
Security Orchestration, Automation & Incident Response
New Research On SOAR

Introduction

In early 2017, Siemplify, in partnership with Enterprise Strategy Group (ESG), conducted extensive research on the priorities and challenges within security operations. There is no shortage of noise in the industry and we are committed to helping security leaders cut through that noise with hard data to drive real improvement in security operations.

ESG & Siemplify Research

As a security professional, I see shoring up security operations as critical to the stability and success of companies across many industries. The joint ESG and Siemplify research on Security Operations validates these points and many others that I witness everyday. While still an emerging category, **Security Orchestration** demands are here to stay and accelerating.

CyberSecurity Front Lines

At Siemplify, we are driving the narrative for the entire **Security Orchestration and Incident Response** Market. We often find ourselves leading the discussion on how best to solve security operations greatest challenges. In looking at the research, it's clear that security operations biggest challenges center on keeping up with the volume of alerts and lack of integration among existing tools.

Security Operation Team

The research also tells us that the most time consuming task for Security Operations team is gathering data relevant to an alert or attack. Part of this stems from the proliferation of disconnected systems and reliance on manual process. Cybersecurity teams need to be able to shrink their number of active cases by consolidating the data that they have and not by ignoring meaningful alerts (a reality that is behind too many breaches). That way, analysts are able to focus more on real, tangible threats and less on itemized alerts which have become unbearable to Security Operations teams.

Incident Response

Indeed, when asked how highly they value the idea of consolidating & contextualizing security alerts, 95% of respondents recognize the importance of understanding the complete context of a threat. Focusing your already limited workforce is essential, and consolidating your **incident response** by efficiently triaging security alerts is the way to do exactly that. And that is the starting point for effective process execution and automation.

Integrate to Survive

Out of the ESG respondents, integrating disparate tools was consistently cited as a top priority. Specialization in security controls has become the norm to detect the increasing sophistication of attacks. Yet connecting these controls to a central command platform, and using disparate information efficiently to help dictate your incident response procedure and priorities, is paramount in 2017. To go a step further by integrating these systems (more than 25 tools in some cases according to the data) allows you to create a broader picture through which you and your team can operate, remediate and respond.

Final Thoughts

As a cyber security leader, by investing in orchestration, and making this the cornerstone of your security operations center, you are decreasing the chances of being hit with high impact malicious attacks. Orchestration allows for your approach to be more focused. It minimizes the complexities surrounding your security operations. Through the command and control approach that Security Orchestration enables, you can focus on what matters, standardize response, and increase visibility on real, tangible threats.

Conclusion

By combining the intelligence and data you already have within your broader security operations, you can see the threat storyline come to life. Thus, the characteristic of a threat that you would otherwise overlook can be flagged and appropriately dealt with. No matter how you choose to prioritize, orchestration can and absolutely should, play a role as top priorities in your security operations plan for the foreseeable future. The need for more efficient, orchestrated and automated security operations is palpable and and we are committed to meeting this challenge head on.