ComputerMinds.com

WORK PROCESS SCHEDULE

AND

RELATED INSTRUCTION OUTLINE

Cost breakdown for Related Instruction

Registration	$100.00
Tuition	$8895.00
Books & Supplies	$1500.00
Other – Certification exams	$1500.00
Total	$11995.00

Appendix A

WORK PROCESS SCHEDULE
OCCUPATIONAL TITLE: Cyber Security Support Technician
O*NET-SOC CODE: 15-1122.00 RAPIDS CODE: 2050CB

This schedule is attached to and a part of these Standards for the above identified occupation.

1. TYPE OF OCCUPATION

☐ Time-based ☒ Competency-based ☐ Hybrid

2. TERM OF APPRENTICESHIP

The term of the occupation is competency-based training supplemented by and 340 hours of related instruction.

3. RATIO OF APPRENTICES TO JOURNEYWORKERS

The apprentice to Mentor ratio is: 3 Apprentices to 1 Mentor.

4. APPRENTICE WAGE SCHEDULE

Apprentices shall be paid a progressively increasing schedule of wages based on a dollar amount of the Mentor wage rate, which is $25.00 per hour.

Term:

Unpaid related instruction training (front- loaded)

1st	$10.00 to $15.00 (6 months)
2nd	$15.00 to $20.00 (6 months)

5. WORK PROCESS SCHEDULE (See attached Work Process Schedule)

6. RELATED INSTRUCTION OUTLINE (See attached Related Instruction Outline)

Appendix A

WORK PROCESS
OCCUPATIONAL TITLE: Cyber Security Support Technician
O*NET-SOC CODE: 15-1122.00 RAPIDS CODE: 2050CB

JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols	NICE Framework Specialty Area
A: Locates (in Intranet, employee handbook or security protocols) organizational policies intended to maintain security and minimize risk and explains their use	Education and Training
B: Provides guidance to employees on how to access networks, set passwords, reduce security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files	Information Assurance Compliance
C: Ensures that password characteristics are explained and enforced and that updates are required and enforced based on appropriate time intervals	Information Assurance Compliance
D: Explains company or organization's policies regarding the storage, use and transfer of sensitive data, including intellectual property and personally identifiable information. Identifies data life cycle, data storage facilities, technologies and describes business continuity risks	Education and Training
E: Assists employees in the use of technologies that restrict or allow for remote access to the organization's information technology network	Education and Training
F: Articulates the business need or mission of the organization as it pertains to the use of IT systems and the storage of sensitive data	System Security Architecture
JOB FUNCTION 2: Provides technical support to users or customers	
A: Manages inventory of IT resources	Customer Service and Technical Support
B: Diagnoses and resolves customer-reported system incidents	Digital forensics
C: Installs and configures hardware, software and peripheral equipment for system users	Customer service Technical support
D: Monitors client-level computer system performance	Customer service Technical support

E: Tests computer system performance	Customer Service and Technical Support
F: Troubleshoots system hardware and software	Customer Service and Technical Support
G: Administers accounts, network rights, and access to systems and equipment	Customer Service and Technical Support
JOB FUNCTION 3: Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information	
A: Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components	Systems Security Architecture
B: Assists in network backup and recovery procedures	Network Services
C: Diagnoses network connectivity problems	Network Services
D: Integrates new systems into existing network architecture	Network Services
E: Patches network vulnerabilities to ensure information is safeguarded against outside parties	Network Services
F: Repairs network connectivity problems	Network Services
G: Tests and maintains network infrastructure including software and hardware devices	Network Services
H: Establishes adequate access controls based on principles of least privilege and need-to-know	Systems Security Analysis
I: Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines	
JOB FUNCTION 4: Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration	
A: Checks system hardware availability, functionality, integrity and efficiency	System Admin

B: Conducts functional and connectivity testing to ensure continuing operability	System Admin
C: Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and testing	System Admin
D: Documents compliance with or changes to system administration standard operating procedures	System Admin
E: Installs server fixes, updates and enhancements	System Admin
F: Maintains baseline system security according to organizational policies	System Admin
G: Manages accounts, network rights and access to systems and equipment	System Admin
H: Monitors and maintains server configuration	System Admin
I: Supports network components	System Admin
J: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs	System Admin
K: Verifies data redundancy and system recovery procedures	System Admin
L: Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software	System Admin
M: Provides ongoing optimization and problem-solving support	System Admin
N: Resolves hardware/software interface and interoperability problems	System Admin
JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats	
A: Installs and maintains cyber security detection, monitoring and threat management software	Computer Network Defense Analysis
B: Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list	Computer Network Defense Analysis
C: Manages IP addresses based on current threat environment	
D: Ensures application of security patches for commercial products integrated into system design	Systems security analysis

JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities	
A: Applies security policies to meet security objectives of the system	Systems Security Analysis
B: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices	Systems Security Analysis
C: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs	Systems Security Analysis
D: Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results	Vulnerability Assessment and Management
E: Documents systems security operations and maintenance activities	Systems Security Analysis
JOB FUNCTION 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats	
A: Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities	Systems Security Analysis
B: Assists in researching cost-effective security controls to mitigate risks	Vulnerability Assessment and Management
C: Documents and escalates incidents that may cause immediate or long-term impact to the environment	Computer network Defense Analysis
D: Sets containment blockers to align with company policy regarding computer use and web access	Computer network Defense Analysis
JOB FUNCTION 8: Responds to cyber intrusions and attacks and provides defensive strategies	
A: Tracks and documents computer network defense incidents from initial detection through final resolution	Incident Response
B: Performs virus scanning on digital media	Digital forensics

Appendix A

RELATED INSTRUCTION OUTLINE
OCCUPATIONAL TITLE: Cyber Security Support Technician
O*NET-SOC CODE: 15-1122.00   RAPIDS CODE: 2050CB

A Business Framework for the Governance and Management of Enterprise IT	
Overview of COBIT 5	
Meeting Stakeholder Needs, Introduction COBIT 5 Goals Cascade Stakeholder Drivers Influence Stakeholder Needs Stakeholder Needs Cascade to Enterprise Goals Enterprise Goals Cascade to IT-related Goals IT-related Goals Cascade to Enabler Goals	
Covering the Enterprise End-to-end, Governance Approach Governance Enablers, Governance Scope, Roles, Activities and Relationships	
Applying a Single Integrated Framework COBIT 5 Framework Integrator	
Enabling a Holistic Approach, COBIT 5 Enablers, Systemic Governance and Management through Interconnected Enablers, COBIT 5 Enabler Dimensions, Enabler Dimensions, Enabler Performance Management, Example of Enablers in Practice	
Separating Governance from Management, Governance and Management, Interactions between Governance and Management	
Implementation Guidance – Introduction, Considering the Enterprise Context Creating the Appropriate Environment, Recognizing Pain Points and Trigger Events Enabling Change, A Life Cycle Approach, Getting Started: Making the Business Case	
Process Capability Model, Introduction Differences Between the COBIT 4.1 Maturity Model and the COBIT 5 Process Capability Model, Differences in Practice, Benefits of the Changes, Performing Process Capability Assessments in COBIT 5	
Exit –COBIT 5 certification exam	**40**

Appendix A

RELATED INSTRUCTION OUTLINE
OCCUPATIONAL TITLE: Cyber Security Support Technician
O*NET-SOC CODE: 15-1122.00   RAPIDS CODE: 2050CB

Familiarizing Yourself with Linux	
Managing User and Group Accounts	
Managing Partitions and the Linux Filesystem	
Managing Files in Linux -	
Working with Linux Permissions and Ownership -	
Printing Files -	
Managing Packages -	
Essential System Services Managing Kernel Services	
Working with the Bash Shell and Shell Scripts	
Managing Jobs and Processes	
Managing System Services	
Configuring Network Services	
Configuring Basic Internet Services	
Securing Linux	
Managing Hardware	
Troubleshooting Linux Systems	
Installing Linux	
Configuring the GUI	
Exit – CompTIA Linux Certification	**120**

Appendix A

RELATED INSTRUCTION OUTLINE
OCCUPATIONAL TITLE: Cyber Security Support Technician
O*NET-SOC CODE: 15-1122.00 RAPIDS CODE: 2050CB

Secure Access - Secure management, AAA concepts, 802.1X authentication, BYOD	
VPN - VPN concepts, Remote access VPN, Site-to-site VPN, Securing routing protocols, Securing the control plane, Common Layer 2 attacks, VLAN security	
Secure Routing and Switching – Security on Cisco routers, Securing routing protocols Securing the control plane, Common Layer 2 attacks Mitigation procedures VLAN security	
Cisco Firewall Technologies – Describe operational strengths and weaknesses of the different firewall technologies, Compare stateful vs. stateless firewalls, Implement NAT on Cisco ASA 9.x Implement zone-based firewall, Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x	
IPS - Describe IPS deployment considerations, Describe IPS technologies	
Content and Endpoint Security – Describe mitigation technology for email-based threats, Describe mitigation technology for web-based threats, Describe mitigation technology for endpoint threats	
Exit – CEH Certification exam	80

Appendix A

RELATED INSTRUCTION OUTLINE
OCCUPATIONAL TITLE: Cyber Security Support Technician
O*NET-SOC CODE: 15-1122.00   RAPIDS CODE: 2050CB

Understanding Cybersecurity Fundamentals – 100 clock hours	**100**
Network Concepts - Understanding the TCP/IP Protocol Suite, Understanding the Network Infrastructure, Understanding Common TCP/IP Attacks, Understanding Basic Cryptography Concepts	
Security Concepts - Network Applications and Endpoint Security - Describing Information Security Concepts, Understanding Network Applications, Understanding Common Network Application Attacks, Understanding Windows Operating System Basics, Understanding Linux Operating System Basics, Understanding Common Endpoint Attacks, Understanding Network Security Technologies, Understanding Endpoint Security Technologies	
Cryptography	
Host-Based Analysis	
Security Monitoring and Analysis - Describing Security Data Collection, Describing Security Event Analysis	
Implementing Cybersecurity Operations	
SOC Overview - Defining the Security Operations Center, Understanding NSM Tools and Data, Understanding Incident Analysis in a Threat-Centric SOC, Identifying Resources for Hunting Cyber Threats	
Security Incident Investigations - Understanding Event Correlation and Normalization Identifying Common Attack Vectors. Identifying Malicious Activity, Identifying Patterns of Suspicious Behavior, Conducting Security Incident Investigations	
SOC Operations - Describing the SOC Playbook, Understanding the SOC Metrics Understanding the SOC WMS and Automation, Describing the Incident Response Plan	
Data and Event Analysis - Explore Network Security Monitoring Tools, Investigate Hacker Methodology, Hunt Malicious Traffic, Correlate Event Logs, PCAPs, and Alerts of an Attack, Investigate Browser-Based Attacks, Analyze Suspicious DNS Activity, Investigate Suspicious Activity Using Security Onion, Investigate Advanced Persistent Threats, Explore SOC Playbooks	
Exit - Cisco Cyber Ops certification	**40**
	140