SOAR

Security Orchestration, Automation and Response

By: Team 9.2

John Aaromal

Sachin Bharti

Sanjit Narayanan G

Revanth P

22 June 2023

What Is SOAR?

"SOAR" stands for Security Orchestration, Automation, and Response. SOAR refers to a set of technologies and processes that help organizations streamline and automate their security operations, incident response, and threat intelligence activities. While SOAR is not exclusive to red teaming, it can certainly be used to enhance red teaming efforts

Threat intelligence platforms (TIP), security orchestration and automation, and security incident response platforms (SIRP) are the three technologies that make up SOAR (Security Orchestration, Automation and Response).

Using SOAR technology, enterprises may gather and compile a sizable quantity of security data and warnings from several sources. They may use this to standardise threat detection and remediation processes and construct automated processes to react to low-level security events more efficiently.

Businesses may greatly enhance how quickly they can recognise and react to assaults thanks to SOAR. We describe what SOAR security entails, its advantages for business, and any possible drawbacks in this post.

WHAT IS THE PURPOSE OF SOAR?

The term SOAR describes technology that allow businesses to gather information about security risks and react to security events with little to no human involvement. The strain on security operations teams is greatly lessened as a result. In order to ensure that all systems are operating in harmony while preserving speed and efficiency, SOAR addresses a number of the major issues that these teams encounter.

• Getting the information needed to distinguish between real threats and false positives and correlating that data.

• Planning the best course of action to address threats

By vastly increasing effectiveness, SOAR security eliminates all of these difficulties. It offers a standardised method for data aggregation to aid in both human and machine-led analysis, automates detection and response procedures to lessen alert fatigue, and concentrates analysts' attention on activities that need more in-depth human analysis and intervention. In order to strengthen their cyber security posture, a growing number of businesses are turning to SOAR.

WHAT IS INCLUDED IN SOAR?

The research company Gartner is credited with the term's first use, and its three essential competencies are as follows:

- **Security Incident Handling:** Technologies that promote repeatable and scalable processes by enabling the management, tracking, and coordination of incident response.
- **Data Enrichment for Threat Intelligence:** Threat and vulnerability management solutions aid in the remediation of vulnerabilities, enabling companies to respond to threats more quickly and intelligently, setting higher priorities, and assisting in the confirmation of incident resolution.
- **Automated Security Measures and Orchestration:** The automation and orchestration of workflows, processes, and reporting are supported by security orchestration and automation technologies, which link and simplify numerous systems.

Maximising SOAR: Example Use Cases

Common use cases for SOAR security include:

- An excessive amount of manual security processes necessitating automation;
- Additional incident response support needed by the internal security team;
- Evaluating and responding to an excessive amount of phishing emails;
- Querying certificate management tools to identify expiring certs;
- Automating the isolation of infected machines;
- Simplifying SOC case management when multiple solutions are in use.

How SOAR can be used in Red Teaming Scenario

1. Scenario: The red team is tasked with assessing the security of a financial institution's network infrastructure.
2. Automation and Orchestration: The red team utilizes a SOAR platform to automate certain aspects of their testing. They configure the platform to perform automated

vulnerability scanning against the target network, identify open ports, and map the network topology. This automation saves time and allows the team to focus on more complex attack vectors.

3. Threat Intelligence Integration: The SOAR platform is integrated with threat intelligence feeds that provide real-time information on emerging threats and known attack patterns. The red team leverages this integration to stay updated on the latest attack techniques and incorporate them into their testing methodologies.
4. Incident Response Automation: During the red team engagement, the SOAR platform detects suspicious activities generated by the simulated attacks. The platform automatically triggers predefined incident response playbooks, which include actions such as capturing network traffic, isolating compromised systems, and generating alerts for the blue team (the defenders).
5. Collaboration and Reporting: As the red team progresses, they utilize the collaboration features of the SOAR platform to share findings, communicate securely, and coordinate their actions. They can annotate and document their findings in real-time, ensuring that critical information is captured and shared efficiently.
6. Post-Engagement Analysis: After the red team engagement concludes, the SOAR platform assists in generating comprehensive reports summarizing the vulnerabilities, attack paths, and recommendations for improving the organization's security posture. These reports can be shared with the blue team and other stakeholders to facilitate remediation efforts.

SOAR Benefits

Because of the constantly changing threats, the lack of experienced security people, and the need to manage and monitor expanding IT estates, SOAR assists companies of all sizes in enhancing their capacity to quickly identify and react to assaults. It does this by using

1. **Delivering a higher standard of intelligence**

Attackers' strategies, methods, and procedures (TTPs), as well as the capacity to spot indications of compromise (IOCs), must be well understood in order to combat the risks posed by the increasingly complex cyber security threats. By enabling them to combine and evaluate data from a variety of sources, SOAR helps SOCs to become more intelligence-driven.

Platforms for threat intelligence, exchanges, and security tools like firewalls, intrusion detection systems, security information and event management (SIEM), and user and entity behaviour analytics (UEBA) may all be included in this list. This helps security professionals contextualise occurrences more quickly, make wiser choices, and hasten issue identification and response.

2. **Enhancing operational efficiency**

Due to the need to handle a variety of technologies, security employees are under growing strain. In addition to the continuous monitoring necessary to guarantee the reliable operation of systems, the many alerts they produce each day may also cause alert fatigue.

The use of SOAR technologies enables security operations centres (SOCs) to automate and partially automate a number of their normal functions. Because they display intelligence and controls via a single pane of glass and make use of AI and machine learning, SOAR products considerably decrease the need for SOC teams to transfer from one technology to another.

In addition to ensuring that procedures are handled more effectively, SOAR security solutions may increase an organization's productivity without requiring them to hire additional staff. Because of this, a major advantage of SOAR is that it encourages security personnel to work more efficiently rather than harder.

3. **Accelerating incident response**

Rapid action is essential for reducing the risk of breaches and the serious harm and disruption they may bring. SOAR helps enterprises shorten the mean time to detect (MTTD) and mean time to react (MTTR) by allowing security alarms to be qualified and addressed in minutes as opposed to days, weeks, and months.

Security teams may automate playbooks, or incident response processes, with the help of SOAR. It may assist with various automatic actions, such as banning an IP address on a firewall or IDS system, suspending user accounts, and removing infected endpoints from a network.

4. **Streamlining reporting and information acquisition**

Employees on the front lines of cyber security operations spend an excessive amount of time monitoring cases, writing reports, and capturing incident response protocols.

Due to its ability to compile information from a variety of sources and show it via dashboards that are specifically designed for each company, SOAR aids in the reduction of this kind of paperwork while also enhancing communication between the C-suite and the frontline.

Better time to resolution comes from completing activities more quickly. This is crucial since there is a larger risk of harm and disruption the longer hazards go neglected.

Integration of SOAR in Red Teaming: Enhancing Efficiency and Effectiveness

1. **Introduction**
    a. Definition of SOAR (Security Orchestration, Automation, and Response)
    b. Overview of Red Teaming and its objectives
2. **Understanding Red Teaming**
    a. Definition and purpose of Red Teaming
    b. Key steps involved in the Red Teaming process
    c. Identification of vulnerabilities and weaknesses in security systems

3. **Introduction to SOAR**
    a. Definition and components of SOAR
    b. Role of SOAR in security incident response
    c. Benefits of integrating SOAR into Red Teaming activities
4. **Integration of SOAR in Red Teaming**
    a. Pre-Engagement Phase
        - Assessing the organization's security infrastructure
        - Defining objectives and scope of the Red Teaming exercise
        - Identifying potential attack vectors and techniques
    b. Planning Phase
        - Mapping out the Red Team's attack scenarios
        - Creating test cases and attack vectors
        - Defining rules and triggers for automated response actions in SOAR
    c. Execution Phase
        - Simulating real-world attacks and exploiting vulnerabilities
        - Generating security incidents and alerts
        - Leveraging SOAR to automate incident response actions
    d. Response Phase
        - Analyzing and triaging security incidents
        - Utilizing SOAR to orchestrate response workflows
        - Automating containment, mitigation, and remediation actions
    e. Reporting Phase
        - Documenting findings, vulnerabilities, and successful exploits
        - Detailing the effectiveness of SOAR in incident response
        - Recommending improvements for future Red Teaming exercises
5. **Benefits of SOAR Integration in Red Teaming**
    a. Enhanced Efficiency
        - Automating repetitive tasks and incident response workflows
        - Streamlining incident triage and resolution processes
        - Reducing response time and minimizing human error
    b. Improved Effectiveness
        - Orchestrating and coordinating multiple security tools and systems
        - Enabling real-time threat intelligence integration
        - Facilitating proactive threat hunting and rapid response
    c. Scalability and Consistency
        - Enabling consistent response actions across multiple incidents
        - Adapting to evolving threats and security landscapes
        - Supporting the scalability of Red Teaming activities
6. **Challenges and Consideration**
    a. Integration complexity and learning curve
    b. Ensuring compatibility with existing security infrastructure
    c. Balancing automation with human decision-making
    d. Maintaining confidentiality and data privacy during automation
7. **Conclusion**
    a. Recap of the benefits of integrating SOAR in Red Teaming

b. Importance of continuous improvement and adaptation in security practices
c. Future prospects and potential advancements in SOAR integration

How to implement SOAR?

1. **Choose a SOAR platform**:

There are a number of SOAR platforms available on the market, including:

- **Splunk Phantom**: Splunk Phantom is a popular SOAR platform that is known for its flexibility and scalability.
- **IBM Resilient**: IBM Resilient is another popular SOAR platform that offers a wide range of features and integrations.
- **Siemplify**: Siemplify is a cloud-based SOAR platform that is easy to use and manage.
- **ThreatConnect**: ThreatConnect is a SOAR platform that is focused on threat intelligence and incident response.

The best SOAR platform for your organization will depend on your specific needs and requirements. If you are not sure which platform to choose, you can contact a SOAR vendor for assistance.

2. **Configure the SOAR platform**:

Once you have chosen a SOAR platform, you will need to configure it to meet your specific needs. This may involve adding integrations with your existing security tools and defining workflows for different types of incidents.

The configuration process will vary depending on the SOAR platform you are using. However, most platforms will have a wizard or other tool to help you get started.

3. **Train your team:**

Once the SOAR platform is configured, you will need to train your team on how to use it. This will help to ensure that they are able to effectively respond to incidents.

The training process should cover the following topics:

- How to use the SOAR platform to automate tasks
- How to define workflows for different types of incidents
- How to use the SOAR platform to track the progress of incidents

The training process should be tailored to the specific needs of your team. However, most organizations will need to cover the topics listed above.

SOAR Challenges

According to Gartner, the absence of or immaturity of processes and procedures within SOC teams continues to be the biggest barrier to the implementation of SOAR security. This is why seeking professional guidance is essential while preparing to deploy SOAR. Other significant difficulties related to SOAR adoption include:

Unrealistic expectations: SOAR cannot solve all security issues. When adopting SOAR, enterprises run the danger of failing to identify use cases that are clearly defined and objectives that are doable.

Integration issues: The capacity to successfully combine the tools and technology necessary for security monitoring and incident response is a significant hurdle in the implementation of SOAR. Information sharing and automating processes might be difficult and time-consuming since various technologies will differ in terms of data formats, APIs, or protocols.

Over-reliance on automation: It's important to avoid relying only on the playbooks and procedures that SOAR first established. Companies should use modern security knowledge to make sure its SOAR is always prepared to handle all kinds of attacks.

Unclear metrics: Organisations run the risk of failing to get the SOAR outcomes they need if they don't explicitly identify their success criteria. This implies that it is crucial to comprehend the whole scope of what they are attempting to automate.

Limited in-house expertise: While SOAR helps in the medium and long terms to lessen the workload on in-house teams, it demands a maturity level that needs SOCs to have certain kinds of skills and competencies to guarantee a timely and successful deployment.