Cisco CyberVision Deployment and Operation

Varighed: 3 Days **Kursus Kode: N1_INCVDO**

Beskrivelse:

INCVDO, Cisco CyberVision 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 todays 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.

Målgruppe:

The primary audience for this course is as follows:
- Systems Administrators and Engineers
- Technical Solutions Architects
- Systems Integrators
- Channel Partners
- Value-Added Resellers

Agenda:

- Upon completing this course, the learner will be able to meet these overall objectives:
- Explain the common vulnerabilities in the IoT deployments.
- Explain the cybersecurity approach for IoT architectures.
- Define the Cyber Vision main concepts.
- Describe Cyber Vision solution portfolio.
- Describe and use the Cyber Vision GUI.
- Identify and explain Cyber Vision Installation and Support procedures.
- Define Cyber Vision Assessment.
- Identify Cyber Vision Assessment components.
- Explain and use Cyber Vision Asset solution.
- Describe and use Cyber Vision API for Automation.
- Identify Cyber Vision use cases.

Forudsætninger:

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

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

Indhold:

Lesson 1: Industrial Internet of Things Security Threats

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

Lesson 2: Introducing Cyber Vision

- Cybersecurity overview in IIoT deployments
- Cyber Vision overview
- Cyber Vision solution components
- Cyber Vision installation procedure

Lesson 3: Cyber Vision Concepts

- Preset
- Filters
- Component
- Activity
- Flow
- Time span
- Tags
- Properties
- Vulnerabilities
- Events
- Credentials
- Variable accesses

Lesson 4: Cyber Vision GUI Exploration

- General Dashboard
- Preset Views
- Panels
- Reports
- Events
- Monitor
- Search
- Admin
- Systems Statistics
- My Settings

Lesson 5: Cyber Vision Operation

- Using General Dashboard
- Explore Preset Views and Panels
- Examine and generate Reporting features
- Working with Events, Alerts and Audits.
- Using Monitor Mode and its Views
- Describing and Exploring Monitor Mode Differences
- Creating Baselines from default preset and from groups
- Defining with Weekend Baselines
- Enabling and using Baselines
- Cyber Vision Use Cases
- Administering Cyber Vision System and Data Management
- Cyber Vision Center and Sensors general administration
- Administering Users
- Administering Events
- Administering Licensing
- Working with RBAC and LDAP Settings
- Exploring and using Cyber Vision API
- Cyber Vision Context Information Exchange with pxGrid
- IDS functionality with SNORT
- Cyber Vision Integrations and Extensions
- Working with My Settings

LAB OUTLINE:

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

- Lab 1: Explore Overall system architecture
- Lab 2: Work with Asset and flow visibility
- Lab 3: Work with Organization and viewing data in the system
- Lab 3: Use System events to quickly identifying changes in the environment
- Lab 4: Generate Reports for compliance and tracking
- Lab 5: Quickly identify vulnerabilities
- Lab 6: Use Role Based Access Control
- Lab 7: Configure Syslog Integrations (SIEM)
- Lab 8: Explore Cisco Cyber Vision operation and upgrade
- Lab 9: Configure dashboard for auto-login to CV

Lab 10: Configure and use Packet replay and capture

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre