XENTAURS

Cisco Secure Workload
Workshop

Duration: ***1 Day***
Format: ***Interactive Workshop***

This 1-day, hands-on workshop is for Network and/or Security Engineers who are deploying Cisco Secure Workload (formerly Tetration). Cisco Secure Workload is a platform that automates application micro-segmentation and enforcement across on-prem data centers and public cloud environments.

This interactive workshop will kick off with an executive briefing and provide insights as to why CSW is needed in today's multi-cloud application environments and will include use case examples. The second half of the workshop will focus on the technical aspects of CSW with a hands-on approach focusing on key CSW concepts; application blueprinting; zero-trust methods, workload, and application life cycle health; and best practices for application modeling and enforcement.

Workshops are customized based on customer environment and needs, with a sample agenda provided below.

Course Details

Who Should Attend

- Executive stakeholders (First section)
- Security engineers
- Network engineers
- Cloud architects
- Application security architects

Learning Objectives

- Understand why Cisco Secure Workload is a critical part of a zero-trust approach
- Learn key capabilities, workload protection, and application micro-segmentation
- Learn how to enable a zero-trust security approach with CSW for your applications with micro-segmentation

Delivery Methods

Interactive Remote Workshop
With the Xentaurs Webinars, you can expect engaging 2-way discussions and learning.

In-person Workshop
On-site in person workshops available upon request.

Cisco Partner
Business Enablement Partner

Xentaurs is also an approved MINT Service Partner. Visit www.mintibn.com to leverage our services for your Cisco Secure Workload deployments.

XENTAURS

Sample Agenda

Workshops are customized on a per-customer basis

Cisco Secure Workload
Workshop

Cisco Secure Workload Overview

Cisco Secure Workload Overview

- Executive overview
- Business objectives and road map discussion
- Current state of workload/DC security
- Why CSW
- Overview of key features

Workload Security

- Micro segmentation
- Workload behavior anomalies
- Reducing attack surface
- Policy compliance
- Unify visibility and automation with SecureX

Organizing & verifying applications

- Scope design
- Annotations & attributes
- Flow search
- Application workspaces
- Application modeling
- Endpoint grouping
- Container policy enforcement (if applicable)
- Cloud workload enforcement
- Security scoring overview
- Workload health overview
- Vulnerability overview

Application segmentation methodology & best practices

- Build
- Discovery
- Analysis
- Enforce