

Certified Detection Engineering Associate (CDEA)

Formerly Certified Junior Detection Engineer (CJDE)

Proposed instructor-led schedule: 5 days |

Course Overview

Certified Detection Engineering Associate (CDEA), formerly named Certified Junior Detection Engineer (CJDE), develops practical skills for creating, testing, and improving security detections. The provider states that the name change effective 15 September 2026 does not change the course content, hands-on labs, or exam. The published course content covers networking, Windows, Linux, Python, incident response, Git workflows, network analysis, YARA and Sigma, Zeek, malware analysis for detection engineering, rule creation and tuning, threat intelligence integration, behavioural analytics, AI for defenders, and exam preparation. This five-day plan is a suggested instructor-led grouping of those topics.

Day-wise Breakdown

Day 1: Technical Foundations

- Networking essentials
- Windows essentials and endpoint telemetry
- Linux essentials and system activity
- Python essentials for security data and automation
- Incident response essentials and converting findings into detection needs

Day 2: Detection Workflow and Network Analysis

- Git workflows for detection engineering
- Repositories, version control, change tracking, and collaborative review
- Network analysis essentials
- Interpreting network traffic and identifying suspicious activity
- Turning investigative observations into testable detection hypotheses

Day 3: Detection Languages and Network Telemetry

- YARA essentials and file-based detection rules
- Sigma essentials and log-based detection logic
- Rule structure, selection criteria, conditions, and validation
- Zeek essentials and analysis of network telemetry
- Developing and reviewing detections using relevant telemetry

Day 4: Detection Development and Tuning

- Malware analysis for detection engineering
- Extracting behavioural indicators useful for detection
- Detection rule creation and tuning
- Testing detections and reviewing false positives and false negatives
- Detection coverage, documentation, and maintenance

Day 5: Intelligence, Behavioural Analytics, AI, and Exam Preparation

- Threat intelligence integration for detection
- IOC context, enrichment, and operational limitations
- Behavioural analytics for threat detection
- AI for defenders: appropriate uses in detection research and development
- Reviewing and validating AI-assisted outputs
- CDEA exam preparation and course-content review