ORCHESTRATION AND AUTOMATION OF SECURITY MANAGEMENT SYSTEMS

BY

Pankaj Khemani
IMT2018054

INTRODUCTION

Security Management Orchestration(SMO) is a strategy for merging diverse security systems and integrating security technologies. It's the connected layer that supports security automation and streamlines security processes.

SMO tools help us in creating behaviors that continuously improve security and include,

- Real-time updates
- Reduced effort, deduplication
- Integrated security program modules
- Comprehensive security management functions in one tool.

WHY IS SECURITY ORCHESTRATION AND AUTOMATION NEEDED?

The most effective security operation centers (SOCs) are based on efficiency and response time. It is really difficult to integrate security systems, tools, and teams in a way that simplifies detection, reaction, and repair. Cobbling together warning details to assess if a security incident is a true threat, as well as correlating data and coordinating the necessary reaction, is one of the most time-consuming duties of all. As a result, security instruments must be connected, security processes must be efficient, and the sector must begin to collaborate. Security teams need a method to become more nimble as new technologies emerge every day. (IoT, BOYD, and ongoing virtualization of everything)

Security orchestration and automation can help here. By no means is orchestration a novel term. DevOps orchestration, which aims to automate infrastructure deployments and document 'infrastructure as code’, is certainly familiar to us. So, it's now time to apply this knowledge to security procedures.

Given the massive amount of data generated by today's security systems, it's no surprise that SOCs are suffering from alert fatigue and, as a result, are missing intrusions. By combining existing tools and procedures into a repeatable, automatable workflow, SOCs can coordinate the flow of data and duties (for example, monitoring SIEM warnings). A security orchestration solution integrates your systems, tools, and processes, allowing you to automate as needed and maximize the value of your people, processes, and technologies. Furthermore, SOCs can eliminate slow, manual processes in favor of contextual decision-making and quick reactions. After all, security professionals should be using their knowledge to respond to events swiftly and effectively, not wasting time on time-consuming, manual chores.

Automating security operations and processes is no longer a “nice to have”, it’s a “need to have”. Manually managing many security tools and processes has grown increasingly difficult, also not to mention inefficient and prone to human error.

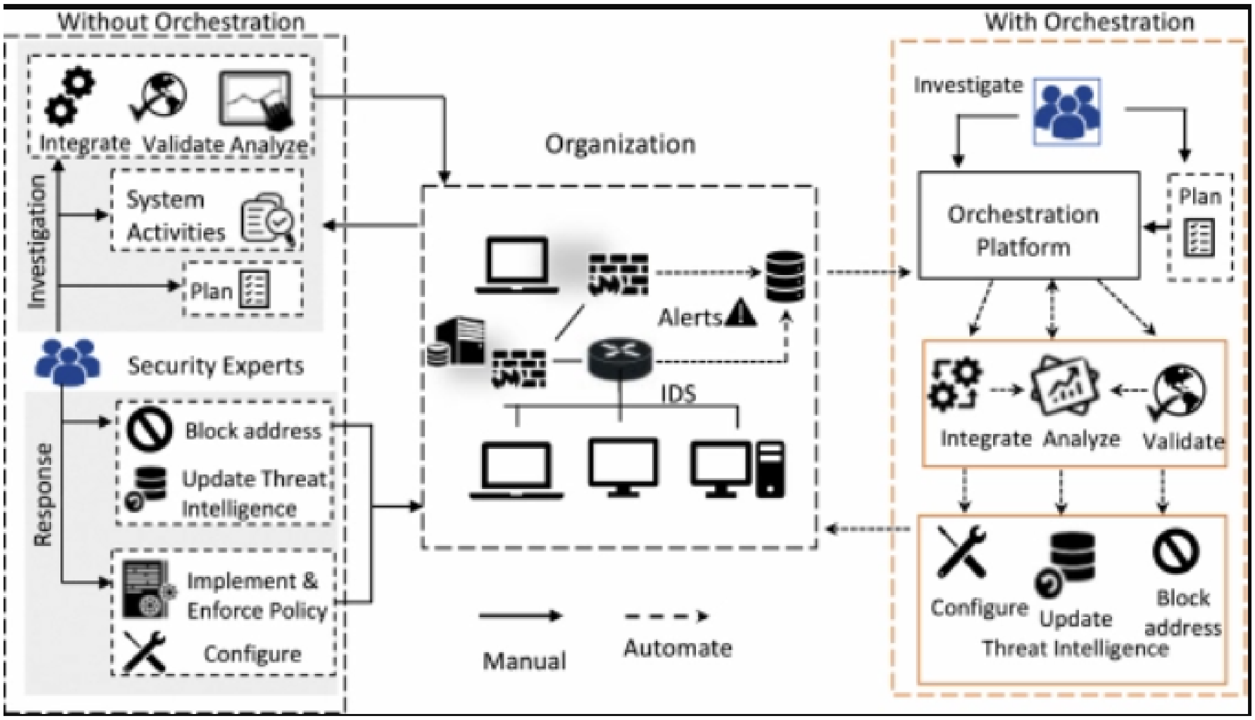
AN EXAMPLE TO EXPLAIN THE NEED FOR SECURITY ORCHESTRATION AND AUTOMATION

Common risks like phishing emails, for example, take a long time to investigate manually, which leaves room for human error. By moving from system to system to test email content, security analysts and incident responders must look for malicious attachments, phishing URLs, or strange requests for sensitive information. The time and effort required to manually retrieve that information is considerable.
It's also impractical to expect a modern security team to work with a "single solution" or technology for all of their tasks. A CISO can no longer just purchase 'Trusted Security Vendor X' and tick off a compliance box. Security teams are increasingly being held accountable for missed breaches, therefore they hunt for 'best of class' tools to protect against the dangers that threaten their companies. Using a wide range of vendors, on the other hand,

adds complexity to security teams, which can be tough to manage.

The good news is that security orchestration can automate and perform these basic investigative procedures with significantly greater precision, freeing up time for human insight and response. It can also help CISOs make better use of their security budget: by orchestrating the integration of security products, security teams can still acquire the "best of breed" in protection while remaining productive.

HOW CAN ORGANIZATIONS IMPLEMENT SECURITY ORCHESTRATION AND AUTOMATION IN VERY SIMPLE AND EFFECTIVE STEPS?



Step 1: Automate repetitive assessment and remediation tasks:-

As a result, man hours are saved. Rather than bi-weekly patching, system upgrades, or generating arbitrary reports, time is spent identifying and fixing higher-level threats. Organizations see immediate benefits in terms of work efficiency and, eventually, more effective protection.

SIEM solutions that provide real-time security alert analysis become more effective, allowing for the automation of some post-alert inquiries, rather than the present technique of immediately assigning them to human analysts for additional examination.

According to Gartner's Preparing Your Security Operations for Orchestration and Automation Tools report: "SIEM tools are… limited in their ability to query additional data sources and verification services after an initial set of conditions is met. The usual approach is to do as much as possible with that set of conditions and then provide the alert to an analyst for triage, where those additional queries take place."

"The ability to automate post-alert queries, such as submitting indicators of compromise (IOCs) to IT services or even artifacts to external sandboxes, allows organizations to implement more threat detection use cases with a high number of initial alerts….The automated triage by SOAR effectively acts as the remaining stages of the multistage detection process."

Step 2: Implement an incident assessment and response workflow:-

The processes that go into alert triage, assessment, and reaction are usually documented as part of operational management or to meet regulatory needs. While these might be considered processes, they are most typically utilized as a reference for security analysts.

It's an ineffective use of useful data in a world where threats and breaches multiply on a regular basis. According to Gartner's SOAR report: "…Most of them will quickly realize that a system capable of recording the data in a structured format, usually while controlling the process workflow, is required to handle the increasing volume and complexity [of alerts]."

Security orchestration is a method of elevating these tools to a more central zone. As said in the SOAR report: "The process workflow documented in the tool is no longer used only as guidance to the analysts. O&A system moves these tools to an active role in performing tasks of those processes, and occasionally the entire end-to-end process."

Step 3: Integrate internal and external threat intelligence resources:-

Our goal is to improve the quality of our security alerts to the point where we can spot problems from a mile away. So, the usage of high-quality, comprehensive threat intelligence resources is then critical.

Internally, we have historical data that can help us identify risky activities and mobilize our team to respond quickly and with minimal damage.

We can get danger and security risk information from numerous publicly available sources. For example, the US-Cert reports include network-based indicators and selected contextual data. This knowledge was critical in detecting c2 nodes, which are indicators of malware in systems. There are also DHS/FBI,.gov, and commercial threat bulletins, to name a few.

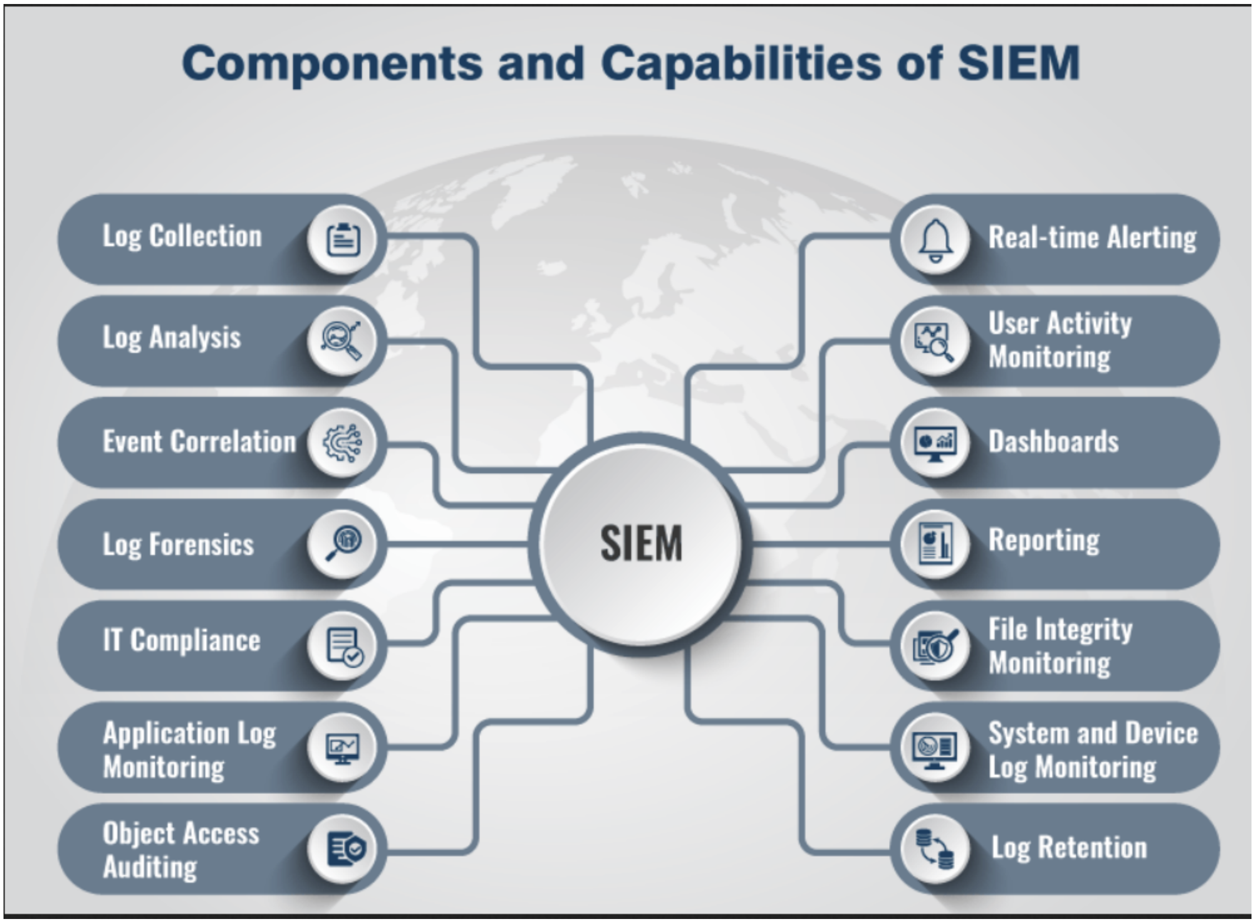
Step 4: Monitor, assess, and repeat:-

It's unlikely that we'll be able to acquire the best security orchestration calibration straight away. It takes some time and a couple of missed calls/alerts. Keep an eye on the system and identify areas for improvement. Repeat and correct where necessary.

Remember the OODA (observe, orient, determine, and act) loop, which was designed by US Air Force Colonel John Boyd as a decision-cycle approach. When it comes to security orchestration, it allows you to be more nimble and responsive to risks and difficulties.

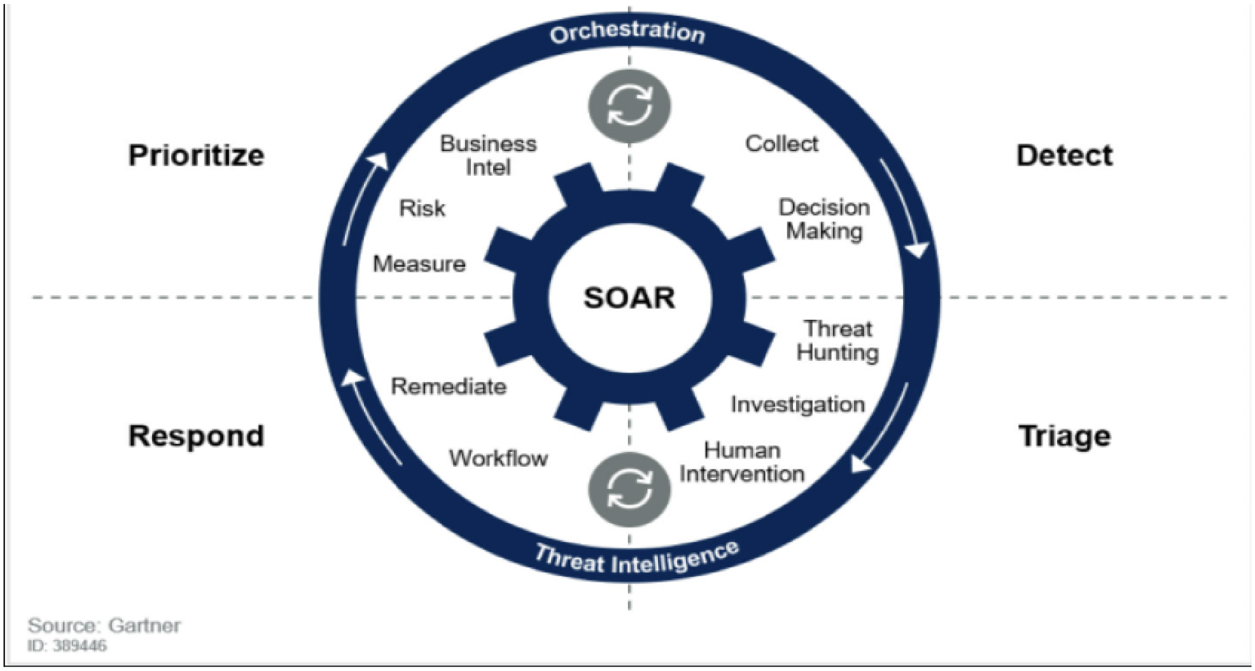
ABOUT SIEM, SOAR AND THE DIFFERENCE BETWEEN THE TWO:

SIEM collects and aggregates security data from integrated platforms that log event-related data - firewalls, network appliances, intrusion detection and prevention systems, and so on - and then correlates data across devices, categorizes, and analyses occurrences before delivering warnings. Advanced analytical approaches and machine learning are used to identify the alarms, which require fine tuning. This leaves a security team or SOC with a large number of alerts to prioritize and remediate, which is a tough and time-consuming task.



SOAR, on the other hand, is designed to assist security teams in automating the response process by collecting alerts, managing cases, and responding to SIEM's never-ending alarms. Security teams can use SOAR to connect to security alerts and establish adaptive, automated incident response workflows. SecOps will be able to prioritize threats and deliver faster outcomes as a result of this. They automate security operations in three major areas: threat and vulnerability monitoring, incident response, and security

Organizations use the SOAR strategies and tools to implement security orchestration and automation. SOAR stands for Security Orchestration, Automation and Response.



Source: Gartner
ID: 389446

In a nutshell, SIEM collects and correlates data from numerous security systems to generate alerts, whereas SOAR handles the alerts' cleanup and reaction. So, basically SIEM can be considered like a subset of SOAR, as collecting logs is also a part of SOAR mechanisms.

USE CASES OF SOAR:

The use cases for Security Orchestration, Automation, and Response (SOAR) will vary depending on a variety of factors, including the internal environment of the company, the industry or vertical it serves, and even the legal and regulatory compliance requirements.

Here, we will discuss five of the most common use cases for a Security Orchestration Automation and Response (SOAR) solution and how by utilizing this technology, a security alert and potential incident can be quickly detected, responded to, and resolved without having a major impact on the organization.

1) Phishing:

Over the last few years, phishing emails have become one of the most serious concerns confronting businesses. Some of the most high-profile data breaches in recent years have been the consequence of well-crafted phishing emails.

SOAR is well positioned to provide automatic triage and examination of suspicious phishing emails by extracting artifacts from the email, doing additional enrichment on these artifacts, and, if necessary, containing the harmful email and any malicious payloads.

2) Malicious Network Traffic:

Because of the proliferation of detecting technology, businesses are constantly bombarded with alarms. Many of these warnings are triggered by traffic that has been flagged as possibly malicious by one or more detection technologies. This is usually based on a threat indication that may or may not be accurate. It's frequently left to the business to further evaluate and investigate each of these warnings to see if they're a false positive or a genuine potential security threat.

A SOAR may receive harmful traffic alerts directly or after they have been ingested and forwarded by a SIEM. In either situation, the benefit of using a SOAR to automate and orchestrate activities around these types of occurrences comes from the automatic enrichment and potential containment of the discovered signs.

3) Vulnerability Management:

Security Orchestration Automation and Response was never designed to be a vulnerability management platform, and it will never be able to take the place of today's strong vulnerability management systems. However, a SOAR platform can help with some components of a strong vulnerability management programme. Vulnerability management is frequently done outside of the security team in larger organizations. This can result in a danger because the security team may be unaware of vulnerabilities in the infrastructure.

A SOAR solution can be used to notify the security team of any new vulnerabilities discovered within the company. This enables the security team to proactively review the susceptible host to confirm that no evidence of exploitation exists, implement any necessary extra safeguards, and subject the host to greater monitoring until the vulnerability has been addressed.

4) Managed Security Service Providers (MSSPs):

Computer Security Incident Response Teams (CSIRTs) and Security Operations Centers (SOCs) confront many of the same difficulties as Managed Security Service Providers (MSSPs), but on a much bigger scale. MSSPs confront several particular concerns that SOAR technology can address in addition to these common challenges. MSSPs are required to adhere to tight service level agreements (SLAs). Failure to meet these SLAs may result in a loss of business, a tarnished reputation, and possibly legal action. MSSPs can work more efficiently by automating and orchestrating tasks with a Security Orchestration, Automation, and Response SOAR system, ensuring that all SLAs are met.

5) Case Management:

Case management, while not strictly an orchestration and automation function, is a crucial aspect of the incident response process that SOAR may help expedite. Many businesses struggle to manage the massive volumes of different data collected following a security event. For managing a complex cyber incident, spreadsheets and shared documents are simply insufficient.

SOAR not only keeps track of all the information and enriched data collected through automated and choreographed operations, but it also keeps track of all the actions made during the response. A comprehensive SOAR solution should also include detailed task management, allowing incident managers to create, assign, and track tasks for all analysts involved in the response.

CONCLUSION

Security orchestration is about to revolutionize security operations. Using orchestration, we can increase our team's power so they can focus on strategic insight, spotting compromises, and continuing to develop deep layers of security.

With today's more complex enterprise systems, vast data, and persistent security threats, security orchestration has grown. We get higher-quality warnings that teams can respond to more effectively with a platform that enables for more efficient management of security tools, information, and systems, as well as an implementable process workflow.

The advantages of adding security orchestration to our corporate security systems are obvious and attainable, and if an organization wants to stay competitive in the foreseeable future, it should aim for maximizing security orchestration.

Security orchestration is the next step towards better business, more secure information, and a stronger defense against compounding threats and security risk. So, more and more organizations should try to maximize the orchestration and automation of their security management systems.

REFERENCES

1. https://www.rivialsecurity.com/blog/what-is-security-management-orchestration

2. https://digitalguardian.com/blog/what-security-orchestration

3. https://swimlane.com/solutions/security-automation-and-orchestration/security-orchestration

4. https://www.rapid7.com/solutions/security-orchestration-and-automation/

5. https://www.securaa.io/all-you-need-to-know-about-security-orchestration/

6. https://www.rapid7.com/blog/post/2016/04/05/what-is-security-orchestration/

7. https://www.sumologic.com/blog/5-common-security-orchestration-automation-and-response-soar-use-cases/

8. https://www.peerspot.com/questions/what-is-the-difference-between-siem-and-soar-platforms

9. https://secureops.com/blog/security-orchestration-in-4-simple-steps/

10. https://layots.com/security-information-and-event-management-siem-solution-its-importance/