Cyber Security

Bano Qabil

Instructor: Umar Bilal

My Introduction

- InfoSec Associate at Global Risk Compliance
- InfoSec TA (Teaching Assistant) at FAST NUCES
- Top 1% on tryhackme
- Certified in Cybersecurity (CC) - ISC2
- Certified Network Security Practitioner - SecOps Group
- Certified Cloud Security Practitioner - SecOps Group
- SOC Level 1 - tryhackme
- Ethical Hacking Essentials (EHE) - EC Council

What comes to your mind when you hear the word "Cyber Security"?

- Cybersecurity refers to the practice of safeguarding systems, networks, and data from digital attacks, unauthorized access, damages, or data breaches.
- 3 Types of Hackers: Black Hat, White Hat, Gray Hat
- There are mainly two teams: Red Team & Blue Team

Black Hat Hackers

Motivation: Black Hat hackers are motivated by personal or financial gain, malicious intent, or the desire to challenge established systems. Their activities are illegal and unethical.

Actions: They engage in activities like stealing personal data, credit card information, intruding into systems without permission, distributing malware, ransomware, and creating botnets.

Examples: A hacker who breaches a company's security system to steal sensitive information and then sells that data on the dark web.

White Hat Hackers

Motivation: White Hat hackers, often referred to as "ethical hackers," are driven by the desire to improve security and work within legal boundaries. They're the "good guys" of the hacking world.

Actions: They identify vulnerabilities and weaknesses in systems by using the same techniques as Black Hats but do so with permission and the intention to inform the system's owner of the vulnerabilities they discover. Their aim is to improve security rather than exploit it.

Examples: Security researchers or penetration testers hired by organizations to test the security of their systems. Certifications like "Certified Ethical Hacker (CEH)" exist to train individuals in ethical hacking.

Gray Hat Hackers

Motivation: Gray Hat hackers exist in the ambiguous space between Black Hat and White Hat hackers. Their actions might not be entirely legal, but their intentions are not always malicious.

Actions: They might break into systems without permission but will often do so to bring attention to vulnerabilities, without exploiting them for personal or financial gain. However, because they don't always have explicit permission, their actions can still be considered illegal.

Examples: A hacker who identifies a vulnerability in a system, informs the company of the flaw, and then asks for a "bug bounty" or reward for their discovery, even if the company didn't have a formal bug bounty program.

What is the 'Red Team'?

The Red Team is a group of ethical hackers who mimic the actions of real adversaries. Their goal? To attack systems, just like cybercriminals would.

Key Points:

Simulate Real-world Attacks: Emulate techniques used by actual attackers.

Uncover Weaknesses: Identify vulnerabilities in systems, networks, and applications.

Objective: Discover security flaws before malicious hackers do.

What is the 'Blue Team'?

The Blue Team consists of defenders. Their primary mission? To defend against both real and simulated cyber attacks.

Key Points:
Monitor and Respond: Detect anomalies and manage incidents in real-time.
Strengthen Defenses: Improve security posture by learning from attacks.
Objective: Protect data, assets, and maintain business continuity.

Red Team vs. Blue Team

While they seem to be on opposite sides, the Red and Blue Teams work towards a common goal: a more secure environment.

Key Differences:

Approach: Red Team is offensive, seeking out vulnerabilities. Blue Team is defensive, patching vulnerabilities and responding to attacks.

Tools: Red Team uses penetration testing tools to exploit; Blue Team uses monitoring and defense tools to guard.

Outcome: Collaboration leads to a stronger security posture, benefiting the organization.

Why it Matters for SOC Analysts?

As a future SOC Analyst, you'll primarily align with the Blue Team. However, understanding the tactics, techniques, and procedures (TTPs) of the Red Team helps in:

- Better Defense: Knowing how attackers think aids in crafting better defensive strategies.
- Continuous Learning: Regular Red Team exercises provide feedback on security posture.
- Collaboration: Working with Red Teams during simulations offers real-world experience in defending against attacks.

Our focus is on the Blue Side.
We are going to follow the SOC (Security Operations Center) Analyst Path.

Asset, Vulnerability & Threat:

- Asset: An asset is something in need of protection.
- Vulnerability: A vulnerability is a gap or weakness in those protection efforts. For example, weak password set on a system, an unpatched application running on a system
- Threat: A threat is something or someone that aims to exploit a vulnerability to thwart protection efforts.

What is a SOC?

- A SOC is the centralized unit in an organization responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents. It serves as the first line of defense against cyber threats and coordinates actions to protect, defend, and recover from attacks.


18.3k
9.2k
11.8k
8440
149
26916
13047
2827
870
340
12
49
Top-relevant threats
74%
68%
63%

Who can give me a recent example of a cybersecurity breach in the news?

The Cost of One Click

- Imagine you are an employee at a global company, sifting through hundreds of emails daily. One morning, you receive an email that appears to be from your IT department, asking you to reset your password. You click on the link provided, but nothing seems to happen. Unbeknownst to you, that single click unleashed a ransomware attack that spreads across the company's entire network.

By the evening, the company's systems are locked, data is held hostage, and the attackers demand a multi-million dollar ransom. The result? Financial losses in the hundreds of millions, a tarnished brand reputation, and regulatory fines. This isn't a scene from a movie but the real-life impact of the WannaCry ransomware attack in 2017, which affected over 230,000 computers in 150 countries.

Now, consider the role of a SOC Analyst in such situations – vigilantly monitoring, quickly detecting, and rapidly responding to such threats, making them the first line of defense against cyber adversaries.

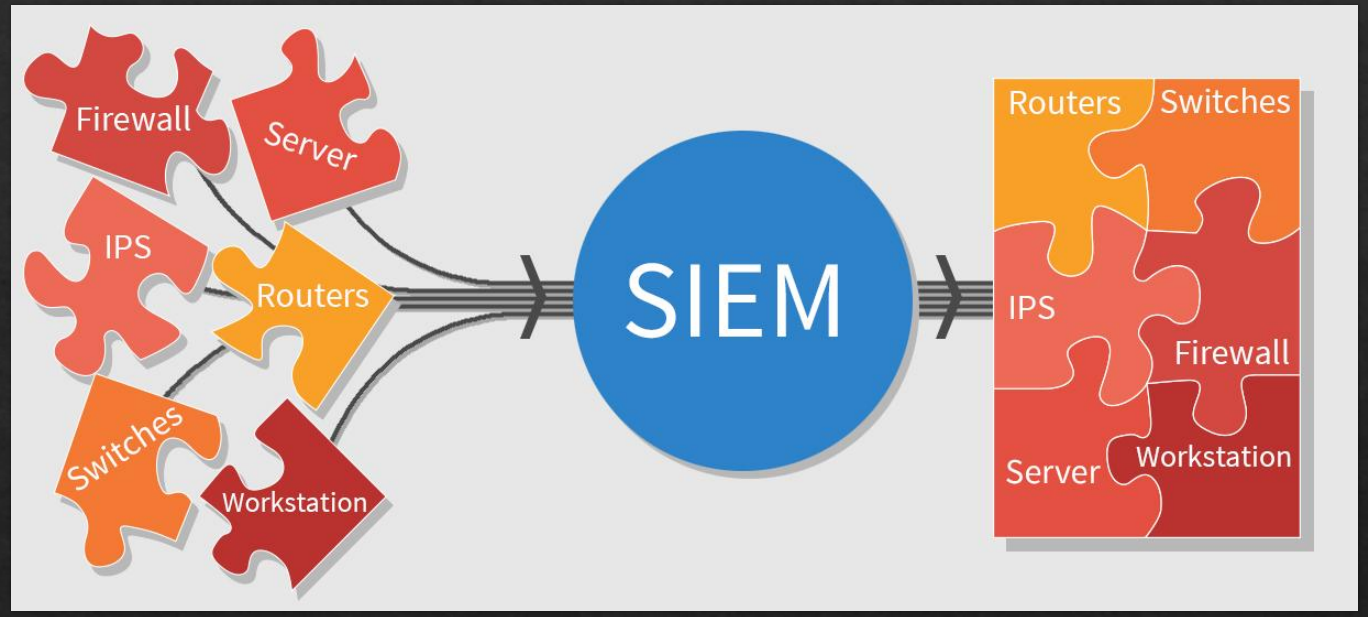
The Heart of the SOC: SIEM

Security Information and Event Management (SIEM) is an integrated solution that aggregates and analyzes log data from various sources across the entire IT infrastructure — from network devices, to servers, to applications.

What's log data?

Event, Suspicious Security Event, Security Incident

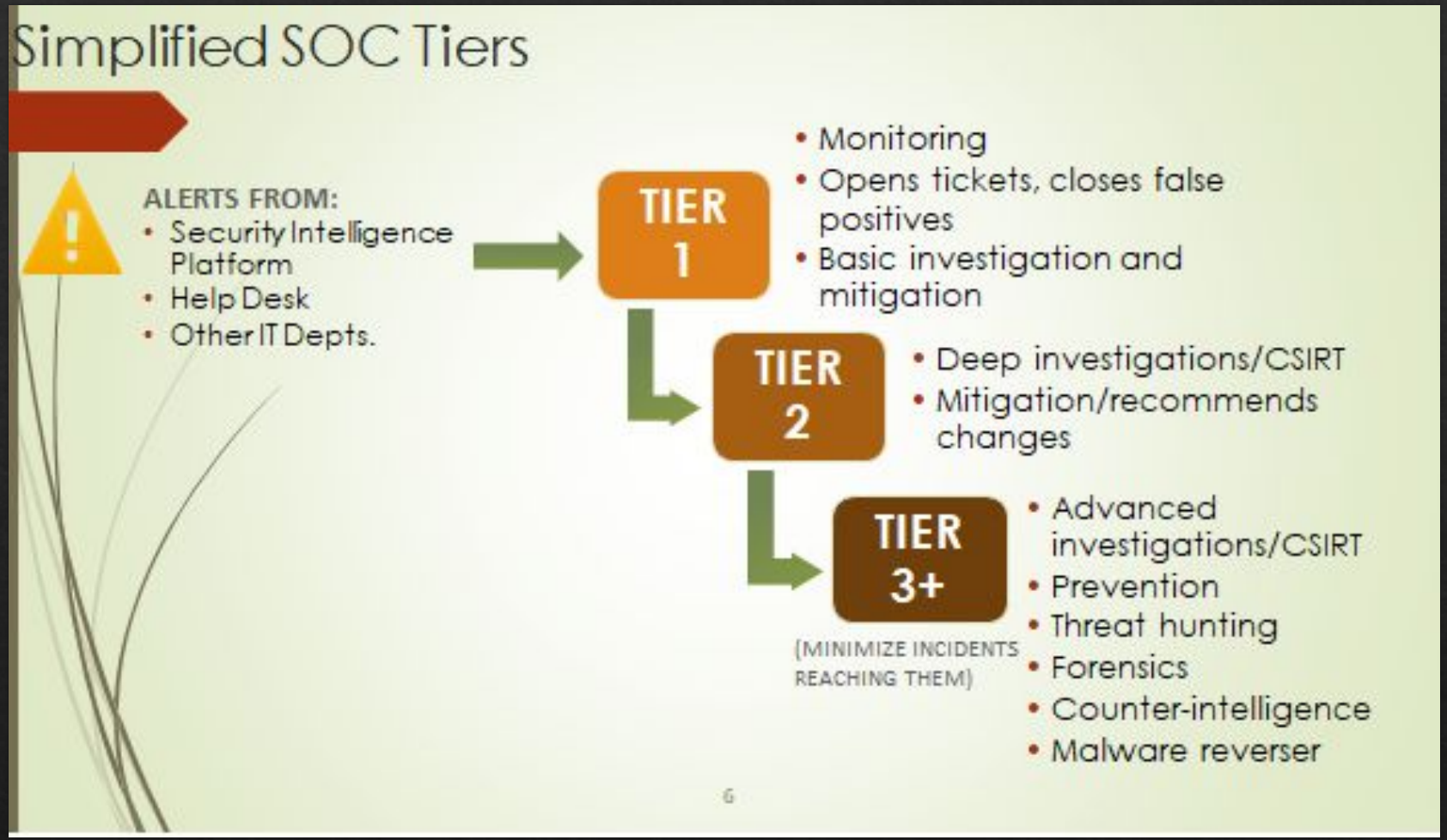
Example: Burglar Alarm System



- Event: Any activity that is logged according to the defined rules, is an event or a security event. Such activity would be related to the security of the system/network. For example, a user logging in, patch updating.
- Suspicious Security Event: A security event that deviates from expected patterns and may require further investigation. For example, a user logging in at an unusual time (such as outside of office working hours) into the employer's corporate network.
- Security Incident: Confirmed violation of security policies or when a suspicious security event is determined to be from an illegitimate user, it becomes a security incident. For example, upon investigation, the IT Security Team determines that the user logging in at the unusual time, was an attacker who compromised the legitimate employee's account.

When a suspicious security event isn't determined to be security incident, then it's labelled as 'Benign' and is called as 'false positive'.

Different levels of SOC Analysts



The CIA Triad

- Confidentiality: Protect the data that needs protection and prevent access to unauthorized individuals.

- Integrity: Ensure the data has not been altered in an unauthorized manner.

- Availability: Ensure data is accessible to authorized users when and where it is needed, and in the form and format that is required.

Authentication

Authentication is a process to prove the identity of the requestor. There are three common methods of authentication:

- Something you know: Passwords or passphrases
- Something you have: Tokens, memory cards, smart cards
- Something you are: Biometrics , measurable characteristics

Failed Authentications in SOC are an indicator of a potential Cyber Security Attack.

There are two types of authentication:

- Using only one of the methods of authentication stated previously is known as single-factor authentication (SFA).
- Granting users access only after successfully demonstrating or displaying two or more of these methods is known as multi-factor authentication (MFA) .

Common best practice is to implement at least two of the three common techniques for authentication:

- Knowledge-based
- Token-based
- Characteristic-based

Is UserID and Password MFA?

Is knowledge-based authentication (such as a password) better than characteristic-based authentication (such as a fingerprint)?

Security Controls

- Physical controls: physical hardware devices, such as a badge reader, architectural features of buildings and facilities that address process-based security needs.
- Technical controls (also called logical controls): security controls that computer systems and networks directly implement.
- Administrative controls (also known as managerial controls): directives, guidelines or advisories aimed at the people within the organization.

-> For example, the way passwords are set according to the provided guidelines, is an administrative control.