For law firms, the goal is the privacy of the legal documents. For factories, the availability of production lines. For hospitals, patient safety. That's why every company has a unique security approach and security team structure.

# Meet the Blue Team:

Managed Security Services Provider (MSSP)

## Humans as Attack Vectors

**The Human Element**

Attackers often find it easier to exploit people than to break through strong technical defenses. Instead of spending days bypassing firewalls or vulnerabilities

An attacker can simply trick an IT administrator with a phishing email. Humans are targeted because they can provide access to websites, mailboxes, databases, and internal systems.

This tactic is known as social engineering, which relies on manipulating human psychology rather than exploiting technical flaws.

For a social-engineering attack to succeed, it must be:
• **Trustworthy:** The attacker must appear legitimate so the victim believes them.
• **Emotional:** The attack must trigger urgency, fear, curiosity, or similar reactions.

**Common Social-Engineering Techniques**

• **Email phishing:** The most widespread method, with an estimated 3.4 billion malicious emails sent daily.

• **Malicious downloads:** Searching for and installing software from untrusted sources may result in installing malware.
• Fake CAPTCHAs, malicious QR codes, and SEO poisoning: Techniques designed to mislead users into interacting with malicious content.

• **Deepfakes**: AI-generated audio or video used to impersonate trusted individuals. Example: A finance worker was tricked into wiring $25 million after receiving a deepfake video call from someone appearing to be their boss.

• USB drop campaigns, physical attacks, insider threats, and fake job offers: Additional avenues through which employees may be targeted.

**Defending Humans**

Mitigation focuses on **preventing or reducing the chance and impact of attacks.** Even with strong defenses, attackers may eventually bypass protections, making SOC detection and investigation skills essential. Understanding mitigation measures helps automate prevention of common threats and reduces the SOC workload while improving organizational security.

Key Mitigation Measures
• Enforce multi-factor authentication for all accounts.
• Apply regular OS and application patching.
• Use email filtering to block phishing and malicious attachments.
• Provide short, recurring security-awareness training for employees.
• Deploy endpoint protection (EDR/antivirus) on all devices.
• Limit user privileges to only what is required.
• Enable automatic backups and regularly test restoration.
• Monitor network activity for unusual or suspicious behavior.

## Systems as Attack Vectors

Imagine a castle again,However, if the **lock on the main gate is fragile** and cheap, **guardian skills do not matter**, as the enemy can just sneak into the castle while no one is watching

Where do the banks store your cards, or where are your emails stored? **The answer - on a system: a physical server,**

such systems is crucial: if the attackers breach one user's mailbox via phishing, they compromise a single mailbox, but if they breach a **mail server**, they now control all **thousands of mailboxes**.**Each system type can have a different value for threat actors,** for example:

| Breached System | Attack Value |
| --- | --- |
| A personal laptop of a school student | Steal Steam profile and add the PC to a botnet |
| A laptop of the bank's senior IT administrator | Get access to the internal banking systems |

In most serious attacks, the first goal is to gain **access to the target system.** What happens next depends on the **attacker's motivation:** stealing data, deploying ransomware, or even destroying information without a way to recover.

## supply chain attack

A supply chain attack happens when hackers break into a **software provider,** not the user. They insert malicious code into an **app or library** before it is distributed. When the provider **releases an update, all users who install it become infected automatically**. One compromise at the source spreads to everyone downstream.

. For example, Shellshock, a major Linux vulnerability, existed since **1992 but wasn't found until 2014.** In the worst-case scenario, attackers discover the vulnerability before anyone else.

Common Vulnerabilities and Exposures (CVE) number

An answer to a CVE is always **a patch** - an update supplied by the software vendor. Even for zero-days, you'll have to wait for a patch,

try to survive the stressful period before the patch is released. For example, by:

- Restricting access to the system to only trusted IPs
- Applying temporary measures provided by the vendor
- Blocking known attack patterns on IPS or WAF

## Misconfigurations

a misconfiguration **isn't a bug in the software** but a mistake in how the system was **set up, often by the IT team**. These errors happen frequently, **usually to make things simpler,** like using "1111" instead of typing a long password every timeMisconfigurations do not require a software update - just a better setup.

Can a system patch or software update fix the misconfigurations : **NO**