CAREER PATHWAY
CYBER DEFENSE FORENSICS ANALYST (212)

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

1 212-CYBER DEFENSE FORENSICS ANALYST

1.1 Work Role Overview

The table below provides an overview of various role-specific elements related to 212-Cyber Defense Forensics Analyst.

Table 1. 212-Cyber Defense Forensics Analyst Work Role Overview

NICE Role Description	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
OPM Occupational Series	Personnel performing the 212-Cyber Defense Forensics Analyst work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210 – Information Technology (INFOSEC) – 85% - 1550-Computer Science – 4% - 1811-Criminal Investigation – 4% - 0343-Management and Program Analysis – 3% - 1801-General Inspection, Investigation, Enforcement, and Compliance Series – 3%
Work Role Pairings	Personnel performing the 212-Cyber Defense Forensics Analyst work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 511-Cyber Defense Analyst – 39% - 531-Cyber Defense Incident Responder – 18% - 211-Forensices Analyst – 11% - 221-Cyber Crime Investigator – 11% - 722-Information Systems Security Manager – 9%
Functional Titles	Personnel performing the 212-Cyber Defense Forensics Analyst work role may unofficially or alternatively be called: - Computer Forensic Analyst - Computer Network Defense (CND) Forensic Analyst - Digital Forensic Examiner - Cyber Forensic Analyst - Forensic Analyst (Cryptologic) - Forensic Technician - Network Forensic Examiner - Host Forensic Examiner
Distribution of GS-Levels	Personnel performing the 212-Cyber Defense Forensics Analyst is most commonly found within the following grades on the General Schedule. *

	- ☐ GS-7 – redacted** - ☒ GS-9 – 4% - ☒ GS-11 – 7% - ☒ GS-12 – 17% - ☒ GS-13 – 47% - ☒ GS-14 – 17% - ☐ GS-15 – redacted** *7% of all 212s are in non-GS pay plans and excluded from this GS distribution **Percentages below 3% and below are redacted
On Ramps	The following work roles are examples of logical roles an individual may perform prior to transitioning into the 212-Cyber Defense Forensics Analyst work role: - 621-Software Developer - 511-Cyber Defense Analyst - 531-Cyber Defense Incident Responder - 211-Forensics Analyst
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 212-Cyber Defense Forensics 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: - 211-Forensics Analyst - 221-Cyber Crime Investigator - 121-Exploitation Analyst - 131-Target Network Analyst *Note: Leveraging the knowledge, skills, abilities, and tasks of the 212-Cyber Defense Forensics Analyst 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* - *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 212-Cyber Defense Forensics Analyst work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 212-Cyber Defense Forensics Analyst Core Tasks

Task ID	Task Description	Core or Additional
T0027	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.	Core
T0036	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.	Core
T0075	Provide technical summary of findings in accordance with established reporting procedures.	Core
T0103	Examine recovered data for information of relevance to the issue at hand.	Core
T0167	Perform file signature analysis.	Core
T0286	Perform file system forensic analysis.	Core
T0432	Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Core
T0048	Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.	Additional
T0049	Decrypt seized data using technical means.	Additional
T0087	Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Additional
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Additional
T0165	Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.	Additional
T0168	Perform hash comparison against established database.	Additional
T0172	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	Additional
T0173	Perform timeline analysis.	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
T0179	Perform static media analysis.	Additional
T0182	Perform tier 1, 2, and 3 malware analysis.	Additional
T0190	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Additional
T0212	Provide technical assistance on digital evidence matters to appropriate personnel.	Additional

Task ID	Task Description	Core or Additional
T0216	Recognize and accurately report forensic artifacts indicative of a particular operating system.	Additional
T0238	Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).	Additional
T0240	Capture and analyze network traffic associated with malicious activities using network monitoring tools.	Additional
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Additional
T0253	Conduct cursory binary analysis.	Additional
T0279	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Additional
T0285	Perform virus scanning on digital media.	Additional
T0287	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	Additional
T0288	Perform static malware analysis.	Additional
T0289	Utilize deployable forensics toolkit to support operations as necessary.	Additional
T0312	Coordinate with intelligence analysts to correlate threat assessment data.	Additional
T0396	Process image with appropriate tools depending on analyst's goals.	Additional
T0397	Perform Windows registry analysis.	Additional
T0398	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Additional
T0399	Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.	Additional
T0400	Correlate incident data and perform cyber defense reporting.	Additional
T0401	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Additional
T0532	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	Additional
T0546	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	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 212-Cyber Defense Forensics Analyst work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 212-Cyber Defense Forensics Analyst Core KSAs

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
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics	Core
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics	Core
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics	Core
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics	Core
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics	Core
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics	Core
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics	Core
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics	Core
S0091	Skill in analyzing volatile data.	Computer Forensics	Core
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics	Core
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics	Core
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense	Core
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense	Core
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation	Core
S0062	Skill in analyzing memory dumps to extract information.	System Administration	Core
K0183	Knowledge of reverse engineering concepts.	Threat Analysis	Core

KSA ID	Description	Competency	Importance to Work Role
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis	Core
K0254	Knowledge of binary analysis.	Threat Analysis	Core
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis	Core
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis	Core
S0131	Skill in analyzing malware.	Threat Analysis	Core
K0021	Knowledge of data backup and recovery.	Business Continuity	Additional
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	Business Continuity	Additional
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics	Additional
K0128	Knowledge of types and collection of persistent data.	Computer Forensics	Additional
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics	Additional
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics	Additional
K0134	Knowledge of deployable forensics.	Computer Forensics	Additional
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	Computer Forensics	Additional
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics	Additional
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics	Additional
S0069	Skill in setting up a forensic workstation.	Computer Forensics	Additional
A0005	Ability to decrypt digital data collections.	Computer Forensics	Additional
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics	Additional
S0074	Skill in physically disassembling PCs.	Computers and Electronics	Additional
K0018	Knowledge of encryption algorithms	Encryption	Additional
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption	Additional
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	Enterprise Architecture	Additional
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Additional
K0145	Knowledge of security event correlation tools.	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

KSA ID	Description	Competency	Importance to Work Role
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence	Additional
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence	Additional
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence	Additional
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence	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
K0060	Knowledge of operating systems.	Operating Systems	Additional
K0077	Knowledge of server and client operating systems.	Operating Systems	Additional
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems	Additional
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems	Additional
K0186	Knowledge of debugging procedures and tools.	Software Development	Additional
K0078	Knowledge of server diagnostic tools and fault identification techniques.	System Administration	Additional
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration	Additional
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration	Additional
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	System Administration	Additional
K0347	Knowledge and understanding of operational design.	Systems Integration	Additional
K0189	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).	Threat Analysis	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 injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	Additional
K0119	Knowledge of hacking methodologies.	Vulnerabilities Assessment	Additional

KSA ID	Description	Competency	Importance to Work Role
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment	Additional
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment	Additional
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	Web Technology	Additional

1.4 Core Competencies

The table below is a compilation of competencies aligned to the 212-Cyber Defense Forensics 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. 212-Cyber Defense Forensics 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. 212-Cyber Defense Forensics 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 212-Cyber Defense Forensics Analyst.

2 APPENDIX: 212-CYBER DEFENSE FORENSICS 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.

2.2 212-Cyber Defense Forensics Analyst Task Analysis and KSA Mapping

Table 8. T0027 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Conduct analysis of all available data sets (e.g. network device logs, PCAP, netflow) in order to determine and identify a network intrusion.	Core
Entry	*Assist with the analysis, correlation, and documentation of all data sets.*	
Intermediate	*Conduct and lead the analysis of all available data sets. Determining if the data sets are sufficient and if/which additional data sets are available/exist.*	
Advanced	*Set criteria and methodology for analysis requirements, develop new methods for analysis and correlation within the diverse data sets, perform quality management and oversight, brief senior leaders on findings, 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
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption
K0018	Knowledge of encryption algorithms	Encryption
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0145	Knowledge of security event correlation tools.	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
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation
S0062	Skill in analyzing memory dumps to extract information.	System Administration
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis
K0254	Knowledge of binary analysis.	Threat Analysis
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
K0119	Knowledge of hacking methodologies.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	Web Technology

Table 10. T0036 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. Identify an intrusion, discover new information, and validate the extent of the intrusion.	Core
Entry	*Assist with discovery with the initial attack/infection vector and identify/research the TTPs of the intrusion.*	
Intermediate	*Identify artifacts associated with the event/intrusion, review for conditions/factors/causality, and document findings.*	
Advanced	*Validate the accuracy of the TTPs surrounding the intrusion, and document forensic analysis findings.*	

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

KSA ID	Description	Competency
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense
K0018	Knowledge of encryption algorithms	Encryption
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0145	Knowledge of security event correlation tools.	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
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design

KSA ID	Description	Competency
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation
S0062	Skill in analyzing memory dumps to extract information.	System Administration
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
K0347	Knowledge and understanding of operational design.	Systems Integration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis
K0254	Knowledge of binary analysis.	Threat Analysis
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	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
K0119	Knowledge of hacking methodologies.	Vulnerabilities Assessment
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment
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

Table 12. T075 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide technical summary of findings in accordance with established reporting procedures.	Core
Entry	*Learning establish reporting procedures and requirements for documentation and draft technical summary of findings.*	
Intermediate	*Author of technical summary of findings and perform initial quality control management and peer reviews.*	
Advanced	*Approve technical summary of finding, develop new templates/requirements for documentation/playbooks, write white papers, oversee the update lifecycle of reports or documentation.*	

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

KSA ID	Description	Competency
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
S0062	Skill in analyzing memory dumps to extract information.	System Administration
K0347	Knowledge and understanding of operational design.	Systems Integration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment

Table 14. T0103 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Examine recovered data for information of relevance to the issue at hand.	Core
Entry	*Understand and be proficient in understanding the artifacts and sources to the matter at hand. Use automated tools and programs to examine recovered data, per agency protocols.*	
Intermediate	*Utilize custom/individual/manual methods to examine recovered data and/or validate the automated tools and program findings, per agency protocols.*	
Advanced	*Author/Develop scripts for advanced examination of recovered data to determine relevance to the issue at hand.*	

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

KSA ID	Description	Competency
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption
K0018	Knowledge of encryption algorithms	Encryption
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0145	Knowledge of security event correlation tools.	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

KSA ID	Description	Competency
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation
S0062	Skill in analyzing memory dumps to extract information.	System Administration
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis
K0254	Knowledge of binary analysis.	Threat Analysis
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	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
K0119	Knowledge of hacking methodologies.	Vulnerabilities Assessment
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	Web Technology

Table 16. T0167 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform file signature analysis.	Core
Entry	*Under supervision, perform file signature analysis.*	
Intermediate	*Perform file signature analysis.*	
Advanced	*Manage and evaluate file signature analysis.*	

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

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0134	Knowledge of deployable forensics.	Computer Forensics
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense
S0074	Skill in physically disassembling PCs.	Computers and Electronics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption
K0018	Knowledge of encryption algorithms	Encryption

KSA ID	Description	Competency
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	Enterprise Architecture
K0145	Knowledge of security event correlation tools.	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation
S0062	Skill in analyzing memory dumps to extract information.	System Administration
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis
K0189	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).	Threat Analysis
K0005	Knowledge of cyber threats and vulnerabilities.	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
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment
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
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	Web Technology

Table 18. T0286 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform file system forensic analysis.	Core
Entry	*Identify different types of file system types, forensic tools sets compatible with the file system, and assist with the analysis.*	
Intermediate	*Perform file system forensic analysis.*	
Advanced	*Perform complex file system forensic analysis and validate peer/subordinate forensic analysis.*	

Table 19. 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
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems
K0060	Knowledge of operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation
S0062	Skill in analyzing memory dumps to extract information.	System Administration
K0078	Knowledge of server diagnostic tools and fault identification techniques.	System Administration

KSA ID	Description	Competency
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis
K0254	Knowledge of binary analysis.	Threat Analysis
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment

Table 20. T0432 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use findings to enable mitigation of vulnerabilities within the enterprise and provide recommendations for remediation.	Core
Entry	*Assist with the collection and analysis of artifacts, as well as the mitigation of vulnerabilities.*	
Intermediate	*Complete dynamic and static analyses, lead attribution activities, independently complete the full lifecycle of collection and analysis of artifacts, document findings to identify potential vulnerabilities, provide remediation recommendations.*	
Advanced	*Provide technical direction to team, proficient at complex collection and analysis of artifacts, recommendations for vulnerability or event remediation, define procedures and processes for the enterprise.*	

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

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	Computer Forensics
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0304	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0134	Knowledge of deployable forensics.	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	Enterprise Architecture
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems

KSA ID	Description	Competency
S0132	Skill in conducting bit-level analysis.	Software Testing and Evaluation
S0062	Skill in analyzing memory dumps to extract information.	System Administration
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	System Administration
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis
S0131	Skill in analyzing malware.	Threat Analysis
K0183	Knowledge of reverse engineering concepts.	Threat Analysis
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis
K0254	Knowledge of binary analysis.	Threat Analysis
S0156	Skill in performing packet-level analysis.	Vulnerabilities Assessment
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	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
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment