Cybersecurity
at Columbus State

Associate of Applied Science in Cybersecurity
Launching 2017

JOB SKILLS ANALYSIS- By Jeremy Porter

Mapped Results from Cyber Security Compression Planning

Introduction

The summary below is an attempt to map the results of compression planning to the Cyber Security Workforce Framework. There are some key points to understand:

- The results of compression planning are in some cases very general and in others very specific.
- The National Cybersecurity Workforce Framework is very good at both general categories and specific tasks/knowledge, skills and abilities, but there are areas where the framework does not have specific coverage, for example mobile devices.
- Mapping results is challenging due to words used, different implementations of technology, etc.
- The true results are a many to many relationship. Many to many relationships are difficult to display are not necessary for correlation between compression planning and the National Cybersecurity Workforce Frame work. Below is a summary of a one to many relationship.

Regardless of the above points, there is clear evidence that the compression planning results align closely with the National Cybersecurity workforce Framework.

Role 1 Network Security Analysis (the primary role)

Framework Summary

Category	Specialty Area
Protect and Defend	Computer Network Defense Analysis, Computer Network Defense Infrastructure Support, Vulnerability Assessment and Management
Operate and Maintain	Network Services
Oversight and Development	Information Systems Security Operations

1.01 Monitor network segmentation

Category	Specialty Area
Protect and Defend	Computer Network Defense Analysis, Computer Network Defense Infrastructure Support

Example Tasks/KSA’s

- Examine network topologies to understand data flows through the network
- Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR)
- Identify applications and operating systems of a network device based on network traffic
- Identify network mapping and operating system (OS) fingerprinting activities
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise
- Perform Computer Network Defense trend analysis and reporting

1.02 Prevent intrusion

Category	Specialty Area
Protect and Defend	Computer Network Defense Analysis, Computer Network Defense Infrastructure Support

Framework Category: Protect and Defend
Specialty Areas: Computer Network Defense Analysis, Computer Network Defense Infrastructure Support
Example Tasks/KSA's

- Skill in applying host/network access controls (e.g., access control list)
- Skill in assessing the robustness of security systems and designs
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)
- Skill in evaluating the trustworthiness of the supplier and/or product
- Skill in mimicking threat behaviors

1.03 Detect intrusion

Category	Specialty Area
Protect and Defend	Computer Network Defense Analysis, Computer Network Defense Infrastructure Support

Example Tasks/KSA's

- Knowledge of network traffic analysis methods
- Knowledge of packet-level analysis
- Knowledge of the types of intrusion detection system hardware and software
- Knowledge of intrusion detection system tools and applications
- Knowledge of incident response and handling methodologies
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)

1.04 Operate and maintain firewalls

Category	Specialty Area
Protect and Defend	Computer Network Defense Analysis, Computer Network Defense Infrastructure Support
Operate and Maintain	Network Services

Example Tasks/KSA's

- Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems)
- Skill in identifying common encoding techniques (XOR, ASCII, Unicode, Base64, Uuencode, URL encode)
- Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)
- Skill in reading and interpreting signatures (e.g. snort)
- Skill in using protocol analyzers
- Skill in using sub-netting tools

1.05 Operate and maintain routing

Category	Specialty Area
Operate and Maintain	Network Services

Example Tasks/KSA's

- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
- 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, v3 (ITIL))
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling, etc.)
- Repair network connectivity problems
- Monitor network capacity and performance

1.06 Engage in offensive security (prevention testing, also known as ethical hacking)

Category	Specialty Area
Protect and Defend	Vulnerability Assessment and Management

Example Tasks/KSA's

- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)
- Skill in mimicking threat behaviors
- Skill in the use of penetration testing tools and techniques
- Skill in the use of social engineering techniques
- Skill in using network analysis tools to identify vulnerabilities
- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution, etc.)

1.07 Follow protocols

Category	Specialty Area
Oversight and Development	Information Systems Security Operations

Example Tasks/KSA's

- Knowledge of systems lifecycle management principles, including software security and usability
- Knowledge of the organization
- Knowledge of organization's risk tolerance and/or risk management approach
- Knowledge of Personally Identifying Information (PII) and personal Payment Card Industry (PCI) data security standards
- Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure
- Knowledge of industry-standard and organizationally accepted analysis principles and methods

Role 2. Risk Analysis

Framework Summary

Category	Specialty Area
Securely Provision	**Systems Development, Information Assurance Compliance, Systems Requirements Planning, Systems Security Architecture**
Oversight and Development	**Information Systems Security Operations**

2.01 Conduct qualitative and quantitative analysis of risks for the current system

Category	Specialty Area
Securely Provision	Systems Development

Example Tasks/KSA's

- Knowledge of organization's risk tolerance and/or risk management approach
- Knowledge of risk management processes, including steps and methods for assessing risk
- Knowledge of risk threat assessment
- Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system
- Perform an information security risk assessment and design security countermeasures to mitigate identified risks
- Skill in designing countermeasures to identified security risks

2.02 Perform methodology for proven risk assessments

Category	Specialty Area
Securely Provision	Information Assurance Compliance

Example Tasks/KSA's

- Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities
- Knowledge of current industry methods for evaluating, implementing, and disseminating IT security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities
- Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Knowledge of the organization's core business/mission processes
- Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
- Skill in evaluating the trustworthiness of the supplier and/or product

2.03 Classify data

Category	Specialty Area
Securely Provision	Information Assurance Compliance, Systems Requirements Planning, Systems Security Architecture

Example Tasks/KSA's

- Knowledge of Personally Identifying Information (PII) and personal Payment Card Industry (PCI) data security standards
- Knowledge of IA principles used to manage risks related to the use, processing, storage, and transmission of information or data
- Develop IA designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET)
- Define appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration
- Identify the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately
- Identify and prioritize critical business functions in collaboration with organizational stakeholders

2.04 Execute compliance against internal policies, industry standards, and pertinent regulations

Category	Specialty Area
Securely Provision	Information Assurance Compliance, Information Systems Security Operations

Example Tasks/KSA's

- Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), 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 relevant to work performed
- Knowledge of current industry methods for evaluating, implementing, and disseminating IT security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities
- Knowledge of disaster recovery continuity of operations plans
- Knowledge of enterprise incident response program, roles, and responsibilities
- Knowledge of IA principles used to manage risks related to the use, processing, storage, and transmission of information or data
- Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure

Role 3. Security Awareness Analysis

Category	Specialty Area
Oversight and Development	Information Systems Security Operations, Education and Training
Protect and Defend	Vulnerability Assessment and Management

3.01 Educate vendors and users on security awareness issues

Category	Specialty Area
Oversight and Development	Information Systems Security Operations, Education and Training

- Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents
- Collect and maintain data needed to meet system IA reporting
- Define and/or implement policies and procedures to ensure protection of critical infrastructure (as appropriate)
- Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures
- Guide employees through relevant development and training choices
- Educate customers in established procedures and processes to ensure professional media standards are met

3.02 Educate vendors and users on phishing campaigns

Category	Specialty Area
Oversight and Development	Education and Training

- Knowledge of emerging security issues, risks, and vulnerabilities
- Skill in talking to others to convey information effectively
- Knowledge of emerging computer-based technology that have potential for exploitation by adversaries
- Determine training requirements (e.g., subject matter, format, location)
- Demonstrate concepts, procedures, software, equipment, and technology applications to coworkers, subordinates, or others
- Conduct interactive training exercises to create an effective learning environment

3.03 Conduct table top exercises

Category	Specialty Area
Oversight and Development	Education and Training

- Support the design and execution of exercise scenarios
- Evaluate the effectiveness and comprehensiveness of existing training programs

- Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)
- Review training documentation (e.g., Course Content Documents [COD], Lesson Plans, Student Texts, examinations, Schedules of Instruction [SOI], course descriptions)
- Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media, cartography)
- Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce

3.04 Conduct war gaming on the existing system

Category	Specialty Area
Oversight and Development	Education and Training

- Support the design and execution of exercise scenarios
- Evaluate the effectiveness and comprehensiveness of existing training programs
- Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)
- Review training documentation (e.g., Course Content Documents [COD], Lesson Plans, Student Texts, examinations, Schedules of Instruction [SOI], course descriptions)
- Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media, cartography)
- Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce

3.05 Conduct social engineering awareness training

Category	Specialty Area
Oversight and Development	Education and Training
Protect and Defend	Vulnerability Assessment and Management

- Support the design and execution of exercise scenarios
- Evaluate the effectiveness and comprehensiveness of existing training programs
- Plan non-classroom educational techniques and formats (e.g., video courses, personal coaching, web-based courses)
- Review training documentation (e.g., Course Content Documents [COD], Lesson Plans, Student Texts, examinations, Schedules of Instruction [SOI], course descriptions)
- Skill in the use of social engineering techniques
- Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce

Role 4. Identity Access Analysis

Category	Specialty Area
Operate and Maintain	System Administration, System Security Analysis, Test and Evaluation
Securely Provision	System Security Architecture
Oversight and Development	Information Systems Security Operations
Protect and Defend	Vulnerability Assessment and Management

4.01 Manage user access rights

Category	Specialty Area
Operate and Maintain	System Administration

- Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs
- Knowledge of file system implementations (e.g., NTFS, FAT, EXT)
- Knowledge of organizational IT user security policies (e.g. account creation, password rules, access, control, etc.)
- Knowledge of basic system administration, network, and operating system hardening techniques

- Manage accounts, network rights, and access to systems and equipment
- Skill in identifying and anticipating server performance, availability, capacity, or configuration problems

4.02 Operate multi-factor authentication

Category	Specialty Area
Operate and Maintain	System Administration, System Security Analysis
Securely Provision	System Security Architecture

- Knowledge of access authentication methods
- Knowledge of network access, identity and access management (e.g., public key infrastructure, PKI)
- Knowledge of organizational IT user security policies (e.g. account creation, password rules, access, control, etc.)
- Knowledge of policy-based and risk adaptive access controls
- Skill in applying host/network access controls (e.g., access control list)
- Skill in developing and applying security system access controls
- Skill in maintaining directory services

4.03 Serve as liaison between the operations team, equipment and space

Category	Specialty Area
Operate and Maintain	System Administration
Oversight and Development	Information Systems Security Operations

- Oversee installation, implementation, configuration, and support of network components
- Manage accounts, network rights, and access to systems and equipment
- Manage server resources including performance, capacity, availability, serviceability, and recoverability
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents
- Recommend resource allocations required to securely operate and maintain an organization

4.04 Conduct "what if" analyses of multiple scenarios

Category	Specialty Area
Securely Provision	Test and Evaluation
Protect and Defend	Vulnerability Assessment and Management

- Knowledge of systems administration concepts
- Knowledge of the systems engineering process
- Skill in conducting test events
- Skill in the use of penetration testing tools and techniques
- Skill in mimicking threat behaviors
- Skill in performing damage assessments

4.05 Serve as a project manager

Category	Specialty Area
Oversight and Development	Security Program Management

- Skill in deconflicting cyber operations and activities
- Manage threat or target analysis of Computer Network Defense information and production of threat information within the enterprise
- Monitor and evaluate the effectiveness of the enterprise's IA security safeguards to ensure they provide the intended level of protection
- Lead and align IT security priorities with the security strategy
- Lead and oversee information security budget, staffing, and contracting

- Evaluate cost benefit, economic, and risk analysis in decision making process

Role 5. Vulnerability Analysis

Category	Specialty Area
Protect and Defend	Vulnerability Assessment and Management
Investigate	Digital Forensics, Investigation
Protect and Defend	Incident Response

5.01 Run scans of the system

Category	Specialty Area
Protect and Defend	Vulnerability Assessment and Management

- Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions
- Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (i.e., local computing environment, network and infrastructure, enclave boundary, and supporting infrastructure)
- Conduct and/or support authorized penetration testing on enterprise network assets
- Knowledge of application vulnerabilities
- Knowledge of content development
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)

5.02 Validate system penetrations

Category	Specialty Area
Protect and Defend	Vulnerability Assessment and Management

- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit, etc.)
- Knowledge of programming language structures and logic
- Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure
- Knowledge of system and application security threats and vulnerabilities
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)

5.03 Triage system penetrations

Category	Specialty Area
Investigate	Digital Forensics, Investigation
Protect and Defend	Incident Response

- Knowledge of basic concepts and practices of processing digital forensic data
- Knowledge of common forensics tool configuration and support applications (e.g., VMWare, WIRESHARK)
- Knowledge of seizing and preserving digital evidence (e.g., chain of custody)
- Knowledge of incident response and handling methodologies
- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies
- Knowledge of malware analysis concepts and methodology

5.04 Manage vendor tool sets

Category	Specialty Area
Protect and Defend	Vulnerability Assessment and Management

- Skill in evaluating the trustworthiness of the supplier and/or product
- Skill in using network analysis tools to identify vulnerabilities
- Knowledge of programming language structures and logic
- Skill in mimicking threat behaviors
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
- Knowledge of application vulnerabilities

Role 6. End Point Security Controls Analysis

Category	Specialty Area
Operate and Maintain	Network Services
Protect and Defend	Computer Network Defense Infrastructure Support
Operate and Maintain	Customer Service and Technical Support

6.01 Manage mobile devices[1]

Category	Specialty Area
Operate and Maintain	Network Services

- Knowledge of communication methods, principles, and concepts (e.g., crypto, dual hubs, time multiplexers, etc.) that support the network infrastructure
- Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN, etc.)
- Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts)
- Knowledge of Voice over IP (VoIP)
- Skill in testing and configuring network workstations and peripherals

6.02 Operate anti-virus software

Category	Specialty Area
Protect and Defend	Computer Network Defense Infrastructure Support

- Perform system administration on specialized Computer Network Defense applications and systems (e.g., anti-virus, Audit/Remediation, or VPN devices) to include installation, configuration, maintenance, and backup/restore
- Skill in protecting a network against malware
- Knowledge of network traffic analysis methods
- Knowledge of packet-level analysis
- Knowledge of web filtering technologies
- Skill in securing network communications

6.03 Monitor and manage firewalls

Category	Specialty Area
Protect and Defend	Computer Network Defense Infrastructure Support
Operate and Maintain	Network Services

- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Knowledge of network traffic analysis methods
- Knowledge of packet-level analysis

[1] National Cybersecurity Workforce Framework does not explicitly cover this.

- Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers, as appropriate)
- Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems)
- Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol)

6.04 Perform disk encryption

Category	Specialty Area
Operate and Maintain	Customer Service and Technical Support
Protect and Defend	Computer Network Defense Analysis

- Skill in testing and configuring network workstations and peripherals
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)
- Knowledge of file system implementations (e.g., NTFS, FAT, EXT)
- Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption
- Knowledge of encryption methodologies

6.05 Perform host based intrusion prevention (HIPS)

Category	Specialty Area
Protect and Defend	Computer Network Defense Analysis

- Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)
- Employ approved Defense-in-Depth principles and practices (i.e., Defense in Multiple Places, Layered defenses, Security robustness, etc.)
- Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR)
- Knowledge of Windows/Unix ports and services
- Skill in reading and interpreting signatures (e.g. snort)
- Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)

Role 7. Application Security Analysis

Category	Specialty Area
Securely Provision	Software and Security Engineering, Software Assurance and Security Engineering, Technology Research and Development
Protect and Defend	Vulnerability Assessment and Management
Investigate	Digital Forensics

7.01 Develop secure coding/secure software

Category	Specialty Area
Securely Provision	Software and Security Engineering

- Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules
- Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements
- Develop threat model based on customer interviews and requirements
- Perform integrated quality assurance testing for security functionality and resiliency attack
- Perform penetration testing as required for new or updated applications

- Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change

7.02 Develop tools

Category	Specialty Area
Protect and Defend	Vulnerability Assessment and Management

- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in mimicking threat behaviors
- Knowledge of system and application security threats and vulnerabilities
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)
- Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit, etc.)
- Knowledge of programming language structures and logic

7.03 Conduct run-time monitoring

Category	Specialty Area
Investigate	Digital Forensics
Securely Provision	Software Assurance and Security Engineering, Technology Research and Development

- Knowledge of debugging procedures and tools
- Knowledge of Middleware
- Knowledge of software debugging principles
- Knowledge of software design tools, methods, and techniques
- Skill in conducting software debugging
- Skill in using code analysis tools to eradicate bugs

Role 8. Incident Response Analysis

Category	Specialty Area
Investigate	Digital Forensics, Investigation
Protect and Defend	Incident Response

8.01 Conduct digital forensics

Category	Specialty Area
Investigate	Digital Forensics

- Skill in identifying obfuscation techniques
- Skill in identifying, modifying, and manipulating applicable system components (Windows and/or Unix/Linux) (e.g., passwords, user accounts, files)
- Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures
- Skill in one way hash functions (e.g., Sha, MDS)
- Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)
- Skill in analyzing anomalous code as malicious or benign

8.02 Maintain chain of custody

Category	Specialty Area
Investigate	Digital Forensics

- Knowledge of seizing and preserving digital evidence (e.g., chain of custody)

- Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Knowledge of legal governance related to admissibility (Federal Rules of Evidence)
- Knowledge of legal rules of evidence and court procedure
- Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies
- Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files
- Knowledge of types and collection of persistent data

8.03 Document findings

Category	**Specialty Area**
Investigate	Investigation

- Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action
- Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations
- Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
- Identify elements of proof of the crime
- Examine recovered data for information of relevance to the issue at hand
- Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion

8.04 Follow incident response methodology

Category	**Specialty Area**
Protect and Defend	Incident Response

- Knowledge of incident categories, incident responses, and timelines for responses
- Knowledge of incident response and handling methodologies
- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies
- Knowledge of malware analysis concepts and methodology
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)