CYBERVIE.COM
A CYBER SECURITY FIRM

## Cybervie Security Operation Center Training Program (SOC)

Duration of the course: **4 Weeks**

Fees of the course: ₹ **25000/-**

Eligibility: **Graduated with Good communication skills**

Batch Time: **1st of every month**

## Course Content

### Week 1 Security Basics and SOC Fundamentals

An extensive coverage of operating systems and networking basics with introduction to Cybersecurity program.
Various Topics including GRC, Vulnerability management, IDAM and perimeter security. Theoretical and Hands-on experience on leading SIEM solutions in the market.

### Week 2 Incident Response

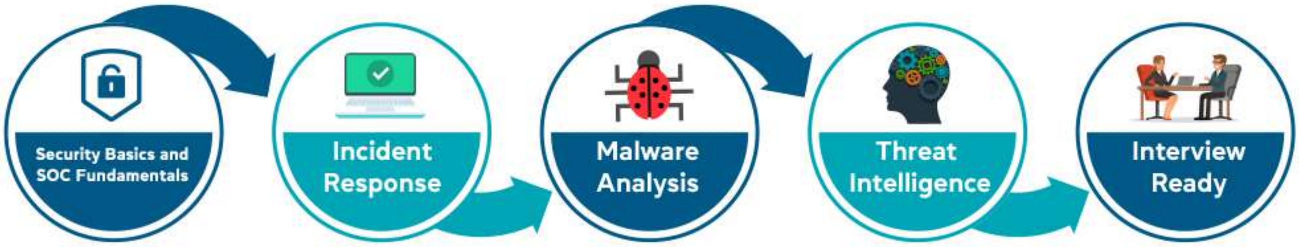
Diving deeper into the enterprise environment by using advanced SIEM features. Effective utilization of IDPS devices. Learning and handling different types of security incidents and attacks with industry recognized security frameworks

### Week 3 Malware Analysis and Forensics

Introduction to Windows Forensics with real time investigative examples. Understanding of malware types, categories, and modern analysis techniques. Hands-on knowledge on modern debugging software and analyzing malware using OSINT and sandbox technologies.

### Week 4 Cyber Threat Intelligence

Introduction to Threat Intel program, terminologies, tools, frameworks and reporting structure.
Hands-on knowledge on YARA,SIGMA and Threat intelligence platforms.

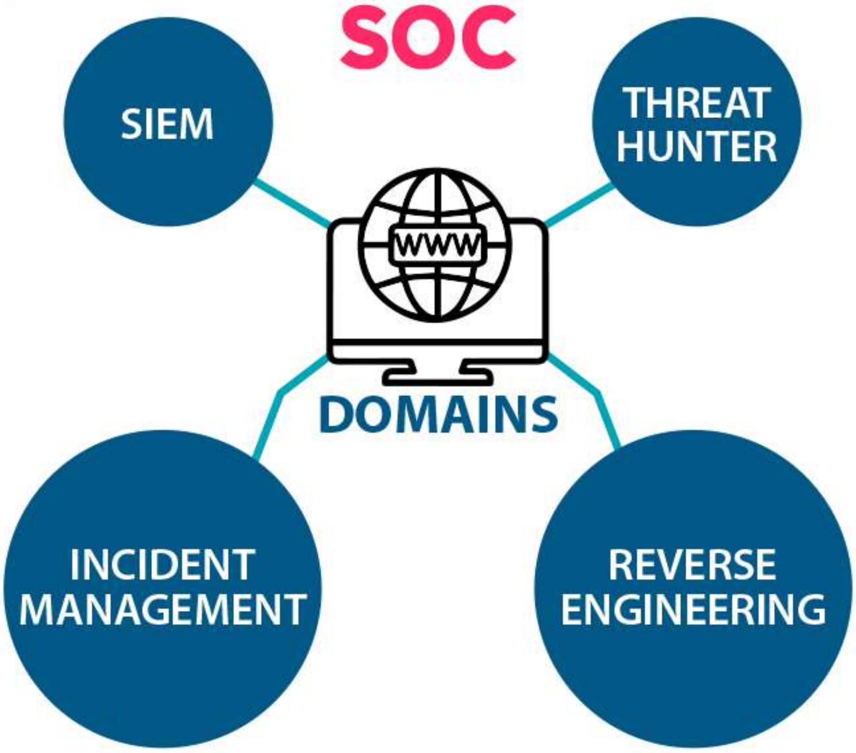


## What is a Security Operations Center (SOC)?

A Security Operation Center (SOC) is a primary function within an organization building processes, employing people and implementing technologies to continuously keep track and improve the organization's security system while warding off, detecting, examining and responding to the cybersecurity incidents.

The responsibility of a security operations center (SOC), is to examine, discover, investigate, and grapple with the cyberthreats around the clock. The SOC is usually led by a SOC manager, and usually includes an incident responder, SOC Analysts (levels 1, 2 and 3), threat hunters, reverse engineering, malware analysis. The SOC is accountable to the CISO, who in turn is to either the CIO or directly to the CEO.

## Domains under SOC



## Functions of a SOC

- To gauge the accessible resources
- Receptive and preventative maintenance
- Incessant and prudent monitoring
- Alert scaling and management
- Threat and risk response
- Recoupment and remediation
- Log Management
- Root cause probe
- Security refinement and advancement
- Compliance management

## Roles under SOC

### Level 1 (Support Security Analyst) 0 to 1 year experience

It receives and examines the alerts
Evaluates the SIEMs alerts and inspects their relevance and exigency
Carries out triage to ensure authenticity of the occurence
Govern the security monitoring tools

### Level 2 (Support Security Analyst) 2 to 5 year experience

Maneuvers the real security incidents and assess the affected system and measures the degree of attack Carries out meteculosly the threat intellegience analysis to discover the perpetrator and the pattern of attack

### Level 3 (Security Analyst) 5+ year experience

Tackle the critical incidents and carry out the vulnerability assessments
Implement the penetration tests to evaluate the pliability of the organisation
Scrutunize the alerts, threat intellegience, and security data

## Why is SOC important?

The cyber threat industry is developing rapidly, and preventing the world from potential cyberattacks requires continuous surveillance and quick response. The longer a cybersecurity incident takes to resolve before it is remediated, the greater the likely impairment and cost to the organization.

Addressing these threats is the accountability of an organization's Security Operations Center (SOC). The SOC should provide unceasing monitoring for cyber threats and the ability to implement instantaneous strategy in incident response.

## Who is this course for?

For those who are interested in a career in the SOC domains

Security managers keen to master the skill of how to construct and manage efficiently the SOC Operations and get a more practical understanding of its functioning

Security experts from other domains that want to get a foundational understanding of how the SOC operates and their various activities

Universities that want to have their students 'valued industry professionals', with domain subjects which lead to industry certifications