TestOut®

TestOut CyberDefense Pro – English 1.0.x

Objective Mappings:

TestOut CyberDefense Pro
CompTIA CySA+ CS0-002

Revised: 2021-04-22

Powered by LABSIM

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut CyberDefense Pro Objective

Section	Title	Objectives
1.0	**Introduction**	
1.1	Introduction to TestOut CyberDefense Pro	
2.0	**Threat Intelligence**	
2.1	Penetration Testing and Threat Hunting	2.1 Perform threat analysis 2.1.3 Determine the types of vulnerabilities associated with different attacks 2.2 Detect threats using analytics and intelligence 2.2.1 Use an Intrusion Detection System (IDS) 3.3 Perform penetration tests 3.3.1 Perform internal penetration testing 3.3.2 Perform external penetration testing
2.2	Organizational Security	
2.3	Security Controls	
3.0	**Risk Mitigation**	
3.1	Risk Identification Process	
3.2	Risk Calculation	
3.3	Risk Communication and Training	
4.0	**Social and Physical Security**	

4.1	Social Engineering	1.2 Monitor software and systems 1.2.4 Monitor email for malware
4.2	Physical Security	
4.3	Countermeasures and Prevention	5.2 Implement physical security controls 5.2.1 Analyze physical security design to protect systems
5.0	**Reconnaissance**	
5.1	Reconnaissance Overview	
5.2	Reconnaissance Countermeasures	1.2 Monitor software and systems 1.2.3 Review web application security 3.2 Implement system hardening 3.2.1 Disable unnecessary services
5.3	Scanning	1.2 Monitor software and systems 1.2.2 Analyze executable processes 2.1 Perform threat analysis 2.1.1 Review firewall configuration 3.3 Perform penetration tests 3.3.2 Perform external penetration testing

		4.3 Analyze Indicators of compromise 4.3.2 Inspect systems for any signs of compromise
6.0	**Enumeration**	
6.1	Enumeration Overview	
6.2	Enumeration Countermeasures	3.2 Implement system hardening 3.2.2 Check service configuration
7.0	**Vulnerability Management**	
7.1	Vulnerability Assessment	
7.2	Vulnerability Management Life Cycle	
7.3	Vulnerability Scoring Systems	
7.4	Vulnerability Analysis	2.1 Perform threat analysis 2.1.3 Determine the types of vulnerabilities associated with different attacks
8.0	**Identity and Access Management Security (IAM)**	
8.1	Identity and Access Management Security	5.1 Implement Identity and Access Management (IAM) 5.1.1 Administer user accounts 5.1.2 Manage user-based and role-based access 5.1.4 Configure account policies and account control
8.2	Privilege Escalation	5.1 Implement Identity and Access Management (IAM)

		5.1.4 Configure account policies and account control
8.3	Identity and Access Management Threats	4.3 Analyze Indicators of compromise 4.3.1 Examine applications for any signs of compromise 5.1 Implement Identity and Access Management (IAM) 5.1.4 Configure account policies and account control
8.4	Certificate Management	
9.0	**Cybersecurity Threats**	
9.1	Malware	4.1 Manage security incidents 4.1.1 Resolve malware, ransomware, and phishing attacks
9.2	Combat Malware	1.1 Monitor networks 1.1.2 Monitor network ports and sockets
9.3	Sniffing	4.3 Analyze Indicators of compromise 4.3.3 Investigate networks for any signs of compromise
9.4	Session Hijacking	1.2 Monitor software and systems 1.2.3 Review web application security 2.1 Perform threat analysis

		2.1.3 Determine the types of vulnerabilities associated with different attacks
9.5	Denial of Service	4.1 Manage security incidents 4.1.3 Respond to Distributed Denial of Service (DDoS) attacks
9.6	SQL Injections	2.1 Perform threat analysis 2.1.3 Determine the types of vulnerabilities associated with different attacks
10.0	**Infrastructure Security**	
10.1	Intrusion Detection Systems	2.2 Detect threats using analytics and intelligence 2.2.1 Use an Intrusion Detection System (IDS)
10.2	Firewalls	2.1 Perform threat analysis 2.1.1 Review firewall configuration 3.1 Implement security controls to mitigate risk 3.1.2 Configure host firewall policies 4.2 Manage devices 4.2.5 Implement network access control (NAC)
10.3	Honeypots and DNS Sinkholes	3.4 Implement defensive deception methods 3.4.1 Deploy a honeypot

		3.4.2 Implement a black hole or sinkhole
10.4	Web Servers	
10.5	Network Access	4.2 Manage devices 4.2.5 Implement network access control (NAC)
10.6	Web Applications	1.2 Monitor software and systems 1.2.3 Review web application security
10.7	Specialized Technology	1.2 Monitor software and systems 1.2.1 Configure execution control and verify digital signatures 4.2 Manage devices 4.2.3 Secure embedded devices
11.0	**Wireless and IoT Security**	
11.1	Wireless Security	
11.2	Bluetooth Security	3.2 Implement system hardening 3.2.1 Disable unnecessary services
11.3	Mobile Device Security	4.2 Manage devices 4.2.1 Secure smartphones, tablets, and laptops

11.4	Cloud Security	3.1 Implement security controls to mitigate risk 3.1.5 Implement cloud security
11.5	Internet of Things Security	4.2 Manage devices 4.2.4 Secure IOT devices
12.0	**Infrastructure Analysis**	
12.1	Hardware Analysis	
12.2	Security Information and Event Management (SIEM)	1.1 Monitor networks 1.1.1 Monitor network traffic 1.3 Implement Logging 1.3.1 Manage and perform analysis using Security Information and Event Management (SIEM) tools 3.1 Implement security controls to mitigate risk 3.1.7 Implement and configure a security appliance
12.3	Log Review	1.3 Implement Logging 1.3.2 Review event logs 1.3.3 Send log events to a remote syslog server 1.3.4 Review firewall logs
12.4	Asset and Change Management	
12.5	Virtualization Management	

13.0	Software Assurance	
13.1	Software Development Overview	
13.2	Automation	
14.0	**Data Analysis**	
14.1	Data Analysis and Protection	4.2 Manage devices 4.2.2 Implement data loss prevention
14.2	Hashing	1.2 Monitor software and systems 1.2.1 Configure execution control and verify digital signatures
14.3	Digital Forensics	2.2 Detect threats using analytics and intelligence 2.2.5 Perform digital forensics investigations
14.4	Email Analysis	1.2 Monitor software and systems 1.2.4 Monitor email for malware
15.0	**Incident Response**	
15.1	Incident Response - Preparation	
15.2	Incident Response - Detection and Containment	4.3 Analyze Indicators of compromise 4.3.1 Examine applications for any signs of compromise 4.3.2 Inspect systems for any signs of compromise 4.3.3 Investigate networks for any signs of compromise 4.3.4 Analyze indicators for false positives and false negatives

15.3	Incident Response - Eradication and Recovery	4.1 Manage security incidents 4.1.2 Eradicate Advanced Persistent Threats (APT)
15.4	Indicators of Compromise	1.2 Monitor software and systems 1.2.2 Analyze executable processes 4.3 Analyze Indicators of compromise 4.3.1 Examine applications for any signs of compromise 4.3.2 Inspect systems for any signs of compromise 4.3.3 Investigate networks for any signs of compromise
A.0	**TestOut CyberDefense Pro Practice Exams**	
A.1	Prepare for TestOut CyberDefense Pro Certification	
A.2	TestOut CyberDefense Pro Domain Review	
B.0	**CompTIA CySA+ CS0-002 - Practice Exams**	
B.1	Prepare for CompTIA CySA+ Certification	
B.2	CompTIA CySA+ CS0-002 Practice Exams (20 Questions)	
B.3	CompTIA CySA+ CS0-002 Practice Exams (All Questions)	

Objective Mapping: TestOut CyberDefense Pro Objective to LabSim Section

#	Domain	Module.Section
1.0	**Monitoring and Log Analysis**	
1.1	Monitor networks 1.1.1 Monitor network traffic 1.1.2 Monitor network ports and sockets	9.2 12.2
1.2	Monitor software and systems 1.2.1 Configure execution control and verify digital signatures 1.2.2 Analyze executable processes 1.2.3 Review web application security 1.2.4 Monitor email for malware 1.2.5 Analyze email headers and impersonation attempts	4.1 5.2, 5.3 9.4, 9.6 10.6, 10.7 14.2, 14.4 15.4
1.3	Implement Logging 1.3.1 Manage and perform analysis using Security Information and Event Management (SIEM) tools 1.3.2 Review event logs 1.3.3 Send log events to a remote syslog server 1.3.4 Review firewall logs	12.2, 12.3
2.0	**Threat Analysis and Detection**	
2.1	Perform threat analysis 2.1.1 Review firewall configuration 2.1.2 Conduct a trend analysis 2.1.3 Determine the types of vulnerabilities associated with different attacks	2.1 5.3 7.4 9.4, 9.6 10.2

2.2	Detect threats using analytics and intelligence 2.2.1 Use an Intrusion Detection System (IDS) 2.2.2 Use a protocol analyzer and packet analysis to determine threats 2.2.3 Use endpoint protection tools 2.2.4 Check for privilege escalation 2.2.5 Perform digital forensics investigations	2.1 10.1 14.3
3.0	**Risk Analysis and Mitigation**	
3.1	Implement security controls to mitigate risk 3.1.1 Detect unpatched systems 3.1.2 Configure host firewall policies 3.1.3 Implement anti-virus and endpoint security 3.1.4 Implement Intrusion Prevention System (IPS) 3.1.5 Implement cloud security 3.1.6 Perform application and data protection tasks 3.1.7 Implement and configure a security appliance	9.6 10.2 11.4 12.2
3.2	Implement system hardening 3.2.1 Disable unnecessary services 3.2.2 Check service configuration 3.2.3 Disable unnecessary ports	5.2 6.2 11.2
3.3	Perform penetration tests 3.3.1 Perform internal penetration testing 3.3.2 Perform external penetration testing	2.1 5.3
3.4	Implement defensive deception methods 3.4.1 Deploy a honeypot	10.3

	3.4.2 Implement a black hole or sinkhole 3.4.3 Configure a captive portal	
4.0	**Incident Response**	
4.1	Manage security incidents 4.1.1 Resolve malware, ransomware, and phishing attacks 4.1.2 Eradicate Advanced Persistent Threats (APT) 4.1.3 Respond to Distributed Denial of Service (DDoS) attacks	9.1, 9.5 15.3
4.2	Manage devices 4.2.1 Secure smartphones, tablets, and laptops 4.2.2 Implement data loss prevention 4.2.3 Secure embedded devices 4.2.4 Secure IOT devices 4.2.5 Implement network access control (NAC)	10.2, 10.5, 10.7 11.3, 11.5 14.1
4.3	Analyze Indicators of compromise 4.3.1 Examine applications for any signs of compromise 4.3.2 Inspect systems for any signs of compromise 4.3.3 Investigate networks for any signs of compromise 4.3.4 Analyze indicators for false positives and false negatives	5.3 8.3 9.3 15.2, 15.4
5.0	**Audit and Compliance**	
5.1	Implement Identity and Access Management (IAM) 5.1.1 Administer user accounts 5.1.2 Manage user-based and role-based access 5.1.3 Manage certificates 5.1.4 Configure account policies and account control	2.3 3.3 5.3 6.2 7.4, 8.1, 8.2, 8.3 9.6 14.4

5.2	Implement physical security controls 5.2.1 Analyze physical security design to protect systems 5.2.2 Analyze system security design to protect systems 5.2.3 Implement drive encryption 5.2.4 Implement physical access controls	4.3

Objective Mapping: LabSim Section to CompTIA CySA+ CS0-002 Objective

TestOut Section	Title	CompTIA CySA+ Objectives
1.0	**Introduction**	
1.1	Introduction to TestOut CyberDefense Pro	
2.0	**Threat Intelligence**	
2.1	Penetration Testing and Threat Hunting	1.1 Explain the importance of threat data and intelligence. 1.1.1 Intelligence sources 1.1.1.1 Open-source intelligence 1.1.1.2 Proprietary/closed-source intelligence 1.1.1.3 Timeliness 1.1.1.4 Relevancy 1.1.1.5 Accuracy 1.1.2 Confidence levels 1.1.3 Indicator management 1.1.3.1 Structured Threat Information eXpression (STIX) 1.1.3.2 Trusted Automated eXchange of Indicator Information (TAXII)

		1.1.3.3 OpenIoC 1.1.4 Threat classification 1.1.4.1 Known threat vs. unknown threat 1.1.4.2 Zero-day 1.1.4.3 Advanced persistent threat 1.1.5 Threat actors 1.1.5.1 Nation-state 1.1.5.2 Hacktivist 1.1.5.3 Organized crime 1.1.5.4 Insider threat - Intentional 1.1.5.5 Insider threat - Unintentional 1.1.6 Intelligence cycle 1.1.6.1 Requirements 1.1.6.2 Collection 1.1.6.3 Analysis 1.1.6.4 Dissemination 1.1.6.5 Feedback 1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.3 Mapping/enumeration 3.3 Explain the importance of proactive threat hunting. 3.3.1 Establishing a hypothesis 3.3.2 Profiling threat actors and activities 3.3.3 Threat hunting tactics

		3.3.3.1 Executable process analysis 3.3.4 Reducing the attack surface area 3.3.5 Bundling critical assets 3.3.6 Attack vectors 3.3.7 Integrated intelligence 3.3.8 Improving detection capabilities 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
2.2	Organizational Security	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.1 Attack frameworks 1.2.1.1 MITRE ATT&CK 1.2.1.2 The Diamond Model of Intrusion Analysis 1.2.1.3 Kill chain 1.2.2 Threat research 1.2.2.1 Reputational 1.2.2.2 Behavioral 1.2.2.3 Indicator of compromise (IoC) 1.2.2.4 Common vulnerability scoring system (CVSS) 1.2.3 Threat modeling methodologies 1.2.3.1 Adversary capability 1.2.3.2 Total attack surface 1.2.3.3 Attack vector 1.2.3.4 Impact

		1.2.3.5 Likelihood 1.2.4 Threat intelligence sharing with supported functions 1.2.4.1 Incident response 1.2.4.2 Vulnerability management 1.2.4.3 Risk management 1.2.4.4 Security engineering 1.2.4.5 Detection and monitoring 3.3 Explain the importance of proactive threat hunting. 3.3.6 Attack vectors 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.1 Frameworks
2.3	Security Controls	5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.1 Frameworks 5.3.1.1 Risk-based 5.3.1.2 Prescriptive 5.3.2 Policies and procedures 5.3.2.1 Code of conduct/ethics 5.3.2.2 Acceptable use policy (AUP) 5.3.2.3 Password policy 5.3.2.4 Data ownership 5.3.2.5 Data retention 5.3.2.6 Account management 5.3.2.7 Continuous monitoring 5.3.2.8 Work product retention

		5.3.3 Category 5.3.3.1 Managerial 5.3.3.2 Operational 5.3.3.3 Technical 5.3.4 Control type 5.3.4.1 Preventative 5.3.4.2 Detective 5.3.4.3 Corrective 5.3.4.4 Deterrent 5.3.4.5 Compensating 5.3.4.6 Physical
3.0	**Risk Mitigation**	
3.1	Risk Identification Process	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.3 Remediation/mitigation 1.3.3.2 Patching 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.2 Vulnerabilities 1.7.2.9 Weak or default configurations 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.6 Impact analysis 3.1.6.1 Organization impact vs. localized impact

		3.1.6.2 Immediate vs. total 4.1 Explain the importance of the incident response process. 4.1.3 Factors contributing to data criticality 5.1 Understand the importance of data privacy and protection. 5.1.2 Non-technical controls 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.2 Risk identification process
3.2	Risk Calculation	5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.1 Business impact analysis 5.2.3 Risk calculation 5.2.3.1 Probability 5.2.3.2 Magnitude 5.2.5 Risk prioritization 5.2.5.1 Security controls 5.2.5.2 Engineering tradeoffs 5.2.6 Systems assessment
3.3	Risk Communication and Training	2.1 Given a scenario, apply security solutions for infrastructure management.

		2.1.10 Honeypot 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.4 Communication of risk factors 5.2.7 Documented compensating controls 5.2.8 Training and exercises 5.2.8.1 Red team 5.2.8.2 Blue team 5.2.8.3 White team 5.2.8.4 Tabletop exercise
4.0	**Social and Physical Security**	
4.1	Social Engineering	1.1 Explain the importance of threat data and intelligence. 1.1.5 Threat actors 1.1.5.1 Nation-state 1.1.5.4 Insider threat - Intentional 1.1.5.5 Insider threat - Unintentional 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.11 Impersonation 1.7.1.12 Man-in-the-middle attack 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.9 E-mail analysis

		3.1.9.5 Phishing 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
4.2	Physical Security	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.1 Asset criticality 1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.7 Physical access control 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 3.3 Explain the importance of proactive threat hunting. 3.3.5 Bundling critical assets 4.1 Explain the importance of the incident response process. 4.1.3 Factors contributing to data criticality 4.1.3.4 High value asset

4.3	Countermeasures and Prevention	2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 2.2 Explain software assurance best practices. 2.2.5 Secure coding best practices
5.0	**Reconnaissance**	
5.1	Reconnaissance Overview	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.2 Threat research 1.2.2.2 Behavioral 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.3 Active vs. passive 4.1 Explain the importance of the incident response process. 4.1.3 Factors contributing to data criticality 4.1.3.1 Personally identifiable information (PII) 4.1.3.6 Intellectual property 4.1.3.7 Corporate information 4.3 Given an incident, analyze potential indicators of compromise.

		4.3.1 Network-related 4.3.1.5 Scan/sweep
5.2	Reconnaissance Countermeasures	1.3 Given a scenario, perform vulnerability management activities. 1.3.3 Remediation/mitigation 1.3.3.3 Hardening 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.3 Client/server 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.4 Network 3.1.4.1 Uniform Resource Locator (URL) and domain name system (DNS) analysis - Domain generation algorithm 4.3 Given an incident, analyze potential indicators of compromise. 4.3.3 Application-related

		4.3.3.5 Service interruption 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures 5.3.2.5 Data retention
5.3	Scanning	1.3 Given a scenario, perform vulnerability management activities. 1.3.4 Scanning parameters and criteria 1.3.4.1 Risks associated with scanning activities 1.3.4.2 Vulnerability feed 1.3.4.3 Scope 1.3.4.4 Credentialed vs. non-credentialed 1.3.4.5 Server-based vs. agent-based 1.3.4.6 Internal vs. external 1.3.4.7 Special considerations - Types of data 1.3.4.8 Special considerations - Technical constraints 1.3.4.9 Special considerations - Workflow 1.3.4.10 Special considerations - Sensitivity levels 1.3.4.11 Special considerations - Regulatory requirements 1.3.4.12 Special considerations - Segmentation 1.3.4.13 Special considerations - Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.1 Web application scanner 1.4.1.1 OWASP Zed Attack Proxy (ZAP) 1.4.1.3 Nikto

		1.4.2 Infrastructure vulnerability scanner 1.4.2.1 Nessus 1.4.4 Enumeration 1.4.4.1 Nmap 1.4.4.2 hping 1.4.4.4 Responder 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
6.0	**Enumeration**	
6.1	Enumeration Overview	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.3 Mapping/enumeration 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap 1.4.4.3 Active vs. passive 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types

		1.7.2 Vulnerabilities 1.7.2.7 Insecure components 1.7.2.9 Weak or default configurations 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.3 Client/server 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
6.2	Enumeration Countermeasures	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.2 Active vs. passive scanning 1.3.1.3 Mapping/enumeration 1.3.3 Remediation/mitigation 1.3.3.3 Hardening 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.13 Session hijacking

		3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.4 Network 3.1.4.1 Uniform Resource Locator (URL) and domain name system (DNS) analysis - Domain generation algorithm 4.3 Given an incident, analyze potential indicators of compromise. 4.3.2 Host-related
7.0	**Vulnerability Management**	
7.1	Vulnerability Assessment	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions 1.2.4.2 Vulnerability management 1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.1 Asset criticality 1.3.1.2 Active vs. passive scanning 1.3.1.3 Mapping/enumeration 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap

		1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.3 Overflow attack - Buffer 1.7.1.15 Cross-site scripting - Reflected 1.7.2 Vulnerabilities 1.7.2.1 Improper error handling 1.7.2.2 Dereferencing 1.7.2.3 Insecure object reference 1.7.2.4 Race condition 1.7.2.5 Broken authentication 1.7.2.6 Sensitive data exposure 1.7.2.7 Insecure components 1.7.2.8 Insufficient logging and monitoring 1.7.2.9 Weak or default configurations 1.7.2.10 Use of insecure functions - strcpy 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
7.2	Vulnerability Management Life Cycle	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.3 Threat modeling methodologies 1.2.3.4 Impact 1.2.3.5 Likelihood

		1.2.4 Threat intelligence sharing with supported functions 1.2.4.2 Vulnerability management 1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.3 Remediation/mitigation 1.3.3.1 Configuration baseline 1.3.3.2 Patching 1.3.3.3 Hardening 1.3.3.4 Compensating controls 1.3.3.5 Risk acceptance 1.3.3.6 Verification of mitigation 1.3.4 Scanning parameters and criteria 1.3.4.6 Internal vs. external 1.6 Explain the threats and vulnerabilities associated with operating in the cloud. 1.6.8 Logging and monitoring 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.6 Systems assessment

7.3	Vulnerability Scoring Systems	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.2 Threat research 1.2.2.4 Common vulnerability scoring system (CVSS) 1.2.3 Threat modeling methodologies 1.2.3.4 Impact 1.2.3.5 Likelihood 1.2.4 Threat intelligence sharing with supported functions 1.2.4.1 Incident response 1.2.4.2 Vulnerability management 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap
7.4	Vulnerability Analysis	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions 1.2.4.2 Vulnerability management 1.4 Given a scenario, analyze the output from common vulnerability assessment tools.

		1.4.1 Web application scanner 1.4.1.1 OWASP Zed Attack Proxy (ZAP) 1.4.1.2 Burp suite 1.4.1.3 Nikto 1.4.1.4 Arachni 1.4.2 Infrastructure vulnerability scanner 1.4.2.1 Nessus 1.4.2.2 OpenVAS 1.4.2.3 Qualys 1.4.4 Enumeration 1.4.4.1 Nmap 1.4.5 Wireless assessment tools 1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.1 Mobile 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures

8.0	Identity and Access Management Security (IAM)	
8.1	Identity and Access Management Security	2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.8 Identity and access management 2.1.8.1 Privilege management 2.1.8.2 Multifactor authentication (MFA) 2.1.8.3 Single sign-on (SSO) 2.1.8.4 Federation 2.1.8.5 Role-based 2.1.8.6 Attribute-based 2.1.8.7 Mandatory 2.1.8.8 Manual review 2.1.11 Monitoring and logging
8.2	Privilege Escalation	1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.8 Privilege escalation 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.8 Identity and access management 2.1.8.2 Multifactor authentication (MFA) 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related

		4.3.1.5 Scan/sweep 4.3.2 Host-related 4.3.2.7 Unauthorized privilege 4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.8 Hashing 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures 5.3.2.2 Acceptable use policy (AUP)
8.3	Identity and Access Management Threats	1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.7 Directory traversal 1.7.1.9 Password spraying 1.7.1.10 Credential stuffing 1.7.2 Vulnerabilities 1.7.2.7 Insecure components 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.8 Identity and access management 2.1.8.2 Multifactor authentication (MFA)

		4.2 Given a scenario, apply the appropriate incident response procedure. 4.2.4 Eradication and recovery 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep 5.1 Understand the importance of data privacy and protection. 5.1.1 Privacy vs. security 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures 5.3.2.3 Password policy
8.4	Certificate Management	2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.13 Certificate management 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.6 Data loss prevention (DLP) 5.1 Understand the importance of data privacy and protection. 5.1.3 Technical controls 5.1.3.3 Data masking

9.0	Cybersecurity Threats	
9.1	Malware	1.1 Explain the importance of threat data and intelligence. 1.1.7 Commodity malware 1.1.8 Information sharing and analysis communities 1.1.8.2 Financial 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.3 Software assessment tools and techniques 1.4.3.1 Static analysis 1.4.3.2 Dynamic analysis 1.4.3.3 Reverse engineering 1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.3 Embedded 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.14 Rootkit 1.7.1.16 Cross-site scripting - Persistent 2.2 Explain software assurance best practices. 2.2.1 Platforms

		2.2.1.4 Embedded 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.10 Malware signatures 3.2.10.1 Development/rule writing 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.1 Bandwidth consumption 4.3.1.5 Scan/sweep
9.2	Combat Malware	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions 1.2.4.2 Vulnerability management 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.3 Software assessment tools and techniques 1.4.3.3 Reverse engineering 1.4.4 Enumeration 1.4.4.1 Nmap

		2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 2.3 Explain hardware assurance best practices. 2.3.6 Anti-tamper 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.3 Endpoint 3.1.3.1 Malware - Reverse engineering 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.10 Malware signatures 3.2.10.1 Development/rule writing 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
9.3	Sniffing	1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap

		1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.11 Impersonation 1.7.1.12 Man-in-the-middle attack 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.3 Segmentation 2.1.3.2 Virtual 2.1.12 Encryption 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.4 Network 3.1.4.3 Packet and protocol analysis - Malware 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.12 Port security 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.4 Rogue device on the network 4.3.1.5 Scan/sweep 4.3.1.7 Common protocol over non-standard port

		4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.1 Network 4.4.1.1 Wireshark 4.4.1.2 tcpdump
9.4	Session Hijacking	1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.12 Man-in-the-middle attack 1.7.1.13 Session hijacking 1.7.1.15 Cross-site scripting - Reflected 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.3 Client/server 2.2.1.4 Embedded 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep 4.4 Given a scenario, utilize basic digital forensics techniques.

		4.4.1 Network
9.5	Denial of Service	1.3 Given a scenario, perform vulnerability management activities. 1.3.5 Inhibitors to remediation 1.3.5.5 Degrading functionality 1.3.5.6 Legacy systems 1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.2 Internet of Things (IoT) 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.3 Overflow attack - Buffer 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.3 Blacklisting 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related

		4.3.1.1 Bandwidth consumption
9.6	SQL Injections	1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.1 Web application scanner 1.4.1.2 Burp suite 1.4.3 Software assessment tools and techniques 1.4.3.4 Fuzzing 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.2 Structured query language (SQL) injection 1.7.1.6 Remote code execution 1.7.2 Vulnerabilities 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.2 Web application
10.0	**Infrastructure Security**	

10.1	Intrusion Detection Systems	1.1 Explain the importance of threat data and intelligence. 1.1.4 Threat classification 1.1.4.1 Known threat vs. unknown threat 1.1.4.2 Zero-day 1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions 1.2.4.5 Detection and monitoring 1.3 Given a scenario, perform vulnerability management activities. 1.3.2 Validation 1.3.2.1 True positive 1.3.2.2 False positive 1.3.2.3 True negative 1.3.2.4 False negative 1.3.4 Scanning parameters and criteria 1.3.4.13 Special considerations - Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap

		2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.1 Heuristics 3.1.2 Trend analysis 3.1.3 Endpoint 3.1.3.3 System and application behavior - Known-good behavior 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.2 Whitelisting 3.2.3 Blacklisting 3.2.5 Intrusion prevention system (IPS) rules 3.2.7 Endpoint detection and response (EDR) 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.1 Bandwidth consumption 4.3.1.5 Scan/sweep 4.3.3 Application-related 4.3.3.4 Unexpected outbound communication
10.2	Firewalls	1.2 Given a scenario, utilize threat intelligence to support organizational security.

		1.2.4 Threat intelligence sharing with supported functions 1.2.4.5 Detection and monitoring 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.12 Man-in-the-middle attack 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.3 Segmentation 2.1.3.1 Physical 2.1.4 Network architecture 2.1.4.1 Physical 2.1.4.2 Software-defined 2.1.4.4 Virtual private network (VPN) 2.1.14 Active defense 3.2 Given a scenario, implement configuration changes to existing controls to improve security.

		3.2.4 Firewall 4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.1 Network 4.4.1.1 Wireshark 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures 5.3.2.4 Data ownership
10.3	Honeypots and DNS Sinkholes	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.3 Threat modeling methodologies 1.2.3.3 Attack vector 1.2.4 Threat intelligence sharing with supported functions 1.2.4.5 Detection and monitoring 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.10 Honeypot

		2.1.11 Monitoring and logging 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.9 Sinkholing 3.3 Explain the importance of proactive threat hunting. 3.3.6 Attack vectors 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.5 Scan/sweep
10.4	Web Servers	1.3 Given a scenario, perform vulnerability management activities. 1.3.5 Inhibitors to remediation 1.3.5.6 Legacy systems 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.1 Web application scanner 1.4.1.1 OWASP Zed Attack Proxy (ZAP) 1.4.4 Enumeration 1.4.4.1 Nmap

		1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.7 Directory traversal 1.7.1.12 Man-in-the-middle attack 1.7.1.15 Cross-site scripting - Reflected 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.3 Segmentation 2.1.3.1 Physical 2.1.11 Monitoring and logging 2.1.14 Active defense 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.2 Web application 2.2.1.3 Client/server 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.9 E-mail analysis 3.1.9.5 Phishing 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.11 Sandboxing

		4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.1 Network 4.4.1.1 Wireshark
10.5	Network Access	1.3 Given a scenario, perform vulnerability management activities. 1.3.3 Remediation/mitigation 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.1 Permissions 3.2.8 Network access control (NAC)
10.6	Web Applications	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.2 Active vs. passive scanning 1.3.4 Scanning parameters and criteria 1.3.4.13 Special considerations - Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.1 Web application scanner 1.4.1.2 Burp suite 1.4.1.3 Nikto

		1.4.1.4 Arachni 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.2 Structured query language (SQL) injection 1.7.1.3 Overflow attack - Buffer 1.7.1.4 Overflow attack - Integer 1.7.1.5 Overflow attack - Heap 1.7.1.7 Directory traversal 1.7.1.12 Man-in-the-middle attack 1.7.1.13 Session hijacking 1.7.1.15 Cross-site scripting - Reflected 1.7.1.16 Cross-site scripting - Persistent 1.7.1.17 Cross-site scripting - Document object model (DOM) 1.7.2 Vulnerabilities 1.7.2.5 Broken authentication 1.7.2.6 Sensitive data exposure 1.7.2.7 Insecure components 1.7.2.9 Weak or default configurations 1.7.2.10 Use of insecure functions - strcpy 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.14 Active defense 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.2 Web application

		3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.5 Log review 3.1.5.5 Proxy 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.3 Blacklisting 3.3 Explain the importance of proactive threat hunting. 3.3.5 Bundling critical assets
10.7	Specialized Technology	1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.2 Internet of Things (IoT) 1.5.3 Embedded 1.5.4 Real-time operating system (RTOS) 1.5.5 System-on-Chip (SoC) 1.5.6 Field programmable gate array (FPGA) 1.5.7 Physical access control 1.5.8 Building automation systems 1.5.9 Vehicles and drones 1.5.9.1 CAN bus 1.5.10 Workflow and process automation systems 1.5.12 Supervisory control and data acquisition (SCADA) 1.5.12.1 Modbus 2.2 Explain software assurance best practices.

		2.2.1 Platforms 2.2.1.5 System-on-chip (SoC) 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.2 Whitelisting 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures 5.3.3 Category 5.3.3.2 Operational
11.0	**Wireless and IoT Security**	
11.1	Wireless Security	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.2 Active vs. passive scanning 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.3 Active vs. passive 1.4.5 Wireless assessment tools 1.4.5.1 Aircrack-ng 1.4.5.2 Reaver

		1.4.5.3 oclHashcat 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.12 Man-in-the-middle attack 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.4 Network architecture 2.1.4.4 Virtual private network (VPN) 2.1.12 Encryption 2.1.14 Active defense 3.3 Explain the importance of proactive threat hunting. 3.3.4 Reducing the attack surface area 4.1 Explain the importance of the incident response process. 4.1.1 Communication plan 4.1.1.4 Using a secure method of communication 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.1.1 Bandwidth consumption 4.3.1.4 Rogue device on the network

		4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.1 Network 4.4.1.1 Wireshark
11.2	Bluetooth Security	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions 1.2.4.5 Detection and monitoring 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.4 Network architecture 2.1.12 Encryption 2.1.14 Active defense 2.2 Explain software assurance best practices. 2.2.5 Secure coding best practices 2.2.5.5 Data protection 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related

11.3	Mobile Device Security	1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.3 Software assessment tools and techniques 1.4.3.3 Reverse engineering 1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.1 Mobile 1.5.7 Physical access control 2.2 Explain software assurance best practices. 2.2.1 Platforms 2.2.1.1 Mobile 2.2.5 Secure coding best practices 2.2.5.5 Data protection 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.3 Endpoint 3.1.3.6 File system 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.11 Sandboxing 5.3 Explain the importance of frameworks, policies, procedures, and controls.

		5.3.2 Policies and procedures 5.3.2.2 Acceptable use policy (AUP) 5.3.2.3 Password policy
11.4	Cloud Security	1.3 Given a scenario, perform vulnerability management activities. 1.3.5 Inhibitors to remediation 1.3.5.4 Business process interruption 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.1 Web application scanner 1.4.1.1 OWASP Zed Attack Proxy (ZAP) 1.4.6 Cloud infrastructure assessment tools 1.4.6.1 ScoutSuite 1.4.6.2 Prowler 1.4.6.3 Pacu 1.6 Explain the threats and vulnerabilities associated with operating in the cloud. 1.6.1 Cloud service models 1.6.1.1 Software as a Service (SaaS) 1.6.1.2 Platform as a Service (PaaS) 1.6.1.3 Infrastructure as a Service (IaaS) 1.6.2 Cloud deployment models

		1.6.2.1 Public 1.6.2.2 Private 1.6.2.3 Community 1.6.2.4 Hybrid 1.6.3 Function as a Service (FaaS)/serverless architecture 1.6.4 Infrastructure as code (IaC) 1.6.5 Insecure application programming interface (API) 1.6.6 Improper key management 1.6.7 Unprotected storage 1.6.8 Logging and monitoring 1.6.8.1 Insufficient logging and monitoring 1.6.8.2 Inability to access 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.1 Extensible markup language (XML) attack 1.7.1.15 Cross-site scripting - Reflected 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.1 Cloud vs. on-premises 2.1.4 Network architecture 2.1.4.3 Virtual private cloud (VPC) 2.1.4.5 Serverless 2.1.9 Cloud access security broker (CASB) 2.1.14 Active defense 3.3 Explain the importance of proactive threat hunting.

		3.3.5 Bundling critical assets 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.2 Risk identification process 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.4 Control type 5.3.4.1 Preventative 5.3.4.4 Deterrent
11.5	Internet of Things Security	1.1 Explain the importance of threat data and intelligence. 1.1.8 Information sharing and analysis communities 1.1.8.1 Healthcare 1.1.8.3 Aviation 1.1.8.5 Critical infrastructure 1.3 Given a scenario, perform vulnerability management activities. 1.3.5 Inhibitors to remediation 1.3.5.6 Legacy systems 1.4 Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.4 Enumeration 1.4.4.1 Nmap

		1.5 Explain the threats and vulnerabilities associated with specialized technology. 1.5.2 Internet of Things (IoT) 1.5.3 Embedded 1.5.11 Industrial control system 1.6 Explain the threats and vulnerabilities associated with operating in the cloud. 1.6.8 Logging and monitoring 1.6.8.1 Insufficient logging and monitoring 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types 1.7.1.1 Extensible markup language (XML) attack 1.7.1.12 Man-in-the-middle attack 1.7.1.16 Cross-site scripting - Persistent 1.7.2 Vulnerabilities 1.7.2.8 Insufficient logging and monitoring 2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.4 Network architecture 2.1.4.1 Physical 2.2 Explain software assurance best practices.

		2.2.1 Platforms 2.2.1.4 Embedded 2.2.1.6 Firmware 4.1 Explain the importance of the incident response process. 4.1.3 Factors contributing to data criticality 4.1.3.1 Personally identifiable information (PII)
12.0	**Infrastructure Analysis**	
12.1	Hardware Analysis	2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.3 Segmentation 2.1.3.1 Physical 2.1.3.2 Virtual 2.1.3.4 Jumpbox 2.1.3.5 System isolation - Air gap 2.1.12 Encryption 2.1.14 Active defense 2.3 Explain hardware assurance best practices. 2.3.1 Hardware root of trust 2.3.1.1 Trusted platform module (TPM) 2.3.2 eFuse 2.3.5 Secure processing 2.3.5.1 Trusted execution 2.3.5.2 Secure enclave

		2.3.5.3 Processor security extensions 2.3.5.4 Atomic execution 5.1 Understand the importance of data privacy and protection. 5.1.3 Technical controls 5.1.3.1 Encryption
12.2	Security Information and Event Management (SIEM)	3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.4 Network 3.1.4.1 Uniform Resource Locator (URL) and domain name system (DNS) analysis - Domain generation algorithm 3.1.5 Log review 3.1.7 Security information and event management (SIEM) review 3.1.7.1 Rule writing 3.1.7.2 Known-bad Internet protocol (IP) 3.1.7.3 Dashboard 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.1 Permissions 3.3 Explain the importance of proactive threat hunting. 3.3.3 Threat hunting tactics 3.3.6 Attack vectors

12.3	Log Review	1.6 Explain the threats and vulnerabilities associated with operating in the cloud. 1.6.8 Logging and monitoring 1.6.8.1 Insufficient logging and monitoring 3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.5 Log review 3.1.5.1 Event logs 3.1.5.2 Syslog 3.1.5.3 Firewall logs 3.1.5.4 Web application firewall (WAF) 3.1.5.5 Proxy 3.1.5.6 Intrusion detection system (IDS)/Intrusion prevention system (IPS) 3.1.8 Query writing 5.3 Explain the importance of frameworks, policies, procedures, and controls. 5.3.2 Policies and procedures 5.3.2.2 Acceptable use policy (AUP)
12.4	Asset and Change Management	1.3 Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification 1.3.1.1 Asset criticality 2.1 Given a scenario, apply security solutions for infrastructure management.

		2.1.2 Asset management 2.1.2.1 Asset tagging 2.1.5 Change management 2.1.14 Active defense 2.3 Explain hardware assurance best practices. 2.3.4 Trusted foundry 4.1 Explain the importance of the incident response process. 4.1.3 Factors contributing to data criticality 4.1.3.4 High value asset 4.2 Given a scenario, apply the appropriate incident response procedure. 4.2.4 Eradication and recovery 4.2.4.4 Secure disposal 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.9 Supply chain assessment 5.2.9.1 Vendor due diligence 5.2.9.2 Hardware source authenticity
12.5	Virtualization Management	2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.6 Virtualization

		2.1.6.1 Virtual desktop infrastructure (VDI) 2.1.7 Containerization 2.1.14 Active defense
13.0	**Software Assurance**	
13.1	Software Development Overview	2.2 Explain software assurance best practices. 2.2.2 Software development life cycle (SDLC) integration 2.2.4 Software assessment methods 2.2.4.1 User acceptance testing 2.2.4.2 Stress test application 2.2.4.3 Security regression testing 2.2.4.4 Code review 2.2.5 Secure coding best practices 2.2.5.1 Input validation 2.2.5.2 Output encoding 2.2.5.3 Session management 2.2.5.4 Authentication 2.2.5.5 Data protection 2.2.5.6 Parameterized queries 2.2.6 Static analysis tools 2.2.7 Dynamic analysis tools 2.2.8 Formal methods for verification of critical software 2.2.9 Service-oriented architecture 2.2.9.1 Security Assertions Markup Language (SAML) 2.2.9.2 Simple Object Access Protocol (SOAP) 2.2.9.3 Representational State Transfer (REST) 2.2.9.4 Microservices

13.2	Automation	2.2 Explain software assurance best practices. 2.2.3 DevSecOps 2.2.9 Service-oriented architecture 2.2.9.3 Representational State Transfer (REST) 3.4 Compare and contrast automation concepts and technologies. 3.4.1 Workflow orchestration 3.4.1.1 Security Orchestration, Automation, and Response (SOAR) 3.4.2 Scripting 3.4.3 Application programming interface (API) integration 3.4.4 Automated malware signature creation 3.4.5 Data enrichment 3.4.6 Threat feed combination 3.4.7 Machine learning 3.4.8 Use of automation protocols and standards 3.4.8.1 Security Content Automation Protocol (SCAP) 3.4.9 Continuous integration 3.4.10 Continuous deployment/delivery
14.0	**Data Analysis**	
14.1	Data Analysis and Protection	3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.1 Heuristics 3.1.2 Trend analysis 3.1.3 Endpoint 3.1.3.2 Memory

		3.1.3.6 File system 3.1.3.7 User and entity behavior analytics (UEBA) 3.1.4 Network 3.1.4.1 Uniform Resource Locator (URL) and domain name system (DNS) analysis - Domain generation algorithm 3.1.4.2 Flow analysis 3.1.4.3 Packet and protocol analysis - Malware 3.1.8 Query writing 3.1.8.1 String search 3.1.8.2 Script 3.1.8.3 Piping 3.2 Given a scenario, implement configuration changes to existing controls to improve security. 3.2.6 Data loss prevention (DLP) 5.1 Understand the importance of data privacy and protection. 5.1.1 Privacy vs. security 5.1.2 Non-technical controls 5.1.2.1 Classification 5.1.2.2 Ownership 5.1.2.3 Retention 5.1.2.4 Data types 5.1.2.5 Retention standards 5.1.2.6 Confidentiality 5.1.2.7 Legal requirements 5.1.2.8 Data sovereignty 5.1.2.9 Data minimization 5.1.2.10 Purpose limitation

		5.1.2.11 Non-disclosure agreement (NDA) 5.1.3 Technical controls 5.1.3.1 Encryption 5.1.3.2 Data loss prevention (DLP) 5.1.3.3 Data masking 5.1.3.4 Deidentification 5.1.3.5 Tokenization 5.1.3.6 Digital rights management (DRM) - Watermarking 5.1.3.7 Geographic access requirements 5.1.3.8 Access controls
14.2	Hashing	2.1 Given a scenario, apply security solutions for infrastructure management. 2.1.12 Encryption 4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.8 Hashing 4.4.8.1 Changes to binaries
14.3	Digital Forensics	4.4 Given a scenario, utilize basic digital forensics techniques. 4.4.1 Network 4.4.1.1 Wireshark 4.4.1.2 tcpdump 4.4.2 Endpoint 4.4.2.1 Disk 4.4.2.2 Memory

		4.4.3 Mobile 4.4.4 Cloud 4.4.5 Virtualization 4.4.6 Legal hold 4.4.7 Procedures 4.4.8 Hashing 4.4.8.1 Changes to binaries 4.4.9 Carving 4.4.10 Data acquisition
14.4	Email Analysis	3.1 Given a scenario, analyze data as part of security monitoring activities. 3.1.9 E-mail analysis 3.1.9.1 Malicious payload 3.1.9.2 Domain Keys Identified Mail (DKIM) 3.1.9.3 Domain-based Message Authentication, Reporting, and Conformance (DMARC) 3.1.9.4 Sender Policy Framework (SPF) 3.1.9.5 Phishing 3.1.9.6 Forwarding 3.1.9.7 Digital signature 3.1.9.8 E-mail signature block 3.1.9.9 Embedded links 3.1.9.10 Impersonation 3.1.9.11 Header
15.0	**Incident Response**	
15.1	Incident Response - Preparation	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions

		1.2.4.1 Incident response 4.1 Explain the importance of the incident response process. 4.1.1 Communication plan 4.1.2 Response coordination with relevant entities 4.1.2.2 Human resources 4.1.2.3 Public relations 4.2 Given a scenario, apply the appropriate incident response procedure. 4.2.1 Preparation 4.2.1.1 Training 4.2.1.2 Testing 4.2.1.3 Documentation of procedures 4.2.2 Detection and analysis 4.2.3 Containment 4.2.4 Eradication and recovery 4.2.5 Post-incident activities 4.3 Given an incident, analyze potential indicators of compromise. 4.3.2 Host-related 4.3.2.8 Data exfiltration
15.2	Incident Response - Detection and Containment	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions

		1.2.4.1 Incident response 4.2 Given a scenario, apply the appropriate incident response procedure. 4.2.1 Preparation 4.2.1.1 Training 4.2.1.2 Testing 4.2.1.3 Documentation of procedures 4.2.2 Detection and analysis 4.2.2.1 Characteristics contributing to severity level classification 4.2.2.2 Downtime 4.2.2.3 Recovery time 4.2.2.4 Data integrity 4.2.2.5 Economic 4.2.2.6 System process criticality 4.2.2.7 Reverse engineering 4.2.2.8 Data correlation 4.2.3 Containment 4.2.3.1 Segmentation 4.2.3.2 Isolation 4.2.4 Eradication and recovery 4.2.4.1 Vulnerability mitigation 4.2.4.2 Sanitization 4.2.4.3 Reconstruction/reimaging 4.2.4.4 Secure disposal 4.2.4.5 Patching 4.2.4.6 Restoration of permissions 4.2.4.7 Reconstitution of resources 4.2.4.8 Restoration of capabilities and services

		4.2.4.9 Verification of logging/communication to security monitoring 4.3 Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related 4.3.2 Host-related 4.3.3 Application-related
15.3	Incident Response - Eradication and Recovery	1.2 Given a scenario, utilize threat intelligence to support organizational security. 1.2.4 Threat intelligence sharing with supported functions 1.2.4.1 Incident response 4.2 Given a scenario, apply the appropriate incident response procedure. 4.2.4 Eradication and recovery 4.2.4.4 Secure disposal 4.2.4.8 Restoration of capabilities and services 4.2.5 Post-incident activities 4.2.5.1 Evidence retention 4.2.5.2 Lessons learned report 4.2.5.3 Change control process 4.2.5.4 Incident response plan update 4.2.5.5 Incident summary report 4.2.5.6 IoC generation 4.2.5.7 Monitoring
15.4	Indicators of Compromise	4.3 Given an incident, analyze potential indicators of compromise.

		4.3.1 Network-related 4.3.1.1 Bandwidth consumption 4.3.1.2 Beaconing 4.3.1.3 Irregular peer-to-peer communication 4.3.1.4 Rogue device on the network 4.3.1.5 Scan/sweep 4.3.1.6 Unusual traffic spike 4.3.1.7 Common protocol over non-standard port 4.3.2 Host-related 4.3.2.1 Processor consumption 4.3.2.2 Memory consumption 4.3.2.3 Drive capacity consumption 4.3.2.4 Unauthorized software 4.3.2.5 Malicious process 4.3.2.6 Unauthorized change 4.3.2.7 Unauthorized privilege 4.3.2.8 Data exfiltration 4.3.2.9 Abnormal OS process behavior 4.3.2.10 File system change or anomaly 4.3.2.11 Registry change or anomaly 4.3.2.12 Unauthorized scheduled task 4.3.3 Application-related 4.3.3.1 Anomalous activity 4.3.3.2 Introduction of new accounts 4.3.3.3 Unexpected output 4.3.3.4 Unexpected outbound communication 4.3.3.5 Service interruption 4.3.3.6 Application log

A.0	**TestOut CyberDefense Pro Practice Exams**	
A.1	Prepare for TestOut CyberDefense Pro Certification	
A.2	TestOut CyberDefense Pro Domain Review	
B.0	**CompTIA CySA+ CS0-002 - Practice Exams**	
B.1	Prepare for CompTIA CySA+ CS0-000 Certification	
B.2	CompTIA CySA+ Domain Review (20 Questions)	
B.3	CompTIA CySA+ Domain Review (All Questions)	

Objective Mapping: CompTIA CySA+ CS0-002 Objective to LabSim Section

#	CompTIA CySA+ (CS0-002) Objective	TestOut Module.Section
1.0	**Threat and Vulnerability Management**	
1.1	Explain the importance of threat data and intelligence. 1.1.1 Intelligence sources ○ 1.1.1.1 Open-source intelligence ○ 1.1.1.2 Proprietary/closed-source intelligence ○ 1.1.1.3 Timeliness ○ 1.1.1.4 Relevancy ○ 1.1.1.5 Accuracy 1.1.2 Confidence levels 1.1.3 Indicator management ○ 1.1.3.1 Structured Threat Information eXpression (STIX) ○ 1.1.3.2 Trusted Automated eXchange of Indicator Information (TAXII) ○ 1.1.3.3 OpenIoC 1.1.4 Threat classification ○ 1.1.4.1 Known threat vs. unknown threat ○ 1.1.4.2 Zero-day ○ 1.1.4.3 Advanced persistent threat 1.1.5 Threat actors ○ 1.1.5.1 Nation-state ○ 1.1.5.2 Hacktivist ○ 1.1.5.3 Organized crime ○ 1.1.5.4 Insider threat - Intentional ○ 1.1.5.5 Insider threat - Unintentional 1.1.6 Intelligence cycle ○ 1.1.6.1 Requirements ○ 1.1.6.2 Collection ○ 1.1.6.3 Analysis ○ 1.1.6.4 Dissemination ○ 1.1.6.5 Feedback 1.1.7 Commodity malware 1.1.8 Information sharing and analysis communities ○ 1.1.8.1 Healthcare	2.1 4.1 9.1 10.1 11.5

	○ 1.1.8.2 Financial ○ 1.1.8.3 Aviation ○ 1.1.8.4 Government ○ 1.1.8.5 Critical infrastructure	
1.2	Given a scenario, utilize threat intelligence to support organizational security. 1.2.1 Attack frameworks ○ 1.2.1.1 MITRE ATT&CK ○ 1.2.1.2 The Diamond Model of Intrusion Analysis ○ 1.2.1.3 Kill chain 1.2.2 Threat research ○ 1.2.2.1 Reputational ○ 1.2.2.2 Behavioral ○ 1.2.2.3 Indicator of compromise (IoC) ○ 1.2.2.4 Common vulnerability scoring system (CVSS) 1.2.3 Threat modeling methodologies ○ 1.2.3.1 Adversary capability ○ 1.2.3.2 Total attack surface ○ 1.2.3.3 Attack vector ○ 1.2.3.4 Impact ○ 1.2.3.5 Likelihood 1.2.4 Threat intelligence sharing with supported functions ○ 1.2.4.1 Incident response ○ 1.2.4.2 Vulnerability management ○ 1.2.4.3 Risk management ○ 1.2.4.4 Security engineering ○ 1.2.4.5 Detection and monitoring	2.2 5.1 7.1, 7.2, 7.3, 7.4 9.2 10.1, 10.2, 10.3 11.2 15.1, 15.2, 15.3
1.3	Given a scenario, perform vulnerability management activities. 1.3.1 Vulnerability identification ○ 1.3.1.1 Asset criticality ○ 1.3.1.2 Active vs. passive scanning ○ 1.3.1.3 Mapping/enumeration 1.3.2 Validation ○ 1.3.2.1 True positive	2.1 3.1 4.2 5.2, 5.3 6.1, 6.2 7.1, 7.2 9.5 10.1, 10.4, 10.5, 10.6

	○ 1.3.2.2 False positive ○ 1.3.2.3 True negative ○ 1.3.2.4 False negative 1.3.3 Remediation/mitigation ○ 1.3.3.1 Configuration baseline ○ 1.3.3.2 Patching ○ 1.3.3.3 Hardening ○ 1.3.3.4 Compensating controls ○ 1.3.3.5 Risk acceptance ○ 1.3.3.6 Verification of mitigation 1.3.4 Scanning parameters and criteria ○ 1.3.4.1 Risks associated with scanning activities ○ 1.3.4.2 Vulnerability feed ○ 1.3.4.3 Scope ○ 1.3.4.4 Credentialed vs. non-credentialed ○ 1.3.4.5 Server-based vs. agent-based ○ 1.3.4.6 Internal vs. external ○ 1.3.4.7 Special considerations - Types of data ○ 1.3.4.8 Special considerations - Technical constraints ○ 1.3.4.9 Special considerations - Workflow ○ 1.3.4.10 Special considerations - Sensitivity levels ○ 1.3.4.11 Special considerations - Regulatory requirements ○ 1.3.4.12 Special considerations - Segmentation ○ 1.3.4.13 Special considerations - Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings 1.3.5 Inhibitors to remediation ○ 1.3.5.1 Memorandum of understanding (MOU) ○ 1.3.5.2 Service-level agreement (SLA) ○ 1.3.5.3 Organizational governance ○ 1.3.5.4 Business process interruption ○ 1.3.5.5 Degrading functionality ○ 1.3.5.6 Legacy systems ○ 1.3.5.7 Proprietary systems	11.1, 11.4, 11.5 12.4
1.4	Given a scenario, analyze the output from common vulnerability assessment tools. 1.4.1 Web application scanner ○ 1.4.1.1 OWASP Zed Attack Proxy (ZAP)	5.1, 5.2, 5.3 6.1 7.1, 7.3, 7.4 9.1, 9.2, 9.3, 9.6

	○ 1.4.1.2 Burp suite ○ 1.4.1.3 Nikto ○ 1.4.1.4 Arachni 1.4.2 Infrastructure vulnerability scanner ○ 1.4.2.1 Nessus ○ 1.4.2.2 OpenVAS ○ 1.4.2.3 Qualys 1.4.3 Software assessment tools and techniques ○ 1.4.3.1 Static analysis ○ 1.4.3.2 Dynamic analysis ○ 1.4.3.3 Reverse engineering ○ 1.4.3.4 Fuzzing 1.4.4 Enumeration ○ 1.4.4.1 Nmap ○ 1.4.4.2 hping ○ 1.4.4.3 Active vs. passive ○ 1.4.4.4 Responder 1.4.5 Wireless assessment tools ○ 1.4.5.1 Aircrack-ng ○ 1.4.5.2 Reaver ○ 1.4.5.3 oclHashcat 1.4.6 Cloud infrastructure assessment tools ○ 1.4.6.1 ScoutSuite ○ 1.4.6.2 Prowler ○ 1.4.6.3 Pacu	10.1, 10.2, 10.3, 10.4, 10.6 11.1, 11.3, 11.4, 11.5
1.5	Explain the threats and vulnerabilities associated with specialized technology. 1.5.1 Mobile 1.5.2 Internet of Things (IoT) 1.5.3 Embedded 1.5.4 Real-time operating system (RTOS) 1.5.5 System-on-Chip (SoC) 1.5.6 Field programmable gate array (FPGA) 1.5.7 Physical access control 1.5.8 Building automation systems 1.5.9 Vehicles and drones ○ 1.5.9.1 CAN bus	4.2 7.4 9.1, 9.5 10.7 11.3, 11.5

	1.5.10 Workflow and process automation systems 1.5.11 Industrial control system 1.5.12 Supervisory control and data acquisition (SCADA) ○ 1.5.12.1 Modbus	
1.6	Explain the threats and vulnerabilities associated with operating in the cloud. 1.6.1 Cloud service models ○ 1.6.1.1 Software as a Service (SaaS) ○ 1.6.1.2 Platform as a Service (PaaS) ○ 1.6.1.3 Infrastructure as a Service (IaaS) 1.6.2 Cloud deployment models ○ 1.6.2.1 Public ○ 1.6.2.2 Private ○ 1.6.2.3 Community ○ 1.6.2.4 Hybrid 1.6.3 Function as a Service (FaaS)/serverless architecture 1.6.4 Infrastructure as code (IaC) 1.6.5 Insecure application programming interface (API) 1.6.6 Improper key management 1.6.7 Unprotected storage 1.6.8 Logging and monitoring ○ 1.6.8.1 Insufficient logging and monitoring ○ 1.6.8.2 Inability to access	7.2 11.4, 11.5 12.3
1.7	Given a scenario, implement controls to mitigate attacks and software vulnerabilities. 1.7.1 Attack types ○ 1.7.1.1 Extensible markup language (XML) attack ○ 1.7.1.2 Structured query language (SQL) injection ○ 1.7.1.3 Overflow attack - Buffer ○ 1.7.1.4 Overflow attack - Integer ○ 1.7.1.5 Overflow attack - Heap ○ 1.7.1.6 Remote code execution ○ 1.7.1.7 Directory traversal ○ 1.7.1.8 Privilege escalation ○ 1.7.1.9 Password spraying	3.1 4.1 6.1, 6.2 7.1 8.2, 8.3 9.1, 9.3, 9.4, 9.5, 9.6 10.2, 10.4, 10.6 11.1, 11.2, 11.4, 11.5

	○ 1.7.1.10 Credential stuffing ○ 1.7.1.11 Impersonation ○ 1.7.1.12 Man-in-the-middle attack ○ 1.7.1.13 Session hijacking ○ 1.7.1.14 Rootkit ○ 1.7.1.15 Cross-site scripting - Reflected ○ 1.7.1.16 Cross-site scripting - Persistent ○ 1.7.1.17 Cross-site scripting - Document object model (DOM) 1.7.2 Vulnerabilities ○ 1.7.2.1 Improper error handling ○ 1.7.2.2 Dereferencing ○ 1.7.2.3 Insecure object reference ○ 1.7.2.4 Race condition ○ 1.7.2.5 Broken authentication ○ 1.7.2.6 Sensitive data exposure ○ 1.7.2.7 Insecure components ○ 1.7.2.8 Insufficient logging and monitoring ○ 1.7.2.9 Weak or default configurations ○ 1.7.2.10 Use of insecure functions - strcpy	
2.0	**Software and Systems Security**	
2.1	Given a scenario, apply security solutions for infrastructure management. 2.1.1 Cloud vs. on-premises 2.1.2 Asset management ○ 2.1.2.1 Asset tagging 2.1.3 Segmentation ○ 2.1.3.1 Physical ○ 2.1.3.2 Virtual ○ 2.1.3.4 Jumpbox ○ 2.1.3.5 System isolation - Air gap 2.1.4 Network architecture ○ 2.1.4.1 Physical ○ 2.1.4.2 Software-defined ○ 2.1.4.3 Virtual private cloud (VPC) ○ 2.1.4.4 Virtual private network (VPN) ○ 2.1.4.5 Serverless	3.3 4.2, 4.3 8.1, 8.2, 8.3, 8.4 9.2, 9.3, 9.4, 9.5, 9.6 10.1, 10.2, 10.3, 10.4, 10.6 11.1, 11.2, 11.4, 11.5 12.1, 12.4, 12.5 14.2

	2.1.5 Change management 2.1.6 Virtualization ○ 2.1.6.1 Virtual desktop infrastructure (VDI) 2.1.7 Containerization 2.1.8 Identity and access management ○ 2.1.8.1 Privilege management ○ 2.1.8.2 Multifactor authentication (MFA) ○ 2.1.8.3 Single sign-on (SSO) ○ 2.1.8.4 Federation ○ 2.1.8.5 Role-based ○ 2.1.8.6 Attribute-based ○ 2.1.8.7 Mandatory ○ 2.1.8.8 Manual review 2.1.9 Cloud access security broker (CASB) 2.1.10 Honeypot 2.1.11 Monitoring and logging 2.1.12 Encryption 2.1.13 Certificate management 2.1.14 Active defense	
2.2	Explain software assurance best practices. 2.2.1 Platforms ○ 2.2.1.1 Mobile ○ 2.2.1.2 Web application ○ 2.2.1.3 Client/server ○ 2.2.1.4 Embedded ○ 2.2.1.5 System-on-chip (SoC) ○ 2.2.1.6 Firmware 2.2.2 Software development life cycle (SDLC) integration 2.2.3 DevSecOps 2.2.4 Software assessment methods ○ 2.2.4.1 User acceptance testing ○ 2.2.4.2 Stress test application ○ 2.2.4.3 Security regression testing ○ 2.2.4.4 Code review 2.2.5 Secure coding best practices ○ 2.2.5.1 Input validation	4.3 5.2 6.1 9.1, 9.4, 9.6 10.4, 10.6, 10.7 11.2, 11.3, 11.5 13.1, 13.2

	○ 2.2.5.2 Output encoding ○ 2.2.5.3 Session management ○ 2.2.5.4 Authentication ○ 2.2.5.5 Data protection ○ 2.2.5.6 Parameterized queries 2.2.6 Static analysis tools 2.2.7 Dynamic analysis tools 2.2.8 Formal methods for verification of critical software 2.2.9 Service-oriented architecture ○ 2.2.9.1 Security Assertions Markup Language (SAML) ○ 2.2.9.2 Simple Object Access Protocol (SOAP) ○ 2.2.9.3 Representational State Transfer (REST) ○ 2.2.9.4 Microservices	
2.3	Explain hardware assurance best practices. 2.3.1 Hardware root of trust ○ 2.3.1.1 Trusted platform module (TPM) ○ 2.3.1.2 Hardware security module (HSM) 2.3.2 eFuse 2.3.3 Unified Extensible Firmware Interface (UEFI) 2.3.4 Trusted foundry 2.3.5 Secure processing ○ 2.3.5.1 Trusted execution ○ 2.3.5.2 Secure enclave ○ 2.3.5.3 Processor security extensions ○ 2.3.5.4 Atomic execution 2.3.6 Anti-tamper 2.3.7 Self-encrypting drive 2.3.8 Trusted firmware updates 2.3.9 Measured boot and attestation 2.3.10 Bus encryption	9.2 12.1, 12.4
3.0	**Security Operations and Monitoring**	
3.1	Given a scenario, analyze data as part of security monitoring activities.	3.1 4.1

	3.1.1 Heuristics 3.1.2 Trend analysis 3.1.3 Endpoint ○ 3.1.3.1 Malware - Reverse engineering ○ 3.1.3.2 Memory ○ 3.1.3.3 System and application behavior - Known-good behavior ○ 3.1.3.4 System and application behavior - Anomalous behavior ○ 3.1.3.5 System and application behavior - Exploit techniques ○ 3.1.3.6 File system ○ 3.1.3.7 User and entity behavior analytics (UEBA) 3.1.4 Network ○ 3.1.4.1 Uniform Resource Locator (URL) and domain name system (DNS) analysis - Domain generation algorithm ○ 3.1.4.2 Flow analysis ○ 3.1.4.3 Packet and protocol analysis - Malware 3.1.5 Log review ○ 3.1.5.1 Event logs ○ 3.1.5.2 Syslog ○ 3.1.5.3 Firewall logs ○ 3.1.5.4 Web application firewall (WAF) ○ 3.1.5.5 Proxy ○ 3.1.5.6 Intrusion detection system (IDS)/Intrusion prevention system (IPS) 3.1.6 Impact analysis ○ 3.1.6.1 Organization impact vs. localized impact ○ 3.1.6.2 Immediate vs. total 3.1.7 Security information and event management (SIEM) review ○ 3.1.7.1 Rule writing ○ 3.1.7.2 Known-bad Internet protocol (IP) ○ 3.1.7.3 Dashboard 3.1.8 Query writing ○ 3.1.8.1 String search ○ 3.1.8.2 Script ○ 3.1.8.3 Piping 3.1.9 E-mail analysis ○ 3.1.9.1 Malicious payload ○ 3.1.9.2 Domain Keys Identified Mail (DKIM) ○ 3.1.9.3 Domain-based Message Authentication, Reporting, and Conformance (DMARC)	5.2 6.2 9.2, 9.3 10.1, 10.4, 10.6 11.3 12.2, 12.3 14.1, 14.4

	○ 3.1.9.4 Sender Policy Framework (SPF) ○ 3.1.9.5 Phishing ○ 3.1.9.6 Forwarding ○ 3.1.9.7 Digital signature ○ 3.1.9.8 E-mail signature block ○ 3.1.9.9 Embedded links ○ 3.1.9.10 Impersonation ○ 3.1.9.11 Header	
3.2	Given a scenario, implement configuration changes to existing controls to improve security. 3.2.1 Permissions 3.2.2 Whitelisting 3.2.3 Blacklisting 3.2.4 Firewall 3.2.5 Intrusion prevention system (IPS) rules 3.2.6 Data loss prevention (DLP) 3.2.7 Endpoint detection and response (EDR) 3.2.8 Network access control (NAC) 3.2.9 Sinkholing 3.2.10 Malware signatures ○ 3.2.10.1 Development/rule writing 3.2.11 Sandboxing 3.2.12 Port security	8.4 9.1, 9.2, 9.3, 9.5 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7 11.3 12.2 14.1
3.3	Explain the importance of proactive threat hunting. 3.3.1 Establishing a hypothesis 3.3.2 Profiling threat actors and activities 3.3.3 Threat hunting tactics ○ 3.3.3.1 Executable process analysis 3.3.4 Reducing the attack surface area 3.3.5 Bundling critical assets 3.3.6 Attack vectors 3.3.7 Integrated intelligence 3.3.8 Improving detection capabilities	2.1, 2.2 4.2 10.3, 10.6 11.1, 11.4 12.2

3.4	Compare and contrast automation concepts and technologies. 3.4.1 Workflow orchestration ○ 3.4.1.1 Security Orchestration, Automation, and Response (SOAR) 3.4.2 Scripting 3.4.3 Application programming interface (API) integration 3.4.4 Automated malware signature creation 3.4.5 Data enrichment 3.4.6 Threat feed combination 3.4.7 Machine learning 3.4.8 Use of automation protocols and standards ○ 3.4.8.1 Security Content Automation Protocol (SCAP) 3.4.9 Continuous integration 3.4.10 Continuous deployment/delivery	13.2
4.0	**Incident Response**	
4.1	Explain the importance of the incident response process. 4.1.1 Communication plan ○ 4.1.1.1 Limiting communication to trusted parties ○ 4.1.1.2 Disclosing based on regulatory/legislative requirements ○ 4.1.1.3 Preventing inadvertent release of information ○ 4.1.1.4 Using a secure method of communication ○ 4.1.1.5 Reporting requirements 4.1.2 Response coordination with relevant entities ○ 4.1.2.1 Legal ○ 4.1.2.2 Human resources ○ 4.1.2.3 Public relations ○ 4.1.2.4 Internal and external ○ 4.1.2.5 Law enforcement ○ 4.1.2.6 Senior leadership ○ 4.1.2.7 Regulatory bodies 4.1.3 Factors contributing to data criticality ○ 4.1.3.1 Personally identifiable information (PII) ○ 4.1.3.2 Personal health information (PHI) ○ 4.1.3.3 Sensitive personal information (SPI) ○ 4.1.3.4 High value asset	3.1 4.2 5.1 11.1, 11.5 12.4 15.1

	○ 4.1.3.5 Financial information ○ 4.1.3.6 Intellectual property ○ 4.1.3.7 Corporate information	
4.2	Given a scenario, apply the appropriate incident response procedure. 4.2.1 Preparation ○ 4.2.1.1 Training ○ 4.2.1.2 Testing ○ 4.2.1.3 Documentation of procedures 4.2.2 Detection and analysis ○ 4.2.2.1 Characteristics contributing to severity level classification ○ 4.2.2.2 Downtime ○ 4.2.2.3 Recovery time ○ 4.2.2.4 Data integrity ○ 4.2.2.5 Economic ○ 4.2.2.6 System process criticality ○ 4.2.2.7 Reverse engineering ○ 4.2.2.8 Data correlation 4.2.3 Containment ○ 4.2.3.1 Segmentation ○ 4.2.3.2 Isolation 4.2.4 Eradication and recovery ○ 4.2.4.1 Vulnerability mitigation ○ 4.2.4.2 Sanitization ○ 4.2.4.3 Reconstruction/reimaging ○ 4.2.4.4 Secure disposal ○ 4.2.4.5 Patching ○ 4.2.4.6 Restoration of permissions ○ 4.2.4.7 Reconstitution of resources ○ 4.2.4.8 Restoration of capabilities and services ○ 4.2.4.9 Verification of logging/communication to security monitoring 4.2.5 Post-incident activities ○ 4.2.5.1 Evidence retention ○ 4.2.5.2 Lessons learned report ○ 4.2.5.3 Change control process ○ 4.2.5.4 Incident response plan update ○ 4.2.5.5 Incident summary report	8.3 12.4 15.1, 15.2, 15.3

	○ 4.2.5.6 IoC generation ○ 4.2.5.7 Monitoring	
4.3	Given an incident, analyze potential indicators of compromise. 4.3.1 Network-related ○ 4.3.1.1 Bandwidth consumption ○ 4.3.1.2 Beaconing ○ 4.3.1.3 Irregular peer-to-peer communication ○ 4.3.1.4 Rogue device on the network ○ 4.3.1.5 Scan/sweep ○ 4.3.1.6 Unusual traffic spike ○ 4.3.1.7 Common protocol over non-standard port 4.3.2 Host-related ○ 4.3.2.1 Processor consumption ○ 4.3.2.2 Memory consumption ○ 4.3.2.3 Drive capacity consumption ○ 4.3.2.4 Unauthorized software ○ 4.3.2.5 Malicious process ○ 4.3.2.6 Unauthorized change ○ 4.3.2.7 Unauthorized privilege ○ 4.3.2.8 Data exfiltration ○ 4.3.2.9 Abnormal OS process behavior ○ 4.3.2.10 File system change or anomaly ○ 4.3.2.11 Registry change or anomaly ○ 4.3.2.12 Unauthorized scheduled task 4.3.3 Application-related ○ 4.3.3.1 Anomalous activity ○ 4.3.3.2 Introduction of new accounts ○ 4.3.3.3 Unexpected output ○ 4.3.3.4 Unexpected outbound communication ○ 4.3.3.5 Service interruption ○ 4.3.3.6 Application log	2.1 4.1 5.1, 5.2, 5.3 6.1, 6.2 7.1, 7.2, 7.4 8.2, 8.3 9.1, 9.2, 9.3, 9.4, 9.5 10.1, 10.3 11.1, 11.2 15.1, 15.2, 15.4
4.4	Given a scenario, utilize basic digital forensics techniques. 4.4.1 Network	8.2 9.3, 9.4 10.2, 10.4

	○ 4.4.1.1 Wireshark ○ 4.4.1.2 tcpdump 4.4.2 Endpoint ○ 4.4.2.1 Disk ○ 4.4.2.2 Memory 4.4.3 Mobile 4.4.4 Cloud 4.4.5 Virtualization 4.4.6 Legal hold 4.4.7 Procedures 4.4.8 Hashing ○ 4.4.8.1 Changes to binaries 4.4.9 Carving 4.4.10 Data acquisition	11.1 14.2, 14.3
5.0	**Compliance and Assessment**	
5.1	Understand the importance of data privacy and protection. 5.1.1 Privacy vs. security 5.1.2 Non-technical controls ○ 5.1.2.1 Classification ○ 5.1.2.2 Ownership ○ 5.1.2.3 Retention ○ 5.1.2.4 Data types ○ 5.1.2.5 Retention standards ○ 5.1.2.6 Confidentiality ○ 5.1.2.7 Legal requirements ○ 5.1.2.8 Data sovereignty ○ 5.1.2.9 Data minimization ○ 5.1.2.10 Purpose limitation ○ 5.1.2.11 Non-disclosure agreement (NDA) 5.1.3 Technical controls ○ 5.1.3.1 Encryption ○ 5.1.3.2 Data loss prevention (DLP) ○ 5.1.3.3 Data masking ○ 5.1.3.4 Deidentification ○ 5.1.3.5 Tokenization	3.1 8.3, 8.4 12.1 14.1

	○ 5.1.3.6 Digital rights management (DRM) - Watermarking ○ 5.1.3.7 Geographic access requirements ○ 5.1.3.8 Access controls	
5.2	Given a scenario, apply security concepts in support of organizational risk mitigation. 5.2.1 Business impact analysis 5.2.2 Risk identification process 5.2.3 Risk calculation ○ 5.2.3.1 Probability ○ 5.2.3.2 Magnitude 5.2.4 Communication of risk factors 5.2.5 Risk prioritization ○ 5.2.5.1 Security controls ○ 5.2.5.2 Engineering tradeoffs 5.2.6 Systems assessment 5.2.7 Documented compensating controls 5.2.8 Training and exercises ○ 5.2.8.1 Red team ○ 5.2.8.2 Blue team ○ 5.2.8.3 White team ○ 5.2.8.4 Tabletop exercise 5.2.9 Supply chain assessment ○ 5.2.9.1 Vendor due diligence ○ 5.2.9.2 Hardware source authenticity	3.1, 3.2, 3.3 7.2 11.4 12.4
5.3	Explain the importance of frameworks, policies, procedures, and controls. 5.3.1 Frameworks ○ 5.3.1.1 Risk-based ○ 5.3.1.2 Prescriptive 5.3.2 Policies and procedures ○ 5.3.2.1 Code of conduct/ethics ○ 5.3.2.2 Acceptable use policy (AUP) ○ 5.3.2.3 Password policy ○ 5.3.2.4 Data ownership ○ 5.3.2.5 Data retention	2.2, 2.3 5.2 7.4 8.2, 8.3 10.2, 10.7 11.3, 11.4 12.3

	○ 5.3.2.6 Account management ○ 5.3.2.7 Continuous monitoring ○ 5.3.2.8 Work product retention 5.3.3 Category ○ 5.3.3.1 Managerial ○ 5.3.3.2 Operational ○ 5.3.3.3 Technical 5.3.4 Control type ○ 5.3.4.1 Preventative ○ 5.3.4.2 Detective ○ 5.3.4.3 Corrective ○ 5.3.4.4 Deterrent ○ 5.3.4.5 Compensating ○ 5.3.4.6 Physical 5.3.5 Audits and assessments ○ 5.3.5.1 Regulatory ○ 5.3.5.2 Compliance	