Engineering Staff College of India

Autonomous Organ of The Institution of Engineers (India)

Old Bombay Road, Gachi Bowli, Hyderabad – 500 032. Telangana, India

INFORMATION TECHNOLOGY DIVISION

PROFESSIONAL DEVELOPMENT PROGRAMME

Security Operation Centre(SOC) Analyst

19 - 23 August 2024

Introduction

A Security Operation Center(SOC) Analyst is primarily responsible for all activities that occur within the SOC. Analysts in Security Operations work with Security Engineers and SOC Managers to give situational awareness via detection, containment, and remediation of IT threats. With the increment in cyber threats and hacks, businesses are becoming more vulnerable to threats. This has significantly enhanced the importance of a SOC Analyst. For those in cybersecurity, it can be a dynamic role. SOC Analysts cooperate with other team members to detect and respond to information security incidents, develop and follow security events such as alerts, and engage in security investigations. Furthermore, SOC Analysts analyze and react to undisclosed hardware and software vulnerabilities. They also examine reports on security issues and act as ‘security advisors’ for an organization.

Objectives

This SOC Analyst training course allows you to:

- 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

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

Methodology

Methodology of the programme includes

- Class room sessions with Lecture / Discussion
- Hands- on Practical Training , 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

Course Coverage

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

.

Benefits to the participants

- Enables Participants to practice various investigation techniques in a real time and a simulated environment
- The course tools and programs are preloaded on the **Cyber Security Labs** machine, thereby saving productive time and effort.

Programme Dates & Timings

Dates: 19 – 23 August 2024 (6 Hours per day)
Venue for Offline Training : Engineering Staff College of India, Gachibowli, Hyderabad
Session timings will be from 10:00 – 17:00 hrs with 15 Minutes Tea break., One Hrs Lunch Break

Course Director

Mr. Syed Azgar , MBA(IT), RHCE, MCSA
Sr Faculty & Head IT,
Information Technology Division,
Engineering Staff College of India, Hyderabad.

Course Fee

₹ **27,500/- (Residential Fee)** per participant. Fee includes course material, course kit, Single AC/ Double accommodation as per availability, Breakfast, Lunch, Dinner, 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"** in the form of demand draft payable at Hyderabad. Alternatively the payment may be made 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

Online registration shall be available on ESCI **web portal** https://escihyd.org/division/it

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.