

WORKING WITH TANIUM CORE: PROFESSIONAL FOUNDATIONS

OEM: Tanium • Code: WORKING_WITH_TANIUM_CORE_PROFESSIONAL_FO

COURSE DESCRIPTION

Working With Tanium Core is designed for experienced Tanium operators, focusing on practical workflows and hands-on lab activities. By the end of this course, you will be proficient in leveraging core Tanium modules for a variety of advanced use cases and scenarios. Working With Tanium Core sets a common foundation for two specialized learning paths: Endpoint Management and Endpoint Risk & Security. Each learning path includes a series of dedicated sessions, diving deeper into individual Tanium modules. These learning paths are part of the recommended preparation for the Tanium Certified Professional (TCP) level certifications.

AUDIENCE PROFILE

- This course is intended for experienced Tanium operators who are ready to expand their knowledge of the Tanium platform, and desire to become more proficient in advanced workflows.

PREREQUISITES

- (Required) Getting Started with Tanium
- (Recommended) Tanium Essentials or 6 months operator experience

COURSE OBJECTIVES

By the end of this course, participants will be able to:

Discover

- Use Discover's advanced scanning configurations to avoid gaps in management and protect sensitive devices
- Dissect data using Discover labeling techniques
- Alert on critical missing devices
- Identify and correct Discover misconfigurations

Benchmark

- Identify the different categories of Benchmark metrics available (Risk, Guardian, Security, Operations)
- Determine an enterprise's Risk score and identify the risk metrics that contribute to that score
- Understand the concept of criticality, how to tag endpoints for criticality, and how it affects scoring
- Spot trends and changes to endpoint Risk scoring over time
- Compare organizational risk, security, and operational metrics to peers within the same industry

- Conduct an executive risk assessment

Asset

- Identify where Asset gets its data from and how to manage data
- Configure and manage advanced features of Asset including attributes, entities, and sources
- Create and manage custom reports in Asset based on business requirements
- Integrate Asset into your tech stack using out-of-the-box integrations and Import API
- Configure and use software and inventory usage data
- Inventory and report on libraries and dependencies on disk with Software Bill of Materials (SBOM)

Certificate Manager

- Find and alert on expired or expiring certificates across Windows, macOS, and Linux endpoints
- Replace expired or expiring certificates
- Gain visibility into listening services
- Run reports to identify weak algorithms and key lengths
- View self-signed and unauthorized CA certificates
- Integrate Certificate Manager with other Tanium modules

Investigate

- Gain immediate access to important data points
- Correlate performance events and activities to increase the speed of triage
- Diagnose related issues across endpoints to reduce repetitive troubleshooting
- Take advantage of Investigate's unique tie-in functionalities, such as Windows Event Browser, Registry Browser, and Service Control
- Leverage file browsing and tailing of files

Enforce

- Work with Enforce policy types and recognize the best situations to use them (ADMX, cluster, Linux and MacOS settings)
- Use Enforce to onboard endpoints to your specifications
- Use Tanium Enforce in endpoint expansion roles (MDM, IoT, OT, etc.)
- Use Enforce policy deployments to resolve Tanium Comply findings
- Use Enforce device management capabilities for incident response

COURSE OUTLINE

Module 1: Discover

Overview

- Key benefits
- Features and functions overview

Comprehensive scanning configurations

- Discovery methods
- Scan profile types
- Scan exclusions and inclusions
- Ncap versions

- Port specifications
- Scheduling scans
- Analyzing scan results
- Hands-on: Proactive asset discovery and network hygiene enforcement

Dissecting the data

- Labels and activities
- Locations and permissions
- Hands-on: Contextualize data with granular location mapping

Identifying and correcting misconfigurations

- Locate lost interfaces
- Exporting data
- Hands-on: Streamlined IT operations and continuous compliance through data remediation
- Troubleshooting

Module 2: Benchmark

Overview

- Key benefits
- Features and functions overview

Identifying important devices

- Understanding criticality
- Hands-on: Use criticality to identify endpoints with a high business impact

Deciding remediation priority

- Identifying remediation priority
- Using dashboards to visualize priority
- Hands-on: Use dashboards to create a remediation plan

Tanium Risk Assessment

- Conducting a Tanium Risk Assessment
- Hands-on: Conduct a Tanium Risk Assessment
- Troubleshooting

Module 3: Asset

Overview

- Key benefits
- Features and functions overview
- Where does Asset get its data?
- Entities and attributes

- Reporting
- Monitoring software and inventory

Build reports to create business value

- Expanding visibility with reporting
- Creating a custom report
- Hands-on: Creating a custom report

Design solutions using sources

- Sources in Asset
- Source and data management
- Hands-on: Managing sources in Asset

Extending visibility with integrations

- Integrating Asset and your tech stack
- Configuring exports and integrations
- Designing solutions using integrations
- Hands-on: Extending visibility with integrations

Business solutions for Software Inventory Usage (SIU)

- Software inventory and usage
- Working with SIU data
- Using SIU data

Software Bill of Materials (SBOM)

- Overview of SBOM
- Configuring SBOM
- Interpreting and taking action on SBOM data
- Troubleshooting

Module 4: Certificate Manager

Overview

- Key benefits
- Features and functions overview

Inventorying & reporting on certificates

- Certificate inventory
- Reports & dashboards
- Sending reports
- Hands-on: Certificate inventory

Finding & replacing expired certificates

- Reviewing certificates in your environment

- Deploying certificate audits
- Managing certificates
- Hands-on: Emergency certificate replacement

Exposing weak cipher usage

- Certificate cipher visibility
- Exposing weak certificates
- Post-quantum cryptography
- Hands-on: Managing weak ciphers
- Troubleshooting

Module 5: Investigate

Overview

- Key benefits
- Features and functions overview
- ServiceNow integration

Root cause analysis

- Investigations and activities
- Remediating from Single Endpoint View
- Hands-on: Investigating the root cause of an issue

Cooperative troubleshooting

- Working an investigation as a team
- Hands-on: Crafting an Investigation

Remotely managing Windows

- Service control
- Windows Event Browser
- Resource summary
- Hands-on: Remediating endpoint issues
- Troubleshooting

Module 6: Enforce

Overview

- Key benefits
- Features and functions overview
- Enforce policies
- Hands-on: Create and enforce a BitLocker policy

Operational hygiene for newly acquired endpoints

- Implementing Windows Device Control
- Configuring AppLocker
- Configuring Windows firewall
- Configuring Linux firewall
- Hands-on: Practical endpoint security configuration

Enforcing disk encryption standards

- Configuring disk encryption policies
- Disk encryption workflow
- Hands-on: Enforcing disk encryption standards

Configuring Microsoft Defender

- Understanding Defender and MDE Integration with Tanium
- Configuring core Defender settings
- Scanning
- Managing advanced Defender features
- Monitoring Defender health and compliance
- Hands-on: Defender policy configuration and compliance monitoring

Securing sensitive endpoints

- Hardening public and shared devices
 - Applying device control and network isolation
 - Monitoring and alerting for sensitive endpoint activity
 - Hands-on: Endpoint hardening and network isolation
-
- Troubleshooting