WHITE PAPER

How To Leverage Your Existing SIEM Tool With SOAR Technology.

Fuse intelligence, reduce time to incident resolution and increase ROI on existing security operations tools.

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.

DFLABS.COM

Automate.
Orchestrate.
Measure.

ACADIA TECHNOLOGY GROUP

DFLABS
CYBER INCIDENTS UNDER CONTROL

Introduction.

With a vast range of security technologies, tools and platforms now widely available in the market for security teams, it is ever more complex to decide which tools are best to deploy in order to suitably defend the organization's infrastructure against the increasing array and veracity of cyber security threats they are currently faced with in today's ever-growing threat landscape. With factors such as constricted budgets, lack of resources and legal and regulatory compliance to take into consideration, as well as security operations performance and return on investment of tools and resources, a well-defined security strategy and structure is required.

Depending on the size and maturity level of the security program in question may to some degree determine its structure and the levels and range of technologies used, but it is generally common practice to have a security information and event management (SIEM) tool in place, alongside or sitting on top of several other systems. These other systems may include an intrusion prevention system (IPS), database activity monitoring (DAM), web application firewall (WAF), data loss prevention (DLP) and vulnerability assessment system (VAS) for example. So why, when and how should a security team be looking to implement a Security Orchestration, Automation and Response (SOAR) solution on top of its existing SIEM infrastructure, to further manage its security operations and incident response processes and tasks?

The aim of this whitepaper is to ultimately answer these questions. We will firstly define what a SIEM and a SOAR solution is, discussing the differences between the two. We will go on to cover why security operations teams should consider implementing a SOAR solution with a SIEM, including the benefits, when to utilize and more importantly, how to implement successfully.

It is ever more complex to decide which tools are best to deploy in order to suitably defend the organization's infrastructure.

What is SIEM?

Security information and event management (SIEM) is an approach to security management that combines information and event management functions into one security management system, to provide a holistic view of an organization's information technology security. The main principle of a SIEM is to act as a security monitoring system to collate relevant data from multiple sources, such as applications and network hardware to provide real-time analysis and identify deviations from the norm. If an anomaly is detected the SIEM will generate an alert for the security team to investigate. A SIEM is typically renowned for generating a high number of alerts, including many that are found to be "false positives" after additional investigation. At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries, while advanced SIEMs have evolved to include user and entity behavior analytics (UEBA) and some orchestration and automation capabilities.

What is SOAR?

Security orchestration, automation and response (SOAR), terminology adopted by Gartner, is an approach to security operations and incident response used today to improve security operations efficiency, efficacy and consistency. Gartner defines SOAR as technologies that enable organizations to collect security data and alerts from different sources. SOAR allows incident analysis, triage, to be performed leveraging a combination of human and machine power. This helps to define, prioritize and drive standardized incident response activities to a standard workflow. *

The increasing complexity of IT, evolving threats and the need to coordinate multiple security products gave rise to SOAR technology and it is commonly deployed by security operations centers (SOCs), computer security incident response teams (CSIRTs) and managed security service providers (MSSPs).

Acting as a force multiplier, it allows security teams to do more with less resources, while providing features to automate, orchestration and measure the full incident response lifecycle, including detection, security incident qualification, triage and escalation, enrichment, containment and remediation. The key factor of SOAR technology, such as the IncMan SOAR solution from DFLabs, is to reduce the time from breach discovery to resolution, minimize the risk resulting from security incidents, while increasing the return on investment for existing security technologies.

*Gartner Technical Paper, Preparing Your Security Operations for Orchestration and Automation Tools, February 2018.

The key factor of SOAR technology, such as the IncMan SOAR solution from DFLabs, is to reduce the time from breach discovery to resolution.

How Does a SOAR Solution Differ from a SIEM?

In simple terms, a SIEM collates and analyzes the information generated from various sources, identifying issues and raising the initial security alerts. Alert triage is then often carried out by security analysts in a very manual and non-methodical way and subject to mistakes and errors due to the sheer volumes and number of repetitive and mundane actions required, often not being able to fulfil all of them. One of the original core drivers for SIEM technology was to ingest and process large volumes of security events; a function which SIEMs continue to excel at today. However, although some advanced SIEMs have incorporated additional features, such as integration with threat intelligence and other third-party solutions, many SIEMs are still largely focused on data ingestion and presentation.

Another fundamental limitation of many SIEM solutions is that the communication between the SIEM and other third-party products is unidirectional. SIEMs were designed to ingest information, however support for two-way communication with third-party tools is often limited at best. In most cases, this severely limits a SIEM's ability to carry out actions beyond the initial alert; this is where a SOAR solution can add significant additional value.

A SOAR solution is often used in conjunction with a SIEM as opposed to being used independently as a standalone tool; however, a SOAR solution is not dependent on having a SIEM in place. A SOAR solution is not intended to be a SIEM replacement; instead, when used in conjunction with a SIEM it is intended to be utilized to help security teams automate and orchestrate actions across their entire portfolio of security products in a bidirectional manner to reduce analyst workload, alert fatigue, time to respond and remediate and reduce overall risk.

Sitting on top of the SIEM, the SOAR solution would orchestrate and automate multiple third-party tools from different vendors, whereas the SIEM would be used to collate and analyze data and generate the alert, which is just the first step of a multistep process. SOAR technology would then be leveraged once the initial security threat had been detected and the security alert generated by the SIEM.

Once an alert was generated via the SIEM, an incident would be triggered within the SOAR solution. Taking the alert to the next stage of the response process, it would combine automation and human interaction to carry out a number of enrichment and response actions. A set of activities based on previously defined incident workflows, combined with machine learning to recommend actions based on previously observed incidents, can be used to automate and guide the entire response process. For example, a specific set of playbooks and runbooks for incident types such as phishing or ransomware, used to enrich data, containing the threat and remediating the incident.

When to Consider Implementing a SOAR Solution.

The amount of security events that cybersecurity professionals deal with on a day to day basis can be overwhelming and analysts often have to delve through a deluge of data to find what they are looking for, ultimately preventing them from tackling incidents more efficiently. SIEM tools collect large amounts of information from different areas of the IT framework, but too much information sometimes is just as crippling as not enough information.

A SIEM used in isolation helps to centralize information gathered from various other security tools being used, but it can often lead to an overwhelming amount of information, that then needs to be filtered and correlated to eliminate the false positives to leave only the critical events that need to be acted upon. It can produce a vast quantity of security alerts, leaving security analysts inundated, not knowing which alerts should take priority and be tackled first. This will have a negative impact on the security team, with what is already considered a scarce resource.

The overwhelming number of alerts means that analysts are not able to effectively and efficiently manually respond to and manage each alert and this frequently results in a vast majority of alerts not being properly investigated and verified. As we all know, it only takes that one alert to slip through the net for a serious incident to start to take shape, potentially having a detrimental effect on the organization. Most security teams do not realize the sheer number of alerts that will be received and the resulting alert fatigue, until they have deployed a SIEM and a full advanced threat detection architecture. There is a common misconception that a SIEM will reduce the number of incoming alerts by applying correlation rules. However, this is not always the case and correlation rules may only reduce a small percentage of the total number of alerts.

When considering the need for implementing a SOAR solution, it is key for the security team manager and/or CISO to carry out a thorough analysis of the current day to day and overall performance of the security team. E.g. How many security alerts are being generated? How many are legitimate alerts and not "false positives"? How long does it take to detect and respond to a security alert? How many other security tools are in place and must be used when investigating alerts? How many security alerts are passing by the wayside and not being actioned? What is the mean time to resolution? How many resources/security analysts do you currently have? Is the existing resource at their maximum capacity and effectiveness threshold? etc. Once these questions have been answered and figures are identified, analyzed and compared against set predefined security operations and incident response goals and best practices, it should be much clearer to see the results indicating if there is a business need for implementing a SOAR solution to help reduce alert fatigue, orchestrate the organization's different security tools and automate menial tasks.

In most instances, the security team is not performing at maximum efficiency and the existing resources are not being utilized to the best of their abilities and skill set. With the increasing number of cyber security threats, security teams are commonly overloaded with security alerts and overworked with mundane and repetitive tasks making them ineffective and inefficient. This can also result in security teams not following standardized processes and procedures as they try to handle events as quickly as possible, resulting in a lack of knowledge transfer for dealing with future alerts. If this is the case, then the organization can only benefit from implementing a SOAR solution within its infrastructure.

The overwhelming number of alerts means that analysts are not able to effectively and efficiently manually respond to and manage each alert.

The Benefits of Implementing a SOAR Solution with a SIEM.

Integrating a SIEM with a SOAR solution combines the power of each to create a more robust, efficient and responsive security program. Taking advantage of the SIEM's ability to ingest large volumes of data and generate alerts, the SOAR solution can be layered on top of the SIEM to manage the incident response process to each alert, automating and orchestrating a number of mundane and repetitive tasks that would take many manual man hours to complete.

SOAR solutions, such as IncMan SOAR from DFLabs, support SIEM integrations and present a comprehensive solution for all organizations that are trying to create a successful and affordable security program, by effectively reducing the noise generated by a high number of alerts and sometimes less than reliable threat intelligence. This can ultimately enable security teams to minimize incident resolution time, maximize analyst efficiency and overall increase handled incidents. By utilizing a SOAR solution to take away some of this unnecessary burden, security analysts can become more proactive, as opposed to always being reactive. They can restructure their workloads to use their time more wisely to undertake activities such as threat hunting, to be one step ahead of the potential alert before it has even been triggered.

The combined power of a SOAR solution working alongside a SIEM is crucial to ensure that alerts do not go untouched or ignored. More importantly, it ensures all alerts are dealt with in a timely manner and are acted upon following a standard set of consistent and repeatable practices and procedures. This factor will become more essential with regulations such as GDPR, amongst others, in order to meet incident notification and breach reporting requirements.

The SOAR solution will automate the opening of incident tickets when security alerts occur, and with the help of playbooks and runbooks, will trigger the appropriate steps to conduct some of the trivial validations to ensure that enrichment of the incident information happens automatically and accurately, enhancing the time to remediation. Containment or remediation options are also available through a SOAR solution and can be automatically triggered and orchestrated as needed. Depending on the specific organization and security requirements, a SOAR solution allows decision makers to pre-determine the proper balance of automated and human actions to be carried out for each incident.

The SOAR solution will automate the opening of incident tickets when security alerts occur.

How to Build an Integrated SIEM and SOAR Workflow?

To fully utilize the functionality of a SIEM and a SOAR solution combined, it is important to build integrated workflows that help make incident detection, response and remediation more effective and efficient for security teams. These workflows should focus on utilizing the strengths of each solution to their fullest potential, maximizing the effectiveness of the combination of the two solutions.

Due to the volume of data that a SIEM is designed to ingest, as well as the correlation ability of most SIEMs, it often makes sense to continue to collect raw logs via the SIEM. The SIEM will be responsible for aggregating and storing the raw logs for the appropriate amount of time, as well as correlating similar logs and events. Once all third-party applications are configured to forward logs to the SIEM, it will be up to the SIEM administrators to properly tune the SIEM and determine which events should be investigated and therefore should be forwarded to the SOAR solution. The tuning process will likely take some time to ensure that the proper events are being escalated to the SOAR solution and that a limited number of spurious events are sent.

Passing events from the SIEM to the SOAR solution can be accomplished in several different ways. Most often, the simplest solution is to utilize syslog to push the events from the SIEM to the SOAR solution, since both solutions should easily support syslog. Utilizing syslog to forward events from the SIEM will require that rules be configured on the SIEM to forward only the necessary events. It will also require that parsing rules be configured within the SOAR solution to properly parse the information from the syslog messages in to a usable format.

Most SOAR solutions, including IncMan, also offer purpose-built integrations with the most common SIEM products. There are several advantages to utilizing a purpose-built integration over syslog. Most SOAR-SIEM integrations allow the SOAR solution to pull data from the SIEM based on one or more customizable queries; this may provide a greater level of flexibility in determining what events are passed to the SOAR solution than forwarding events via syslog will permit. Because these integrations are purpose-built for the individual SIEM, utilizing a SOAR-SIEM integration will likely also reduce the amount of parsing rules which must be defined in the SOAR solution when compared to forwarding events via syslog.

Once the appropriate events are being escalated to the SOAR solution, the final step is to define suitable workflows for investigating different event types within the SOAR solution. From this point on, the event should be handled from within the SOAR solution. Integrations between the SOAR solution and the SIEM should permit the querying of additional data from the SIEM, as well as any other security products in the environment.

The process of defining the workflows within the SOAR solution will vary depending on the maturity of the organization's existing security workflows. If detailed process workflows for common event types already exist, this may be a very straightforward process of simply codifying these processes within the SOAR solution. If such detailed process workflows do not already exist, the first step will be to determine what the proper workflows should be. This will likely involve speaking with management, as well as analysts to determine what the current undocumented processes are for each event type. These processes should first be documented and refined on paper, then codified into the SOAR solution. As with any other product, there should be a period of evaluation and tuning to ensure that the workflows are achieving the desired results.

Most SOAR solutions, including IncMan, also offer purpose-built integrations with the most common SIEM products.

Final Thoughts.

A SIEM is a crucial tool within any security infrastructure, amongst other tools. However, it is critical to keep in mind what a SIEM is designed to achieve, and what gaps may still exist within the security program. The combination of a SIEM and a SOAR solution can transform the security operations and incident response capability and take it from one level to the next, in an intelligent and predetermined manner.

It uses a shared trigger point to move the detected threat in the form of a security alert from the SIEM to generate the start of an incident within the SOAR solution, to modernize and streamline the incident response process to facilitate automation and orchestration, accelerating response capabilities. The SOAR solution acts as a force multiplier for the security team, enabling it to do more with less resource, freeing up valuable analyst time from the overwhelming amounts of data, mundane and repetitive tasks. It allows the security team to become more efficient and effective, and most importantly proactive, while reducing alert fatigue.

Adopting this structure will inevitably minimize the time from threat discovery to resolution, increase the return on investment of existing security technologies and solutions, reduce the risk resulting from security incidents, while meeting legal and regulatory compliance. Overall it adds enormous amounts of value to an existing security program.

Automate.
Orchestrate.
Measure.

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

CONTACT US:

BOSTON - UNITED STATES
150 State Street
Boston, 02109
T – +1 201 579 0893
E – sales@dflabs.com

LONDON - UNITED KINGDOM
1 Primrose Street
London, EC2A 2EX
T – +44 203 286 4193
E – sales@dflabs.com

MILAN - ITALY
Via Bergognone, 31
20144, Milan
T – +39 0373 82416
E – sales@dflabs.com

CUSTOMER SUPPORT:

T – +39 0373 82416
E – support@dflabs.com

Automate.
Orchestrate.
Measure.

DFLABS.COM