

Tanium Advanced Threat Response

Course Description

Tanium's Advanced Threat Response training is designed for security incident response practitioners investigating breaches involving lateral movement, fileless attacks using "living off the land" methods, injected code, and data exfiltration. Students will benefit from hands-on experience with Tanium Threat Response including Sensors, host-Level forensic timelines, analysis of acquired files, memory analysis techniques for finding common injection tradecraft, use of intelligence such as Tanium Signals and Indicators of Compromise.

Length

1 Day

Target Audience

This is an advanced course and is recommended for incident response practitioners with a basic understanding of Tanium.

Delivery Options

This instructor-led training course is offered either onsite at your location, or remotely through virtual classrooms. Both delivery options provide valuable knowledge through live instruction and reinforce what is taught with hands-on labs throughout the course.

Topics

01 – Introduction and Threat Response Capability Overview

- Threat Response Capabilities
 - Realtime monitoring and alerting
 - Single-host investigations and forensic data acquisition
 - Enterprise-wide hunting

02 – Threat Response Components

- IR Sensors
- Tanium Recorder
- Live Response
- Index
- Alerts
- Actions
- Sources of Evidence
 - Sensors
 - Index
 - Recorder

03 – Threat Response Alerts

- Navigating Alerts
 - Sorting
 - Filtering
 - Review of Alert Details

04 – Host Investigations and Remediation

- Navigating, Searching, and Filtering Recorded Forensic Timelines and Data Visualizations
- Working with Saved Evidence and Obfuscated Attacks
- Conducting Enterprise-wide Searches for Related Activity
- Applying Investigative Reasoning
- Understanding and Finding Injected code
- Remediation

05 – Developing and Applying Threat Intel

- Signals
- IOCsTanium shared tools