**Assignment 3**

**Intro to Security Operations center (SOC)**

A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization’s entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible. It also continually analyzes threat data to find ways to improve the organization's security posture.

What an Security Operations Center (SOC) does

SOC activities and responsibilities fall into three general categories.

1. Preparation, planning and prevention
2. Monitoring, detection and response
3. Recovery, refinement and compliance

SOC Security Functions :-

1. Maintaining Inventory of Available Resources

The SOC oversees two asset types—processes, devices, and applications that require protection and defensive tools that can help achieve this protection.

### 2. Preparation and Preventative Maintenance

Even the best-equipped and most agile response methodology is not as good as stopping issues from happening in the first place.

### 3. Continuous Monitoring

The SOC uses tools to scan the network continuously and flag any suspicious activities or abnormalities. Monitoring the network 24/7 provides the SOC with notifications of emerging threats, making it possible to mitigate them or prevent attacks in their early stages.

### 4. Alert Prioritization and Management

When monitoring tools provide alerts, the SOC must examine each one closely, do away with false positives, and decide how serious any actual threats are and what they might be targeting. The SOC is responsible for prioritizing alerts, identifying which ones are likely to be real security incidents, and investigating them to enable rapid response.

### 5. Threat Response

As soon as the SOC team identifies an incident they function as a first responder, carrying out actions such as isolating or shutting down infected endpoints, stopping harmful processes, removing malware, and more. The aim is to mitigate the threat with minimal disruption to the organization’s continuity.

### 6. Recovery and Remediation

An SOC oversees the steps taken in the wake of an attack, ensuring that the organization effectively mitigates the threat and communicates with affected parties. It is not enough for SOC teams to issue alerts and view logs. A core component of incident response is assisting organizations so they can effectively recover from an incident.

For instance, recovery may involve cleaning ransomware or malware from affected systems, resetting passwords for compromised accounts, wiping and reimaging infected endpoints.

### 7. Log Management

The SOC should gather, maintain, and regularly review logs of all network communications and activities across the whole organization. This information helps establish a baseline for regular network activity, can expose threats, and can be used by IT and security specialists for forensics and remediation following an incident.

Many SOCs utilize a SIEM to correlate and aggregate the data feeds from firewalls, operating systems and endpoints, and applications, creating a central repository of security data.

### 8. Root Cause Investigation

Following an incident, the SOC needs to work out precisely what happened, why, how, and when. Throughout this investigation, SOC teams rely on log data and other details to discover the source of the issue which will help them stop similar issues from arising in the future.

### 9. Security Process Improvement

Cybercriminals constantly refine their tactics and tools to stay one step ahead of defenses, the SOC must carry out improvements on an ongoing basis. One way to improve the security process is to perform post-mortem investigations of incidents and identify how the SOC team could have done better. Another way is to carry out realistic practice sessions such as war games with blue teams and red teams.

### 10. Compliance Management

Organizations protect themselves through external security standards and adherence to a security policy. External standards include the ISO 27001x, the General Data Protection Regulation (GDPR), and the NIST Cybersecurity Framework (CSF). Organizations need an SOC to help make sure that they meet the requirements of key best practices and security standards.

**SIEM Systems**

Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behaviour anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.

SIEM is an important part of an organization’s cybersecurity ecosystem. SIEM gives security teams a central place to collect, aggregate, and analyze volumes of data across an enterprise, effectively streamlining security workflows. It also delivers operational capabilities such as compliance reporting, incident management, and dashboards that prioritize threat activity.

**Why is SIEM beneficial to a business?**

* **Mass application.**SIEM technology is incredibly flexible, making it suitable for almost any business – regardless of the size of the company, the industry in which it works, or the complexity of the existing IT infrastructure.
* **Improved threat detection**. SIEM allows for rapid threat detection, which in turn helps to reduce security breaches across a business’ entire IT infrastructure. The quicker that threats are identified, the quicker the response is, and thus the more secure the business’ IT systems will be.
* **Straightforward compliance reporting.**Compliance reporting is crucially important in the modern, data-sensitive world, with businesses required to comply with regulations such as HIPAA, GPG13, and the European Union’s GDPR. SIEM allows businesses to apply constant vigilance on security issues that may be problematic in terms of compliance, which subsequently helps to limit (potentially costly) compliance violations in the future.

**IBM Qradar**

IBM QRadar is an enterprise [security information and event management (SIEM)](https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM) product. It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors.

**IBM Security QRadar features :-**

* AI/Machine Learning
* Behavioral Analytics
* Compliance Management
* Endpoint Management
* Endpoint Protection
* Incident Management
* Network Monitoring
* Prioritization

QRadar can be deployed in different ways, depending on your organization's requirements and preferences. The two primary deployment options for QRadar are on-premises and cloud-based deployments.

On-Premises Deployment:

* In an on-premises deployment, QRadar software and hardware appliances are installed and maintained within your organization's data center or physical infrastructure.

Cloud Deployment:

* In a cloud-based deployment, QRadar is hosted and managed by a cloud service provider (e.g., IBM Cloud, AWS, Azure) in their data centers.

Factors to consider :-

* Security and Compliance: Consider your organization's security and compliance requirements. Some industries or regulations may mandate on-premises deployments for certain types of data.
* Cost: Evaluate the total cost of ownership (TCO) for both deployment options, including hardware, software, maintenance, and operational costs.
* Scalability: Assess your organization's scalability needs. Cloud deployments can scale more easily to accommodate growth or fluctuations in data volume.
* IT Expertise: Consider your team's expertise and resources for managing on-premises hardware and software versus leveraging managed cloud services.
* Geographic Distribution: If your organization has multiple locations or a distributed workforce, cloud deployments can offer improved accessibility and performance.
* Disaster Recovery and Redundancy: Cloud providers often offer robust disaster recovery options and redundancy, which can be beneficial for business continuity.

Top of Form

**Use Cases**

KBC Group - Financial

When KBC implemented the IBM Security SOAR platform, previously Resilient, it gained a central hub for cybersecurity incident response. The company now visualizes threats in its entities and launches local and group-level responses required by numerous regulations.

KBC operates across Europe through fully-owned banks and insurance companies with a high level of local autonomy in its core markets of Belgium, the Czech Republic, Slovakia, Hungary, Bulgaria and Ireland.

In 2016, KBC formed its Cyber-Expertise and Response Team (CERT) in its Brussels, Belgium, headquarters. The team was tasked with orchestrating the response to cyberthreats throughout the group’s multiple entities throughout Europe. The CERT needed to centrally oversee its incident response process, but it did not want to create a large, centralized department for doing so. The group’s various European and international entities had well-established, and largely autonomous, security and incident response teams. Rather than duplicate efforts, the KBC CERT would supplement them and ultimately improve on the group’s overall cybersecurity effort through heightened awareness and response coordination at the group level.

KBC sought a mechanism by which the CERT could record and visualize threats in the group’s various entities and launch local and group reporting and responses required by the various regulations.

KBC conducted a request for proposal (RFP) process, which included demonstrations of a number of security reporting platforms, and selected the IBM Security SOAR Platform, previously Resilient. The IBM Security SOAR solution offers a powerful foundation for response planning, management and mitigation for a wide range of incident types at multiple levels of the KBC organization.