Introduction to Key Cybersecurity Concepts

Course Incharge: **Yahya Batla**

Course Instructor: **Instruct**

Security Operations Cener - SOC

A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, and responding to cybersecurity threats and incidents in real-time. It serves as the nerve center for an organization's cybersecurity efforts, employing advanced technologies such as SIEM (Security Information and Event Management) tools and threat intelligence feeds. SOC analysts constantly analyze network traffic, logs, and security alerts to identify and mitigate security breaches and vulnerabilities.

SOC Team Structure

SOC Manager/Director

SOC Team Lead

Security Analysts (L1, L2, and L3)

Threat Hunters

Compliance Analysts

Threat Intelligence Analysts

SIEM Engineer

VA/PT

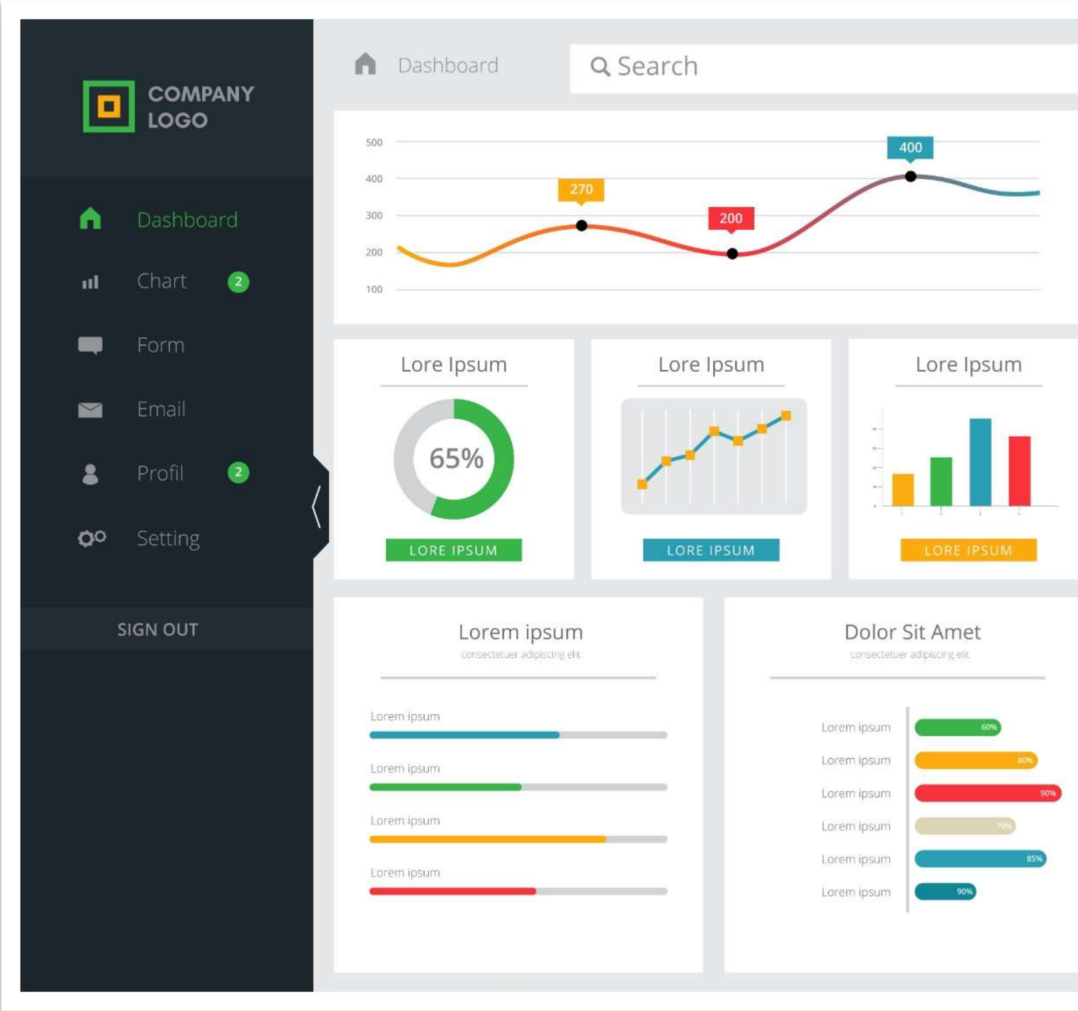
Technologies Used in SOC

SIEM

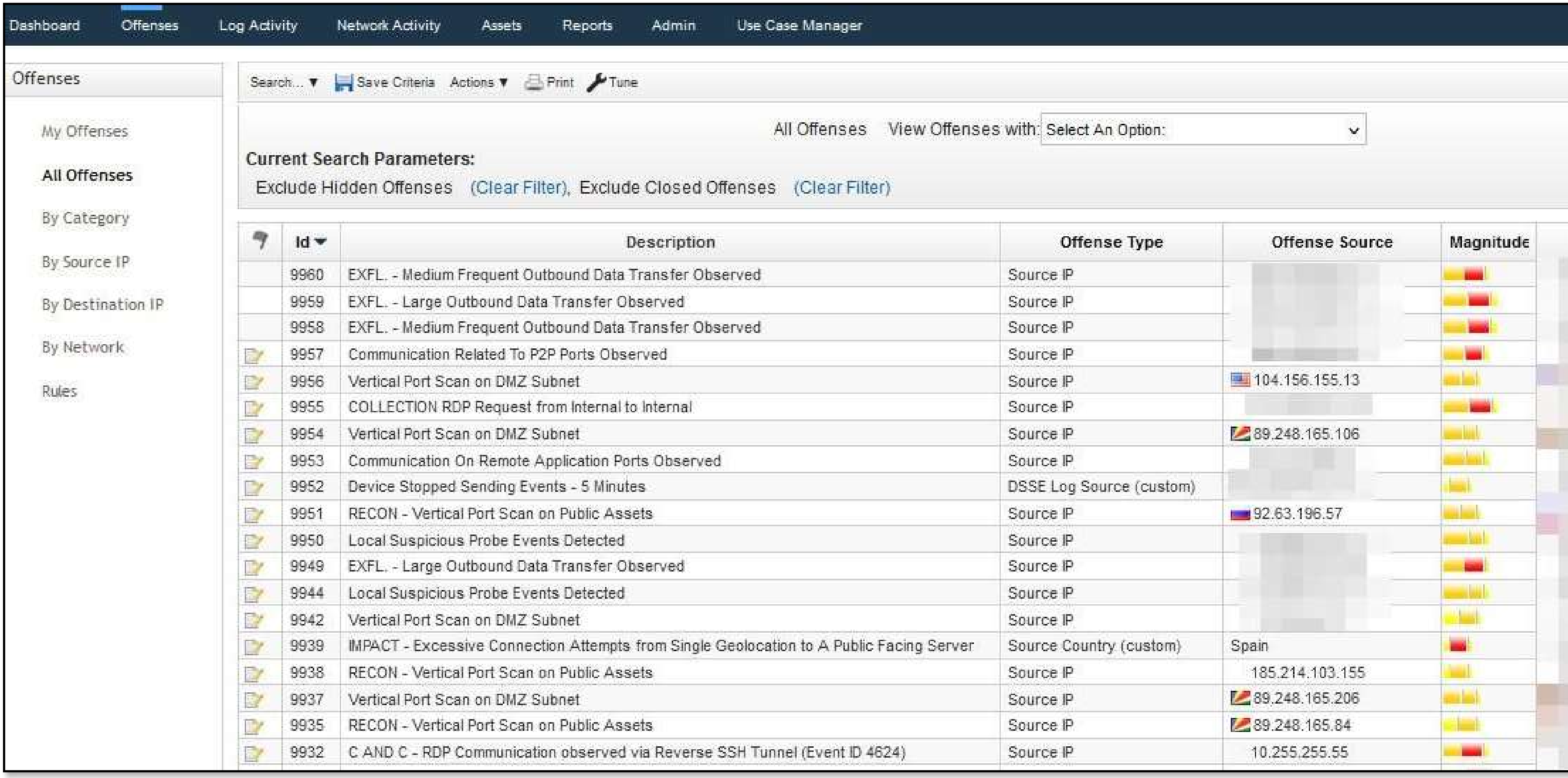
A centralized security platform that collects, correlates, and analyzes security data from various sources to detect and respond to cybersecurity threats.

EDR / EPP

A cybersecurity solution focused on monitoring and securing individual endpoints (computers, servers, devices) to detect, investigate, and respond to suspicious activities and threats at the endpoint level. **EDR is like an antivirus but more advanced.**



SIEM Example - QRadar

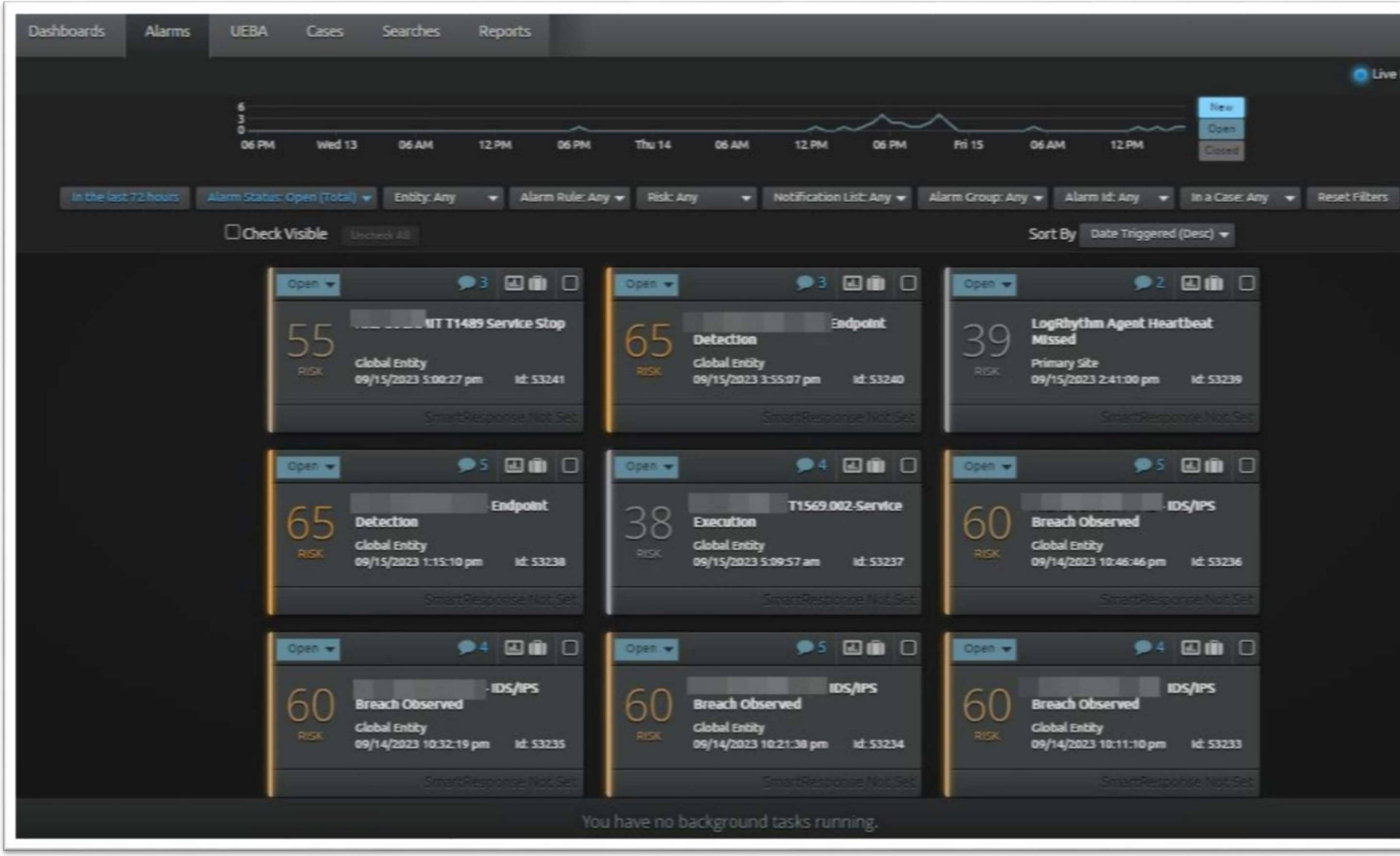


All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id ▾	Description	Offense Type	Offense Source	Magnitude
	9960	EXFL. - Medium Frequent Outbound Data Transfer Observed	Source IP	[redacted]	
	9959	EXFL. - Large Outbound Data Transfer Observed	Source IP	[redacted]	
	9958	EXFL. - Medium Frequent Outbound Data Transfer Observed	Source IP	[redacted]	
	9957	Communication Related To P2P Ports Observed	Source IP	[redacted]	
	9956	Vertical Port Scan on DMZ Subnet	Source IP	104.156.155.13	
	9955	COLLECTION RDP Request from Internal to Internal	Source IP	[redacted]	
	9954	Vertical Port Scan on DMZ Subnet	Source IP	89.248.165.106	
	9953	Communication On Remote Application Ports Observed	Source IP	[redacted]	
	9952	Device Stopped Sending Events - 5 Minutes	DSSE Log Source (custom)	[redacted]	
	9951	RECON - Vertical Port Scan on Public Assets	Source IP	92.63.196.57	
	9950	Local Suspicious Probe Events Detected	Source IP	[redacted]	
	9949	EXFL. - Large Outbound Data Transfer Observed	Source IP	[redacted]	
	9944	Local Suspicious Probe Events Detected	Source IP	[redacted]	
	9942	Vertical Port Scan on DMZ Subnet	Source IP	[redacted]	
	9939	IMPACT - Excessive Connection Attempts from Single Geolocation to A Public Facing Server	Source Country (custom)	Spain	
	9938	RECON - Vertical Port Scan on Public Assets	Source IP	185.214.103.155	
	9937	Vertical Port Scan on DMZ Subnet	Source IP	89.248.165.206	
	9935	RECON - Vertical Port Scan on Public Assets	Source IP	89.248.165.84	
	9932	C AND C - RDP Communication observed via Reverse SSH Tunnel (Event ID 4624)	Source IP	10.255.255.55	

SIEM Example - LogRhythm



Open 3
55 RISK
[redacted] T1489 Service Stop
Global Entity
09/15/2023 5:00:27 pm Id: 53241
SmartResponse Not Set

Open 3
65 RISK
[redacted] Endpoint Detection
Global Entity
09/15/2023 3:55:07 pm Id: 53240
SmartResponse Not Set

Open 2
39 RISK
LogRhythm Agent Heartbeat Missed
Primary Site
09/15/2023 2:41:00 pm Id: 53239
SmartResponse Not Set

Open 5
65 RISK
[redacted] Endpoint Detection
Global Entity
09/15/2023 1:15:10 pm Id: 53238
SmartResponse Not Set

Open 4
38 RISK
[redacted] T1569.002-Service Execution
Global Entity
09/15/2023 5:09:57 am Id: 53237
SmartResponse Not Set

Open 5
60 RISK
[redacted] IDS/IPS Breach Observed
Global Entity
09/14/2023 10:46:46 pm Id: 53236
SmartResponse Not Set

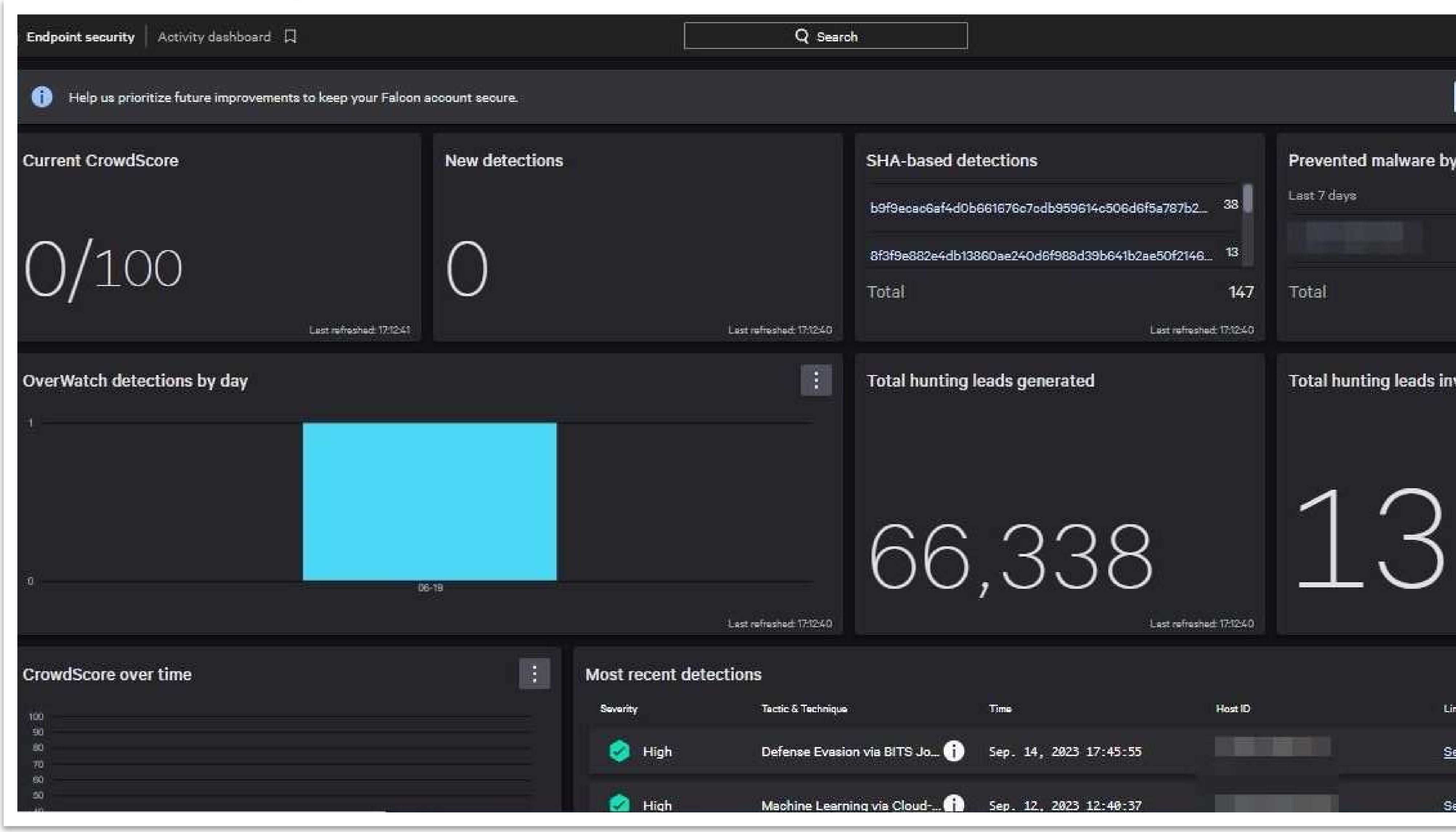
Open 4
60 RISK
[redacted] IDS/IPS Breach Observed
Global Entity
09/14/2023 10:32:19 pm Id: 53235
SmartResponse Not Set

Open 5
60 RISK
[redacted] IDS/IPS Breach Observed
Global Entity
09/14/2023 10:21:38 pm Id: 53234
SmartResponse Not Set

Open 4
60 RISK
[redacted] IDS/IPS Breach Observed
Global Entity
09/14/2023 10:11:10 pm Id: 53233
SmartResponse Not Set

You have no background tasks running.

EDR Example - CrowdStrike



Help us prioritize future improvements to keep your Falcon account secure.

Current CrowdScore

0/100

Last refreshed: 17:12:41

New detections

0

Last refreshed: 17:12:40

SHA-based detections

b9f9ecac6af4d0b661676c7cdb959614c506d6f5a787b2...	38
8f3f9e882e4db13860ae240d6f988d39b641b2ae50f2146...	13
Total	147

Last refreshed: 17:12:40

Prevented malware by

Last 7 days

[redacted]

Total

OverWatch detections by day

Last refreshed: 17:12:40

Total hunting leads generated

66,338

Last refreshed: 17:12:40

Total hunting leads in

13

CrowdScore over time

Most recent detections

Severity	Tactic & Technique	Time	Host ID	Li
High	Defense Evasion via BITS Jo...	Sep. 14, 2023 17:45:55	[redacted]	Se
High	Machine Learning via Cloud-...	Sep. 12, 2023 12:40:37	[redacted]	Se

Key Routine Tasks

Monitoring Offenses

Raising Tickets/Cases

Threat Hunting

Creating Use Cases

Dealing with Customer

Creating Reports

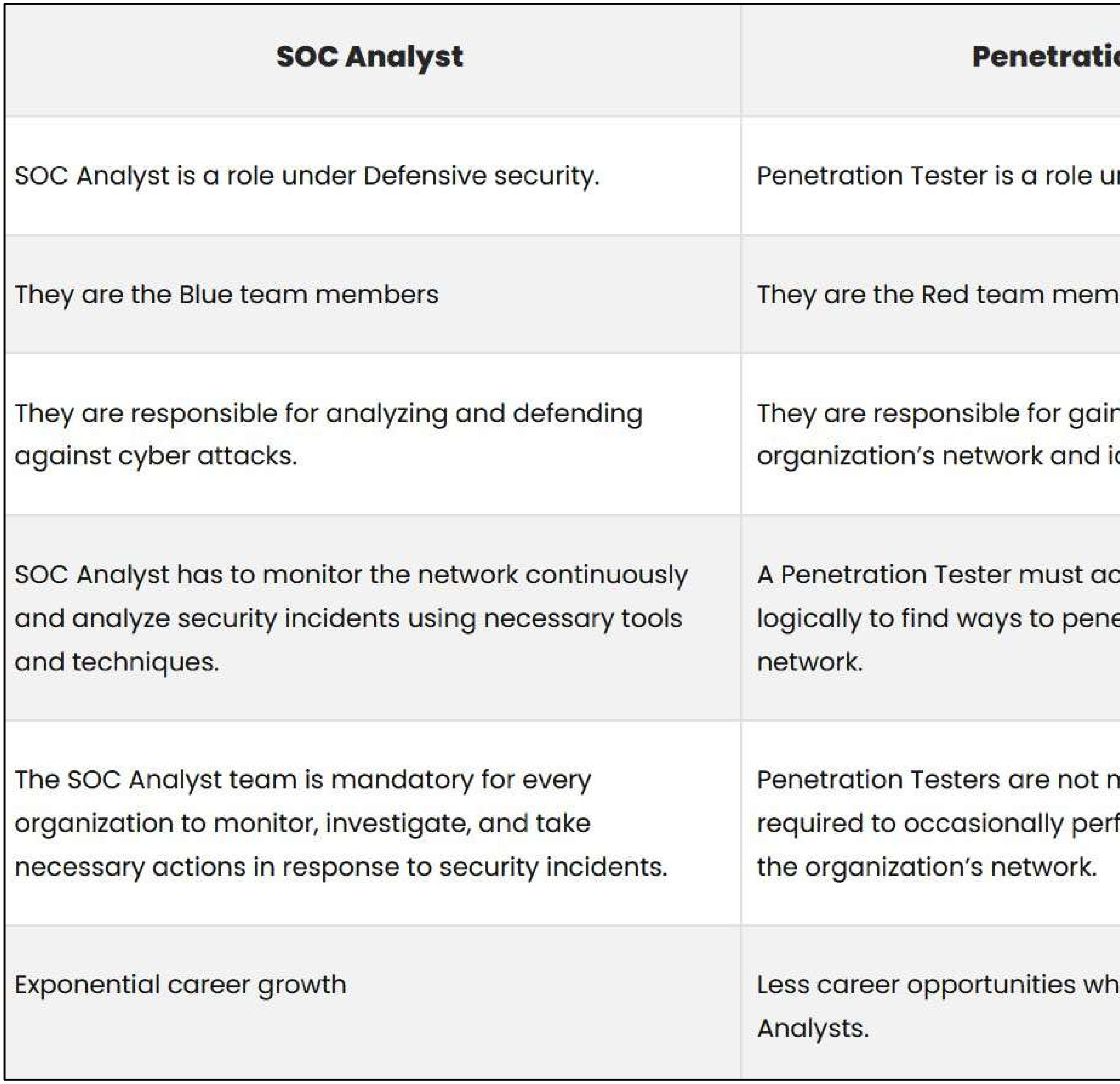
Introduction to Penetration Testing

Penetration testing, or ethical hacking, is a systematic process of evaluating computer systems, networks, or applications for vulnerabilities. Conducted by cybersecurity professionals, known as penetration testers, the goal is to identify and address potential security risks before malicious actors can exploit them. By simulating real-world cyber attacks, penetration testing helps organizations enhance their defenses, secure sensitive data, and fortify against evolving threats.

SOC

VS

P T



SOC Analyst	Penetratio
SOC Analyst is a role under Defensive security.	Penetration Tester is a role u
They are the Blue team members	They are the Red team mem
They are responsible for analyzing and defending against cyber attacks.	They are responsible for gai organization's network and i
SOC Analyst has to monitor the network continuously and analyze security incidents using necessary tools and techniques.	A Penetration Tester must a logically to find ways to pen network.
The SOC Analyst team is mandatory for every organization to monitor, investigate, and take necessary actions in response to security incidents.	Penetration Testers are not r required to occasionally per the organization's network.
Exponential career growth	Less career opportunities wh Analysts.

Introduction to Security Controls

Security controls in cybersecurity refer to measures and safeguards implemented to protect information systems, data, and technology infrastructure from security risks and potential threats. These controls are designed to mitigate vulnerabilities and ensure the confidentiality, integrity, and availability of sensitive information. Security controls can be categorized into three main types:

1. Administrative Controls
2. Technical Controls
3. Physical Controls

Administrative Controls

Policies, procedures, and guidelines that define the framework for security management, such as access control policies, employee training programs, and risk management frameworks. Imagine having clear rules for who can access certain information and what they can do with it. It's like setting up guidelines to make sure everyone behaves securely.

Policies and Procedures: These are like the rulebook for an organization's cybersecurity. They define who has access to what, how data should be handled, and what to do in case of a security incident.

Employee Training: Think of this as ongoing education to make sure everyone in the organization knows how to spot and respond to potential security threats.

Technical Controls

Automated tools and technologies that enforce security policies and protect systems, including firewalls, encryption, antivirus software, intrusion detection systems, and access controls. These are like digital superheroes that work in the background to stop bad guys. They include things like antivirus software, locks on digital doors, and security systems that watch for any unusual activity.

Firewalls and Encryption: Firewalls act as digital bouncers, deciding who gets in and who stays out. Encryption is like converting your information into a secret code that only the intended recipient can decode.

Antivirus Software: This is akin to having a security guard in your computer, constantly scanning for and neutralizing malicious software.

Physics Controls

Measures to safeguard physical assets, facilities, and resources, such as biometric access systems, surveillance cameras, locks, and environmental controls (e.g., temperature and humidity monitoring). Imagine putting locks on your front door and having security cameras around your house. In the digital world, physical controls include measures like fingerprint scanners and special locks to keep your information safe.

Biometric Access Systems: These are like using your fingerprint or eye scan as a super-secure key to access digital information.

Surveillance Cameras and Environmental Controls: Cameras keep an eye on things, and environmental controls ensure that the physical space where data is stored stays safe from things like temperature fluctuations or humidity.

Authentication and Authorization

Think of the library as a secure place with valuable books. To borrow a book, you need a library card. When you show your library card at the counter, you're **authenticating** yourself. The library card is like your proof of identity.

Authorization is like determining which sections you're allowed to enter based on your library card. For example, if you have a regular membership, you might be authorized to borrow books from the general fiction and non-fiction sections. However, the rare books section might be off-limits unless you have a special membership or permission

In this example, authentication is proving you're a library member with your library card, and authorization is deciding which parts of the library (sections or services) you can access based on your membership level or permissions.

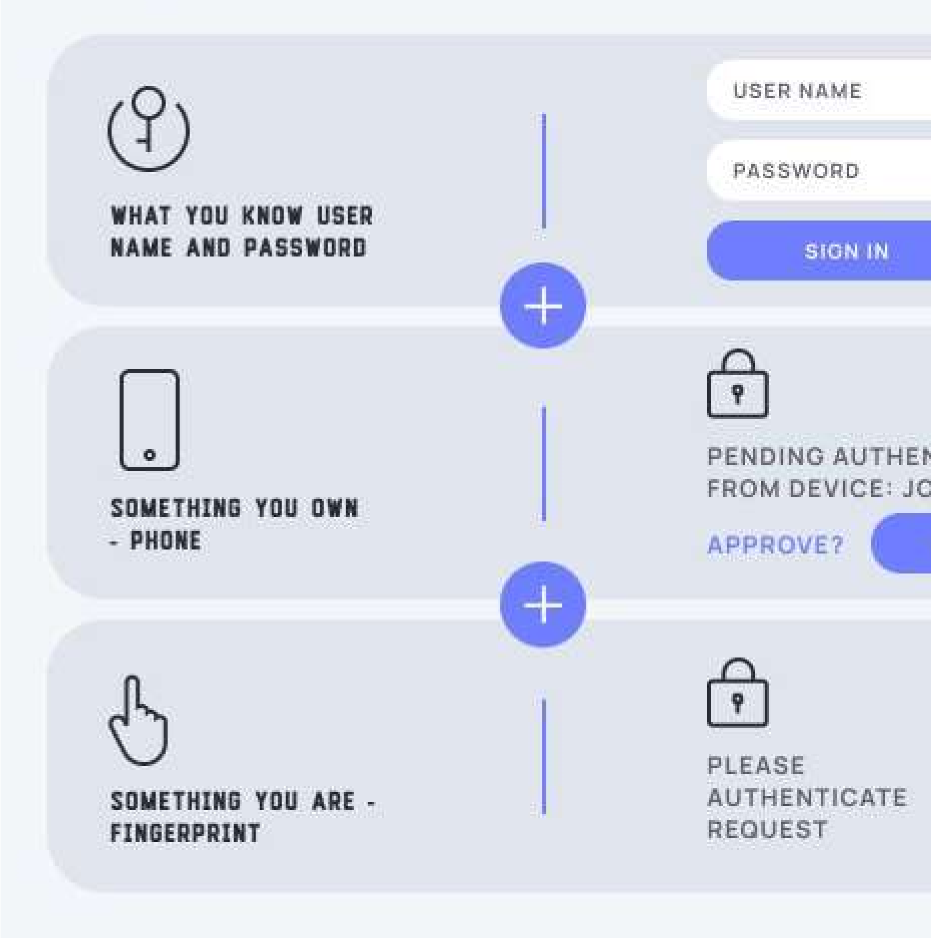
Types of Authentication

There are three basic types of authentication.

Knowledge-based — Something like a password or PIN code that only the identified user would know.

Property-based — This means the user possesses an access card, key, key fob or authorized device unique to them.

Biological-based — This type of authentication might be a physical trait like a user's fingerprint or retinal pattern. It could also be a behavioral process unique to each user, like their voiceprints or keystroke dynamics.

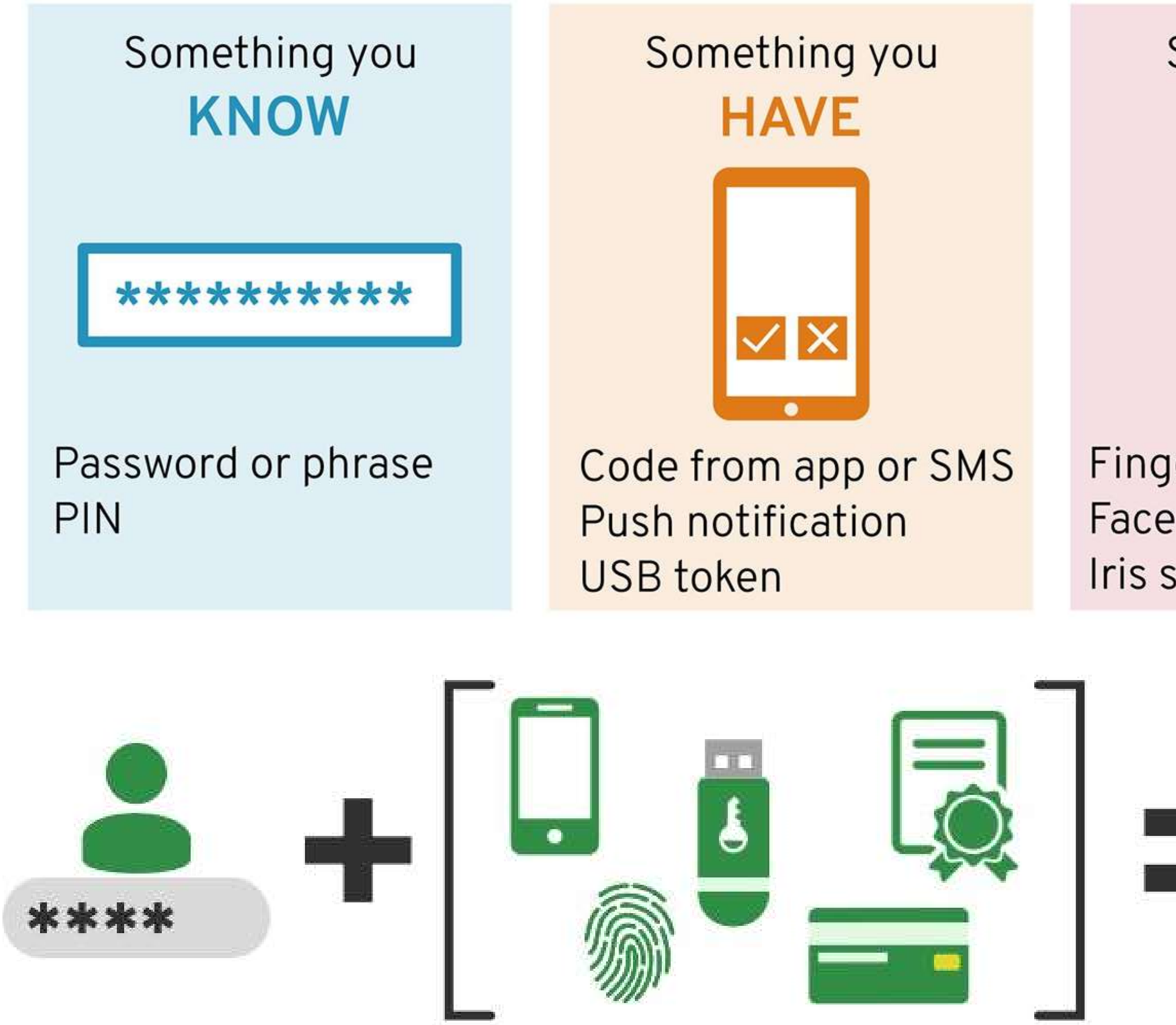

WHAT YOU KNOW USER NAME AND PASSWORD
USER NAME
PASSWORD
SIGN IN
SOMETHING YOU OWN - PHONE
PENDING AUTHEN
FROM DEVICE: JO
APPROVE?
SOMETHING YOU ARE - FINGERPRINT
PLEASE AUTHENTICATE REQUEST

Multifactor Authentication

Involves using two or more authentication methods from different categories (e.g., something you know, something you have, something you are).

Strengths: Enhances security by requiring multiple forms of identification.

Weaknesses: Can be inconvenient for users, and methods must be chosen wisely.



Importance of Authorization

Authorization is critically important for several reasons in the realm of computer security and information systems:

1. Authorization ensures that sensitive data is accessed only by individuals or systems with the appropriate permissi
   helps prevent unauthorized users from viewing, modifying, or deleting important information.
2. Unauthorized access to systems or data can lead to data breaches, unauthorized modifications, or other security in
   Authorization mechanisms prevent unauthorized users from gaining entry and carrying out malicious activities.
3. Authorization helps maintain the confidentiality of sensitive information. By restricting access to authorized users
   organizations can safeguard private data and protect the privacy of individuals.
4. Authorization mechanisms contribute to the overall integrity of a system by preventing unauthorized changes. On
   with the appropriate permissions can modify system configurations, reducing the risk of unintentional or maliciou
   alterations.

بنو قابل
اپنی دُنیا آپ پیدا کر

THANK YOU