Security Operations Center (SOC)

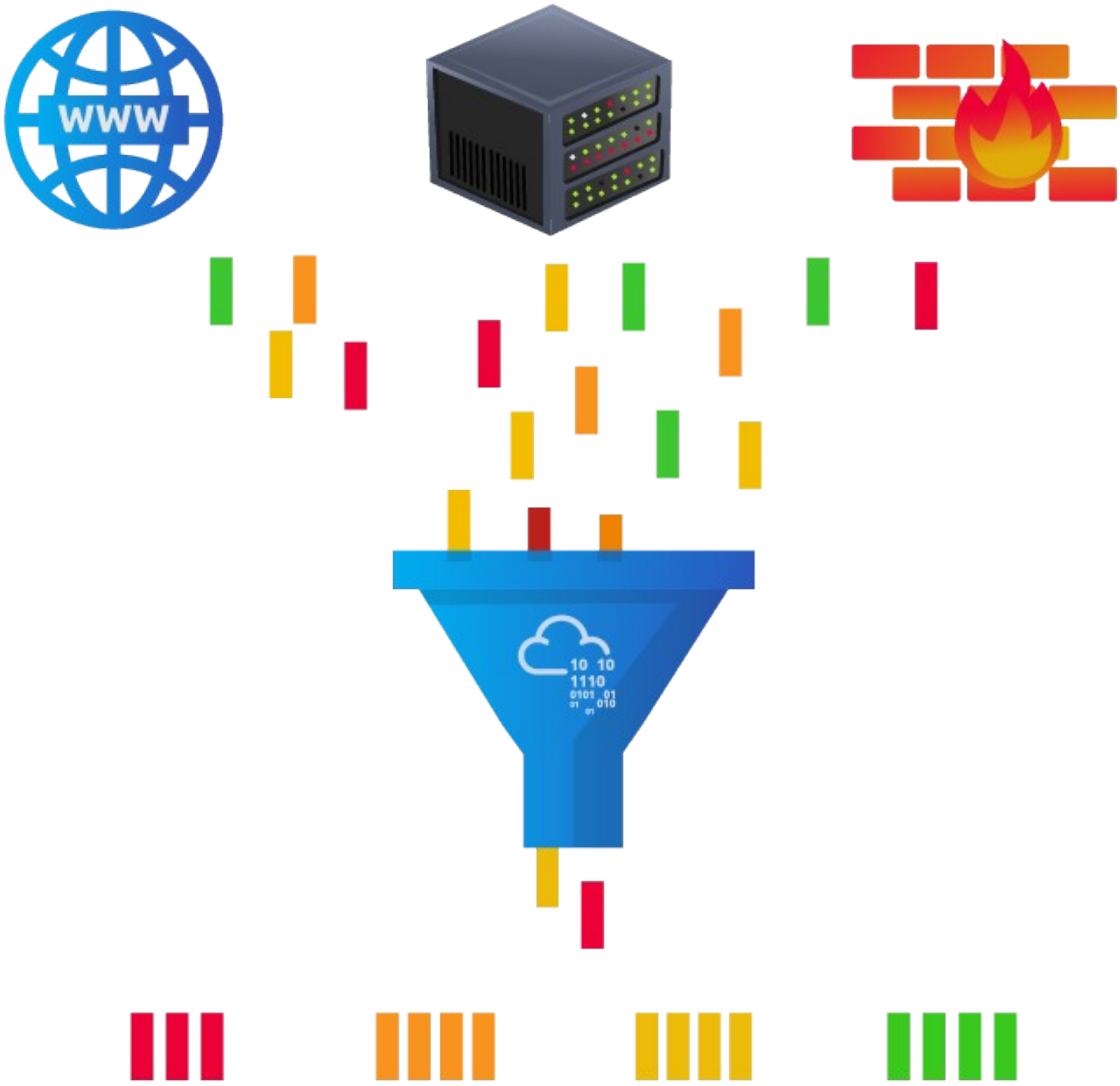
A *Security Operations Center* (SOC) is a team of cyber security professionals that monitors the network and its systems to detect malicious cyber security events. Some of the main areas of :interest for a SOC are

- **Vulnerabilities: Whenever a system vulnerability (weakness) is discovered, it is essential to fix it by installing a proper update or patch. When a fix is not available, the necessary measures should be taken to prevent an attacker from exploiting it. Although remediating vulnerabilities is of vital .interest to a SOC, it is not necessarily assigned to them**
- **Policy violations: We can think of a security policy as a set of rules required for the protection of the network and systems. For example, it might be a policy violation if users start uploading confidential company data to an online .storage service**
- **Unauthorized activity: Consider the case where a user's login name and password are stolen, and the attacker uses them to log into the network. A SOC needs to detect such an event and block it as soon as possible before further .damage is done**
- **Network intrusions: No matter how good your security is, there is always a chance for an intrusion. An intrusion can occur when a user clicks on a malicious link or when an attacker exploits a public server. Either way, when an intrusion occurs, we must detect it as soon as possible to .prevent further damage**

Security operations cover various tasks to ensure protection; one .such task is threat intelligence

Threat Intelligence

In this context, *intelligence* refers to information you gather about actual and potential enemies. A *threat* is any action that can disrupt or adversely affect a system. Threat intelligence aims to gather information to help the company better prepare against potential adversaries. The purpose would be to achieve a *threat-informed defense*. Different companies have different adversaries. Some adversaries might seek to steal customer data from a mobile operator; however, other adversaries are interested in halting the production in a petroleum refinery. Example adversaries include a nation-state cyber army working for political reasons and a ransomware group acting for financial purposes. Based on the company (target), we can expect .adversaries



Intelligence needs data. Data has to be collected, processed, and analyzed. Data collection is done from local sources such as network logs and public sources such as forums. Processing of data aims to arrange them into a format suitable for analysis. The analysis phase seeks to find more information about the attackers and their motives; moreover, it aims to create a list of .recommendations and actionable steps

Learning about your adversaries allows you to know their tactics, techniques, and procedures. As a result of threat intelligence, we identify the threat actor (adversary), predict their activity, and consequently, we will be able to mitigate their attacks and .prepare a response strategy