Cybersecurity
at Columbus State

Entry-level Associate Degree Cybersecurity Technician[1] [2] Job Description

Overview

A successful entry-level associate degree Cybersecurity Technician has two main purposes: (1) to protect data from unauthorized access and (2) to determine how any unauthorized access occurred. The sequence of entry-level tasks focus on an initial triage of the event, verification of the event, disposition of a work ticket or escalation to higher-level personnel when necessary.

Roles of an Entry-level Associate Degree Cybersecurity Technician	
1. Network Security Analysis (the primary role)	5. Vulnerability Analysis
2. Risk Analysis	6. End Point Security Controls Analysis
3. Security Awareness Analysis	7. Applications Security Analysis
4. Identify Access Analysis	8. Incident Response Analysis

For the following eight roles, the primary tasks are identified as well as the primary technology used.

Role 1. Network Security Analysis (the primary role)

1.01 Monitor network segmentation
1.02 Prevent intrusion
1.03 Detect intrusion
1.04 Operate and maintain firewalls
1.05 Operate and maintain routing
1.06 Engage in offensive security (prevention testing, also known as ethical hacking)
1.07 Follow protocols

Technology Used: Numerous

Role 2. Risk Analysis

2.01 Conduct qualitative and quantitative analysis of risks for the current system
2.02 Perform methodology for proven risk assessments
2.03 Classify data
2.04 Execute compliance against internal policies, industry standards, and pertinent regulations

Technology Used: Factor Analysis Information Risk (Fair) Analysis Software

[1] Outcomes from Compression Planning® session held 11-16-2015 with industry representatives and Columbus State Community College faculty members

[2] Project funded by the National Science Foundation grant entitled “Ohio Region CyberSecurity (ORCS) Technician Training Pipeline “ (NSF Project Number 150119)

Role 3. Security Awareness Analysis

3.01 Educate vendors and users on security awareness issues
3.02 Educate vendors and users on phishing campaigns
3.03 Conduct table top exercises
3.04 Conduct war gaming on the existing system
3.05 Conduct social engineering awareness training

Technology Used: Cobalt Strike, Social Engineering Toolkit

Role 4. Identity Access Analysis

4.01 Manage user access rights
4.02 Operate multi-factor authentication
4.03 Serve as liaison between the operations team, equipment and space
4.04 Conduct "what if" analyses of multiple scenarios
4.05 Serve as a project manager

Technology Used: Regularly evolving

Role 5. Vulnerability Analysis

5.01 Run scans of the system
5.02 Validate system penetrations
5.03 Triage system penetrations
5.04 Manage vendor tool sets

Technology Used: Nessus Vulnerability Scanner

Role 6. End Point Security Controls Analysis

6.01 Manage mobile devices
6.02 Operate anti-virus software
6.03 Monitor and manage firewalls
6.04 Perform disc encryption
6.05 Perform host based intrusion prevention (HIPS)

Technology Used: MacAfee Policy Orchestrator, Symantec End Point Protection

Role 7. Application Security Analysis

7.01 Develop secure coding/secure software
7.02 Develop tools
7.03 Conduct run-time monitoring

Technology Used: Kali, Burp Suite, Zed Attack Proxy

Role 8. Incident Response Analysis

8.01 Conduct digital forensics
8.02 Maintain chain of custody
8.03 Document findings
8.04 Follow incident response methodology

Technology Used: Guidance Software

Roles, Responsibilities, and Tasks of the Entry-level Associate Degree Cybersecurity Technician
Segmented according to the
National Cybersecurity Workforce Framework 2.0[3]

A. Securely Provision

A-01 Conduct quantitative and qualitative analysis of risk
A-02 Manage user access rights
A-03 Manage mobile devices
A-04 Manage system life cycle
A-05 Perform networking segmentation and monitoring
A-06 Execute compliance against internal policies, industry standards, and pertinent regulations
A-07 Develop secure software
A-08 Develop tools

B. Operate and Maintain

B-01 Protect data from unauthorized access
B-02 Monitor system for unauthorized access
B-03 Provide access rights to users
B-04 Perform Governance, Risk Management, and Compliance (GRC)
B-05 Monitor network segmentation

C. Protect and Defend

C-01 Protect data from unauthorized access
C-02 Monitor system for unauthorized access
C-03 Understand the attack sequence
C-04 Manage vulnerability
C-05 Prevent data loss
C-06 Monitor network segmentation
C-07 Conduct root cause analysis
C-08 Conduct incident response
C-09 Conduct incident management
C-10 Perform offensive security

D. Investigate

D-01 Determine how unauthorized access occurred
D-02 Understand the attack sequence
D-03 Investigate failure modes
D-04 Conduct root cause analysis
D-05 Conduct incident response
D-06 Conduct incident management
D-07 Reverse engineer code
D-08 Perform offensive security

E. Collect and Operate

E-01 Monitor system for unauthorized access
E-02 Conduct threat intelligence monitoring

F. Analyze

[3] From the National Initiative for Cybersecurity Education (NICE) Framework (http://csrc.nist.gov/nice/framework/)

F-01 Conduct threat intelligence monitoring
F-02 Determine how unauthorized access occurred
F-03 Conduct root cause analysis
F-04 Conduct quantitative and qualitative analysis of risk
F-05 Reverse engineer code

G. Oversight and Development

G-01 Conduct quantitative and qualitative analysis of risk
G-02 Educate vendors and users on security awareness issues
G-03 Conduct risk management of third parties
G-04 Classify data
G-05 Perform Governance, Risk Management, and Compliance (GRC)

General Knowledge	
GN-01 General networking	GN-11 Effective written, verbal communication
GN-02 Experimental design	GN-12 Effective legal and risk communication (know what you can and cannot say outside your organization)
GN-03 Operating Systems	GN-13 Technical writing
GN-04 Computer science word problems	GN-14 General hardware knowledge
GN-05 Data analysis	GN-15 General mathematics and statistics
GN-06 Pattern recognition	GN-16 Troubleshooting
GN-07 Business acumen	GN-17 Principles of project management
GN-08 Security acumen	GN-18 General knowledge of scripting language (Python, Ruby)
GN-08 Information security acumen	GN-19 Working in a team/project-based learning
GN-09 Investigation of failure modes	
GN-10 Root cause analysis	

Soft Skills	
SC-01 Time management and prioritization	SC-06 Flexibility and adaptability
SC-02 Problem solving	SC-07 Teamwork and collaboration
SC-03 Negotiation	SC-08 Natural sense of curiosity; hacker mentality
SC-04 Perseverance	SC-09 Sense of morality and ethics
SC-05 Dealing with ambiguity	

Specialized Equipment/Software	
SE-01 Open source tools	SE-07 Symantec End Point Protection
SE-02 Factor Analysis Information Risk (Fair) Analysis Software	SE-08 Kali
	SE-09 Burp Suite
SE-03 Cobalt Strike	SE-10 Zed Attack Proxy
SE-04 Social Engineering Toolkit	SE-11 Guidance Software
SE-05 Nessus Vulnerability Scanner	SE-12 Python
SE-06 MacAfee Policy Orchestrator	SE-13 Ruby

General Understanding, But not a Specific Task for Entry-level Technicians	
GU-01 Policy development	GU-04 Reverse engineering of code
GU-02 Third-party risk management	GU-05 Standards development (HIPPA, PCI)
GU-03 Governance, Risk Management, and Compliance (GRC)	GU-06 Incident management
	GU-07 Data loss prevention