SECURITY ANALYST
(Time-Based)

APPENDIX A

O*NET CODE 15-1122.00

This training outline is a minimum standard for Work Processes and Related Instruction. Changes in technology and regulations may result in the need for additional on-the-job or classroom training.

A Security Analyst helps ensure the security of an organization's: employees, capital assets, and proprietary information by providing strategic direction, tactical management, policy development and disaster recovery strategies.

Potential Job Titles: Information Security Analyst, Computer Systems Analyst

WORK PROCESSES

	Approximate Hours
A. Workplace Basics	**80**
1. Describe workplace organizational structure.	
2. Describe workplace policies and procedures; general and Information Technology (IT) related.	
3. Demonstrate ability to communicate technical ideas/concepts when assisting users unfamiliar with IT jargon.	
B. Security Analyst Fundamentals	**160**
1. Identify and demonstrate knowledge of computer hardware, including but not limited to: a. Central Processing Unit (CPU); b. hard drive; c. memory; d. ports; e. buses; f. slots.	
2. Acquire and demonstrate knowledge of the information security industry.	
C. Computer and Data Operation	**480**
1. Install and configure IT security firewalls and routers.	
2. Configure and troubleshoot security services including, but not limited to IPS (Intrusion Preventions Systems), IDS (Intrusion Detection Systems), URL Filters, and DDOS (Distributed Denial of Service protection).	
3. Review monitoring and security system logs and directly coordinate remediation of identified issues.	

D. Intelligence and Security Networking **320**

1. Configure a network operating system, including protocols, accessibility, and layering.
2. Support and maintain network equipment including, but not limited to, Cisco, Meraki, SonicWall, and HP.
3. Install, configure and troubleshoot remote access VPN (Virtual Private Network).
4. Maintain security intelligence network by designing and implementing organizational security policies and strategies.
5. Configure and troubleshoot site to site IPSVPN (Internet Protocol Security Virtual Private Networks) on routers and firewall platforms.

E. Internal Cyber Security **320**

1. Secure the organization and its people by maintaining an intelligence network, designing and implementing policies and strategies of organization security, i.e. Social Media, Disaster Recovery (D/R), Payment Card Industry (PCI) Data Security Standard, etc.
2. Develop new security programs by reviewing existing security procedures, conducting comprehensive studies of threats and continuously review and assess other potential threats.
3. Develop security awareness by providing orientation, educational programs, and on-going communication.
4. Establish system controls by developing framework for controls and levels of access; recommend improvements.
5. Evaluate, assess, and report on all new technologies and products to be used within the organization for security risks.

F. External Cyber Security **640**

1. Consult with clients on information security best practices and solutions.
2. Perform risk audits for clients and effectively develop a roadmap for subsequent steps which will allow the client to maintain an understanding of the risk.
3. Effectively develop policies and procedures for clients to employ within their corporate environment.
4. Perform ethical hacking/penetration testing to assess external risks.

5. Utilize computer forensics to reconstruct a security breach.
6. Maintain relationships with key technology vendors such as: Blue Coat, IBM, Barracuda, etc.

Approximate Total Hours 2000

Apprenticeship work processes are applicable only to training curricula for apprentices in approved programs. Apprenticeship work processes have no impact on classification determinations under Article 8 or 9 of the Labor Law. For guidance regarding classification for purposes of Article 8 or 9 of the Labor Law, please refer to https://dol.ny.gov/public-work-and-prevailing-wage.

SECURITY ANALYST

APPENDIX B

RELATED INSTRUCTION

Safety/Health/Environment

1. General Workplace Safety
2. First Aid & CPR (minimum 6.5 hours)
3. Right-to-Know/ Safety Data Sheets (SDS)
4. Sexual Harassment Prevention – must comply with Section 201-g of the Labor Law

Computer and Network Components and Operations

1. Hardware
2. Peripherals
3. Software/Installation and configuration of software
4. Operating Systems, e.g., Microsoft, MacOS
5. Troubleshooting
6. Networks: Local Area Network (LAN); Wide Area Network (WAN)
7. Domain Name Servers
8. Domain Controllers
9. Transmission Control Protocol (TCP) / Internet Protocol (IP)
10. Installation and configuration of various network devices
11. Network Functions
12. Routers/Routing Protocol
13. Cybersecurity and Computer Forensics
14. Databases (if Work Process E is selected in Appendix A)
15. Multi-Media applications (if Work Process E is selected in Appendix A)
16. Video applications (if Work Process E is selected in Appendix A)

Professional Development

1. Technical Support Communication
2. Time Management

3. Basic Project Management
4. Team and Supervisor Communication Skills
5. Customer Service Fundamentals
6. Industry recognized credentials/certifications pertaining to the field

Other Topics as Necessary

A minimum of 144 hours of Related Instruction is required for each apprentice for each year.

Appendix B topics are approved by New York State Education Department.