**SOAR**

Security orchestration, automation, and response (SOAR) is a security incident management and response solution.

## Definition of SOAR

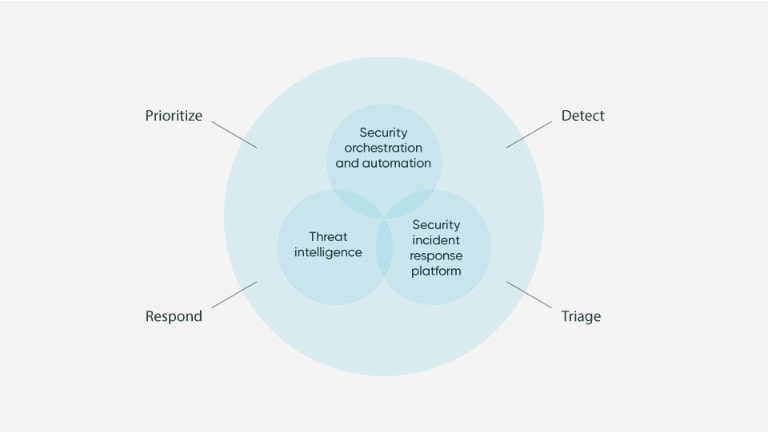
Security orchestration, automation, and response (SOAR) primarily focuses on threat management, security operations automation, and security incident responses. SOAR platforms can instantly assess, detect, intervene, or search through incidents and processes without the consistent need for human interaction.

**SOAR capabilities include:**

* The prioritization of potential threats.
* Assessing potential impact.
* Triaging the most important threats.
* Responding to the threats accordingly.

**Aspects of those capabilities are:**

* Security orchestration and automation to create a strong security foundation, based on best practices.
* Security incident response platform to use as a tool for orchestrated security responses, establishing repeatable and scalable workflows.
* Threat intelligence usage to understand threats preemptively, accelerating prioritization, and after a security threat to confirm the incident is resolved.



## How is SOAR different from SIEM

A security information and event management (SIEM) system collects, analyzes, and stores security related data, including security incidents and events—data could range from firewalls and network devices to patterns that would indicate a cyber attack. SIEM tools typically need a degree of calibration and oversight to determine the accuracy of the data collected and to triage the more important data, which can be labor intensive. SOAR programs are often automated and typically do not require a large degree of expert human oversight to determine if the security events are false positives or actual incidents that require investigation. Time spent investigating and mitigating can be used much more efficiently and usefully.

## Using SIEM and SOAR for improved security operations

Success with security is ideally the combination of SIEM and SOAR. A lot is dependent on the size and type of data gathered around events, and a larger organization could receive up to millions of alerts a day, which a SIEM will gather and analyze. But a lot of data analysis is required to process through all of the data, which is where SOAR can be used in conjunction with a SIEM to process and manage incident response much faster, removing the time consuming and laborious manual incident prioritization and response processes.

## SOAR tools

SOAR is capable of integrating into a wider network of both security and IT platforms, which creates a larger degree of flexibility for any organization and their security operations. There is minimal disruption while enhancing security and efficiency.

## The benefits of SOAR

Every organization should take security practices very seriously, and SOAR is a proven solution for all organizations, as they continue to struggle with increasingly high volumes of information about security and network activity. Multiple teams need to interact with security platforms, and SOAR can help keep everything centralized, efficient and responsive.

### **SOAR helps build workflows & streamline operations**

Orchestration layers are more successful with the implementation of plugins for the most common use cases and technology, which provide pre-built workflows. IT processes and security workflows can then be automated and your technology stack can be connected and collaborative. While you’ll likely need to add additional orchestrations or customize some workflows, there are many templates and building blocks that are easily accessible and help streamline the process.

### **SOAR helps increase flexibility, extensibility, and collaboration**

SOAR solutions can provide the flexibility to either adapt the templated use case workflows to your processes, or build out new workflows easily. There are also collaboration opportunities between other organizations, among teams, and across the enterprise, which can further the need of customization and development of current and new workflows.

### **Respond more quickly and accurately**

SOAR solutions constantly gather information and prioritize incidents using automation that functions based on both pre-planned and custom rules. This ever vigilant approach delivers faster and more accurate incident assessment and prioritization, which can then be utilized to confirm whether a threat is valid, enabling security teams to focus on the threats that matter most.

### **Improve analyst job satisfaction**

Repeated tasks and consistently checking data can be monotonous—such mundane tasks can be automated to increase speed and team morale. Employees can then spend more time innovating and orchestrating, focusing on only those threats that are most impactful.

### **Improve time management and productivity**

Automated responses to threats using SOAR can free up time, which allows employees more opportunities to focus on priority tasks rather than digging through the through alerts to determine which ones should be responded to.

### **Effectively manage incidents**

SOAR technology can accelerate response time to threats and vulnerabilities, as well as increase the accuracy of responses. This machine and data driven workflow significantly reduces the chances of human error, such as missed relevant data, misinterpreted analysis, or also false positives.

### **Automate repeated and error-prone tasks**

SOAR solutions can make security more self-operating and less manual—this helps eliminate repeated tasks, like constantly checking alerts and data that are continually gathered. Repeated tasks and constant human interaction can increase the chance of human error. Automated programs can significantly reduce errors, especially as monotonous tasks are eliminated.

### **Simplify collaboration across operational teams**

Multiple processes and teams are often needed for effective incident response, and SOAR is capable of streamlining processes to create centralized and accessible areas for teams to collaborate.