Cybersecurity 101

DURATION : 1’30

Summary

1. Introduction to cybersecurity
2. What is an ethical hacking
3. Different types of hacker
4. Hacking vocabulary
5. Other vocabulary words
6. All steps to execute a pentest & Kill chain frameworks
7. Improve your skills

Cybersecurity

- Cybersecurity is the practice of protecting computer systems, networks, devices, and data from unauthorized access, theft, damage, or disruption *(perturbation)*.
- In simpler terms, it's about keeping digital information safe and trustworthy *(fiable)* whether it's stored on your phone, a company server, or in the cloud.

CIA Triad: The Foundation of Security Policies

- 5 pillars of information security are:
  - **Confidentiality:**
    Cleartext or password stealing has an impact on confidentiality.
  - **Integrity:**
    Data tampering has an impact on integrity.
  - **Availability:**
    DoS attack has an impact on availability.
  - **Authenticity:**
    Verifies the sender's identity and source of the message.
  - **Non repudiation:**
    Guarantee that the sender of a message cannot deny having sent the message and the recipient cannot deny having received it.

Confidentiality

Ensuring that sensitive data is only accessible to authorized individuals.

Security Policy Considerations:

- Define access control policies (e.g., role-based access control – RBAC).
- Implement least privilege and need-to-know principles.
- Establish encryption standards for data at rest and in transit.

Security Solution Deployment:

- Use **encryption (AES, TLS)** for securing sensitive data.
- Implement **multi-factor authentication (MFA)** to prevent unauthorized access.
- Deploy **firewalls, VPNs, and access control lists (ACLs)** to restrict network exposure.

Integrity

Ensuring that data remains accurate and unaltered by unauthorized modifications.

Security Policy Considerations:

Define policies for data validation and integrity checks.	Establish logging and monitoring requirements.	Implement change management controls for critical systems.

Security Solution Deployment:

Use **hashing (SHA-256, HMAC)** for verifying data integrity.	Deploy **file integrity monitoring (FIM)** and digital signatures.	Implement **version control and audit logs** to track data modifications.

Availability

Ensuring that systems and data are accessible when needed.

Security Policy Considerations:

Define uptime and recovery time objectives (RTO).	Establish redundancy and failover mechanisms.	Implement business continuity and disaster recovery (BC/DR) plans.

Security Solution Deployment:

Deploy **load balancers, DDoS protection, and redundant servers**.	Implement **automatic backups and failover systems**.	Use **high-availability (HA) architectures** to minimize downtime.

DAD Model: Identifying and Mitigating Threats

The DAD model focuses on the three primary security risks that oppose the CIA triad.

Disclosure (Threat to Confidentiality)
Unauthorized exposure of sensitive information.

Mitigation:
- Apply data masking, encryption, and access controls.
- Implement security awareness training to prevent phishing attacks.

Alteration (Threat to Integrity)
Unauthorized modifications to data or systems.

Mitigation:
- Use digital signatures, checksums, and blockchain for verification.
- Deploy SIEM (Security Information and Event Management) to detect anomalies.

Destruction (Threat to Availability)
Loss or deletion of critical data or service disruptions.

Mitigation:
- Implement automated backups and disaster recovery solutions.
- Use redundancy, failover clusters, and cloud replication.

AAA Framework: Controlling Access and Monitoring Activity (1/2)

1. **Identification :** The information on credentials identifies the user.
   - Example: Name, username, ID number, employee number, SSN etc.

2. **Authentication :** "Prove you are the legitimate User" (Should always be done with Multifactor Authentication).
   - Authentication Factors:
     - Something you know (e.g. - password)
     - Something you have (e.g. - smart card)
     - Something you are (e.g. - fingerprint)
     - Something you do (e.g. - android pattern; manual signature)
     - Somewhere you are (e.g. - geolocation)

- *Multi-factor authentication generally uses two of this examples (e.g. - Something you Know and Something you Have (but never on same category).*

AAA Framework: Controlling Access and Monitoring Activity (2/2)

3. **Authorization** : Defines the permissions (allow/grant or deny).
4. **Auditing:** Record a log of events and activities.
5. **Accouting:** Review log files to check for compliance or violations.

Bringing It All Together: Designing & Deploying a Security Solution

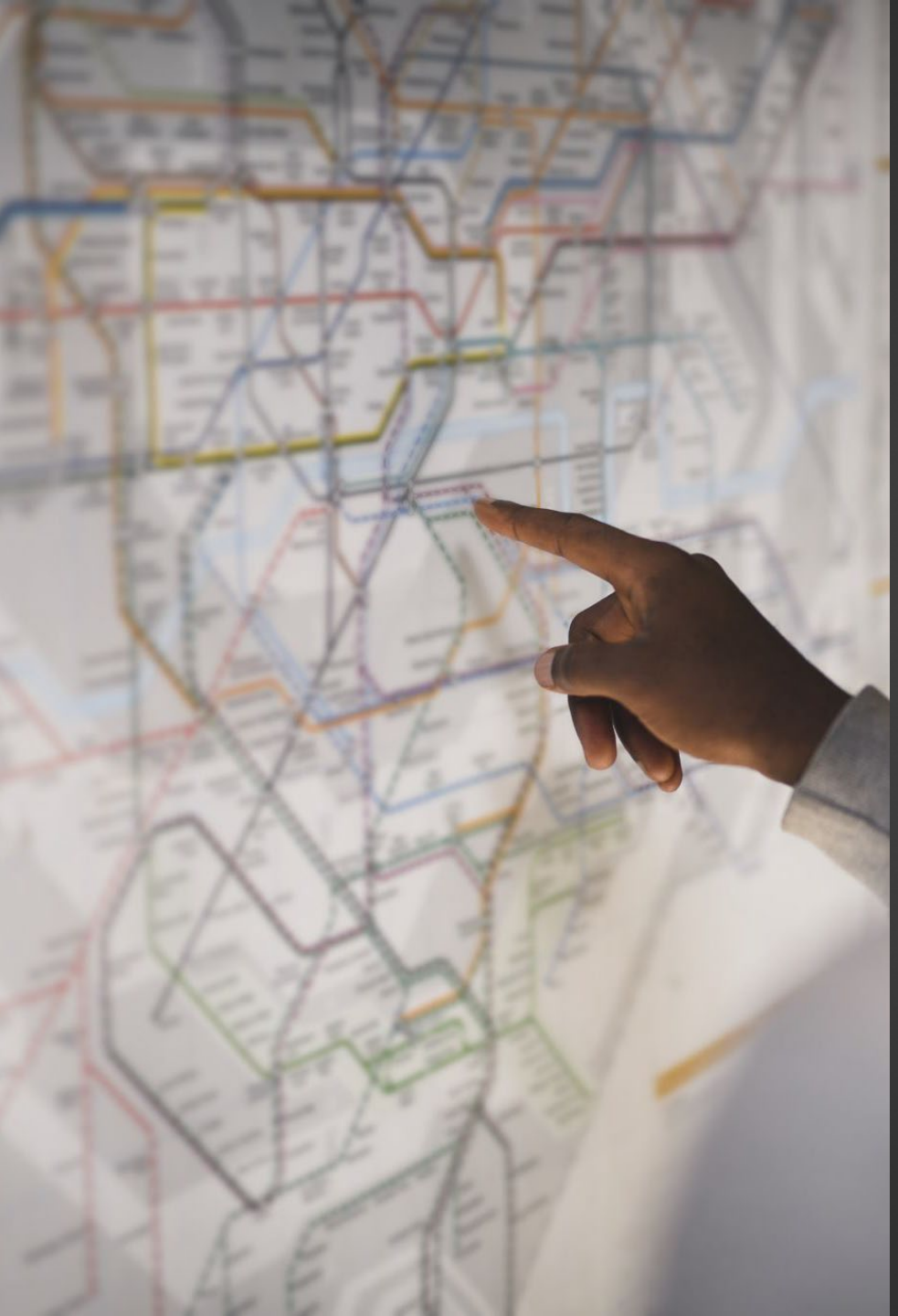
To build an effective security strategy, organizations should:

1 Use CIA to define protection goals (Confidentiality, Integrity, Availability).

2 Identify DAD threats and implement countermeasures.

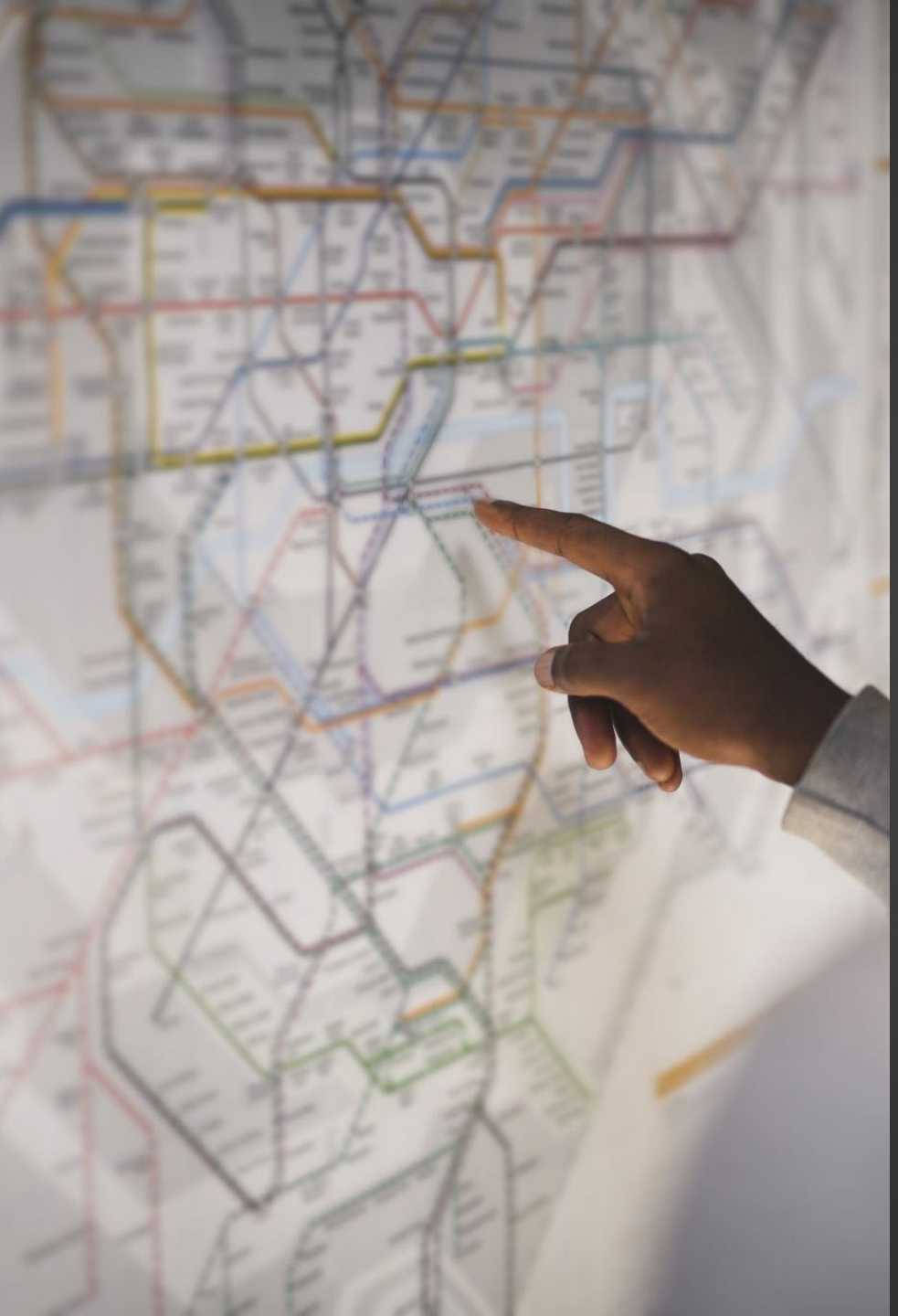
3 Enforce AAA to secure access and track activities.

By integrating these models into security policies and solutions, organizations can enhance data protection, reduce risks, and improve compliance.



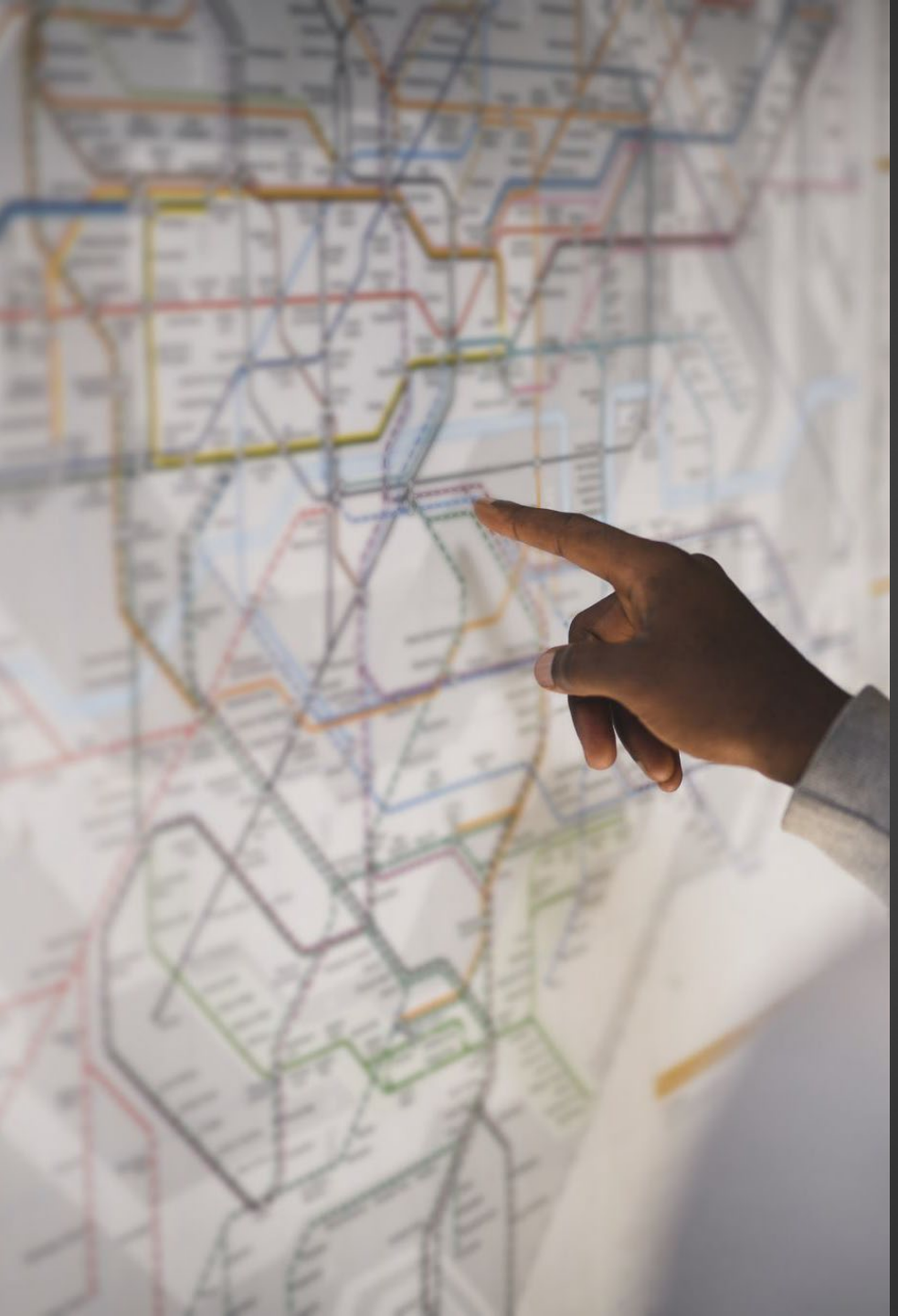
Security Management Planning (1/3)

- Strategic Plan (5 years)
  - Purpose:
    Define the **long-term cybersecurity vision** and align it with the organization's **business strategy**.
  - Content:
    - Cybersecurity vision and mission
    - Compliance and regulatory targets (e.g., ISO 27001, NIST, GDPR)
    - High-level objectives (e.g., "achieve zero major incidents")
  - Example: "In five years, our organization will have a fully integrated, risk-based cybersecurity program aligned with NIST CSF, with a mature SOC, strong identity management, and resilience capabilities."



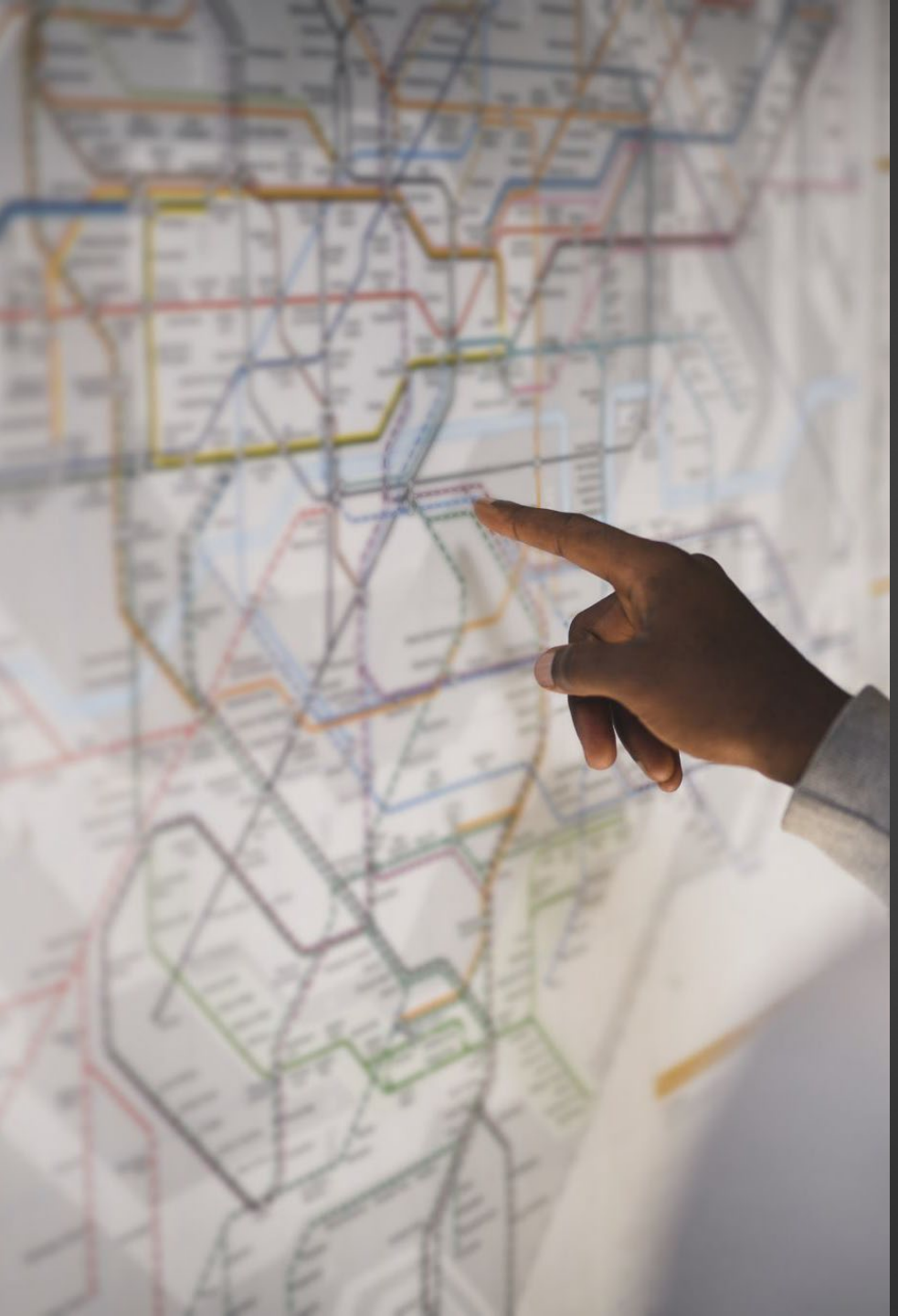
Security Management Planning (1/4)

- Tactical Plan (1 year)
  - Purpose:
    Translate the strategic plan into **concrete annual objectives and projects**.
    This is often represented in an **annual security roadmap or Cybersecurity Master Plan**.
  - Content:
    - Annual objectives and KPIs
    - Policy updates
    - Milestones for technical improvements (SIEM, IAM, DLP, etc.)
  - Example:
    - Deploy MFA for all privileged accounts
    - Improve SOC coverage with cloud log ingestion



Security Management Planning (2/4)

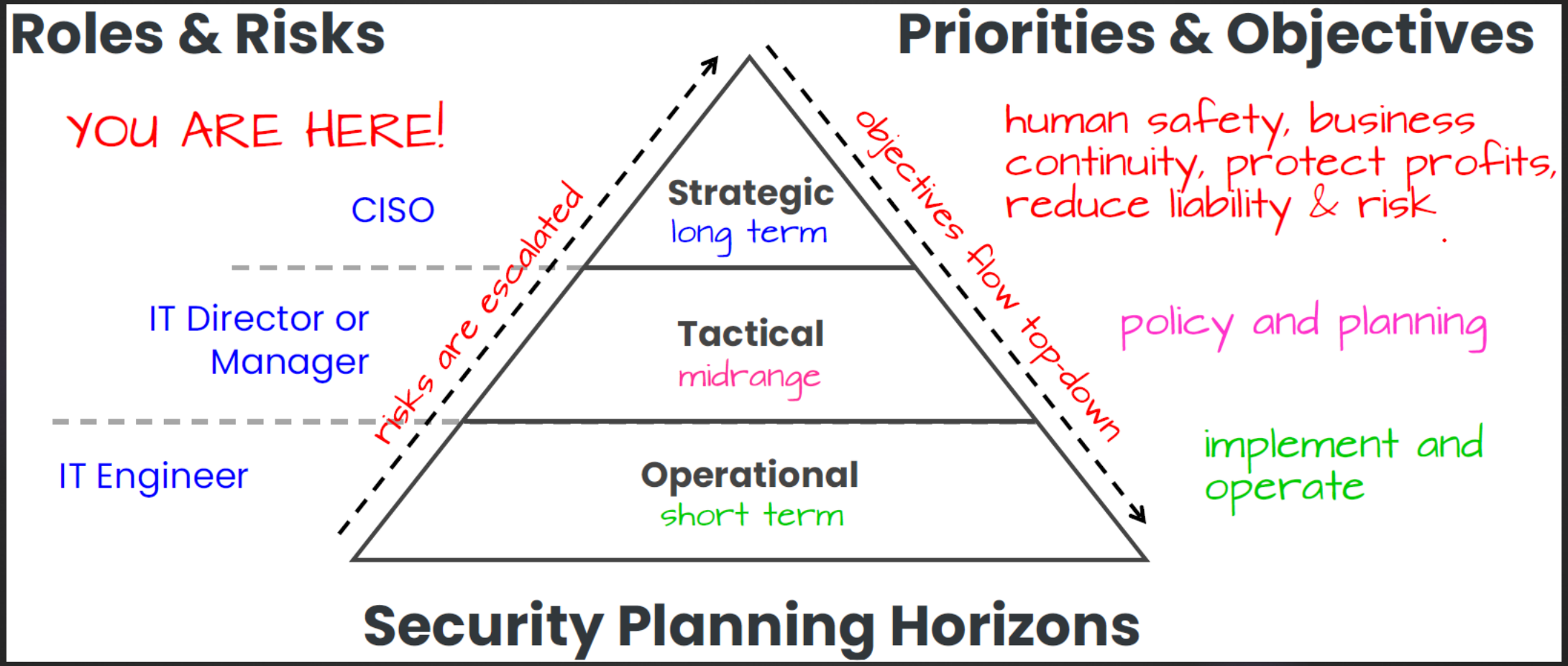
- Operational Plan (daily to quarterly)
  - Purpose:
    Execute the tactical plan through **day-to-day activities**, ensuring consistent protection and monitoring.
  - Content:
    - Daily/weekly operations (monitoring, patching, backups)
    - Vulnerability scanning and remediation
  - Example:
    - Review firewall rules monthly
    - Patch critical systems within 10 days
    - Run phishing simulations quarterly
    - Generate monthly security dashboards



Security Management Planning (3/4)

- Operational Plan (daily to quarterly)
  - Purpose:
    Execute the tactical plan through **day-to-day activities**, ensuring consistent protection and monitoring.
  - Content:
    - Daily/weekly operations (monitoring, patching, backups)
    - Vulnerability scanning and remediation
  - Example:
    - Review firewall rules monthly
    - Patch critical systems within 10 days
    - Run phishing simulations quarterly
    - Generate monthly security dashboards

Security Management Planning (4/4)



Security Control Frameworks (1/2)

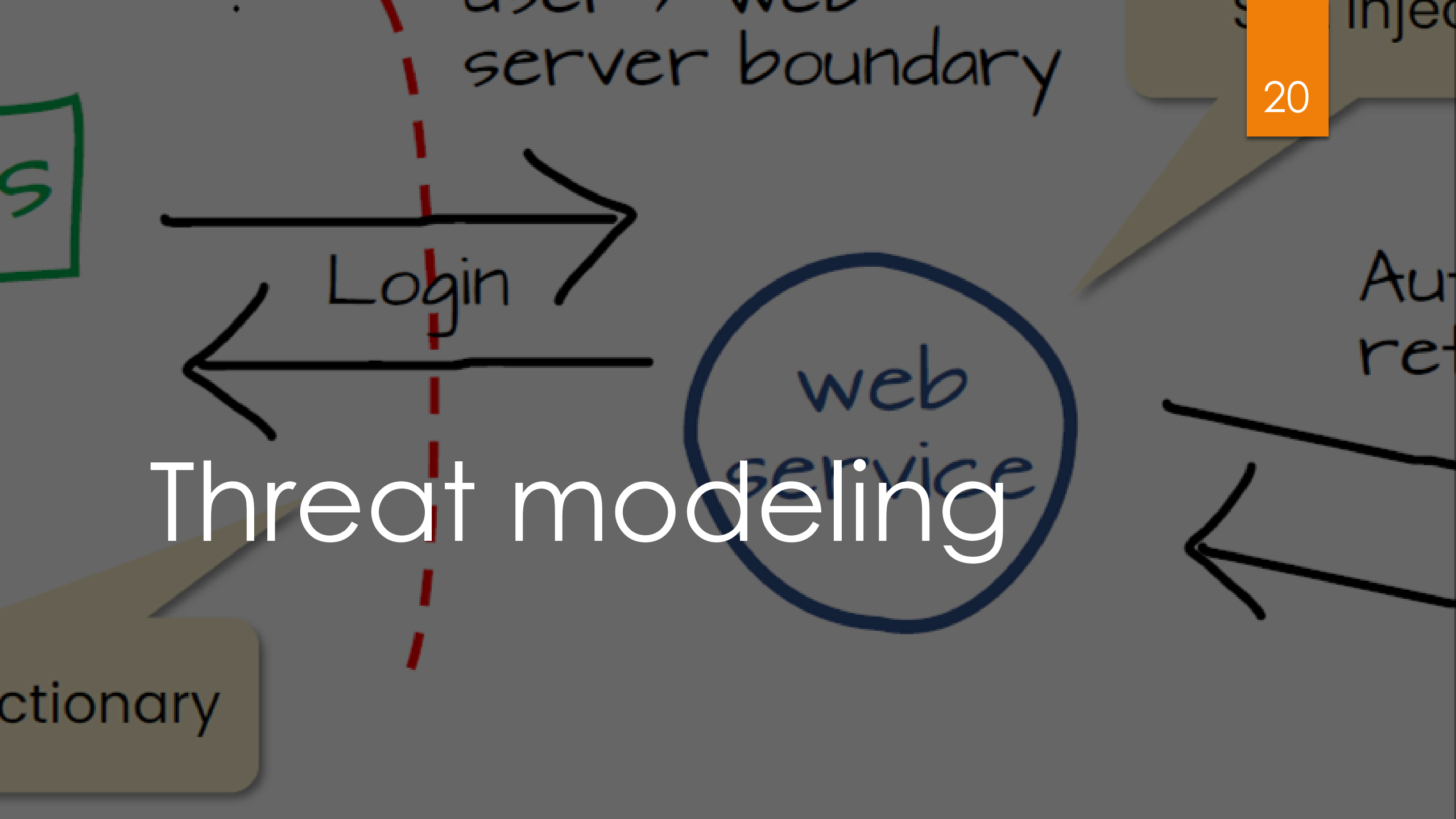
- ISO (International Organization for Standardization) defines standards for many items (industrial, commercial software, protocols, etc.
- NIST (National Institute of Standards and Technology) is a US federal and the well-known publications is the NIST Special Publication 800-53 "Security and Privacy Controls for Information Systems and Organizations".
- COBIT (Control Objectives for Information and Related Technologies) is a documented set of best IT security practices crafted by ISACA (Information Systems Audit and Control Association).
- SABSA (Sherwood Applied Business Security Architecture) is a methodology for developing risk-driven enterprise security and information assurance architectures.

Security Control Frameworks (2/2)

- PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards and requirements designed to ensure the protection of sensitive credit card and debit card information.
- FedRAMP (Federal Risk and Authorization Management Program) is a US government wide program designed to standardize the security assessment, authorization and continuous monitoring processes for cloud products and services used by federal agencie.
- ITIL (Information Technology Infrastructure Library) initially crafted by the British government, is a set of recommended best practices for the optimization of IT services to support business growth, transformation and change.

Security Policy, Standards, Procedures and Guidelines

- **Security Policies**
  - Define the organization's overall security objectives.
    Ex: "All users must authenticate using strong passwords to protect organizational systems and data."
- **Security Standards, Baselines and Guidelines**
  - **Standards** define requirements for the use of hardware, software, etc.
    Ex: "All passwords must be at least 12 characters long, include upper and lower case letters, numbers, and special characters. Passwords must expire every 90 days."
  - **Baselines** defines a minimum level of security that every system throughout the organization must meet.
    Ex: "All company laptops and servers must have password complexity enabled and account lockout after 5 failed login attempts."
  - **Guidelines** offers recommendations on how standards and baselines are implemented.
    Ex: "It is recommended to use a password manager approved by the IT department to store complex passwords securely."
- **Security Procedures**
  - Detailed step-by-step / how-to document. Ex: "Create a GPO…"



Threat modeling

Threat modeling

3 approaches to threat modeling

Common approaches to threat modeling:

Focused on Assets. Uses **asset valuation** results to identify threats to the valuable assets.

Focused on Attackers. Identify potential attackers and identify threats based on the **attacker's goals**

Focused on Software . Considers **potential threats** against the software the org develops.

Threat modeling

STRIDE

developed by Microsoft

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

Threat modeling

PASTA

Stage I: Definition of Objectives

Stage II: Definition of Technical Scope

Stage III: App Decomposition & Analysis

Stage IV: Threat Analysis

Stage V: Weakness & Vulnerability Analysis

Stage VI: Attack Modeling & Simulation

Stage VII: Risk Analysis & Management

focuses on developing countermeasures based on asset value

Threat modeling

VAST

based on Agile PM principles

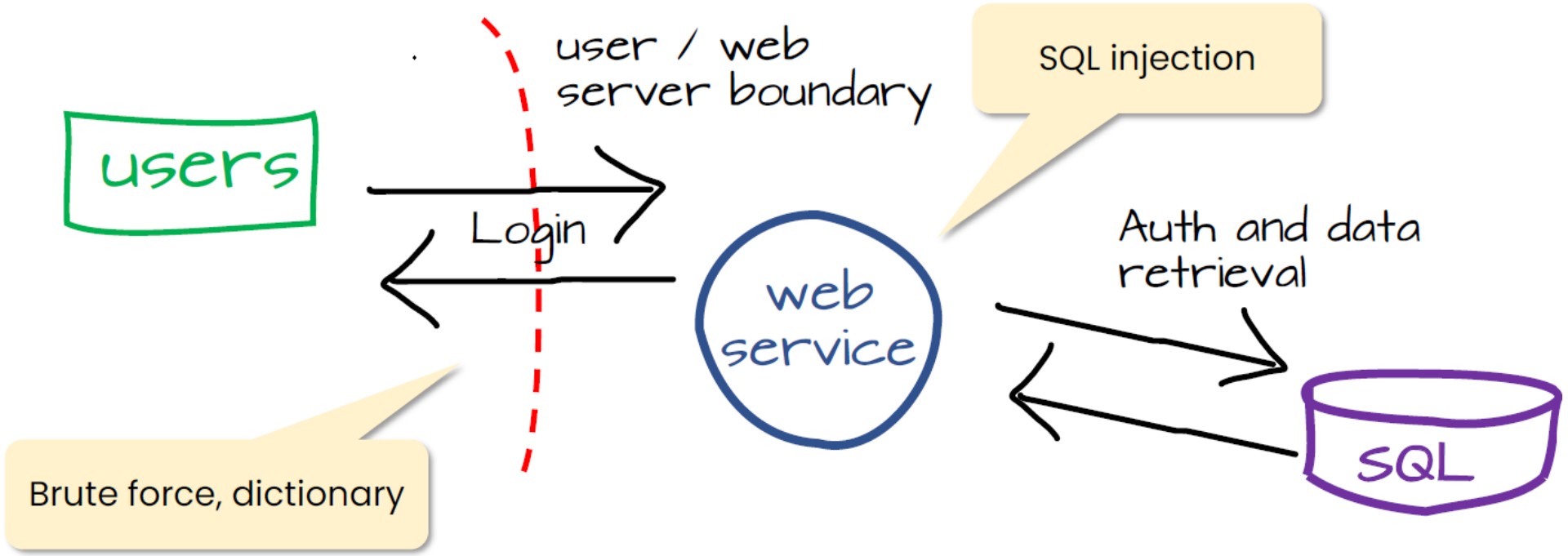
Visual

Agile

Simple

Threat

GOAL: Scalable integration of threat management into an Agile programming environment



Threat modeling

Threat modeling: Prioritization & Response

DREAD

based on answer to 5 questions

Damage potential

Reproducibility

Exploitability

Affected users

Discoverability

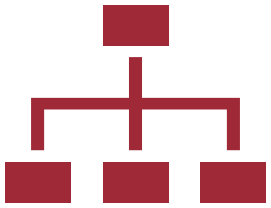
Threat modeling: Prioritization & Response

- **DREAD is based on the answers to five main questions about each threat:**
  - Damage: How severe is the damage if exploited ?
  - Reproducibility: How easy is it to reproduce the attack ?
  - Exploitability: How easy is it to launch the attack ?
  - Affected Users: How many users would be impacted?
  - Discoverability: How easy is it to find the vulnerability?

	Consequence				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Almost Certain	**Medium**	**High**	**High**	**Extreme**	**Extreme**
Likely	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Possible	**Medium**	**Medium**	**High**	**High**	**Extreme**
Unlikely	**Low**	**Medium**	**Medium**	**High**	**High**
Rare	**Low**	**Low**	**Medium**	**High**	**High**


SUPPLY
CHAIN
RISK
MANAGEMENT

SCRM Overview



Definition:

Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating risks that arise from an organization's suppliers, vendors, partners, or service providers.

Why it matters:

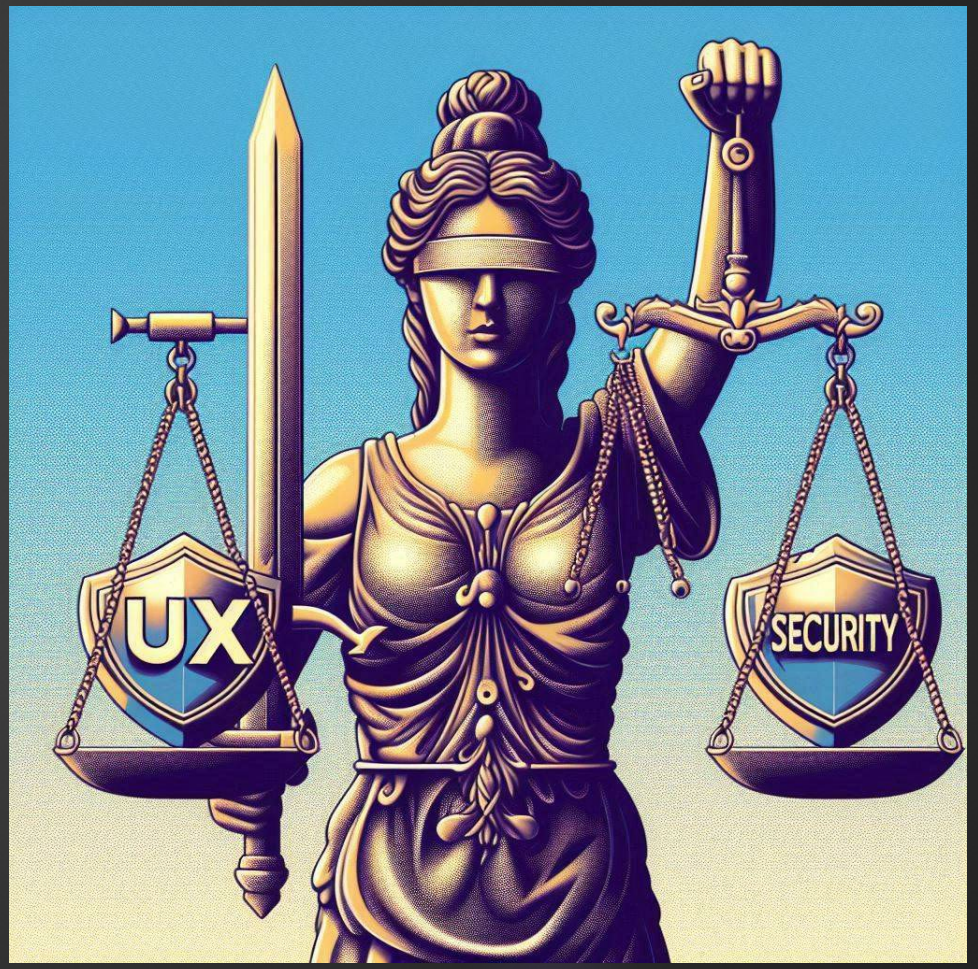
Modern systems rely on third-party hardware, software, and services.

A single compromised supplier can introduce security weaknesses or malware (e.g., SolarWinds).

"***You can outsource services, not responsibility***".

Security vs UX

- There is an inter dependency between these two attributes.
- When security goes up, UX come down and vice versa.
- Any organization should balance between these two qualities to arrive at a balanced information system.



What is an Ethical Hacking ?

- Ethical hacking involves the use of hacking tools, tricks and techniques to identify vulnerabilities and secure system security.
- If focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system.
- Ethical hackers perform security assessments for an organization with the permission of concerned authorities.

Different types of hacker

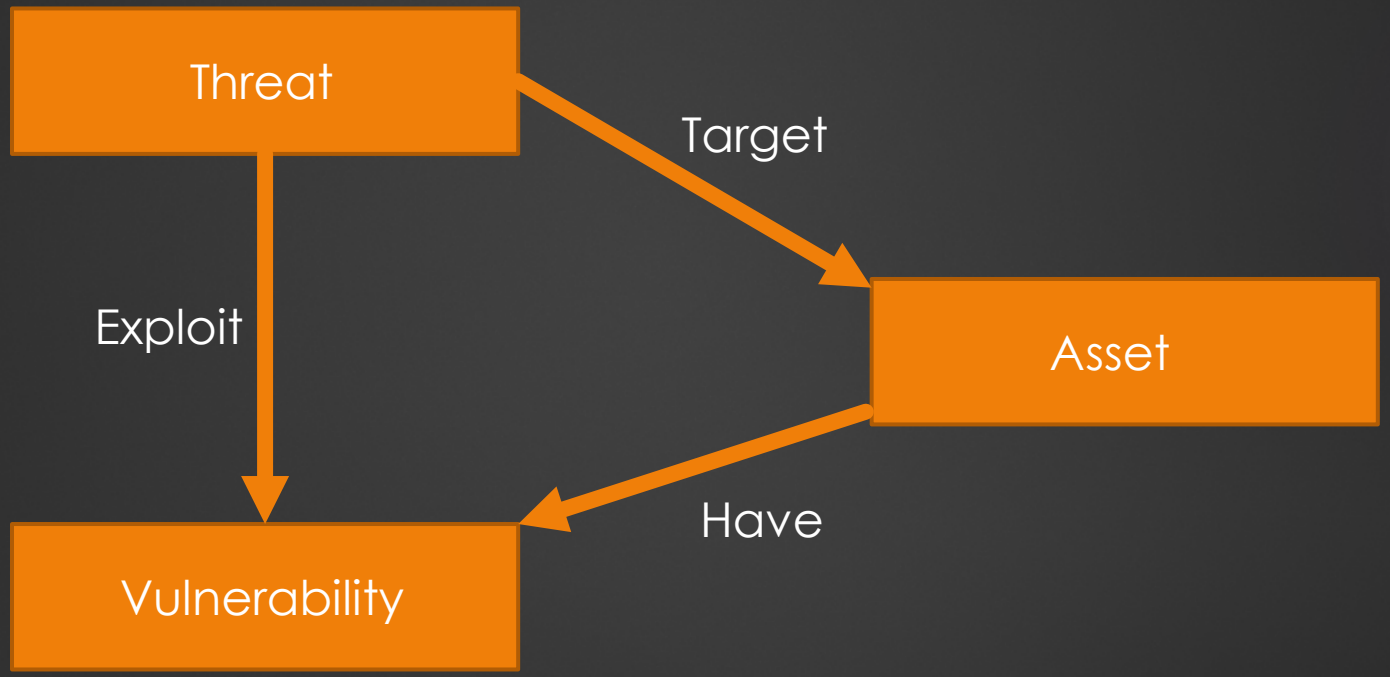
- **White Hats** is a good guys also called ethical hackers.
- **Black Hats** is a bad guys, malicious hackers.
- **Gray Hats** is a good and bad guys depends on the situation.

- **Hacktivist** is a guy who defend a political opinion.
- **Script Kiddies** is an unskilled hacker who compromises a system by running scripts, tools, or other developed by real hackers.
- **Cyber Terrorists** are guys motivated by religious or political.
- **State-sponsored Hackers** are guys employed by the government to hack another government.

Hacking vocabulary (1/2)

- **Threat** that could lead to a potential breach of security.
- **Exploit** takes advantage of a bug or vulnerability, leading to unauthorized access, privilege escalation, or Denial Of Service.
- **Vulnerability** is a software flaw or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system.
- **Risk analysis** aim to identify, assess and prioritize the risks associated with the activities of an organization.
- **Payload** is a component of an attack. It could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- **Zero-day attack** is an attack that occurs before a vendor knows or is able to patch a flaw.
- **Pivoting** involves gaining access to a network and / or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.
- **Doxing** is the act of publicly providing PII (Personally Identifiable Information) about an individual or organization, usually via the Internet and without their consent.
- **Defense in depth** also known as layering when you put more than one layer for a protection.

Hacking vocabulary (2/2)



Vulnerabilities vocabulary

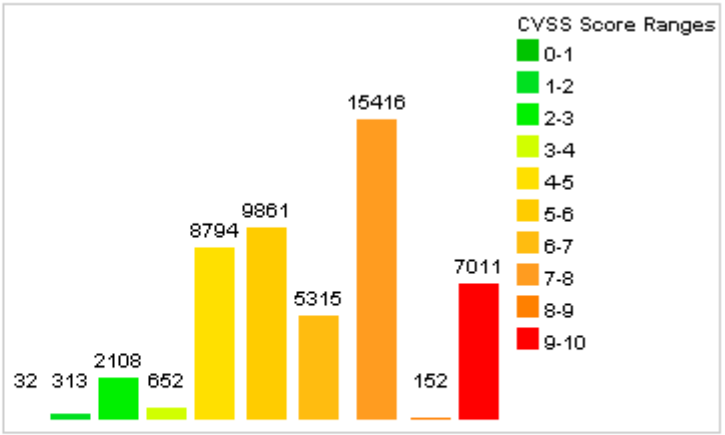
- **CVE** (Common Vulnerabilities and Exposures) is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.
- **MITRE** is an American not-for-profit organization created to improve IT security.
- **CVSS** (Common Vulnerability Scoring System) places numerical score based on severity :

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	32	0.10
1-2	313	0.60
2-3	2108	4.20
3-4	652	1.30
4-5	8794	17.70
5-6	9861	19.90
6-7	5315	10.70
7-8	15416	31.00
8-9	152	0.30
9-10	7011	14.10
Total	49654	

Weighted Average CVSS Score: **6.9**

Vulnerability Distribution By CVSS Scores

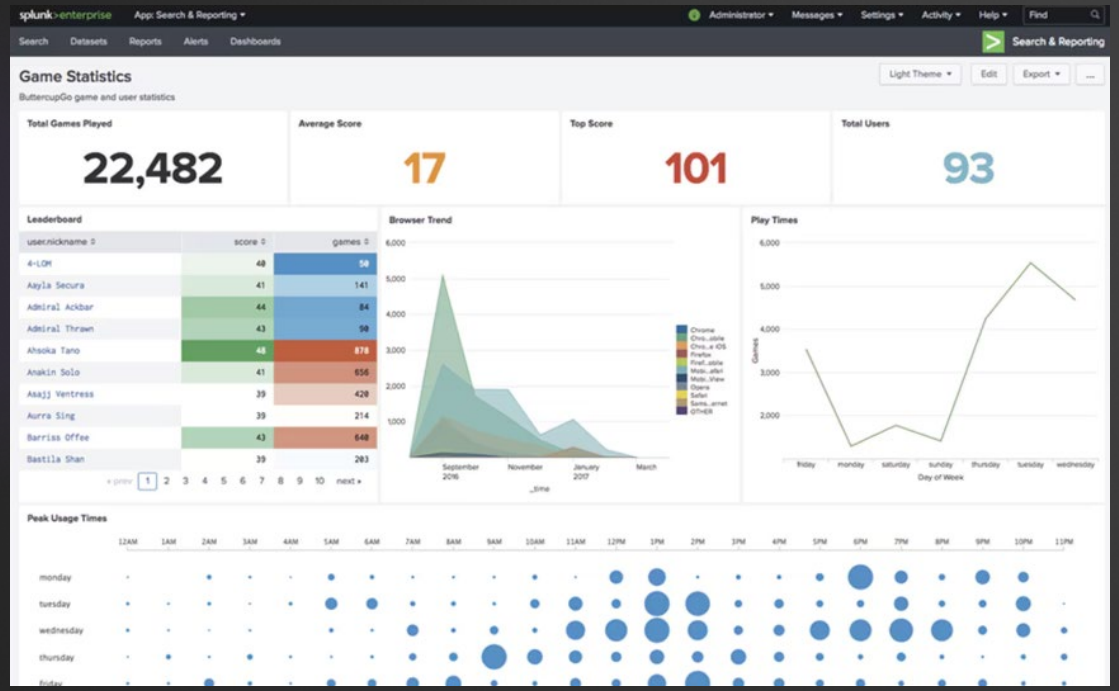


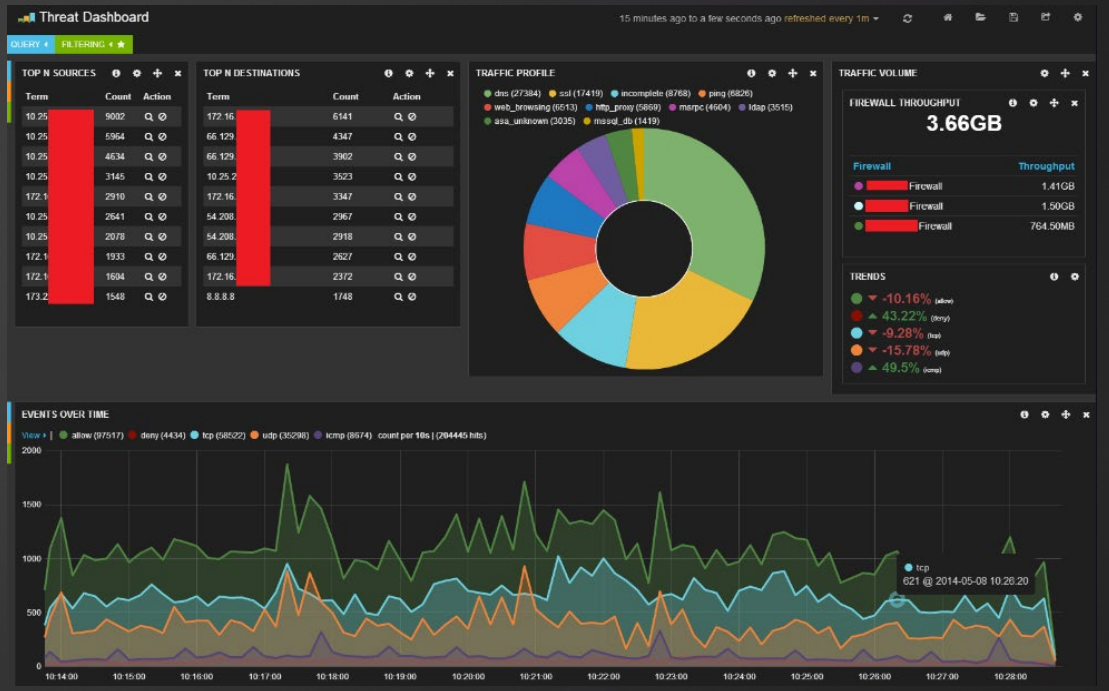
Managing the Risk

- **Risk Management** is the identification, evaluation, and prioritization of risks.
  - **Risk Identification :** Identifies the sources, causes, consequences of the internal and external risks.
  - **Risk Assessment :** Assesses the organization risk and provides an estimate on the likelihood and impact of the risk.
  - **Risk Treatment :** Selects and implements appropriate controls on the identified risks.
  - **Risk Tracking :** Ensures appropriate control are implemented.
  - **Risk Review :** Evaluates the performance of the implemented risk management strategies.

SIEM (Security Information and Event Management)

- A **SIEM** is a tool that collects, correlate, and alert (depending on the use cases created).





Indicators Of Compromise (IOCs)

- Indicators of Compromise (IOC) are the clues and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.
- Security professionals need to perform continuous monitoring of IOC to detect and respond to evolving cyber threats.

IAM (Identity and Access Management)

- IAM is a **comprehensive discipline** that covers how **identities and access rights** are managed across an organization.
- It includes **the full identity lifecycle** from account creation to deprovisioning as well as **roles, policies, governance**, and **auditing**.
- **Goal:** Ensure the *right person* has the *right access* to the *right resources* at the *right time*, for the *right reason*.
- **Key components:**
  - Identity lifecycle management
  - Authentication (proving identity)
  - Authorization (granting permissions)
  - Access governance and reviews
  - Privileged Access Management (PAM)
  - Federation / SSO / MFA / Directory Services (AD, LDAP, etc.)
  - Audit and compliance reporting

DLP (Data Lost Prevention)

- A DLP is a a practice of **detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.** Organizations use DLP to protect and secure their data and comply with regulations.
- The DLP term refers to defending organizations against both **data loss and data leakage prevention**.
- Organizations typically use DLP to:
  - Protect Personally Identifiable Information (PII) and comply with relevant regulations;
  - Protect Intellectual Property critical for the organization;
  - Achieve data visibility in large organizations;
  - Secure data on remote cloud systems and on mobile equipments.

Testing types in pentest

- **Black box:** testing involves performing a security evaluation and testing with no prior knowledge of the infrastructure.
- **White box** testing involves performing a security evaluation and testing with complete knowledge of the infrastructure.
- **Gray box** testing involves a combination of white-box testing and black-box testing. The aim of this testing is to search for the defects if any due to improper structure or improper usage of applications.

All steps to execute a pentest

1. Talk to the client about the perimeter (IP, domain, etc.) and types of attacks that may create a risk for the customer (brute force, DoS, etc.).
2. Prepare and sign with the client the NDA (non-disclosure agreement)
3. Conduct the pentest and collect information in order to provide a report.
4. Write the report and have it proofread by a colleague.
5. Present the report findings to the client (report, documentation, etc.).

Warning : It is legally forbidden to scan / pentest / etc. if you haven't been commissioned for it or that the solution is not yours.

Hacking phase

- In general there are five phases of hacking :
  - **Reconnaissance**
  - **Scanning**
  - **Gaining Access**
  - **Maintaining Access**
  - **Clearing Tracks**

Hacking phase : Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- The reconnaissance target range may include the target organization's clients, employees, operations, network and systems.
  - **Passive reconnaissance** there will be no traffic generated on the target's infrastructure, it is a matter of finding public data by conventional or specialized search engines (wireshark, shodan, etc.).
  - **Active reconnaissance** it is a question of going directly to question the "target". For example, a server's ports can be scanned to see which services they are responding to.

Hacking phase : Scanning

- **Pre-attack** : Scanning refers to the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance.
- **Port scanner** : Scanning can include many tools like port scanners, network mappers, ping tools, vulnerability scanners, etc.
- **Extract information** : Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch attack.

Hacking phase : Gaining Access

- Gaining access refers to the point where the attacker obtains access to the operating system or applications on the target computer or network.
- The attacker can gain access at the operating system, application or network levels.
- The attacker can escalate privileges to obtain complete control of the system.
- Type of gaining access:
  - password cracking,
  - buffer overflows,
  - session hijacking,
  - Etc.

Hacking phase : Maintaining Access

- Maintaining access refers to the phase when the attacker tries to retain their ownership of the system.
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with backdoors by example.
- Attackers can upload, download or manipulate data, applications and configurations on the owned system.
- Attackers use the compromised system to launch further attacks (example with pivoting).

Hacking phase : Clearing Tracks

- Clearing tracks refers to the activities carried out by an attacker to hide malicious acts.
- The attacker's intentions is to remain unnoticed by deleting evidence that might lead to their prosecution.

MITRE ATT&CK® Frameworks

- MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
- With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world by bringing communities together to develop more effective cybersecurity.
- ATT&CK is open and available to any person or organization for use at no charge.
- MITRE ATT&CK® : https://attack.mitre.org/

ATT&CK Tactics, Techniques and Procedures

- **Tactics** are the guidelines that describe the way of an attacker performs the attack from beginning to the end : https://attack.mitre.org/tactics/enterprise/

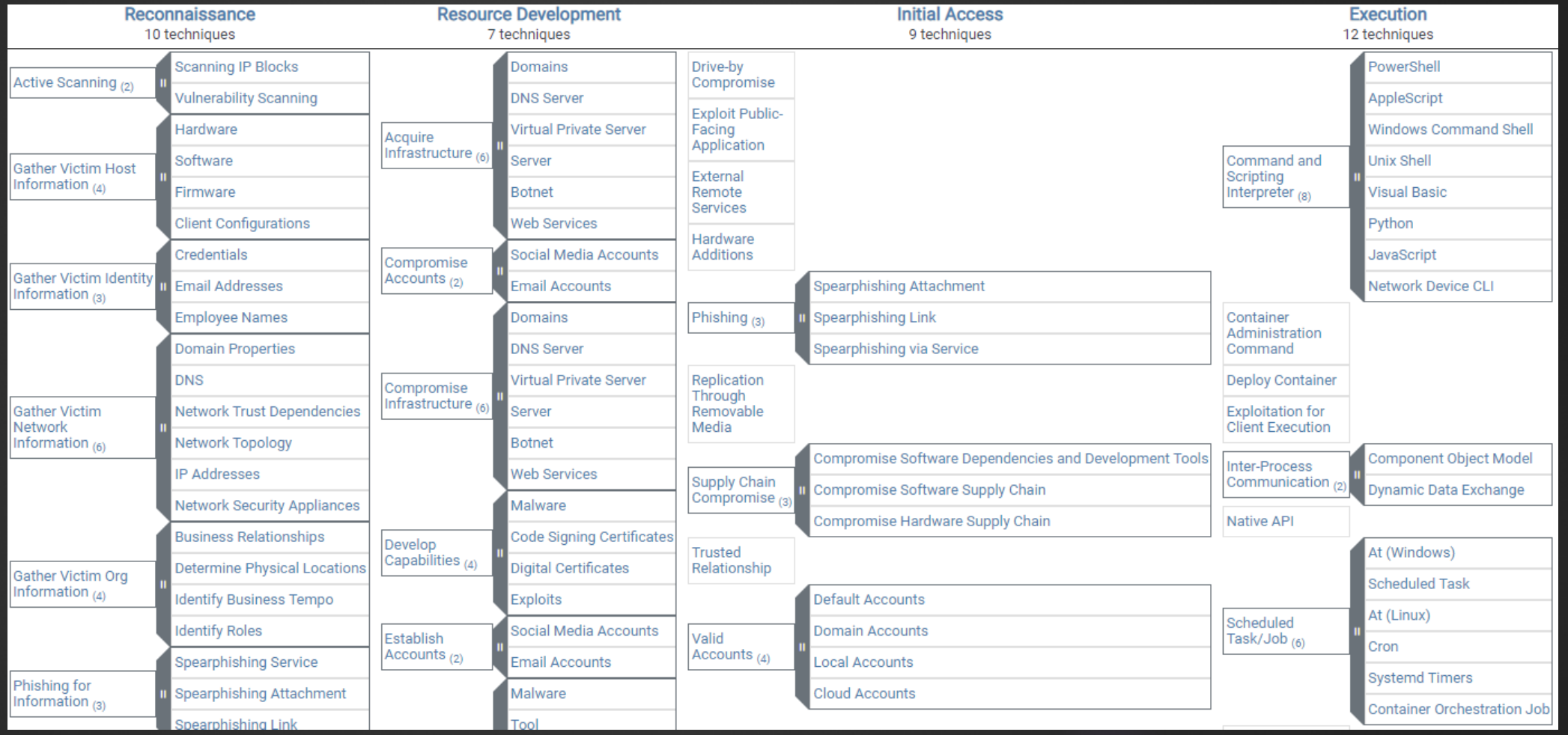
- **Techniques** are the technical methods used by an attacker to achieves his wish (exploitation , command and control, covering the tracks, etc.). https://attack.mitre.org/techniques/enterprise/

- **Procedures** are organizational approaches that threat actors follow to launch an attack.
  Example how hacker can gather informations ?

Tactics, Techniques and Procedures

Tactics

Techniques



Tactics, Techniques and Procedures

Active Scanning: Vulnerability Scanning

Other sub-techniques of Active Scanning (2)

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to Gather Victim Host Information that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.[1] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: Exploit Public-Facing Application).

ID: T1595.002
Sub-technique of: T1595
Tactic: Reconnaissance
Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 15 April 2021

Version Permalink

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[2]
G0016	APT29	APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.[3]
G0034	Sandworm Team	Sandworm Team has scanned network infrastructure for vulnerabilities as part of its operational planning.[4]
G0139	TeamTNT	TeamTNT has scanned for vulnerabilities in IoT devices and other related resources such as the Docker API.[5]
G0123	Volatile Cedar	Volatile Cedar has performed vulnerability scans of the target server.[6][7]

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

Improve your skills

Plateform	Description	URL	Skills to begin
DVWA	Damn Vulnerable Web App is a web vulnerable application	https://dvwa.co.uk	☆☆☆
TryHackMe	Platform with interactive lessons.	https://tryhackme.com	☆☆☆
HackTheBox	Platform to test your skills in penetration testing.	https://www.hackthebox.com	★☆☆
RootMe	Plateform with many little games and CTF	https://www.root-me.org	★☆☆
VulnHub	Plateform to share vulnerable VM.	https://www.vulnhub.com	★★☆

Improve your skills ++

- A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

- Bug bounty plateform:
  - https://www.hackerone.com/
  - https://www.bugcrowd.com/
  - https://www.yeswehack.com/
  - https://www.openbugbounty.org/