Security Incident Response (SIR) Implementation

Course Duration : 32 Hours **Course code : SN-SIR-IMP-301**

1. Course Overview

The **Security Incident Response (SIR) Implementation** course focuses on implementing and managing security incident response processes using the ServiceNow SIR module. This course helps organizations detect, investigate, and resolve security incidents efficiently while improving coordination between security and IT teams.

2. What you'll learn?

- Security Incident Response framework
- SIR module architecture
- Incident detection and intake
- Investigation and response workflows
- Automation and integrations
- Reporting and compliance tracking

3. Target Audience

- Security operations teams
- SOC analysts
- Incident response managers
- ServiceNow implementers
- IT security professionals

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

4. Pre-Requisites

- Basic understanding of cybersecurity concepts
- Familiarity with ServiceNow platform
- Knowledge of incident management processes

5. Course Content (Modules)

Module 1: Introduction to Security Incident Response

- SIR overview
- Incident lifecycle

Module 2: Incident Intake and Detection

- Alert ingestion
- Threat intelligence integration

Module 3: Investigation and Response

- Incident analysis
- Containment and remediation

Module 4: Automation and Orchestration

- Playbooks and workflows
- Integration with security tools

Module 5: Reporting and Compliance

- Dashboards and metrics
- Compliance and audit support