EC-Council Certified

SOC Analyst

Training Brochure

Noida Address: B 77-78 2nd Floor Sec. 6 Noida 201301

Noida Address: B 106 2nd Floor Sec. 6 Noida 201301

Karol Bagh Address: 16/8 3rd Floor Karol Bagh New Delhi 110005

For queries on Training, please contact the undersigned:-

Nikita Bhasin 9310719612

Silicon Univ EC-Council Accredited Training Centre- Training Arm of Silicon Comnet Pvt. Ltd.

EC-Council Certified SOC Analyst Training Details:-

- **Duration: 30 Hours**
- **Mode: Hybrid (Online/Classroom)**
- **Classes: Weekdays/Weekends/Evening**

Silicon Univ EC-Council Accredited Training Centre- Training Arm of Silicon Comnet Pvt. Ltd.

COURSE CONTENTS

EC-COUNCIL CERTIFIED SOC ANALYST

Modules	Topics
Module 1	**Security Operations and Management**
	Security Management
	Security Operations
	Security Operations Centre (SOC)
	Need of SOC
	SOC Capabilities
	SOC Operations
	SOC Workflow
	Components of SOC
	Type of SOC Models
	SOC Implementation
	Challenges in implementation of SOC
Module 2	**Understanding Cyber Threats, IoCs, and Attack Methodology**
	Cyber Threats
	Intent- Motive- Goal
	Tactics- Techniques-Procedures (TTP)
	Opportunity-Vulnerability- Weakness
	Network, Host, and Application Level Attacks
	Cyber Threats IoC's
	Hacking Methodologies
Module 3	**Incidents, Events and Logging**
	Log, Event, and Incident
	Typical Log Sources
	Need of Log
	Logging Requirements
	Typical Log Format
	Local Logging
	Centralized Logging
	Centralized Logging Challenges
Module 4	**Incident Detection with Security Information and Event Management (SIEM)**

	Security Information and Event Management (SIEM)
	Need of SIEM
	Typical SIEM Capabilities
	SIEM Architecture and its components
	SIEM Deployment
	Incident Detection with SIEM
	Use case examples of Application Level Incident Detection
	Use case examples of Insider Incident Detection
	Use case examples of Network Level Incident Detection
	Use case examples of Host Level Incident Detection
	Handling Alert Triaging and Analysis
Module 5	**Enhanced Incident Detection with Threat Intelligence**
	Cyber Threat Intelligence (CTI)
	Types of Threat Intelligence
	Threat Intelligence-driven SOC
	Benefit of Threat Intelligence to SOC Analyst
	Threat Intelligence use cases for SOC Analyst
	Integration of Threat Intelligence into SIEM
	Threat Intelligence use cases for Enhanced Incident Response
	Enhancing Incident Response by establishing SOP's for Threat Intelligence
Module 6	**Incident Response**
	Incident Response
	SOC and IRT Collaboration
	Incident Response (IR) Process Overview
	Responding to Network Security Incidents
	Responding to Application Security Incidents
	Responding to Email Security Incidents
	Responding to an Insider Incidents
	Responding to Malware Incidents