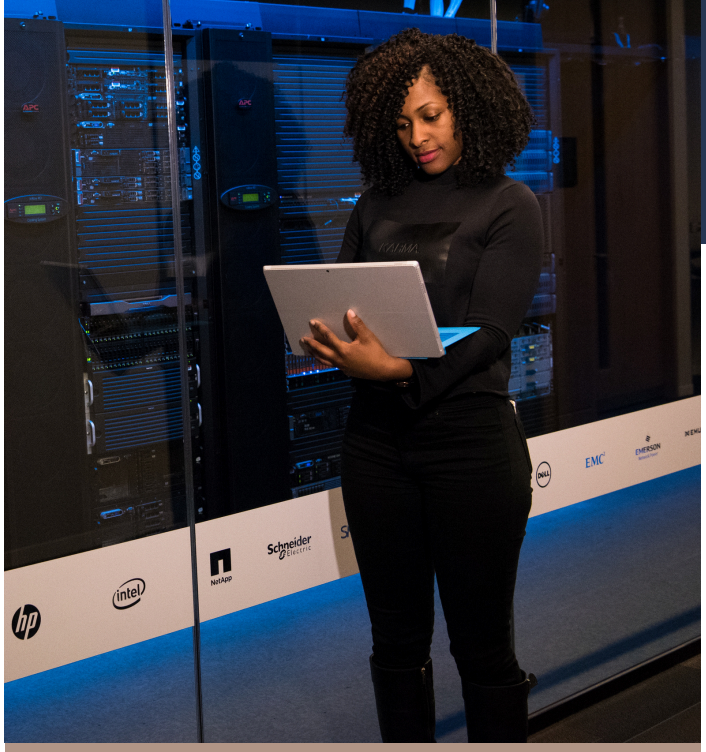

SCS STATE CYBERSECURITY OFFICE

CYBER CENTER OF EXCELLENCE

Cybersecurity Practitioner

FOCUSED LEARNING PATH

self-paced training
in-person training

Role Description

A Cybersecurity Practitioner strengthens an organization's cyber maturity by developing practical, adaptable skills that support multiple areas of security. This pathway is ideal for individuals in smaller environments where IT staff manage diverse responsibilities, or for those seeking a holistic understanding of cybersecurity without committing to a specialized role.

Practitioners build foundational knowledge across monitoring, governance, risk management, threat defense, and incident response. Through hands-on learning and real-world application, they gain the ability to identify vulnerabilities, implement protective measures, and support consistent security operations. As learners progress, they develop the confidence and experience needed to support more mature cybersecurity functions and serve as reliable security resources within their organizations. Ultimately, practitioners help establish consistent security practices, reduce organizational risk, and contribute to a stronger statewide security posture.

For support in accessing hands-on training opportunities or coordinating practical experience related to this development path, individuals or supervisors may reach out to Raymond.Girdler@arkansas.gov.

Phase 1: Cybersecurity Foundations

Training Options (choose one)

- Cisco NetAcad Junior Cybersecurity Analyst (120 hours)
- Grow with Google: Google Cybersecurity (133 hours)

Practical Skill Development

Aligned to NICE Framework Technical Support

- Gain exposure to the MITRE ATT&CK framework and common attack vectors (phishing, credential theft, misconfigurations).
- Gain introductory exposure to security frameworks such as NIST CSF and CIS Controls.
- Establish baselines for system configuration, Windows logs, authentication activity, and network traffic.
- Participate in the review, triage, and mitigation of cybersecurity alerts.
- Create or refine a cybersecurity-focused asset inventory to understand what you are protecting.
- Learn basic identity and access management concepts (least privilege, MFA, account lifecycle).
- Develop a business-focused, risk-aware mindset.
- Build strong operational habits by documenting cybersecurity processes and creating operational checklists.

CYBER CENTER OF EXCELLENCE

SCS STATE CYBERSECURITY OFFICE

Phase 2: Operational Defense

Training Options

- NCPC Comprehensive Cybersecurity Defense (32 hours) 🤝
- Introduction to the MITRE D3FEND Matrix
- NIST Risk Management Framework Online Introductory Courses (6 hours) ⏱️

Practical Skill Development

*Aligned to TKS **defender** subset of NICE Framework Systems Security Analysis*

- Engage in hands-on digital incident response simulations or cyber range exercises to practice detection, analysis, containment, and recovery.
- Expand understanding beyond your primary domain to support cross-functional operations.
- Support external audits by assisting with evidence collection and gaining exposure to audit procedures.
- Begin reviewing alerts from InfraGard, FBI, MS-ISAC, and other threat intelligence sources.
- Strengthen log analysis skills by identifying anomalies and validating potential incidents.
- Help refine or establish baseline security configurations for systems, applications, and user access.
- Assist in documenting incident response steps and lessons learned.
- Participate in patch and vulnerability management activities.
- Shadow or assist with change management processes to understand how changes impact security.

Optional Learning Develoment

- Security Operations Analyst Associate (SC-200) (40 hours) ⏱️
- Cisco NetAcad Cybersecurity Defense Analyst (30 hours) ⏱️

Phase 3: Proactive Defense

Training Options

- NCPC Cybersecurity Proactive Defense (32 hours) 🤝
- NCPC Cybersecurity First Responder (32 hours) 🤝
- MITRE ATT&CK Cyber Threat Intelligence (CTI) Training ⏱️

Practical Skill Development

*Aligned to TKS **threat hunter** subset of NICE Framework Systems Security Analysis*

- Create or refine an incident response plan.
- Participate in tabletop exercises to strengthen incident coordination and communication.
- Proactively scan and assess your environment to identify vulnerabilities and misconfigurations.
- Perform threat modeling to anticipate attacker behavior.
- Adopt an attacker-informed mindset to harden systems before issues arise (defensive hardening, not penetration testing).
- Establish or support a cybersecurity training and awareness program, including role-based training and phishing campaigns.
- Participate in the cybersecurity community by attending events, sharing lessons learned, and building a resource network.
- Integrate a risk-based approach into organizational processes and business decisions.
- Develop procedures, playbooks, and repeatable workflows to support consistent operations.
- Monitor baselines to identify configuration drift or anomalies.
- Conduct periodic access reviews to prevent privilege creep.
- Gain exposure to vendor, third-party, and supply chain risk considerations.
- Apply continuous improvement practices to strengthen security posture and capability maturity over time.

Optional Learning Develoment

- Identity and Access Administrator Associate (SC-300) (15 hours) ⏱️
- Cisco NetAcad Ethical Hacker (70 hours) ⏱️
- Review CIS Benchmarks List for system hardening and baseline development.
- Review CISA's Secure Cloud Business Applications (SCuBA) guidance for Microsoft 365 and Google Workspace secure configuration baselines.