Day 4 - Cybersecurity Roles & Career Paths

Domains of Cybersecurity:

- **Offensive Security (Red Team):** Ethical hackers who find vulnerabilities.

- **Defensive Security (Blue Team):** Defend against attacks (SOC, IR, etc.).

- **Governance, Risk, Compliance (GRC):** Policy, audits, and compliance.

- **Security Engineering:** Build secure systems & architecture.

- **Cloud Security, AppSec, Threat Intel, etc.** — more specialized tracks.

Popular roles in Cybersecurity:

Role	Description
SOC Analyst (Blue)	Monitor logs, detect and report threats. Entry-level.
Penetration Tester (Red)	Ethical hacker who tests systems for vulnerabilities.
Security researcher	Finds new attack vectors or malware. Deep knowledge.

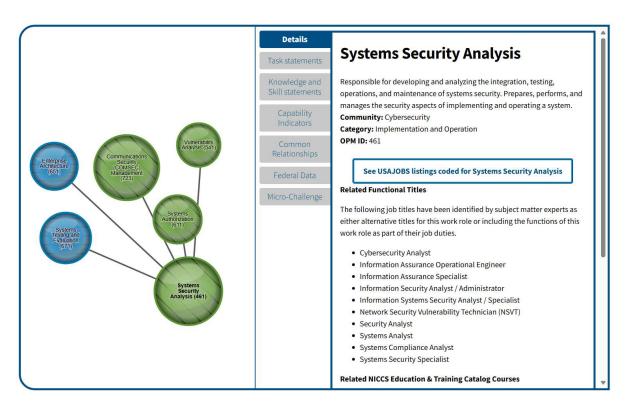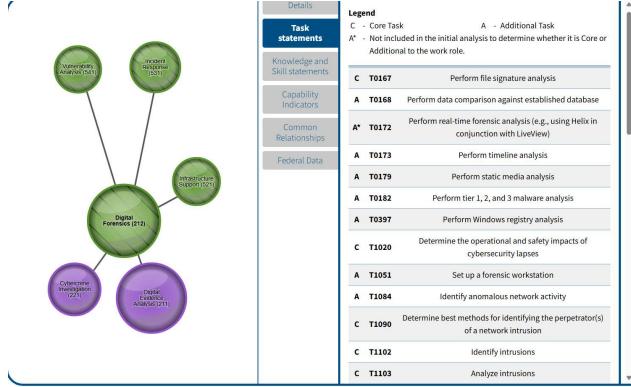|	
GRC Analyst	Ensures security rules and compliance standards are followed.
Security Engineer	Builds secure systems, tools, and processes.
Threat Intelligence Analyst	Tracks threat actors and upcoming cybercrime trends.

Cyber Career Pathways Tool | NICCS

Systems Security Analysis

Details

Task statements

Knowledge and Skill statements

Capability Indicators

Common Relationships

Federal Data

Micro-Challenge

Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system.
Community: Cybersecurity
Category: Implementation and Operation
OPM ID: 461

See USAJOBS listings coded for Systems Security Analysis

Related Functional Titles

The following job titles have been identified by subject matter experts as either alternative titles for this work role or including the functions of this work role as part of their job duties.

- Cybersecurity Analyst
- Information Assurance Operational Engineer
- Information Assurance Specialist
- Information Security Analyst / Administrator
- Information Systems Security Analyst / Specialist
- Network Security Vulnerability Technician (NSVT)
- Security Analyst
- Systems Analyst
- Systems Compliance Analyst
- Systems Security Specialist

Related NICCS Education & Training Catalog Courses

Details

Task statements

Knowledge and Skill statements

Capability Indicators

Common Relationships

Federal Data

Legend
C - Core Task   A - Additional Task
A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

C	T0167	Perform file signature analysis
A	T0168	Perform data comparison against established database
A*	T0172	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView)
A	T0173	Perform timeline analysis
A	T0179	Perform static media analysis
A	T0182	Perform tier 1, 2, and 3 malware analysis
A	T0397	Perform Windows registry analysis
C	T1020	Determine the operational and safety impacts of cybersecurity lapses
A	T1051	Set up a forensic workstation
A	T1084	Identify anomalous network activity
C	T1090	Determine best methods for identifying the perpetrator(s) of a network intrusion
C	T1102	Identify intrusions
C	T1103	Analyze intrusions