



CAREER PROGRAM OCCUPATION PROFILE:

CYBERSECURITY ASSOCIATE

The Cybersecurity Associate career training program prepares adults to help keep a company's technology safe — from user accounts and devices to networks and cloud systems. Trainees learn to monitor security alerts, investigate potential threats, and follow established response procedures under supervision. Working alongside IT and business teams, they help protect company systems and data by spotting vulnerabilities, documenting issues, and supporting ongoing improvements to security practices.

This occupation is ideal for someone who:

- Enjoys investigating problems and figuring out what went wrong.
- Is detail-oriented and likes following structured processes to find answers.
- Sees themselves in a role that combines technical analysis, clear communication, and hands-on security work.

Do trainees pay a fee to participate?

No, trainees are not required to pay anything to participate.

How much do trainees earn while they're completing the program?

While compensation varies by industry, organization size, and the full scope of the role, trainees can expect pay in the range of **\$17-25/hour** during the program. Trainees are employees and fall under their employer's policies for paid time off, benefits, performance reviews, and salary increases.

What do trainees do as an Cybersecurity Associate?

- **Alert monitoring and triage:** Monitor, triage, and document security alerts using standardized workflows and decision criteria; prioritize work based on severity, confidence, and business impact.
- **Investigation:** Perform initial investigations by correlating identity, endpoint, and network evidence into timelines; identify common threats and attack patterns such as phishing, malware, and credential theft.
- **Response and containment:** Execute approved response actions (contain, block, reset, isolate, revoke) following playbooks and escalation rules.
- **Vulnerability and remediation:** Support vulnerability remediation tracking and validation of fixes in collaboration with IT teams; document exceptions and risk acceptance.
- **Documentation, reporting, and security:** Maintain accurate tickets, evidence, and concise summaries for escalation and reporting; contribute to runbooks, detection tuning recommendations, and process improvements; follow security best practices including access controls, data handling, and safe use of AI tools.

All work is performed under supervision, with increasing independence over time.

TYPICAL SCHEDULE

Training program length

Two years of full-time paid learning, split between on-the-job experience with an employer and specialized instruction at an intercompany training center.

Typical week

Months 1–3:

Foundations and safe exposure

- 3 days/week at the training center (labs + simulations)
- 2 days/week at the employer (shadow + controlled tasks)

Months 4–6:

Supervised ownership of day-to-day tasks

- 2 days/week at the training center
- 3 days/week at the employer

Months 7–12:

Productive throughput and applied learning

- 1 day/week at the training center
- 4 days/week at the employer

Months 13–18:

Deeper investigations and impact

- Half day/week at the training center
- 4.5 days/week at the employer

Months 19–24:

Associate-level work and capstone portfolio

- All time spent at employer with exception of 1 day/month at the training center

What are some of the skills trainees learn on the job?

- Security foundations and communication
- Identity, endpoint, and access protection
- Network, cloud, and data security
- Monitor, response, and continuous improvement
- Applied AI for detection, triage, and reporting

What prior education or experience should trainees have before starting the program?

While not required, there are several prerequisite and bridge learning opportunities that provide a strong foundation for success. Prior to or alongside their training program, adults are encouraged to complete self-paced online courses in IT fundamentals and cybersecurity basics to accelerate their readiness. Examples include:

- Foundational courses
 - Information technology fundamentals
 - Digital applications and responsibility
 - Networking fundamentals
- Core IT support courses
 - IT support
 - Computer hardware and operating systems
 - IT essentials/help desk operations
- Advanced/related courses
 - Cybersecurity fundamentals
 - Cloud and virtualization concepts
 - Project management

What credential does a trainee receive when they complete the program?

Trainees earn an INCAP credential that will be recognized by TechIndiana and technology-related companies across Indiana as equivalent to an academic associate degree in an IT- or technology-related degree program. They also may receive college credit toward a related degree program.

Opportunities are also available to earn stackable industry certifications during the program, including ISC2 Certified in Cybersecurity (CC), CompTIA Security+, and Microsoft Security, Compliance, and Identity Fundamentals (SC-900).

What career opportunities are available after completing the program?

This program prepares a trainee to move into junior roles that support security operations and IT infrastructure, including:

- Security Analyst
- Incident Responder
- Security Operations Center (SOC) Analyst
- Threat Hunter
- Vulnerability Analyst
- Governance, Risk, and Compliance (GRC) Analyst
- Cloud Security Associate
- Network Administrator
- Systems Administrator
- Database Administrator
- IT Project Manager
- Cloud Engineer
- DevOps Engineer

Who should I contact for more information?

TechIndiana is managing INCAP Career Programs for Tech/IT. You can learn more at TechIndiana.org.



IndianaCAP.org

09/15/26

