CAREER PATHWAY CYBER DEFENSE INCIDENT RESPONDER (531)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

CIO COUNCIL

CHIEF HUMAN CAPITAL OFFICERS COUNCIL
CHCO COUNCIL
UNITED STATES OF AMERICA

Table of Contents

1 531-CYBER DEFENSE INCIDENT RESPONDER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 531-Cyber Defense Incident Responder.

Table 1. 531-Cyber Defense Incident Responder Work Role Overview

NICE Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
OPM Occupational Series	Personnel performing the 531-Cyber Defense Incident Responder work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 82% - 301-Misc. Administration and Program – 5% - 0080-Security Administration – 4% - 1801-General Inspection, Investigation, Enforcement, and Compliance Series – 4% - 0391-Telecommunications – 2%
Work Role Pairings	Personnel performing the 531-Cyber Defense Incident Responder work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 511-Cyber Defense Analyst – 30% - 541-Vulnerability Assessment Analyst – 9% - 422-Data Analyst – 8% - 521-Cyber Defense Infrastructure Spt. Spec – 8% - 411-Technical Support Specialist – 8%
Functional Titles	Personnel performing the 531-Cyber Defense Incident Responder work role may unofficially or alternatively be called: - Computer Network Defense Incident Responder - Computer Security Incident Response Team Engineer - Disaster Recovery Specialist - Incident Handler - Incident Responder - Incident Response Analyst - Incident Response Coordinator - Incident Response Engineer
Distribution of GS-Levels	Personnel performing the 531-Cyber Defense Incident Responder work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-5 – redacted**

	- ☐ GS-6 – redacted** - ☐ GS-7 – redacted** - ☒ GS-9 – 3% - ☒ GS-11 – 11% - ☒ GS-12 – 30% - ☒ GS-13 – 34% - ☒ GS-14 – 14% - ☐ GS-15 – redacted** *6% of all 531s 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 531-Cyber Defense Incident Responder work role: - 461-Systems Security Analyst - 511-Cyber Defense Analyst - 521-Cyber Defense Infrastructure Support Specialist
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 531-Cyber Defense Incident Responder. 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: - 211-Forensics Analyst - 212-Cyber Defense Forensics Analyst - 221-Cyber Crime Investigator - 541-Vulnerability Assessment Analyst - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 531-Cyber Defense Incident Responder 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*

1.2 Core Tasks

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 531-Cyber Defense Incident Responder work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 531-Cyber Defense Incident Responder Core Tasks

Task ID	Task Description	Core or Additional
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.	Core
T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	Core
T0510	Coordinate incident response functions.	Core
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.	Core
T0164	Perform cyber defense trend analysis and reporting.	Core
T0170	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.	Core
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Core
T0395	Write and publish after action reviews.	Core
T0246	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	Core
T0312	Coordinate with intelligence analysts to correlate threat assessment data.	Additional
T0047	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	Additional
T0262	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).	Additional
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.	Additional
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.	Additional
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).	Additional
T0279	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Additional
T0233	Track and document cyber defense incidents from initial detection through final resolution.	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 531-Cyber Defense Incident Responder work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 531-Cyber Defense Incident Responder 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
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity	Core
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics	Core
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
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense	Core
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management	Core
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Core
S0080	Skill in performing damage assessments.	Incident Management	Core
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Core
S0077	Skill in securing network communications.	Information Systems/Network Security	Core
S0173	Skill in using security event correlation tools.	Information Systems/Network Security	Core
K0034	Knowledge of network services and protocols interactions that provide network communications.	Infrastructure Design	Core
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design	Core
K0230	Knowledge of cloud service models and how those models can limit incident response.	Infrastructure Design	Core

KSA ID	Description	Competency	Importance to Work Role
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Core
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration	Core
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis	Core
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis	Core
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis	Core
K0259	Knowledge of malware analysis concepts and methodologies.	Threat Analysis	Core
S0003	Skill of identifying, capturing, containing, and reporting malware.	Threat Analysis	Core
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	Core
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment	Core
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment	Core
K0021	Knowledge of data backup and recovery.	Business Continuity	Additional
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense	Additional
S0365	Skill to design incident response for cloud service models.	Incident Management	Additional
A0121	Ability to design incident response for cloud service models.	Incident Management	Additional
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security	Additional
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.	Infrastructure Design	Additional
K0058	Knowledge of network traffic analysis methods.	Network Management	Additional
K0062	Knowledge of packet-level analysis.	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional

1.4 Core Competencies

The table below is a compilation of competencies aligned to the 531-Cyber Defense Incident Responder 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. 531-Cyber Defense Incident Responder 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. [K0046] - Knowledge of cyber defense and information security policies, procedures, and regulations. [K0157] - Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). [S0079] - Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies. [A0128]	Core
Incident Management	C021	KSAs that relate to the tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents.	- Knowledge of incident categories, incident responses, and timelines for responses. [K0041] - Knowledge of incident response and handling methodologies. [K0042] - Skill in performing damage assessments. [S0080] - Skill to design incident response for cloud service models. [S0365] - Ability to design incident response for cloud service models. [A0121]	Core
Information Systems / Network Security	C024	This area contains KSAs that relate to the 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. [K0004] - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). [K0179] - Skill in securing network communications. [S0077] - Skill in using security event correlation tools. [S0173] - Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). [K0033]	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	This area contains KSAs that relate to the 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. [K0001] - Knowledge of network services and protocols interactions that provide network communications. [K0034] - Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). [K0221] - Knowledge of cloud service models and how those models can limit incident response. [K0230] - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. [K0332] - 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. [K0565]	Core
Threat Analysis	C055	KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks.	- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). [K0161] - Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). [K0162] - Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). [K0177] - Knowledge of malware analysis concepts and methodologies. [K0259] - Skill of identifying, capturing, containing, and reporting malware. [S0003]	Core
Vulnerabilities Assessment	C057	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	- Knowledge of cyber threats and vulnerabilities. [K0005] - Knowledge of specific operational impacts of cybersecurity lapses. [K0006] - 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). [K0070] - Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. [K0106] - Skill in recognizing and categorizing types of vulnerabilities and associated attacks. [S0078] - Knowledge of packet-level analysis. [K0062] - Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) [K0624]	Core

1.5 Suggested Qualifications / Capability Indicators

Table 5. 531-Cyber Defense Incident Responder Suggested Qualifications / Capability Indicators

For indicators of capability for the 531-Cyber Defense Incident Responder 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 531-Cyber Defense Incident Responder.*

2 APPENDIX: 531-CYBER DEFENSE INCIDENT RESPONDER 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.

2.2 531-Cyber Defense Incident Responder Task Analysis and KSA Mapping

Table 8. T0278 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Collect intrusion artifacts (e.g., source code, malware, trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Core
Entry	*Organize intrusion artifacts, identify and catalogue/categorize artifacts, and assist in looking at dashboards for alerts. Use incident response tools to carve out files from PCAP or off of a media. Basics about how to analyze PCAP. Provide input and recommendations on mitigation and resolution.*	
Intermediate	*Collect intrusion artifacts (e.g., source code, malware, trojans), categorize and identify artifact and potential vulnerability or targeted environment, use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. Provide feedback to team members, leaders, and customers/stakeholders.*	
Advanced	*Collect and decode artifacts carve files from uncommon/allocated spaces from within a system (e.g. memory, XXD manipulation, etc.) to understand if it was encapsulated or encrypted to mitigate. Perform advanced analysis un unknown and uncommon threats to closeout. Author after action and other related reports. Brief senior leadership/customers/stakeholders, as appropriate.*	

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

KSA ID	Description	Competency
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0034	Knowledge of how network services and protocols interact to provide network communications.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design
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.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	Threat Analysis
S0003	Skill of identifying, capturing, containing, and reporting malware.	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment

Table 10. T0041 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	Core
Entry	*Communicate with enterprise-wide cyber defense technicians to resolve cyber defense incidents.*	
Intermediate	*Collaborate with enterprise-wide cyber defense technicians to resolve cyber defense incidents.*	
Advanced	*Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.*	

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

KSA ID	Description	Competency
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
S0079	Skill in protecting a network against malware.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
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
S0077	Skill in securing network communications.	Information Systems/Network Security
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	Information Systems/Network Security
K0230	Knowledge of cloud service models and possible limitations for an incident response.	Infrastructure Design
K0034	Knowledge of how network services and protocols interact to provide network communications.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design
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.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	Threat Analysis

KSA ID	Description	Competency
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	Threat Analysis
S0003	Skill of identifying, capturing, containing, and reporting malware.	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
K0062	Knowledge of packet-level analysis.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 12. T0510 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Coordinate incident response functions.	Core
Entry	*Understand and apply IR lifecycle principles. Compile analyst notes and report back.*	
Intermediate	*Coordinate incident response functions. Double check notes and validates.*	
Advanced	*Assign IR role. Consumes and analyzes information.*	

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

KSA ID	Description	Competency
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0080	Skill in performing damage assessments.	Incident Management
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	Threat Analysis
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	Threat Analysis
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 14. T0503 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Support monitoring of 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.*	
Intermediate	*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.*	
Advanced	*Oversee the monitoring of 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.*	

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

KSA ID	Description	Competency
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
S0080	Skill in performing damage assessments.	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
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	Information Systems/Network Security
K0034	Knowledge of how network services and protocols interact to provide network communications.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design
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.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	Threat Analysis
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment

KSA ID	Description	Competency
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 16. T0164 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform cyber defense trend analysis and reporting.	Core
Entry	*Record cyber defense trend analysis and reporting.*	
Intermediate	*Perform cyber defense trend analysis and reporting.*	
Advanced	*Direct and evaluate cyber defense trend analysis and reporting.*	

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

KSA ID	Description	Competency
K0026	Knowledge of disaster recovery continuity of operations plans.	Business Continuity
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
S0080	Skill in performing damage assessments.	Incident Management
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	Information Systems/Network Security
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 18. T0170 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.	Core
Entry	*Perform initial collection of the image using industry best practices and conduct initial triage.*	
Intermediate	*Perform forensic collection using industry-vetted best practices and analyze the image for signs of compromise and abnormalities. Perform timeline analysis and log analyses to investigate within different environments. Develop mitigation/remediation recommendations.*	
Advanced	*Validate the mitigation /remediation recommendations. Perform complex forensic examinations using advanced TTPs. Validate findings and verify evidence. Set vision for mission and capability and ensure organization is resourced to meet capability. Develop and update policies and procedures for mission activities.*	

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

KSA ID	Description	Competency
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0080	Skill in performing damage assessments.	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
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	Information Systems/Network Security
K0230	Knowledge of cloud service models and possible limitations for an incident response.	Infrastructure Design
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.	Infrastructure Design
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	Threat Analysis
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	Threat Analysis
S0003	Skill of identifying, capturing, containing, and reporting malware.	Threat Analysis

KSA ID	Description	Competency
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
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	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	*Perform open source and intelligence research of indicators and alerts.*	
Intermediate	*Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. Rule out false positives and examine context to identify positives. Pivot off alert to correlate information from other log sources. Produce findings for report.*	
Advanced	*Verify and validate findings and analytical methodology used, categorize/classify findings as incidents/events, and determine if follow-on actions need to be conducted.*	

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

KSA ID	Description	Competency
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0034	Knowledge of how network services and protocols interact to provide network communications.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
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.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	Threat Analysis
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
K0062	Knowledge of packet-level analysis.	Vulnerabilities Assessment

Table 22. T0395 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Write and publish after action reviews.	Core
Entry	*Assist in the development of an after action report*	
Intermediate	*Write and publish after action reviews.*	
Advanced	*Lead, author and validate subordinate After Action Reviews*	

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

KSA ID	Description	Competency
K0026	Knowledge of disaster recovery continuity of operations plans.	Business Continuity
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	Business Continuity
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
S0079	Skill in protecting a network against malware.	Computer Network Defense
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
K0042	Knowledge of incident response and handling methodologies.	Incident Management
S0080	Skill in performing damage assessments.	Incident Management
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
S0077	Skill in securing network communications.	Information Systems/Network Security
S0173	Skill in using security event correlation tools.	Information Systems/Network Security
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	Information Systems/Network Security
K0230	Knowledge of cloud service models and possible limitations for an incident response.	Infrastructure Design
K0034	Knowledge of how network services and protocols interact to provide network communications.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design
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.	Infrastructure Design
K0058	Knowledge of network traffic analysis methods.	Network Management
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	Threat Analysis

KSA ID	Description	Competency
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment
K0062	Knowledge of packet-level analysis.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 24. T0246 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	Core
Entry	*Developing input to contribute and provide for cyber defense techniques, guidance, and reports on incident findings.*	
Intermediate	*Authoring cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. Provide additional guidance for different defense techniques and providing recommendations to fineness taxonomy and technical writing.*	
Advanced	*Perform quality control and assurance (QAQC) and approve for publication/dissemination/release of cyber defense techniques, guidance, and reports.*	

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

KSA ID	Description	Competency
K0157	Knowledge of cyber defense policies, procedures, and regulations.	Computer Network Defense
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	Computer Network Defense
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	Incident Management
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information 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
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	Infrastructure Design
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	Threat Analysis
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0259	Knowledge of malware analysis concepts and methodologies.	Threat Analysis
S0003	Skill of identifying, capturing, containing, and reporting malware.	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 the relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	Vulnerabilities Assessment