**ASSIGNMENT-3**

**Introduction to SOC**

A Security Operations Center (SOC) is a centralized team within an organization that handles cybersecurity operations. The purpose of a SOC is to monitor, identify, analyze, and respond to cyber threats and incidents on an organization's IT systems and infrastructure in real-time. SOCs allow organizations to rapidly detect and mitigate security risks before major damage occurs.

**The primary functions of a SOC involve:**

- Monitoring - Accumulating and reviewing data from various network and system sources to identify abnormalities and events. This includes firewall logs, IDS/IPS, endpoints, servers, databases etc.

- Threat Detection - Utilizing threat intelligence feeds and conducting correlation analysis to pinpoint indicators of compromise and flag potential security incidents.

- Alert Triage - Prioritizing alerts to differentiate between actual incidents and false positives. Creating tickets for alerts needing investigation.

- Investigation - Examining incidents further through log analysis, forensic data gathering, and reverse engineering malware. Understanding the scope and impact of incidents.

- Incident Response - Implementing proven response procedures like containment, eradication, recovery, and post-incident analysis. Facilitating communication and coordination across stakeholders.

- Threat Hunting - Proactively combing through data to uncover advanced threats that evade existing controls. Identifying anomalies and attacker behaviors.

By housing these critical capabilities, an organization gains greater awareness and control over its security posture. SOCs provide timely threat detection, coordinated response, and continuous learning - making them a vital part of a robust cybersecurity approach.

**SIEM Systems**

SIEM (Security Information and Event Management) platforms provide real-time analysis of security alerts, events, and logs from across an organization's IT infrastructure. SIEM solutions aggregate and correlate data from diverse systems to deliver a unified view of security activity. This enables monitoring the environment to detect, investigate, and respond to cyber threats effectively.

**Key capabilities of SIEM solutions include:**

- Centralized log management - Accumulating and normalizing log data from OS, apps, networks etc. Provides visibility through normalized logs.

- Real-time monitoring - Applying analytics like rules, signatures, statistical models to detect anomalies and threats as they occur.

- Alerting and workflow - Generating notifications for security events and facilitating investigation through ticket assignments and documentation.

- Reporting - Creating reports for compliance, audits, management dashboards, and analyzing trends.

- Threat intelligence - Incorporating threat feeds and adversary data to detect known IOCs and TTPs.

- Incident response - Providing capabilities for forensic analysis, tracking infections, containment, and remediation.

By leveraging SIEM platforms, SOCs gain the ability to overcome data silos and monitor their environment holistically. The automated threat detection and workflow capabilities make SOCs more efficient and productive. SIEM is a force multiplier for modern cyber defense.

**QRadar Overview**

IBM QRadar is a widely adopted SIEM platform providing intelligent threat detection, compliance, and security analytics. It utilizes behavior analytics algorithms to detect sophisticated threats and provides a unified architecture for gathering, storing, and analyzing security data.

**Key capabilities of QRadar include:**

- Log management - Accumulating, parsing, and normalizing events from thousands of data sources. Deduplicating events for efficient storage.

- Offense analytics - Using anomaly detection, machine learning algorithms, and rules to detect threats. Prioritizing risky events for quick response.

- Network activity monitoring - Analyzing flows, packets, and performing deep packet inspection to identify issues.

- Incident forensics - Pivoting across events through interactive searches to determine the root cause of incidents.

- Custom apps and extensions - Allow integrating with existing infrastructure through REST APIs and adding custom capabilities.

- Reporting and compliance - Pre-built reports for security, risk, and compliance requirements. Custom reporting also available.

QRadar is offered as software, an appliance, and in the cloud. This provides deployment flexibility based on infrastructure and scale needs. The modular architecture also allows efficiently adding capabilities like SIEM, log management, vulnerability management etc.

**Use Cases**

Here are some examples of how QRadar can be leveraged in SOCs:

- Monitor firewall logs to detect abnormal traffic patterns like spikes in blocked outbound communications indicating potential botnets or data exfiltration.

- Ingest web proxy logs to identify threats like users accessing malicious sites, abnormal file transfers, and command and control communications.

- Analyze VPN logs to pinpoint compromised user accounts, brute force attacks, and logins from suspicious locations.

- Scan endpoint logs for indicators of malware or attacker activity such as execution of droppers, privilege escalation, suspicious registry or system file changes.

- Identify brute force attempts and account takeover by inspecting authentication events across infrastructure.

- Incorporate threat feeds to detect communications with known bad IPs, domains, hashes, and implement threat hunting.

- Use integrated case management to document security incidents for coordination across teams like IR, forensics, engineering etc.

By leveraging QRadar's capabilities, SOCs can achieve comprehensive visibility across their environment and utilize smart automation to rapidly detect and respond to all types of threats before they result in data breaches.