IOT Security Course

Course Duration: 16 Hrs. **Course Code: IOT-SEC-101**

Course Overview

The **IoT Security** course is designed for IT, security, and IoT professionals responsible for securing Internet of Things (IoT) devices and networks. This course covers the unique challenges of IoT security, including device vulnerabilities, network threats, and data privacy concerns. Participants will learn best practices for protecting IoT ecosystems, implementing security controls, and ensuring compliance with industry standards while gaining hands-on experience with real-world IoT security scenarios.

What You'll Learn?

By completing this course, you will be able to:

- Understand the architecture and components of IoT ecosystems
- Identify IoT security threats, vulnerabilities, and attack vectors
- Implement device-level, network-level, and application-level security controls
- Secure communication protocols and data transmission
- Monitor IoT networks for anomalies and security incidents
- Apply risk assessment, governance, and compliance best practices
- Develop an IoT security strategy for enterprise environments

Target Audience

This course is ideal for:

- IoT Security Engineers and Administrators

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

- Network and Security Engineers managing IoT environments
- SOC Analysts monitoring IoT networks
- IT Infrastructure and IoT Solution Architects
- Professionals responsible for securing connected devices and systems

Pre-Requisites

Participants should have:

- Basic understanding of networking, cybersecurity, and IoT concepts
- Familiarity with network protocols and endpoint devices
- Knowledge of risk management and compliance is recommended

Course Content

Module 1: Introduction to IoT Security

- IoT ecosystem overview
- IoT architecture and components
- Security challenges in IoT environments

Module 2: Threats and Vulnerabilities

- Common IoT attacks and threat actors
- Vulnerability assessment for IoT devices
- Case studies of IoT security breaches

Module 3: Device Security

- Secure device configuration and firmware management
- Authentication and access control for IoT devices

- Endpoint protection for IoT

Module 4: Network Security for IoT

- Securing communication protocols (MQTT, CoAP, HTTP/HTTPS)
- Network segmentation and IoT gateways
- Intrusion detection and anomaly monitoring

Module 5: Data Protection and Privacy

- Data encryption at rest and in transit
- Secure storage and cloud integration
- Privacy and regulatory compliance

Module 6: Risk Management and Best Practices

- Risk assessment and mitigation strategies
- IoT security frameworks and standards
- Operational best practices for enterprise IoT security