majentai GUARDIANS

Cisco Secure Workload Advanced Enablement

Majentai's Cisco Secure Workload (CSW) Enablement Workshop is designed for technical professionals responsible for securing modern hybrid applications. This advanced, hands-on training guides participants through the architecture, capabilities, and real-world application of Cisco Secure Workload. The workshop blends theory and practice, equipping teams with both strategic understanding and operational expertise. Participants will deploy sensors, segment applications, analyze traffic patterns, and enforce security policy across on-premise and cloud environments—building the foundation for a scalable, zero-trust security framework tailored to their organization's needs.

What You'll Learn

This workshop equips participants with the practical skills and confidence needed to deploy and operate Cisco Secure Workload effectively in real-world environments. Attendees will learn how to architect and implement a secure segmentation strategy across hybrid infrastructures, including on-prem and cloud. Through guided labs and interactive instruction, participants will gain hands-on experience visualizing east-west application traffic in real time, identifying and addressing policy gaps, and applying adaptive, zero-trust security controls. The training emphasizes the operationalization of Cisco Secure Workload as a core component of a modern security stack—empowering engineers to detect and refine escaped flows, map application dependencies, and enforce dynamic, risk-informed policy across their enterprise.

Agenda

Sessions 1-3: Foundation & Policy Strategy

Lesson: Why CSW

- The Drive for Real-Time Visibility
- The Hidden Cost of Invisibility
- Containing Lateral Movement with Micro-Segmentation

Lesson: Platform Overview

- CSW Architecture Deep Dive
- Scopes and RBAC Strategies
- Role-Based Access and User Management

Lesson: Building Your Environment

- Creating a Scalable Scope Hierarchy
- Dynamic Tagging for Adaptive Policy
- Inventory Filtering
- Demo: Annotation File Build and Upload

Lesson: Analyze

- Policy Refinement via Flow Analysis
- Escaped Flow Detection
- Demo: Using CSW to Refine Policies

Sessions 4-8: Discovery, Mapping, and Enforcement

Lesson: Discover

- Application Dependency Mapping (ADM)
- Clustering and Conversation Views
- Interpreting Policy Recommendations

Lesson: Policy Creation & Optimization

- Post-ADM Policy Refinement
- Global Policy Development
- Demo: ADM Run, Results Review, and Policy Build

Who Should Attend

- Network Engineers
- Security Engineers
- Cloud Architects
- Application Security Architects

Course Format

- Delivery Method: Remote, Instructor-Led / Interactive Virtual Labs and Demos
- Duration: 16 Hours (Delivered over 2 days or 4 sessions)
- Minimum Students: 4 attendees

majentai GUARDIANS

Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit https://majentai.com