TANIUM LEARNING CENTER

WORKING WITH TANIUM: ENDPOINT RISK & SECURITY

COURSE DESCRIPTION

Working With Tanium Endpoint Risk & Security is an immersive training bundle covering the installation, maintenance, usage, and configuration of risk and security-focused Tanium modules, including Impact, Enforce, Threat Response, Comply, Integrity Monitor, Reveal, and Benchmark.
Participants will learn how to use Tanium's powerful abilities to gain valuable network visibility, assess potential risks, plan for threat remediation, and empower IT teams to continuously secure, control, and manage every endpoint at speed and scale. Interactive lab access will be provided for hands-on activities.

This course bundle is included in the recommended training path for the Tanium Certified Professional Risk and Security (TCPRS) Certification.

DELIVERY OPTIONS

Instructor-Led Training (ILT)

Virtual Instructor-Led Training (VILT)

Web-Based Training (WBT)

ADDITIONAL RESOURCES

- Tanium Knowledge Base
- Tanium Resource Center

Delivery options and duration

ILT/vILT: 2 days | WBT: 4-6 hours

Prerequisites

Working With Tanium Core is recommended.
TCO Certification is recommended. Certifications | Tanium to "TCO Certification".

Target audience

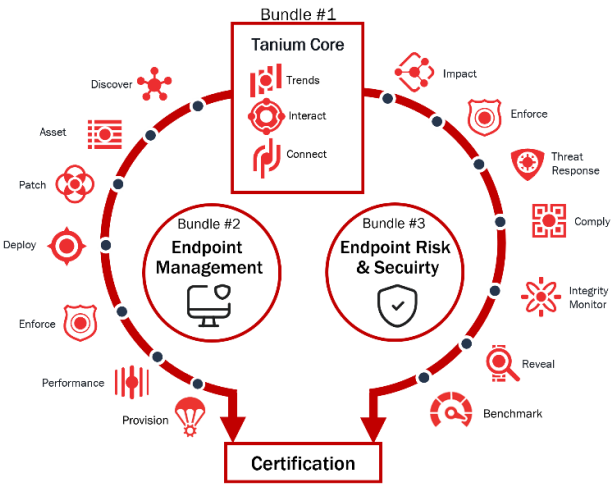
This course is intended for experienced Tanium users who are ready to expand their knowledge of Tanium risk & security modules and their capabilities.

Registration information

This training course is available to purchase for new and existing customers. For information on our training courses, or to receive a quote, please contact your Tanium/Partner Representative. If you are uncertain of who your representative is, please reach out to training@tanium.com.

WORKING WITH TANIUM SERIES

Working With Tanium: Core sets the foundation for two specialized learning paths: Endpoint Management and Endpoint Risk & Security. Each learning path includes a series of dedicated sessions (training bundle) diving deeper into individual Tanium modules in preparation for advanced-level certifications.



COURSE OBJECTIVES

IMPACT

- Configure Tanium Impact
- Use Impact to identify lateral movement risks
- Measure improvement as lateral movement risks are mitigated

ENFORCE

- Configure Tanium Enforce
- Create baseline policies
- Troubleshoot and resolve common issues

THREAT RESPONSE

- Configure Tanium Threat Response
- Locate and remediate compromised endpoints
- Troubleshoot and resolve common issues

COMPLY

- Configure Tanium Comply
- Import assessment engines, java runtime environments, and standards
- Manage assessments
- Customize compliance benchmarks and vulnerability sources
- Troubleshoot and resolve common issues

INTEGRITY MONITOR

- Describe the features, benefits, and use cases for Tanium Integrity Monitor
- Configure Integrity Monitor
- Import and configure customized watchlists
- Use monitors to watch changes in files and directories
- Work with rules in Integrity Monitor
- Use Connect to send Integrity Monitor events to a file
- Integrate ServiceNow
- Troubleshoot and resolve common issues

REVEAL

- Configure Tanium Reveal
- Create a rule
- Develop custom rule patterns
- Create an advanced rule using a custom regex and keyword list
- Investigate and validate rule results
- Configure profiles
- Troubleshoot and resolve common issues

BENCHMARK

- Configure Tanium Benchmark
- Determine an enterprise's risk score and asset criticality
- View metrics and dashboards
- Identify individual sources of risk
- Pivot into supporting products for deeper analysis
- Troubleshoot and resolve common issue

COURSE OUTLINE

IMPACT

- Feature and functions
- Benefits
- Feature and functions
- Business use cases
- Configuration
- Collecting data
- Prioritizing alert remediation with Tanium Threat Response
- Prioritizing risk reduction with Tanium Risk
- Analyzing potential lateral movement from attacks
- Exporting data with Tanium Connect
- Troubleshooting unresolved assets
- Needs Attention or Unsupported status is reported

ENFORCE

- Benefits
- Feature and functions
- Business use cases
- Configuration
- Firewall rules
- Windows Defender
- Anti-malware deployment
- AppLocker
- Troubleshooting common scenarios

THREAT RESPONSE

- Benefits
- Feature and functions
- Business use cases
- Configuration
- Profiles
- Live Connection
- Saving evidence
- Quarantining endpoints
- Live Response
- Creating and deploying threat intelligence
- Reputation Service and Threat Response
- Alerts
- Using system notifications to audit Threat Response functions
- View Threat Response management tasks for auditing
- Hunting threats in the enterprise
- Common troubleshooting scenarios

COMPLY

- Benefits
- Features and functions
- Business use cases
- Configuration
- RBAC and Comply
- Creating Computer Groups
- Assessment engines
- Java runtime environments
- Managing assessments
- Remote vulnerability assessments
- Compliance benchmarks
- Custom compliance setup
- Vulnerability sources
- Custom vulnerability setup
- Logs and data collection
- Export support data

INTEGRITY MONITOR

- Benefits
- Features and functions
- Business use cases
- Configuration
- Importing and configuring customized Integrity Monitor watchlists
- Using monitors to watch changes in files and directories
- Working with rules
- Using Connect to send Integrity Monitor events to a file
- Integrating ServiceNow
- Troubleshooting with sensors
- Common troubleshooting scenarios

REVEAL

- Benefits
- Features and functions
- Business use cases
- Configuration
- Creating a rule
- Developing custom rule patterns
- Configuring profiles
- Logs and data collection
- Using sensors to troubleshoot issues
- Common troubleshooting scenarios

BENCHMARK

- Benefits
- Features and functions
- Business use cases
- Configuration
- Risk score
- Risk vectors
- Asset criticality
- Compensating controls
- Data collection and timing
- Monitoring risk health
- Investigating endpoint tools
- Collecting a support bundle