Introduction to
Security Operations Centre (SOC)

What Is a Cyber Attack?

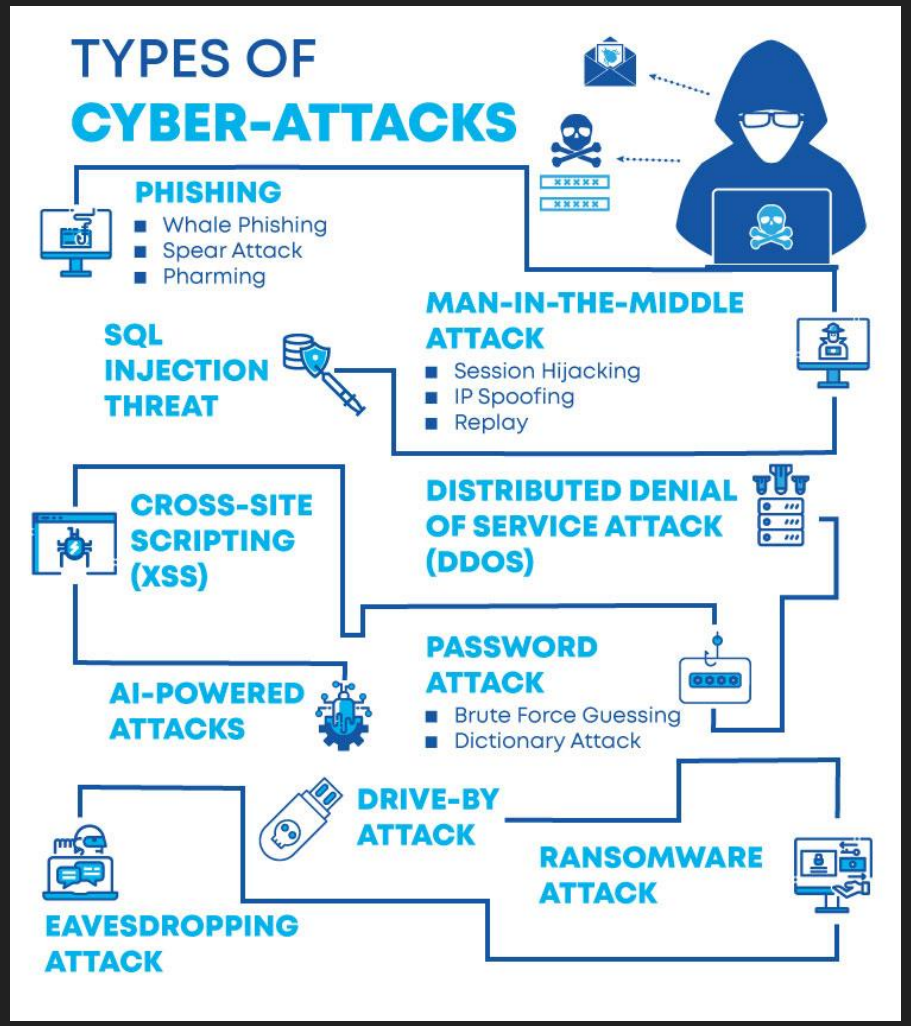
- **Why do cyber attacks happen?**

Cyber attacks have become increasingly **sophisticated**. The increase in such instances every year hints at a few common motives. Some of the most reported reasons include:

- **Ransom:** Cyber attacks are aimed at extracting ransom from the owner of the device or network.
- **Accessing financial details:** The aim of such attacks can be to access the financial details of the clients of a company or the company itself. This information can be publicized or used for personal monetary benefits. It can also be used to hack one's bank account and drain out the cash.

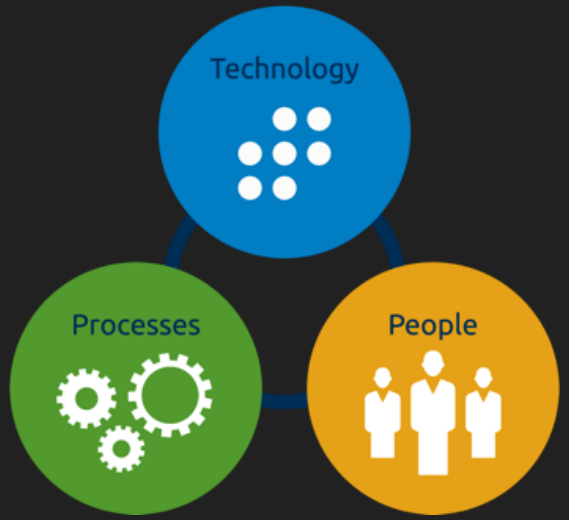
Types of Cyber-attacks

https://www.mygreatlearning.com/blog/types-of-cyber-attacks-and-why-cybersecurity-is-important/

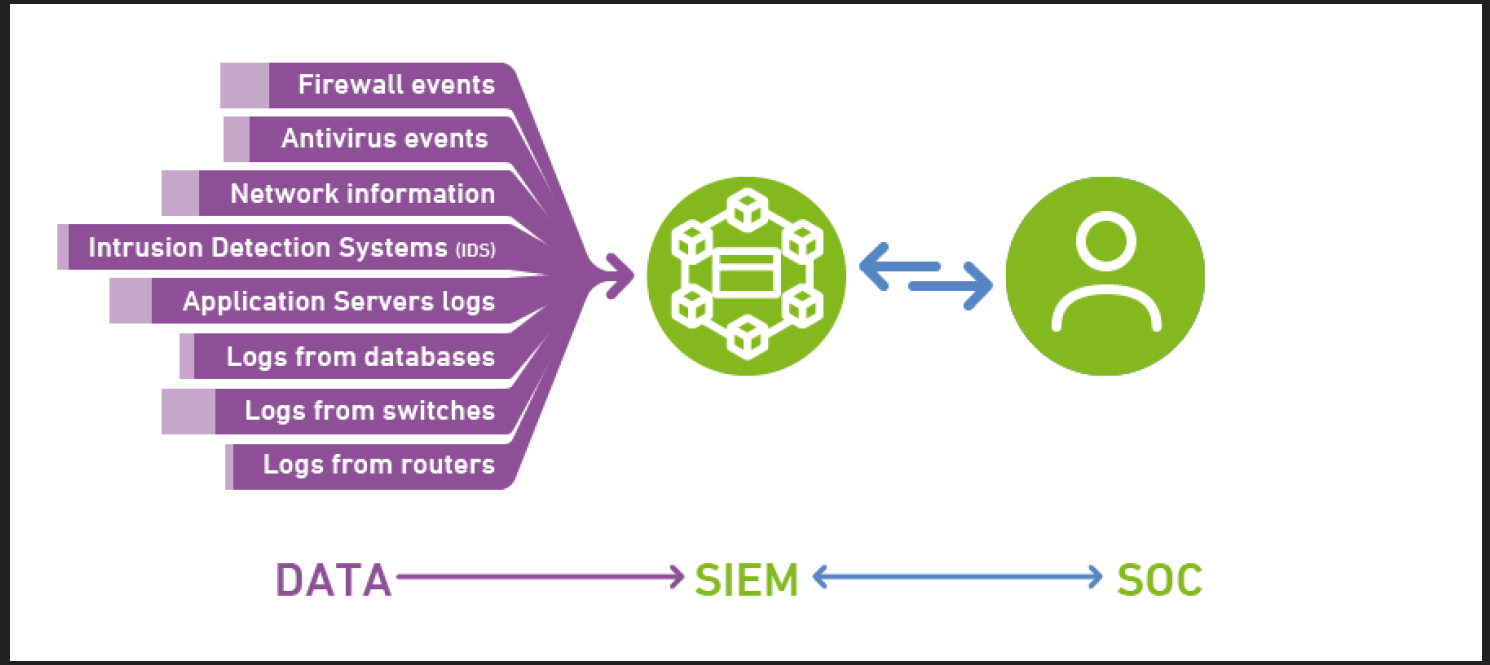


What is a Security Operations Center (SOC)?

- A Security Operations Center (SOC) is part of the security team of an organization that is responsible for analyzing and protecting the organization from cyber-attacks. Although SOC employees work with other teams and departments, they are usually their own independent department.



What is a Security Operations Center (SOC)?



SOC ~ logs

Triad of soc

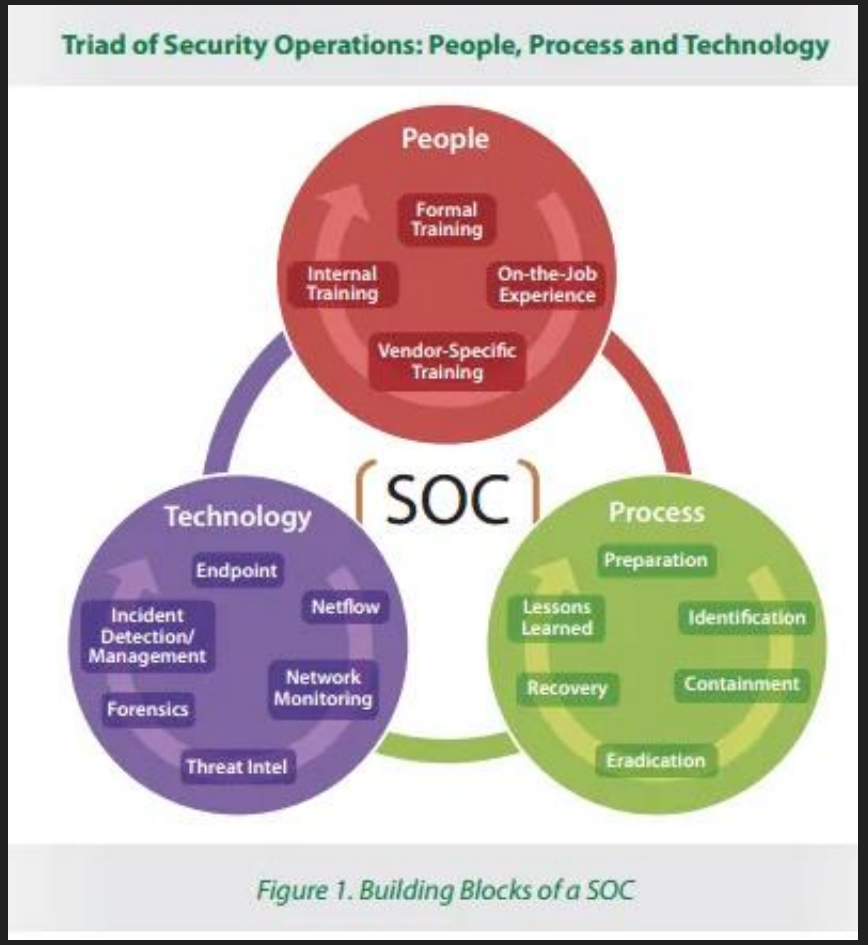


Figure 1. Building Blocks of a SOC

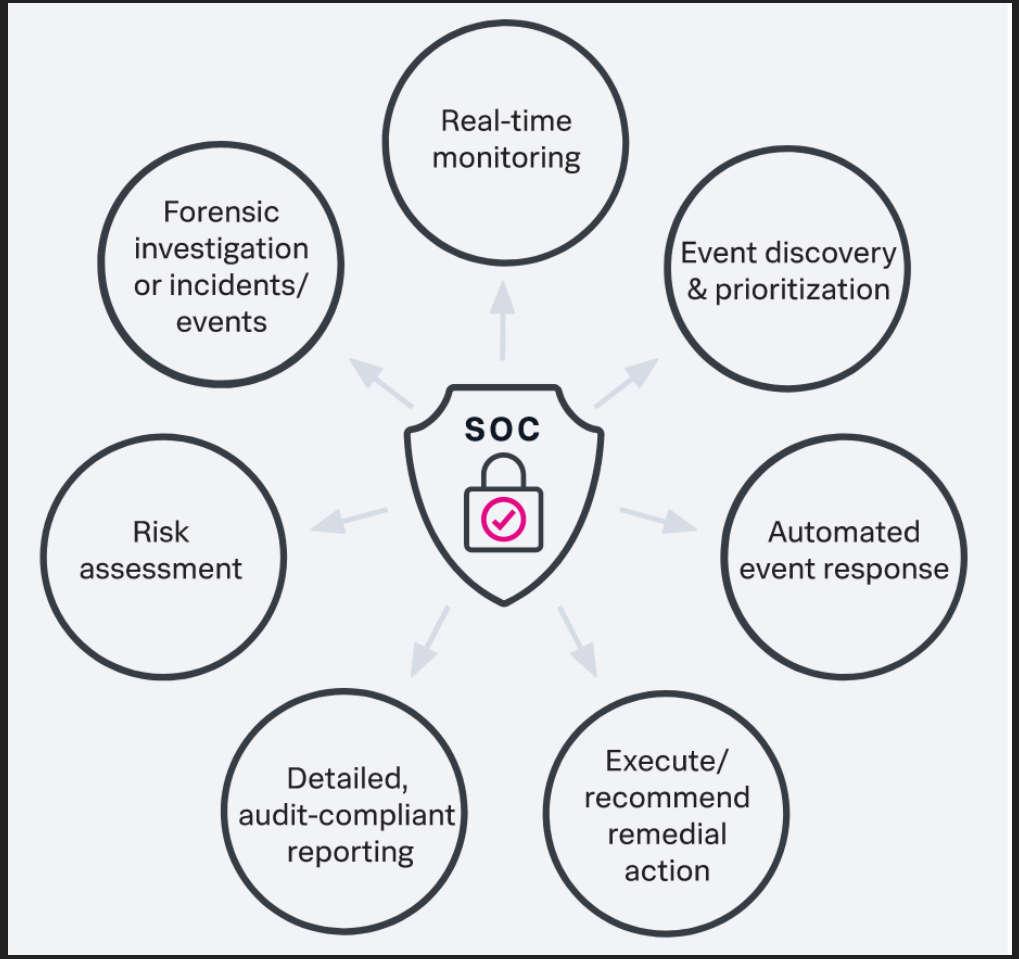
Q: What should a SOC monitor?

A: SOC tools and teams should monitor all traffic on a network from external sources. This means that every **server, router, and database** must be within the scope of the security operations center team.

What is SIEM's role in the SOC?

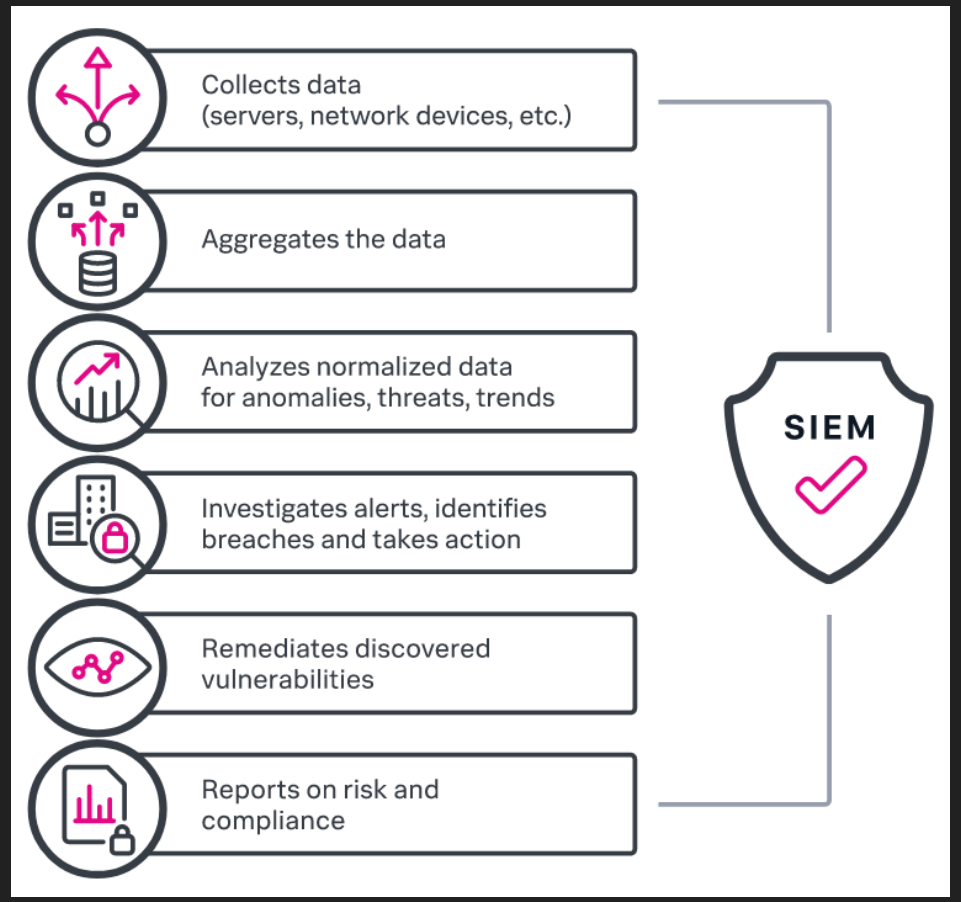
SIEM's role is to provide analysts in the SOC (security operations center) with consolidated insights from analysis of event data too varied and voluminous for manual review. SIEM analysis of machine data and log files can surface malicious activity and trigger automated responses, significantly improving response time against attacks.

While SOCs existed before SIEM came along, SIEM is a vital tool for the modern SOC's mission to respond to internal and external attacks, simplify threat management, minimize risk, and achieve organization-wide visibility and security intelligence.



How Does a SIEM Work?

A security event is any occurrence in a IT environment that has the possibility of becoming a vulnerability, or an indication that the environment has already been exploited. Such events include unauthorized access, configuration changes, and abnormal user activity. A SIEM helps interpret these events to determine what threats pose the most risk and how they should be prioritized.



SIM vs SEM

- **What is Security Information Management (SIM)?**
- **S**ecurity **I**nformation **M**anagement (**SIM**) is the collection, monitoring, and analysis of security-related data from computer logs. Also referred to as log management.

- **What is Security Event Management (SEM)?**

- **S**ecurity **E**vent **M**anagement (**SEM**) is the practice of network event management including real-time threat analysis, visualization, and incident response.

Evolution of Terminology

- SIM – System Information Management
- SEM - Security Event Management
- Log Management – Log file capture & storage
- SIEM - SIM & SEM

A Brief History of SIEM Tools

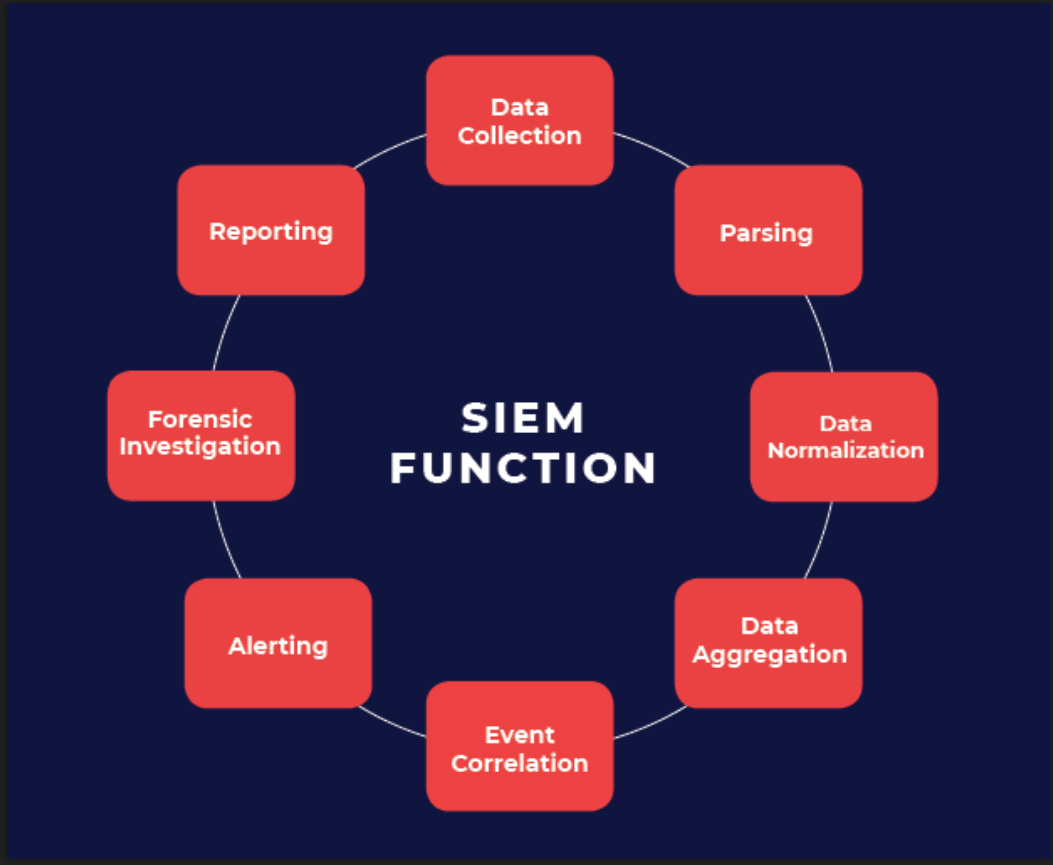
- **Gartner** coined the term 'SIEM' (pronounced "sim") in a 2005 report called "Improve IT Security With Vulnerability Management."

The very term SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.

Mark Nicolett and Amrit Williams

What Is a SIEM?

Security Information and Event Management (SIEM) is a software and solution for logging, monitoring, alerting, anticipating, correlating and visualizing security-related events and information garnered from networked devices. Plainly, SIEM is a combination of both processes and tools, or products.



How Does SIEM Work?

- SIEM provides two primary capabilities to an Incident Response team:
  - **Reporting and forensics** about security incidents
  - **Alerts based** on analytics that **match a certain rule** set, indicating a security issue

- User Event Behavioral Analysis (UEBA)

- Lateral movement – attackers move through a network by using IP addresses, credentials and machines, in search of key assets. By analyzing data from across the network and multiple system resources, SIEMs can detect this lateral movement.

A SIEM system not only identifies that an attack has happened, but allows you to see how and why it happened as well.

Next-Generation SIEMs

New SIEM platforms provide advanced capabilities such as:

-**Lateral movement** – attackers move through a network by using IP addresses, credentials and machines, in search of key assets. By analyzing data from across the network and multiple system resources, SIEMs can detect this lateral movement.

-**Detection without rules or signatures** – many threats facing your network can't be captured with manually-defined rules or known attack signatures. SIEMs can **use machine learning** to detect incidents without pre-existing definitions.

effective SIEM must address the following eight crucial use cases

1	Real-time monitoring
2	User monitoring
3	Threat correlation and context
4	Meet compliance mandates
5	Incident management
6	Forensic investigation and threat hunting
7	Long-term event storage
8	Reporting and dashboards

Advanced Threat Detection

SIEMs can help detect, mitigate and prevent advanced threats, including:

- **Malicious insiders** – a SIEM can use browser forensics, network data, authentication and other data to identify insiders planning or carrying out an attack
- **Data exfiltration (sensitive data illicitly transferred outside the organization)** – a SIEM can pick up data transfers that are abnormal in their size, frequency or payload
- **Outside entities, including Advanced Persistent Threats (APTs)** – a SIEM can detect early warning signals indicating that an outside entity is carrying out a focused attack or long-term campaign against the organization

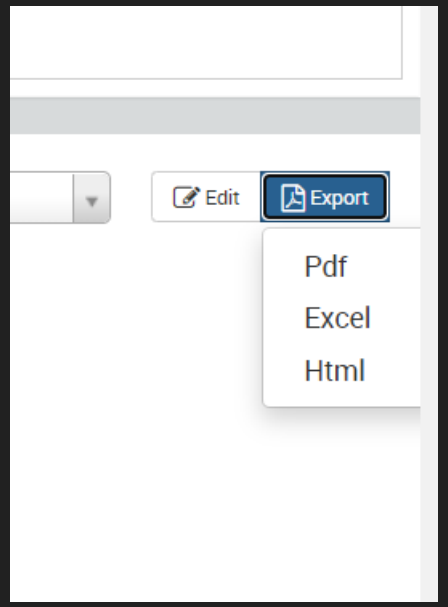
What is EPS in SIEM?

Two key numbers are the amount of data generated in your network, measured in Events per Second (**EPS**) and Gigabytes per Day (GB/day)

Alerts & Categories

- BruteForce 10
- D/Dos 17
- Database 37
- Exploit 21
- File 14
- Honeypot 7
- Identity 88
- Lateral Movement 2
- Mail 5
- Malware 16
- Reconnaissance 36
- System 22
- Threat 19
- Traffic 35
- Vulnerability 4
- Web 22

Results can be exported in PDF, Excel, and HTML. We have exported the report in PDF.



SIEM capabilities

- **Log Collection**
- **Normalization – Collecting logs and normalizing them into a standard format)**
- **Notifications and Alerts** – Notifying the user when security threats are identified
- **Security Incident Detection**

Visibility

SIEM tools provide:

•Real-time visibility across an organization's information security systems.

•Event log management that consolidates data from numerous sources.

•A correlation of events gathered from different logs or security sources, using if-then rules that add intelligence to raw data.

•Automatic security event notifications. Most SIEM systems provide dashboards for security issues and other methods of direct notification.

Event log source

Security Events

- Intrusion Detection Systems
- Endpoint Security (Antivirus, antimalware)
- Data Loss Prevention
- VPN Concentrators
- Web Filters
- Honeypots
- Firewalls

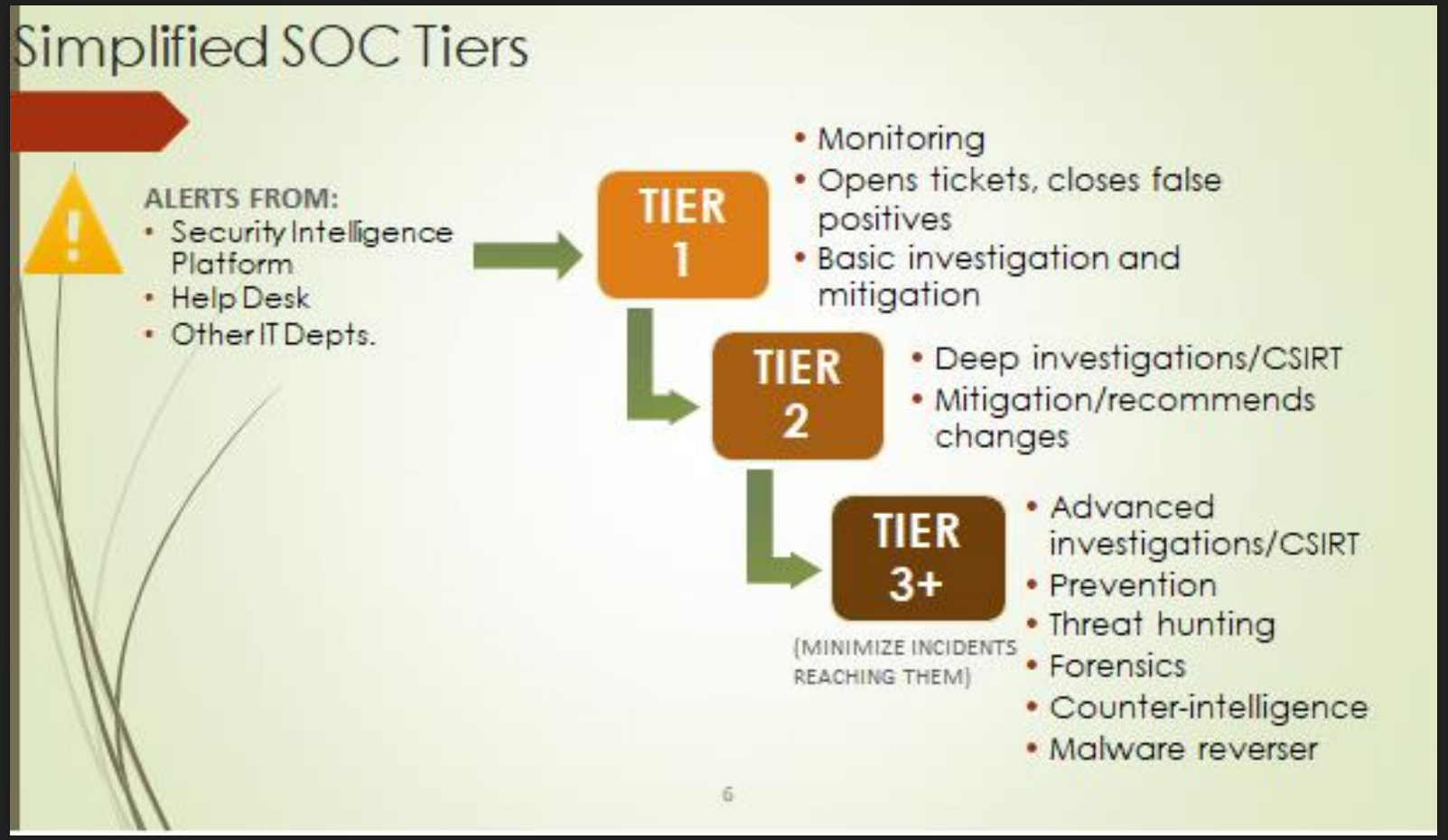
Network Logs

- Routers
- Switches
- DNS Servers
- Wireless Access Points
- WAN
- Data Transfers
- Private Cloud Networks (VPC)

Applications and Devices

- Application Servers
- Databases
- Intranet Applications
- Web Applications
- SaaS Applications
- Cloud-Hosted Servers
- End-User Laptops or Desktops
- Mobile Devices

SOC Tiers


Simplified SOC Tiers
ALERTS FROM:
• Security Intelligence Platform
• Help Desk
• Other IT Depts.
TIER 1
• Monitoring
• Opens tickets, closes false positives
• Basic investigation and mitigation
TIER 2
• Deep investigations/CSIRT
• Mitigation/recommends changes
TIER 3+
(MINIMIZE INCIDENTS REACHING THEM)
• Advanced investigations/CSIRT
• Prevention
• Threat hunting
• Forensics
• Counter-intelligence
• Malware reverser
6

	Role	Qualifications	Duties
	**Tier 1 Analyst** Alert Investigator	System administration skills, web programming languages such as Python, Ruby, PHP, scripting languages, security certifications such as CISSP or SANS SEC401	Monitors SIEM alerts, manages and configures security monitoring tools. Prioritizes alerts or issues and performs triage to confirm a real security incident is taking place.
	**Tier 2 Analyst** Incident Responder	Similar to Tier 1 analyst but with more experience including incident response. Advanced forensics, malware assessment, threat intelligence. White-hat hacker certification or training is a major advantage.	Receives incidents and performs deep analysis, correlates with threat intelligence to identify the threat actor, nature of the attack and systems or data affected. Decides on strategy for containment, remediation and recovery and acts on it.
	**Tier 3 Analyst** Subject Matter Expert / Threat Hunter	Similar to Tier 2 analyst but with even more experience including high-level incidents. Experience with	Day-to-day, conducts vulnerability assessments and penetration tests, and reviews alerts, industry news, threat intelligence and security data.

Monitoring

24/7/365 Monitoring

- Monitoring involves checking systems for cyber security threats and usually involves using specialized cyber security tools to pick up suspicious patterns. These cyber security tools link into a centralized management system with dashboards that provide any alerts to suspicious activities and patterns.

Incident Management

- Incident management is dealing with the alerts to suspicious activities and patterns, involving trying to determine firstly the criticality of the threat and then running through various incident management processes to try to neuter the threat. The processes generally involve people to manage them and technology to help pinpoint more information about the threats and try to stop it in it's wake.

Abnormal Behaviors

- SIEM's visibility capabilities help shed light on your users and third parties. With SIEM, you can establish behavioral baselines for each user, device, application, and third party as they conduct their business workflows. If they deviate from these behaviors—as in an insider threat or credentials compromise—your SIEM solution can detect it. Then it can alert your IT security team or freeze the activity or user in more severe cases.

Managed SOC vs Dedicated SOC

1-Dedicated or Internal SOC

The enterprise sets up its own cybersecurity team within its workforce.

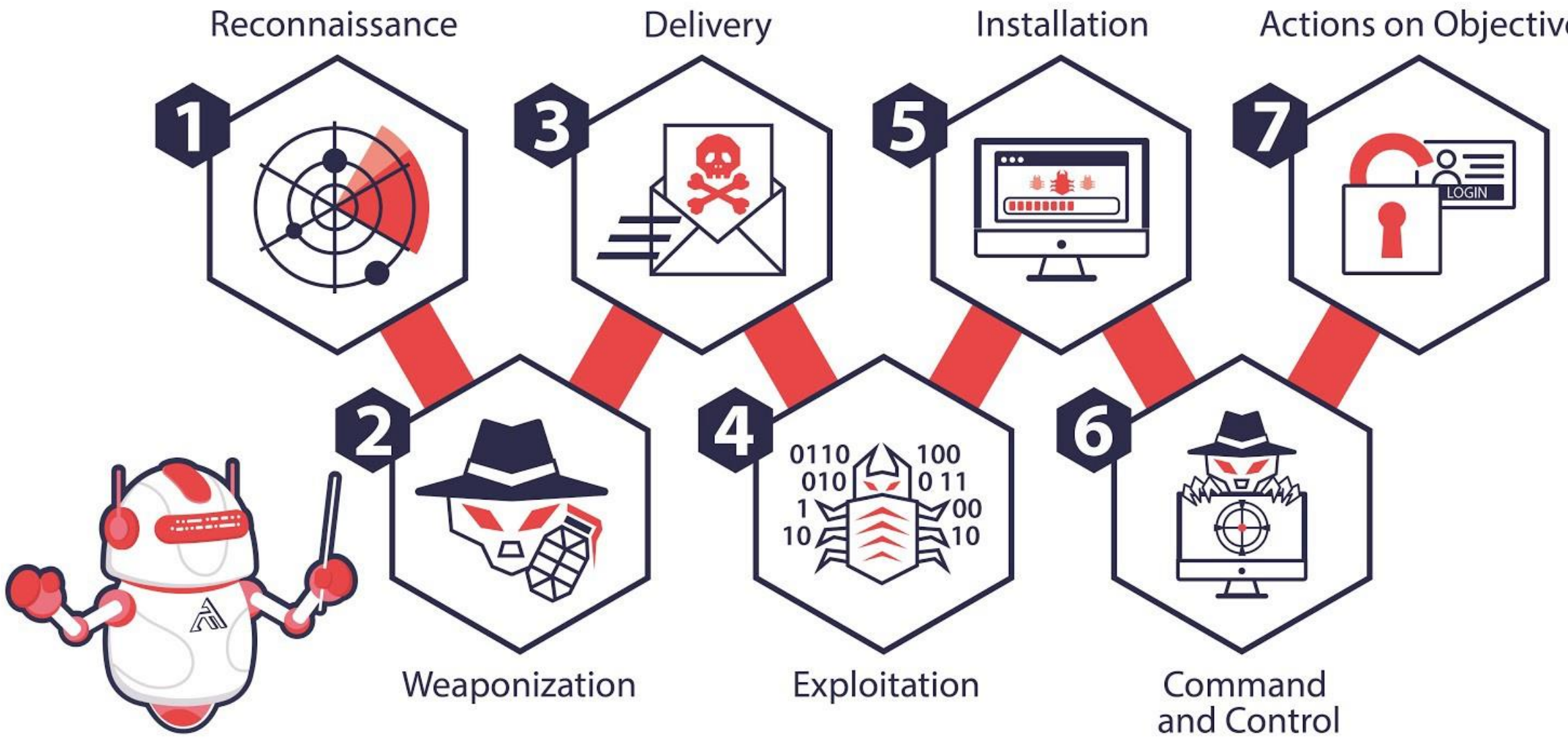
2-Managed SIEM - third-party MSSP -service provider

- This can be beneficial for organizations who can ill afford the high costs of SIEM combined with the in-house expertise to manage it.
- That being said, this also throws in issues around privacy as the data passing into the SIEM is always going to be quite sensitive. It could contain not only details of individuals in the organizations but also details of systems feeding into the SIEM and secret information related to a company's activities.

2020 Gartner Magic Quadrant for SIEM

Miter Attack & Cyber Kill Chain Framework

THE CYBER KILL CHAIN



ATT&CK Matrix for Enterprise

Best SIEM Tools

Become a SOC Analyst

References

1. **Security Information and Event Management (SIEM) Reviews and Ratings**

https://www.gartner.com/reviews/market/security-information-event-management

2. **Use of Machine Learning Algorithms with SIEM for Attack Prediction**

https://www.researchgate.net/publication/283835962_Use_of_Machine_Learning_Algorithms_with_SIEM_for_Attack_Prediction

3. **2020 Gartner Magic Quadrant for SIEM**

https://www.rsa.com/en-us/offers/2020-gartner-magic-quadrent-siem

4. **What is SIEM?**

https://www.exabeam.com/siem-guide/what-is-siem/

5. **What is a Security Operations Center (SOC)?**

https://www.varonis.com/blog/security-operations-center-soc/

6 **.10 Best SIEM Tools of 2021: Vendors & Solutions Ranked**

https://www.comparitech.com/net-admin/siem-tools/

7. Advanced Threat Detection With Modern SIEM Solutions

https://www.innominds.com/blog/advanced-threat-detection-with-modern-siem-solutions

8.Certified Threat Intelligence Analyst (CTIA)

https://www.testpreptraining.com/tutorial/certified-threat-intelligence-analyst-exam/