COURSE TABLE OF CONTENTS

TANIUM ESSENTIALS 7.6

OEM: Tanium • Code: TANIUM_ESSENTIALS_7_6

COURSE DESCRIPTION

Tanium Essentials 7.6 is an immersive training covering the primary use cases and operation of the Tanium platform and its solution modules. You will learn how to use Tanium's powerful abilities to gain network visibility, apply control and remediation, manage endpoints, enhance the employee experience, manage risk and compliance, and respond to incidents using Tanium modules in a variety of practical scenarios. This course is divided into several sections based on common workflows, each one displaying how Tanium modules can work together to solve challenging scenarios.

AUDIENCE PROFILE

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

PREREQUISITES

- Getting Started With Tanium

COURSE OBJECTIVES

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

Tanium Platform

- Identify the benefits of the Tanium Platform and its unique linear-chain architecture
- Review the purpose and benefits of Tanium's foundational modules
- Introduction to key components of Tanium's Autonomous Endpoint Management (AEM)
- Identify Tanium's Shared Services and the functionality they add
- Discuss Tanium partner integrations and how they let you do even more with Tanium

Gaining Visibility

- Describe the basic features, functions, and benefits of the Tanium Discover, Asset, and Benchmark modules
- Pivot between Discover, Asset, and Benchmark to bring endpoints under control in a scenario
- Explain how Discover active scanning works
- Create a Discover profile to install the Tanium Client on unmanaged endpoints
- Apply labels to interfaces

- Create an Asset report to identify software usage
- Set Report attributes and create a View
- Use SBOM to identify software at risk for a known vulnerability
- Determine an enterprise's risk score and asset criticality
- View metrics and dashboards to compare against industry peers

Applying Control & Remediation

- Describe the basic features, functions, and benefits of the Tanium Enforce, Certificate Manager, and Investigate modules
- Pivot between Enforce, Certificate Manager, and Investigate to ensure compliance standards in a scenario
- Identify expiring or expired certificates
- Use Certificate Manager to prepare for post-quantum cryptography
- Deploy a certificate audit package
- Describe the uses of different policy types
- Create and manage Configuration policies and remediation policies
- Leverage Tanium knowledge for activities of interest across endpoints
- Assign an owner to each investigation
- Manage and troubleshoot on a single endpoint remotely

Managing Endpoints

- Describe the basic features, functions, and benefits of the Tanium Provision, Patch, and Deploy modules
- Pivot between Provision, Patch, and Deploy to rollout new operating systems and software in a scenario
- Create OS bundles
- Describe the OS refresh deployment process
- Create bare metal deployments
- Choose proper methods for patch scan configurations
- Manage patch lists and block lists
- Specify targeted endpoints with deployment templates
- Import third-party software package templates
- Use Self Service to install and remove software
- Align deployments with maintenance windows

Enhancing the Employee Experience

- Describe the basic features, functions, and benefits of the Tanium Performance and Engage modules
- Pivot between Performance and Engage in a scenario
- Get insights into performance and health metrics on all your endpoints
- Monitor and be notified about critical performance and other metrics
- Analyze and evaluate employee and customer digital experiences
- Learn and quantify the impact of automation and self-help workflows
- Create custom surveys and deploy them
- Notify employees about issues impacting their experience
- Measure and baseline the sentiment and satisfaction of the entire organization as well as each employee

Managing Risk & Compliance

- Describe the basic features, functions, and benefits of the Tanium Reveal, Integrity Monitor, and Comply modules
- Pivot between Reveal, Integrity Monitor, and Comply in a scenario

- Find and review sensitive data on endpoints
- Create secondary validations for automatic confirmation
- Monitor operating system files, application data, and registry settings
- Continuously monitor sensitive files and folders for changes and activity
- Verify endpoints in an organization meet security compliance
- Use industry-standard benchmarks for compliance scans

Responding to Incidents

- Describe the basic features, functions, and benefits of the Tanium Threat Response and Impact modules
- Pivot between Threat Response and Impact in a scenario
- Act upon threats using Threat Response features
- Identify users, groups, and endpoints with high potential for lateral movement
- Use the Impact categories to locate potential causes of excessive rights
- Use Impact to devise a strategy aimed at minimizing horizontal movement within the enterprise network

COURSE OUTLINE

Module 1: Tanium Platform

- Welcome
- Tanium Platform (review)
- Tanium foundations (review): Interact, Reporting, Connect
- Console components: Guide, Guardian, Automate
- Shared Services overview: Direct Connect, Satellites, Endpoint Configuration, Client Management, Recorder, Index, Reputation, Software Bill of Materials (SBOM), Criticality, End-user Notification, Directory Query
- Tanium partner integrations overview: Microsoft, ServiceNow, ScreenMeet, Deep Instinct, Gateway

Module 2: Gaining Visibility

Discover module

- What is Discover?
- Use cases
- Discover Overview page
- Scanning
- Designating locations
- Creating labels

Asset module

- What is Asset?
- Use cases
- Asset Overview page
- Reports
- Sources
- Software Inventory & Usage (SIU)

- Software Bill of Materials (SBOM)

Benchmark module

- What is Benchmark?
- Use cases
- Benchmark Overview page
- Risk scoring
- Benchmark dashboards

Module 3: Applying Control & Remediation

Enforce module

- What is Enforce?
- Use cases
- Enforce Overview page
- Policies
- Device actions
- Configuration policies
- Enforcements

Certificate Manager module

- What is Certificate Manager?
- Use cases
- Certificate Manager Overview page
- Dashboards and data
- Managing certificates
- Post-quantum cryptography

Investigate module

- What is Investigate?
- Use cases
- Investigate Overview page
- Investigations and activities
- Working with investigations
- Remediate with remote management

Module 4: Managing Endpoints

Provision module

- What is Provision?
- Use cases
- Provision Overview page
- Provision endpoint types

- USB boot drives
- Staging OS bundle files
- Bare metal deployment
- OS refresh deployments

Patch module

- What is Patch?
- Use cases
- Patch Overview page
- Scan configurations
- Patches
- Patch lists
- Patch Confidence Score
- Block lists
- Maintenance windows
- Deployments

Deploy module

- What is Deploy?
- Use cases
- Deploy Overview page
- Managing software
- Deployments
- Deploy Confidence Score
- End-user self service

Module 5: Enhancing the Employee Experience

Performance module

- What is Performance?
- Use cases
- Performance Overview page
- Profiles
- Events
- Direct Connect
- Working with Performance and Reporting

Engage module

- What is Engage?
- Use cases
- Engage Overview page
- Creating surveys
- Deploying surveys
- Survey details

- Endpoint experience

Module 6: Managing Risk & Compliance

Reveal module

- What is Reveal?
- Use cases
- Reveal Overview page
- Patterns
- Rules
- Validations
- Quick Search

Integrity Monitor module

- What is Integrity Monitor?
- Use cases
- Integrity Monitor Overview page
- Labels and rules
- Watchlists, monitors, and events

Comply module

- What is Comply?
- Use cases
- Comply Overview page
- Assessments
- Standards
- Findings and filtering
- SCAP
- Exporting findings
- Remediation Visibility

Module 7: Responding to Incidents

Threat Response module

- What is Threat Response?
- Use cases
- Threat Response Overview page
- Threat detection engine
- Deployment workflows
- Incident response
- Threat Response and Reporting

Impact module

- What is Impact?
- Use cases
- Impact Overview page
- Inbound vs. outbound impact
- Identifying highest potential impact
- Integrations

Module 8: Conclusion

- Solidify key points of the training
- Introduce Tanium Certified Operator (TCO) program and additional learning opportunities