TANIUM TRAINING COURSE

Tanium Operations and Security Essentials

Course Description

The Tanium Operations and Security Essentials course is an immersive four-day training covering the primary operational use cases of the Tanium platform and modules. Participants learn how to use Tanium's powerful abilities to gain valuable network visibility, assess potential risks, plan for threat remediation, and empower security and IT operations teams to continuously secure, control, and manage every endpoint at speed and scale.

Topics include the primary operational use cases of the Tanium Core Platform, Interact, Connect, Trends, Asset, Map, Deploy, Patch, Integrity Monitor, Protect, Comply, Discover, Reveal, and Threat Response.

Length

4 Days

Target Audience

This course is intended for both new and experienced Tanium users who are ready to expand their knowledge of the Tanium Core Platform, and desire to become more proficient in the primary operational and security use cases of the Tanium modules.

Prerequisites

Attendees of this class will be automatically enrolled in the Tanium Core Online Training course. It's highly recommended that users complete this self-paced, 90-minute online training prior to attending class.

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.

Course Outline

01 – Tanium Introduction & Topology

- Introduction to Tanium
- Tanium Topology
- Tanium Console

02 – Tanium Server Overview

- Interact Overview
- Asking Questions
- Question Syntax and Structure
- Drilldown and Working with Results
- Creating Saved Questions
- Sensors Overview
- Creating Sensors
- Creating and Deploying with Packages
- Actions and Action Groups
- Basic Action Deployment
- Scheduled Action Deployment
- Dashboards and Categories Overview
- Viewing Dashboards and Categories
- Creating Dashboards and Categories

03 – Connect

- Connect Overview
- Creating Sources
- Creating Destinations
- Write to File Connection
- Microsoft SQL Database Connection

04 – Trends

- Trends Overview
- llustrating Data Over Time with Trends
- Visualization
- Detailed Views for Data Vulnerability and Patch Compliance
- Working with Trends Boards and Panels
- Publishing Trends Boards

05 – Asset

- Asset Overview
- Quick Export
- Software Inventory Reports
- Customized Reports on a Schedule

06 – Map

- Map Overview
- Importing Existing Applications
- Custom Applications
- Creating Endpoint Maps
- Introduction to Troubleshooting

07 – Deploy

- Deploy Overview
- Creating Software Packages
- Package Gallery
- Creating Software Bundles
- Viewing Package Applicability
- Creating a Maintenance Window
- Creating a Software Removal Deployment
- Monitoring Deployment Progress
- Working with the End User Self Service Profile/Client

08 – Patch

- Patch Overview
- Creating Deployment Templates
- Designing Efficient Enterprise Windows Patching
- Monthly Patch Walkthrough

09 – Integrity Monitor

- Integrity Monitor Overview
- Working with Watchlists and Exclusions
- Creating and Monitoring Watchlists
- Working with Labels, Notes, and Rules
- Integrating with Tanium Connect
- Working with Integrity Monitor Sensors

10 – Protect

- Protect Overview
- Creating Anti-Malware Reports
- Create and Deploy AppLocker Whitelist Policies
- Create and Deploy AppLocker Blacklist Policies
- Creating Windows Firewall Rules
- Creating Linux Firewall Rules

11 – Comply

- Comply Overview
- Creating and Deploying a Compliance Report Scan
- Creating and Deploying a Vulnerability Report Scan
- Creating and Running a Customized Compliance Report
- Using Tanium Connect to Export Comply Reports

12 – Discover

- Discover Overview
- Identifying Unmanaged Clients
- Deploying Tanium Client to Unmanaged Clients
- Monitoring Lost Interfaces
- Adjusting Lost Asset Time
- Labeling Interfaces for Grouping
- Finding a Lost Interface
- Ignoring/Removing Old Interfaces

13 – Reveal

- Reveal Overview
- Creating Rules and Rule Sets
- View Rules and Rule Sets
- Creating Live Connections
- Investigating File Matches and Snippets
- Publishing Validations
- Creating and Using Quick Searches
- Introduction to Troubleshooting

14 – Threat Response

- Threat Response Overview
- Configuring Tanium Detect
- Investigating Incidents with Tanium Trace
- Threat Hunting for Specific Artifacts
- Running a Quickscan
- Reviewing Alerts in Tanium Detect
- Working with Tanium Live Response
- Building Threat Intelligence
- Sending Data Outside of Tanium
- Conducting Basic Remediation
- Index Overview
- Searching for Filenames Using Question Builder and the Question Bar
- Searching for Blacklisted Hashes
- Searching for File Vulnerabilities
- Searching for Executables Masquerading as Other File Types