Security threats are often classified by their **origin** (who is attacking) and their **method** (how organized the attack is). Understanding these classifications helps organizations determine the necessary defence strategies.

---

a. External Threats

These threats originate outside the organization's network and are typically launched by individuals or groups without authorized access to internal systems.

- **Origin:** Hackers, organized crime syndicates, rival companies, nation-states, or even natural disasters (though the term usually focuses on human adversaries).
- **Access:** They must exploit vulnerabilities (weak points) to penetrate the network perimeter (e.g., firewall, exposed servers, public-facing applications).
- **Motivation:** Financial gain, espionage, political activism (hacktivism), or military intelligence.
- **Examples:** Phishing attacks targeting employees, Distributed Denial of Service (DDoS) attacks against a public website, and external zero-day exploits.

b. Internal Threats

These threats originate from **within** the organization's network and are carried out by individuals who already have **authorized access** to systems and data.

- **Origin:** Current or former employees, contractors, partners, or vendors who have/had legitimate login credentials and physical access.
- **Motivation:** Can be intentional (e.g., disgruntled employee seeking revenge, espionage for financial gain) or unintentional (e.g., employee negligence, error, or poor security awareness).
- **Danger:** Often considered more dangerous than external threats because the perpetrator **bypasses perimeter defenses** and is already familiar with the network architecture and location of critical data.
- **Examples:** A system administrator abusing their privilege to steal customer data, an employee accidentally emailing sensitive files to a personal account, or a contractor installing unapproved software.

c. Unstructured Threats

This classification relates to the **skill level and planning** of the adversary. Unstructured threats are characterized by a lack of sophistication.

- **Attacker Profile:** Typically **amateurs, novices, or "script kiddies."** They have limited technical knowledge.
- **Methodology:** They rely on **easily available, automated tools** (like shell scripts, public exploits, or password crackers) that require little modification.

- **Targeting:** Attacks are usually **unfocused, random, or opportunistic**. They often don't target a specific organization but rather sweep large ranges of IP addresses looking for simple, well-known vulnerabilities.
- **Motivation:** Often driven by curiosity, notoriety, or minor vandalism rather than high-value financial gain.
- **Prevention Focus:** Can often be prevented by simply keeping software **patched and up-to-date**, and applying basic security configurations.

d. Structured Threats

This classification represents the **most dangerous** and sophisticated type of threat, involving high levels of planning and technical expertise.

- **Attacker Profile:** Highly **skilled, organized, and well-resourced** groups, such as state-sponsored actors, organized crime, or Advanced Persistent Threat (APT) groups.
- **Methodology:** Involves extensive **reconnaissance**, developing **customized exploits**, and using complex tactics, techniques, and procedures (TTPs) over a long period.
- **Targeting:** Attacks are **highly focused** on a specific target (a bank, a government agency, a competitor) to achieve a clear, high-value objective.
- **Motivation:** Corporate espionage, large-scale financial theft, intellectual property theft, or disruption of critical infrastructure.
- **Prevention Focus:** Requires advanced defenses like **Threat Hunting**, **Security Information and Event Management (SIEM)**, and continuous monitoring to detect subtle anomalies.