INE

Incident Response: Analysis

Building on the foundations of the previous course, Incident Response: Detection, this course guides you through key analysis phases, including deep-dive investigations, evidence triage, and log analysis. You'll learn how to interpret endpoint and network data, distinguish between live and dead-box analysis, and use tools like Splunk, Wireshark, and EvtxECmd. By mastering techniques for analyzing PCAPs, system logs, and network activity, you'll be equipped to respond confidently to complex incidents and uncover critical forensic insights.

Active

Alexis Ahmed

15h 53m | 21 CPE Credits | Professional | Download files | Resume

Welcome

Jump to category

Overview

Activities: 1

0/1 items finished

Hide details

- Incident Response: Analysis Overview — 5m 59s — Resume video

Incident Analysis

Analysis Primer

Activities: 8

0/8 items finished

- Bridging the Gap: Detection & Analysis — 39m 30s — Resume video
- Test your knowledge: Bridging the Gap: Detection & Analysis — 4 questions — Start quiz
- First Response: The First 5 Minutes — 29m 49s — Resume video
- Test your knowledge: First Response: The First 5 Minutes — 6 questions — Start quiz
- Beyond First Response: Deep Analysis — 53m 6s — Resume video
- Test your knowledge: Beyond First Response: Deep Analysis — 5 questions — Start quiz
- Evidence Triage & Collection — 57m 39s — Resume video
- Test your knowledge: Evidence Triage & Collection — 4 questions — Start quiz

Hide details

Endpoint Analysis

Endpoint Introduction

Activities: 4

0/4 items finished

- Introduction to Endpoint Analysis — 24m 9s — Resume video
- Test your knowledge: Introduction to Endpoint Analysis — 5 questions — Start quiz
- Live Response vs. Dead-Box — 14m 41s — Resume video
- Test your knowledge: Live Response vs. Dead-Box — 5 questions — Start quiz

Hide details

Log Analysis

Activities: 8

0/8 items finished

- Introduction to Log Analysis — 24m — Resume video
- Test your knowledge: Introduction to Log Analysis — 5 questions — Start quiz
- Log Analysis with Splunk: Investigating a Linux Intrusion — 25m 27s — Resume video
- Test your knowledge: Log Analysis with Splunk: Investigating a Linux Intrusion — 4 questions — Start quiz
- Log Analysis — Cyber Security — Start lab
- Log Analysis Using Linux — 35m 18s — Resume video
- Test your knowledge: Log Analysis Using Linux — 5 questions — Start quiz
- Log Analysis Using Linux — Cyber Security — Start lab

Hide details

Windows Event Log Analysis

Activities: 16

0/16 items finished

- Windows Logging Primer: Channels, Providers & Key Logs — 4m 37s — Resume video
- Test your knowledge: Windows Logging Primer: Channels, Providers & Key Logs — 5 questions — Start quiz
- Sysmon Essentials for Incident Responders — 23m 26s — Resume video
- Test your knowledge: Sysmon Essentials for Incident Responders — 6 questions — Start quiz
- Deploying Sysmon for Enhanced Threat Detection — Cyber Security — Start lab
- High-Value Windows Event IDs Every Responder Should Know — 13m 9s — Resume video
- Test your knowledge: High-Value Windows Event IDs Every Responder Should Know — 4 questions — Start quiz
- Exporting Windows Event Logs with wevtutil — 12m 25s — Resume video
- Test your knowledge: Exporting Windows Event Logs with wevtutil — 3 questions — Start quiz
- Parsing Windows Event Logs with EvtxECmd — 6m 47s — Resume video
- Test your knowledge: Parsing Windows Event Logs with EvtxECmd — 4 questions — Start quiz
- Analyzing Windows Event Logs with Timeline Explorer — 34m 50s — Resume video
- Test your knowledge: Analyzing Windows Event Logs with Timeline Explorer — 5 questions — Start quiz
- Windows Log Analysis with Chainsaw & Sigma — 21m 12s — Resume video
- Test your knowledge: Windows Log Analysis with Chainsaw & Sigma — 3 questions — Start quiz
- Windows Event Log Analysis for IR — Cyber Security — Start lab

Hide details

Network Analysis

Network Introduction

Activities: 4

0/4 items finished

- Introduction to Network Analysis In IR — 15m 23s — Resume video
- Test your knowledge: Introduction to Network Analysis In IR — 4 questions — Start quiz
- Network Data Types & Analysis Tools — 9m 57s — Resume video
- Test your knowledge: Network Data Types & Analysis Tools — 5 questions — Start quiz

Hide details

Network Traffic Analysis

Activities: 12

0/12 items finished

- Analyzing PCAPs with Wireshark — 15m 17s — Resume video
- Test your knowledge: Analyzing PCAPs with Wireshark — 4 questions — Start quiz
- Wireshark: Packet Captures Analysis & Files Extraction — Cyber Security — Start lab
- Network File Carving with Wireshark — 18m 19s — Resume video
- Test your knowledge: Network File Carving with Wireshark — 5 questions — Start quiz
- Network File Carving — Cyber Security — Start lab
- Investigating Network Scans — 19m 18s — Resume video
- Test your knowledge: Investigating Network Scans — 4 questions — Start quiz
- Investigating Network Scans — Cyber Security — Start lab
- Investigating Network Attacks — 28m 29s — Resume video
- Test your knowledge: Investigating Network Attacks — 5 questions — Start quiz
- Investigating Network Attacks — Cyber Security — Start lab

Hide details

Goodbye

Summary

Activities: 1

0/1 items finished

- Incident Response: Analysis Summary — 4m 26s — Resume video

Hide details