



## ISE – IoT Security Essentials (e-Learning)

EC-Council

- **Nível:**
  - **Duração:** 8h
- 

### Sobre o curso

[Spring Deals: Cursos EC-Council com 5% de desconto até 30 de abril](#)

#### IoT Security Essentials (ISE)

ISE is a comprehensive guide to securing Internet of Things (IoT) systems. It covers IoT fundamentals, advanced security threats, and security engineering. No IT/Cybersecurity experience required.

Test your skills with CTF-based Capstone Project. This course provides 5 labs, 8+ hours of premium video training, and 11 modules with industry-aligned expertise.

#### Key Features:

- 5 lab practical exercises
- 8+ hours of premium self-paced video training
- 900+ pages of eCourseware
- Capstone Project
- Year-long access to courseware and 6-month access to labs
- Proctored exam voucher with 1-year validity
- Gain globally recognized EC-Council certification
- Enhance your relevancy in the job market

#### What skills you'll learn:

- Gain insights into the emergence of the Internet of Things (IoT)
  - Learn about the devices that make your home a smart home
  - Dive deep into IoT communication models
  - Understand information security threats and vulnerabilities
  - Gain a deep understanding of IoT networking and communication
  - Understand cloud computing in depth
  - Learn about the different types of threats to IoT
-

# Destinatários

## Who is I|SE for?

- High School/College/University students
  - Teams and organizations
  - Career starters
  - Working professionals
- 

## Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

---

## Metodologia

**Training Details:** Self-paced in-demand lecture videos led by world-class instructors and hands-on labs.

### Exam Details:

- Exam Code: 112-58
  - Number of Questions: 75
  - Duration: 2 hours
  - Test Format: Multiple Choice
- 

## Programa

- IoT Fundamentals
- IoT Networking and Communication
- IoT Processors and Operating Systems
- Cloud and IoT
- IoT Advanced Topics
- IoT Threats
- Basic Security
- Cloud Security
- Threat Intelligence
- IoT Incident Response
- IoT Security Engineering

### IoT Fundamentals

This module will introduce you to the basics of IoT and the different sectors where IoT is established.

### IoT Networking and Communication

This module will provide insights into the basics of networking concepts, the OSI Model, and the TCP Model. It will also cover the IEEE IoT Standards List.

### **IoT Processors and Operating Systems**

This module will help you understand the hardware devices, processors, and operating systems used in IoT.

### **Cloud and IoT**

This module will teach you about cloud computing, its characteristics, and the types of cloud services.

### **IoT Advanced Topics**

This module will brief you about web communications, mobile applications, and native applications.

### **IoT Threats**

This module will introduce you to some of the common IoT attacks, such as Mirai, BrikerBot, Sybii, and Blackhole attacks.

### **Basic Security**

This module will discuss the CIA triangle, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and IoT security measures.

### **Cloud Security**

This module will discuss the state of cloud security, cloud vulnerabilities, NSA guidance, and secure cloud computing.

### **Threat Intelligence**

This module will start with the topic of the National Vulnerability Database, covering US Cert, Shodan, STRIDE, DREAD, PASTA, and CVSS.

### **IoT Incident Response**

This module will provide information on incident response in IoT, including standards, processes, procedures, tools, and indicators of compromise.

### **IoT Security Engineering**

This module will cover the 12 practices of the Microsoft Secure Development Lifecycle and Threat Modeling.