SOC-AS-A-Service

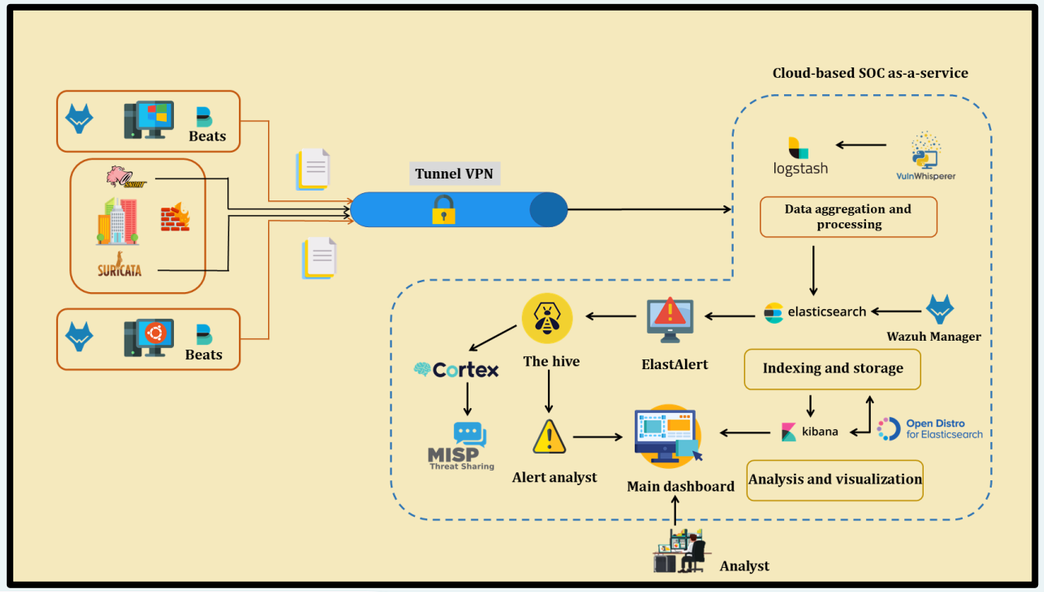
Infrastructure

The Service Operational Centre (SOC) provides the necessary infrastructure and technology to One Link Private Limited to mitigate cyber threats. SOC is a "Security information and event management" (SIEM) system that collects events and logs using numerous security tools and systems. The hardware and software that will be used in SOC and supplier networks are shown in the diagram.

Supply Chain Technology

The Snort and Suricata will be used as a threat detection engine in the network. Both can act as Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). Wazuh will be used for incident response, security monitoring, regulatory compliance, and threat detection. It monitors cloud services, containers, and endpoints to analyse and combine data from external sources.

Supply chain and SOC-as-a-Service



Hardware

- End points
- Servers
- Router
- Firewall

Software

- Beats
- ELK stack
- Suricata
- Virtual Private Network (VPN)
- Snort
- MISP
- Wazuh
- The Hive
- Cortex

Roles and responsibility

Tier 1 Analyst

The analyst of tier 1, also known as **Alert Investigator**, is responsible for monitoring alerts of SIEM, configuring and managing security monitoring tools. They tirage and prioritize alerts. They also determine if the actual incident is happening.

Tier 2 Analyst

The analyst of tier 2 also known as the **Incident Responder** is like the tier 1 analyst but has a lot of experiences in incident response. They perform deep analysis on received incidents. They associate with threat intelligence to identify the attacker and the nature of attack. For remediation, containment, and recovery, they define and implement strategies.

Tier 3 Analyst

The analyst of tier 3 is also known as **Subject Matter Expert** or **Threat Hunter.** They have more experience in high level incident that tier 2 analyst. They conduct daily penetration testing and vulnerability assessments and reviews threat intelligence, vigilance, and security data. Tier 2 and 3 analyst responds when a major incident occurs.

Tier 4 SOC Manager

The SOC Manager of tier 4 also known as **Commander** oversees offensive and defensive tactics and is responsible for recruiting and training SOC staff. They manage project resources and priorities and manage teams while responding to critical business security events. The company contacts them for compliance and security related issues.

Security Engineer

Security Engineers must be hardware or software experts and be responsible for all the security aspects of the design. They create tools and solution to deal robustly with malicious attacks and disruption of operations. They may be employed within the SOC or sometimes supported as a part of development teams.

Processes and task of SOC-as-a Service

Proactive Monitoring

The SOC team is responsible for proactive monitoring (threat monitoring) and log file analysis. Logs are recorded from network resources such as firewalls, routers, and intrusion detection system (IDS) or from end points such as computer, an IOT device and phone. They work with numerous resources including other IT workers, log tools and artificial intelligence.

Incident Response and Recovery

The SOC coordinates the company's ability to properly communicate and take the necessary steps to reduce losses to sustain the organization running after the incident. The main purpose of incident response is to help the company recover from the incidents. For instance, handling ransomware events.

Recovery and Remediation

After an incident, the SOC is responsible for restoring systems and recovering compromised or lost data including restarting and wiping endpoints, reconfiguring systems. The move will return the company's network to its original state as before the incident.

Prioritize and Analyse

The SOC qualifies and triage alarms before determining what steps to take to resolve the issue. The analysts focus on hazards and shorten response time when prioritizing alarms.

Classify and Triage Events

The SOC uses excellent security technologies including SIEM capabilities. Normalizes log and machine data using NextGen SIEM and secures the network. A centralized SOC can be built around an SIEM to quickly categorize events and identify critical events before damage to networks and systems.

Log management

The SOC collects, manages, maintains, and regularly reviews all network activities of the organization. The compiled log helps the organization to define normal network activity and can easily identify the existence of threats in the network. It can be used for the forensics and remediation in the incidents. SIEM is used by many SOCs to correlate and combine the data from firewall, endpoints, applications, and operating system.

NIST Cybersecurity Framework

The "**NIST Cybersecurity Framework"** (CSF) is used as a key point for guidelines, standards, and best practises for managing the risk lifecycle. This framework can be applied by the SOC to establish mature approach to secure the organization to access, guide, and provide key security metrics. NIST CSF is the starting point for establishing an enterprise cybersecurity strategy.

Evaluation

The cyber attackers can go into hiding for a long period of time without Security Operation Centre (SOC) services because the organization does not have the skills to detect and respond to cyber threats. For instance, Yahoo did not know that their account had been hacked for many years. Therefore, SOC is essential for the better visibility in the organization's environment. The organization should focus on mitigating cyber threats by detecting and responding to them. The organization with SOC has higher speed to identify threats and resolve them. A centralized function where individuals, technology and processes are operated within the organization for monitoring and improving the security situation of the organization while analysing, detecting, responding, and preventing cybersecurity attacks is a SOC. It acts as a central command post or hub. This is the correlation point of each event logged in to the organization that is being monitored. The SOC team has been provided security strategy and appropriate infrastructure by the organization. The main responsibilities of the SOC team are to investigate suspicious activities and maintain security monitoring tools. The "Security information and event management" (SIEM) system collects incidents and logs using multiple security tools and systems and the SOC team analyses and responds. SOC analysts are divided into four tiers. At the beginning, SIEM alerts flow to analysts of Tier 1 (Alert Investigator), who are responsible for monitoring, prioritizing, and investigating them. Then, the real threats are sent to the analysts of Tier 2 (Incident Responder) to conduct in-depth analysis and decide strategies for restraint. Then, critical violations are flowed to senior analyst of Tier 3 (Threat hunter or Subject Matter Expert). They are responsible for managing the incident and actively hunting for threats. Finally, the analyst of Tier 4 (Commander) direct SOC staff of management when security event occurs because they are responsible for strategies, prioritization, and recruitment. (Cassetto, 2022)

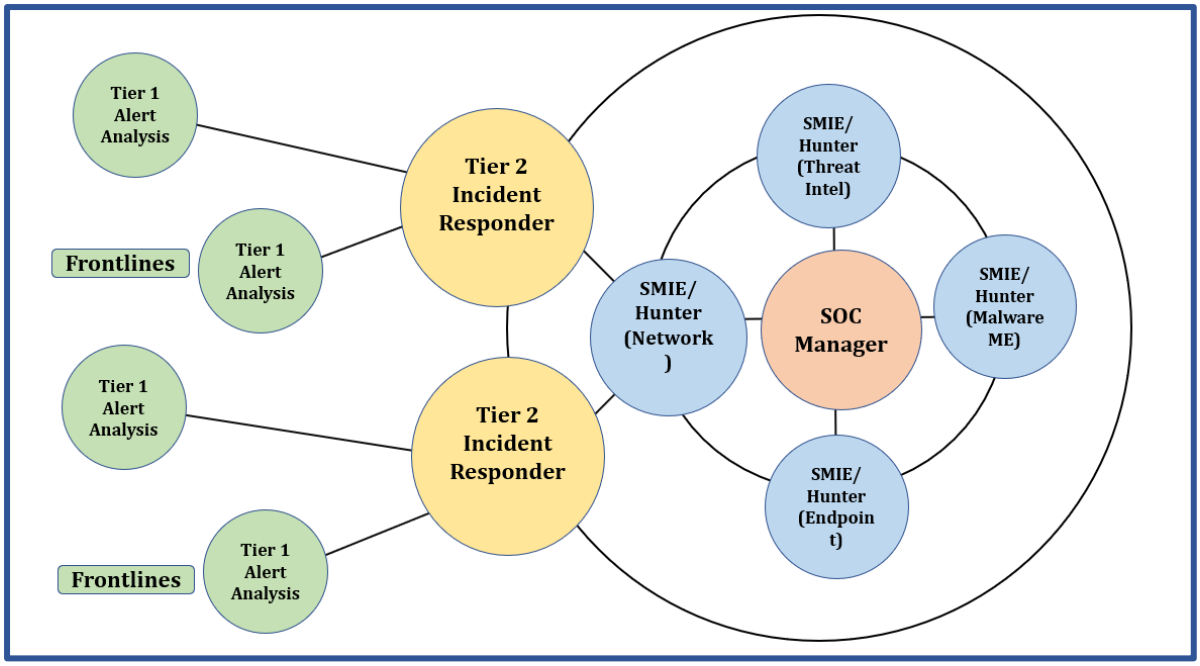


Figure 1 The SOC analysts

The SOC teams are responsible for various of activities and some of them are listed below:

i. Compliance Management
ii. Security Improvement and Refinement
iii. Coordination and Context
iv. Incident Response and Recovery
v. Log Management
vi. Remediation Activities
vii. Proactive Monitoring
viii. Root Cause Investigation

This poster was created for the analysis, monitoring, reports generation, log retention and incident response of One Link Pvt. Ltd. A variety of events and logs will be collected from the network and host components. Those logs will be consumed in Logstash through a VPN tunnel. Wazuh-agent and ELK beats will be used for collecting data and logs and send them to ELK SIEM. Kibana will receive the forwarded data and handle the analysis and visualization of the stored data. (Ayadhi 2020)