Eliminating Alert Fatigue to Get to the Data That Matters: A New Approach to Threat Detection and Response

Now that state and local governments have adjusted operations to cope with the pandemic, it is clear that many changes made during this time will become permanent moving forward. Remote work, digital services, online collaboration and other recently implemented solutions have put government organizations in extraordinary circumstances to meet constituent requirements with uprooted IT infrastructure. Once considered conveniences, they are now necessities for constituents and government employees.

Despite their benefits, these solutions create new attack vectors and vulnerabilities, and can exacerbate ongoing challenges associated with monitoring and protecting the network, cloud services and a multitude of endpoints. Cybersecurity teams are often so inundated with alerts coming from siloed security tools that it is difficult to home in on the most important issues.

Outwitting cybercriminals in this complex environment requires a new approach to threat prevention, detection, investigation and response. By integrating and unifying endpoint, network and cloud threat data, security teams can more accurately detect and prevent attacks before they happen and simplify investigations when they do, allowing for more immediate response. When fueled by AI-driven analytics and machine learning, this approach can quickly transform security operations.

Alert Fatigue Is Real

The following challenges keep security leaders and their teams awake at night:

Onslaught of new vectors and vulnerabilities. The move to remote work has generated a multitude of new endpoints, network configurations and cloud solutions that are ripe targets for cybercriminals. The race to deploy urgently needed digital services has also increased risks. To save time, developers often draw on third-party code libraries; if not caught, vulnerabilities in these code snippets may be proliferated into new programs. In addition, as websites connect to backend systems of record and other workflows, legacy code that was not designed with security in mind may be more exposed.

Sophistication of threats. Highly sophisticated threats have become the norm. The four recent zero-day exploits that targeted vulnerabilities on Microsoft Exchange Servers came on the heels of the nation-state attacks against SolarWinds and other vendors. Although the full extent of the SolarWinds attacks is still being investigated, industry leaders say it's one of the largest and most sophisticated attacks ever.[1]

Detecting known threats and zero-day malware. While common vulnerabilities and exposures (CVE) lists help identify known security flaws, patching those flaws is often a monumental task. Most security teams simply don't have enough hands to manually patch every vulnerability. In addition, traditional attack detection and prevention tools can only detect known threats. They don't have the analytic capabilities to automatically identify and deflect behavioral anomalies that indicate a potential compromise or zero-day exploit.

Separating "noise" from true threats. Seventy percent of IT security respondents in a recent survey said the number of security alerts they receive daily has more than doubled in the past five years.[2] Overwhelmed security teams may overlook true threats or generate backlogs of uninvestigated tickets as they manually comb through false positives and relatively minor threats. Adding more personnel isn't always the answer. The root problem is tools that do not have enough context to properly identify and classify potential threats when they create an alert.

The Force Multiplier: Automated, AI-Driven Threat Detection and Response

To more effectively, efficiently and rapidly detect and respond to threats at scale, state and local governments are turning to highly automated, AI-driven solutions.

At the center of these solutions is a platform that provides a single, integrated view into all the threat data coming from networks, endpoints, the cloud and third parties. Mature solutions also include tools to see what the organization's attack surface

looks like from the outside (i.e., from the viewpoint of attackers probing for vulnerabilities).

By consolidating all this data onto a robust, highly scalable platform and then applying AI and machine learning (ML), these solutions act as a force multiplier and transcend what's possible in even the most well-staffed security operations centers. They automatically filter out the noise, identify and correlate behavioral anomalies and actionable events, and then apply contextualized threat intelligence to enable security teams to prioritize and remediate the events that present the highest risk.

These capabilities enable near-immediate discovery and filtering of known threats, zero-day exploits and stealthy attacks. By dramatically reducing alert volumes and automatically handling the bulk of remediation processes, these AI-driven solutions enable security teams to focus on the alerts and threats that matter most. They also help maximize the value of investments in security tools by enabling organizations to leverage their full functionality without becoming overwhelmed by the data they generate.

Getting Started – Funding and Support

The following steps help organizations justify funding and obtain support for a modern threat detection and response platform:

- Build trust and strong relationships with the people who control the budget by being transparent, communicating regularly and including them in important decisions.
- Present a strong business case that includes data to quantify existing challenges and demonstrate potential benefits of a modern solution.
- Conduct a proof of concept, either in house or with the help of a third-party vendor.
- Start with (and communicate) quick wins to increase buy-in and further demonstrate the value of the investment.

Leveling the Playing Field

As the attack surface expands and cybercriminals become more resourceful and sophisticated, organizations will need practical ways to detect, respond to and remediate threats. An AI-driven, automated solution — powered by a robust, integrated platform — levels the playing field and enables even the leanest staff to stay ahead of threats.

AI and Automation Change the Game for Gainesville

When the city of Gainesville, Ga., determined that its traditional antivirus, heuristics analysis and other tools weren't enough to keep threats at bay, it turned to an advanced, behavior-based solution that is driven by AI and ML.

"We were getting too many false positives and missed alerts. In addition, we were concerned that we couldn't identify zero-day attacks. It kept everyone guessing about what was actually happening," says Jonathan Reich, city IT manager for Gainesville.

The new solution — Palo Alto Network's Cortex — automatically weeds out the majority of false or irrelevant alerts, reducing alert fatigue and enabling Reich's team to act decisively. "I have very few notifications on my dashboard, but my team responds immediately to those alerts because we know they are reliable and worthy of our time," says Reich.

In addition, he and his team have a single pane of glass to quickly correlate information. "Within minutes, we can see where an incident came from, where it's trying to go, and what and who triggered it," says Reich. Once an incident is identified, Reich can use the dashboard to isolate it instantaneously (even if he is geographically separated from the device) and begin remediation.

"People in local government don't usually have a lot of staff. We're running lean FTE, so anything that lets me maximize the time on task is huge. This is a game changer," says Reich.[3]

This paper was written and produced by the Center for Digital Government, with information and input from Palo Alto Networks.

[1] *L. Tung. ZDNet. Microsoft: SolarWinds Attack Took More Than 1000 Engineers to Create. February 2021. https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/*

[2] *D. Raywood. InfoSecurity Magazine. Alert Fatigue and Overload an Issue for Majority of Security Analysts. July 2020. https://www.infosecurity-magazine.com/news/alert-fatigue-overload-issue/*

[3] *Government Technology Webinar: No More Alert Fatigue – How Good Data Drives a Sophisticated Cyber Strategy. August 2020. https://webinars.govtech.com/No-More-Alert-Fatigue-How-Good-Data-Drives-a-Sophisticated-Cyber-Strategy-128368.html*

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: paloalto® NETWORKS

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting thousands of government and education organizations across their clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before, and we are passionate about protecting the services, systems, and data that drive government. For more information, visit paloaltonetworks.com or our State & Local Government page **paloaltonetworks.com/security-for/government/government-state-local.**