# XENTAURS

Protecting Workloads with Tetration Analytics

Designed for technical IT leaders and systems architects charged with adressing immediate business challenges and driving strategy. This course will help attendees understand use cases for Tetration and how it can help the business improve their security posture by reducing attack surfaces, remaining compliant, and gaining visibility across all environments.
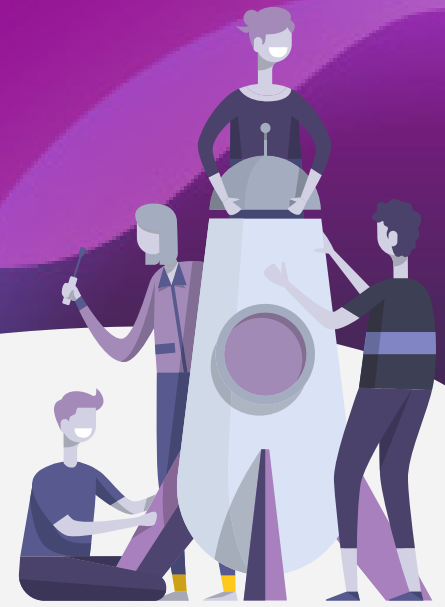
Course Overview

This course incorporates a series of DEMOs, Whiteboards, and Hands-On labs which serve to reinforce Tetration fundamentals such as: creating a scalable scope structure, mapping application dependencies, and analyzing and enforcing policy. We then dive deeper into what drives the Tetration Dashboard Composite Security Score and how that information can be leveraged to provide comprehensive workload-protection capability and unprecedented insights across a hybrid cloud infrastructure.

Audience

- Data Center Architects
- Solution Architects
- Network Engineers
- Systems Engineers
- System Administrators
- Storage Administrators
- Systems Integrators
- Applications Owners
- DevOops Engineers
- Cloud Engineers

Day 1

Lesson: Why Tetration
- The Drive for Real-Time Visibility
- Invisibility Challenges
- Security Challenges
- Micro-Segmentation: Contain Lateral Movement

Lesson: Tetration Overview
- Tetration Architecture
- Creating Users and Assigning Roles
- Scopes and RBAC
- Annotating and Filtering Concepts
- Tetration Sensor Options
- Cisco and Third-Party Integrations

Whiteboard: Creating a Scalable Scope Structure
Demo: Installing Windows and Linux Sensors
Demo: VMM Integration
Lesson: Features of Tetration
- Tetration Dashboard: Composite Security Score
- Real-Time Inventory
- Gaining Visibility with Sensors

Day 2

Lesson: Vulnerability
- Application Dependency Mapping
- Automated Whitelist Policy Generation
- Segmentation Policy

Demo: Conducting an ADM Run
Lesson: Process Hash
- Anomolies and Whitelisting

Demo: Booting Workload Process Details
Lesson: Reduce Attack Surface
- Workload Profiles
- Software Package Vulnerabilities
- Vunerability Dashboard

Lesson: Forensics
- Tagging and VMM Integration
- BYOD (Bring your own data)
- Security Breach Investigation/ Mitigation
- Alerting
- Policy Deviation and Detection
- Identify Behavior Anomolies
- **Data Leaks**
- **Expected versus Flagged Workloads**
- **Segmentation Compliance**
- **Policy Analysis Scoring**
- **Escaped/ Rejected Flows**

Day 3

Lesson: Use Cases
- Segmentation using Whitelist Policy
- Server Process Baseline and Behavior Deviation
- Software Inventory and Vulnerability Detection

Lab: Installing a Tetration Agent
Lab: Inventory, Filters, & Application Dependency Maps
Lab: Policy Discovery using Application Dependency
Lab: Mapping
Lab: Policy Analysis and Enforcement
Lab: Policy Simulation and Compliance Demonstration
Lab: Advanced Security
Lab: REST API Demonstration

Xentaurs is a next-generation consulting agency and digital systems integrator helping businesses transform. We are a leader in DevOps, Infrastructure-as-Code, Cloud and Software-Defined Infrastructure. Learn more at http://demand.cisco.com/dsixentaurs