Security Operations Infrastructure

Security Operations infrastructure includes a security information and event management (SIEM) platform, analysis tools, and SOC engineering.

Security information and event management

A SIEM platform, commercial or homegrown, is used as a central repository to ingest logs from all corporate-owned systems. SIEMs collect and process audit trails, activity logs, security alarms, telemetry, metadata, and other historical or observational data from a variety of different applications, systems, and networks in an enterprise. Most provide correlation capabilities as well.

For a SIEM to operate properly, connectors and interfaces are required to ensure translated flow from the system of interest to the SIEM data lake. The SecOps organization should define how ownership of an event will be established, as well as the central point to where an analyst will go to receive alerts. Sometimes it is the SIEM, in other cases, it is a security orchestration, automation, and response (SOAR) platform or ticketing system.

The selected SIEM approach should address any governance, risk, and compliance requirements for the separation of data, privacy, and retention times. This will drive requirements on storage space and controls. Limiting data redundancy between the SIEM and feeder systems can help control costs, as well as offline storage for long-term compliance needs.

Analysis tools

Analysis tools include advanced techniques, tools, and algorithms that provide the ability to detect evidence of security compromise within large volumes of data. Processes should be defined around how an analyst will determine if an alert is malicious and the chosen tools should assist or automate this process. Additionally, the tools should provide access to gather context about the given event, preferably automated. Ownership, budget, and the support model for the tools needs to be defined.

Analysis tools are often based on machine learning, deep learning, and artificial intelligence—that provide either stand-alone, embedded, or add-on functionality to detect evidence of a security compromise. Security analytics can be performed on data that is either stored at rest or collected in motion—even at line speed on a massive network. This is a capability that can be obtained by SecOps teams in a variety of different ways with most security products and service including some sort of security analytics function.

SOC engineering

The SOC engineering team is responsible for the implementation and ongoing maintenance of the SecOps team's tools, including the SIEM and analysis tools. It is important to clearly define the responsibilities of this team. Will they be responsible for the licensing, maintenance, and updating of the tools? Will they manage the underlying architecture (CPU, RAM, storage, cloud implementation) or will that be handled by another team? SLAs with the team should be defined to cut down friction between teams, as well as to establish clear communication plans.

Security Operations Automation

Security Operations automation includes security orchestration, automation, and response (SOAR) and security automation.

Security orchestration, automation, and response

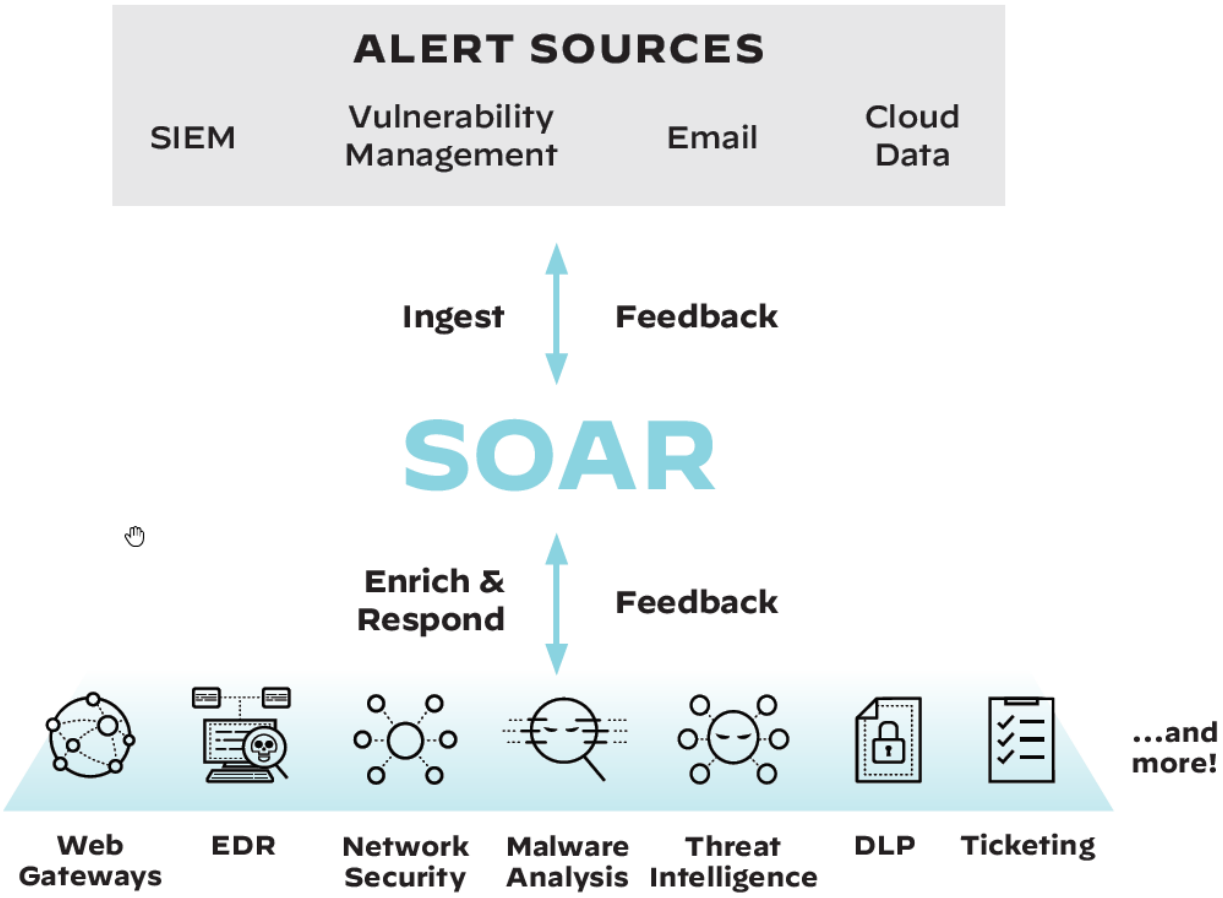
According to Gartner:

> SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.[1]

SOAR systems allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows. SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts. The playbooks coordinate across technologies, security teams, and external users for centralized data visibility and action. They help accelerate incident response times and increase analyst productivity. By standardizing processes, they provide consistency which improves operational confidence in SOC capabilities (see Figure 4-2).

[1] Gartner Glossary. (n.d.). *Security Orchestration, Automation and Response (SOAR)*. Gartner. Retrieved June 4, 2020, from https://www.gartner.com/it-glossary/security-orchestration-automation-response-soar

Figure 4-2 *High-level view of how SOAR tools sit in a SOC*



Security automation

Consistency is a key factor in the effectiveness of a SecOps team. Automation helps ensure consistency through machine-driven responses to security issues. A security automation function will own and maintain these automation tools. They must be tightly integrated with the SecOps team to continuously maintain the automation playbooks. They are also responsible for implementing new automation technology and playbooks in response to new workflows and processes defined by the SecOps team. The requirements, and eventual vetting of the solution, should be the responsibility of the SecOps teams. This vetting should consider the time-savings, accuracy, and usefulness of the automation.

There are some cases in which automation increases the need for resources. It is always necessary to consider the return on investment (ROI) before investing in automation. When doing an ROI analysis, take special care to consider the ongoing cost of maintenance and support.