Threat

A threat is any form of potential danger or action that can exploit a vulnerability to cause a damage to the system or network. It doesn't mean damage is happening instead it means that there is a possibility for a damage to occur on the system. It can come from external sources (hackers, malware) or internal sources (disgruntled employees, accidental mistakes).

Threat Hunting

It is the practice of proactively searching for cyber threats that are lurking undetected in a network. Unlike reactive methods (like responding to alerts from firewalls or antivirus software), threat hunting involves actively searching through networks, endpoints, and datasets to identify signs of malicious activity that may not have triggered any alerts.

Threat Hunting Steps:

Here are the key events or steps in a typical threat hunting process:

1. Hypothesis Creation
Forming a question or assumption based on threat intelligence, behavior anomalies, or system baselines.

Example: "What if a threat actor is using remote desktop protocol (RDP) to move laterally across the network?"

2. Data Collection
Collect logs and telemetry from endpoints, networks, servers, and security tools like SIEMs.

Sources: Firewall logs, EDR logs, DNS logs, user authentication logs, etc.

3. Data Analysis
Manually or automatically analyzing the collected data to find unusual patterns or suspicious behavior.

Techniques: Statistical anomaly detection, behavioral analysis, signature-based detection.

4. Threat Detection
Identifying Indicators of Compromise (IOCs) or Indicators of Attack (IOAs).

Example IOCs: Unusual command-line activity, connections to known malicious IPs, privilege escalation attempts.

5. Investigation
Digging deeper into discovered anomalies to confirm whether it is a real threat or a false positive.

Includes correlating events across time and systems.

6. Response & Remediation
If a threat is confirmed, take corrective actions: isolate systems, block IPs, disable user accounts, etc.

7. Documentation & Feedback
Document the hunt process and findings to improve future detection rules and refine hypotheses.

Update SIEM rules, IDS signatures, and awareness training.

Threat vs Normal Security

1. Threat Hunting gives you the ability to uncover stealthy and advanced threats by actively probing systems and logs before damage is done.

2. Normal security is necessary for automated, known threat protection, but it misses the unknowns.

The two work best together: automated tools catch the known stuff, while threat hunting finds what slips through.

There are two types of Threat Hunting:

1. Structured Threat Hunting:

Structured hunting follows a predefined methodology or hypothesis, often based on threat intelligence, known attack tactics (like those from MITRE ATT&CK), or indicators of compromise (IOCs).

Driven by:

Known threats or patterns

Security frameworks

Previous incidents

Threat intelligence feeds

2. Unstructured Threat Hunting:

Unstructured hunting is exploratory and hypothesis-free, often used when something feels "off," or as a routine check for anomalies without specific triggers.

Driven by:
Human intuition and experience

Anomalies spotted in dashboards

Behavioral deviations

Curiosity

Types of Cybersecurity Threats:

Some of the major threats are:

1. Malware (Malicious Software)

Malicious programs that damage systems, steal data, or disrupt operations.
Types:

Virus, Worms: Spread and infect systems

Trojans: Disguised as safe software

Ransomware: Locks files for ransom

Spyware, Adware: Steal info or push ads

Rootkits: Hide other malware

2. Phishing & Social Engineering

Tricking people into giving up sensitive info.
Forms:

Phishing, Spear Phishing: Fake emails/websites

Vishing, Smishing: Scam calls/texts

Pretexting, Baiting: Impersonation or traps

3. Insider Threats

Threats from people inside the organization.

Malicious: Intentional harm

Negligent: Accidental mistakes

Compromised: Hacked accounts

4. Network Threats

Attacks on network communication.

Examples:

Man-in-the-Middle (MitM), DNS Spoofing

Packet Sniffing, Session Hijacking

5. DoS / DDoS Attacks

Overloading systems with traffic to crash them.
Example: A botnet floods a website until it goes offline.

6. Advanced Persistent Threats (APTs)

Stealthy, long-term attacks often by nation-states.
Focus: espionage, sabotage, or data theft.

7. Zero-Day Exploits

Attacks on unknown software flaws before a fix exists.
Hard to detect, very dangerous.

8. Credential Threats

Targeting usernames and passwords.
Tactics:

Brute Force, Credential Stuffing

Keyloggers

9. Physical Threats

Physical access or damage to systems.
Examples: Device theft, sabotage, natural disasters.

10. Supply Chain Attacks

Targeting vendors or third parties to reach the main victim.
Example: SolarWinds breach via infected software updates.