Getty Images

SECURITY > THREAT MANAGEMENT

How-To: Combating Security Alert Fatigue

Alert overload is taking its toll on security pros. Security experts weigh in on ways to reduce security alert fatigue.

Karen D. Schwartz | May 14, 2020

Eric Adams understands the effect of security alert fatigue from many vantage points. As a longtime security professional, he has experienced it many times

"We have seen that if there are more than about 75 events over an hour, it's just too many alerts," he said. "It's like being an air traffic controller. When you have a certain threshold of events per hour, you run the risk of an analyst not running the full playbook or analysis of an event."

In fact, alert overload is a huge problem, and it can sabotage security operations. According to one recent report, the vast majority of security analysts say it takes more than 10 minutes to investigate each alert. It's just a matter of doing the math.

In addition to alert overload, other challenges contributing to security alert fatigue include false positives and security analyst churn. One study found that more than two-fifths of organizations experience false positive alerts in more than 20% of cases, while 15% reported that more than half of their security alerts are false positives.

Here, experts weigh in on ways to reduce security alert fatigue.

Upgrade and modernize if you can. Ideally, this will include as much automation as possible. Jason Mical, cybersecurity evangelist at Devo Technology, says the best way to do that is by replacing your legacy security information and event management (SIEM) system with a newer version that is a more automated, rule-based system and relies more on artificial intelligence and machine learning. Newer SIEMs have access to all of the data in an environment instead of just security data. That gives more context to every alert and helps with prioritization. More modern SIEMs also tend to provide more visibility. These capabilities can help winnow down the number of alerts that are actually actionable, helping reduce alert fatigue.

For Kyriba, the solution was an automated security operations center (SOC) based nature of this solution helps reduce alert fatigue and frees analysts up to work on other tasks.

If you can't upgrade, you're not completely out of luck; focus on fine-tuning what you have. That includes:

- **Customizing your rules or change some settings.** "There is constant management that has to be done with alert rules," Mical said. "There may be an alert set up that says if you see someone communicate on Port 443, alert me to that. Now you have 20 other devices because new applications have been spun up that are firing a ton of alerts, so auditing your alert rule engine is important, especially if you have a legacy SIEM environment."
- **Tuning the network signatures in your intrusion detection system (IDS) to make them as tight as possible.** "Having quick access to network metadata related to security alerts will also help analysts quickly identify false positives and not waste too much time investigating them," said Andre Ludwig, chief product officer at Bricata.
- **Dealing with configuration issues.** "If you ensure that proper administrative configurations are enabled, you can minimize superfluous alerts," said Armond Caglar, a principal at Cybeta, a business threat intelligence company. Ensuring proper access control is another important configuration issue; if the right people have access to the right alerts, the entire system will be more effective. "Network teams should be constantly improving, refining and updating processes tied to access and alert generation of their various technology sensors," Caglar continued. "This includes continuous adjustments made to each team member's access, the topics assigned to them, and criticality protocol."

Be careful how many point solutions you add. While it may be tempting to add more tools to your legacy SIEM, choose carefully or you will add more you have to be able to handle that data in an effective way." Make sure your personnel and processes can handle the load, he added. "We don't bring on any more tooling that makes any more load for us. We look at tools that allow us to reduce the load on the human personnel."

No matter which route you go, testing is critical. Make sure you are doing red team/blue team exercises to validate your rules, and do penetration testing to ensure that there is no way to circumvent them, Michal said.

0 COMMENTS

RECOMMENDED READING

looking through a magnifying

McAfee Reworks Enterprise Security Manager for the Cloud
JUL 14, 2020

hands typing on a laptop

How to Get the Most Out of Your Penetration Tests
JUL 13, 2020

Cybersecurity

As Offices Reopen, Hardware from Home Threatens Security
JUL 10, 2020

security alert on laptop

Proofpoint Insider Threat Platform Detects, Prevents Risks
JUL 04, 2020

About
Advertise
Contact Us

CCPA: Do not sell my personal info
Privacy Policy
Terms of Service

tech