Secureworks®

WHITE PAPER

5 Signs You Have Gaps in Your Security Stack

When are daily frustrations a sign of bigger issues within your security operation? Most security teams would like to know the answer to that question, but CISOs and analysts only have limited sources of information to draw from. Security professionals can only really compare their current environment to ones they've worked in before and whatever they hear from their peers in the industry.

Dealing with complexity is a fact of life in cybersecurity. A constant stream of new tools addressing the threat landscape and a relatively short tenure for CISOs has led to layered environments with forgotten tools that fell out of favor as leadership and trends in the industry have changed. Between those tools and complexities lie gaps where threat actors can seek opportunity. Complexity is now so pervasive that many security professionals struggle to identify when complexity is a result of gaps in their stack, or when it's just part of the job. Below are five signs that the complexity you experience stems from gaps in your security stack.

Dealing with complexity is a fact of life in cybersecurity.

Sign 1:
You're Constantly Playing Whack-A-Mole With Incidents

If you feel like you can never get on top of all the incidents and events in your environment, that's a sign there could be gaps in your operation. This is common for security teams where the correlation of telemetry to threat intelligence is mostly manual. Staff are burdened by painstaking tasks that take great time and effort, such as checking threat intel feeds against events. The number of events to correlate causes analysts to feel like they will never catch up. Teams should also have time to reflect and learn from their responses to incidents, but if analysts are constantly moving on to the next issue, this won't happen.

Sign 2:
You're Not Seeing Many Incidents

There are two possibilities in this situation: 1. One or more of your tools is misconfigured and missing threats you need it to catch. 2. Your team is seeing more alerts than they can cope with. Excessive alerts are common, especially in environments without strong correlation tools. These alerts may obscure real threats and force analysts to spend time on triage that would be better spent elsewhere.

Security teams often have an awkward relationship with alerts. Many organizations expect to see lots of alerts as proof the security team is needed and working hard. Without this proof, the security department might not get the budget it needs. A good solution is to find a tool that can automatically analyze and correlate alerts against threat intelligence to reduce the need for alert triage. This saves time and allows analysts to focus on more interesting parts of the job. Choose a tool that offers reporting capabilities, and you'll have no trouble presenting proof of alerts when needed. However, a period of education is often needed as modern tools get better at ignoring the alerts that don't matter.

Sign 3:
You Can't Keep up With Your Patching Needs

Patching is a reliable way to close gaps and reduce the potential points of entry for threat actors, but it is a large, ongoing task that is hard to keep under control. If at the end of every month you find yourself with a large number of assets yet to be patched, it's a bad sign. Each unpatched system represents a real risk to your organization. If you use a vulnerability management service, take a close look at what your vendor is doing and troubleshoot with them. Look at whether a system is on-premises versus web-based, whether it's covering your entire environment, or whether you're running something else to identify what needs patching.

Sign 4:
You Overlook People and Processes

Don't let tools distract you from implementing efficient processes and training your people. Find a middle ground with your processes. Documenting is critical, but it shouldn't get in the way of offering clear ways to proceed under different sets of circumstances. Using security analytics software can help you close gaps by applying automatic correlation to your telemetry. However, if your team isn't given sufficient time to learn how to use and configure the software, this could create gaps where threat actors can enter. Automatic correlation from security analytics software will close gaps and help remove blind spots. It can also help you identify critical assets, as well as provide convenient reporting capabilities to facilitate risk discussions with managers and executive leadership.

Sign 5:
There's a Breakdown in Communication Between Analysts and the CISO

If analysts can't fulfill all the reporting requirements of the CISO, that's a sign there are gaps in the stack. The team should be able to account for all the data the CISO needs to do the job. If they can't, there's a major gap in understanding the security stack. Likewise, if you're a CISO and you feel like the team isn't giving you the information you need to understand risk and posture, it means some of the tools aren't the right ones and a level of consolidation is needed. Every security team should be able to measure the security environment holistically to build a full picture of what is going on.

Is a Vendor the Answer?

Identifying gaps is the first step, next comes closing them. This is a daunting task for many organizations. Complex environments hide a multitude of variables for security teams to consider as they plan how to close the gaps they've identified. The experience of most security professionals with closing gaps is naturally limited to their experience as one person. This can lead to uncertainty about what the most effective course of action is. In such a situation, a trusted vendor can help.

Vendors must accurately process alerts for customers across a wide range of industries. This experience allows a vendor to accurately identify threats they have seen in environments similar to yours. Having a vendor manage alert triage frees up your resources to focus on more important tasks. Some vendors can also handle vulnerability management for you, making the process more efficient and highly prioritized. Security companies see what gaps threat actors are exploiting every day, which means they can quickly identify which patches are most critical across different organizations and industries.

Security vendors may also have excellent in-house threat intelligence and incident response (IR) practices. A mature threat intelligence operation offers deep threat knowledge that far outperforms any single organization's ability to reference and use threat feeds. Threat intelligence is strengthened further by an expert incident response team. Every day, IR consultants come face-to-face with threats as they behave in the real world. This knowledge can help analysts identify unknown threats from subtle clues that they might otherwise miss, while also giving you a reliable partner to call on in the event of a breach.

A mature threat intelligence operation offers deep threat knowledge that far outperforms any single organization's ability to reference and use threat feeds.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.