Tanium 7 Foundation, Operations, & IR Deep Dive

Course Description

Intended for both new and seasoned users alike, the Tanium Foundation, Operations, and IR Deep-Dive training course covers examining the state of endpoints across the enterprise, retrieving data, and quickly executing changes as necessary. Participants learn how to automate the detection and remediation of threats and outages in seconds, empowering your frontline, security, and IT operations teams to secure, control and manage every endpoint.

Topics include questions & sensors, dashboards, Windows and Linux patching, hardware and software reporting, software distribution, support and troubleshooting. Attendees also learn to hunt with the incident response module, use IOC Detect to locate indicators of compromise, perform forensic analysis with IR Gatherer and Trace, and use Tanium Connect to integrate with other tools.

Length

3 days

Target Audience

This course is for all users from beginners to those already acquainted with Tanium and its usage.

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.

Day 1: Tanium Foundation

01 – Introduction to Tanium
- Introduction to Tanium
- Topology
- Demonstration of the Platform
- System Requirements

02 – Sensors and Questions
- Overview
- Filtering
- Advanced Question Builder
- Drill-Down into Results
- Sensor Overview & Examples
- Sensor Configuration
- Authoring Custom Sensors

03 – Hardware Reporting
- Hardware Inventory
- Hardware Utilization
- General Client Health

04 – Software Reporting
- General Software Information
- Application Visibility
- Microsoft Software
- Licensing
- SQL Licensing
- Software Metering

05 – Packages & Actions
- Creating Packages
- Using Parameters
- Deploy Custom Packages
- Running Sensor-Based Packages
- Actions & Logs

06 – Dashboards
- Overview
- Creating Custom Dashboards
- Changing Out-of-box Dashboards
- Default Packages
- Saved Questions
- Packages Assigned to Saved Questions

07 – Scheduled Actions
- Scheduled Actions Overview
- When to Use Scheduled Actions

08 – Action Groups
- Manual vs Dynamic Groups
- Custom Tagging
- Action and Computer Groups

09 – Targeting
- Overview
- Targeting Guidelines
- Best Practices

Day 2: Operations

01 – Software Distribution
- Package Creation
- Package Verification
- Application Packages (EXE, MSI, ZIP)
- Package Deployment

02 – Patch Management
- Patching Dashboards
- Windows Patch Management
- Linux Patch Management
- Managed Application Upgrades

03 – Patch Workbench
- Overview
- Patch Workflow
- Whitelists
- Blacklists
- Patch Deployment Process

04 – Tanium Connect
- Overview
- Existing Connectors
- Export to File
- Export to Email
- Syslog

05 – 3rd Party Tools and Tanium
- Overview
- SCCM
- Anti-Virus

06 – Users and Groups
- User Permissions
- Adding Users
- Adding Groups
- Managing Users and Groups
- Action Approval
- Tanium Login Process

07 – AD Sync
- Assigning Permissions Using AD Groups
- Assigning Permissions Using AD Users

08 – Client Deployment Tool
- Deploying the Client
- Create Custom EXE
- Create Custom EXE with Tag
- Unmanaged Assets

09 – Content Signing
- XML Signing

10 – Intro to Support & Troubleshooting
- Overview
- Server Log Files
- Client Log Files
- Basic Client Troubleshooting
- Action Logs
- Verbosity Level
- Support process
- Knowledgebase

Day 3: IR Deep Dive with Tanium

01 – Hunting with the Incident Response Module

- Network activity
- Processes and related artifacts
- Persistence mechanisms
- Files at rest
- Searching with whitelist & blacklists
- Other useful sensors

02 – Indicators of Compromise & IOC Detect

- Creating & managing IOCs
- Understanding OpenIOC vs. Yara
- Setting up and running detections
- Indicator construction walk through

03 – Forensic Analysis with IR Gatherer

- IR gatherer overview
- Windows IR Gatherer
- Mac IR Gatherer
- Linux IR Gatherer

04 – Forensic Analysis with Trace

- Trace vs. IR Gatherer
- Trace setup and configuration
- Trace workbench usage & walkthrough

05 – Integration with Tanium Connect

- Connection workflow
- Types of filters
- Sample integrations