Orchestration and Automation of Security Management Systems.

By

Pankaj Khemani

IMT2018054

What is Security Management Orchestration?

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.

WHY IS SECURITY ORCHESTRATION AND AUTOMATION NEEDED?

1) Increased Efficiency
2) Better Response Time (Quick Decision Making)
3) Saves a lot of manual effort
4) That saved effort can be utilized in more important tasks
5) Manual Errors are avoided
6) No longer a “nice to have”, but a “need to have”

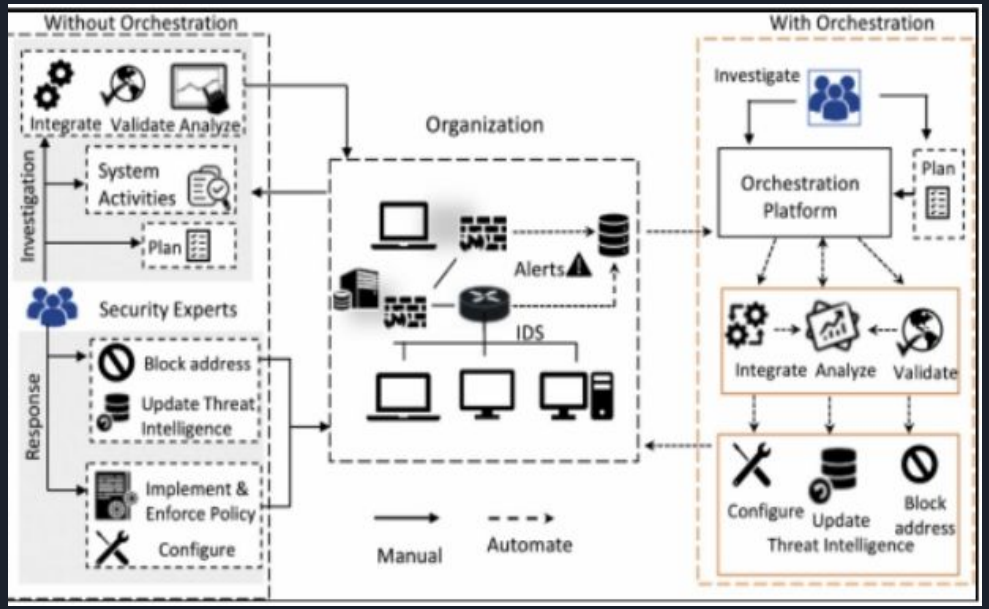
Examples to explain the need.

1) Phishing Emails
2) Single Solution or Technology for all the tasks does not exist
3) Giving out security tasks to a single security vendor also doesn’t work out because nowadays the number of security breaches have increased
4) Giving security tasks to multiple vendors on the other hand increases complexity of the system and it becomes difficult to manage multiple people

Solution

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.

Generalized Implementation of Security Orchestration.



Generalized Steps:-

1) Automate repetitive assessment and remediation tasks
2) Implement an incident assessment and response workflow
3) Integrate internal and external threat intelligence resources
4) Monitor, assess, and repeat

SIEM v/s SOAR

SOAR 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.

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.

SecOps

DevOps - Sounds Familiar Right!

Recently organizations have started to make a shift towards DevOps from their traditional SDLC, because organizations have started to understand the need and importance of automation.

The term SecOps has also emerged quite well along with SOAR as it aims towards automating the security operations.

Use Cases of SOAR:

1) Phishing
2) Malicious Network Traffic
3) Vulnerability Management
4) Management Security Service Providers
5) Case Management

Conclusion

Security orchestration is about to revolutionize security operations. 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.

Thank you!