Security: Orchestration of Time

THREAT NOTIFICATION: In 2018 a Demisto survey of security professionals found that the average security team was bombarded with roughly 174,000 security alerts or threat notifications in a week. It was reported they were only able to effectively respond to roughly 12,000 of them, which is less than a 15% rate of actual remediation on alerts.[1] While some of these alerts may be low severity, or even false positives, many teams do not have enough time to actually investigate each one thoroughly. When alert fatigue sets in, analysts begin to prioritize alerts, often leaving many of 'low importance' to fall through the cracks. The team not being properly invested in, or company culture are also factors that can lead to these practices. There are ways to rectify these common problems, which can potentially leading to data breaches.

What causes huge numbers of alerts? One might believe that it stems from how often attackers are attempting to penetrate the network, however, there are several internal factors that might be causing such an influx of alerts. With the tech industry having one of the highest attrition rates, it's no wonder the number of alerts and how they are handled takes a back seat.

First and foremost, the number of alerts can be caused by misconfigured appliances that monitor the network and endpoints. On the outside looking in, this may seem like a quick fix, go into settings & tell it to stop. Unfortunately, it's just not that easy & security pro's are aware that configuring appliances takes a certain level of technical know-how and can be a real nuisance on the front end, yet a breach is even worse on the back end.

Configure the sensitivity of an appliance too high & you can bury your analysts alive with notifications, sending them on a wild goose chase. The result can be reduced effectiveness within the team because they are spread too thin & aren't laser focused on stopping real, serious threats from penetrating your network & compromising data.

On the flip side, configuring the sensitivity too low leads to the appliance essentially being "numb" and useless. Collaborating appliances such as a SIEM, a behaviour analytics tool and a machine learning solution, is a never-ending, fine-tuning process that requires good data to be fed in, in order to get good data out. As the saying goes, "Garbage in, equals garbage out". [4] Yet, nothing in security is 'set it & forget it', a well-trained human factor in combination with the security appliance orchestration will optimize your security event processing. A piece of advice from Allan Alford, CISO of Mitel, on the Defense in Depth podcast, "Automate when you can."[3]

> *"With the tech industry having one of the highest attrition rates, it's no wonder the number of alerts and how they are handled takes a back seat."*

Security orchestration and automation utilize Artificial Intelligence and/or Machine Learning by taking strings of textual security data that are generated by your environment and transforms them into context-rich detailed data. Not unlike the universal translator from Star Trek, taking all the "languages" of different worlds and translating it to English. However, orchestration can take things one step further to create a more effective Security Operation Center (SOC) by automatically grouping these translations into manageable, cases. This means that rather than just working a plethora of alerts, the analyst or

team is actually working a case that may be a culmination of all of these alerts, painting a more complete and detailed picture of threats.

Ensuring smooth orchestration through automation and investment in people can be your competitive edge when conquering a mountain of alerts. Having great allies, like SecureNation, is the best way to begin any climb.

“Ensuring smooth orchestration through automation and investment in people can be your competitive edge when conquering a mountain of alerts.”

One team started with asking their SOC engineers to list which of their duties took up most of their time & some ideas of how to automate them. As they began automating some of their processes the team was free to complete more of those fine-tuning tasks that lead to less alerts overall, creating a snowball effect of more valuable time to complete urgent tasks & requests. Over time the team shifted from being a reactive atmosphere to a more empowered, enriched & prepared team.

The human factor has been optimized, which is great, but there is still a lot of data coming at your team that lacks context. There are several tools in the industry that can help you, the first of which being a Security Information Event Manager (SIEM). A SIEM will help by generating reports and alerts from communicating with multiple sources & collaborating event logs. While providing clarity, a SIEM can still generate the dreaded alert fatigue by itself.

An extra layer of context can be added with AI & ML tools, such as behaviour analysis tools that learn from user & system patterns in order to determine a potential threat. User behavior analysis will profile a user based on time, location, typing style & patterns, and more. If a user strays outside of their typical profile by accessing the network outside of usual hours, for example, an alert will be generated for human intervention. The same concept can be applied to IoT devices in a network by learning how the organization uses that specific device.

There are many other tools and resources that can be used to help orchestrate and automate your security defense and response. SecureNation’s partnerships with hundreds of security manufacturers can be a resource for you to find open-source and pay-to-play tools that can take your security program to the next level of functionality. Reach out today or follow us on LinkedIn to get bite-sized tips & tricks on how to keep your security team with the competitive edge.

References

[1] https://www.demisto.com/news/latest-research-shows-security-teams-review-an-average-12000-alerts-week-setting-the-stage-for-automation/

[2] https://www.csoonline.com/article/2134247/inside-knowledge-likely-in-target-breach--experts-say.html

[3] https://cisoseries.com/defense-in-depth-amplifying-your-security-posture/

[4] https://www.scmagazine.com/home/security-news/in-depth/crying-wolf-combatting-cybersecurity-alert-fatigue/