CYBERSECURITY SUPPORT TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among their many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

In most organizations, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Support Technician may perform a variety of the following functions:

- Provide technical support to users or customers.
- Install, configure, test, operate, maintain, and manage networks and their firewalls including hardware and software that permit sharing and transmission of information.
- Review network utilization data to identify unusual patterns, suspicious activity or signs of potential threats.
- Configure tools and technologies to detect, mitigate and prevent potential threats.
- Assess and mitigate system network, business continuity and related security risks and vulnerabilities.
- Respond to cyber intrusions and attacks and provide defensive strategies.
- Test computer system operations to ensure proper functioning.
- Document computer security and emergency measures policies, procedures, and tests.
- Monitor use of data files and regulate access to safeguard information in computer files.

TOP SKILLS*

Professional Skills

- Complex Problem Solving
- Coordination
- Critical Thinking
- Judgment & Decision Making
- Mathematics
- Reading Comprehension
- Time Management
- Writing

Technical Skills

- Equipment Selection
- Operations Analysis
- Operation and Control
- Operation Monitoring
- Quality Control Analysis
- Systems Analysis
- Systems Evaluation
- Troubleshooting

TOP KNOWLEDGE AREAS

- Computers and electronics knowledge of circuit boards, processors, chips, electronic equipment, and computer hardware and software, including applications and programming.
- Transmission, broadcasting, switching, control, and operation of telecommunications systems.
- Principles and processes for providing customer and personal services, including customer needs assessment, meeting quality standards for services, and evaluation of customer satisfaction.

MEDIAN SALARY*

$50,000

10-YEAR PROJECTED JOB GROWTH RATE*

11%

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

VULNERABILITY ASSESSMENT ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Vulnerability Assessment Analyst may perform a variety of the following functions:

- Identify critical flaws in applications and systems that cyber attackers could exploit.
- Conduct vulnerability assessments to networks, applications, and operating systems.
- Conduct network security audits and scanning on a predetermined basis.
- Use automated tools to pinpoint vulnerabilities and reduce time-consuming tasks.
- Use manual testing techniques and methods to gain a better understanding of the environment and reduce false negatives.
- Develop, test, and modify custom scripts and applications for vulnerability testing.
- Write and present a comprehensive vulnerability assessment and maintain a database.
- Supply hands-on training for networks and systems administrators.

TOP SKILLS*

- Alternative Problem Solving
- Curious and Creative
- Attention to Detail
- Strong Communications
- Interest in Hacking

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$75,000

10-YEAR PROJECTED JOB GROWTH RATE*

20%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

TECHNICAL SUPPORT SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Technical Support Specialist may perform a variety of the following functions:

- Install and maintain network infrastructures and device operating systems.
- Troubleshoot system hardware and software issues.
- Analyze incident data for emerging trends.
- Develop and deliver technical training to users and other customers.
- Diagnose and resolve customer-reported system incidents, problems, and security events.
- Make recommendations based on trend analysis for changes to software and hardware to enhance user experience.
- Install and configure hardware, software, and other equipment for systems users that adheres to security standards.
- Administer accounts, network rights, and access to systems and equipment.
- Perform asset management / inventory of information technology (IT) resources.

TOP SKILLS*

- Complex Problem Solving
- Systems Thinking
- Attention to Detail
- Resource Management

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$50,000

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

SYSTEMS ADMINISTRATOR

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Systems Administrator may perform a variety of the following functions:

- Manage accounts, network rights, and access to systems and equipment.
- Maintain baseline system security according to organizational policies.
- Provide ongoing optimization and problem-solving support.
- Install, update, and troubleshoot systems / servers.
- Troubleshoot hardware / software interface and interoperability problems.
- Oversee installation, implementation, configuration, and support of system components.
- Manage system / server resources including performance, capacity, availability, serviceability, and recoverability.
- Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.

TOP SKILLS*

- Strong Leader and Communicator
- Organization
- Problem-Solver
- Analytical

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, or field certification.

MEDIAN SALARY*

$67,000

10-YEAR PROJECTED JOB GROWTH RATE*

8%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

CRIME INVESTIGATOR

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Crime Investigator may perform a variety of the following functions:

- Find and navigate the dark web.
- Process cybersecurity crime scenes.
- Conduct interviews of victims, witnesses, and/or suspects.
- Examine recovered data for information.
- Fuse computer network attack analysis with criminal and counterintelligence investigations and operations.
- Determine whether a security incident is indicative of a violation of law that requires specific legal action.
- Identify elements of proof of the crime.
- Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.
- Provide criminal investigative support to trial counsel during judicial processes.
- Prepare reports to document investigations.

TOP SKILLS*

- Curiosity and Persistence
- Strong Communication
- Information Use
- Critical Thinking

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$67,000

10-YEAR PROJECTED JOB GROWTH RATE*

10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

DEFENSE INCIDENT RESPONDER

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Defense Incident Responder may perform a variety of the following functions:

- Actively monitor systems and network intrusions.
- Identify security flaws and vulnerabilities.
- Perform security audits, risk analysis, network forensics and penetration testing.
- Perform malware analysis and reverse engineering.
- Develop a procedural set of responses to security problems.
- Establish protocols for communication within an organization and dealings with law enforcement during security incidents.
- Create a program development plan that includes security gap assessment, policies, procedures, playbooks, training, and tabletop testing.
- Produce detailed incident reports and technical briefs for management, administrators, and end-users.
- Liaison with other cyber threat analysis entities.

TOP SKILLS*

- Capable of Handling Stress
- Flexible
- Problem Solving
- Analytical
- Good Communication

DEGREE REQUIRED?*

- No
- Some employers require an Associate's degree, Bachelor's degree, related work experience, or field certification.

MEDIAN SALARY*

$80,000

10-YEAR PROJECTED JOB GROWTH RATE*

20%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

SYSTEMS TESTING AND EVALUATION SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Systems Testing and Evaluation Specialist may perform a variety of the following functions:

- Develop test plans to address specifications and requirements.
- Analyze the results of software, hardware, or interoperability testing.
- Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.
- Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
- Make recommendations based on test results.
- Perform environmental testing on systems under development.
- Record and manage test data.
- Validate specifications and requirements for testability.

TOP SKILLS*

- Planning and Organization
- Problem Solving
- Analytical
- Systems Thinking

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$47,000

10-YEAR PROJECTED JOB GROWTH RATE*

20%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by the National Integrated Cyber Education Research Center (NICERC).

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

COMPUTER NETWORK SUPPORT SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Computer Network Support Specialist may perform a variety of the following functions:

- Configure security settings or access permissions for groups or individuals.
- Analyze the results of software, hardware, or interoperability testing.
- Identify the causes of networking problems, using diagnostic testing software and equipment.
- Document network support activities.
- Back up network data.
- Evaluate local area network (LAN) or wide area network (WAN) performance data to ensure availability or speed, to identify network problems, or for disaster recovery purposes.
- Troubleshoot network or connectivity problems for users or user groups.
- Install network software, including security or firewall software.

TOP SKILLS*

- Critical Thinking
- Active Listening
- Judgment and Decision Making
- Active Learning

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$62,770

10-YEAR PROJECTED JOB GROWTH RATE*

4% to 6%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

COMPUTER SYSTEMS ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Computer Systems Analyst may perform a variety of the following functions:

- Expand or modify systems to serve new purposes or improve workflow.
- Consult with management to ensure agreement on system principles.
- Confer with clients regarding the nature of the information processing or computation needs a computer program is to address.
- Develop, document and revise system design procedures, test procedures, and quality standards.
- Train staff and users to work with computer systems and programs.
- Coordinate and link computer systems within an organization to increase compatibility and so information can be shared.
- Assess the usefulness of pre-developed application packages and adapt them to a user environment.
- Define the goals of the system and devise flow charts and diagrams describing logical operational steps of programs.
- Provide staff and users with assistance solving computer related problems, such as malfunctions and program problems.

TOP SKILLS*

- Critical Thinking
- Active Listening
- Systems Analysis and Evaluation
- Active Learning

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$88,740

10-YEAR PROJECTED JOB GROWTH RATE*

7% to 10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

COMPUTER USER SUPPORT SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Computer User Support Specialist may perform a variety of the following functions:

- Answer user inquiries regarding computer software or hardware operation to resolve problems.
- Oversee the daily performance of computer systems.
- Read technical manuals, confer with users, or conduct computer diagnostics to investigate and resolve problems or to provide technical assistance and support.
- Set up equipment for employee use, performing or ensuring proper installation of cables, operating systems, or appropriate software.
- Develop training materials and procedures, or train users in the proper use of hardware or software.
- Refer major hardware or software problems or defective products to vendors or technicians for service.
- Enter commands and observe system functioning to verify correct operations and detect errors.
- Maintain records of daily data communication transactions, problems and remedial actions taken, or installation activities.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Systems Analysis and Evaluation
- Active Learning

DEGREE REQUIRED?*

- No
- Some employers may require training in vocational schools, related work experience, or a recognized apprenticeship program.

MEDIAN SALARY*

$50,980

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

COMPUTER OPERATOR

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Computer Operator may perform a variety of the following functions:

- Enter commands, using computer terminal, and activate controls on computer and peripheral equipment to integrate and operate equipment.
- Oversee the operation of computer hardware systems, including coordinating and scheduling the use of computer terminals and networks to ensure efficient use.
- Monitor the system for equipment failure or errors in performance.
- Answer telephone calls to assist computer users encountering problems.
- Respond to program error messages by finding and correcting problems or terminating the program.
- Retrieve, separate, and sort program output as needed, and send data to specified users.
- Record information such as computer operating time, problems that occurred, and actions taken.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Systems Analysis and Evaluation
- Monitoring
- Operation and Control

DEGREE REQUIRED?*

- No
- Some employers may require one or two years of work experience, informal training with experienced workers, or a recognized apprenticeship program.

MEDIAN SALARY*

$45,840

10-YEAR PROJECTED JOB GROWTH RATE*

-2%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

FINANCIAL & RISK ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Financial & Risk Analyst may perform a variety of the following functions:

- Develop contingency plans to deal with emergencies.
- Recommend ways to control or reduce risk.
- Analyze areas of potential risk to the assets, earning capacity, or success of organizations.
- Document and ensure communication .
- Maintain input or data quality of risk management systems
- Challenge security control design at third parties that use the latest information technology, from cloud to big data analytics.
- Develop process for assessing security controls within cloud environments.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Judgment and Decision Making
- Monitoring
- Systems Analysis

DEGREE REQUIRED?*

- No
- Some employers may require a Bachelor's degree or related work experience.

MEDIAN SALARY*

$70,280

10-YEAR PROJECTED JOB GROWTH RATE*

4% to 6%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine and LinkedIn.com

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

GEOGRAPHIC INFORMATION SYSTEMS TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Geographic Information Systems Technician may perform a variety of the following functions:

- Design or prepare graphic representations of Geographic Information Systems (GIS) data, using GIS hardware or software applications
- Analyze GIS data to identify spatial relationships or display results of analyses, using maps, graphs, or tabular data.
- Maintain or modify existing GIS databases.
- Enter data into GIS databases, using techniques such as coordinate geometry, keyboard entry of tabular data, manual digitizing of maps, scanning or automatic conversion to vectors, or conversion of other sources of digital data.
- Review existing or incoming data for currency, accuracy, usefulness, quality, or completeness of documentation.
- Perform geospatial data building, modeling, or analysis, using advanced spatial analysis, data manipulation, or cartography software.
- Coordinate or design the development of integrated GIS spatial or non-spatial databases.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Judgment and Decision Making
- Systems Analysis

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, vocational training, or field certifications.

MEDIAN SALARY*

$90,270

10-YEAR PROJECTED JOB GROWTH RATE*

7% to 10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

MEDICAL RECORDS & HEALTH INFORMATION TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Medical Records & Health Information Technician may perform a variety of the following functions:

- Protect the security of medical records to ensure that confidentiality is maintained.
- Review records for completeness, accuracy, and compliance with regulations.
- Retrieve patient medical records for physicians, technicians, or other medical personnel.
- Assign the patient to diagnosis-related groups (DRGs), using appropriate computer software.
- Process patient admission or discharge documents.
- Transcribe medical reports.
- Resolve or clarify codes or diagnoses with conflicting, missing, or unclear information by consulting with doctors, or others, or by participating in the coding team's regular meetings.

TOP SKILLS*

- Critical Thinking
- Active Listening
- Reading Comprehension

DEGREE REQUIRED?*

- No
- Some employers may require training in vocational schools, related work experience, field certifications, or a recognized apprenticeship program.

MEDIAN SALARY*

$40,350

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

INFORMATION TECHNOLOGY SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An Information Technology Specialist may perform a variety of the following functions:

- Answer user inquiries regarding computer software or hardware operation to resolve problems.
- Oversee the daily performance of computer systems.
- Read technical manuals, confer with users, or conduct computer diagnostics to investigate and resolve problems or to provide technical assistance and support.
- Set up equipment for employee use, performing or ensuring proper installation of cables, operating systems, or appropriate software.
- Develop training materials and procedures, or train users in the proper use of hardware or software.
- Refer major hardware or software problems or defective products to vendors or technicians for service.
- Enter commands and observe system functioning to verify correct operations and detect errors.
- Maintain records of daily data communication transactions, problems and remedial actions taken, or installation activities.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Systems Analysis and Evaluation
- Active Learning

DEGREE REQUIRED?*

- No
- Some employers may require one or two years of related work experience, field certifications, or a recognized apprenticeship program.

MEDIAN SALARY*

$70,625

10-YEAR PROJECTED JOB GROWTH RATE*

7% to 10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

INFORMATION TECHNOLOGY STRATEGY ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An Information Technology Strategy Analyst may perform a variety of the following functions:

- Manage project execution to ensure adherence to budget, schedule, and scope.
- Confer with project personnel to identify and resolve problems.
- Monitor or track project milestones and deliverables.
- Submit project deliverables, ensuring adherence to quality standards.
- Assess current or future customer needs and priorities by communicating directly with customers, conducting surveys, or other methods.
- Initiate, review, or approve modifications to project plans.
- Schedule and facilitate meetings related to information technology projects.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Coordination
- Time Management

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, or field certifications.

MEDIAN SALARY*

$90,270

10-YEAR PROJECTED JOB GROWTH RATE*

7% to 10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

ELECTRONICS ENGINEERING TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An Electronics Engineering Technician may perform a variety of the following functions:

- Read blueprints, wiring diagrams, schematic drawings, or engineering instructions for assembling electronics units, applying knowledge of electronic theory and components.
- Identify and resolve equipment malfunctions, working with manufacturers or field representatives as necessary to procure replacement parts.
- Test electronics units, using standard test equipment, and analyze results to evaluate performance and determine need for adjustment.
- Adjust or replace defective or improperly functioning circuitry or electronics components, using hand tools or soldering iron.
- Assemble, test, or maintain circuitry or electronic components, according to engineering instructions, technical manuals, or knowledge of electronics, using hand or power tools.

TOP SKILLS*

- Critical Thinking
- Complex Problem Solving
- Judgment and Decision Making
- Operation Monitoring

DEGREE REQUIRED?*

- No
- Some employers may require one or two years of related work experience, informal training with experienced workers, or field certifications

MEDIAN SALARY*

$64,330

10-YEAR PROJECTED JOB GROWTH RATE*

1%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

ELECTRICAL ENGINEERING TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An Electrical Engineering Technician may perform a variety of the following functions:

- Build or test electrical components of electric-drive vehicles or prototype vehicles.
- Interpret test information to resolve design-related problems.
- Provide technical assistance in resolving electrical engineering problems encountered before, during, or after construction.
- Install or maintain electrical control systems or solid-state equipment.
- Evaluate engineering proposals, shop drawings, or design comments for sound electrical engineering practice or conformance with established safety or design criteria.
- Collaborate with electrical engineers or other personnel to identify, define, or solve developmental problems.
- Set up or operate test equipment to evaluate performance of developmental parts, assemblies, or systems under simulated operating conditions.

TOP SKILLS*

- Systems Analysis
- Complex Problem Solving
- Judgment and Decision Making
- Equipment Maintenance
- Quality Control Analysis

DEGREE REQUIRED?*

- No
- Some employers may require one or two years of related work experience, informal training with experienced workers, or field certifications

MEDIAN SALARY*

$64,330

10-YEAR PROJECTED JOB GROWTH RATE*

0% to 1%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

ELECTRONICS ENGINEERING TECHNOLOGIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An Electronics Engineering Technologist may perform a variety of the following functions:

- Modify, maintain, or repair electronics equipment or systems to ensure proper functioning.
- Replace defective components or parts, using hand tools and precision instruments.
- Set up and operate specialized or standard test equipment to diagnose, test, or analyze the performance of electronic components, assemblies, or systems.
- Prepare or maintain design, testing, or operational records and documentation.
- Assemble circuitry for electronic systems according to engineering instructions, production specifications, or technical manuals.
- Provide support to technical sales staff regarding product characteristics.
- Inspect newly installed equipment to adjust or correct operating problems.
- Educate equipment operators on the proper use of equipment.

TOP SKILLS*

- Complex Problem Solving
- Judgment and Decision Making
- Equipment Maintenance
- Repairing

DEGREE REQUIRED?*

- No
- Some employers may require one or two years of related work experience, informal training with experienced workers, or field certifications

MEDIAN SALARY*

$63,200

10-YEAR PROJECTED JOB GROWTH RATE*

2% to 3%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

TELECOMMUNICATIONS ENGINEERING SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Telecommunications Engineering Specialist may perform a variety of the following functions:

- Communicate with telecommunications vendors to obtain pricing and technical specifications for available hardware, software, or services.
- Keep abreast of changes in industry practices and emerging telecommunications technology by reviewing current literature, talking with colleagues, participating in educational programs, attending meetings or workshops, or participating in professional organizations or conferences.
- Implement or perform preventive maintenance, backup, or recovery procedures.
- Consult with users, administrators, and engineers to identify business and technical requirements for proposed system modifications or technology purchases.
- Assess existing facilities' needs for new or modified telecommunications systems.

TOP SKILLS*

- Complex Problem Solving
- Active Learning
- Monitoring
- Judgment and Decision Making

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, one or two years of related work experience, informal training with experienced workers, or a recognized apprenticeship program.

MEDIAN SALARY*

$109,020

10-YEAR PROJECTED JOB GROWTH RATE*

4% to 6%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

WEB DEVELOPER

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Web Developer may perform a variety of the following functions:

- Write supporting code for web applications or websites.
- Design or maintain websites, using authoring or scripting languages, content creation tools, management tools, and digital media.
- Back up files from websites to local directories for instant recovery in case of problems.
- Write, design, or edit web page content, or direct others producing content.
- Select programming languages, design tools, or applications.
- Evaluate code to ensure that it is valid, properly structured, meets industry standards, and is compatible with browsers, devices, or operating systems.
- Identify problems uncovered by testing or customer feedback, and correct problems or refer problems to appropriate personnel for correction.

TOP SKILLS*

- Complex Problem Solving
- Programming
- Critical Thinking
- Operations Analysis

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, one or two years of related work experience, informal training with experienced workers, or a recognized apprenticeship program.

MEDIAN SALARY*

$69,430

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

CRIME ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Cyber Crime Analyst may perform a variety of the following functions:

- Validate known intelligence with data from a variety of sources.
- Gather, analyze, correlate, or evaluate information from a variety of resources, such as law enforcement databases.
- Assist in sensitive and complex long-term investigations into cybercrime and identity theft.
- Collect, organize, and research a wide range of data to develop intelligence and investigative leads on cybercriminals.
- Examine hard drives and other seized media, using specialized software.
- Perform in-depth computer searches of investigative targets.
- Communicate investigative results to other team members and appropriate supervisors.
- Liaise with prosecutors and other law enforcement agencies.
- Perform data entry and administrative tasks.

TOP SKILLS*

- Complex Problem Solving
- Active Learning
- Monitoring
- Critical Thinking

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, or field certification.

MEDIAN SALARY*

$75,751

10-YEAR PROJECTED JOB GROWTH RATE*

10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Glassdoor.com, and Ziprecruiter.com.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

INCIDENT ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Cyber Incident Analyst may perform a variety of the following functions:

- Perform analysis on hosts running on a variety of platforms and operating systems, to include, but not limited to, Microsoft Windows, Mac Operating System (OS), UNIX, Linux, as well as embedded systems and mainframes.
- Monitor open source channels to maintain a current understanding of Computer Network Defense (CND) threat condition and determine which security issues may have an impact on the enterprise.
- Perform analysis of log files from a variety of sources to identify possible threats to network security.
- Leverage tools such as Tanium, FireEye suite, GRR, Volatility, SIFT Workstation, MISP, and/or Bro as part of duties performing cyber incident response analysis.
- Identify intrusion artifacts at the host and network level, have a strong understanding of how discovered data can be used to enable CND hunts and incident mitigation within the enterprise.
- Perform forensically sound collection of host-based images with ability to perform memory and disk forensics.
- Write technical reports on incident findings (e.g. engagement reports) and provide CND guidance to appropriate stakeholders.

TOP SKILLS*

- Complex Problem Solving
- Active Listening
- Critical Thinking
- Monitoring

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, or field certification.

MEDIAN SALARY*

$85,427

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Cyberdegrees.org, and Google Jobs.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Cybersecurity Specialist may perform a variety of the following functions:

- Provide input and assist in developing technology strategies, road map and target architectures to enable the required mission outcome.
- Evaluate new and emerging technologies meeting mission needs and recommending new practices to accommodate changing technology.
- Develop recommendations for resolution of complex program, project, technical, and resource issues.
- Prepare and present status, progress, issues analyses, information reports, and presentations.
- Assist with the development and evaluation of long- and short-term IT strategic planning.
- Support management in the formulation of cyber-related policies.
- Conduct audits of IT programs and projects to determine the need for new systems and software.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- Critical Thinking
- Customer Service

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$86,335

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine and Ziprecruiter.com.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Cybersecurity Technician may perform a variety of the following functions:

- Provide technical expertise in network-centric operations.
- Detect, protect, react and respond to threats against networks.
- Defend against external and internal threats through in-depth technical and non-technical methods.
- Conduct computer network risk mitigation.
- Perform network vulnerability assessments and incident response/reconstruction.
- Maintain active computer network defense, access tool development, and conduct computer/network forensics.
- Run firewall configuration and troubleshooting.
- Setup and management of VPN tunnels both fixed and user based.
- Develop strong understanding of networking and systems protocols.
- Operate endpoint protection and remediation activities.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- Critical Thinking
- Customer Service

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$60,000

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine and Indeed.com

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

VULNERABILITIES TECHNICIAN

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Cyber Vulnerabilities Technician may perform a variety of the following functions:

- Conduct penetration testing for software and mobile applications.
- Evaluate system function for various software configurations and applications.
- Develop and publish software characterization reports.
- Identify system vulnerabilities across multiple operating systems and mobile applications.
- Recommend mitigating measures for capabilities developed internally.
- Perform black box penetration testing.
- Develop custom code to support assessments using multiple programming languages (e.g. Java, Java Script, Python, C++).
- Apply technical knowledge to the design, development, integration, and support of new solutions or products that identify, exploit, or mitigate cyber security vulnerabilities.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- System Analysis
- Analytical Thinking

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$69,500

10-YEAR PROJECTED JOB GROWTH RATE*

20%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine and Caci.com

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

DOCUMENT CONTROL SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Document Control Specialist may perform a variety of the following functions:

- Manage all technical documents for assigned projects regarding quality, revision status, timely receipt and distribution.
- Utilization of database on document control system allowing for tracking of documents, checking of approval loops, revision identification etc.
- Support teams to receive, check and validate drawings, input drawings and quality documents into database system, verify the metadata of each file and ensure timely distribution of the documents.
- Ensure that circulation durations for distribution list and cycle are tracked and any deviations (delays) are reported, as these may impact the project delivery schedule.
- Partners with managers and supervisors to ensure all training is completed timely and accurately.
- Responsible for maintaining all employee training records.
- Process all change orders for new and revised documents.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- System Analysis
- Analytical Thinking

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$58,500

10-YEAR PROJECTED JOB GROWTH RATE*

7% to 10%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine and Indeed.com

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

INFORMATION SECURITY SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An Information Security Specialist may perform a variety of the following functions:

- Design audits of computer systems to ensure operational security and protection from attack.
- Oversee and monitor routine administration of the information security department.
- Coordinate with other departments to promote awareness and training on security protocols.
- Implement, monitor, and maintain policies and standards for information technology-related controls.
- Prepares, maintains, and implements system security plans for high-visibility production systems.
- Ensures implementation of security measures by conducting interviews and table-top exercises.
- Performs various Information assurance support functions in support of the clients' applications.
- Coordinates with IT leads from partner agencies/components to identify opportunities to collaborate in the development and/or leveraging of IT capabilities.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- System Analysis
- Written and Oral

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$75,263

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Cyberdegrees.org, Payscale.com, and Indeed.com

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

IT AUDITOR

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An IT Auditor may perform a variety of the following functions:

- Interface with clients to review and analyze complex systems (Applications, operating systems, databases, and Networking devices), to identify risks, exposures, and define and implement compensating controls.
- Work independently to collect, consolidate and analyze information required for the evaluation of security controls and gaps.
- Produce final reports on compliance to detail the controls observed during security assessments in accordance with various security standards and regulations.
- Travel to client sites as needed.
- Leading walkthrough meetings and discussions with the purpose of developing audit test programs and identifying control issues.
- Prepare audit planning memoranda.
- Work with outside auditors to address financial reporting risks (e.g., SOX IT general controls) and support the external auditing function.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- System Analysis
- Written and Oral

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, or field certification.

MEDIAN SALARY*

$70,000

10-YEAR PROJECTED JOB GROWTH RATE*

18%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Indeed.com, and Accountingdegree.com.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

IT SECURITY SPECIALIST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. An IT Security Specialist may perform a variety of the following functions:

- Develop plans to safeguard computer files against unauthorized modification, destruction or disclosure.
- Choose, implement, monitor and upgrade computer anti-virus and malware protection systems.
- Encrypt data transmissions and erect firewalls to conceal confidential information during transmit.
- Implement password authentication to keep unauthorized users from accessing sensitive data files.
- Modify security files to incorporate new software, correct errors, and change user access status.
- Perform risk assessments and tests on running data processing activities and security measures.
- Educate workers about computer security and promote security awareness and security protocols.
- Keep accurate and current backup files of all-important data on the shared corporate network.
- Work with other IT security professionals who specialize in computer forensics to gather evidence for prosecuting cyber crimes.
- Communicate with other agencies on developments applicable to the development of policies and planning initiative.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- System Analysis
- Written and Oral

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$91,231

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Payscale.com, Indeed.com, and ITcareerfinder.com.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

JUNIOR ANALYST

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Jr. Cybersecurity Analyst may perform a variety of the following functions:

- Monitor applications and hardware for any unusual activity.
- Mitigate damages and patch software during current cyber threats.
- Set up systems that prevent cyber threats including data breaches and traffic spikes.
- Create security systems that prevent cyber attacks, but still allow employees to work without issues.
- Report current and future security concerns to management.
- Analyze architecture and data for needed updates and patches.
- Create relevant documentation and recommendations for changes to the current security architecture.
- Drive the capabilities and execution to effectively optimize and improve enterprise security.
- Recommend configuration and reporting strategies based on the results of vulnerability assessments, to ensure effective achievement of the organizational objectives.

TOP SKILLS*

- Complex Problem Solving
- Attention to Details
- System Analysis
- Written and Oral

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$64,500

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine and Ziprecruiter.com

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

JUNIOR SECURE SYSTEMS ADMINISTRATOR

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Jr. Secure Systems Administrator may perform a variety of the following functions:

- Patch management functions, such as downloading and staging patching, deploying patching in secure environments, or tracking and addressing security compliance and patch management tasks.
- Image, maintain, troubleshoot, and repair hardware.
- Perform system builds and site buildouts per company standards.
- Perform cable management in server racks and workstation areas.
- Light system administration functions (add, change, remove users).
- End user support / customer support functions.
- Follow pre-established system policies and processes.
- Function as go-to IT Desktop Support Technician to fulfill basic IT needs.
- Perform desktop troubleshooting, migration of IT equipment, telephony MACs, and asset management of all IT components.

TOP SKILLS*

- Problem Solving
- Customer Services
- System Analysis
- Organizational and Task Management

DEGREE REQUIRED?*

- No
- Some employers may require related work experience, field certification, or a recognized apprenticeship program.

MEDIAN SALARY*

$50,000

10-YEAR PROJECTED JOB GROWTH RATE*

4% to 6%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Indeed.com, and LinkedIn.com.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

CYBERSECURITY

JUNIOR SECURITY CONSULTANT

Cybersecurity professionals maintain the security and integrity of information technology (IT) systems, networks and devices. Among the many responsibilities, cybersecurity professionals provide the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. These professionals work in a wide range of industries and organizations, including small to large IT companies, professional service companies, contractors, and government agencies.

KEY JOB FUNCTIONS*

Generally, cybersecurity personnel work in three different groups: network personnel, host (computer) personnel, and policy personnel. Some job functions can be in multiple groups. A Jr. Security Consultant may perform a variety of the following functions:

- Use consulting skills to quickly identify problems, analyze challenges, and recommend solutions to a team and/our clients.
- Make company contributions outside of the project by participating in new business, recruiting, and/or strategic initiatives.
- Conduct host forensics, network forensics, log analysis, and malware triage in support of incident response investigations.
- Recognize and codify attacker tools, tactics, and procedures in indicators of compromise (IOCs) that can be applied to current and future investigations.
- Perform network penetration, web and mobile application testing, source code reviews, threat analysis, wireless network assessments and social engineering assessment.
- Build internal scripts, tools and methodologies to enhance capabilities.
- Develop comprehensive and accurate reports and presentations for both technical and executive audiences.
- Work with security and IT operations at clients to implement remediation plans.

TOP SKILLS*

- Problem Solving
- Customer Service
- System Analysis
- Organizational and Task Management

DEGREE REQUIRED?*

- No
- Some employers may require an Associate's degree, Bachelor's degree, related work experience, or field certification.

MEDIAN SALARY*

$68,000

10-YEAR PROJECTED JOB GROWTH RATE*

11%

TOP CYBERSECURITY CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certification Authorization Professional (CAP)
- System Security Certified Practitioner (SSCP)
- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- A+ Continuing Education
- Security+ Continuing Education
- CompTIA Advanced Security Practitioner (CASP)
- GIAC Certified Incident Handler (GCIH)
- Network+ Continuing Education
- CyberSec First Responder (CFR)
- Certified Ethical Hacker (CEH)
- Certified Chief Information Security Officer (CCISO)
- Computer Hacking Forensics Investigator (CHFI)
- Cisco Certified Network Associate-Security (CCNA-Security)
- Cybersecurity Specialty Certification (SCYBER)
- Certified Information Privacy Professional (CIPP)

*Information on key job functions, top skills, degree requirement, median salary, and job growth provided by O*Net OnLine, Glassdoor.com, and Google Jobs.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.