SOC FUNCTION

A Security Operations Center (SOC) plays a critical role in safeguarding an organization's digital ecosystem. Its functions revolve around continuous monitoring, detection, analysis, and response to cyber threats. Let's break down the key functions:

1️⃣ Collect Telemetry Data from Available Resources

The SOC aggregates telemetry data from various sources like firewalls, intrusion detection/prevention systems, endpoint security tools, SIEMs, cloud platforms, and application logs.

- This data acts as the "eyes and ears" of the SOC.
- It enables real-time visibility across networks, devices, and applications.
- By centralizing telemetry, analysts can correlate events that might otherwise go unnoticed.

2️⃣ Gather Threat Intelligence & Understand Threat Actors

SOC teams utilize internal and external threat intelligence feeds to stay ahead of evolving attack techniques.

- Helps analysts recognize the **tactics, techniques, and procedures (TTPs)** of adversaries.
- Provides context on **who the threat actor is, what their motive might be, and how they operate**.
- Enables proactive defense by detecting early indicators of compromise (IoCs).

3️⃣ Create & Rank Alerts Based on Business Risk

Not every alert has the same level of urgency. The SOC prioritizes alerts based on their potential business impact.

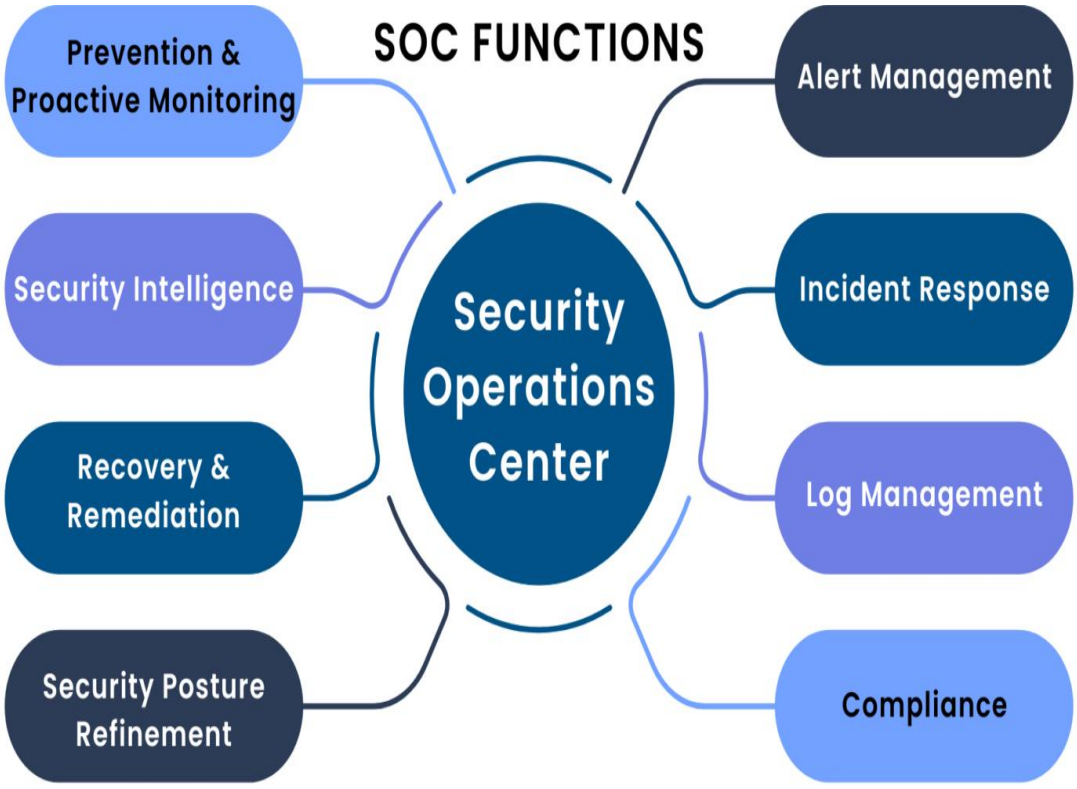
- Alerts are categorized into severity levels (critical, high, medium, low).
- Risk ranking ensures SOC resources are focused on what truly matters to the business.
- This minimizes alert fatigue and enables faster, more efficient triage.

4️⃣ Promptly Respond to Incidents & Minimize Impact

When incidents occur, the SOC acts as the **first line of defense**.

- Analysts investigate, contain, and remediate threats to reduce damage.
- Incident response playbooks and automation help in quick containment.
- Goal: ensure business continuity, reduce downtime, and protect sensitive data.

Key Takeaway:
A SOC is not just about monitoring logs—it's about **transforming raw data into actionable insights, anticipating adversaries, prioritizing threats by business risk, and ensuring swift incident response**. It is the beating heart of an organization's cybersecurity defense.




Security Operation Center (SOC) Function Diagram
• Real-time Monitoring
Threat Detection
• Incident Response
Critical: Ransomware Detected
High: Phishing Attempt