Eliminating Weekend War Rooms—The Shift from Reactive to Proactive Security Operations

By M.K. Palmore, Field CSO, Palo Alto Networks

It's the call no security professional or IT executive wants to get: the call to deal with a critical security incident that occurred over a weekend.

The weekend war room might be considered a rite of passage for some. But more often than not, it's the end result of an organization with a reactive, rather than proactive, approach to security.

It can seem like an out-of-the-blue emergency when the call for the weekend war room happens, and these calls always seem to come at a moment when the organization feels like it's least prepared. However, in my experience, it's often a slow rolling thunder that builds into the emergency security incident. And you never know what the loud clap is gonna sound like at the end.

When I was with the FBI, there were instances where we were called in weeks or even a month after a security incident took place. At that point, the breached organization is really just trying to stop the bleeding and figure out how to make themselves whole again. That's not the position any IT executive or business leader wants to be in. Not on the weekend, and frankly, not any other day of the week, either.

You Can't Manage What You Don't Monitor

So, how do you move from being reactive to proactive? The first step is to ensure that the business has visibility.

Visibility is a challenge, but it's also fundamental. Does the practitioner see everything in the environment? Because if you can't see it, you can't react to it; if you can't see it, you can't mitigate it; if you can't see it, you can't plan for it.

Gaining visibility puts an organization in a position to move from a reactive to a proactive prevention footing.

Also, visibility isn't simply about logging. Every organization has logs of one sort or another from any number of different systems. What's needed is context—the ability to correlate log activity from the different domains and enclaves you have within an environment. Then, the challenge is for a human to sit in the middle of all of that, correlate the information, put context around it, and then be in a position to respond.

Security Frameworks Point the Way Forward

Integrating different logs and visibility tools is only part of a proactive approach. The best security operations centers often make use of a standardized framework that helps to define what's needed.

One of the frameworks I like to reference frequently is the Center for Internet Security (CIS) Critical Security Controls. Not only are they presented to InfoSec practitioners in common language; they're prioritized to provide a roadmap of where to start and where an organization needs to be in terms of cybersecurity engagement.

Those 20 controls have proven helpful time and time again to organizations of all sizes. Nearly every significant cybersecurity incident—certainly that an organization like the FBI investigates—shows some kind of violation of the 20 CIS critical controls.

Move the Weekend War Room to Another Day of the Week

The weekend war room is a result of reactive management, but that doesn't mean that there shouldn't be a weekday war room. Proactive organizations should have periodic check-ins with IT security staff and management.

Engaging key stakeholders simply and regularly can make all the difference. One of the challenges I had in the FBI was that I didn't have an effective dashboard I could share with executives to show them where we were posture-wise. Today, I recommend leaders have a dashboard with visual elements that make it easy for people to understand and digest.

The dashboard and any associated reports should show the relative level of risk associated with vulnerabilities in the organization and a timeline of when they will be fixed. It's also important for the organization to know and show what is connected to a network. Trying to figure that out after an incident has occurred in a weekend war room is not a pleasant task.

The dashboard and associated reports should also provide context around security alerts in a way that's easily understandable to help determine impact. Organizations should actively track incidents as well so that executives can easily understand if there have been any attempts to detonate malicious software within the enterprise—and whether or not those attempts were blocked. Having visibility and a clear picture of the health and maturity of security operations is a cornerstone of building a proactive security organization.

Taking a proactive approach to security doesn't just help save the weekend—it can help solve the challenge of IT security staffing as well. By integrating visibility and automation that enable a proactive approach, an organization can free up personnel to do more high-level, human-intensive work. When humans aren't running around on the weekend dealing with incidents, they can be more efficient, and that might help address the chronic shortfall of IT security professionals.

No one wants to get that call to engage with a weekend war room. The key to preventing that outcome is to embrace a proactive strategy that provides visibility and context that help identify risks before they become weekend war room incidents.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com