SECURITY OPEREATION CENTER(SOC)

What is Sco?

A security operations center, or SOC, is a team of IT security professionals that protects the organization by monitoring, detecting, analyzing, and investigating cyber threats. Networks, servers, computers, endpoint devices, operating systems, applications and databases are continuously examined for signs of a cyber security incident. The SOC team analyzes, feeds, establishes rules, identifies exceptions, enhances responses and keeps a look out for new vulnerabilities.

➤ Life cycle of Soc:

1.Log collection

2.Aggregation correlation

3. Siem

4. Ticketing

5.knowlegde base

6. Threat intelligence

7.Reasearch and development

8. reporting

➤ Explain each of them in a life cycle

1. Log collection:

Log collection is the process of gathering logs or records of events that occur within an information system, such as network devices, servers, applications, and security devices. These logs contain valuable information that can be used for troubleshooting, monitoring, security analysis, and compliance purposes.

2. Aggregation correlation:

Aggregation correlation refers to the process of combining and analyzing multiple data sources or logs to identify patterns, trends, and relationships between different events

or entities. By correlating data from various sources, organizations can gain deeper insights into their systems, detect anomalies, and identify potential security threats or operational issues.

3. SIEM (Security Information and Event Management):

SIEM is a software solution that provides real-time analysis of security alerts generated by various network devices and applications. It aggregates log data from multiple sources, correlates events, and generates alerts for suspicious activities or security incidents. SIEM systems play a crucial role in threat detection, incident response, and regulatory compliance.

4. Ticketing:

Ticketing systems are used to manage and track issues, tasks, or requests within an organization. When an incident or problem is identified, a ticket is created to document the issue, assign responsibility, track its progress, and ensure timely resolution. Ticketing systems help streamline communication, prioritize work, and maintain accountability.

5. Knowledge base:

A knowledge base is a centralized repository of information that contains articles, documents, guides, FAQs, troubleshooting tips, and other resources related to a particular subject or domain. Knowledge bases are used to store and share knowledge within an organization, enabling employees to find answers to common questions, resolve issues independently, and improve productivity.

6. Threat intelligence:

Threat intelligence refers to information about potential or actual cybersecurity Threats, including tactics, techniques, procedures, indicators of compromise (IOCs)Vulnerabilities, and attacker motivations. Threat intelligence sources may include.Open-source feeds, commercial vendors, government agencies, and internalResearch. By leveraging threat intelligence, organizations can better understand theirThreat landscape, anticipate attacks, and improve their security posture.

7. Research and development:

Research and development (R&D) involves activities aimed at creating newProducts, services, technologies, or processes through systematic investigation andExperimentation. In the context of cybersecurity, R&D efforts may focus onDeveloping innovative security solutions, improving detection capabilities, enhancingEncryption algorithms, or studying emerging threats and attack techniques.

8. Reporting:

Reporting involves the creation and dissemination of structured information orAnalysis to communicate key insights, findings, or performance metrics toStakeholders within an organization. In cybersecurity, reporting may includeGenerating compliance reports for regulatory purposes, presenting incident responseMetrics to management, or sharing threat intelligence summaries with securityTeams. Effective reporting helps decision-makers understand the state ofCybersecurity within the organization and make informed decisions.