URL: https://resources.castra.io/

Meta Description: What does the SOAR in SOAR security stand for, and what is SOAR technology anyway? Castra can inform you with a proper definition. Learn all about it!

Primary Keywords:

- ☑ ~~soar security~~

Secondary Keywords:

- ☑ ~~what is soar~~
- ☑ ~~soar cyber security~~
- ☑ ~~soar platform~~
- ☑ ~~what does soar stand for~~
- ☑ ~~soar technology~~
- ☑ ~~what is soar in cyber security~~

Links:

- ☑ ~~https://castra.io/contact/~~

What Is SOAR Security?

The SOAR in SOAR security stands for:

- **S**ecurity
- **O**rchestration
- **A**utomation
- **R**esponse

SOAR security is a set of technologies in a single platform that automatically perform the following tasks regarding security data from a variety of sources:

- Collect
- Coordinate
- Monitor
- Execute

All the data is ingested and integrated into a single platform for visibility, management, and reporting.

Why You Need SOAR Security

There are two main purposes of SOAR security:

1. To detect indicators of compromise at endpoints (e.g., laptops, servers, and VDI machines)
2. To prevent future cybersecurity attacks

SOAR security does this by defining, prioritizing, and driving incident response which is increasingly important in today's world.

Why is SOAR cybersecurity needed so much? Because "in one four-month period (January to April) some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to COVID-19 – were detected by one of INTERPOL's private sector partners reported an uptick in attacks during the pandemic, and 78% of security and IT leaders say remote workers are difficult to secure."

Threats are more numerous, malicious, and complex than ever. Handling these treats manually is no longer possible, even with the help of a very skilled cybersecurity team.

The results of trying it all on your own without SOAR will result in inefficiencies, errors, and overworked staff—Statista posits that 73% of organizations within the industry have reported colleagues quitting due to burnout.

The Three Core Capabilities of SOAR Security

To speak of SOAR's core capabilities, we'll refer to the meaning behind the SOAR acronym.

1. Security Orchestration

Security orchestration is machine-based coordination of interdependent security actions that cover threat and vulnerability management. This orchestration connects and integrates disparate tools and data into one platform (See An Explanation of a SOAR Security Platform below).

At this point, SOAR comprehends and analyzes the data. If a threat is found, an alert is sent to a human security analyst for further investigation.

Security orchestration:

- Provides context for deeper insight into the environment and its threats
- Allows for deeper investigation into why security incidents are occurring
- Places necessary data front and center, allowing for more effective collaboration, problem-solving, and resolution
- Maximizes the value of security tools, processes, and staff

- Uses a highly integrated and intuitive dashboard

The point of all this is to ensure every security and non-security tool works in unison within a single infrastructure, making your job much easier.

2. Automation

SOAR's security automation detects and triages threats in your environment, determining if and how to take action to contain and resolve the issue.

SOAR's security operations utilize automated technologies to enable interoperation playbooks and workflows and use artificial intelligence to predict threats before they happen. This is done when SOAR ingests alert data to trigger its automation capabilities.

Examples of what SOAR can find and automatically alert on include:

- Vulnerability scan findings
- Cloud security alerts
- IoT device alerts
- Environmental threats

With a combination of the following operations, the time to detect and respond to repetitive events, common errors, and false positives is drastically quickened:

- Machine learning
- Human verification
- Automated low-level manual processes

This also grants significant time savings for the SOC team to detect, investigate, and remediate cyberthreats. You'll finally be in a place that allows your team to focus on other valuable work, such as investigative research and security strategy.

3. Response

With SOAR's security incident response, organizations gain the required visibility to:

- **Plan solutions based on access to better intelligence.** The visibility into various technologies offers valuable insight and context your analysts need to know. With the right information, your team can improve practices, conduct deeper and broader investigations, and make the best decisions for resolving issues.
- **Manage all security solutions and tools in one comprehensive platform.** This speeds up the MTTD (mean time to detect) and the MTTR (mean time to respond). Automated processes prevent excess time consumption, as well as false positives.

- **Monitor threats from all sides.** You'll never be caught off guard because of SOAR's automated response tools that immediately assess, prioritize, and send alerts to the right people.
- **Report all security operations activities.** In one easy-to-understand platform, your team and stakeholders can get whatever information that's needed to identify issues and make improvements.

An Explanation of a SOAR Security Platform

SOAR security is a comprehensive tool, but a SOAR platform is needed to bring everything together into a single solution for organizations to improve security operations.

Threats during 2022 have come from a wide range of areas, including:

- Cloud services
- Ransomware
- Software supply chain
- Malware via software updates
- Business email
- Hardware supply chain
- Foreign influence in research and development
- Cryptomining
- Disinformation
- State-sponsored attack on critical infrastructure

Utilizing a SOAR security platform brings all potential threats from every angle into a single view and:

- Provides a single, centralized dashboard for managing and coordinating every aspect of an organization's network security
- Enables automatic actions
- Optimizes case management to create efficiencies
- Facilitates collaboration by enabling visibility across the security stack
- Eases the investigation and resolution of incidents
- Combines and integrates security orchestration, automation, and response into one complete picture

The Similarities and Differences Between SOAR vs. SIEM

There is a common misunderstanding that SOAR and SIEM (security information and event management) are the same or similar products. While these two services have some similarities we'll mention below; they also have their differences.

Similarities Between SOAR and SIEM

Both SOAR and SIEM:

- Detect security issues
- Collect data regarding the root of issues
- Notify security personnel of concerns
- Use a centralized platform

But that's where the similarities stop.

Differences Between SOAR and SIEM

There are key differences between SOAR and SIEM.

SOAR adds automation and response in addition to SIEM's offerings, including alerts for vulnerability scan findings, cloud security and IoT device alerts, and environmental threats (as mentioned above).

Get in Touch

Protecting your environment from security threats should be a top priority—it is ours. The financial and reputational risk that looms large over your business is real. Gartner predicts, "By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

What you want is an integration of SOAR with Threat Intelligence into SIEM. Castra manages Palo Alto Cortex for SOAR using USM Anywhere and Exabeam. The result is outstanding endpoint threat detection and response technology using advanced machine learning and analytics.

Castra wants to help you learn more about the right solution for your business's cybersecurity. That's why we make it easy for you to schedule a meeting or request a quote today.