ENGINEERING STAFF COLLEGE OF INDIA

Autonomous Organ of The Institution of Engineers (India)
ISO 9001:2015 Certified, AICTE & CEA Recognized Institution
4 Decades of Excellence in Nation Building

ESCI

PROFESSIONAL DEVELOPMENT PROGRAM

Security Operations Center (SOC) Analyst

Monitoring | Detecting | Investigating | Responding to Cyber Threats

Key Focus Areas

- SOC Fundamentals & Operations
- Threat Detection and Analysis
- Incident Response & Investigation
- SOC Tools (SIEM, EDR, IDS/IPS, SOAR)
- Log Analysis, Threat Hunting & Threat Intelligence
- Hands-on Labs, Use Cases & Best Practices



28 – 31 Dec 2026

IEI Centre, Visakhapatnam, AP



Introduction

The **Security Operations Center (SOC) Analyst** training program is designed to develop practical skills for monitoring, detecting, analyzing, and responding to cybersecurity threats. Participants will gain exposure to SOC operations, security monitoring, SIEM tools, log analysis, threat intelligence, and incident response. The program emphasizes hands-on techniques for identifying suspicious activities and investigating security incidents. It also covers best practices for protecting organizational IT infrastructure and data from evolving cyber threats

Objective

- Understand the Security Operation Center (SOC) team operations
- Understand Blue Team operations architecture
- In-depth knowledge of digital forensics, threat intelligence, and incident response
- Understand technical strategies, tools, and procedures to safeguard data for your organization
- Understand essential SOC tools like Splunk and Security Onion
- Understand how to recognize threats and implement countermeasures

Course Content

Introduction to SOC

- Building a successful SOC
- Functions of SOC
- SOC Models & Types
- SOC Teams & Roles
- Heart of SOC- SIEM
- SIEM guidelines and architecture

SOC Tools

- Industrial requirements of Splunk in various fields
- Splunk terminologies,
- Splunk universal forwarder
- Introduction to Security Onion NSM
- Security Onion Architecture
- Walkthrough to Analyst Tools
- Alert Triage and Detection
- Hunt with Onion

Fundamentals of Digital Forensics

- Forensics Fundamentals
- Introduction to Digital Forensics
- Digital Evidence First Responder Procedures
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files
- Forensics Investigation Using Access Data FTK & EnCase
- Memory Forensics
- Investigating Web & Mail Attacks
- Email Forensics: Manual & Automated Analysis
- Network Security
- Log Capturing and Event Correlation
- Tools for fingerprinting
- Network Analysis: Wireshark, Network Miner
- Port scanning & Network Traffic

Incident Response Basics

- Introduction to Incident Response
- Security Events vs. Security Incidents
- Incident Response Lifecycle
- Incident Response Plan
- Lockheed Martin Cyber Kill Chain
- Incident Response Plans, Policies, and Procedures
- The Need for an IR Team
- Asset Inventory and Risk Assessment to Identify High-Value Assets
- DMZ and Honeypots
- Host Defences
- HIDS, NIDS
- Antivirus, EDR

Detection and Analysis

- Common Events and Incidents
- Establishing Baselines and Behavior Profiles
- Central Logging (SIEM Aggregation)
- Analysis (SIEM Correlation)

Containment, Eradication, Recovery

- CSIRT and CERT Explained
- Containment Measures
- Network Isolation, Single VLAN,
- Powering System(s) Down, Honeypot Lure
- Taking Forensic Images of Affected Hosts
- Linking Back to Digital Forensics Domain
- Identifying and Removing Malicious Artefacts
- Memory and disk analysis to identify artefacts and securely remove them
- Identifying Root Cause and Recovery Measures

Introduction to Threat Intelligence

- Threat Actors
- Types of Threat Intelligence :
- Operational Intelligence
- Strategical Intelligence
- Tactical Intelligence
- CTI Skills: NIST NICE – CTI Analyst
- OODA Loop, Diamond Model of Intrusion Analysis
- Unleashing Threat Intel with Maltego, AlienVault OTX
- LOTL Based Techniques
- Malware Campaigns & APTs

Methodology

Methodology of the programme includes class room sessions with Lecture / Discussion with Hands- on Practical, with tools, audio visual aid, bench marked video shows, Chalk & Talk sessions, group discussions, case studies, debates, sharing of experiences etc. All the sessions will be interactive demanding active participation from all the members.

Target Participants

- System Administrators / Network Administrators/ IT Managers / Technical Support Engineers
- IT Professionl of DRDO /DGQA /Defence / Forensic Labs
- Cyber Security Analysts, Security System Engineers, SOC Analysts (L1 & L2)
- The program is designed for all IT professionals involved with information system security, computer forensics, and incident response

Course Director

Mr. Syed Azgar , MBA(IT), RHCE, MCSA,
Sr Faculty & Head IT,
Information Technology Division,

Course Fee

- ₹ **40,000/- (Residential Fee)** per participant. Fee includes Single / Double AC accommodation as per the availabulity, course material, course kit, Breakfast. Lunch, Dinner, Tea / Coffee and Snacks during the actual days of the training program.
- ₹ **30,000/- (Non Residential Fee)** per participant. Fee includes, course material, course kit, Lunch, Tea / Coffee and Snacks during the actual days of the training program.

GST @18% is to be paid extra and above the training fee as training. **PAN Card No.** AAATT3439Q. **GST No: 36AAATT3439Q1ZV, HS No.: 999293** (under commercial training or coaching services – clause 65(105) (ZZC) of Finance act – 1994).

Programme fee is to be paid in in favour of **"THE INSTITUTION OF ENGINEERS (INDIA) – ENGINEERING STAFF COLLEGE OF INDIA"** by **Electronic Fund Transfer (EFT)** to ESCI – **Axis Bank** A/c No. **912010049234564** with The Axis Bank Ltd, Old Mumbai Hwy, Cyberhills Colony, P Janardhan Reddy Nagar, GachiBowli Hyderabad-500032 by NEFT/ RTGS/ IFSC Code No. UTIB 0000733 – MICR No.500211020. **While using EFT method of payment, please ensure to communicate us your company name, our invoice reference and programme title.**

Registration

To register manually please send your nominations giving details of name, designation, contact address, email address, mobile no, telephone and fax number of the participant along with the details of mode of payment of fee, addressed to : **it@escihyd.org**

A Certificate of participation will be awarded to each participant on conclusion of the programme.

Glimpses of our Recent Programmes





Information Technology Division, Engineering Staff College of India
Gachi Bowli, Hyderabad – Telangana 500 032
Phone: 040 – 66304100 (EPABX), 66304123/24/25 (Direct), 8886661060 Fax: 040 – 66304103
Email: it@escihyd.org, **web portal**: www.escihyd.org