MISSION: The mission is three-fold: 1) Identify key skill sets within cybersecurity fields that are fundamental to providing an enhanced cyber posture at the State, Local, Tribal, and Territorial (SLTT) level; 2) Find and evaluate professional standards and job descriptions that match identified key skill sets to standardize across SLTT entities; 3) Identify training and educational programs for these key areas.

SYNOPSIS: It is difficult to train and retain qualified cybersecurity professionals at the SLTT level. This is partially due to fierce competition for these jobs. It is estimated that in the United States, there is a need for 500,000 cybersecurity professionals in the workforce. Socializing a standardized list of training opportunities will help to identify skill sets and train individuals within these positions. Due to a shortage of cyber professionals, organizations providing higher salaries and incentives often get the most qualified individuals. Once an individual is trained and certified, SLTT's often lose their home grown talent to the higher paying private sector.

In previous years, the Council agreed to work with the States to establish cybersecurity professional standards. This includes identifying SLTT cyber resources that are available within each State. This is a continuation of that effort. Without established training standards there is room for ambiguity about the skill sets needed by SLTT's for improved cybersecurity posture. Included is a list of positions we advocate SLTT's to adopt, along with the educational institutions that offer training to support them.

AUTHORS: This is a joint project created by the Wyoming Military Department, States of Wyoming and Louisiana, with support from the Governors Homeland Security Offices, National Emergency Management Association (NEMA), Cybersecurity and Infrastructure Security Agency (CISA), Defense Information Systems Agency (DISA), National Association of State Chief Information Officers (NASCIO), National Conference of State Legislature (NCSL) and Federal Emergency Management Agency (FEMA).

SOURCES:

1. National Initiative for Cybersecurity Careers and Studies (NICCS); "Cyber Career Pathways Tool"
2. National Initiative for Cybersecurity Education (NICE)
3. NSA National Centers of Academic Excellence (nsa.gov)
4. DHS Cyber Talent Management System: DHS Cybersecurity Service | Homeland Security
5. Cyber Seek; "Career Pathway"
6. DoD Cyber Exchange Public; "Baseline Certifications"
7. NIST Special Publication 800-181 Rev 1
8. SANS
9. GIAC
10. ISACA
11. ISC2
12. CompTIA
13. DoD 8570.1m

Mission 1:

Identify key skill sets within cybersecurity fields that are fundamental to providing an enhanced cyber posture at the State, Local, Tribal, and Territorial (SLTT) level

Key Positions in Cybersecurity Fields

JOB TITLE(s)	DESCRIPTION
IT Support, Help Desk, Service Branch	Help desk or services branch employees are typically the first line of defense and notification of cybersecurity incidents. A well trained and proficient help desk is critical to cyber response
Network Administrator	Network administration provides base level cybersecurity functions such as firewalls, port security, and hardware authentication
System Administrator	System administration provides base level cybersecurity functions such as user authentication, patching, and system level permissions
Application Developer	Not all organizations develop their own applications, but if they do trained and certified developers are essential in order to not program in vulnerabilities to the environment
Information Security Administrator	Coordination of cybersecurity efforts, subject matter expert, and incident response manager

Defensive Cyber Operations Elements are Army National Guard resources available to all 54 States, territories, and the District of Columbia. DCOE's provide uniquely trained incident response and audit capabilities to SLTT's through collaboration with their local agencies, fusion centers, etc.

Military Occupational Specialty (MOS)	Rank	DCOE Duty Title	DCOE Role per DoD 8570.01-M	EDUCATIONAL INSTITUTIONS
FA 26/30 or 17/25A	**Major/ Lieutenant Colonel**	DCOE Team Chief	Computer Network Defense (CND)- Service Provider (SP) Manager	A mix between military training and civilian education through organizations such as SANS, which provide GIAC certifications.
FA26/30 or 17/25A	**First Lieutenant/ Captain**	Deputy Team Chief	CND-SP Manager	
255A or 170A	**Chief Warrant Officer 2-4**	Senior Information Services Technician	CND-Incident Responder (IR)/Auditor(AU)	
255S or 170A	**Chief Warrant Officer 2-4**	Information Protection Technician	CND-IR	
25B40 or 17C	**Sergeant First Class**	Senior Information Systems Technical Specialist	CND-IR / CND-AU	
25B30 or 17C	**Staff Sergeant**	Information Systems Technician Specialist	CND-IR	
25D30 or 17C	**Staff Sergeant**	Information Systems Technician Specialist	CND-Infrastructure Support(IS)	
25B20 or 17C	**Sergeant**	Information Systems Technician Specialist	CND-IS	
350F or 351L	**Chief Warrant Officer 2**	Computer Network Defense Analysts	CND-Analyst	
350F or 351L	**Chief Warrant Officer 2-4**	Computer Network Defense Analysts	CND-Analyst	

Cyber Protection Teams (CPT) are also a resource some states have access to. CPT's have 39 positions and more capabilities than a DCOE team. There are a total of 10 CPT's throughout the country.
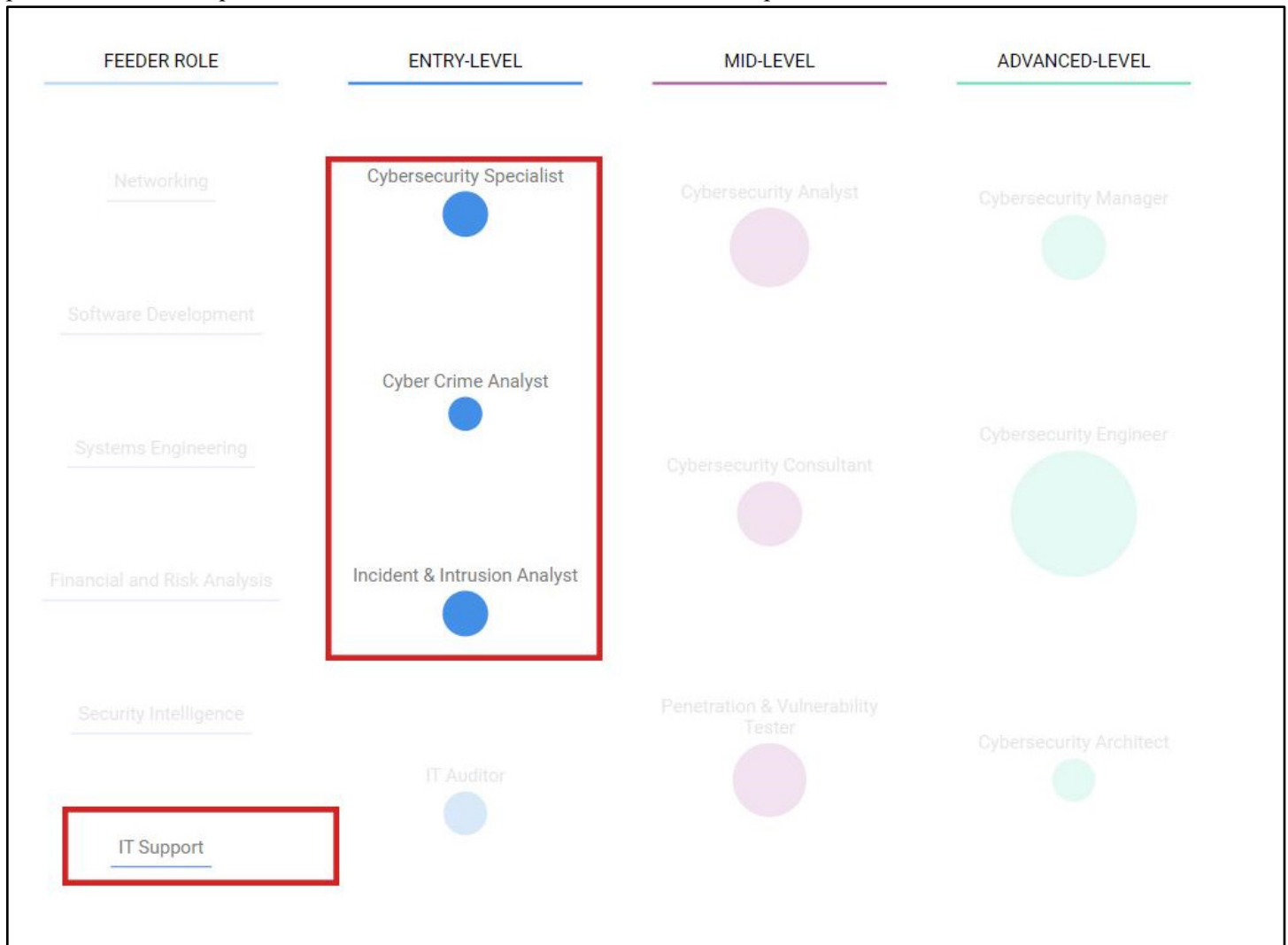
Mission 2:
Find and evaluate professional standards and job descriptions that match identified key skill sets to standardize across SLTT entities

IT Support, Help Desk, Service Branch

Description: Help desk or services branch employees are typically the first line of defense and notification of cybersecurity incidents. A well trained and proficient help desk is critical to cyber response.

Common Job Titles: Help Desk Technician, IT Support Specialist, Desktop Support Technician

Career Pathway: IT Support, Help Desk, and Service Branch roles are typically entry-level. After acquiring entry-level positions, mid-level positions can be achieved but are associated with a specific area of interest.

(n.d.). ©Cyber Seek. Cybersecurity Career Pathway. https://www.cyberseek.org/pathway.html

Career Focus: IT Support, Help Desk, Service

Role: Cybersecurity Specialist

Entry-Level Role

Common Job Titles:
- Information Security Specialist
- Security Specialist
- Cyber Security Specialist
- Information Technology Specialist
- Operations Specialist

Common Job Skills:
- Network security
- Vulnerability assessment
- Project management
- Information security
- Threat hunting

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- SANS/GIAC Certification (Various)
- CompTIA Security+
- Information Systems Certification
- IT Infrastructure Library (ITIL) Certification

$104,000*   *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: IT Support, Help Desk, Service

Role: Cyber Crime Analyst

Entry-Level Role

Common Job Titles:
- Security Analyst
- Information Security Analyst
- Network Analyst
- Security Engineer
- Cyber Defense Forensics Analyst

Common Job Skills:
- Information systems
- Threat hunting
- Network firewalls
- Anomaly detection

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- EnCase Certified Examiner (EnCE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Forensic Analyst
- Certified Information Privacy Professional (CIPP)
- GIAC Certified Forensic Examiner

$100,000*   *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: IT Support, Help Desk, Service

Role: Incident and Intrusion Analyst

Entry-Level Role

Common Job Titles:
- Information Technology Specialist
- Information Security Analyst
- Threat Warning Analyst
- Vulnerability Assessment Analyst
- Security Analyst
- Cyber Defense Incident Responder

Common Job Skills:
- Information systems
- Technical support
- Threat hunting
- Network firewalls
- Anomaly detection

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- GIAC Certified Incident Handler (GCIH)
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification
- IT Infrastructure Library (ITIL) Certification
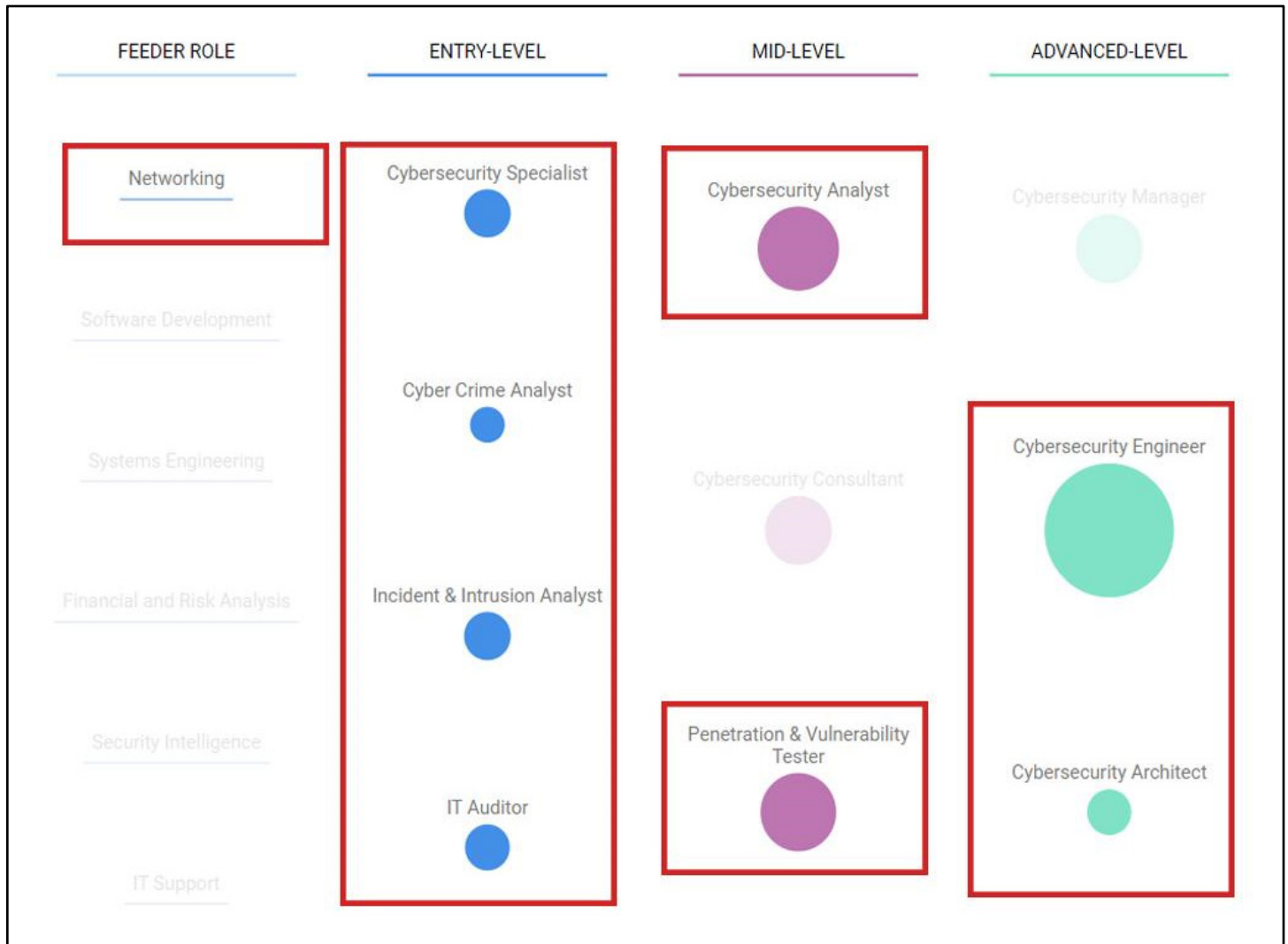
$88,000*   *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Network Administration

Description: Network administrators provide the configuration of core infrastructure, the management and essential functions such as ensuring reliable network connectivity, managing firewalls, port security, and hardware authentication

Common Job Titles: Network Engineer, Systems Administrator, Network Administrator, Senior Systems Administrator

Career Pathway: Cybersecurity careers with a focus on Networking can include Cybersecurity Specialist, Cyber Crime Analyst, Incident & Intrusion Analyst, IT Auditor, Cybersecurity Analyst, Penetration & Vulnerability Tester, Cybersecurity Engineer, and Cybersecurity Architect.

(n.d.). ©Cyber Seek. Cybersecurity Career Pathway. https://www.cyberseek.org/pathway.html

Career Focus: Network Administration

Role: *Cybersecurity Specialist*

Entry-Level Role

Common Job Titles:
- Information Security Specialist
- Security Specialist
- Cyber Security Specialist
- Information Technology Specialist
- Operations Specialist

Common Job Skills:
- Network security
- Vulnerability assessment
- Project management
- Information security
- Threat hunting

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- SANS/GIAC Certification (Various)
- CompTIA Security+
- Information Systems Certification
- IT Infrastructure Library (ITIL) Certification

$104,000*   *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Network Administration

Role: Cyber Crime Analyst

Entry-Level Role

Common Job Titles:
- Security Analyst
- Information Security Analyst
- Network Analyst
- Security Engineer
- Cyber Defense Forensics Analyst

Common Job Skills:
- Information systems
- Threat hunting
- Network firewalls
- Anomaly detection

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- EnCase Certified Examiner (EnCE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Forensic Analyst
- Certified Information Privacy Professional (CIPP)
- GIAC Certified Forensic Examiner

$100,000*   *average salary according to cyberseek.org

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Network Administration

Role: Incident & Intrusion Analyst

Entry-Level Role

Common Job Titles:
- Information Technology Specialist
- Information Security Analyst
- Threat Warning Analyst
- Vulnerability Assessment Analyst
- Security Analyst
- Cyber Defense Incident Responder

Common Job Skills:
- Information systems
- Technical support
- Threat hunting
- Network firewalls
- Anomaly detection

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- GIAC Certified Incident Handler (GCIH)
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification
- IT Infrastructure Library (ITIL) Certification

$88,000*   *average salary according to cyberseek.org

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Network Administration

Role: IT Auditor

Entry-Level Role

Common Job Titles:
- Information Technology Auditor
- Information Technology Manager
- Information Technology Analyst
- Security Control Assessor
- Cyber Policy and Strategy Planner

Common Job Skills:
- Information systems
- Security roles and user privileges
- User security management
- Risk assessment
- Internal auditing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Auditor (CISA)
- Information Systems Certification
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification

$110,000*   *average salary according to cyberseek.org

Mid-level careers may be Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Network Administration

Role: Cybersecurity Analyst

Mid-Level Role

Common Job Titles:
- Security Analyst
- Information Security Analyst
- Systems Security Analyst
- Compliance Analyst
- Cyber Defense Incident Responder
- Exploitation Analyst

Common Job Skills:
- Information systems
- Vulnerability assessment
- Intrusion detection
- Risk assessment
- Network security

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Information Security Manager (CISM)

$107,000*   *average salary according to cyberseek.org*

Advanced-level careers may be Cybersecurity Manager, Cybersecurity Engineer, Cybersecurity Architect

Career Focus: Network Administration

Role: Penetration & Vulnerability Tester

Mid-Level Role

Common Job Titles:
- Security Analyst
- Security Engineer
- Information Security Analyst
- Systems Engineer
- Information Security Engineer

Common Job Skills:
- Information security
- Vulnerability assessment
- Software development
- Penetration testing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Ethical Hacker (CEH)

$101,000*   *average salary according to cyberseek.org

Advanced-level careers may be Cybersecurity Engineer, Cybersecurity Architect

Career Focus: Network Administration

Role: Cybersecurity Engineer

Advanced-Level Role

Common Job Titles:
- Security Engineer
- Cyber Security Engineer
- Information Security Engineer
- Network Security Engineer
- Systems Security Engineer

Common Job Skills:
- Information security
- Vulnerability assessment
- Software development
- Penetration testing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Security Manager (CISM)
- CompTIA Security+
- Certified Information Systems Auditor (CISA)

$117,000*   *average salary according to cyberseek.org*

Career Focus: Network Administration

Role: Cybersecurity Architect

Advanced-Level Role

Common Job Titles:
- Security Architect
- Information Security Architect
- Solutions Architect
- Security Engineer
- Applications Architect

Common Job Skills:
- Information security
- Network security
- Cryptography
- Container / Cloud security

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- IT Infrastructure Library (ITIL) Certification

$159,000*   *average salary according to cyberseek.org*

Application Development

Description: Certified software developers are essential to create custom programs, modify existing applications, or create connectors across applications using secure practices.

Common Job Titles: Java Developer, Software Developer, DevOps Engineer, .Net Developer, Applications Developer

Career Pathway: Cybersecurity careers with a focus on Application Development begin at mid-level positions and can include Cybersecurity Analyst, Penetration & Vulnerability Tester, Cybersecurity Engineer, and Cybersecurity Architect.

(n.d.). ©Cyber Seek. Cybersecurity Career Pathway. https://www.cyberseek.org/pathway.html

Career Focus: Application Development

Role: Cybersecurity Analyst

Mid-Level Role

Common Job Titles:
- Target Developer
- Exploitation Analyst
- Systems Testing and Evaluation Specialist
- Compliance Analyst
- Security Analyst
- Information Security Analyst

Common Job Skills:
- Linux
- Python
- Cryptography
- Information systems
- Vulnerability assessment
- Software development
- Risk assessment

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Information Security Manager (CISM)

$107,000*   *average salary according to cyberseek.org*

Advanced-level careers may be Cybersecurity Manager, Cybersecurity Engineer, Cybersecurity Architect

Career Focus: Application Development

Role: Penetration & Vulnerability Tester

Mid-Level Role

Common Job Titles:
- Security Analyst
- Target Developer
- Security Engineer
- Information Security Analyst
- Secure Software Assessor
- Information Security Engineer

Common Job Skills:
- Linux
- Python
- Java
- Vulnerability assessment
- Software development
- Penetration testing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Ethical Hacker (CEH)

$101,000*   *average salary according to cyberseek.org*

Advanced-level careers may be Cybersecurity Engineer, Cybersecurity Architect

Career Focus: Application Development

Role: Cybersecurity Engineer

Advanced-Level Role

Common Job Titles:
- Systems Developer
- Cyber Defense Analyst
- Threat Warning Analyst
- Security Control Assessor
- Information Systems Security Developer

Common Job Skills:
- Linux
- Python
- Cryptography
- Information security
- Vulnerability assessment
- Software development
- Penetration testing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Security Manager (CISM)
- CompTIA Security+
- Certified Information Systems Auditor (CISA)

$117,000* *average salary according to cyberseek.org*

Career Focus: Application Development

Role: Cybersecurity Architect

Advanced-Level Role

Common Job Titles:
- Security Architect
- Information Security Architect
- Information Systems Security Developer
- Solutions Architect
- Security Engineer
- Applications Architect

Common Job Skills:
- Linux
- Python
- Cryptography
- Information security
- Network security
- Container / Cloud security
- Cybersecurity frameworks

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
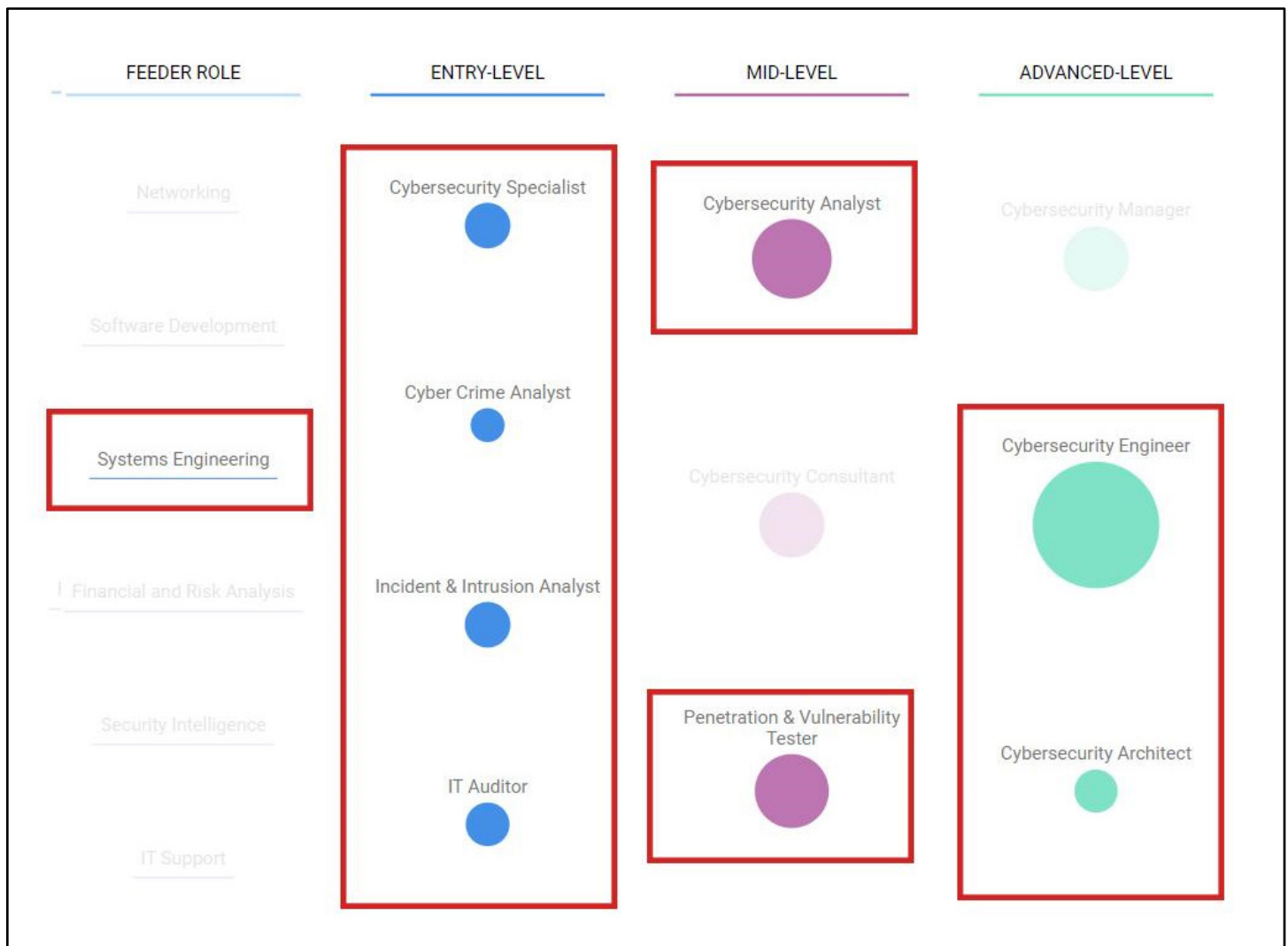- IT Infrastructure Library (ITIL) Certification

$159,000*   *average salary according to cyberseek.org

Systems Administration

Description: Systems Administrators are responsible for the maintenance, configuration, and operation of the hardware and software in an organization. This includes the configuration and maintenance of user workstations, servers, and other essential services in the organization.

Common Job Titles: Systems Administrator, Systems Engineer, IT Manager, Data Center Administrator

Career Pathway: Cybersecurity careers with a focus on Systems Administration can include Cybersecurity Specialist, Cyber Crime Analyst, Incident & Intrusion Analyst, IT Auditor, Cybersecurity Analyst, Penetration & Vulnerability Tester, Cybersecurity Engineer, and Cybersecurity Architect.

(n.d.). ©Cyber Seek. Cybersecurity Career Pathway. https://www.cyberseek.org/pathway.html

Career Focus: Systems Administration

Role: Cybersecurity Specialist

Entry-Level Role

Common Job Titles:
- Information Security Specialist
- Security Specialist
- Cyber Security Specialist
- Information Technology Specialist
- Operations Specialist

Common Job Skills:
- Network security
- Vulnerability assessment
- Project management
- Information security
- Threat hunting

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- SANS/GIAC Certification (Various)
- CompTIA Security+
- Information Systems Certification
- IT Infrastructure Library (ITIL) Certification

$104,000* *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Systems Administration

Role: Cyber Crime Analyst

Entry-Level Role

Common Job Titles:
- Security Analyst
- Information Security Analyst
- Network Analyst
- Security Engineer
- Cyber Defense Forensics Analyst

Common Job Skills:
- Information systems
- Threat hunting
- Network firewalls
- Anomaly detection

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- EnCase Certified Examiner (EnCE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Forensic Analyst
- Certified Information Privacy Professional (CIPP)
- GIAC Certified Forensic Examiner

$100,000*   *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Systems Administration

Role: Incident & Intrusion Analyst

Entry-Level Role

Common Job Titles:
- Information Technology Specialist
- Information Security Analyst
- Threat Warning Analyst
- Vulnerability Assessment Analyst
- Security Analyst
- Cyber Defense Incident Responder

Common Job Skills:
- Information systems
- Technical support
- Threat hunting
- Network firewalls
- Anomaly detection

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- GIAC Certified Incident Handler (GCIH)
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification
- IT Infrastructure Library (ITIL) Certification

$88,000*   *average salary according to cyberseek.org*

Mid-level careers may be Cybersecurity Analyst, Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Systems Administration

Role: IT Auditor

Entry-Level Role

Common Job Titles:
- Information Technology Auditor
- Information Technology Manager
- Information Technology Analyst
- Security Control Assessor
- Cyber Policy and Strategy Planner

Common Job Skills:
- Information systems
- Security roles and user privileges
- User security management
- Risk assessment
- Internal auditing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Auditor (CISA)
- Information Systems Certification
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification

$110,000*   *average salary according to cyberseek.org

Mid-level careers may be Cybersecurity Consultant, Penetration and Vulnerability Tester

Career Focus: Systems Administration

Role: Cybersecurity Analyst

Mid-Level Role

Common Job Titles:
- Security Analyst
- Information Security Analyst
- Systems Security Analyst
- Compliance Analyst
- Cyber Defense Incident Responder
- Exploitation Analyst

Common Job Skills:
- Information systems
- Vulnerability assessment
- Intrusion detection
- Risk assessment
- Network security

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Information Security Manager (CISM)

$107,000*   *average salary according to cyberseek.org

Advanced-level careers may be Cybersecurity Manager, Cybersecurity Engineer, Cybersecurity Architect

Career Focus: Systems Administration

Role: Penetration & Vulnerability Tester

Mid-Level Role

Common Job Titles:
- Security Analyst
- Security Engineer
- Information Security Analyst
- Systems Engineer
- Information Security Engineer

Common Job Skills:
- Information security
- Vulnerability assessment
- Software development
- Penetration testing

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Ethical Hacker (CEH)

$101,000*   *average salary according to cyberseek.org*

Advanced-level careers may be Cybersecurity Engineer, Cybersecurity Architect

Career Focus: Systems Administration

Role: Cybersecurity Engineer

Advanced-Level Role

Common Job Titles:
- Security Engineer
- Cyber Security Engineer
- Information Security Engineer
- Network Security Engineer
- Systems Security Engineer

Common Job Skills:
- Information security
- Vulnerability assessment
- Software development
- Penetration testing

Educational Requirements:

Recommended Educational Requirements:

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Security Manager (CISM)
- CompTIA Security+
- Certified Information Systems Auditor (CISA)

$117,000*   *average salary according to cyberseek.org*

Career Focus: Systems Administration

Role: Cybersecurity Architect

Advanced-Level Role

Common Job Titles:
- Security Architect
- Information Security Architect
- Solutions Architect
- Security Engineer
- Applications Architect

Common Job Skills:
- Information security
- Network security
- Cryptography
- Container / Cloud security

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- IT Infrastructure Library (ITIL) Certification

$159,000*   *average salary according to cyberseek.org*

Information Security Administration

Description: Information Security Administrators are responsible for implementing security procedures, policies, and response plans for an organization. Commonly they implement and administer an organization's security systems and oversee the security of all IT related issues.

Common Job Titles: Information Security Officer, Security Manager, Cybersecurity Manager

Career Pathway: Various fields within Cybersecurity can move into the advanced-level Information Security Administrator Role

(n.d.). ©Cyber Seek. Cybersecurity Career Pathway. https://www.cyberseek.org/pathway.html

Career Focus: Information Security Administration

Role: Cybersecurity Manager

Advanced-Level Role

Common Job Titles:
- Security Manager
- Information Systems Security Officer
- Information Security Manager
- Security Administrator
- Information Security Officer

Common Job Skills:
- Information security
- Network security
- Cybersecurity and risk management framework
- Security control and evaluations
- Cyber defense response
- Vulnerability assessment

Recommended Educational Requirements:

Bachelor's Degree

Professional certifications
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- CompTIA Security+
- Certified Information Systems Auditor (CISA)
- SANS/GIAC Certification (Various)

$130,000*   *average salary according to cyberseek.org*

Mission 3:
Identify training and educational programs for these key areas.

Below is a list of some of the widely accepted industry training mentioned throughout this document that provides a certification. There are many others that have not been covered in this document that may provide similar training.

Provider / Average Certificate or Course Cost	Entry Level	Mid Level	Advanced Level
GIAC / $4000-$9000	GCIH/GSEC	GNFA/GCIA/GAWN	GCPM/GWEB/GREM
ISACA / $760	CISA	CRISC	CISM
COMPTIA / $392	Security+, A+	Network+, Linux+, Server+	Cloud+, CASP+, PenTest+
ISC^2 / $750	CASP, SSCP, CAP	CISSP, CAP, CCSP	CISSP-Concentrations
EC-Council / $1200	CEH	CNDA	ECSA
Offensive Security / $2500			OSCP
Multiple Vendor Specific Certifications			

With the growing demand for training in cybersecurity jobs, many universities and colleges now offer specific degree programs. Some of these institutions also have an internship program that allow students to gain valuable on the job experience with an entity that performs cybersecurity functions related to their studies. These opportunities vary state to state and are too numerous to list out here. Often the intern will seek full-time employment with the organization they have worked with after graduation. SLTT's could benefit by supporting these intern programs with their local universities and colleges.

Despite the high cost of some certifications or courses, there are potentially free resources available to assist in preparing for some of these courses. One resource that is free to SLTT's is FedVTE (Federal Virtual Training Environment) https://fedvte.usalearning.gov. This has various IT and cyber classes available to build capacity for a cybersecurity workforce. Another low-cost option for training is LinkedIn Learning at https://www.linkedin.com/learning. LinkedIn Learning allows you to use your library card from participating local libraries to log in for free to this resource. There are many more options available but, we wanted to focus on some that could be provided at low to no cost to SLTT's.