Cisco CyberVision Deployment and Operation

Duration: 3 Days **Course Code: N1_INCVDO**

Overview:

INCVDO, Cisco Cyber Vision Deployment and Operation, is a 3-day instructor-led course. Security is every enterprise's top priority in today's connected world and keeping enterprise architecture secure will protect business values and outcomes. Thus, a critical element to the success of any network is ensuring and maintaining security – it's a need that is applicable to all networks and network devices, including those that power Cisco Internet of Things technologies and solutions. In an effort to simplify cybersecurity and increase device visibility within systems utilized by our IoT customers and partners, Cisco introduces Cisco Cyber Vision – a software cybersecurity solution for Operations Technology (OT). This course uses Cisco Validated Designs (CVD) to build a foundational understanding of the potential security threats impacting today's IoT Extended Enterprise and IT – OT integration using Cyber Vision. The goal of this course is to help the student understand the types of attacks, the types of targets and the tools available to protect the Industrial IoT architecture and to use Cyber Vision to keep the IoT infrastructure safe. Practical skills will be achieved using real-world scenarios and examples in a lab developed for such a purpose.

Cisco Cyber Vision provides organizations the ability to gain visibility into industrial environments including full details of what assets are on the network, how those assets are communicating, and application level understanding of operational information. As a result, Cisco Cyber Vision provides views and capabilities, including integrations, that can be leveraged by security teams, IT infrastructure teams, and operational teams to ensure system integrity and protect against cyber risks. Features **Cyber Vision 5.4**

The course qualifies for 18 Cisco Continuing Education Credits (CE).

Updated 11/08/2026

Target Audience:

The primary audience for this course is as follows:

- Systems Administrators and Engineers

- Technical Solutions Architects

- Systems Integrators

- Channel Partners

- Value-Added Resellers

Objectives:

- Upon completion of this course, the learner will be able to meet these overall objectives:
- Explore fundamental OT, ICS, and Industrial IoT cybersecurity challenges and vulnerabilities
- Deploy and operate Cisco Cyber Vision in real-world industrial environments
- Effectively monitor, assess, and manage OT/IIoT security posture and incidents using Cyber Vision
- Understand Cybersecurity OT assessments fundamental concepts
- Optimize and troubleshoot Cisco Cyber Vision deployment for continuity and effectiveness

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- Basic knowledge of Cisco Security.
- Familiarity with networking and Internet of Things Concepts.
- Basic Operational and Cybersecurity understanding in OT or

Testing and Certification

- N\A

Follow-on-Courses:

- None Recommended

Content:

Course Outline

Module 1: OT Cybersecurity Fundamentals and Cisco Cyber Vision Introduction

- An Overview of ICS/OT and Industrial IoT architectures
- Identifying common threats, vulnerabilities, and attack surfaces in OT/ICS environments
- OT concepts, terms, and daily operational challenges
- Understanding convergence challenges (IT/OT integration)
- Key components and elements of Cisco Cyber Vision architecture
- Introducing Cisco Cyber Vision UI (navigation and main functionalities overview)

Module 2: Cisco Cyber Vision Deployment and Implementation

- Deployment methodologies (Centralized, Distributed Sensor deployment approaches)
- Detailed review of sensor types, functionalities, and appropriate deployment scenarios
- Installation and provisioning Cisco Cyber Vision Center
- Installation and configuration of Cisco Cyber Vision sensors
- Performing initial data capturing and validating sensor communications

Module 3: Cisco Cyber Vision Operational Management

- Familiarization with advanced GUI features and customizations (Dashboards, Views, Panels)
- Event Management: Monitoring events, alerts, and audits for cyber incidents and anomalies
- Understanding the use and management of monitor mode
- Baselining facilities and managing change detection
- Intrusion Detection System (IDS) integration, configuration, and management using SNORT
- Advanced Vulnerability Management within Cisco Cyber Vision usage
- Active Discovery methodology and best practices
- Administration of the Cisco Cyber Vision ecosystem (licensing, user management, RBAC, LDAP

Module 4: Cisco Cyber Vision Integration with Cisco Catalyst Center

- Integration Architecture Overview

Discovery Lab 4: Deploy CCV Sensor on Cat9300

Task 1: Install CCV Deployment Tool

Discovery Lab 5: Configure event-forwarding from Cisco Cyber Vision to Splunk (CEF/syslog)

Task 1: Manage Cyber Vision apps in Splunk

Task 2: Generate an API token in Cyber Vision Center

Task 3: Add Account to Cisco Cyber Vision Splunk Add-On

Discovery Lab 6: Import and configure Cyber Vision dashboards and analytics views in Splunk

Task 1: Add inputs to Splunk

Task 2: Add syslog data source in Splunk

Task 3: Add syslog configuration in Cyber Vision Center

Discovery Lab 7: Organizing initial dataset using groups and network presets

Task 1: Organizing the Devices in Groups

Task 2: Organize Data by Preset Filters

Discovery Lab 8: Creating and managing security baselines, event management, and real-time alerting

Task 1: Creating and managing security baselines

Task 2: Review CCV Events

Task 2: Vulnerability Dashboard

Discovery Lab 10: System administration and practical configuration tasks: user management, licensing, RBAC

Task 1: Create an Account

Task 2: Licensing

Discovery Lab 11: Configuring advanced IDS profiles and analyzing threat data

Task 1: Anomaly Detection and IDS

Discovery Lab 12: Configure pxGrid integration between Cisco Cyber Vision and Cisco ISE

Task 1: Enable pxGrid in Cisco ISE

Task 2: Create profiling policies in Cisco ISE using the endpoint device attribute data collected from Cisco Cyber Vision

Task 3: Generate Client Certificate in Cisco ISE

Task 4: Create Client Certificate in Cisco Cyber Vision

Task 5: Import Cisco Cyber Vision's Certificate Authority into Cisco ISE and Enable Trust for Authentication

Task 6: Validate the integration in Cisco ISE and Cisco Cyber Vision

Discovery Lab 13: Cisco Catalyst Center and ISE Integration

Task 1: Integrating ISE with Catalyst Center

Task 2 Cisco Cyber Vision Sensor discovery

- Use Cases for Integration
- Configuration Workflow
- Operational Verification

Module 5: Cisco Cyber Vision Integration with Cisco Identity Services Engine (ISE)

- Overview of Cisco ISE in OT Environments
- Value of asset profiling and visibility in OT networks
- Understanding role-based access control and segmentation in OT environments
- Integration architecture between Cisco Cyber Vision and Cisco ISE
- Configuration and data exchange using pxGrid integration
- Operational workflow of asset profiling, visibility, and dynamic policy enforcement based on Cyber Vision insights
- Best practices and use-case scenarios (segmentation, dynamic NAC enforcement, access control)

Module 6: Cisco Cyber Vision Integration with Splunk (SIEM)

- Introduction to Splunk integration and OT cybersecurity use-cases
- Understanding the value-added by integration with SIEM platforms
- Configuring Cisco Cyber Vision event-forwarding integration with Splunk:
- Syslog configuration (CEF)
- Event data normalization and parsing
- Splunk dashboards design for Cisco Cyber Vision:
- Scenario-driven OT/ICS risk visibility dashboards
- Incident detection and operational analytics dashboards
- Alerting and event correlation using Splunk Cyber Vision integration for security operations teams
- Practical use-cases: OT security event and incident response management

Lab Outline

Labs are designed to assure learners a whole practical experience, through the following practical activities:

Discovery Lab 1: Installation of Cyber Vision Center and Global Center

Task 1: Cyber Vision Architecture Overview

Task 2: Installation of Cisco Cyber Vision

Task 3: Filter and Search in the Events

Discovery Lab 9: Performing Active Discovery and Identify Vulnerabilities

Task 1: Active Discovery

Discovery Lab 14: Practical scenario: detection, observation, correlation, and response to simulated OT network security events via Splunk dashboards and features

Task 1 Cyber Vision dashboards

Task 2: Detection, observation, correlation, and response to simulated OT network security events via Splunk dashboards

Task 3: Loading a PCAP		
Task 4: Initial interaction and familiarity with Cisco Cyber Vision GUI		
Discovery Lab 2: Exploring practical OT attack scenarios and their potential impacts		
Task 1: Unauthorized PLC Control Command		
Task 2 Unauthorized Write to PLC Variables		
Discovery Lab 3: Configue Catalyst 9300 for CCV Sensor deployment		
Task 1 Catalyst 9300 configuration		

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar