Cisco Cyber Vision Deployment and Operation

Duration: *3 Day(s)*

Course 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.

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

Review this course online at https://www.alta3.com/courses/INCVDO

Objectives

- Explain common vulnerabilities and security solutions in IoT deployments.
- Describe and utilize the features of the Cisco Cyber Vision software.
- Implement Cyber Vision tools to secure Industrial IoT architecture.
- Navigate and operate the Cyber Vision GUI for enhanced system protection.

Who Should Attend

- Systems Administrators and Engineers
- Technical Solutions Architects
- Systems Integrators
- Channel Partners
- Value-Added Resellers

Prerequisites

- Basic knowledge of Cisco Security.
- Sound knowledge of Internet of Things Concepts.
- Sound knowledge of IIoT Architectures.

Course Outline

Lesson 1: Industrial Internet of Things Security Threats

1. Describe security threats and potential impacts on the network
2. Understand the security challenges faced by the IIoT staff on a daily basis
3. Explain why Cisco Validated Designs lead to a more secure infrastructure
4. Describe security threats in the Extended Enterprise network

Lesson 2: Introducing Cyber Vision

5. Cybersecurity overview in IIoT deployments
6. Cyber Vision overview
7. Cyber Vision solution components
8. Cyber Vision installation procedure

Lesson 3: Cyber Vision Concepts

9. Preset
10. Filters
11. Component
12. Activity
13. Flow
14. Time span
15. Tags
16. Properties
17. Vulnerabilities
18. Events
19. Credentials
20. Variable accesses

Lesson 4: Cyber Vision GUI Exploration

21. General Dashboard
22. Preset Views
23. Panels
24. Reports
25. Events
26. Monitor
27. Search
28. Admin
29. Systems Statistics
30. My Settings

Lesson 5: Cyber Vision Operation

31. Using General Dashboard
32. Explore Preset Views and Panels
33. Examine and generate Reporting features
34. Working with Events, Alerts and Audits.
35. Using Monitor Mode and its Views
36. Describing and Exploring Monitor Mode Differences
37. Creating Baselines from default preset and from groups
38. Defining with Weekend Baselines
39. Enabling and using Baselines
40. Cyber Vision Use Cases
41. Administering Cyber Vision System and Data Management
42. Cyber Vision Center and Sensors general administration
43. Administering Users
44. Administering Events
45. Administering Licensing
46. Working with RBAC and LDAP Settings
47. Exploring and using Cyber Vision API
48. Cyber Vision Context Information Exchange with pxGrid
49. IDS functionality with SNORT
50. Cyber Vision Integrations and Extensions
51. Working with My Settings

Lab Outline

52. Lab 1: Explore Overall system architecture
53. Lab 2: Work with Asset and flow visibility
54. Lab 3: Work with Organization and viewing data in the system
55. Lab 4: Use System events to quickly identifying changes in the environment
56. Lab 5: Generate Reports for compliance and tracking
57. Lab 6: Quickly identify vulnerabilities
58. Lab 7: Use Role Based Access Control
59. Lab 8: Configure Syslog Integrations (SIEM)
60. Lab 9: Explore Cisco Cyber Vision operation and upgrade
61. Lab 10: Configure dashboard for auto-login to CV
62. Lab 11: Configure and use Packet replay and capture