauthorized access, disclosure, or exfiltration. DLP solutions and strategies aim to prevent the accidental or intentional leakage of sensitive data, including personal information, intellectual property, financial records, and other confidential data.

Key Components and Features of DLP:

- Content Discovery: DLP solutions often include content discovery mechanisms to identify and locate sensitive data within an organization's network. This involves scanning files, databases, emails, and other repositories to detect patterns or content that match predefined criteria for sensitivity.
- Policy Enforcement: DLP solutions enable organizations to define and enforce policies that dictate how sensitive data should be handled. Policies can include rules for data encryption, access controls, data sharing, and other measures to prevent data breaches or leaks.
- Endpoint Protection: DLP extends to endpoints, such as laptops, desktops, and mobile devices. Endpoint DLP solutions monitor and control the flow of data on individual devices, preventing unauthorized transfers or leakage of sensitive information.
- Network Monitoring and Filtering: DLP solutions monitor network traffic in real-time, analyzing data packets for sensitive content. They can block or quarantine data that violates established policies, helping to prevent the unauthorized transmission of sensitive information over the network.
- Email Security: DLP is often integrated into email security solutions to prevent the unauthorized sharing of sensitive information through email. This includes scanning email content and attachments for sensitive data and enforcing policies to control email communication.
- Cloud Security: With the increasing use of cloud services, DLP extends to cloud security, helping organizations protect sensitive data stored in cloud environments. DLP solutions for the cloud monitor and control data transfers, ensuring compliance with security policies.
- Incident Response and Reporting: DLP solutions provide incident response capabilities, alerting security teams when policy violations occur. They also generate reports and logs for auditing purposes, helping organizations assess their security posture and respond to incidents effectively.
- Integration with Other Security Technologies: DLP is often integrated with other security technologies such as firewalls, SIEMs, data discovery/classification tools and identity and access management solutions to create a comprehensive security infrastructure.

DLP is critical for organizations across various industries, especially those handling sensitive data subject to regulatory compliance requirements. It helps mitigate the risks associated with data breaches, intellectual property theft, and accidental data exposure. Implementing a robust DLP strategy involves a combination of technology, policies, and user education to create a holistic approach to data protection.

DATA CLASSIFICATION TOOLS

Data classification tools are software solutions designed to automate the process of categorizing and labeling data based on its sensitivity, value, and the level of protection required. These tools play a crucial role in data governance, helping organizations manage and secure their information assets by assigning appropriate classifications to data.

Key Features and Functionalities of Data Classification Tools:

- Automated Classification: Data classification tools automate the process of assigning classification labels to data based on predefined policies and rules. This includes identifying sensitive information, intellectual property, personally identifiable information (PII), or other categories of data that require specific handling.
- Content Discovery: Many data classification tools include content discovery mechanisms to scan and analyze data across various repositories, including file servers, databases, email systems, and cloud storage. These tools help identify sensitive data, even if it is stored in unstructured formats.
- Policy-Based Classification: Data classification tools allow organizations to define policies that determine how data should be classified. These policies may consider factors such as keywords, file types, context, or patterns to automatically classify data according to established criteria.
- User-Driven Classification: Some tools empower end-users to classify data based on their knowledge of the content. This can involve providing users with classification options within applications, email clients, or file systems, allowing them to make informed decisions about the sensitivity of the data they handle.
- Integration with Data Loss Prevention (DLP): Data classification tools often integrate with Data Loss Prevention (DLP) solutions. The classification information helps DLP systems enforce policies related to data protection, preventing unauthorized access or transmission of sensitive information.
- Metadata Tagging: Data classification tools often add metadata tags to files or records, indicating their classification. This metadata helps in tracking and managing data throughout its lifecycle, facilitating search, retrieval, and auditing processes.
- Reporting and Auditing: Data classification tools generate reports and logs to provide insights into the distribution of classified data, compliance with policies, and potential risks. These reports are valuable for audits, regulatory compliance, and overall data governance.
- Integration with Information Rights Management (IRM): Some data classification tools integrate with Information Rights Management (IRM) solutions to extend control over how classified information is used. IRM helps enforce access and usage policies, even when data is shared outside the organization.
- Machine Learning and Contextual Analysis: Advanced data classification tools may leverage machine learning and contextual analysis to improve accuracy. They can learn from user behavior, adapt to evolving data patterns, and enhance the precision of automated classification.

Implementing data classification tools is essential for organizations seeking to establish effective data governance, comply with regulatory requirements, and protect sensitive information. By automating the classification process, these tools contribute to a more proactive and consistent approach to data management and security.

VULNERABILITY SCANNER

A vulnerability scanner is a cybersecurity tool designed to identify and assess security vulnerabilities in computer systems, networks, applications, and other IT infrastructure. The primary goal of vulnerability

scanning is to proactively discover weaknesses in a system's security posture before malicious actors can exploit them. By identifying vulnerabilities, organizations can take corrective actions to strengthen their defenses and reduce the risk of security incidents.

Main features of vulnerability scanners:

- Automated Scanning: Vulnerability scanners automate the process of scanning networks, systems, and applications to identify potential security vulnerabilities. Automated scanning allows for a comprehensive and systematic examination of a large number of assets within a relatively short timeframe.
- Network and Host Scanning: Vulnerability scanners can perform both network and host-based scans. Network scanning involves examining the entire network to identify devices and open ports, while host scanning focuses on individual systems to find vulnerabilities in operating systems and installed applications.
- Application Scanning: Application vulnerability scanners specifically target web applications, APIs, and other software to identify vulnerabilities such as code flaws, misconfigurations, and potential security weaknesses in the application layer.
- Database Scanning: Some vulnerability scanners include capabilities to scan databases for potential vulnerabilities. This includes identifying weak access controls, misconfigurations, and vulnerabilities related to database security.
- Credential-Based Scanning: In some cases, vulnerability scanners use authenticated or credential-based scanning. This involves providing the scanner with valid credentials to access systems and applications, allowing for a more accurate assessment of vulnerabilities that require authenticated access to be identified.
- Compliance Checks: Vulnerability scanners often include checks for compliance with industry standards and regulations. This helps organizations ensure that their systems adhere to security best practices and meet specific compliance requirements.
- Risk Prioritization: Vulnerability scanners assess the severity of identified vulnerabilities and prioritize them based on the potential risk they pose. This helps organizations focus their efforts on addressing the most critical security issues first.
- Reporting and Analysis: Vulnerability scanners generate detailed reports that provide information about identified vulnerabilities, their severity, and recommendations for remediation. These reports are valuable for security teams, IT administrators, and other stakeholders involved in the remediation process.
- Integration with Other Security Tools: Many vulnerability scanners can integrate with other security tools, such as Security Information and Event Management (SIEM) systems and patch management solutions. Integration enhances the overall security ecosystem by facilitating coordinated responses to vulnerabilities.
- Continuous Monitoring: Some modern vulnerability scanners offer continuous monitoring capabilities, allowing organizations to regularly scan and monitor their infrastructure for new vulnerabilities and changes in the security landscape.
- Penetration Testing Collaboration: While vulnerability scanners focus on identifying vulnerabilities, they may collaborate with penetration testing tools and teams to validate and simulate real-world attack scenarios. This combination helps organizations comprehensively assess and improve their security posture.

By regularly conducting vulnerability scans, organizations can identify and address security weaknesses proactively, reducing the likelihood of successful cyberattacks. Vulnerability scanning is an integral part of a broader cybersecurity strategy aimed at maintaining a resilient and secure IT environment.

Main Types of Vulnerability Scanners:

- Network Vulnerability Scanners: Network vulnerability scanners focus on identifying weaknesses within the network infrastructure. They scan devices, servers, routers, switches, and other network

components to discover vulnerabilities such as open ports, misconfigurations, and potential points of exploitation.

- Host-Based Vulnerability Scanners: Host-based vulnerability scanners concentrate on individual systems or hosts, examining the operating system, installed applications, and system configurations. These scanners help identify vulnerabilities specific to the host's environment, including missing patches, weak configurations, and software vulnerabilities.
- Web Application Scanners: Web application scanners are designed to identify security vulnerabilities within web applications and APIs. They analyze the application's code, structure, and behavior to uncover common issues such as SQL injection, cross-site scripting (XSS), and insecure configurations.
- Database Vulnerability Scanners: Database vulnerability scanners focus on identifying weaknesses within database management systems (DBMS). They examine access controls, configurations, and potential vulnerabilities related to database security to ensure that sensitive data is adequately protected.
- Cloud-Based Vulnerability Scanners: With the rise of cloud computing, some vulnerability scanners are specifically designed to assess the security of cloud-based infrastructure and services. These scanners check for misconfigurations, insecure interfaces, and other vulnerabilities in cloud environments.
- Wireless Network Scanners: Wireless network scanners concentrate on identifying vulnerabilities within wireless networks. They assess the security of Wi-Fi networks, examining encryption protocols, authentication mechanisms, and potential vulnerabilities that could be exploited by unauthorized users.
- Passive Scanners: Passive scanners monitor network traffic passively, without actively sending packets or probes. They analyze network traffic and identify vulnerabilities and potential security issues by observing communication patterns and behaviors.
- Active Scanners: Active scanners interact directly with the target system by sending probes, packets, or requests to discover vulnerabilities actively. Active scanners are more intrusive but can provide a more comprehensive assessment of potential security issues.
- Open-Source Vulnerability Scanners: Open-source vulnerability scanners are community-driven tools that organizations can use without purchasing commercial licenses. These tools are often customizable and may offer a cost-effective solution for security assessments.

NETWORK SCANNER

A network scanning tool is software designed to identify devices, open ports, and vulnerabilities within a computer network. Network scanning tools serve the purpose of evaluating and understanding the security state of a computer network by examining its components, identifying potential vulnerabilities, and providing insights for security improvements.

Main Features of Network Scanners:

- Device Discovery: These tools actively search and identify devices connected to a network, allowing administrators to maintain an inventory of devices and track changes in the network's composition.
- Port Scanning: Port scanning is a technique used by network scanning tools to discover open ports on devices. Open ports represent potential entry points for attackers and need to be monitored and secured.
- Vulnerability Detection: Network scanning tools analyze devices for known vulnerabilities, providing information to security teams about potential weaknesses that could be exploited by malicious actors.
- Mapping Network Topology: Network scanning helps create a map of the network's topology, illustrating how devices are interconnected. This visualization aids administrators in understanding the layout of the network.

- Network Inventory: By identifying and cataloging connected devices, network scanning tools assist in maintaining a comprehensive inventory. This inventory is essential for effective network management, resource allocation, and security assessment.
- Security Audits: Network scanning is a fundamental component of security audits, allowing organizations to regularly assess the security of their networks, identify vulnerabilities, and implement corrective measures.
- Automation: Automation is a key feature of network scanning tools. These tools can perform scans automatically, saving time for administrators and providing up-to-date information on the network's security status.
- IP Address Management: Network scanning tools aid in the management of IP addresses by tracking allocations, identifying unused addresses, and ensuring proper assignment to devices.
- Policy Enforcement: Network scanning tools contribute to enforcing security policies by identifying areas of non-compliance, allowing organizations to address deviations and maintain a secure network environment.

In summary, network scanning tools are essential for maintaining a secure and well-managed network infrastructure. They automate the process of discovering and assessing devices, ports, and vulnerabilities, providing valuable information for security teams to enhance the overall security posture of the network.

HUMAN ASPECT

Success of any SOC relies heavy on the people that it employs. It is crucial to attract highly skilled and knowledgeable staff to reach to the maximum effectiveness and efficiency. In this section, the most common workforce frameworks will be presented and the single most common one will be selected to investigate in more detail.

These frameworks are:

1. NIST NICE (National Initiative for Cybersecurity Education) Framework:

NICE Framework [12] is the most common and comprehensive reference for cybersecurity roles. Its latest version includes 7 categories, 33 Specialty Areas under those categories and 52 cybersecurity roles as well. It is highly modular, meaning the readers can pick and choose which roles fit their organizations and then use those role definitions as reference to close the skill gaps.

Each role definition adopts a building block approach, making it even more modular, as described in the figure below:

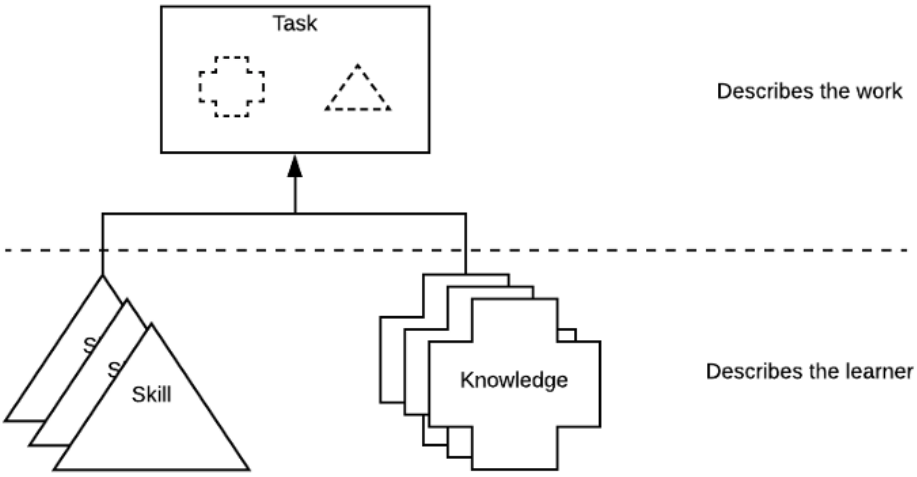

Figure 1 NICE Framework Building Blocks

NICE Framework is the selected framework to describe the workforce requirements of a typical SOC. Out of 52 roles 20 of them have been selected for this work and their details can be found in Appendix-1.

2. SFIA (Skills Framework for the Information Age)

The Skills Framework for the Information Age (SFIA) [13] is a global skills and competency framework for the digital world. It defines the skills and competencies required by business and technology professionals who design, develop, implement, manage, and protect the data and technology that power the digital world.

SFIA covers many of the world's most in-demand occupations, such as information and cyber security, software engineering, digital product development, and user-centered design. It is flexible, generic, and updated by real practitioners.

The framework is structured into 7 levels of responsibility, each characterized by generic attributes which describe behavioral factors, along with professional skills and competencies described at one or more of

those 7 levels. Many roles in the industry are blended and require a mix of technical and non-technical skills, and SFIA is ideally suited to this.

SFIA 8 is the latest version of the framework. SFIA Framework offers skill profiles that are collections of skills to look for in a role. For cybersecurity, it offers 4 skill profiles:

Information and cyber security role family		
Role: Security leadership, strategy and management	Roles responsible for leading the development and execution of security strategies and policies.	
Example Job Titles:	Look at these SFIA skills first:	Other SFIA skills to consider:
Chief Information Security Officer CISO, Information security manager, Security architect, Information security analyst, Cyber security manager, Cyber security governance manager, Cyber security analyst	Information security SCTY Governance GOVN Risk management BURM Information management IRMG Information assurance INAS Stakeholder relationship management RLMT	Organisational capability development OCDV Enterprise and business architecture STPL Measurement MEAS

Table 1 SFIA Security Leadership, Strategy and Management

Information and cyber security role family		
Role: Security operations	Roles responsible for day to day execution of security policies and procedures. Using monitoring tools to identify threats and incidents.	
Example Job Titles:	Look at these SFIA skills first:	Other SFIA skills to consider:
Cyber Security Technician, Information Security Technician, Security Operations Manager, Infrastructure Specialist, Operations Support Analyst, Security Operations Centre (SOC) Service Desk Analyst, Security Operations Centre (SOC) Analyst	Security operations SCAD IT infrastructure ITOP Incident management USUP Network support NTAS System software SYSP Information security SCTY Asset management ASMG Supplier management SUPP Technology service management ITMG	Measurement MEAS Specialist advice TECH Knowledge management KNOW Software configuration PORT Systems installation and removal HSIN Problem management PBMG Facilities management DCMA Stakeholder relationship management RLMT Risk management BURM Penetration testing PENT

Table 2 SFIA Security Operations

Information and cyber security role family		
Role: Security risk management, audit and compliance	Roles responsible for assessing risk and ensuring security systems and operations comply with organisational and regulatory requirements.	
Example Job Titles:	Look at these SFIA skills first:	Other SFIA skills to consider:
IT auditor, Info sec compliance consultant, Security assessment auditor, Audit manager, Security leadership, strategy and management	Information assurance INAS Risk management BURM Testing TEST Audit AUDT	Consultancy CNSL Measurement MEAS

Table 3 SFIA Security Risk Management, Audit and Compliance

Information and cyber security role family		
Role: Incident management practitioners	Roles responsible for analysing, designing, managing and delivering the services required to minimise the negative impact of security incidents and restoring normal service operation as quickly as possible.	
Example Job Titles:	Look at these SFIA skills first:	Other SFIA skills to consider:
Incident Analyst, Incident Manager, Major Incident Manager, Lead Incident Manager, Cyber Incident Manager	Incident management USUP Security operations SCAD Digital forensics DGFS	Continuity management COPL Information security SCTY Testing TEST Supplier management SUPP Stakeholder relationship management RLMT Methods and tools METL Business intelligence BINT

Table 4 SFIA Incident Management Practitioners

3. ENISA European Cybersecurity Skills Framework (ECSF)

The European Cybersecurity Skills Framework (ECSF) [14] is a practical tool designed to support the identification and articulation of tasks, competences, skills, and knowledge associated with the roles of European cybersecurity professionals. It serves as the EU reference point for defining and assessing relevant skills.

The ECSF summarizes the cybersecurity-related roles into 12 profiles, each analyzed in detail for their corresponding responsibilities, skills, synergies, and interdependencies. This facilitates recognition of cybersecurity skills and supports the design of cybersecurity-related training programs.

The ECSF was presented during the 1st ENISA cybersecurity skills conference in September 2022. In April 2023, the Commission adopted the Communication on a Cybersecurity Skills Academy, a policy initiative aiming to bring together existing initiatives on cyber skills and improve their coordination[1]. The ECSF forms the basis on which the Academy will define and assess relevant skills, monitor the evolution of the skill gaps, and provide indications on the new needs.

Figure 2 ECSF Role Profiles

For this project, NIST NICE Framework has been selected as reference model because it is:

- Modular,
- Most utilized,
- Most comprehensive and
- Most cybersecurity focused.

Here are the work profiles selected from NICE Framework that are determined to be crucial for any SOC's function:

Role Category - Analyze: Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

- Exploitation Analyst: Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
- Threat/Warning Analyst: Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.

Role Category - Collect and Operate: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

- Cyber Operator: Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.

Role Category - Investigate: Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

- Cyber Defense Forensics Analyst: Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Role Category - Operate and Maintain: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

- Technical Support Specialist: Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
- Data Analyst: Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
- Network Operations Specialist: Plans, implements, and operates network services/systems, to include hardware and virtual environments.
- System Administrator: Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
- Systems Security Analyst: Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Role Category - Oversee and Govern: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

- Information Systems Security Manager: Responsible for the cybersecurity of a program, organization, system, or enclave.
- Executive Cyber Leadership: Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
- Cyber Policy and Strategy Planner: Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
- Cyber Workforce Developer and Manager: Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
- Cyber Instructor: Develops and conducts training or education of personnel within cyber domain.

Role Category - Protect and Defend: Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

- Cyber Defense Analyst: Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
- Cyber Defense Incident Responder: Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
- Vulnerability Assessment Analyst: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from

acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Role Category - Securely Provision: Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

- Security Control Assessor: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
- Security Architect: Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
- System Testing and Evaluation Specialist: Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

SOC GOVERNANCE

PERFORMANCE MEASUREMENT AND KPIS

Key Performance Indicators (KPIs) for Security Operations Centers (SOCs) are essential metrics that help assess the effectiveness and efficiency of security monitoring, incident response, and overall cybersecurity efforts. Here are some KPI examples for Security Operation Centers:

1. Mean Time to Detect (MTTD): The average time taken to detect a security incident from the moment it occurs. A lower MTTD indicates quicker detection, allowing for faster response to security incidents.
2. Mean Time to Respond (MTTR): The average time taken to respond and mitigate a security incident after its detection. A lower MTTR suggests efficient incident response capabilities, minimizing potential damage.
3. Incident Closure Rate: The percentage of incidents that are successfully resolved and closed. A high closure rate indicates effective incident management and resolution processes.
4. False Positive Rate: The percentage of alerts or incidents that are determined to be false positives upon investigation. A lower false positive rate reduces the workload on security analysts and ensures accurate alert prioritization.
5. Incident Severity Levels: Categorizing incidents based on severity levels (e.g., low, medium, high). Helps prioritize responses based on the potential impact of incidents on the organization.
6. Percentage of Incidents Investigated: The proportion of detected incidents that undergo a thorough investigation. Ensures that all potential security incidents are properly examined, minimizing the risk of overlooking threats.
7. Escalation Rate: The percentage of incidents that require escalation to higher-level response teams or management. Indicates the complexity of incidents and the effectiveness of tiered response strategies.
8. Percentage of Compliance Violations Detected: The proportion of incidents related to non-compliance with security policies and regulations. Ensures alignment with regulatory requirements and internal security policies.
9. Percentage of Vulnerabilities Remediated: The proportion of identified vulnerabilities that have been successfully mitigated or patched. Measures the efficiency of vulnerability management efforts in reducing potential attack surfaces.
10. User Awareness and Training Effectiveness: Evaluating the success of security awareness programs through simulated phishing exercises or knowledge assessments. Reflects the organization's efforts in improving employee cybersecurity awareness and reducing social engineering risks.
11. Security Incident Trends: Analyzing trends in the volume and types of security incidents over time. Provides insights into evolving threats and helps in strategic planning for enhanced cybersecurity measures.
12. Percentage of Critical Assets Monitored: The proportion of critical assets under continuous monitoring. Ensures that security monitoring efforts prioritize the protection of the most important assets in the organization.

These KPIs can serve as a foundation for assessing the performance and impact of a Security Operations Center. Organizations may tailor these indicators based on their specific security goals, industry requirements, and risk landscape. Regularly monitoring and analyzing these KPIs can help SOC teams refine their strategies and continually improve their cybersecurity capabilities.

INTERNAL AUDIT

Internal audits are integral to ensuring the effectiveness, efficiency, and compliance of Security Operations Centers (SOCs). These audits play a critical role in evaluating the design and functionality of security controls within the SOC, ensuring alignment with industry best practices and organizational security policies. By identifying weaknesses and gaps in processes and procedures, internal audits pinpoint areas that may be vulnerable to security threats or require improvement.

Furthermore, internal audits are essential for compliance assurance, ensuring that the SOC adheres to relevant regulatory requirements, industry standards, and internal policies. They contribute to risk management by evaluating potential risks and assessing the effectiveness of mitigation strategies. Internal audits also assess operational efficiency, including resource allocation, response times, incident resolution processes, and overall personnel performance.

Validating incident response capabilities is a key focus of internal audits, with simulated scenarios assessing the SOC's preparedness for real security incidents. The findings from audits are invaluable for continuous improvement, enabling SOC managers to refine processes, enhance training programs, and implement corrective actions.

Internal audits align SOC activities with broader business objectives, ensuring that security efforts support core business functions. They also validate the effectiveness of security investments, assessing whether implemented solutions contribute to the overall security strategy. Additionally, audits enhance stakeholder confidence by providing assurance to executive leadership, board members, and external regulators that the organization is committed to maintaining a strong cybersecurity posture.

The documentation and reporting resulting from internal audits are crucial for demonstrating compliance, responding to inquiries, and providing evidence of due diligence in cybersecurity practices. In summary, internal audits are fundamental to maintaining a resilient and effective SOC, contributing to risk management, compliance assurance, operational efficiency, and continuous improvement.

VERIFICATION OF RESULTS AND OUTPUTS

Verifying the results of a Security Operations Center (SOC) is a multifaceted process essential for gauging its effectiveness. One crucial aspect involves a comprehensive review of past incidents handled by the SOC. This analysis assesses the efficiency of threat detection, incident response, and the overall mitigation of security events.

Key performance metrics and indicators established for the SOC, such as mean time to detect (MTTD), mean time to respond (MTTR), and incident closure rates, are vital benchmarks. These metrics should be regularly compared against predefined goals to identify areas for improvement. Simulated exercises, ranging from tabletop simulations to red teaming, offer a practical evaluation of the SOC's readiness and response capabilities. These exercises help uncover any weaknesses or gaps that may exist in the team's approach to different security scenarios. Continuous monitoring is a cornerstone of SOC effectiveness. Regularly reviewing alerts generated by security tools ensures the SOC promptly identifies and investigates potential threats. It's crucial to verify the accuracy of alert prioritization and the efficacy of ongoing monitoring efforts.

The implementation and effectiveness of security controls demand scrutiny. This involves reviewing the configurations of security devices, confirming consistent enforcement of security policies, and validating the appropriateness of access controls.

Integration of threat intelligence is another critical aspect. Assess how well the SOC leverages external threat feeds to stay informed about emerging threats and evaluate the impact of threat intelligence on the accuracy and timeliness of threat detection.

The validation of incident response playbooks and procedures ensures the SOC team follows established protocols during incidents. Regular updates to playbooks to address new threat vectors and evolving attack techniques are essential for maintaining relevance.

Assessment of training programs and skill levels of SOC personnel ensures team members are equipped to handle evolving cybersecurity challenges. Skill assessments or certifications can be utilized to validate the competency of SOC analysts. Conducting regular compliance audits ensures the SOC adheres to relevant regulatory requirements and industry standards. This includes frameworks such as ISO 27001, NIST, or industry-specific standards. Soliciting feedback from SOC analysts, incident responders, and stakeholders

provides valuable insights. This feedback, coupled with lessons learned from incidents and exercises, informs improvement plans.

External assessments by third-party entities provide an unbiased evaluation of the SOC's capabilities and identify potential blind spots. These assessments contribute to a more comprehensive understanding of the SOC's strengths and areas for enhancement. A review of documentation, including incident reports, response logs, and documentation of security controls, ensures accuracy and alignment with actual SOC practices. This documentation serves as a critical reference for assessing the SOC's historical performance.

A holistic approach to verification involves assessing incident handling, monitoring metrics, conducting simulations, validating security controls, integrating threat intelligence, refining incident response procedures, ensuring ongoing training, conducting compliance audits, gathering feedback, engaging in external assessments, and reviewing documentation. This comprehensive process ensures a thorough evaluation of the SOC's effectiveness in safeguarding against cybersecurity threats.

REFERENCES

1. NIST SP 800-92 Guide to Computer Security Log Management https://csrc.nist.gov/pubs/sp/800/92/final January 2024

2. NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations https://csrc.nist.gov/pubs/sp/800/137/final January 2024

3. NIST SP 800-150 Guide to Cyber Threat Information Sharing https://csrc.nist.gov/pubs/sp/800/150/final January 2024

4. NIST SP 800-61 Rev.2 Computer Security Incident Handling Guide https://csrc.nist.gov/pubs/sp/800/61/r2/final January 2024

5. NIST SP 800-40 Rev. 4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology https://csrc.nist.gov/pubs/sp/800/40/r4/final January 2024

6. NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final January 2024

7. NIST SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final January 2024

8. NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1 https://csrc.nist.gov/pubs/sp/800/218/final January 2024

9. NIST Risk Management Framework https://csrc.nist.gov/projects/risk-management/about-rmf January 2024

10. NIST SP 800-50 Rev. 1 (Initial Public Draft) Building a Cybersecurity and Privacy Learning Program https://csrc.nist.gov/pubs/sp/800/50/r1/ipd January 2024

11. NIST SP 800-16 Rev. 1 (3rd Public Draft) A Role-Based Model for Federal Information Technology/Cybersecurity Training https://csrc.nist.gov/pubs/sp/800/16/r1/3pd January 2024

12. NIST Workforce Framework for Cybersecurity (NICE Framework) https://niccs.cisa.gov/workforce-development/nice-framework January 2024

13. SFIA - The global skills and competency framework for a digital world. https://sfia-online.org/en January 2024 January 2024

14. European Cybersecurity Skills Framework (ECSF) — ENISA. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework January 2024

APPENDIX

Appendix - 1 Details of Selected NIST NICE Framework Role

Role	Exploitation Analyst
Description	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0009: Knowledge of application vulnerabilities. K0108: Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless). K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). K0131: Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies. K0142: Knowledge of collection management processes, capabilities, and limitations. K0143: Knowledge of front-end collection systems, including traffic collection, filtering, and selection. K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. K0349: Knowledge of website types, administration, functions, and content management system (CMS). K0351: Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation. K0354: Knowledge of relevant reporting and dissemination procedures. K0362: Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.). K0368: Knowledge of implants that enable cyber collection and/or preparation activities. K0371: Knowledge of principles of the collection development processes (e.g., Dialed Number Recognition, Social Network Analysis). K0376: Knowledge of internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc. K0379: Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc. K0388: Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies. K0393: Knowledge of common networking devices and their configurations. K0394: Knowledge of common reporting databases and tools. K0397: Knowledge of concepts for operating systems (e.g., Linux, Unix.) K0417: Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).

	K0418: Knowledge of data flow process for terminal or environment collection. K0430: Knowledge of evasion strategies and techniques. K0443: Knowledge of how hubs, switches, routers work together in the design of a network. K0444: Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP). K0447: Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http). K0451: Knowledge of identification and reporting processes. K0470: Knowledge of Internet and routing protocols. K0471: Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering). K0473: Knowledge of intrusion sets. K0484: Knowledge of midpoint collection (process, objectives, organization, targets, etc.). K0487: Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection). K0489: Knowledge of network topology. K0509: Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives. K0510: Knowledge of organizational and partner policies, tools, capabilities, and procedures. K0523: Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, McAfee, Outpost, and Panda) and how those products affect exploitation and reduce vulnerabilities. K0529: Knowledge of scripting K0535: Knowledge of strategies and tools for target research. K0544: Knowledge of target intelligence gathering and operational preparation techniques and life cycles. K0557: Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.). K0559: Knowledge of the basic structure, architecture, and design of converged applications. K0560: Knowledge of the basic structure, architecture, and design of modern communication networks. K0608: Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).
Skills	S0066: Skill in identifying gaps in technical capabilities. S0184: Skill in analyzing traffic to identify network devices. S0199: Skill in creating and extracting important information from packet captures. S0200: Skill in creating collection requirements in support of data acquisition activities. S0201: Skill in creating plans in support of remote operations. S0204: Skill in depicting source or collateral data on a network map. S0207: Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments. S0214: Skill in evaluating accesses for intelligence value. S0223: Skill in generating operation plans in support of mission and target requirements. S0236: Skill in identifying the devices that work at each level of protocol models. S0237: Skill in identifying, locating, and tracking targets via geospatial analysis techniques S0239: Skill in interpreting compiled and interpretive programming languages. S0240: Skill in interpreting metadata and content as applied by collection systems. S0245: Skill in navigating network visualization software. S0247: Skill in performing data fusion from existing intelligence for enabling new and continued collection. S0258: Skill in recognizing and interpreting malicious network activity in traffic. S0260: Skill in recognizing midpoint opportunities and essential information.

	S0264: Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information). S0269: Skill in researching vulnerabilities and exploits utilized in traffic. S0279: Skill in target development in direct support of collection operations. S0286: Skill in using databases to identify target-relevant information. S0290: Skill in using non-attributable networks. S0294: Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction. S0300: Skill in writing (and submitting) requirements to meet gaps in technical capabilities.
Tasks	T0028: Conduct and/or support authorized penetration testing on enterprise network assets. T0266: Perform penetration testing as required for new or updated applications. T0570: Apply and utilize authorized cyber capabilities to enable access to targeted networks. T0572: Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements. T0574: Apply and obey applicable statutes, laws, regulations and policies. T0591: Perform analysis for target infrastructure exploitation activities. T0600: Collaborate with other internal and external partner organizations on target access and operational issues. T0603: Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers. T0608: Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access. T0614: Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access. T0641: Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities. T0695: Examine intercept-related metadata and content with an understanding of targeting significance. T0701: Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development. T0720: Identify gaps in our understanding of target technology and developing innovative collection approaches. T0727: Identify, locate, and track targets via geospatial analysis techniques. T0736: Lead or enable exploitation operations in support of organization objectives and target requirements. T0738: Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications. T0754: Monitor target networks to provide indications and warning of target communications changes or processing failures. T0775: Produce network reconstructions. T0777: Profile network or system administrators and their activities.

Role	Threat/Warning Analyst
Description	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

	K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0036: Knowledge of human-computer interaction principles. K0058: Knowledge of network traffic analysis methods. K0108: Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless). K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). K0349: Knowledge of website types, administration, functions, and content management system (CMS). K0362: Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.). K0377: Knowledge of classification and control markings standards, policies and procedures. K0392: Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.). K0395: Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.). K0405: Knowledge of current computer-based intrusion sets. K0409: Knowledge of cyber intelligence/information collection capabilities and repositories. K0415: Knowledge of cyber operations terminology/lexicon. K0417: Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media). K0427: Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP). K0431: Knowledge of evolving/emerging communications technologies. K0436: Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects. K0437: Knowledge of general Supervisory control and data acquisition (SCADA) system components. K0440: Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability. K0444: Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP). K0445: Knowledge of how modern digital and telephony networks impact cyber operations. K0446: Knowledge of how modern wireless communications systems impact cyber operations. K0449: Knowledge of how to extract, analyze, and use metadata. K0458: Knowledge of intelligence disciplines. K0460: Knowledge of intelligence preparation of the environment and similar processes. K0464: Knowledge of intelligence support to planning, execution, and assessment. K0469: Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions. K0471: Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering). K0480: Knowledge of malware. K0499: Knowledge of operations security. K0511: Knowledge of organizational hierarchy and cyber decision-making processes.

	K0516: Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc. K0556: Knowledge of telecommunications fundamentals. K0560: Knowledge of the basic structure, architecture, and design of modern communication networks. K0561: Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection). K0565: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications. K0603: Knowledge of the ways in which targets or threats use the Internet. K0604: Knowledge of threat and/or target systems. K0610: Knowledge of virtualization products (VMware, Virtual PC). K0612: Knowledge of what constitutes a "threat" to a network. K0614: Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.
Skills	S0194: Skill in conducting non-attributable research. S0196: Skill in conducting research using deep web. S0203: Skill in defining and characterizing all pertinent aspects of the operational environment. S0211: Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists. S0218: Skill in evaluating information for reliability, validity, and relevance. S0227: Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes. S0228: Skill in identifying critical target elements, to include critical target elements for the cyber domain. S0229: Skill in identifying cyber threats which may jeopardize organization and/or partner interests. S0249: Skill in preparing and presenting briefings. S0256: Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships. S0278: Skill in tailoring analysis to the necessary levels (e.g., classification and organizational). S0285: Skill in using Boolean operators to construct simple and complex queries. S0288: Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.). S0289: Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. S0296: Skill in utilizing feedback to improve processes, products, and services. S0297: Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint). S0303: Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
Tasks	T0569: Answer requests for information. T0583: Provide subject matter expertise to the development of a common operational picture. T0584: Maintain a common intelligence picture. T0585: Provide subject matter expertise to the development of cyber operations specific indicators. T0586: Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. T0589: Assist in the identification of intelligence collection shortfalls. T0593: Brief threat and/or target current situations.

	T0597: Collaborate with intelligence analysts/targeting organizations involved in related areas. T0615: Conduct in-depth research and analysis. T0617: Conduct nodal analysis. T0660: Develop information requirements necessary for answering priority information requests. T0685: Evaluate threat decision-making processes. T0687: Identify threats to Blue Force vulnerabilities. T0707: Generate requests for information. T0708: Identify threat tactics, and methodologies. T0718: Identify intelligence gaps and shortfalls. T0748: Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. T0749: Monitor and report on validated threat activities. T0751: Monitor open source websites for hostile content directed towards organizational or partner interests. T0752: Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements. T0758: Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). T0761: Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. T0783: Provide current intelligence support to critical internal/external stakeholders as appropriate. T0785: Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. T0786: Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. T0792: Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. T0800: Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. T0805: Report intelligence-derived significant network events and intrusions. T0834: Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.

Role	Cyber Operator
Description	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0009: Knowledge of application vulnerabilities. K0021: Knowledge of data backup and recovery. K0051: Knowledge of low-level computer languages (e.g., assembly languages).

	K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). K0142: Knowledge of collection management processes, capabilities, and limitations. K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. K0363: Knowledge of auditing and logging procedures (including server-based logging). K0372: Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages). K0373: Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications. K0375: Knowledge of wireless applications vulnerabilities. K0379: Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc. K0403: Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations. K0406: Knowledge of current software and methodologies for active defense and system hardening. K0420: Knowledge of database theory. K0423: Knowledge of deconfliction reporting to include external organization interaction. K0427: Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP). K0428: Knowledge of encryption algorithms and tools for wireless local area networks (WLANs). K0429: Knowledge of enterprise-wide information management. K0430: Knowledge of evasion strategies and techniques. K0433: Knowledge of forensic implications of operating system structure and operations. K0438: Knowledge of Global Systems for Mobile Communications (GSM) architecture. K0440: Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability. K0452: Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP. K0468: Knowledge of internal and external partner reporting. K0480: Knowledge of malware. K0481: Knowledge of methods and techniques used to detect various exploitation activities. K0485: Knowledge of network administration. K0486: Knowledge of network construction and topology. K0516: Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc. K0528: Knowledge of satellite-based communication systems. K0530: Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation. K0531: Knowledge of security implications of software configurations. K0536: Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network). K0560: Knowledge of the basic structure, architecture, and design of modern communication networks. K0565: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications. K0573: Knowledge of the fundamentals of digital forensics to extract actionable intelligence. K0608: Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).

	K0609: Knowledge of virtual machine technologies.
Skills	S0062: Skill in analyzing memory dumps to extract information. S0182: Skill in analyzing target communications internals and externals collected from wireless LANs. S0183: Skill in analyzing terminal or environment collection data. S0190: Skill in assessing current tools to identify needed improvements. S0192: Skill in auditing firewalls, perimeters, routers, and intrusion detection systems. S0202: Skill in data mining techniques (e.g., searching file systems) and analysis. S0206: Skill in determining installed patches on various operating systems and identifying patch signatures. S0221: Skill in extracting information from packet captures. S0236: Skill in identifying the devices that work at each level of protocol models. S0242: Skill in interpreting vulnerability scanner results to identify vulnerabilities. S0243: Skill in knowledge management, including technical documentation techniques (e.g., Wiki page). S0252: Skill in processing collected data for follow-on analysis. S0255: Skill in providing real-time, actionable geolocation information utilizing target infrastructures. S0257: Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data). S0266: Skill in relevant programming languages (e.g., C++, Python, etc.). S0267: Skill in remote command line and Graphic User Interface (GUI) tool usage. S0270: Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools. S0275: Skill in server administration. S0276: Skill in survey, collection, and analysis of wireless LAN metadata. S0281: Skill in technical writing. S0282: Skill in testing and evaluating tools for implementation. S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target. S0295: Skill in using various open source data collection tools (online trade, DNS, mail, etc.). S0298: Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.). S0299: Skill in wireless network target analysis, templating, and geolocation. S0363: Skill to analyze and assess internal and external partner reporting.
Tasks	T0566: Analyze internal operational architecture, tools, and procedures for ways to improve performance. T0567: Analyze target operational architecture for ways to gain access. T0598: Collaborate with development organizations to create and deploy the tools needed to achieve objectives. T0609: Conduct access enabling of wireless computer and digital networks. T0610: Conduct collection and processing of wireless computer and digital networks. T0612: Conduct exploitation of wireless computer and digital networks. T0616: Conduct network scouting and vulnerability analyses of systems within a network. T0618: Conduct on-net activities to control and exfiltrate data from deployed technologies. T0619: Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies. T0620: Conduct open source data collection via various online tools. T0623: Conduct survey of computer and digital networks. T0643: Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers). T0644: Detect exploits against targeted networks and hosts and react accordingly. T0664: Develop new techniques for gaining and keeping access to target systems. T0677: Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.

	T0696: Exploit network devices, security devices, and/or terminals or environments using various methods or tools. T0697: Facilitate access enabling by physical and/or wireless means. T0724: Identify potential points of strength and vulnerability within a network. T0740: Maintain situational awareness and functionality of organic operational infrastructure. T0756: Operate and maintain automated systems for gaining and maintaining access to target systems. T0768: Conduct cyber activities to degrade/remove information resident in computers and computer networks. T0774: Process exfiltrated data for analysis and/or dissemination to customers. T0796: Provide real-time actionable geolocation information. T0804: Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects. T0828: Test and evaluate locally developed tools for operational use. T0829: Test internal developed tools and techniques against target tools.

Role	Cyber Defense Forensics Analyst
Description	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0018: Knowledge of encryption algorithms K0021: Knowledge of data backup and recovery. K0042: Knowledge of incident response and handling methodologies. K0060: Knowledge of operating systems. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0077: Knowledge of server and client operating systems. K0078: Knowledge of server diagnostic tools and fault identification techniques. K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). K0117: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]). K0118: Knowledge of processes for seizing and preserving digital evidence. K0119: Knowledge of hacking methodologies. K0122: Knowledge of investigative implications of hardware, Operating Systems, and network technologies. K0123: Knowledge of legal governance related to admissibility (e.g. Rules of Evidence). K0125: Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody. K0128: Knowledge of types and collection of persistent data. K0131: Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies. K0132: Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.

	K0133: Knowledge of types of digital forensics data and how to recognize them. K0134: Knowledge of deployable forensics. K0145: Knowledge of security event correlation tools. K0155: Knowledge of electronic evidence law. K0156: Knowledge of legal rules of evidence and court procedure. K0167: Knowledge of system administration, network, and operating system hardening techniques. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0182: Knowledge of data carving tools and techniques (e.g., Foremost). K0183: Knowledge of reverse engineering concepts. K0184: Knowledge of anti-forensics tactics, techniques, and procedures. K0185: Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark). K0186: Knowledge of debugging procedures and tools. K0187: Knowledge of file type abuse by adversaries for anomalous behavior. K0188: Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro). K0189: Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device). K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. K0254: Knowledge of binary analysis. K0255: Knowledge of network architecture concepts including topology, protocols, and components. K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). K0304: Knowledge of concepts and practices of processing digital forensic data. K0347: Knowledge and understanding of operational design. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0032: Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. S0047: Skill in preserving evidence integrity according to standard operating procedures or national standards. S0062: Skill in analyzing memory dumps to extract information. S0065: Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics). S0067: Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). S0068: Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. S0069: Skill in setting up a forensic workstation. S0071: Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK). S0073: Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). S0074: Skill in physically disassembling PCs. S0075: Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems). S0087: Skill in deep analysis of captured malicious code (e.g., malware forensics). S0088: Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump). S0089: Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).

	S0090: Skill in analyzing anomalous code as malicious or benign. S0091: Skill in analyzing volatile data. S0092: Skill in identifying obfuscation techniques. S0093: Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures. S0131: Skill in analyzing malware. S0132: Skill in conducting bit-level analysis. S0133: Skill in processing digital evidence, to include protecting and making legally sound copies of evidence. S0156: Skill in performing packet-level analysis.
Tasks	T0027: Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. T0036: Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. T0048: Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats. T0049: Decrypt seized data using technical means. T0075: Provide technical summary of findings in accordance with established reporting procedures. T0087: Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. T0103: Examine recovered data for information of relevance to the issue at hand. T0113: Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. T0165: Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment. T0167: Perform file signature analysis. T0168: Perform hash comparison against established database. T0173: Perform timeline analysis. T0175: Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). T0179: Perform static media analysis. T0182: Perform tier 1, 2, and 3 malware analysis. T0190: Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures). T0212: Provide technical assistance on digital evidence matters to appropriate personnel. T0216: Recognize and accurately report forensic artifacts indicative of a particular operating system. T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost). T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools. T0241: Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. T0253: Conduct cursory binary analysis. T0279: Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. T0285: Perform virus scanning on digital media. T0286: Perform file system forensic analysis. T0287: Perform static analysis to mount an "image" of a drive (without necessarily having the original drive). T0288: Perform static malware analysis.

	T0289: Utilize deployable forensics toolkit to support operations as necessary. T0312: Coordinate with intelligence analysts to correlate threat assessment data. T0396: Process image with appropriate tools depending on analyst's goals. T0397: Perform Windows registry analysis. T0398: Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. T0399: Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired. T0400: Correlate incident data and perform cyber defense reporting. T0401: Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. T0432: Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. T0532: Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information. T0546: Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.

Role	Technical Support Specialist
Description	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0053: Knowledge of measures or indicators of system performance and availability. K0088: Knowledge of systems administration concepts. K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). K0114: Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.). K0116: Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip). K0194: Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration. K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. K0237: Knowledge of industry best practices for service desk. K0242: Knowledge of organizational security policies. K0247: Knowledge of remote access processes, tools, and capabilities related to customer support. K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0287: Knowledge of an organization's information classification program and procedures for information compromise.

	K0292: Knowledge of the operations and processes for incident, problem, and event management. K0294: Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly. K0302: Knowledge of the basic operation of computers. K0317: Knowledge of procedures used for documenting and querying reported incidents, problems, and events. K0330: Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.
Skills	S0039: Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation. S0058: Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. S0142: Skill in conducting research for troubleshooting novel client-level problems. S0159: Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications. S0365: Skill to design incident response for cloud service models.
Tasks	T0125: Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). T0237: Troubleshoot system hardware and software. T0308: Analyze incident data for emerging trends. T0315: Develop and deliver technical training to educate others or meet customer needs. T0331: Maintain incident tracking and solution database. T0468: Diagnose and resolve customer reported system incidents, problems, and events. T0482: Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience. T0491: Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards. T0494: Administer accounts, network rights, and access to systems and equipment. T0496: Perform asset management/inventory of information technology (IT) resources. T0502: Monitor and report client-level computer system performance. T0530: Develop a trend analysis and impact report.

Role	Data Analyst
Description	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0015: Knowledge of computer algorithms. K0016: Knowledge of computer programming principles K0020: Knowledge of data administration and data standardization policies. K0022: Knowledge of data mining and data warehousing principles. K0023: Knowledge of database management systems, query languages, table relationships, and views. K0025: Knowledge of digital rights management. K0031: Knowledge of enterprise messaging systems and associated software. K0051: Knowledge of low-level computer languages (e.g., assembly languages).

	K0052: Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). K0060: Knowledge of operating systems. K0065: Knowledge of policy-based and risk adaptive access controls. K0068: Knowledge of programming language structures and logic. K0069: Knowledge of query languages such as SQL (structured query language). K0083: Knowledge of sources, characteristics, and uses of the organization's data assets. K0095: Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines). K0129: Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep). K0139: Knowledge of interpreted and compiled computer languages. K0140: Knowledge of secure coding techniques. K0193: Knowledge of advanced data remediation security features in databases. K0197: Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]). K0229: Knowledge of applications that can log errors, exceptions, and application faults and logging. K0236: Knowledge of how to utilize Hadoop, Java, Python, SQL, Hive, and PIG to explore data. K0238: Knowledge of machine learning theory and principles. K0325: Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression). K0420: Knowledge of database theory.
Skills	S0013: Skill in conducting queries and developing algorithms to analyze data structures. S0017: Skill in creating and utilizing mathematical or statistical models. S0028: Skill in developing data dictionaries. S0029: Skill in developing data models. S0037: Skill in generating queries and reports. S0060: Skill in writing code in a currently supported programming language (e.g., Java, C++). S0088: Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump). S0089: Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]). S0094: Skill in reading Hexadecimal data. S0095: Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode). S0103: Skill in assessing the predictive power and subsequent generalizability of a model. S0106: Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering, smoothing). S0109: Skill in identifying hidden patterns or relationships. S0113: Skill in performing format conversions to create a standard representation of the data. S0114: Skill in performing sensitivity analysis. S0118: Skill in developing machine understandable semantic ontologies. S0119: Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic). S0123: Skill in transformation analytics (e.g., aggregation, enrichment, processing). S0125: Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots). S0126: Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS). S0127: Skill in using data mapping tools.

	S0129: Skill in using outlier identification and removal techniques. S0130: Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc. S0160: Skill in the use of design modeling (e.g., unified modeling language). S0202: Skill in data mining techniques (e.g., searching file systems) and analysis. S0369: Skill to identify sources, characteristics, and uses of the organization's data assets.
Tasks	T0007: Analyze and define data requirements and specifications. T0008: Analyze and plan for anticipated changes in data capacity requirements. T0068: Develop data standards, policies, and procedures. T0146: Manage the compilation, cataloging, caching, distribution, and retrieval of data. T0195: Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. T0210: Provide recommendations on new database technologies and architectures. T0342: Analyze data sources to provide actionable recommendations. T0347: Assess the validity of source data and subsequent findings. T0349: Collect metrics and trending data. T0351: Conduct hypothesis testing using statistical processes. T0353: Confer with systems analysts, engineers, programmers, and others to design application. T0361: Develop and facilitate data-gathering methods. T0366: Develop strategic insights from large data sets. T0381: Present technical information to technical and nontechnical audiences. T0382: Present data in creative formats. T0383: Program custom algorithms. T0385: Provide actionable recommendations to critical stakeholders based on data analysis and findings. T0392: Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method. T0402: Effectively allocate storage capacity in the design of data management systems. T0403: Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data). T0404: Utilize different programming languages to write code, open files, read files, and write output to different files. T0405: Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line). T0460: Develop and implement data mining and data warehousing programs.

Role	Network Operations Specialist
Description	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0010: Knowledge of communication methods, principles, and concepts that support the network infrastructure. K0011: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. K0029: Knowledge of organization's Local and Wide Area Network connections.

	K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). K0050: Knowledge of local area and wide area networking principles and concepts including bandwidth management. K0053: Knowledge of measures or indicators of system performance and availability. K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). K0071: Knowledge of remote access technology concepts. K0076: Knowledge of server administration and systems engineering theories, concepts, and methods. K0093: Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing). K0104: Knowledge of Virtual Private Network (VPN) security. K0108: Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless). K0111: Knowledge of network tools (e.g., ping, traceroute, nslookup) K0113: Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN). K0135: Knowledge of web filtering technologies. K0136: Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). K0137: Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA). K0138: Knowledge of Wi-Fi. K0159: Knowledge of Voice over IP (VoIP). K0160: Knowledge of the common attack vectors on the network layer. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. K0200: Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). K0201: Knowledge of symmetric key rotation techniques and concepts. K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0274: Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0622: Knowledge of controls related to the use, processing, storage, and transmission of data.
Skills	S0004: Skill in analyzing network traffic capacity and performance characteristics. S0035: Skill in establishing a routing schema. S0040: Skill in implementing, maintaining, and improving established network security practices.

	S0041: Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches. S0056: Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol). S0077: Skill in securing network communications. S0079: Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). S0084: Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems). S0150: Skill in implementing and testing network infrastructure contingency and recovery plans. S0162: Skill in sub-netting. S0170: Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).
Tasks	T0035: Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling). T0065: Develop and implement network backup and recovery procedures. T0081: Diagnose network connectivity problem. T0121: Implement new system design procedures, test procedures, and quality standards. T0125: Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). T0126: Install or replace network hubs, routers, and switches. T0129: Integrate new systems into existing network architecture. T0153: Monitor network capacity and performance. T0160: Patch network vulnerabilities to ensure that information is safeguarded against outside parties. T0200: Provide feedback on network requirements, including network architecture and infrastructure. T0232: Test and maintain network infrastructure including software and hardware devices.

Role	System Administrator
Description	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). K0050: Knowledge of local area and wide area networking principles and concepts including bandwidth management. K0053: Knowledge of measures or indicators of system performance and availability. K0064: Knowledge of performance tuning tools and techniques. K0077: Knowledge of server and client operating systems. K0088: Knowledge of systems administration concepts. K0100: Knowledge of the enterprise information technology (IT) architecture. K0103: Knowledge of the type and frequency of routine hardware maintenance. K0104: Knowledge of Virtual Private Network (VPN) security.

	K0117: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]). K0130: Knowledge of virtualization technologies and virtual machine development and maintenance. K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control). K0167: Knowledge of system administration, network, and operating system hardening techniques. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0274: Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly. K0280: Knowledge of systems engineering theories, concepts, and methods. K0289: Knowledge of system/server diagnostic tools and fault identification techniques. K0318: Knowledge of operating system command-line tools. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0346: Knowledge of principles and methods for integrating system components.
Skills	S0016: Skill in configuring and optimizing software. S0033: Skill in diagnosing connectivity problems. S0043: Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.). S0073: Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). S0076: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). S0111: Skill in interfacing with customers. S0143: Skill in conducting system/server planning, management, and maintenance. S0144: Skill in correcting physical and technical problems that impact system/server performance. S0151: Skill in troubleshooting failed system components (i.e., servers) S0153: Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems. S0154: Skill in installing system and component upgrades. (i.e., servers, appliances, network devices). S0155: Skill in monitoring and optimizing system/server performance. S0157: Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.). S0158: Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).
Tasks	T0029: Conduct functional and connectivity testing to ensure continuing operability. T0054: Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs. T0063: Develop and document systems administration standard operating procedures. T0136: Maintain baseline system security according to organizational policies. T0144: Manage accounts, network rights, and access to systems and equipment. T0186: Plan, execute, and verify data redundancy and system recovery procedures. T0207: Provide ongoing optimization and problem-solving support. T0418: Install, update, and troubleshoot systems/servers. T0431: Check system hardware availability, functionality, integrity, and efficiency.

	T0435: Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing. T0458: Comply with organization systems administration standard operating procedures. T0461: Implement and enforce local network usage policies and procedures. T0498: Manage system/server resources including performance, capacity, availability, serviceability, and recoverability. T0501: Monitor and maintain system/server configuration. T0507: Oversee installation, implementation, configuration, and support of system components. T0514: Diagnose faulty system/server hardware. T0515: Perform repairs on faulty system/server hardware. T0531: Troubleshoot hardware/software interface and interoperability problems.
Processes	

Role	Systems Security Analyst
Description	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0015: Knowledge of computer algorithms. K0018: Knowledge of encryption algorithms K0019: Knowledge of cryptography and cryptographic key management concepts K0024: Knowledge of database systems. K0035: Knowledge of installation, integration, and optimization of system components. K0036: Knowledge of human-computer interaction principles. K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). K0052: Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). K0060: Knowledge of operating systems. K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). K0063: Knowledge of parallel and distributed computing concepts. K0075: Knowledge of security system design tools, methods, and techniques. K0082: Knowledge of software engineering. K0093: Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing). K0102: Knowledge of the systems engineering process. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

	K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. K0200: Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). K0227: Knowledge of various types of computer architectures. K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0263: Knowledge of information technology (IT) risk management policies, requirements, and procedures. K0266: Knowledge of how to evaluate the trustworthiness of the supplier and/or product. K0267: Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures. K0275: Knowledge of configuration management techniques. K0276: Knowledge of security management. K0281: Knowledge of information technology (IT) service catalogues. K0284: Knowledge of developing and applying user credential management system. K0285: Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0290: Knowledge of systems security testing and evaluation methods. K0297: Knowledge of countermeasure design for identified security risks. K0322: Knowledge of embedded systems. K0333: Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs. K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
Skills	S0024: Skill in designing the integration of hardware and software solutions. S0027: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. S0031: Skill in developing and applying security system access controls. S0036: Skill in evaluating the adequacy of security designs. S0060: Skill in writing code in a currently supported programming language (e.g., Java, C++). S0141: Skill in assessing security systems designs. S0147: Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). S0167: Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning). S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Tasks	T0015: Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications. T0016: Apply security policies to meet security objectives of the system. T0017: Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. T0085: Ensure all systems security operations and maintenance activities are properly documented and updated as necessary. T0086: Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment. T0088: Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.

	T0123: Implement specific cybersecurity countermeasures for systems and/or applications. T0128: Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. T0169: Perform cybersecurity testing of developed applications and/or systems. T0177: Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. T0187: Plan and recommend modifications or adjustments based on exercise results or system environment. T0194: Properly document all systems security implementation, operations, and maintenance activities and update as necessary. T0202: Provide cybersecurity guidance to leadership. T0205: Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). T0243: Verify and update security documentation reflecting the application/system security design features. T0309: Assess the effectiveness of security controls. T0344: Assess all the configuration management (change configuration/release management) processes. T0462: Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements. T0469: Analyze and report organizational security posture trends. T0470: Analyze and report system security posture trends. T0475: Assess adequate access controls based on principles of least privilege and need-to-know. T0477: Ensure the execution of disaster recovery and continuity of operations. T0485: Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed. T0489: Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. T0492: Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment. T0499: Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative. T0504: Assess and monitor cybersecurity related to system implementation and testing practices. T0508: Verify minimum security requirements are in place for all applications. T0526: Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. T0545: Work with stakeholders to resolve computer security incidents and vulnerability compliance. T0548: Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.

Role	Information Systems Security Manager
Description	Responsible for the cybersecurity of a program, organization, system, or enclave.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles.

	K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0008: Knowledge of applicable business processes and operations of customer organizations. K0018: Knowledge of encryption algorithms K0021: Knowledge of data backup and recovery. K0026: Knowledge of business continuity and disaster recovery continuity of operations plans. K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). K0042: Knowledge of incident response and handling methodologies. K0043: Knowledge of industry-standard and organizationally accepted analysis principles and methods. K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. K0048: Knowledge of Risk Management Framework (RMF) requirements. K0053: Knowledge of measures or indicators of system performance and availability. K0054: Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities. K0058: Knowledge of network traffic analysis methods. K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies. K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0072: Knowledge of resource management principles and techniques. K0076: Knowledge of server administration and systems engineering theories, concepts, and methods. K0077: Knowledge of server and client operating systems. K0087: Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design. K0090: Knowledge of system life cycle management principles, including software security and usability. K0092: Knowledge of technology integration processes. K0101: Knowledge of the organization's enterprise information technology (IT) goals and objectives. K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. K0121: Knowledge of information security program management and project management principles and techniques. K0126: Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) K0149: Knowledge of organization's risk tolerance and/or risk management approach. K0150: Knowledge of enterprise incident response program, roles, and responsibilities. K0151: Knowledge of current and emerging threats/threat vectors. K0163: Knowledge of critical information technology (IT) procurement requirements.

	K0167: Knowledge of system administration, network, and operating system hardening techniques. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. K0169: Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. K0170: Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. K0199: Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]). K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0267: Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0342: Knowledge of penetration testing principles, tools, and techniques. K0622: Knowledge of controls related to the use, processing, storage, and transmission of data. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0018: Skill in creating policies that reflect system security objectives. S0027: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. S0086: Skill in evaluating the trustworthiness of the supplier and/or product.
Tasks	T0001: Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. T0002: Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. T0003: Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. T0004: Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. T0005: Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture. T0024: Collect and maintain data needed to meet system cybersecurity reporting. T0025: Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. T0044: Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. T0089: Ensure that security improvement actions are evaluated, validated, and implemented as required. T0091: Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment. T0092: Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).

	T0093: Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture. T0095: Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy. T0097: Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed. T0099: Evaluate cost/benefit, economic, and risk analysis in decision-making process. T0106: Identify alternative information security strategies to address organizational security objective. T0115: Identify information technology (IT) security program implications of new technologies or technology upgrades. T0130: Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information. T0132: Interpret and/or approve security requirements relative to the capabilities of new information technologies. T0133: Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program. T0134: Lead and align information technology (IT) security priorities with the security strategy. T0135: Lead and oversee information security budget, staffing, and contracting. T0147: Manage the monitoring of information security data sources to maintain organizational situational awareness. T0148: Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. T0149: Manage threat or target analysis of cyber defense information and production of threat information within the enterprise. T0151: Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. T0157: Oversee the information security training and awareness program. T0158: Participate in an information security risk assessment during the Security Assessment and Authorization process. T0159: Participate in the development or modification of the computer environment cybersecurity program plans and requirements. T0192: Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations. T0199: Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. T0206: Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities. T0211: Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents. T0213: Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters. T0215: Recognize a possible security violation and take appropriate action to report the incident, as required. T0219: Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements. T0227: Recommend policy and coordinate review and approval. T0229: Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.

	T0234: Track audit findings and recommendations to ensure that appropriate mitigation actions are taken. T0239: Use federal and organization-specific published documents to manage operations of their computing environment system(s). T0248: Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. T0254: Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. T0255: Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. T0256: Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. T0263: Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. T0264: Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. T0265: Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. T0275: Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). T0276: Participate in the acquisition process as necessary, following appropriate supply chain risk management practices. T0277: Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. T0280: Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance. T0281: Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary. T0282: Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.

Role	Executive Cyber Leadership
Description	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0009: Knowledge of application vulnerabilities. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. K0147: Knowledge of emerging security issues, risks, and vulnerabilities. K0296: Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.

	K0314: Knowledge of industry technologies' potential cybersecurity vulnerabilities. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) K0628: Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
Skills	S0018: Skill in creating policies that reflect system security objectives. S0356: Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience). S0357: Skill to anticipate new security threats. S0358: Skill to remain aware of evolving technical infrastructures. S0359: Skill to use critical thinking to analyze organizational patterns and relationships.
Tasks	T0001: Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. T0002: Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. T0004: Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. T0006: Advocate organization's official position in legal and legislative proceedings. T0025: Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. T0066: Develop and maintain strategic plans. T0130: Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information. T0134: Lead and align information technology (IT) security priorities with the security strategy. T0135: Lead and oversee information security budget, staffing, and contracting. T0148: Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. T0151: Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. T0227: Recommend policy and coordinate review and approval. T0229: Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. T0248: Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. T0254: Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. T0263: Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. T0264: Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. T0282: Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. T0337: Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. T0356: Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. T0429: Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. T0445: Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan. T0509: Perform an information security risk assessment.

	T0763: Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. T0871: Collaborate on cyber privacy and security policies and procedures T0872: Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation T0927: Appoint and guide a team of IT security experts T0928: Collaborate with key stakeholders to establish a cybersecurity risk management program

Role	Cyber Policy and Strategy Planner
Description	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0127: Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure). K0146: Knowledge of the organization's core business/mission processes. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. K0234: Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation). K0248: Knowledge of strategic theory and practice. K0309: Knowledge of emerging technologies that have potential for exploitation. K0311: Knowledge of industry indicators useful for identifying technology trends. K0313: Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development). K0335: Knowledge of current and emerging cyber technologies. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0176: Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures. S0250: Skill in preparing plans and related correspondence.
Tasks	T0074: Develop policy, programs, and guidelines for implementation. T0094: Establish and maintain communication channels with stakeholders. T0222: Review existing and proposed policies with stakeholders. T0226: Serve on agency and interagency policy boards. T0341: Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. T0369: Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. T0384: Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.

	T0390: Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. T0408: Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. T0425: Analyze organizational cyber policy. T0429: Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. T0441: Define and integrate current and future mission environments. T0445: Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan. T0472: Draft, staff, and publish cyber policy. T0505: Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. T0506: Seek consensus on proposed policy changes from stakeholders. T0529: Provide policy guidance to cyber management, staff, and users. T0533: Review, conduct, or participate in audits of cyber programs and projects. T0537: Support the CIO in the formulation of cyber-related policies.

Role	Cyber Workforce Developer and Manager
Description	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0072: Knowledge of resource management principles and techniques. K0101: Knowledge of the organization’s enterprise information technology (IT) goals and objectives. K0127: Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure). K0146: Knowledge of the organization's core business/mission processes. K0147: Knowledge of emerging security issues, risks, and vulnerabilities. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. K0169: Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. K0204: Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes). K0215: Knowledge of organizational training policies. K0233: Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities. K0234: Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation). K0241: Knowledge of organizational human resource policies, processes, and procedures. K0243: Knowledge of organizational training and education policies, processes, and procedures. K0309: Knowledge of emerging technologies that have potential for exploitation. K0311: Knowledge of industry indicators useful for identifying technology trends.

	K0313: Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development). K0335: Knowledge of current and emerging cyber technologies.
Skills	S0108: Skill in developing workforce and position qualification standards. S0128: Skill in using manpower and personnel IT systems.
Tasks	T0001: Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. T0004: Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. T0025: Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. T0044: Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. T0074: Develop policy, programs, and guidelines for implementation. T0094: Establish and maintain communication channels with stakeholders. T0099: Evaluate cost/benefit, economic, and risk analysis in decision-making process. T0116: Identify organizational policy stakeholders. T0222: Review existing and proposed policies with stakeholders. T0226: Serve on agency and interagency policy boards. T0341: Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. T0352: Conduct learning needs assessments and identify requirements. T0355: Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards. T0356: Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. T0362: Develop and implement standardized position descriptions based on established cyber work roles. T0363: Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies. T0364: Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers. T0365: Develop or assist in the development of training policies and protocols for cyber training. T0368: Ensure that cyber career fields are managed in accordance with organizational HR policies and directives. T0369: Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. T0372: Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel. T0373: Establish and oversee waiver processes for cyber career field entry and training qualification requirements. T0374: Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields. T0375: Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements. T0376: Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements. T0384: Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. T0387: Review and apply cyber career field qualification standards.

	T0388: Review and apply organizational policies related to or influencing the cyber workforce. T0390: Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. T0391: Support integration of qualified cyber workforce personnel into information systems life cycle development processes. T0408: Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. T0425: Analyze organizational cyber policy. T0429: Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. T0437: Correlate training and learning to business or mission requirements. T0441: Define and integrate current and future mission environments. T0445: Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan. T0472: Draft, staff, and publish cyber policy. T0481: Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). T0505: Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. T0506: Seek consensus on proposed policy changes from stakeholders. T0529: Provide policy guidance to cyber management, staff, and users. T0533: Review, conduct, or participate in audits of cyber programs and projects. T0536: Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). T0537: Support the CIO in the formulation of cyber-related policies. T0552: Review and approve a supply chain security/risk management policy.

Role	Cyber Instructor
Description	Develops and conducts training or education of personnel within cyber domain.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0007: Knowledge of authentication, authorization, and access control methods. K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies. K0115: Knowledge that technology that can be exploited. K0124: Knowledge of multiple cognitive domains and tools and methods applicable for learning in each domain. K0130: Knowledge of virtualization technologies and virtual machine development and maintenance. K0146: Knowledge of the organization's core business/mission processes. K0147: Knowledge of emerging security issues, risks, and vulnerabilities. K0204: Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes). K0208: Knowledge of computer based training and e-learning services. K0213: Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation). K0215: Knowledge of organizational training policies. K0216: Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).

	K0217: Knowledge of Learning Management Systems and their use in managing learning. K0218: Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic). K0220: Knowledge of modes of learning (e.g., rote learning, observation). K0226: Knowledge of organizational training systems. K0239: Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media. K0245: Knowledge of principles and processes for conducting training and education needs assessment. K0246: Knowledge of relevant concepts, procedures, software, equipment, and technology applications. K0250: Knowledge of Test & Evaluation processes for learners. K0252: Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0313: Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development). K0319: Knowledge of technical delivery capabilities and their limitations. K0628: Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
Skills	S0001: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. S0004: Skill in analyzing network traffic capacity and performance characteristics. S0006: Skill in applying confidentiality, integrity, and availability principles. S0051: Skill in the use of penetration testing tools and techniques. S0052: Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.). S0053: Skill in tuning sensors. S0055: Skill in using knowledge management technologies. S0056: Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol). S0057: Skill in using protocol analyzers. S0060: Skill in writing code in a currently supported programming language (e.g., Java, C++). S0064: Skill in developing and executing technical training programs and curricula. S0070: Skill in talking to others to convey information effectively. S0073: Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). S0075: Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems). S0076: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). S0081: Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.). S0084: Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems). S0097: Skill in applying security controls. S0100: Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises). S0101: Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes. S0121: Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.). S0131: Skill in analyzing malware. S0156: Skill in performing packet-level analysis.

	S0184: Skill in analyzing traffic to identify network devices. S0270: Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools. S0271: Skill in reviewing and editing assessment products. S0281: Skill in technical writing. S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target. S0301: Skill in writing about facts and ideas in a clear, convincing, and organized manner. S0356: Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience). S0358: Skill to remain aware of evolving technical infrastructures.
Tasks	T0030: Conduct interactive training exercises to create an effective learning environment. T0073: Develop new or identify existing awareness and training materials that are appropriate for intended audiences. T0101: Evaluate the effectiveness and comprehensiveness of existing training programs. T0224: Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions). T0230: Support the design and execution of exercise scenarios. T0247: Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. T0316: Develop or assist in the development of computer based training modules or classes. T0317: Develop or assist in the development of course assignments. T0318: Develop or assist in the development of course evaluations. T0319: Develop or assist in the development of grading and proficiency standards. T0320: Assist in the development of individual/collective development, training, and/or remediation plans. T0321: Develop or assist in the development of learning objectives and goals. T0322: Develop or assist in the development of on-the-job training materials or programs. T0323: Develop or assist in the development of written tests for measuring and assessing learner proficiency. T0352: Conduct learning needs assessments and identify requirements. T0365: Develop or assist in the development of training policies and protocols for cyber training. T0367: Develop the goals and objectives for cyber curriculum. T0381: Present technical information to technical and nontechnical audiences. T0382: Present data in creative formats. T0395: Write and publish after action reviews. T0443: Deliver training courses tailored to the audience and physical/virtual environments. T0444: Apply concepts, procedures, software, equipment, and/or technology applications to students. T0450: Design training curriculum and course content based on requirements. T0451: Participate in development of training curriculum and course content. T0467: Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness. T0519: Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment. T0520: Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses). T0535: Recommend revisions to curriculum and course content based on feedback from previous training sessions. T0536: Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).

	T0926: Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations

Role	Cyber Defense Analyst
Description	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0007: Knowledge of authentication, authorization, and access control methods. K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities. K0015: Knowledge of computer algorithms. K0018: Knowledge of encryption algorithms K0019: Knowledge of cryptography and cryptographic key management concepts K0024: Knowledge of database systems. K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). K0042: Knowledge of incident response and handling methodologies. K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). K0058: Knowledge of network traffic analysis methods. K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies. K0060: Knowledge of operating systems. K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). K0065: Knowledge of policy-based and risk adaptive access controls. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0074: Knowledge of key concepts in security management (e.g., Release Management, Patch Management). K0075: Knowledge of security system design tools, methods, and techniques. K0093: Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).

	K0098: Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization. K0104: Knowledge of Virtual Private Network (VPN) security. K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. K0107: Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. K0110: Knowledge of adversarial tactics, techniques, and procedures. K0111: Knowledge of network tools (e.g., ping, traceroute, nslookup) K0112: Knowledge of defense-in-depth principles and network security architecture. K0113: Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN). K0116: Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip). K0139: Knowledge of interpreted and compiled computer languages. K0142: Knowledge of collection management processes, capabilities, and limitations. K0143: Knowledge of front-end collection systems, including traffic collection, filtering, and selection. K0157: Knowledge of cyber defense and information security policies, procedures, and regulations. K0160: Knowledge of the common attack vectors on the network layer. K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). K0162: Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). K0167: Knowledge of system administration, network, and operating system hardening techniques. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. K0190: Knowledge of encryption methodologies. K0191: Signature implementation impact for viruses, malware, and attacks. K0192: Knowledge of Windows/Unix ports and services. K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). K0221: Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). K0222: Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities. K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0290: Knowledge of systems security testing and evaluation methods. K0297: Knowledge of countermeasure design for identified security risks. K0300: Knowledge of network mapping and recreating network topologies. K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). K0303: Knowledge of the use of sub-netting tools. K0318: Knowledge of operating system command-line tools. K0322: Knowledge of embedded systems.

	K0324: Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0339: Knowledge of how to use network analysis tools to identify vulnerabilities. K0342: Knowledge of penetration testing principles, tools, and techniques. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0020: Skill in developing and deploying signatures. S0025: Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). S0027: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. S0036: Skill in evaluating the adequacy of security designs. S0054: Skill in using incident handling methodologies. S0057: Skill in using protocol analyzers. S0063: Skill in collecting data from a variety of cyber defense resources. S0078: Skill in recognizing and categorizing types of vulnerabilities and associated attacks. S0096: Skill in reading and interpreting signatures (e.g., snort). S0147: Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). S0156: Skill in performing packet-level analysis. S0167: Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning). S0169: Skill in conducting trend analysis. S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). S0370: Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.
Tasks	T0020: Develop content for cyber defense tools. T0023: Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources. T0043: Coordinate with enterprise-wide cyber defense staff to validate network alerts. T0088: Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. T0155: Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment. T0164: Perform cyber defense trend analysis and reporting. T0166: Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. T0178: Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. T0187: Plan and recommend modifications or adjustments based on exercise results or system environment. T0198: Provide daily summary reports of network events and activity relevant to cyber defense practices. T0214: Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. T0258: Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.

	T0259: Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity. T0260: Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. T0290: Determine tactics, techniques, and procedures (TTPs) for intrusion sets. T0291: Examine network topologies to understand data flows through the network. T0292: Recommend computing environment vulnerability corrections. T0293: Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR). T0294: Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). T0295: Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. T0296: Isolate and remove malware. T0297: Identify applications and operating systems of a network device based on network traffic. T0298: Reconstruct a malicious attack or activity based off network traffic. T0299: Identify network mapping and operating system (OS) fingerprinting activities. T0310: Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave. T0332: Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan. T0469: Analyze and report organizational security posture trends. T0470: Analyze and report system security posture trends. T0475: Assess adequate access controls based on principles of least privilege and need-to-know. T0503: Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. T0504: Assess and monitor cybersecurity related to system implementation and testing practices. T0526: Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. T0545: Work with stakeholders to resolve computer security incidents and vulnerability compliance. T0548: Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.

Role	Cyber Defense Incident Responder
Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0021: Knowledge of data backup and recovery. K0026: Knowledge of business continuity and disaster recovery continuity of operations plans.

	K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). K0034: Knowledge of network services and protocols interactions that provide network communications. K0041: Knowledge of incident categories, incident responses, and timelines for responses. K0042: Knowledge of incident response and handling methodologies. K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. K0058: Knowledge of network traffic analysis methods. K0062: Knowledge of packet-level analysis. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. K0157: Knowledge of cyber defense and information security policies, procedures, and regulations. K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). K0162: Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). K0167: Knowledge of system administration, network, and operating system hardening techniques. K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0221: Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). K0230: Knowledge of cloud service models and how those models can limit incident response. K0259: Knowledge of malware analysis concepts and methodologies. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0565: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0003: Skill of identifying, capturing, containing, and reporting malware. S0047: Skill in preserving evidence integrity according to standard operating procedures or national standards. S0077: Skill in securing network communications. S0078: Skill in recognizing and categorizing types of vulnerabilities and associated attacks. S0079: Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). S0080: Skill in performing damage assessments. S0173: Skill in using security event correlation tools. S0365: Skill to design incident response for cloud service models.
Tasks	T0041: Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.

	T0047: Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. T0161: Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. T0163: Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. T0164: Perform cyber defense trend analysis and reporting. T0170: Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. T0175: Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). T0214: Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. T0233: Track and document cyber defense incidents from initial detection through final resolution. T0246: Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. T0262: Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness). T0278: Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. T0279: Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. T0312: Coordinate with intelligence analysts to correlate threat assessment data. T0395: Write and publish after action reviews. T0503: Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. T0510: Coordinate incident response functions.

Role	Vulnerability Assessment Analyst
Description	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0009: Knowledge of application vulnerabilities. K0019: Knowledge of cryptography and cryptographic key management concepts K0021: Knowledge of data backup and recovery. K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

	K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). K0068: Knowledge of programming language structures and logic. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0089: Knowledge of systems diagnostic tools and fault identification techniques. K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. K0139: Knowledge of interpreted and compiled computer languages. K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). K0162: Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). K0167: Knowledge of system administration, network, and operating system hardening techniques. K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). K0206: Knowledge of ethical hacking principles and techniques. K0210: Knowledge of data backup and restoration concepts. K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. K0265: Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). K0308: Knowledge of cryptology. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0342: Knowledge of penetration testing principles, tools, and techniques. K0344: Knowledge of an organization's threat environment. K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0001: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. S0009: Skill in assessing the robustness of security systems and designs. S0025: Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). S0044: Skill in mimicking threat behaviors. S0051: Skill in the use of penetration testing tools and techniques. S0052: Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.). S0081: Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.). S0120: Skill in reviewing logs to identify evidence of past intrusions.

	S0137: Skill in conducting application vulnerability assessments. S0171: Skill in performing impact/risk assessments. S0364: Skill to develop insights about the context of an organization's threat environment S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Tasks	T0010: Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. T0028: Conduct and/or support authorized penetration testing on enterprise network assets. T0138: Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. T0142: Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. T0188: Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. T0252: Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews). T0549: Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). T0550: Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).

Role	Security Control Assessor
Description	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0007: Knowledge of authentication, authorization, and access control methods. K0008: Knowledge of applicable business processes and operations of customer organizations. K0009: Knowledge of application vulnerabilities. K0010: Knowledge of communication methods, principles, and concepts that support the network infrastructure. K0011: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities. K0018: Knowledge of encryption algorithms K0019: Knowledge of cryptography and cryptographic key management concepts K0021: Knowledge of data backup and recovery. K0024: Knowledge of database systems. K0026: Knowledge of business continuity and disaster recovery continuity of operations plans. K0027: Knowledge of organization's enterprise information security architecture. K0028: Knowledge of organization's evaluation and validation requirements.

	K0029: Knowledge of organization's Local and Wide Area Network connections. K0037: Knowledge of Security Assessment and Authorization process. K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). K0048: Knowledge of Risk Management Framework (RMF) requirements. K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). K0054: Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities. K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). K0084: Knowledge of structured analysis principles and methods. K0089: Knowledge of systems diagnostic tools and fault identification techniques. K0098: Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization. K0100: Knowledge of the enterprise information technology (IT) architecture. K0101: Knowledge of the organization's enterprise information technology (IT) goals and objectives. K0126: Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) K0146: Knowledge of the organization's core business/mission processes. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. K0169: Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. K0170: Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0199: Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]). K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0267: Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0322: Knowledge of embedded systems. K0342: Knowledge of penetration testing principles, tools, and techniques. K0622: Knowledge of controls related to the use, processing, storage, and transmission of data.

	K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
Skills	S0001: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. S0006: Skill in applying confidentiality, integrity, and availability principles. S0027: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. S0034: Skill in discerning the protection needs (i.e., security controls) of information systems and networks. S0038: Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system. S0073: Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). S0078: Skill in recognizing and categorizing types of vulnerabilities and associated attacks. S0097: Skill in applying security controls. S0100: Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises). S0110: Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements. S0111: Skill in interfacing with customers. S0112: Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events. S0115: Skill in preparing Test & Evaluation reports. S0120: Skill in reviewing logs to identify evidence of past intrusions. S0124: Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution. S0128: Skill in using manpower and personnel IT systems. S0134: Skill in conducting reviews of systems. S0135: Skill in secure test plan design (e. g. unit, integration, system, acceptance). S0136: Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. S0137: Skill in conducting application vulnerability assessments. S0138: Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). S0141: Skill in assessing security systems designs. S0145: Skill in integrating and applying policies that meet system security objectives. S0147: Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). S0171: Skill in performing impact/risk assessments. S0172: Skill in applying secure coding techniques. S0173: Skill in using security event correlation tools. S0174: Skill in using code analysis tools. S0175: Skill in performing root cause analysis. S0176: Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures. S0177: Skill in analyzing a target's communication networks. S0184: Skill in analyzing traffic to identify network devices. S0232: Skill in identifying intelligence gaps and limitations. S0233: Skill in identifying language issues that may have an impact on organization objectives. S0234: Skill in identifying leads for target development. S0235: Skill in identifying non-target regional languages and dialects S0236: Skill in identifying the devices that work at each level of protocol models.

	S0237: Skill in identifying, locating, and tracking targets via geospatial analysis techniques S0238: Skill in information prioritization as it relates to operations. S0239: Skill in interpreting compiled and interpretive programming languages. S0240: Skill in interpreting metadata and content as applied by collection systems. S0241: Skill in interpreting traceroute results, as they apply to network analysis and reconstruction. S0242: Skill in interpreting vulnerability scanner results to identify vulnerabilities. S0243: Skill in knowledge management, including technical documentation techniques (e.g., Wiki page). S0244: Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results. S0248: Skill in performing target system analysis. S0249: Skill in preparing and presenting briefings. S0250: Skill in preparing plans and related correspondence. S0251: Skill in prioritizing target language material. S0252: Skill in processing collected data for follow-on analysis. S0254: Skill in providing analysis to aid writing phased after action reports. S0271: Skill in reviewing and editing assessment products. S0273: Skill in reviewing and editing plans. S0278: Skill in tailoring analysis to the necessary levels (e.g., classification and organizational). S0279: Skill in target development in direct support of collection operations. S0280: Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies). S0281: Skill in technical writing. S0296: Skill in utilizing feedback to improve processes, products, and services. S0304: Skill to access information on current assets available, usage. S0305: Skill to access the databases where plans/directives/guidance are maintained. S0306: Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance. S0307: Skill to analyze target or threat sources of strength and morale. S0325: Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed. S0329: Skill to evaluate requests for information to determine if response information exists. S0332: Skill to extract information from available tools and applications associated with collection requirements and collection operations management. S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). S0370: Skill to use cyber defense Service Provider reporting structure and processes within one's own organization. S0374: Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.
Tasks	T0145: Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). T0177: Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. T0178: Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. T0181: Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. T0184: Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.

	T0205: Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). T0221: Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. T0243: Verify and update security documentation reflecting the application/system security design features. T0244: Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. T0251: Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers). T0255: Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. T0264: Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. T0265: Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. T0268: Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. T0272: Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. T0275: Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). T0277: Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. T0309: Assess the effectiveness of security controls. T0344: Assess all the configuration management (change configuration/release management) processes. T0371: Establish acceptable limits for the software application, network, or system. T0495: Manage Accreditation Packages (e.g., ISO/IEC 15026-2).

Role	Security Architect
Description	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0007: Knowledge of authentication, authorization, and access control methods. K0008: Knowledge of applicable business processes and operations of customer organizations. K0009: Knowledge of application vulnerabilities. K0010: Knowledge of communication methods, principles, and concepts that support the network infrastructure. K0011: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.

	K0012: Knowledge of capabilities and requirements analysis. K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities. K0015: Knowledge of computer algorithms. K0018: Knowledge of encryption algorithms K0019: Knowledge of cryptography and cryptographic key management concepts K0024: Knowledge of database systems. K0026: Knowledge of business continuity and disaster recovery continuity of operations plans. K0027: Knowledge of organization's enterprise information security architecture. K0030: Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware). K0035: Knowledge of installation, integration, and optimization of system components. K0036: Knowledge of human-computer interaction principles. K0037: Knowledge of Security Assessment and Authorization process. K0043: Knowledge of industry-standard and organizationally accepted analysis principles and methods. K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). K0052: Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). K0055: Knowledge of microprocessors. K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). K0057: Knowledge of network hardware devices and functions. K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies. K0060: Knowledge of operating systems. K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). K0063: Knowledge of parallel and distributed computing concepts. K0071: Knowledge of remote access technology concepts. K0074: Knowledge of key concepts in security management (e.g., Release Management, Patch Management). K0082: Knowledge of software engineering. K0091: Knowledge of systems testing and evaluation methods. K0092: Knowledge of technology integration processes. K0093: Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing). K0102: Knowledge of the systems engineering process. K0170: Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. K0198: Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions). K0200: Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). K0202: Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing). K0211: Knowledge of confidentiality, integrity, and availability requirements.

	K0212: Knowledge of cybersecurity-enabled software products. K0214: Knowledge of the Risk Management Framework Assessment Methodology. K0227: Knowledge of various types of computer architectures. K0240: Knowledge of multi-level security systems and cross domain solutions. K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0264: Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements). K0275: Knowledge of configuration management techniques. K0277: Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features). K0286: Knowledge of N-tiered typologies (e.g. including server and client operating systems). K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0291: Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.) K0293: Knowledge of integrating the organization's goals and objectives into the architecture. K0320: Knowledge of organization's evaluation and validation criteria. K0322: Knowledge of embedded systems. K0323: Knowledge of system fault tolerance methodologies. K0325: Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression). K0326: Knowledge of demilitarized zones. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. K0333: Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs. K0336: Knowledge of access authentication methods. K0565: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
Skills	S0005: Skill in applying and incorporating information technologies into proposed solutions. S0022: Skill in designing countermeasures to identified security risks. S0024: Skill in designing the integration of hardware and software solutions. S0027: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. S0050: Skill in design modeling and building use cases (e.g., unified modeling language). S0059: Skill in using Virtual Private Network (VPN) devices and encryption. S0061: Skill in writing test plans. S0076: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). S0116: Skill in designing multi-level security/cross domain solutions. S0122: Skill in the use of design methods. S0138: Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). S0139: Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). S0152: Skill in translating operational requirements into protection needs (i.e., security controls).

	S0168: Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks. S0170: Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). S0374: Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.
Tasks	T0050: Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. T0051: Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. T0071: Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). T0082: Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. T0084: Employ secure configuration management processes. T0090: Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. T0108: Identify and prioritize critical business functions in collaboration with organizational stakeholders. T0177: Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. T0196: Provide advice on project costs, design concepts, or design changes. T0203: Provide input on security requirements to be included in statements of work and other appropriate procurement documents. T0205: Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). T0268: Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. T0307: Analyze candidate architectures, allocate security services, and select security mechanisms. T0314: Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. T0328: Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. T0338: Write detailed functional specifications that document the architecture development process. T0427: Analyze user needs and requirements to plan architecture. T0448: Develop enterprise architecture or system components required to meet user needs. T0473: Document and update as necessary all definition and architecture activities. T0484: Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. T0542: Translate proposed capabilities into technical requirements. T0556: Assess and design security management functions as related to cyberspace.

Role	System Testing and Evaluation Specialist

Description	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
Knowledge	K0001: Knowledge of computer networking concepts and protocols, and network security methodologies. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. K0004: Knowledge of cybersecurity and privacy principles. K0005: Knowledge of cyber threats and vulnerabilities. K0006: Knowledge of specific operational impacts of cybersecurity lapses. K0027: Knowledge of organization's enterprise information security architecture. K0028: Knowledge of organization's evaluation and validation requirements. K0037: Knowledge of Security Assessment and Authorization process. K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). K0057: Knowledge of network hardware devices and functions. K0088: Knowledge of systems administration concepts. K0091: Knowledge of systems testing and evaluation methods. K0102: Knowledge of the systems engineering process. K0126: Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) K0139: Knowledge of interpreted and compiled computer languages. K0169: Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. K0170: Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). K0199: Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]). K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). K0212: Knowledge of cybersecurity-enabled software products. K0250: Knowledge of Test & Evaluation processes for learners. K0260: Knowledge of Personally Identifiable Information (PII) data security standards. K0261: Knowledge of Payment Card Industry (PCI) data security standards. K0262: Knowledge of Personal Health Information (PHI) data security standards. K0287: Knowledge of an organization's information classification program and procedures for information compromise. K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
Skills	S0015: Skill in conducting test events. S0021: Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data). S0026: Skill in determining an appropriate level of test rigor for a given system. S0030: Skill in developing operations-based testing scenarios. S0048: Skill in systems integration testing. S0060: Skill in writing code in a currently supported programming language (e.g., Java, C++). S0061: Skill in writing test plans. S0082: Skill in evaluating test plans for applicability and completeness. S0104: Skill in conducting Test Readiness Reviews. S0107: Skill in designing and documenting overall program Test & Evaluation strategies. S0110: Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.

	S0112: Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events. S0115: Skill in preparing Test & Evaluation reports. S0117: Skill in providing Test & Evaluation resource estimate. S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Tasks	T0058: Determine level of assurance of developed capabilities based on test results. T0080: Develop test plans to address specifications and requirements. T0125: Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). T0143: Make recommendations based on test results. T0257: Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. T0274: Create auditable evidence of security measures. T0393: Validate specifications and requirements for testability. T0426: Analyze the results of software, hardware, or interoperability testing. T0511: Perform developmental testing on systems under development. T0512: Perform interoperability testing on systems exchanging electronic information with other systems. T0513: Perform operational testing. T0539: Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements. T0540: Record and manage test data.