

ISECIN (SECURING INDUSTRIAL IOT NETWORKS WITH CISCO TECHNOLOGIES) 1.0

Objetivo

After taking this course, you should be able to:

- Understand convergent enterprise and industrial IoT architecture, components and applications;
- Contrast enterprise IT and industrial OT security;
- Define layered security requirements from the network edge to the core, and from access to applications layer;
- Protect endpoints and communications as well as data at rest and in motion;
- Comply with standards and regulations for auditing requirements;
- Understand protocols, applications and IPv6 for IIoT;
- Identify vulnerabilities and threats;
- Address common implementation issues;
- Assess, monitor, and detect vulnerabilities;
- Walk through IIoT attacks;
- Adopt best practices in design principles and process for securing and segmenting IIoT networks;
- Apply the converged security model for the broader industry: manufacturing, utilities, transportation, O&G;
- Secure and monitor the IIoT framework with next generation security products and tools.

Público Alvo

IT and senior OT professionals currently responsible for network or OT security who are expanding their roles into IIoT initiatives.

Pré-Requisitos

We recommend that you have knowledge of one or more of the following before attending this course:

- College or advanced technical degrees with several years of experience in IT or OT;
- Solid understanding of IP networking and industrial protocols;
- Cisco CCNA® Security level of knowledge.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Course Introduction

Course Outline

Course Goals & Objectives

Describing Converged Enterprise and Industrial IoT Networks, Architectures, and Frameworks

Describing Industrial IoT Network Security Requirements

Describing Protocols Used in Converged Enterprise and Industrial IoT Networks

Analyzing IoT Vulnerabilities

Exploiting Vulnerabilities in Industrial IoT Networks

Describing the Process of Securing Industrial IoT Networks
Hardening Devices in Industrial IoT Networks
Implementing Network Infrastructure Security in Industrial IoT Networks
Describing the Characteristics of Cisco NGFWs in Industrial IoT Networks
Securing Communications in Industrial IoT Networks Using Basic Cisco NGFW and NGIPS Features
Implementing Advanced Security Features on NGFW and NGIPS in Industrial IoT Networks
Using the Cisco TrustSec® Solution in Industrial IoT Networks
Implementing VPN Solutions in Industrial IoT Networks
Describing the Industrial IoT Network Framework and Regulations
Bonus Content: Describing Physical Security in Industrial IoT Networks
Bonus Content: Monitoring Industrial IoT Networks

Lab Outline

Lab 1: Explore an Industrial IoT Network
Lab 2: Explore Industrial IoT Network Components and Identify Their Security Requirements
Lab 3: Analyze Layer 2 and Layer 3 Network Protocol Traffic in an Industrial IoT Network
Lab 4: Analyze Operations Technology Protocol Traffic
Lab 5: Explore Assets and Detect Vulnerabilities in an Industrial IoT Network
Lab 6: Insert a Rogue Device
Lab 7: Implement an Attack Against OT Assets
 Analyze Attacks Against IoT Networks
 Classify Assets and Identify Relationships Between Assets in Industrial IoT Network
Lab 8: Implement Device Hardening on Industrial Network Devices
Lab 9: Explore Network Infrastructure Security Features on Cisco Industrial Ethernet Switches
Lab 10: Explore Network Infrastructure Security Features on Cisco Industrial Ethernet Switches 2
Lab 11: Implement Cisco NGFWs in Routed Mode and in Transparent Mode in an Industrial IoT Network
Lab 12: Implement Access Control for Network Segments
Lab 13: Implement a Cisco FirePOWER™ Module with Basic Settings
Lab 14: Implement Advanced Access Control and OT Application Inspection for Network Segments
Lab 15: Implement IEEE 802.1X on Industrial Switches
Lab 16: Implement SGTs on Industrial Switches
Lab 17: Implement a Remote-Access VPN to Manage Industrial IoT Networks
Lab 18: Explore Industrial IoT Network Components and Identify the Applicable Security Standards and Regulations