[Cyber Security Overall + Prep](https://youtube.com/playlist?list=PL0hT6hgexlYwdYBW6yqUQMuRqvABiQPXk&si=0keHv_T5CuTYlcAJ)

[Cyber Security Network questions](https://www.youtube.com/watch?v=Y3ozkAFuiHc&list=PL0hT6hgexlYzX6AWwcyDbAZQUKYJL2Mdt&ab_channel=PrabhNair)

[What is SIEM ?](https://www.youtube.com/watch?v=kllStyjewkw&ab_channel=PrabhNair)

[Full SOC prep playlist](https://youtube.com/playlist?list=PL0hT6hgexlYxd24Jb8OE7vZoas-iTcHAc&si=eGO3O-LM71WhPYnL)

[SPLUNK prep](https://youtube.com/playlist?list=PL0hT6hgexlYz7fOk6XsOFouFHTsbvfaYq&si=86samu_dtoVouR_0)

[Comptia+ Security prep](https://www.youtube.com/playlist?list=PL0hT6hgexlYwNK8DvXvUlDb63xB0zfFeN)

[Internal Audit](https://www.youtube.com/playlist?list=PL0hT6hgexlYyNWBcGYfabwumCr0GKmLWv)

[Threat Intelligence](https://www.youtube.com/playlist?list=PL0hT6hgexlYxb9mXpcgmEU-_AOmQdrZYO)

[Cloud Security prep](https://www.youtube.com/playlist?list=PL0hT6hgexlYwEOk4HtUck4ydj24akizba)

Defense

[Wireshark playlist](https://www.youtube.com/playlist?list=PLhfrWIlLOoKMO9-7NxYN3TxCdcDecwOtj)

[Malware analysis](https://www.youtube.com/watch?v=KNe4hTVhpPQ&ab_channel=LetsDefend)

Practical

[Attack and Defend and Firewall](https://www.youtube.com/watch?v=N0dEC1nuWCQ&ab_channel=TheSocialDork) (WEB APP )

Virtual Machine And Hyper Visiors:

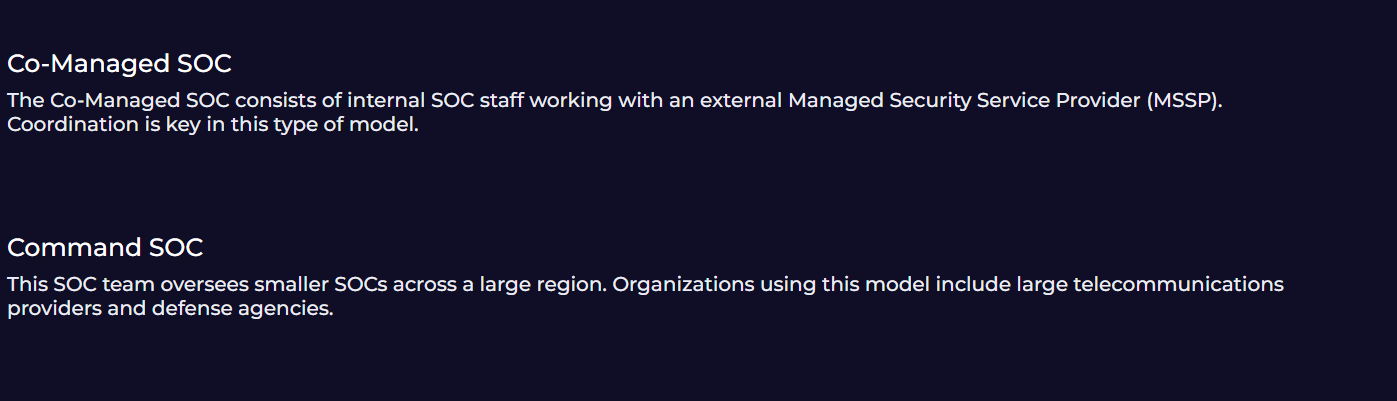
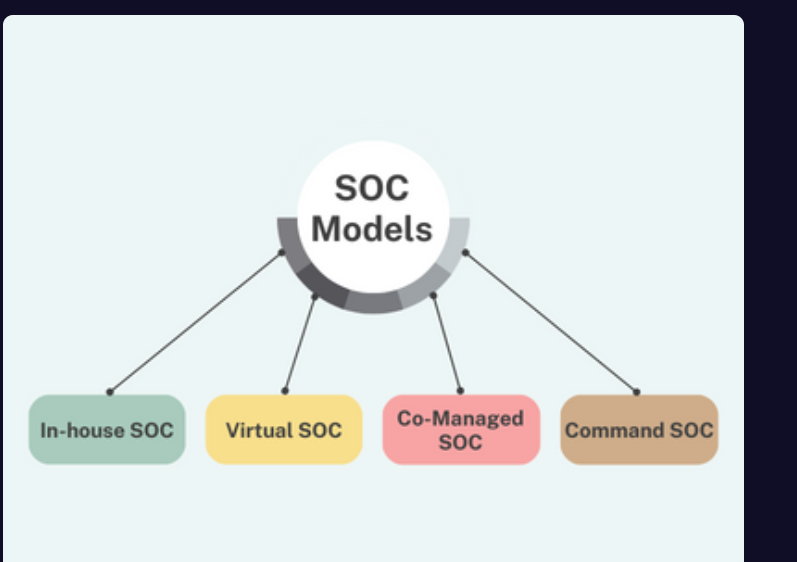
[What is Hypervisior?](https://www.youtube.com/watch?v=73XTW67TOZ0&ab_channel=GateSmashers)

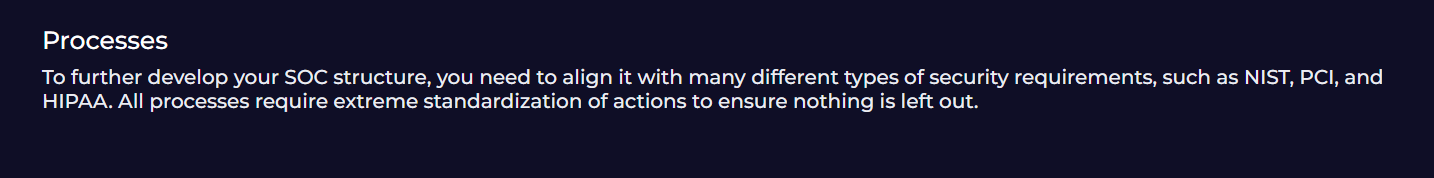
Attack Tools

[Metasploit tutorial](https://www.youtube.com/watch?v=xuYZNJCvHgQ&ab_channel=HackerJoe) (basic intro and basic use )

[Complete Playlist to advance metasploit](https://youtube.com/playlist?list=PLa2xctTiNSCgtlM7S6FkNC2396_xNwtm8&si=hNNeaueP9h8kS7zA)

Soc notes





**SOC Roles**

SOC Analyst

This role can be categorized as Level 1, 2, and 3 according to the SOC structure. A security analyst classifies the alert, looks for the cause, and advises on remediation.

Incident Responder

An Incident Response Officer is an individual responsible for threat detection. This role performs the initial assessment of security breaches.

Threat Hunter

A Threat Hunter is a cybersecurity professional who proactively seeks out and investigates potential threats and vulnerabilities within an organization's network or system. They use a combination of manual and automated techniques to detect, isolate, and mitigate advanced persistent threats (APTs) and other sophisticated attacks that may evade traditional security measures. Threat hunters typically have a deep understanding of the organization's IT infrastructure and security posture, as well as knowledge of emerging threats and attack tactics. They aim to find and eliminate threats before they can damage or disrupt the business.

Security Engineer

Security engineers are responsible for maintaining the security infrastructure of Security Information and Event Management (SIEM) solutions and security operations center (SOC) products. For example, a security engineer builds the connection between SIEM and Security Orchestration, Automation, and Response (SOAR) products.

SOC Manager

A SOC manager takes on management responsibilities such as budgeting, strategizing, managing staff, and coordinating operations. They deal with operational rather than technical issues.

**What is SIEM?**

SIEM is a security solution that combines security information and event management, which involves real-time logging of events in an environment. The ultimate purpose of event logging is to detect security threats.

Overall, SIEM products have a lot of features. The ones that interest us most as SOC analysts are those that collect and filter data and provide alerts for suspicious events.

Example alert: If someone on a Windows operating system tries to enter 20 incorrect passwords in 10 seconds, this is suspicious activity. It is unlikely that someone who has forgotten their password would try to re-enter it that many times in such a short period of time. So we create a SIEM rule/filter to detect such activity that exceeds the threshold. Based on this SIEM rule, an alert will be generated when such a situation occurs.

**What is CVE?**

CVE is a publicly available system that identifies and catalogs known **cybersecurity vulnerabilities** in software and hardware. Each CVE has a unique ID that allows people to share information across different tools and platforms consistently.

**Example:**

CVE-2024-12345

In CVE-2024-12345 , 2024 is the year this malware was registered , and 12345 is malware’s ID number

This might refer to a specific vulnerability in a software product, like a buffer overflow in a certain version of Apache.

**Key Points:**

* **Maintained by:** MITRE Corporation, with support from the U.S. Department of Homeland Security (DHS).
* **Purpose:** Standardize the identification of vulnerabilities so organizations can talk about the same issue using the same ID.
* **Content:** Includes a brief description and references (like vendor advisories), but not exploit code or detailed technical analysis.

**Why CVE Matters:**

* Helps organizations prioritize patching and defense.
* Used by security tools (like scanners and SIEMs) for identifying known vulnerabilities.
* Forms the foundation for vulnerability databases like **NVD (National Vulnerability Database)**.

**Where are CVEs registered?**

CVE identifiers are managed by the [**CVE Program**](https://cve.org/), which is sponsored by the **Cybersecurity and Infrastructure Security Agency (CISA)** and overseen by **MITRE Corporation**.

* **MITRE** manages the CVE list as part of its public-interest work.
* **CNAs (CVE Numbering Authorities)** such as software vendors (e.g., Microsoft, Google), security research organizations, or other bodies are authorized to assign CVE IDs.
* Once a CVE is assigned and made public, it is added to the official [**CVE list**](https://cve.org) and often also appears in databases like:
  + [NVD (National Vulnerability Database)](https://nvd.nist.gov/)
  + [Security advisories from vendors](https://msrc.microsoft.com/), etc.

**How CVEs relate to Metasploit and Malware**

**🔐 1. CVE (Common Vulnerabilities and Exposures)**

* A **CVE** describes a **vulnerability** — a weakness in software or hardware.
* Example: CVE-2024-12345 might describe a buffer overflow in a web server.

**💣 2. Metasploit Framework**

* **Metasploit** is a **penetration testing tool** developed by **Rapid7**.
* It contains **exploits** — scripts or code that take advantage of **known CVEs**.
* When a CVE becomes public, Metasploit often adds a **module** that demonstrates or automates exploitation of it.
* So, for example:
  + **CVE-2024-12345** could have an associated **Metasploit module** that lets you exploit it in a test environment.

👉 Think of it this way:

CVE = weakness  
Metasploit = tool that attacks the weakness (using a matching exploit module)

**🦠 3. Malware**

* Malware (malicious software) is **often built using exploits** for known CVEs.
* Attackers may copy or modify **Metasploit code** to build real malware payloads.
* But Metasploit itself is **not malware** — it's a security tool, used ethically for **penetration testing** or **research** (with permission).

**🧩 Example in Practice**

Let’s say:

1. A vulnerability is found in a web server.
   * It’s assigned **CVE-2024-12345**.
2. A Metasploit module is released that exploits CVE-2024-12345.
3. A hacker uses that module (or copies the exploit code) to build malware that attacks thousands of vulnerable servers.

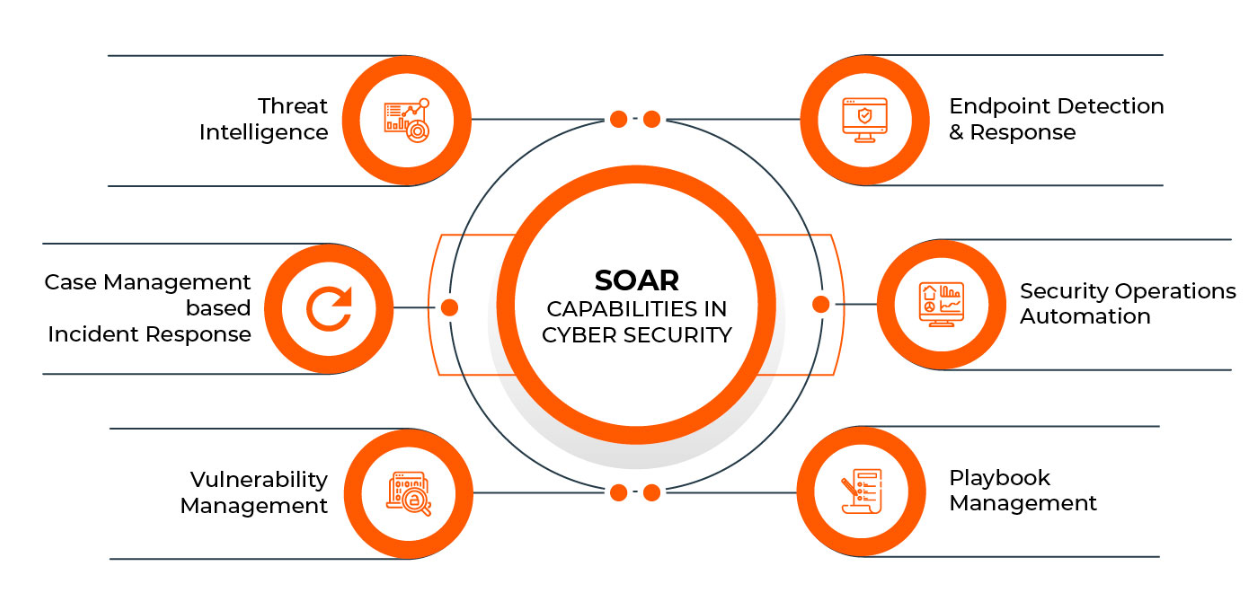
**SOAR (Security Orchestration Automation and Response)**

SOAR stands for Security Orchestration Automation and Response. It enables security products and tools in an environment to work together, streamlining the tasks of SOC team members. For example, it will automatically search VirusTotal for the source IP of a SIEM alert, reducing the workload of the SOC analyst.

Some SOAR products commonly used in the industry:

* Splunk Phantom
* IBM Resilient
* Logsign
* Demisto

The image below shows what can be achieved with a SOAR solution.



**Centralization (A single platform for everything you need)**

It allows you to use different security tools in your environment (sandbox, log management, 3rd party tools, etc.) by providing an all-in-one software. These tools are integrated into the SOAR solution and can be used on the same platform.

**Common Mistakes made by SOC Analysts**

Like everyone else, SOC analysts can make mistakes. In this section, we will discuss common mistakes made by SOC analysts and how to avoid making them yourself.

* Over-reliance on VirusTotal Results
* Hasty Analysis of Malware in a Sandbox
* Inadequate Log Analysis
* Overlooking VirusTotal Dates
* **Inadequate Log Analysis**
* Occasionally we see that some log analysis is not performed properly. For example, let's say that a piece of malware has been detected on a machine with the hostname "LetsDefend", and that malware is secretly sending data to the address "letsdefend.io". As a SOC analyst, you should use Log Management solutions to determine if any other device is also attempting to connect to this address.
* **Overlooking VirusTotal Dates**
* If the search you performed in VirusTotal has already been queried, a result from the cache will be displayed. For example: We searched the address "letsdefend.io" in VirusTotal and the result is shown below.