1.1 Understanding of Exploring Cyber Security :

Cybersecurity has become a critical concern in the digital era, where cyber threats such as malware, ransomware, phishing, and advanced persistent threats (APTs) continue to evolve. To protect digital assets, organizations implement robust security solutions like Security Operations Centres (SOC) and Security Information and Event Management (SIEM) tools to detect, analyse, and respond to threats in real time.

1. Security Operations Center (SOC) :

A Security Operations Center (SOC) is a centralized unit responsible for monitoring, detecting, investigating, and responding to cybersecurity incidents. It functions as the frontline defence against cyber threats by continuously analysing network activity and responding to potential attacks.

2. Security Information and Event Management (SIEM)

SIEM (Security Information and Event Management) is a cybersecurity solution that collects, analyses, and correlates security data from different sources to detect potential threats and ensure compliance.

3. Related Cybersecurity Tools

In addition to SOC and SIEM, various cybersecurity tools enhance digital security:

Intrusion Detection & Prevention Systems (IDS/IPS):

- Snort (open-source IDS/IPS)
- Suricata (real-time threat detection)

Vulnerability Scanners:

- Nessus (detects security vulnerabilities)
- OpenVAS (open-source vulnerability assessment)

Endpoint Detection & Response (EDR):

- CrowdStrike Falcon (AI-driven endpoint security)
- Microsoft Defender ATP (integrated threat protection)