SOAR - Security Orchestration, Automation and response

Traditional SOC works

Socs in the organization gives a lot of help as it enhances the security and makes sure that the organization is safe from any kind of online cyber attacks and this is made sure by continuously monitoring and analysis with the help of various tool analyzing to get results.

The SOCs perform tasks:

- **Monitoring and Detection** : This focuses on continuously scanning and flagging the suspicious activity in the network environment. This lead to awareness of emerging threats and how to prevent them in their early stages.

```
eg.1) detecting no. of failed login attampts.
eg.2) login from unknown location.
```

- **Recovery and Remediations** : Organization rely on their SOC to provide a hub for recovery and remediation when incidents occur. SOC teams operate as first responders when cyber threats are identified. They perform operations such as isolating or shutting down infected endpoints, removing malware, and stopping malicious processes. During this process, they often utilize other security solutions like EDR, firewalls, IAM, etc.

```
eg.1) isolating an endpoint through EDR
eg.2) blocking an IP on the firewall
eg.3) disabling a user on the IAM
```

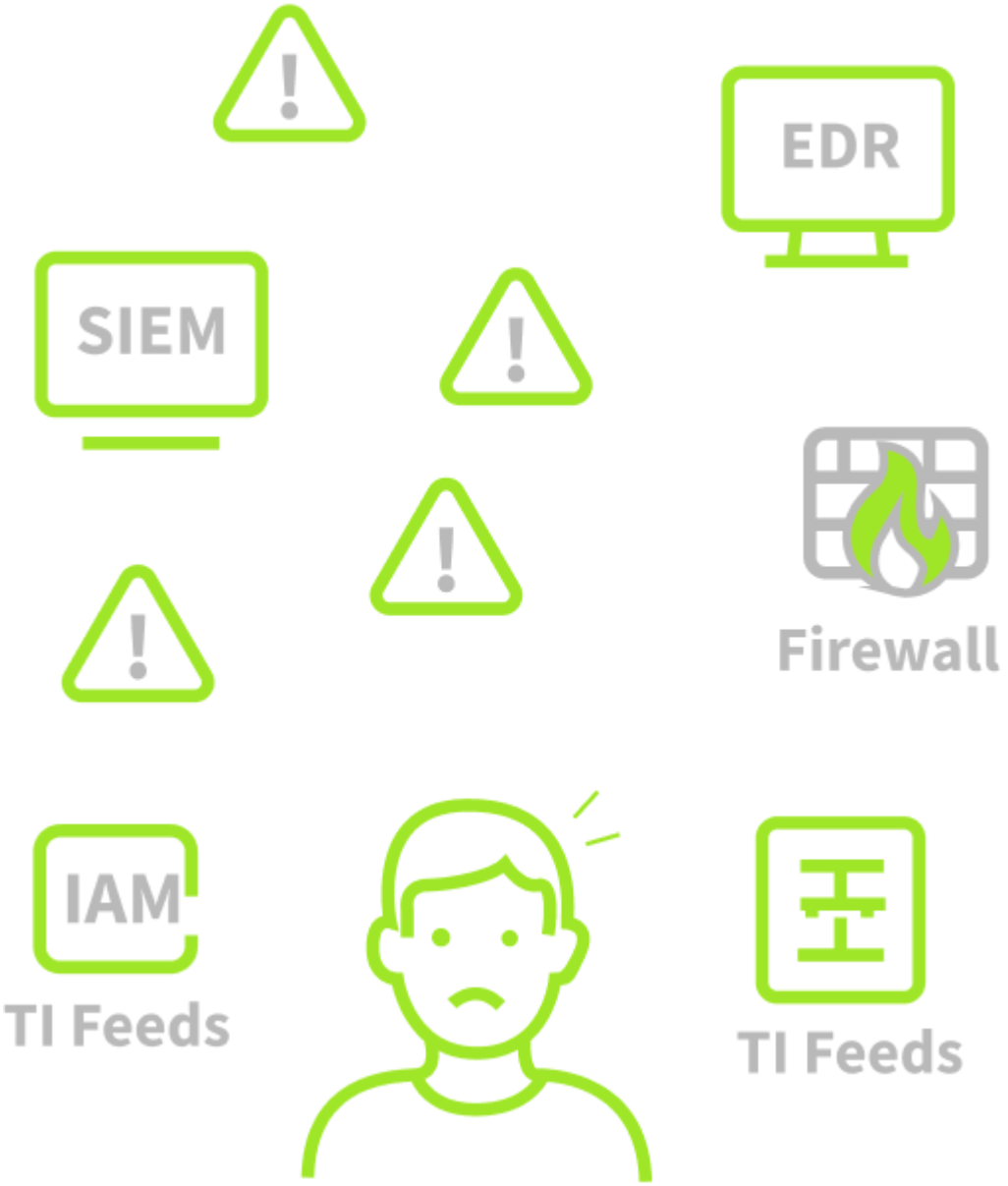
- **Threat Intelligence:** Monitoring environments continuously requires a constant flow of threat intelligence. This ensures that SOC teams have continuous and the latest feeds of threat data, such as IP addresses, hashes, domains, and other indicators.

```
blocking a malicious domain flagged by the threat
```

- **Communication:** The SOC teams not only detect and respond to threats but also coordinate with IT teams and management to effectively communicate the threats and ensure that the incidents are addressed.

```
generating a ticket for the IT team to verify a recently deployed patch.
```

Challenges Faced by SOCs

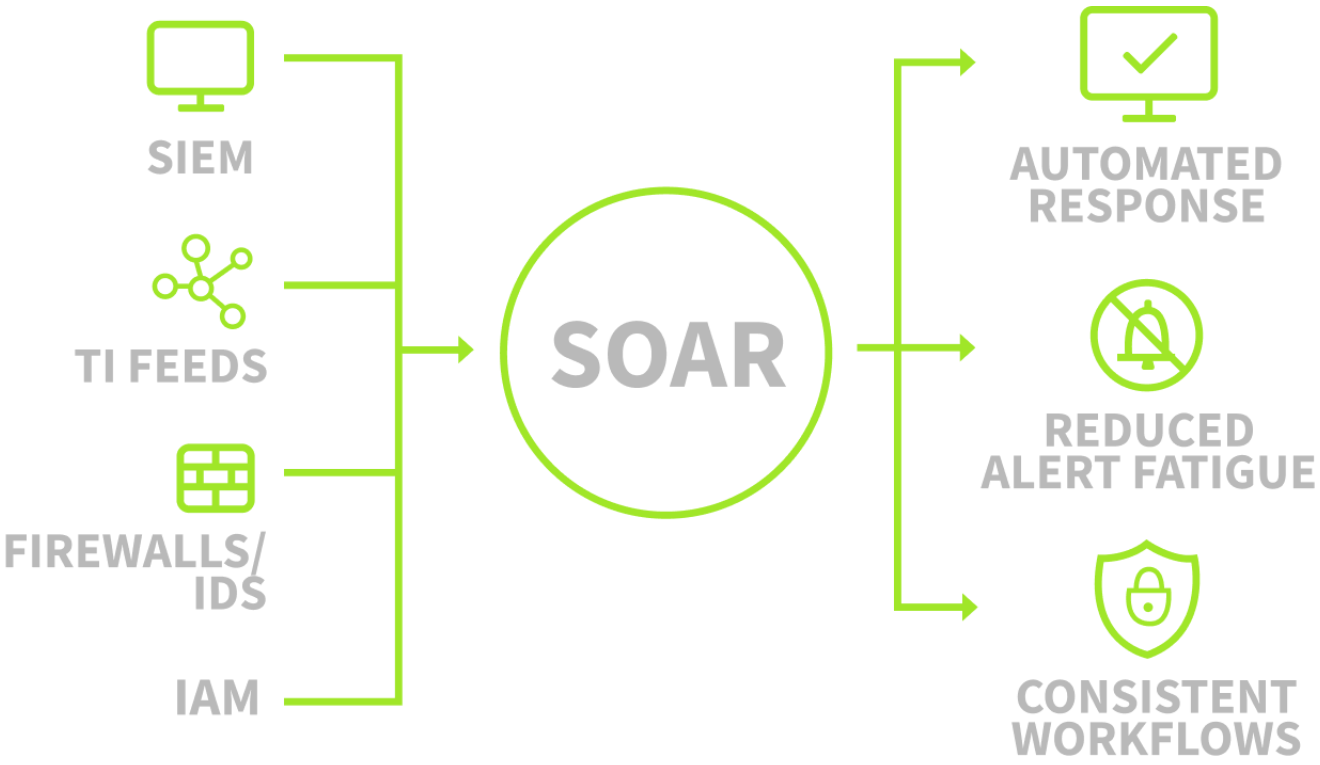


- **Alert Fatigue:** Using numerous security tools triggers a large amount of alerts and noise as many of the alerts found are false positive and hence it leaves analyst overwhelmed and unable to address the real situation.
- **Too many Disconnected Tools:** Security tools are often deployed without integration within an organization. Security teams are tasked with navigating through firewall logs and rules, which are handled independently from endpoint security logs. This also leads to an overload of tools.
- **Manual Processes:** SOC investigation procedures are often not documented, leading to inefficient means of addressing threats. Most rely on established tribal knowledge built by experienced analysts, and the processes are never documented. This results in slowing down the investigation and increasing response times.
- **Talent Shortage:** SOC teams find recruiting and expanding their talent pool difficult to address the growing security landscape and sophisticated threats. Combining this with the alert overload teams face, security analysts become more overwhelmed with the responsibilities they have to undertake, resulting in less efficient work and extended incident response times that allow adversaries to wreak havoc within an organization.

Overcoming SOC Challenges with SOAR

SOAR????

- Security orchestration , Automation and Response is a tool which inculcates all the tool together that are used by SOC.
- This helps SOCs with not switching between various tools like SIEM , firewalls , EDR etc.. as all are at one place helping in effectively and efficiently managing all the things at one place with a single SOAR interface.
- This also gives a ticketing aspect where the case management is been done to the analysis through which they can document, track and resolve their incidents in a structured way .



Orchestrations : It helps in coordinating all the tools together inside the SOAR. It connects different tools from various vendors within the unified SOAR interface. It defines workflows for investigating various types of alerts, known as **Playbooks**.

```
These playbooks are predefined steps that tell the SOAR how to investigate
an alert.
```

For example, the VPN brute force alert we discussed above would have the following playbook:

1. Received alert from SIEM
2. Query SIEM to check if the User normally uses the IP
3. Check TI platforms for the IP's reputation
4. Query SIEM for any successful logins

5. Escalate to containment actions

Automation: The art of coordinating with multiple tools through predefined actions (Playbooks), which we studied in Orchestration, can be automated. Automation means no more manual clicks needed from SOC analysts. SOAR will itself follow the playbooks. Let's resume the playbook for VPN brute force alert combined with the Automation.

1. SOAR receives the alert from SIEM
2. It automatically queries the SIEM for the user's historical logins
3. It automatically verifies the IP's reputation through TI platforms
4. If the IP is malicious, it automatically disables the user from the IAM
5. Lastly, it automatically opens a ticket in the ticketing system with all the details to initiate an investigation

Response: Gives the ability to take actions using different tools from one unified interface. It also automates the response, as we saw earlier while looking at its Automation capability. For example, SOAR can follow the playbook of VPN Brute force and block the IP on the firewall, disable the user in the IAM, and open a ticket with all the details.