

Certified Detection Engineering Associate (CDEA) Training

Centri Authorized Training · Applied Technology Academy

Centri's Certified Detection Engineering Associate builds the practical skill of writing detections that work: Sigma and YARA rules, Zeek and network telemetry, SIEM rule creation and tuning, and the Git workflows that keep detection content reviewable and releasable. It closes on behavioural analytics, threat-intelligence integration and where AI genuinely helps a defender. Certification is by practical exam and does not expire. ATA is Centri's exclusive US instructor-led partner.

LEVEL	DURATION	COURSE CODE	DELIVERY
Associate	On-demand · approx. 40 hours	CDEA	Instructor-led

Course Overview

Fifteen modules from networking, Windows, Linux and Python fundamentals through to detection rule creation, tuning and behavioural analytics.

- Built around the work itself — writing rules, testing them, and cutting the noise until what reaches the SOC is worth acting on.
- Treats detection content as code: Git workflows, review and release are part of the syllabus, not an afterthought.
- Certification is a practical exam, and the credential is for life.

Course Outline

- **Module 1. Networking Essentials**
 - The network fundamentals detection work rests on.
- **Module 2. Windows Essentials**
 - Windows internals and the telemetry they produce.
- **Module 3. Linux Essentials**
 - Linux fundamentals, services and logging.
- **Module 4. Python Essentials**
 - Scripting for detection engineering tasks.
- **Module 5. Incident Response Essentials**
 - How detections feed the response process.
- **Module 6. Git Workflows for Detection Engineering**
 - Version control for detection content: branching, review and release.
- **Module 7. Network Analysis Essentials**

- Reading traffic with Wireshark and TCPDump.
- **Module 8. YARA & Sigma Essentials**
 - Writing portable detection rules in both formats.
- **Module 9. Zeek Essentials**
 - Network security monitoring and Zeek logs as a detection source.
- **Module 10. Malware Analysis for Detection Engineering**
 - Extracting detection-worthy behaviour and indicators from samples.
- **Module 11. Detection Rule Creation and Tuning**
 - Building rules, then tuning them down to a signal a SOC can actually work.
- **Module 12. Threat Intelligence Integration for Detection**
 - Turning intelligence into detection content.
- **Module 13. Behavioural Analytics for Threat Detection**
 - Detecting on behaviour rather than static indicators.
- **Module 14. AI for Defenders**
 - Where AI helps detection work, and where it does not.
- **Module 15. CDEA Exam Preparation**
 - Consolidation and practice ahead of the practical exam.

Prerequisites

- Centri recommends one to three years of experience in cybersecurity.
- Comfort with networking, Windows and Linux fundamentals helps, though the course covers each of them.
- No prior detection-engineering experience is assumed.

Follow-On Courses

- Blue Team Level 2 (BTL2)
- Certified Security Operations Manager (CSOM)

Who Should Attend

- SOC analysts moving from consuming detections to writing them.
- Detection engineers and SIEM administrators who want a structured grounding.
- Incident responders and threat intelligence analysts who need their findings to become durable detections.
- Security engineers responsible for detection coverage.

What You'll Learn

By the end of this course, participants will be able to:

- write and test detection rules in Sigma and YARA
- use Zeek and network telemetry as a detection source
- create and tune SIEM rules so that alerting is actionable rather than noisy
- manage detection content through Git workflows with review and release
- extract detection-worthy behaviour and indicators from malware analysis
- turn threat intelligence into working detection content
- apply behavioural analytics where static indicators fall short
- judge where AI assists detection work and where it does not

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.