Stage 3:

Title: **The Role of SOC and SIEM in Strengthening Cybersecurity Defense.**

- Security Operations Center (SOC)

A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats in real time. It plays a crucial role in strengthening an organization's cybersecurity defense by ensuring that potential security incidents are identified and addressed quickly. - SOC Cycle

Monitoring: The SOC provides continuous monitoring of an organization's networks, systems, and data. This ensures that any potential security breaches or anomalies are detected as soon as they occur, regardless of time zones or working hours.

Threat Detection: Using various tools and techniques, such as intrusion detection systems (IDS), endpoint detection, and other security technologies, the SOC analyzes network traffic, logs, and events for any signs of malicious activity. It can identify various types of threats, including malware, ransomware, phishing, insider threats, and more.

Incident Response: Once a threat is identified, the SOC team is responsible for investigating and responding to the incident. This includes containment (limiting the damage), eradication (removing the threat), and recovery (restoring systems to normal operation).

Security Event Management: The SOC collects and analyzes security data from various sources, including firewalls, network devices, servers, and applications. It performs real-time analysis to identify patterns and potential threats, and stores this data for future analysis and compliance.

Vulnerability Management: The SOC works closely with other teams to identify and patch vulnerabilities in the organization's systems. This can include regular vulnerability scans and applying patches to software and hardware to reduce the attack surface.

- Security Information and Event Management (SIEM)

SIEM stands for **Security Information and Event Management**. It is a comprehensive solution that combines both **Security Information Management (SIM)** and **Security Event Management (SEM)** functionalities. The primary goal of a SIEM system is to provide real-time analysis and visibility of an organization's security events to help detect, monitor, and respond to potential security threats.

- SIEM Cycle

The SIEM cycle involves a series of steps that enable efficient threat detection and management. It consists of:

1. Data Collection – Gathering log data from various security devices, applications, and endpoints.

2. Normalization & Correlation – Structuring collected data and correlating events to identify patterns.

3. Threat Detection – Analyzing logs to detect anomalies, suspicious activities, or known attack patterns.

4. Alerting & Incident Response – Generating alerts based on risk severity and initiating incident response actions.

5. Investigation & Forensics – Conducting in-depth analysis to understand attack methodologies.

6. Compliance & Reporting – Generating reports for audits, compliance, and post-incident reviews.

By implementing an effective SIEM cycle, organizations can proactively defend against cyber threats and improve security posture.

- MISP (Malware Information Sharing Platform & Threat Sharing)

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed to help organizations share, store, and collaborate on cybersecurity threat data. MISP is widely used by security professionals to improve their collective understanding of cyber threats, enabling more proactive defense measures and faster responses to emerging threats.

- College Network Information

At DYP-ATU, Talsande, the campus network comprises various interconnected systems, including faculty and student portals, learning management systems, research databases, and administrative servers. The network is secured using basic firewall configurations, access controls, and antivirus software. However, the increasing reliance on digital platforms and cloud services introduces security risks such as phishing attacks, unauthorized access, and malware infections. Strengthening cybersecurity infrastructure through advanced security measures like SOC and SIEM would significantly enhance network protection.

- Deploying SOC in College Network

Deploying a SOC at DYP-ATU would involve the following steps:

1. Infrastructure Assessment – Identifying critical assets, data storage points, and potential security vulnerabilities.

2. Implementing SIEM – Deploying a SIEM solution to collect logs from college servers, student and faculty portals, and security devices.

3. Real-time Monitoring – Setting up continuous threat monitoring using intrusion detection systems (IDS) and firewalls.

4. Incident Response Plan – Establishing a dedicated team to handle cyber incidents and conduct forensic analysis.

5. Security Awareness Training – Educating students and faculty about cybersecurity best practices to reduce human-related risks.

Integrating SOC in the college environment would improve network visibility, enhance threat detection, and minimize security risks.

- Threat Intelligence

Threat Intelligence refers to the collection, analysis, and sharing of information about potential or existing cyber threats to help organizations proactively protect themselves against malicious activities. It involves identifying indicators of compromise (IOCs), understanding attack methods, and predicting potential threats based on current data and trends. Threat intelligence is essential for enhancing an organization's ability to prevent, detect, and respond to cyberattacks.

Threat intelligence is categorized into three types:

Strategic – High-level threat reports for decision-makers.

Tactical – Analysis of attacker tactics, techniques, and procedures (TTPs).

Operational – Real-time indicators of compromise (IoCs) to respond to threats quickly.

Integrating threat intelligence into SOC and SIEM enhances an organization’s ability to detect and mitigate cyber threats effectively.

-Incident Response

Incident response is the process of managing and mitigating cybersecurity incidents to minimize damage and recover from attacks efficiently. An effective incident response plan (IRP) consists of:

1. Preparation – Establishing policies, training staff, and setting up response teams.
2. Detection & Analysis – Identifying incidents through SIEM alerts and log analysis.
3. Containment & Eradication – Isolating affected systems and removing threats.
4. Recovery – Restoring systems to normal operations.

- QRadar & Understanding the Tool

IBM QRadar is a leading SIEM solution that helps organizations detect, investigate, and respond to security threats in real time.

It provides:

1.Log Management – Aggregating security logs from multiple sources.

2.Behavioral Analytics – Detecting anomalies based on user and system behavior.

3.Automated Threat Detection – AI-driven analysis to identify potential attacks.

4.Integration with Threat Intelligence – Correlating external threat data with internal logs for enhanced security.

Understanding QRadar’s functionalities allows cybersecurity teams to effectively manage security events and mitigate risks efficiently.