

## WSCDO

# WorkShop: Cisco Defense Orchestrator

24 horas

Security

Telecon

## INTRODUÇÃO

Este Workshop apresenta o Cisco Defense Orchestrator, sua arquitetura, o processo de integração do CDO, SDC e o Cisco FMC/FTD, utilizando as ferramentas e funcionalidades do CDO aplicadas.

## OBJETIVO DO CURSO

Ao concluir este treinamento, o aluno será capaz de cumprir estes objetivos gerais:

- Descrever as funcionalidades do CDO;
- Explicar o processo de integração do CDO junto ao Cisco FMC/FTD;
- Descrever as funcionalidades e ferramentas do CDO.

## PÚBLICO-ALVO

Profissionais de segurança que necessitam de conhecimentos na instalação, configuração, operação e administração do Cisco FTD/FMC e a utilização do CDO e suas funcionalidades de integração e gerência.

## PRÉ-REQUISITOS

É recomendado que os alunos possuam as seguintes habilidades e conhecimentos prévios ao treinamento:

- Conhecimento prático em redes IP (básico);
- Conhecimento básico de firewall de segurança.

## **Introdução ao WorkShop**

Apresentações Iniciais

Objetivos do Workshop

## **Arquitetura: Cisco Defense Orchestrator**

Estratégia de Segurança em Redes

Gerenciamento & Segurança

Solução Cisco Defense Orchestrator

Opções em Licenciamento

Soluções Cisco Suportadas pelo CDO

Benefícios da Solução CDO

## **Implementação do CDO**

Instalação e Inicialização

SDC: Secure Device Connector

SAL: Security Analytics & Logging

Integração dos Produtos Cisco: ASA

Integração dos Produtos Cisco: FTD

Integração dos Produtos Cisco: FMC

## **Gerenciamento do Tenant Cisco CDO**

Configurações Gerais

Gerenciamento de Usuários

Cisco RBAC & CDO

Parametrização dos Logs

## **Gerenciamento dos Produtos Cisco**

Cisco ASA

Cisco FTD

Cisco FMC

CDO & Cisco Tenant

Utilização do SDC na Rede Local

Integração dos Produtos Cisco

Configuração dos Produtos Cisco

## **Demonstrações do Cisco CDO**

Lab 1. Network health status

Lab 2. Onboard devices

Lab 3. Clean up configurations and policies

Lab 4. Use the Command-Line

Lab 5. User ManagementInterface (CLI)

Lab 6. Schedule deployments

Lab 7. Manage VPN

Lab 8. Use the Logging and Security Analytics service

Lab 9. Analytics and Detection

Lab 10. Total Network Analytics and Detection

Lab 11. Multi-Domain Management