CAREER PATHWAY CYBER DEFENSE ANALYST (511)

October 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 511-CYBER DEFENSE ANALYST

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 511-Cyber Defense Analyst.

Table 1. 511-Cyber Defense Analyst Work Role Overview

NICE Role 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.*
OPM Occupational Series	Personnel performing the 511-Cyber Defense Analyst work role are most commonly aligned to the following Occupational Series: - 2210-Information Technology – 86% - 1550-Computer Science – 7% - 0132-Intelligence – 2% - 0854-Computer Engineering – 2% - 0855-Electronics Engineering – 1%
Work Role Pairings	Personnel performing the 511-Cyber Defense Analyst work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 531-Cyber Defense Incident Responder – 34% - 541-Vulnerability Assessment Analyst – 15% - 521-Cyber Defense Infrastructure Spt. Spec – 13% - 332-Cyber Ops Planner – 6% - 431-Knowledge Manager – 4%
Functional Titles	Personnel performing the 511-Cyber Defense Analyst work role may unofficially or alternatively be called: - Computer Network Defense (CND) Analyst - Enterprise Network Defense (END) Analyst - Cybersecurity / Information Security Analyst - Incident Analyst - Network Security Analyst / Specialist / Engineer - Network Defense Technician - Security Operator - Sensor Analyst

Distribution of GS-Levels	Personnel performing the 511-Cyber Defense Analyst work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-5 – redacted** - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☐ GS-10 – redacted** - ☒ GS-11 – 11% - ☒ GS-12 – 23% - ☒ GS-13 – 41% - ☒ GS-14 – 14% - ☐ GS-15 – redacted** *9% of all 511s are in non-GS pay plans and excluded from this section **Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 511-Cyber Defense Analyst work role: - 422-Data Analyst - 441-Network Operations Specialist - 451-System Administrator - 461-Systems Security Analyst
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 511-Cyber Defense Analyst. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 111-All-Source Analyst - 141-Threat/Warning Analyst - 212-Cyber Defense Forensics Analyst - 521-Cyber Defense Infrastructure Support Specialist - 531-Cyber Defense Incident Responder - 541-Vulnerability Assessment Analyst - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 411-Technical Support Specialist work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711- Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *732-Privacy Compliance Manager / Officer* - *751-Cyber Workforce Developer and Manager*

	- *752-Cyber Policy and Strategy Planner* - *802-IT Project Manager* - *803-Product Support Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 511-Cyber Defense Analyst work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 511-Cyber Defense Analyst Core Tasks

Task ID	Task	Core or Additional
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.	Core
T0259	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Core
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.	Core
T0260	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Core
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.	Core
T0294	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	Core
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Core
T0164	Perform cyber defense trend analysis and reporting.	Core
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Core
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Core
T0293	Identify and analyze anomalies in network traffic using metadata.	Core
T0198	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Core
T0297	Identify applications and operating systems of a network device based on network traffic.	Core
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.	Additional
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Additional
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Additional
T0295	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Additional

Task ID	Task	Core or Additional
T0299	Identify network mapping and operating system (OS) fingerprinting activities.	Additional
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.	Additional
T0298	Reconstruct a malicious attack or activity based off network traffic.	Additional
T0290	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Additional
T0088	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Additional
T0291	Examine network topologies to understand data flows through the network.	Additional
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.	Additional

1.3 CORE KNOWLEDGE, SKILLS, AND ABILITIES

The table below provides a ranking of KSAs that represent the Core, or baseline, expectations for performance in the 511-Cyber Defense Analyst work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 511-Cyber Defense Analyst Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to All Work Roles
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence	Foundational to All Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to All Work Roles
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense	Core
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense	Core
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense	Core
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense	Core
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management	Core
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security	Core
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]).	Infrastructure Design	Core
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Core
K0058	Knowledge of network traffic analysis methods.	Network Management	Core
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness	Core
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis	Core

KSA ID	Description	Competency	Importance to Work Role
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis	Core
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	Vulnerabilities Assessment	Core
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment	Core
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment	Core
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment	Core
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment	Core
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages	Additional
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense	Additional
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense	Additional
K0191	Knowledge of signature implementation impact for viruses, malware, and attacks.	Computer Network Defense	Additional
S0020	Skill in developing and deploying signatures.	Computer Network Defense	Additional
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense	Additional
S0096	Skill in reading and interpreting signatures (e.g., snort).	Computer Network Defense	Additional
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense	Additional
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense	Additional
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense	Additional
S0169	Skill in conducting trend analysis.	Data Analysis	Additional
K0142	Knowledge of collection management processes, capabilities, and limitations.	Data Management	Additional
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Data Management	Additional
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Additional
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Additional
K0024	Knowledge of database systems.	Database Management Systems	Additional
K0018	Knowledge of encryption algorithms	Encryption	Additional

KSA ID	Description	Competency	Importance to Work Role
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption	Additional
K0104	Knowledge of Virtual Private Network (VPN) security.	Encryption	Additional
K0190	Knowledge of encryption methodologies.	Encryption	Additional
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management	Additional
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management	Additional
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management	Additional
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Additional
S0054	Skill in using incident handling methodologies.	Incident Management	Additional
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Information Assurance	Additional
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance	Additional
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security	Additional
K0075	Knowledge of security system design tools, methods, and techniques.	Information Systems/Network Security	Additional
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security	Additional
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Additional
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.	Information Technology Assessment	Additional
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	Infrastructure Design	Additional
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design	Additional

KSA ID	Description	Competency	Importance to Work Role
K0300	Knowledge of network mapping and recreating network topologies.	Infrastructure Design	Additional
K0303	Knowledge of the use of sub-netting tools.	Infrastructure Design	Additional
K0322	Knowledge of embedded systems.	Infrastructure Design	Additional
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.	Legal, Government, and Jurisprudence	Additional
K0222	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	Legal, Government, and Jurisprudence	Additional
K0015	Knowledge of computer algorithms.	Mathematical Reasoning	Additional
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management	Additional
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management	Additional
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Additional
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management	Additional
K0060	Knowledge of operating systems.	Operating Systems	Additional
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	Operating Systems	Additional
K0192	Knowledge of Windows/Unix ports and services.	Operating Systems	Additional
K0318	Knowledge of operating system command-line tools.	Operating Systems	Additional
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration	Additional
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation	Additional
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).	Telecommunications	Additional
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis	Additional
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis	Additional
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis	Additional
A0010	Ability to analyze malware.	Threat Analysis	Additional
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment	Additional
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	Vulnerabilities Assessment	Additional

KSA ID	Description	Competency	Importance to Work Role
	injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).		
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment	Additional
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment	Additional
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment	Additional
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment	Additional
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 511-Cyber Defense Analyst work role, and their associated importance. Listed competencies are collections of three or more similar Knowledge, Skills, or Abilities aligned to the Work Role. *These competencies originate from the NICE Framework Competency Pivot Tool.*

Table 4. 511-Cyber Defense Analyst Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Computer Network Defense	C007	KSAs that relate to the defensive measures to detect, respond, and protect information, information systems, and networks from threats.	- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. - Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization. - Knowledge of adversarial tactics, techniques, and procedures. - Knowledge of cyber defense and information security policies, procedures, and regulations. - Knowledge of the common attack vectors on the network layer. - Knowledge of signature implementation impact for viruses, malware, and attacks. - Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. - Skill in developing and deploying signatures. - Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). - Skill in reading and interpreting signatures (e.g., snort). - Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). - Skill to use cyber defense Service Provider reporting structure and processes within one's own organization. - Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Threat Analysis	C055	Knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks.	- Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. - Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). - Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). - Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). - Knowledge of countermeasure design for identified security risks. - Ability to analyze malware.	Core
Vulnerabilities Assessment	C057	Principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	- Knowledge of cyber threats and vulnerabilities. - Knowledge of specific operational impacts of cybersecurity lapses. - Knowledge of cyber defense and vulnerability assessment tools and their capabilities. - Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). - 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). - Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. - Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). - Knowledge of how to use network analysis tools to identify vulnerabilities. - Knowledge of penetration testing principles, tools, and techniques. - Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) - Skill in evaluating the adequacy of security designs. - Skill in using protocol analyzers. - Skill in recognizing and categorizing types of vulnerabilities and associated attacks. - Skill in performing packet-level analysis. - Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
			- Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	
Incident Management	C021	Tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents.	- Knowledge of incident response and handling methodologies. - Skill in using incident handling methodologies.	Core
Network Management	C033	Operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.	- Knowledge of network tools (e.g., ping, traceroute, nslookup) - Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute). - Knowledge of network traffic analysis methods. - Knowledge of front-end collection systems, including traffic collection, filtering, and selection. - Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Core
Data Management	C013	Development and execution of data management plans, programs, practices, processes, architectures, and tools that manage, control, protect, deliver, archive, dispose of, and enhance the value of data and information assets.	- Knowledge of collection management processes, capabilities, and limitations. - Skill in collecting data from a variety of cyber defense resources. - Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Core
Information Systems / Network Security	C024	Methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	- Knowledge of cybersecurity and privacy principles. - Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). - Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). - Knowledge of security system design tools, methods, and techniques. - Knowledge of defense-in-depth principles and network security architecture. - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Legal, Government, and Jurisprudence	C030	Laws, regulations, policies, and ethics that can impact organizational activities.	- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. - 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. - Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	Additional
Infrastructure Design	C026	Architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.	- Knowledge of computer networking concepts and protocols, and network security methodologies. - 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]). - Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN). - Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). - Knowledge of network mapping and recreating network topologies. - Knowledge of the use of sub-netting tools. - Knowledge of embedded systems. - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Additional

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Information Assurance	C022	Methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Knowledge of key concepts in security management (e.g., Release Management, Patch Management). - Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Additional
Encryption	C017	Operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.	- Knowledge of encryption algorithms - Knowledge of cryptography and cryptographic key management concepts - Knowledge of Virtual Private Network (VPN) security. - Knowledge of encryption methodologies.	Additional
Operating Systems	C034	Computer network, desktop, and mainframe operating systems and their applications.	- Knowledge of operating systems. - Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip). - Knowledge of Windows/Unix ports and services. - Knowledge of operating system command-line tools.	Additional
Data Privacy and Protection	C014	Computer network, desktop, and mainframe operating systems and their applications.	- Knowledge of Personally Identifiable Information (PII) data security standards. - Knowledge of Payment Card Industry (PCI) data security standards. - Knowledge of Personal Health Information (PHI) data security standards.	Additional
Identity Management	C020	Security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons"	- Knowledge of authentication, authorization, and access control methods. - Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). - Knowledge of policy-based and risk adaptive access controls.	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 511-Cyber Defense Analyst Suggested Qualifications / Capability Indicators

For indicators of capability for the 511-Cyber Defense Analyst work role, please see Draft NISTR 8193 - National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators.

Section to be populated with updated DoD-8140 Qualification Matrix for 511-Cyber Defense Analyst.

2 APPENDIX: 511-CYBER DEFENSE ANALYST TASK ANALYSIS AND KSA MAPPING

2.1 KEY TO READING THE TASK ANALYSIS AND KSA MAPPING

Table 6. Key to Reading the Task Analysis and KSA Mapping

Proficiency	Task Statement	Importance
As Written	Task as written within the NICE Cybersecurity Workforce Framework (NICE Framework).	Overall Importance to Work Role
Entry	*Example behavioral indicator / task permutation for performing this task at an Entry skills proficiency level.*	
Intermediate	*Example behavioral indicator / task permutation for performing this task at an Intermediate skills proficiency level.*	
Advanced	*Example behavioral indicator / task permutation for performing this task at an Advanced skills proficiency level.*	

Table 7. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
ID of K, S, or A	Knowledge, Skill or Ability needed to perform the task as written within the NICE Framework	Competency mapped to the individual K, S, or A.

2.2 511-CYBER DEFENSE ANALYST TASK ANALYSIS AND KSA MAPPING

Table 8. T0258 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Core
Entry	*Support the timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these rudimentary incidents and events from benign activities.*	
Intermediate	*Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.*	
Advanced	*Oversee timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these complex incidents and events from benign activities.*	

Table 9. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security

KSA ID	Description	Competency
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
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]).	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management
K0060	Knowledge of operating systems.	Operating Systems
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	Operating Systems
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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).	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
S0054	Skill in using incident handling methodologies.	Incident Management
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management

KSA ID	Description	Competency
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0096	Skill in reading and interpreting signatures (e.g., snort).	Computer Network Defense
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
S0169	Skill in conducting trend analysis.	Data Analysis
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Data Management
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

Table 10. T0259 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Core
Entry	*Use cyber defense tools for continual monitoring and basic analysis of system activity to identify/escalate potential malicious activity.*	
Intermediate	*Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.*	
Advanced	*Use cyber defense tools for continual monitoring and advanced analysis of system activity to identify malicious activity.*	

Table 11. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0058	Knowledge of network traffic analysis methods.	Network Management
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
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]).	Infrastructure Design
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).	Vulnerabilities Assessment
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management

KSA ID	Description	Competency
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0191	Knowledge of signature implementation impact for viruses, malware, and attacks.	Computer Network Defense
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
S0020	Skill in developing and deploying signatures.	Computer Network Defense
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management

KSA ID	Description	Competency
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0096	Skill in reading and interpreting signatures (e.g., snort).	Computer Network Defense
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
A0010	Ability to analyze malware.	Threat Analysis
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Data Management
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

Table 12. T0155 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Document and escalate events (including event's history, status, and potential impact for further action).*	
Intermediate	*Identify and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.*	
Advanced	*Evaluate escalated incidents and report on those that will cause ongoing and immediate impact to the environment.*	

Table 13. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
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).	Vulnerabilities Assessment
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
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.	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0222	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	Legal, Government, and Jurisprudence
S0054	Skill in using incident handling methodologies.	Incident Management
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

Table 14. T0260 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Core
Entry	*Gather data and assist in preliminary analysis of suspected malicious activity to provide for further analysis and triage.*	
Intermediate	*Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.*	
Advanced	*Conduct complex analysis and provide after action report with recommendations for identified malicious activity, providing weaknesses exploited, exploitation methods, effects on system and information.*	

Table 15. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
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).	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis

KSA ID	Description	Competency
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0054	Skill in using incident handling methodologies.	Incident Management
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
S0169	Skill in conducting trend analysis.	Data Analysis
A0010	Ability to analyze malware.	Threat Analysis
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

Table 16. T0166 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and escalate for further analysis.*	
Intermediate	*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.*	
Advanced	*Perform analysis on correlated event information gathered from a variety of sources within the enterprise to gain situational awareness, determine the effectiveness of an observed attack, and provide recommendations for remediation.*	

Table 17. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
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).	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis

KSA ID	Description	Competency
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0054	Skill in using incident handling methodologies.	Incident Management
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

Table 18. T0294 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	Core
Entry	*Conduct preliminary research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).*	
Intermediate	*Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).*	
Advanced	*Conduct advanced research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).*	

Table 19. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0142	Knowledge of collection management processes, capabilities, and limitations.	Data Management
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Data Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0054	Skill in using incident handling methodologies.	Incident Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	Operating Systems

KSA ID	Description	Competency
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat 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).	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment

Table 20. T0214 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Core
Entry	*Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.*	
Intermediate	*Receive and analyze network alerts from various sources within the enterprise and determine causes of such alerts.*	
Advanced	*Receive and analyze network alerts from various sources within the enterprise, determine causes of such alerts, and identify items for trend analysis.*	

Table 21. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0191	Knowledge of signature implementation impact for viruses, malware, and attacks.	Computer Network Defense
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
S0020	Skill in developing and deploying signatures.	Computer Network Defense
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
S0096	Skill in reading and interpreting signatures (e.g., snort).	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Data Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management

KSA ID	Description	Competency
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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).	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment

Table 22. T0164 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform cyber defense trend analysis and reporting.	Core
Entry	*Assist with cyber defense trend analysis and reporting.*	
Intermediate	*Perform cyber defense trend analysis and reporting.*	
Advanced	*Perform advanced cyber defense trend analysis and reporting.*	

Table 23. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
S0169	Skill in conducting trend analysis.	Data Analysis
K0142	Knowledge of collection management processes, capabilities, and limitations.	Data Management
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	Data Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0054	Skill in using incident handling methodologies.	Incident Management
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

KSA ID	Description	Competency
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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).	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment

Table 24. T0023 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Core
Entry	*Characterize and analyze network traffic to assist in identifying anomalous activity and potential threats to network resources.*	
Intermediate	*Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.*	
Advanced	*Characterize and provide advanced analysis of network traffic to identify anomalous activity and potential threats to network resources.*	

Table 25. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management
K0192	Knowledge of Windows/Unix ports and services.	Operating Systems
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment

Table 26. T0043 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Core
Entry	*Coordinate with local cyber defense staff to validate network alerts.*	
Intermediate	*Coordinate with enterprise-wide cyber defense staff to validate network alerts.*	
Advanced	*Coordinate with enterprise-wide cyber defense staff to provide advanced analysis of network alerts.*	

Table 27. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0058	Knowledge of network traffic analysis methods.	Network Management
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management

Table 28. T0293 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify and analyze anomalies in network traffic using metadata.	Core
Entry	*Assist in analyzing anomalies in network traffic using metadata.*	
Intermediate	*Identify and analyze anomalies in network traffic using metadata.*	
Advanced	*Conduct advanced analysis and determine impacts of anomalies in network traffic using metadata.*	

Table 29. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0160	Knowledge of the common attack vectors on the network layer.	Computer Network Defense
K0191	Knowledge of signature implementation impact for viruses, malware, and attacks.	Computer Network Defense
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
S0096	Skill in reading and interpreting signatures (e.g., snort).	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
S0169	Skill in conducting trend analysis.	Data Analysis
S0063	Skill in collecting data from a variety of cyber defense resources.	Data Management
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0058	Knowledge of network traffic analysis methods.	Network Management
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	Network Management
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management

KSA ID	Description	Competency
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment

Table 30. T0198 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Core
Entry	*Draft daily summary reports of network events and activity relevant to cyber defense practices.*	
Intermediate	*Review and validate daily summary reports of network events and activity relevant to cyber defense practices.*	
Advanced	*Approve and provide daily summary reports of network events and activity relevant to cyber defense practices to senior leadership.*	

Table 31. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0191	Knowledge of signature implementation impact for viruses, malware, and attacks.	Computer Network Defense
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.	Computer Network Defense
S0169	Skill in conducting trend analysis.	Data Analysis
K0142	Knowledge of collection management processes, capabilities, and limitations.	Data Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0075	Knowledge of security system design tools, methods, and techniques.	Information Systems/Network Security
K0112	Knowledge of defense-in-depth principles and network security architecture.	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 32. T0297 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify applications and operating systems of a network device based on network traffic.	Core
Entry	*Identify applications and operating systems of a network device based on network traffic.*	
Intermediate	*Identify anomalous or suspicious applications and operating systems of a network device based on network traffic.*	
Advanced	*Take corrective actions to reduce impact of anomalous or suspicious applications and operating systems of a network device based on network traffic.*	

Table 33. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0142	Knowledge of collection management processes, capabilities, and limitations.	Data Management
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	Network Management
A0159	Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	Network Management
K0060	Knowledge of operating systems.	Operating Systems
K0192	Knowledge of Windows/Unix ports and services.	Operating Systems
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
S0057	Skill in using protocol analyzers.	Vulnerabilities Assessment