IoT Security Essentials

Course Duration: 16 Hrs. **Course code: 112-58**

Course Overview

The IoT Security Essentials (I|SE) is a comprehensive guide to securing the Internet of Things (IoT) systems. It covers essential topics from IoT fundaments to advanced security threats and security engineering, providing the knowledge and skills to design, deploy, and maintain secure IoT solutions.

What you'll learn?

- **IoT Fundamentals:**
  Understand the basics of the Internet of Things, including its architecture, components, and various use cases.
- **IoT Security Landscape:**
  Gain insights into the emergence of IoT and the associated security challenges and threats.
- **IoT Architecture & Threats:**
  Learn about the structure of IoT systems and identify common security threats and vulnerabilities specific to connected devices and networks.

Target Audience

- **Students and Graduates:**
  Individuals pursuing or recently completed studies in IT, cybersecurity, or related fields.
- **Professionals:**
  Those already working in IT, technology, or cybersecurity roles who want to expand their knowledge and skills in IoT security.
- **Career Starters and Switchers:**
  Individuals looking to enter or transition into cybersecurity careers, particularly those interested in IoT security.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Pre-Requisites

For EC-Council's IoT Security Essentials (ISE) course, there are no formal prerequisites, meaning no prior cybersecurity knowledge or IT experience is required.

Course content

Module 1: IoT Fundamentals

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

Module 2: 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 3: IoT Processors and Operating Systems

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

Module 4: Cloud and IoT

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

Module 5: IoT Advanced Topics

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

Module 6: IoT Threats

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

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Module 7: Basic Security
This module will discuss the CIA triangle, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and IoT security measures.

Module 8: Cloud Security
This module will discuss the state of cloud security, cloud vulnerabilities, NSA guidance, and secure cloud computing.

Module 9: 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.

Exam Preference

Exam Code	112-58
Length Of Test	120 Minutes
Number Of Questions	75
Passing Score	70%

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com