Cybersecurity Specialist
WORK PROCESSES & SKILLS

Work Processes & Skills

- Provides technical support to users or customers. Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware and software that permit sharing and transmission of information.

- Installs, configures, troubleshoot, 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. Configures tools and technologies to detect, mitigate and prevent potential threats.

- Responds to cyber intrusions and attacks and provides defensive strategies.

- Responds to cyber intrusions and attacks and provides defensive strategies. Reviews network utilization data to identify unusual patterns, suspicious activity, or signs of potential threats.

REGISTERED WITH:

DIVISION OF
APPRENTICESHIP
STANDARDS
DAS
STATE OF CALIFORNIA
DEPARTMENT OF INDUSTRIAL RELATIONS

DEPARTMENT OF LABOR
UNITED STATES OF AMERICA

Cybersecurity Specialist
WORK PROCESSES & SKILLS

Apprentices shall satisfactorily complete prescribed courses of related and supplemental instruction, which will not be less than **144 hours per year**. Related and supplemental instruction will be provided by Community Colleges. Time spent in related and supplemental instruction may not be compensated. The following related training outline identifies subject matter that must be mastered by the Apprentice (although not necessarily in the order listed) in order to successfully complete the program. While working, apprentices must complete a minimum of 144 hours of instruction per year. Leading up to on-the-job learning, apprentices may frontload the related instruction as full-time students. Based on previous education and experience, apprentices may need all or a portion of the RSI track.

Related Instruction Content May Include

ADVANCED SECURITY CONCEPTS AND PRACTICES	72 HOURS
COMPUTERS FORENSICS FUNDAMENTALS	72 HOURS
FUNDAMENTALS: INFORMATION SYSTEMS SECURITY AUDITING	54 HOURS
HEALTHCARE INFORMATION SECURITY & PRIVACY FOR PRACTITIONERS	80 HOURS
INFORMATION AND COMMUNICATION TECHNOLOGY ESSENTIALS	80 HOURS
INFORMATION COMPETENCY & TECHNOLOGY LITERACY	54 HOURS
INFORMATION AND NETWORK SECURITY	54 HOURS
INTRODUCTION TO CYBERSECURITY: ETHICAL HACKING	72 HOURS
INTRODUCTION TO COMPUTER INFORMATION SYSTEMS	72 HOURS
INTRODUCTION TO PYTHON PROGRAMMING	75 HOURS
PRINCIPLES OF CYBERSECURITY ANALYSIS	80 HOURS
SYSTEMS AND NETWORK ADMINISTRATION	80 HOURS