Securing Industrial IoT Networks with Cisco Technologies (ISECIN)

Duration: 5 days

Course Overview

A perfect security storm is brewing with the shortage of security professionals and the additional vulnerabilities with IoT enabled infrastructures. "Securing Industrial IoT Networks with Cisco Technologies" (ISECIN) aims to narrow this talent gap and upskill security professionals to secure and defend critical IoT enabled infrastructures such as utilities, transportation and smart cities.

This course provides an overview of the IoT enabled industrial verticals (manufacturing, energy, O&G, utilities, process control), architectures, and IIoT security requirements, frameworks, and regulations. Security protocols, vulnerabilities, and the process of securing against the vulnerabilities are examined in depth and practiced in the hands-on lab environment.

Who should attend?

1. **Security Engineer**
2. **Security Operations**
3. **Security Analysts**
4. **Systems, Solutions Architects**
5. **System Integrators**
6. **Senior OT Engineers**

Course Objectives

Upon completion of this course, you will be able to:

1. **Understand the convergent enterprise and industrial IoT architecture, components and applications**
2. **Contrast enterprise IT vs. industrial OT security**
3. **Define layered security requirements from the network edge to the core, and from access to applications layer**
4. **Protect endpoints, communications as well as data at rest and in motion**
5. **Compliance to standards and regulations and auditing**
6. **Understand protocols, applications and IPv6 for IIoT**
7. **Identify vulnerabilities and threat**
8. **Familiarize with common implementation issues**
9. **Assess, monitor and detect vulnerabilities**

10. Walk through IIoT attacks
11. Adopt best practices in design principles and process for securing and segmenting IIoT networks
12. Application of the converged security model for the broader industry: manufacturing, utilities, transportation, O&G
13. Secure and monitor/detect the IIoT framework with next generation security products and tools

Course Content

Lesson 1: Describing Converged Enterprise and Industrial IoT Networks, Architectures, and Frameworks
Lesson 2: Describing Industrial IoT Network Security Requirements
Lesson 3: Describing Protocols Used in Converged Enterprise and Industrial IoT Networks
Lesson 4: Analyzing IoT Vulnerabilities
Lesson 5: Exploiting Vulnerabilities in Industrial IoT Networks
Lesson 6: Describing the Process of Securing Industrial IoT Networks
Lesson 7: Hardening Devices in Industrial IoT Networks
Lesson 8: Implementing Network Infrastructure Security in Industrial IoT Networks
Lesson 9: Describing the Characteristics of Cisco NGFWs in Industrial IoT Networks
Lesson 10: Securing Communications in in Industrial IoT Networks Using Basic Cisco NGFW and Cisco NGIPS Features
Lesson 11: Implementing Advanced Security Features on NGFW and NGIPS in Industrial IoT Networks
Lesson 12: Using the Cisco TrustSec Solution in Industrial IoT Networks
Lesson 13: Implementing VPN Solutions in Industrial IoT Networks
Lesson 14: Describing the Industrial IoT Network Framework and Regulations
Lesson 15: Bonus Content: Describing Physical Security in Industrial IoT Networks
Lesson 16: Bonus Content: Monitoring Industrial IoT Networks