deepwatch

WHITEPAPER

Best Practices to Apply to Your SOAR Solution

Executive Summary

Threat detection and response is critical as threats continue to evolve and grow exponentially in terms of overall number and impact. However, today many companies rely on a series of disparate and unconnected solutions that make threat response and resolution complex and time consuming. A smart incident response process—like security operations, automation, and response (SOAR)—can help dramatically improve your security posture. To make SOAR successful, organizations need to apply some best practices, recognizing that a successful SOAR implementation is really the culmination of a comprehensive and ongoing process to establish and mature your overall cybersecurity approach.

Key Whitepaper Highlights

- A fully implemented and successful SOAR solution should align to security operations center (SOC) maturity.
- Before you begin the SOAR implementation process, understand the needs of your organization, the extent to which your organization is committed to SOAR, and the availability and capabilities of your staff.
- Understand the scope and scale of your customers, your business, and your platforms (and the logic within them) during SOAR implementation.
- Apply data standards and regularly 'clean' and 'normalize' your data to optimize SOAR.
- An understanding of workflows and an organized approach to playbooks are critical to SOAR.
- SOAR is a comprehensive system of systems requiring regular monitoring to ensure full performance.

Table of Contents

Introduction

IT and security teams are increasingly turning to SOAR—security orchestration, automation, and response—to address the challenges associated with the sheer volumes of alerts and incidents that bombard analysts and systems on a daily basis. SOAR is a proven approach to help increase security operations' efficiency by correlating disparate and unconnected solutions, automating the response, and providing response components, such as playbooks, for the incident management process.

In this paper, we'll explore best practices that need to be implemented and in place to reach full SOAR maturity, focusing on seven essential components to help you ensure an effective SOAR solution.

SOAR DEFINITION

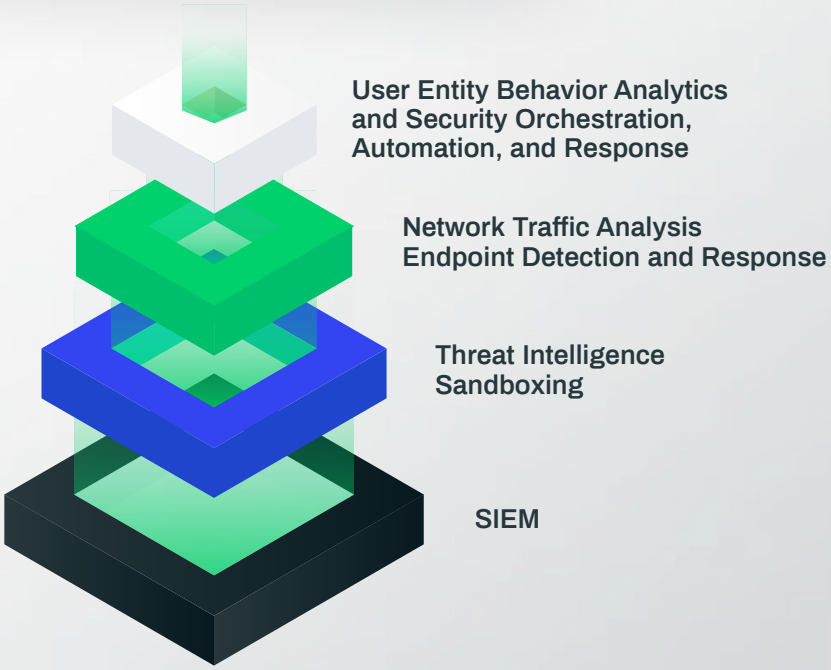
"…solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform."

—Gartner's 2020 Market Guide for Security Orchestration, Automation and Response Solutions

SOAR — A Journey to Operational Maturity

SOAR is based on many different technologies and concepts, and a fully implemented and successful SOAR solution can make a tremendous and positive difference to a company's security and IT operations activities. However, it would be incorrect to view SOAR as a 'silver bullet'—that is, a simple solution that can be implemented in a few short steps or with the addition of a few automation tools. SOAR is the culmination in the evolution of your company's IT and security maturity, with underlying IT and security foundations that need to be implemented and established to ensure that SOAR can be successful and work properly.

SOC Maturity Phases



The foundational components of SOAR include security information and event management (SIEM) technologies, mature and robust threat intelligence and sandboxing, network traffic analysis and endpoint detection and response, and user and entity behavior analytics tools. All of these technologies must also be combined with consistent and established policies and strategies in order to achieve full SOAR maturity.

Understanding Your Cybersecurity Maturity

SOAR Implementation: Seven Best Practices

The SOAR toolset offers security professionals the most beneficial and expedient process to create order out of chaos. Based on our experience, we've found that there are seven critical 'best practice' categories to SOAR implementation:

1. **Assess Organization & Capabilities**
2. **Understand Scope**
3. **Apply Standards**
4. **Clean Your Data**
5. **Understand & Manage Your Workflow**
6. **Plan Your Playbooks**
7. **Monitor SOAR**

1

Assess Organization & Capabilities

You can't begin to implement a SOAR solution without first understanding the needs of your organization, the extent to which your organization is committed to SOAR, and the availability and capabilities of your staff.

Define and manage stakeholders

Implementing SOAR can make a huge difference to effective security operations. But it also means added time and money. The implementation process may require you to consult or work directly with other divisions within your organization such as IT, HR, or Finance. Before you begin the SOAR process, define your stakeholders, engage them, and consult with them to ensure complete organizational buy-in and support.

Staff the SOAR process appropriately

Having the right combination of skills on your team as you implement SOAR is critical. (Total staff numbers will vary depending on your organization's size and complexity.) Team members with "DevSecOps" expertise are necessary, specifically skills and experience in software engineering, computer engineering, security engineering, development and operations.

2

Understand Scope

The concept of "scope" is a crucial topic when it comes to SOAR. Scope can reference the size or geographic scale of a system or the structure of a system (that is, the logic platform on which the system is based). This means "scope" can impact how you implement and manage a SOAR solution.

Business/Customer Scope

The size of your organization, your customers, and even the risk factors can determine your IT/security strategies, policies, and solutions, including SOAR processes and technologies. Organizations that possess large security operations or manage large-scale global networks—or security providers that support customers with large, complex systems—will have additional security and compliance requirements, as well as different response plans than much smaller companies, depending on the type of incident and the systems impacted.

As you implement SOAR, you need to understand how an incident might impact your business or your customers' businesses. What are your business goals and how would an incident impact the bottom line? What are the critical business risks as defined by your organization or industry and what are the mitigation and tolerance levels? What are your customers' goals and risks and how would an incident impact them?

GLOBAL ROUTER PARADIGM

The team at deepwatch has created a concept that we call the "Global Router Paradigm" (GRP) to address problems we often see around scope. **This breaks down scope at the global level (80% of incidents and responses) and at the local level (20% of incidents and responses).**

This GRP solution can help solve the "Goldilocks problem" that often exists in security—that is, how do you manage your development assets to ensure you have exactly the right number of assets to manage your security.

Logic Scope

The scope can also be inherited from existing platforms underneath the umbrella of SOAR, and this, in turn, can determine the level and extent of customization and automation. A thorough understanding of scope within the context of SOAR affords a degree of flexibility in this regard. For example, when an alert is triggered, metadata passes from the security and event management (SIEM) system to SOAR. This metadata needs to be inspected to determine scope. The outcome of the inspection will decide whether the response follows a global playbook or custom route, and with SOAR maturity you have the ability to accommodate some level of customization and automation if that is preferred.

Managing Scope

To manage scope as you implement SOAR, you need to make sure your logic and decision making are based on a deep understanding of why you are doing something and what you hope to achieve with the end result.

3

Apply Standards

Standards within cybersecurity are critical and without them confusion can reign. In security terms, the concept of "standards" can mean a variety of things—ranging from consistent naming conventions to defining the threshold that determines a successful incident outcome. Applying a standardization process as part of SOAR can help ensure both a smooth implementation and an effective incident response.

Create standards for names and definitions

Simple as it may sound, using the same naming convention and clearly and consistently defining terms across all code, scripting, and documentation can go a long way to ensuring you avoid major problems during incident response. What you call a 'duck' in one program, should always be called a 'duck' in every other program. You should also make sure that everyone—from the IT manager to the CIO—understands a consistent definition of 'duck'.

Create coding and scripting standards

An ability to write script, doesn't mean that the script is written well. And, while someone's code may work 99% of the time, the 1% of the time it doesn't work could create major headaches for your department or the entire organization by allowing security incidents to slip through. Therefore, it is critical to set performance standards around the assets you have within a platform and ecosystem.

Standardize your playbooks

Security playbooks are critical. They define roles, responsibilities, processes, and anticipated results for incidents. They also ensure all organizational staff involved in the incident—from security and IT to public relations and legal—have a clear understanding of what they need to do during incident response. If your security playbooks do not contain consistent standards, naming conventions, and definitions, you could face problems later on during the development and automation processes.

Standardize system integrations

Many disparate security solutions often make-up an organization's defenses. When you have so many security components from different suppliers, it isn't wise to take a shotgun approach to integration. Integration standardization needs to include identifying the target data, knowing where the data will be located in the new system, identifying data transaction dependencies, knowing how the target systems will be connected and what security may apply, and understanding the interface options.

Align standards to your company's software development lifecycle (SDLC)

Understand your deployment and release cycle and ensure standards are in place and aligned to your SDLC. Software needs to be fully aligned in terms of how it works, how you control it, and how you intend to deploy it. For example, if the people managing the platform do not understand how the rest of the company uses the software, then problems tend to arise. Additionally, the SOAR platform isn't designed to operate effectively during massive releases of information, because in addition to managing deployment, the SOAR platform also needs to ingest information to identify security incidents and run automated systems—all simultaneously. Therefore, creating a standard of incremental deployments as part of your SDLC is critical.

Standardize your documentation

Standardized documentation is essential to ensure staff understand your systems and applications. The Common Information Model (CIM) is useful to apply here, since it defines the elements in an IT environment individually, as a collective, and the relationships between them. CIM not only enables different individuals and teams to exchange information about these elements, it also allows the individuals and teams to control and manage the IT elements to the same set of operational standards.

Use CIM to standardize workflows

In addition to applying the CIM to your documentation, also consider building the CIM into your workflows. CIM helps everyone understand why a problem may have happened and provides a consistent response.

4

Clean Data

Data is at the bottom of the IT and security pyramid. It is the foundation that underpins all other structures, platforms, and applications. For this reason, clean data is critical to using SOAR effectively.

Maintain clean datasets

Scrub your data and enforce criteria around it. Many people looking to adopt SOAR assume that if they use SIEM or clean their Office 365 logs, once the data gets into SOAR, then SOAR will take care of the rest. Unfortunately, this isn't the case. You need to continually 'normalize' your data (even if you've already done this as part of your SIEM process), because SOAR will likely have its own fields and criteria and all the sources feeding SOAR (e.g., SIEM, incidents from a phishing inbox, EDR system, etc.) need to match. Even if you use a SIEM to organize your data, expect that you will need to repeat the process once that data is integrated into SOAR.

5

Understand and Manage Your Workflows

In addition to ensuring you maintain the same set of standards when you develop workflows, it is important to understand your workflows at both the micro and macro level.

Understand user logic and user processes

As part of the SOAR implementation process (and as an ongoing best practice), interview your teams, managers, and directors and determine what is important to them, and then ensure that this is reflected in the workflow. Do not simply sit down and begin building the SOAR platform, assuming you'll get immediate value without first having spent some time understanding what is important to the individuals that use the systems within your organization. Try to get the best outcome for your workflows based on a thorough understand of user logic and user processes.

Integrate SOAR into your workflows

SOAR is about incident identification, management, and response. If your SOAR platform goes down, you may find this has a greater impact on your security operations than if an individual security application were to fail. Have a workflow process in place to address a platform-failure scenario so you can address the issue and get SOAR up and running again as quickly as possible.

Understand events within the workflow

SOAR is meant to ensure that security operations have repeatable and organized processes. This means that when you develop your workflow templates, you need to take time to understand event origins and how the event management system organizes and prioritizes events. Think of the event as a single atom within a larger ecosystem and analyze how that event is managed and how it became an incident. Once you get to the incident phase, take time to understand your response. Understanding the event details is critical to creating a repeatable response.

Incorporate standard operating procedures (SOP) into your workflows

Standard operating procedures within a workflow can not only enable the automation of some or all parts of the workflow but they can also create an expectation for your analysts to have a consistent output at the end of an incident.

Convert workflows into logical diagrams

Once you understand the logic, the process, and the individual event details, and have established SOPs, convert this workflow into an easily understandable diagram. The diagram could be a flow chart or simply a series of statements. Also, remember to include your diagram in within the appropriate playbook.

6

Plan your Playbooks

While your workflows are the logical representation of what your company wants to do when an incident occurs (the "if-else" statement), the Playbook is the actual SOAR tool to encapsulate everything in your security processes. When developing and planning playbooks so they align with SOAR tools, it is important to think in terms of a "crawl, walk, run" process. It can be tempting to immediately rush to the run phase by starting playbook development on day one and cranking them out. But consistency among playbooks is key, because the minute you find inconsistencies between two playbooks, you will question all the playbooks, which means going back and doing a complete audit against all of them.

Start small

Apply the principle of crawl-walk-run. Don't start with playbooks on day one, because consistency among all playbooks is key and playbooks need to be built on the premise of understanding scope, applying standards, having clean data, and understanding and managing workflows. Before you begin to build a playbook, create a plan that leads into playbooks instead of automatically backing into solutions.

Include the human factor in your playbook

While full automation may be your goal, it is impossible to completely exclude humans from the security process. Therefore, any process that involves human interaction needs to be included in your playbook. If the human component within the playbook can't be read and understood in five seconds or less, then your playbook is probably too large or complex and should be broken down into something more manageable.

Organize your playbook logically

Playbooks need to be organized and structured in a way that makes sense to both the reader and your overall objective. They also need to be a length that is manageable. During an incident you don't want your responders to have to wade through hundreds of pages of unstructured content.

7

Monitor SOAR

SOAR is a "system of systems." It controls both input and output. The SOAR platform, by its very nature, is a large-scale system, which means there are many ways for things to go wrong. Therefore, once you've implemented SOAR, ongoing monitoring of the platform and the underlying infrastructure is critical.

Connect SOAR to all monitoring systems

Make sure SOAR is connected to your monitoring platforms and to your event management system.

Develop a SOAR response plan

Because of the nature of SOAR as a 'system of systems', a response plan is critical if something breaks down within SOAR.

Designate 'tiers' for your components

SOAR has multiple different components and widgets that you need to interact with. Understand what exists within your SOAR platform, as well as the platforms beneath and around it. Matrix the issues and incidents that may exist within this platform so you can then create tiers to understand what is critical and what is less important.

Devote staff to monitoring

The SOAR platform is always evolving, which means you need people monitoring it to make sure you're capturing issues. With SOAR, the more you use it and the more you put into it, the more the responses and results will change—that is, more data, more volume, and more syntax means changes on the back end. Make sure you have at least one person or your team devoted only to monitoring the SOAR platform, not only from a security outcome perspective, but also from an operational perspective. Further, make sure they understand how to capture, classify, and move conversations and response plans forward when something occurs within that platform. Central to SOAR's adoption is the expression of business workflows, leading to SOC alignment and security use case value realization. Ensure SOAR teammates are involved, understand, and are able to further security maturity through SOAR outcomes.

Capture data on failure points

If something within SOAR fails, have a method in place that captures all the details so you can understand what happened and address any issues. Problems in SOAR result from two well-known root causes—technology failures and process failures. SOAR teams should be involved with continuous improvement efforts to further align process and technology to drive security outcomes.

Conclusion

Leveraging the latest technologies, architectures, and automation to support cybersecurity efforts is more important than ever. SOAR can help consolidate the increasing number of security solutions and functions found in today's SOC environment. But to make SOAR successful, it is critical to view it as more than a means to an end; SOAR is a framework requiring ongoing and proactive response and engagement to help your organization manage threats, prevent attacks, and gain insight into the dangers and risks associated with threats. To enjoy the benefits of SOAR, security teams need to be prepared to engage in several best practices, including understanding your organization, its capabilities, and the scope and scale of your business and systems. Teams also need to apply standards, clean data, and manage workflows and playbooks effectively. Finally, with SOAR operational, security teams need to monitor the framework regularly. When implemented correctly and with best practices applied, SOAR enables the security team to manage and respond to alerts and threats quickly and efficiently, leaving time to focus on mission-critical, security-based tasks which contribute to a higher functioning SOC.

What's Next?

If you would like to learn more about how deepwatch ally's with its customers to secure their networks, please visit **www.deepwatch.com** or reach out to us at **sales@deepwatch.com**

deepwatch

ABOUT DEEPWATCH

deepwatch secures enterprises via its unique, highly automated cloud based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. Deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. deepwatch's managed security services are trusted by leading global organizations.

CONTACT US

sales@deepwatch.com
7800 E Union Ave, Suite 900 Denver, CO 80237
855.303.3033

deepwatch.com