

IoT Security Essentials (ISE)

Course Duration: 5 Days

Course overview

EC-Council's IoT Security Essentials Series provides comprehensive coverage of essential topics in securing Internet of Things (IoT) systems. From understanding the fundamental concepts of IoT to addressing advanced security threats, students will gain the knowledge and skills necessary to design, deploy, and maintain secure IoT solutions. Through a combination of theoretical learning and hands-on exercises, participants will explore IoT fundamentals, networking and communication protocols, cloud integration, threat intelligence, incident response, and security engineering principles. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

Ultimately, students will be equipped with the expertise needed to effectively identify, assess, and mitigate security risks in IoT environments, ensuring the integrity, confidentiality, and availability of IoT systems and data.

Target Audience

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- Individuals who want to start a career in cybersecurity and are interested in IoT Security.
- Anyone interested in gaining in-depth knowledge on safeguarding their smart devices or those within their organization

What you will 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.
- Gain a deep understanding of IoT networking and communication.
- Understand cloud computing in depth.
- Learn about the different types of threats to IoT.

Course Outline

| Module # | Module Topic | Description |
|-----------|--------------------------------------|---|
| Module 01 | IoT Fundamentals | This module will introduce you to the basics of IoT and the different sectors where IoT is established. |
| Module 02 | 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. |
| Module 03 | IoT Processors and Operating Systems | This module will help you understand the hardware devices, processors, and operating systems used in IoT. |
| Module 04 | Cloud and IoT | This module will teach you about cloud computing, its characteristics, and the types of cloud services. |
| Module 05 | IoT Advanced Topics | This module will brief you about web communications, mobile applications, and native applications. |
| Module 06 | IoT Threats | This module will introduce you to some of the common IoT attacks, such as Mirai, BrikerBot, Sybii, and Blackhole attacks. |
| Module 07 | Basic Security | This module will discuss the CIA triangle, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and IoT security measures. |
| Module 08 | Cloud Security | This module will discuss the state of cloud security, cloud vulnerabilities, NSA guidance, and secure cloud computing. |

| | | |
|-----------|--------------------------|--|
| Module 09 | Threat Intelligence | This module will start with the topic of the National Vulnerability Database, covering US Cert, Shodan, STRIDE, DREAD, PASTA, and CVSS. |
| Module 10 | IoT Incident Response | This module will provide information on incident response in IoT, including standards, processes, procedures, tools, and indicators of compromise. |
| Module 11 | IoT Security Engineering | This module will cover the 12 practices of the Microsoft Secure Development Lifecycle and Threat Modeling. |

Key Features

- Engage in 5 lab practical exercises in modules that provide you with a practical understanding of how you can secure your smart devices.
- Get 8+ hours of premium self-paced video training.
- 900+ pages of ecourseware.
- Capstone Projects with Real-World CTF Challenges
- Gain a year-long access to courseware and 6-month access to labs.
- Acquire a proctored exam voucher with one-year validity.
- Enhance your relevancy in the job market to advance your career.
- Gain the globally recognized EC-Council's certification.

Exam Details:

| Exam Details | ISE (Exam 112-58) |
|---------------------|------------------------------|
| Number of Questions | 75 |
| Test Duration | 2 Hours |
| Test Format | Multiple Choice |
| Test Delivery | ECC Exam Portal |
| Passing Score | Score should be at least 70% |