Certified Junior Detection Engineer (CJDE)

Course Duration: 5 Days
Exam Reference: CJDE

Course Overview

This course provides a pathway into detection engineering and cyber security operations, focusing on identifying, analyzing, and responding to threats using detection tools and strategies. It is ideal for roles such as Junior Security Analysts, Detection Engineers, SIEM Administrators, Incident Response Analysts, and SOC Analysts, and is suited to individuals with foundational cyber security knowledge who wish to specialize in detection and response or enhance their existing skills.

Prerequisites

1-3 Years Security

Course Objectives

- Automate Detection Workflows: Design and implement Git-based automation workflows to manage the continuous deployment, testing, and version control of detection logic.
- Develop Network Detection Rules: Create, test, and tune network detection rules to accurately identify malicious activity and anomalous traffic patterns, minimizing false positives.
- Implement Cross-Platform Rules (Sigma): Construct and refine Sigma rules to enable detection coverage across heterogeneous logging environments (SIEMs), ensuring portability and consistency.
- Integrate AI for Detection: Evaluate and utilize AI and machine learning tools within detection engineering pipelines to enhance threat identification, anomaly analysis, and automate alert triage.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

Certified Junior Detection Engineer (CJDE)

Course Outline

Module 1: Networking Essentials

Module 2: Windows Essentials

Module 3: Python Essentials

Module 4: Incident Response Essentials

Module 5: GIT Workflows for Detection Engineering

Module 6: Network Analysis Essentials

Module 7: Yara and Sigma Essentials

Module 8: Zeek Essentials

Module 9: Malware Analysis for Detection Engineering

Module 10: Detection Rule Creation and Tuning

Module 11: Threat Intelligence Integration for Detection

Module 12: Behavioral Analysis for Threat Detection

Module 13: AI for Defenders