Service Brief

Workshop

majentai

Cisco Secure Workload (CSW) Workshop

This Cisco Secure Workload (CSW) Workshop is a structured engagement designed to align stakeholders, assess current-state realities, and define a phased deployment path with limited risk. Majentai documents architecture, telemetry, labeling, and operating model decisions needed to move from discovery toward controlled onboarding, validation, and enforcement readiness.

Overview

This Cisco Secure Workload (CSW) Workshop is a focused planning engagement designed to define a low-risk path to deployment with alignment and practical next steps. The workshop validates current-state realities, target architecture decisions, and rollout assumptions while establishing the governance, design direction, and readiness criteria required to move toward implementation with more confidence.

- Stakeholder alignment and decision rights
- Current-state architecture and telemetry assessment
- Segmentation roadmap and deployment planning
- Labeling, integration, and onboarding strategy
- Operating model and governance design

Business Outcomes

This Workshop reduces early program risk by aligning stakeholders, documenting constraints, and defining an execution-ready path before implementation begins. Majentai establishes a practical architecture, rollout model, and governance approach so teams can onboard and enforce with clearer decisions.

- Reduce planning risk before implementation starts
- Clarify ownership, governance, and decision rights
- Improve readiness for onboarding and validation
- Create controlled path toward enforcement

At a Glance

Objectives

- Establish greenfield approach for CSW adoption
- Align business, IT, and OT requirements
- Define target architecture and low-risk roadmap

Scope

- Structured workshop and planning engagement
- Pilot scope, success criteria, and current-state inputs
- No deployment, enforcement, or production changes

Deliverables

- Strategy and requirements artifacts
- High-level design and execution blueprint
- Closeout report and knowledge transfer

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, confirm scope and success criteria, and assess current-state platforms, telemetry, tagging, and governance constraints that will shape the initial CSW adoption approach.

Phase 2: Solution Design and Planning

Define target architecture, telemetry and integration approach, segmentation model, label taxonomy, and rollout plan needed to deploy CSW safely across the agreed pilot scope.

Phase 3: Build, Implement and Validate

Produce an execution-ready blueprint covering onboarding sequence, telemetry requirements, readiness checks, and application dependency approach so implementation teams can validate feasibility before delivery begins.

Phase 4: Operations & Recommendations

Define the operating model, policy governance workflow, and knowledge transfer outputs needed to support post-implementation adoption and a controlled path from onboarding toward enforcement.

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