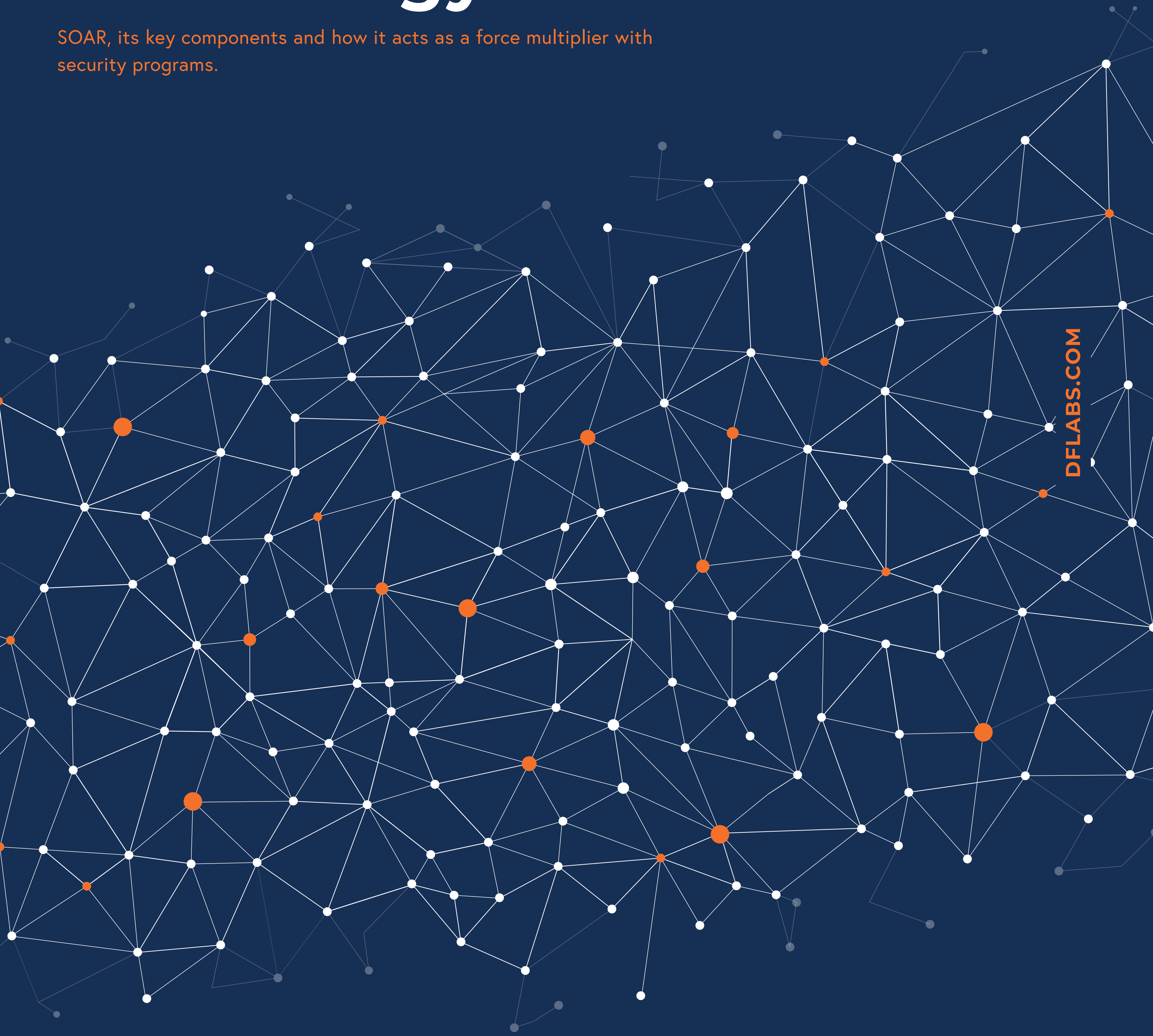
WHITE PAPER

Security Orchestration, Automation and Response (SOAR) Technology.

SOAR, its key components and how it acts as a force multiplier with security programs.



DFLABS.COM

Automate.
Orchestrate.
Measure.

ACADIA TECHNOLOGY GROUP

DFLABS
CYBER INCIDENTS UNDER CONTROL

Contents.

This document contains confidential and proprietary information for use only by DFLabs S.p.A and its intended recipients and must not be disclosed to unauthorized individuals without prior, written consent.

Introduction.

The Security Orchestration, Automation and Response (SOAR), formally defined by Gartner as Security Automation and Orchestration (SAO), product space has grown exponentially in recent years as an increasing number of enterprises, security operations centers and managed security service providers have looked to new and innovative solutions to address several pervasive problems.

Gartner estimates that by 2019, 30% of mid to large-sized enterprises will leverage a SOAR technology, up from an estimated 5% in 2015. As has historically been the case with many other emerging product categories, the exact definition of what constitutes a SOAR solution, the key components of a SOAR solution, and where a SOAR solution fits into the security ecosystem has continued to evolve as the market matures.

https://www.gartner.com/doc/reprints?id=1-4O4VC17&ct=180109

Why SOAR?

Gartner estimates that by 2019, 30% of mid to large-sized enterprises will leverage a SOAR technology.

Like many new product categories, SOAR was born from problems without solutions (or perhaps more accurately, problems which had grown beyond the point that they could be adequately solved with existing solutions). To more accurately define the product category, it is crucial to first understand what problems drove its creation. There are five key problems the SOAR market space has evolved to address.

Increased workload combined with budget constraints and competition for skilled analysts means that organizations are being forced to do more with less.

As the number and sophistication of threats has grown over the past decade, there has been an explosion in the number of security applications in the enterprise. Although each security application solves a specific problem, the growing number of security applications in the enterprise creates an additional problem; as the number of applications grow so too does the workload of monitoring, correlating and responding to alerts from these applications. Analysts are being forced to work within multiple platforms, manually gathering desperate data from each source, then manually enriching and correlating that data.

Limited security budgets, compounded by the fact that it is often easier to garner executive support for additional security applications than it is for additional personnel resources, mean that most security teams must find innovative ways to achieve more without increasing staff levels.

Although it may not be as difficult to find security analysts as it once was, a truly skilled security analyst is still somewhat of a rare breed. Intense competition for these skill analysts means that organizations must often choose between hiring one highly skilled analyst, or several more junior analysts.

Valuable analyst time is being consumed sorting through a plethora of alerts and performing mundane tasks to triage and determine the veracity of the alerts.

As the threat landscape has expanded and evolved over the last decade, the number of different security tools in the average organization has exploded. Even when alerts from these tools are centrally managed and correlated through a SIEM, the number of alerts is often overwhelming for security teams. Each one of these alerts must be manually verified and triaged by an analyst. Alerts which are determined to be valid then require additional manual research and enrichment before any real action can be taken to address the potential threat. While these manual processes are taking place, other alerts sit unresolved in the queue and additional alerts continue to roll in. Any one of the numerous benign looking alerts left untouched in the queue for minutes or hours, while these manual processes take place, represent ongoing risk to the organization.

> **The cost of the average incident has increased year on year.**

Security incidents are becoming more costly, meaning that organizations must find new ways to further reduce the mean time to detection and the mean time to resolution.

The cost of the average incident has increased steadily year on year. The immediate cost of an incident due to lost sales, employee time spent, consulting hours, legal fees and lawsuits is relatively easy to quantify. The financial loss due to reputational damage however, can be much more difficult to accurately measure. Numerous laws and regulations across the globe now require a timely and efficient response to a potential security incident; failing to meet these standards may result in hefty fines and other penalties.

Each of these facts means that reducing the time to detect and resolve potential security incidents must be an absolute priority. Each hour that a security incident persists is effectively money out of the door. This means that having an efficient, documented and repeatable process in place to detect and resolve security incidents as quickly as possible is no longer a good idea, it is an absolute must requirement for any organization.

> **Documenting security processes is a complex, but critical task for all security teams.**

Tribal knowledge is inherently difficult to codify, and often leaves the organization with personnel changes.

Training new analysts takes time, especially when processes are manual and complex. Documenting security processes is a complex, but critical task for all security teams. Even when security processes are documented in traditional linear-style playbooks, choosing the most appropriate course of action is often left to the judgment of an analyst. As such, even with highly documented processes, organizations often rely heavily on the more tenured analysts to make manual decisions based on their experience and knowledge of the organization, something commonly referred to as tribal knowledge.

Employee retention is an issue faced by almost every security team. Highly skilled analysts are an extremely valuable resource for which competition is always high. Each time an organization loses a seasoned analyst, some tribal knowledge is lost with them and they are replaced with an analyst who, even if they possess the same technical skills, will lack this tribal knowledge for at least a period of time. Organizations must hope that at least one seasoned analyst remains in order to transfer that tribal knowledge to new analysts. The more manual and complex the security process is, the longer it takes to transfer that tribal knowledge.

Security operations are inherently difficult to measure and manage effectively.

Unlike other business units which may have more concrete methods for measuring the success or failure of a program, security metrics are often much more abstract and subjective. Traditional approaches to measuring return on investment are often not appropriate for security projects and can lead to inaccurate or misleading results. Properly measuring the effectiveness and efficiency of a security product or program requires a measurement process specially designed to meet these unique requirements.

Security incidents are dynamic, complex events which require a management process unlike those used to manage daily information technology processes. Failing to correctly manage a security incident can result in exponential increases in loss and reputational damage to the organization. As previously mentioned, properly managing security incidents requires a documented, repeatable system which has been thoroughly tested and is well understood by each stakeholder in the response process.

What is SOAR?

Security Orchestration, Automation and Response (SOAR) solutions should provide three core functions; Orchestration and Automation, which enable Response, as well as Measurement.

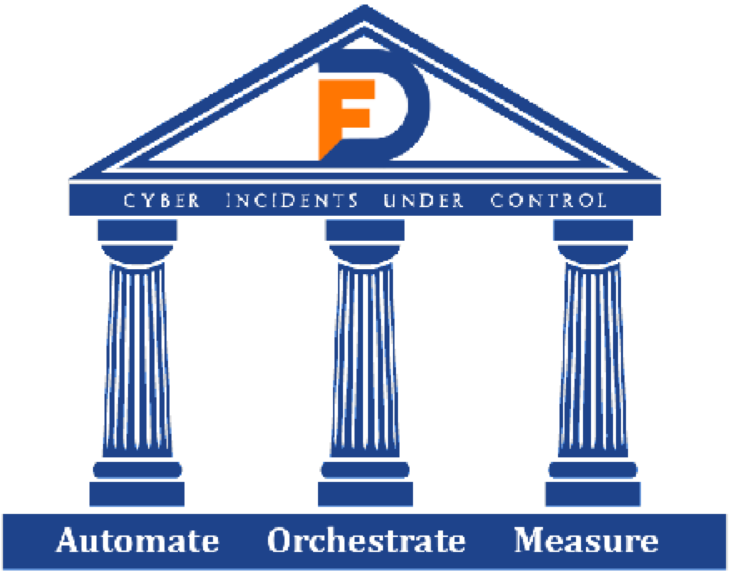


Figure 1. The Three Pillars of SOAR.

Orchestration.

The number of technologies involved in today's advanced security and incident response programs is exponentially more than it was even five years ago. While this has become necessary in order to effectively detect and respond to the current range and complexity of today's threats, it has created its own problem; coordinating these into one seamless process. When triaging or responding to an advanced threat, analysts are often required to interact with many individual technologies, forced to manually perform tasks in each technology and correlate information by hand before an informed decision can be made. Gartner refers to this as "context switching", and it can create enormous inefficiencies in an organization's security program.

Technology integrations are the most common method used to support technology orchestration. There are numerous methods which can be used to integrate technologies through a SOAR solution. There are both pros and cons to each method used to support technology integrations, discussed in greater detail in the Flexible Integrations section ahead.

Although technology is typically the primary focus of orchestration, it is equally important to consider the orchestration of people and processes in a holistic security program. Technology should be supported by effective processes, which should enable people to respond appropriately to security events. A strictly technology-centric security program is no longer adequate; people and processes must also be orchestrated properly to ensure that a security program is operating at its maximum efficiency. For a SOAR solution to achieve its maximum potential, it must support the seamless orchestration of technology, processes and people.

Response to a security incident will likely include multiple individuals and potentially multiple teams and even organizations. A critical component in the orchestration of people throughout the security process is enabling collaboration between individuals and teams. To function effectively, individuals and teams must function as a unified entity. Collaboration is discussed in greater detail in the Collaboration and Information Sharing section ahead.

For a SOAR solution to achieve its maximum potential, it must support the seamless orchestration of technology, processes and people.

Automation.

Although the concepts of orchestration and automation are closely related, the goals they seek to achieve are fundamentally different. While orchestration is intended to increase efficiency through increased coordination and decreased context switching to support faster, more informed decision making, automation is intended to reduce the time these processes take by automating repeatable processes and applying machine learning to appropriate tasks. Typically, automation is utilized to increase the efficiency of the orchestrated technologies, processes and people.

The key to successful automation is the identification of predictable, repeatable processes which require minimal human intervention to perform. Automation should act as a force multiplier for security teams, reducing the mundane actions that must be manually performed and allowing analysts to focus on those actions which require human intervention. Although some processes may be fully automated, a SOAR solution must also support automation which allows for human intervention at critical decision points. A common example is the automation of the enrichment of alert data, followed by a human decision to determine if containment of certain indicators or hosts is appropriate, followed by automated containment actions.

To provide maximum flexibility, automation should be capable of being implemented in numerous forms. Although lacking in flexibility, there are still many use cases for linear playbooks which follow a top-down flow. These linear playbooks are much easier to create and manage, and are appropriate when there are very few decisions which impact the way a process is performed. This often includes more detailed processes, such as static malware analysis or memory analysis. Full-featured orchestration and automation requires a greater level of flexibility than linear playbooks can provide. To support fully automated or semi-automated decision making, more flexible workflows or runbooks are required. Runbooks allow multi-path processes to be defined, enabling the automated, semi-automated or manual execution differing workflows depending on any number of conditions.

Over time, decisions which may not be codified into playbooks or runbooks will emerge. This most commonly includes which types of playbooks, runbooks or other actions are chosen based on any number of incident attributes. A SOAR solution should be capable of recognizing these decision patterns and automating the recommendation of playbooks, runbooks and actions for new incidents, based on the actions performed during previous incidents.

The key to successful automation is the identicication of predictable, repeatable processes, which require minimum human intervention to perform.

Measurement.

Measurement of security information is key for making informed tactical and strategic security decisions; a SOAR solution must support the measurement and display of security information to support both types of decisions. Information to support tactical decisions typically consists of incident data, targeted towards analysts and managers, which may include indicators of compromise, related events, assets, process status and threat intelligence. This tactical information enables informed decision making from incident triage and investigation, through containment and eradication.

Strategic information on the other hand is typically targeted towards managers and executives and is used to make informed high-level decisions. Strategic information may include incident trends and statistics, associated costs, threat intelligence and incident correlation. More advanced security programs may also use strategic information to enable proactive threat hunting.

Measurement of both tactical and strategic information is useless without proper display and visualization. A SOAR solution must support multiple methods for displaying and visualizing all information in an effective and easy to digest manner. This normally consists of different report generation mechanisms, as well as interactive dashboards.

Critical Components.

Orchestration, Automation and Measurement defines SOAR.

Orchestration, Automation and Measurement defines SOAR; however, not all SOAR solutions are created equal. To effectively solve today's complex security problems, there are certain critical components that all SOAR solutions should provide.

Customizability.

A SOAR solution must be flexible in its implemention, the data it collects and the way in which it integrates with other security tools.

No two security programs will be alike; this is especially true when you cross vertical lines. For a SOAR solution to be effective, it should be capable of being the single tool on top of the security stack. "one size fits all" approach to SOAR will leave customers with a solution that does not adequately address all their use cases, forcing customers to look to other tools to supplement the gaps.

A SOAR solution must be flexible in its implementation, the data it collects and the way in which it integrates with other security tools (discussed in more detail in the following section). A SOAR solution should be able to be implemented in a manner that is optimized for CSIRT teams, as well as SOCs, MSSPs and security teams. Data input from a multitude of sources, including machine to machine, email, user submissions and manual input should be supported. The importance of security metrics mean that customers should be able to customize not only the values available in the solution, but also what attributes are tracked as well. Higher customizability of the SOAR solution will result in greater ease of use and a better fit for the customer, as well as substantially increased ROI.

Flexible Integrations.

The number of security solutions, commercial, open source and developed in-house, means that any viable SOAR solution must be flexible enough to support a multitude of security products. Any SOAR solution will support many security products out of the box, however the likelihood that all the organization's security products will be supported by default is low. For that reason, it is crucial that a SOAR solution has a flexible solution in place that allows customers to easily create bidirectional integrations with security products which are not supported by default. The methods used to support this type of flexible integration may vary, but could include scripting languages such as Perl or Python, APIs or proprietary methods. Whatever the chosen method, it should be easy to implement and should not involve a steep learning curve on the part of the user.

Bidirectional integrations are crucial in supporting full automation and orchestration, however in some cases full bidirectional functionality may not be required by the customer. For some security products, it may only be necessary to support the ingestion data from the security product to the SOAR platform. These unidirectional integrations are generally much easier for the customer to create in cases where full bidirectional integration is not required. For this reason, a SOAR platform should support common methods of data ingestion, such as syslog, database connections, APIs, email and online forms, as well as common data standards such as CEF, OpenIOC and STIX/TAXII.

Incident Management.

Incident response is a complex process. Orchestration and automation of security products provides obvious value to any security program, but to maximize the time and monetary investment in a SOAR solution, a comprehensive SOAR solution should include additional features to manage the entire incident response lifecycle. This should include basic case management functionality, such as tracking cases, recording actions taken during the incident and providing reporting on critical metrics and KPIs.

However, a SOAR solution's incident management capabilities should not consist solely of case management functionality. To properly manage the entire incident response lifecycle, a SOAR solution should also provide the following incident management features:

- Phase and objective tracking
- Detailed task tracking, including assignment, time spent and status
- Asset management, tracking all physical and virtual assets involved in the incident
- Evidence and chain of custody management
- Indicator and sample tracking, correlation and sharing
- Document and report management
- Time and monetary effort tracking

A comprehensive SOAR solution should include additional features to manage the entire incident response lifecycle.

Process Workflows.

One of the key benefits to a SOAR solution is being able to automate and orchestrate process workflows to achieve force multiplication and reduce the burden of repetitive tasks on analysts. To achieve these benefits, a SOAR solution must be able to support flexible methods for implementing process workflows. As discussed in the previous Automation section, there are two fundamental ways to codify process workflows within a SOAR solution; typically, either classified as linear-style playbooks or flow controlled workflows or runbooks.

Because both methods have their own pros and cons and are each suitable for different use cases, both methods should be supported by a SOAR solution. In either case, the implementation of these workflows must be flexible enough to support almost any process which may need to be codified within the solution. Workflows should support the use of both built-in and custom integrations, as well as the creation of manual tasks to be completed by an analyst. Flow controlled workflows should support multiple types of flow control mechanisms, including those which allow for an analyst to make a manual decision before the workflow continues. Allowing control to be passed between the automation engine and an analyst allows for a much greater level of flexibility and enables the automation to continue beyond the first point at which a human decision is required.

Building workflows should not require a high level of scripting or programming knowledge. Because workflows are at the heart of the automation and orchestration activities of a SOAR solution, great attention should be paid to both the flexibility and ease of use. Workflows which are difficult to build or complex to understand by a wide range of users will cause confusion and sub-optimal performance during an incident.

A SOAR solution must be able to support flexible methods for implementing process workflows.

Threat Intelligence.

To provide true value, a SOAR solution must go beyond simply gathering threat intelligence.

Actionable threat intelligence is a critical component in effective and efficient incident response. While simple threat intelligence feeds still provide some value and should be supported by a SOAR solution, to be truly effective in today's threat landscape, threat intelligence must go above and beyond simple feeds. As discussed in the previous section, tracking of indicators and samples, such as IP addresses, URLs, malware samples, and TTPs is a critical component of incident management. However, to become actionable threat intelligence, these indicators must be surrounded with further context. Because a SOAR solution has access to not only the indicators, but also the rest of the incident information which can provide the additional context, it is in a unique position to gather actionable threat intelligence.

To provide true value, a SOAR solution must go beyond simply gathering threat intelligence. A proactive security program requires threat intelligence to be properly correlated to discover attack patterns, potential vulnerabilities and other ongoing risks to the organization. This correlation should be done automatically and it should be immediately clear if an ongoing incident may share common factors with any previous incidents.

Although automated correlation is critical for analysts to make informed decision during the incident response process, visual correlation is also an important factor when assessing threat intelligence capabilities. Many proactive security programs now include various forms of threat hunting; actively looking for attacks and patterns that may not have been detected through automated methods. To facilitate this process, threat intelligence and correlated events should be able to be displayed in an easy to understand visual manner to allow analysts to most effectively analyze the information.

Collaboration and Information Sharing.

To be effective in a team environment, a SOAR solution must support seamless collaboration and information sharing between team members in a controlled manner.

Incident response is not a one player sport. Response to a security incident will likely include multiple individuals and potentially multiple teams and even organizations. To be effective in a team environment, a SOAR solution must support seamless collaboration and information sharing between team members in a controlled manner. Those with authorization should be able to have instant access to the status of the incident they are collaborating on, as well as any information gathered and other actions performed by team members. Team members should also have the ability to communicate securely within the SOAR platform, providing an out-of-band communication mechanism when other mediums may not be trusted.

Collaboration and information sharing must also be possible outside of the organization itself. This is especially true in the context of threat intelligence. Open sharing of threat intelligence, when possible, it a critical tool in fighting cybercrime. There are numerous avenues available to share threat intelligence, open, closed and industry specific. The majority of these threat intelligence sharing programs utilize one of the open standards for threat intelligence, such as STIX/TAXII, OpenIOC or MISP. A SOAR solution should support both the ingestion and sharing of threat intelligence information via these common standards in a controlled and secure manner.

Multitenancy.

Many large enterprises have multiple internal security teams performing unique sets of tasks. In some instances, it may not be appropriate for some internal teams to have access to the data collected by other internal teams. MSSPs are also beginning to turn to SOAR solutions as a force multiplier, and require very strict segregation of customer data.

In either case, it is not cost effective to deploy an individual SOAR solution for each team or customer. A SOAR solution must be capable of supporting multiple instances on a single host, providing accurate data segregation and access controls for each tenant's information.

To be effective in a team environment, a SOAR solution must support seamless collaboration and information sharing between team members in a controlled manner.

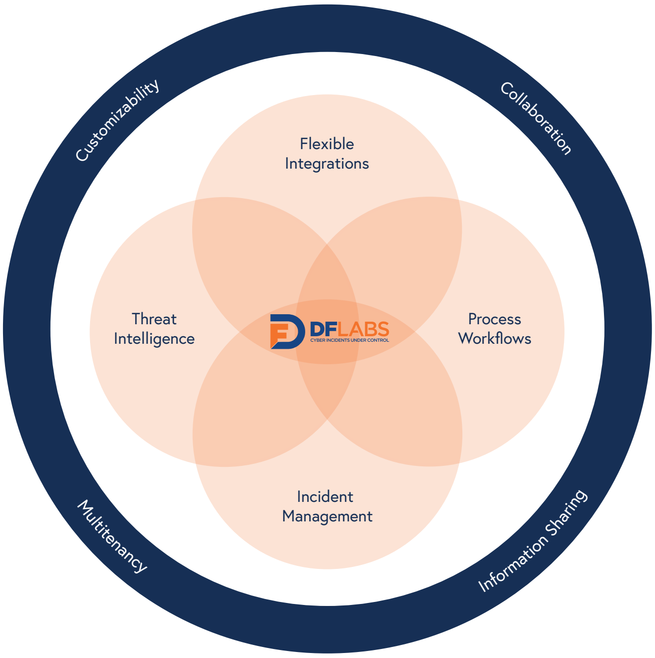


Figure 2. Components of a Comprehensive SOAR Solution.

What SOAR is Not.

Perhaps equally important is to understand what a SOAR solution is not. First and foremost, a SOAR solution is not intended to be a replacement for skilled analysts. Deploying a SOAR solution with the intended goal of replacing analysts will inevitably create more risk than it mitigates. Instead, a SOAR solution should be viewed as an enabler for the security program and the security analysts alike. As mentioned previously, a SOAR solution should be viewed as a force multiplier for security analysts, allowing them to work smarter and provide increased value to the organization.

A SOAR solution is also not the same as a SIEM. While at first glance, SOAR and SIEM may appear to solve the same problems, their approaches to solving these problems have several fundamental differences which have resulted in very different use cases. At its core, a SIEM was designed to collect, correlate and store security events and generate appropriate security alerts. Since its inception, SIEM functionality has evolved to include various levels of threat intelligence which allow the more accurate generation of security alerts as well as basic enrichment of previously generated alerts.

A SOAR solution should be viewed as an enabler for the security program and the security analysts alike.

Following alert generation and perhaps basic enrichment, incident response has remained a largely manual process in SIEM-only environments. Using the SANS PICERL Incident Response Framework (Planning, Identification, Containment, Eradication, Recovery and Lessons Learned), a SIEM falls squarely in the Identification Phase.

SOAR solutions, on the other hand, are not designed to ingested large volumes of raw events. Instead, SOAR solutions are designed to pick up the incident response process where SIEM functionality ends; providing an automated and orchestrated response throughout the Identification Phase, as well as the Containment, Eradication and Recovery Phases. Some SOAR solutions, such as IncMan from DFLabs, also enable the Planning and Recovery Phases through features such as knowledge bases, key performance indicators and advanced reporting. In fact, although a SOAR solution does not require a SIEM to function properly, SOAR and SIEM are complementary solutions. Each provides a unique set of values to the organization which are extremely powerful when combined as part of a holistic security program.

SOAR Use Cases.

Use cases for SOAR will vary depending on the environment and are limited only by the creativity of the organization. The following are several common use cases for SOAR solutions.

Phishing.

Phishing emails have become one of the most critical issues faced by organizations over the past several years. Some of the most recent high-profile data breaches have resulted from carefully crafted phishing emails. SOAR is perfectly positioned to enable automatic triage and examination of suspected phishing emails by extracting artifacts from the email, then performing additional enrichment on these artifacts and if necessary, containing the malicious email and any malicious payloads.

Suspicious emails may be received via any one of the numerous email scanning solutions available today, or via a monitored email address provided to end users to submit suspicious emails to. Once the email is received, SOAR can extract artifacts, such as header information, email addresses, URLs and even attachments. What happens next will largely depend on the organizations individual technology integrations. Extracted information may be submitted to various threat reputation and intelligence services, SIEM, EDR or network appliance logs may be queried, and attachments may be detonated in a sandbox. Once the available information has been enriched, if determined to be malicious, automated or semi-automated containment actions may be taken, such as quarantining or deleting the phishing email, searching for and deleting other instance of the phishing email in other user's accounts, blocking IP addresses or URLs, banning executables from running or quarantining the user's workstation.

Regardless of the integrations used, utilizing SOAR to examine and respond to phishing emails can reduce the time to investigate these pervasive threats from hours to minutes, automatically containing the attack and minimizing risk to the organization.

Some of the most recent high-profile data breaches have resulted from carefully crafted phishing emails.

Malicious Network Traffic.

Alerts regarding potentially malicious traffic are common-place, and often sit in the queue for some time before they are investigated.

The influx of detection technologies means that organizations are facing a constant barrage of alerts. Many of these alerts are generated due to traffic that one detection technology or another has deemed to be potentially malicious. This is usually based on some type of threat indicator, which may or may not be reliable. It is often left up to the organization to further triage and investigate each of these alerts to determine if they are a false positive or an actual potential security event.

Alerts regarding malicious traffic may be received by a SOAR directly, or after being ingested and forwarded by a SIEM. In either case, the advantage of using a SOAR to automate and orchestrate actions surrounding these types of events comes from the automatic enrichment, as well as potential containment of the detected indicators. Under normal circumstances, analysts would use whatever data enrichment tools are available, such as threat intelligence, reputation services, IT asset inventories and tools such as nslookup and whois. Analysts would then determine if the indicators appeared to be malicious, at which point containment and further investigation would begin. Using SOAR, it is simple to codify a process such as this into an automated workflow, automatically performing data enrichment as soon as the alert is received. SOAR can also automate the process of searching for additional instances of the same indicator across the organization, alerting analysts to any additionally detected occurrences. Automated or semi-automated containment is also possible; for example, blocking an IP address or URL via the firewall or proxy, or isolating a host pending further investigation.

Alerts regarding potentially malicious traffic are common-place, and often sit in the queue for some time before they are investigated. While most are false positives or low priority, any one of these could be the only indicator of a potentially serious data breach. SOAR allows immediate triage and response to each of these alerts almost instantaneously, automating the mundane, repeatable processes while allowing analysts to focus on the most significant alerts.

Vulnerability Management.

A SOAR solution can be used to ensure that the security team is made aware of any new vulnerabilities within the organization.

SOAR was not intended to be a vulnerability management platform and will never replace the robust vulnerability management systems available today. However, there are some aspects of a good vulnerability management program that a SOAR platform can streamline. In larger enterprises, vulnerability management is often a task performed outside the security team. This can lead to potential risk as the security team may not be aware of vulnerabilities that exist within the infrastructure.

A SOAR solution can be used to ensure that the security team is made aware of any new vulnerabilities within the organization. This allows the security team to proactively examine the vulnerable host, when appropriate, to ensure that there is no evidence of exploitation, place any appropriate additional safeguards in place, and subject the host to increased monitoring until the vulnerability has been mitigated.

Beyond notifying the security team, a SOAR solution may also be used to further enrich vulnerability and host information. For example, a SOAR solution could be used to query a database of vulnerabilities to gather additional information on the vulnerability, query Active Directory or CMDB for asset information, or query a SIEM or EDR for events. Based on vulnerability, host or event information, the case could be automatically upgraded or reassigned, or the host could even be temporarily isolated until appropriate mitigation tasks could be performed.

While suitable testing and deployment of patches are critical in an enterprise environment, existing vulnerabilities present an ongoing risk to the organization. It is crucial that the security team are aware of these risks and take the proper steps to ensure that the vulnerability has not and will not be exploited until it can be properly addressed. A SOAR solution can be utilized to ensure that the security team remains informed of all current vulnerabilities and can efficiently evaluate the possible risk of each vulnerability in order to take proper risk mitigation actions.

SOAR for MSSPs.

MSSPs face many of the same issues as CSIRTs and SOCs, but on a much larger scale. In addition to these shared challenges, MSSPs also face some unique issues which SOAR can address. MSSPs must work within the confines of strict service level agreements (SLAs). Failing to meet these SLAs could result in loss of business, loss of reputation and even the potential for legal action. Automating and orchestrating actions with a SOAR solution allows MSSPs to work more efficiently, ensuring that all SLAs are met. In addition, MSSPs are constantly under pressure to prove to customers that these SLAs are being met, that they are taking appropriate, timely actions and that they are continuing to provide value to their customers. The advanced metrics and audit logs of a SOAR addresses these needs by providing a robust set of metrics suitable for both analysts and executives alike.

MSSPs must also find a method to manage each customers data securely and in a segregated manner. At the same time, MSSPs must also ensure that each customer is provided access to their data to ensure transparency and to allow seamless teamwork between the MSSP and the customer's internal teams. SOAR accomplishes these tasks by providing individual tenants for each customer, physically segregating each customers data to ensure confidentiality, while allowing the MSSP access across customer tenants for ease of use.

Automating and orchestrating actions with a SOAR solution allows MSSPs to work more efficiently, ensuring that all SLAs are met.

DFLABS.COM

Case Management.

Although not strictly an orchestration and automation function, case management is an important part of the incident response process, and is another function that SOAR can help streamline. Many organizations struggle with managing the vast amounts of disparate information that is gathered during a security incident. Spreadsheets and shared documents are simply not sufficient for managing a complex incident.

Not only does SOAR maintain all information and enriched data gathered from automated and orchestrated activities, it also maintains a detailed audit log of all actions taken during the response. A full featured SOAR should also allow for detailed task management, allowing incident managers to create, assign and monitor tasks assigned to all analysts taking part in the response. In addition, a full featured SOAR should also allow users to track assets involved in the incident and maintain a detailed chain of custody for all physical and logical evidence.

A SOAR with full case management functionality will help ensure the smooth and efficient handling of an incident from identification through remediation, providing responders will the information they need right at their fingertips and allowing them to focus on the task at hand.

Many organizations struggle with managing the vast amounts of disparate information that is gathered during a security incident.

Selecting a SOAR Solution.

There are numerous SOAR solutions on the market today. While each solution fundamentally seeks to solve the same set of problems, approaches and functionality varies from vendor to vendor. When selecting a SOAR solution, it is critical to begin by identifying the gaps in the current security program you are trying to solve. Are you trying to better orchestrate and automate your disparate security technologies? Are you trying to better define your security workflow? Are you seeking a solution which provides better incident management capabilities?

Once the core target problems have been documented, identify the processes which will be performed by the SOAR solution. Categorize these processes as either must-support or nice to support. When evaluating SOAR solutions, it will be critical to ensure that it is possible to perform each process in the desired manner. Finally, identify any integrations with existing tools and technologies that may be needed; again, categorize these integrations requirements as either must-have or nice to have.

Assess each SOAR solution based on the problems you are trying to solve, the ability to implement your desired processes and the capacity to support your required integrations. Keep in mind that assessing technology integrations may not be as straight forward as it appears. Some SOAR solutions may not support a certain technology out of the box, however it may be very easy for the integration to be added by the vendor or through the vendor's custom scripting or integration engine. On the flip side, just because a technology is supported does not mean that the specific functions desired are supported. For example, Microsoft Exchange Web Services may be supported, however quarantining of emails may not be supported.

A SOAR solution should increase the effectiveness and efficiency of the overall security program. ROI should be a key factor when evaluating SOAR solutions. Keep in mind that the focus of automation should be on supporting people and processes and force multiplication, not replacing analysts.

About Us.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting & investigation and threat containment.

IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide.

The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information, visit our website www.dflabs.com or connect with us on Twitter @DFLabs.

ACADIA TECHNOLOGY GROUP

DFLABS
CYBER INCIDENTS UNDER CONTROL

DFLABS.COM

HEAD OFFICE

DFLabs S.p.A
Address: Via Pietro Donati, 16
26013 Crema (CR), Italy

T – +39 0373 82416

E – info@dflabs.com

SALES

ITALY
Via Bergognone, 31
20144, Milan

T – +39 0373 82416

UNITED KINGDOM
1 Primrose Street
London, EC2A 2EX

T – +44 203 286 4193

UNITED STATES
200 Portland Street
Boston, 02114

T – +1 201 579 0893

E – sales@dflabs.com

CUSTOMER SUPPORT

T – +39 0373 82416

E – support@dflabs.com

Automate.
Orchestrate.
Measure.