6 Lessons for Cybersecurity Leaders

splunk>
turn data into doing®

The state of security is highly adrenalized these days — more so than usual. More than two years into the deadly and disruptive global pandemic, not only are we still seeing more attacks, we're also seeing more breaches.

New global research conducted by Splunk and the Enterprise Strategy Group of more than 1,200 security leaders found that 49% of organizations say they'd suffered a data breach over the past two years, up from 39% in our survey a year earlier. And while certain attack vectors dominated headlines in the last year or two, criminals are still finding success with traditional playbooks:

51% report business email compromise, up from 42% a year ago.

39% of organizations report insider attacks, up from 27% a year ago.

79% say they've encountered ransomware attacks, and 35% admit one or more of those attacks led them to lose access to data and systems.

Additionally, 40% of respondents report a regulatory violation (up from 28% a year ago). More and more sophisticated attacks, acute talent shortages and pandemic-specific challenges have SOCs reeling.

It's not clear whether these numbers are a sobering indication that attackers are significantly more successful today or if, as Splunk Distinguished Security Strategist Ryan Kovar notes, it's a question of causation versus correlation. Are intruders better at penetrating our defenses, or are security teams better at detecting intruders? The answer is probably "both," with offense and defense each improving aspects of their game.

"And ransomware skewers this because they actively tell you that you're compromised," Kovar says, "while traditional attackers try to get in and out without being detected."

Regardless of why security teams are detecting more breaches, they're having to work a lot harder, and are feeling greater effects than ever before.

There's more attention on security concerns, from the board of directors on down. There's more pressure on security teams, from the chief information security officer (CISO) on down. And for many organizations, there's more funding — but does anyone ever think it's enough?

In a world suffering from ever-rising threats of ransomware, supply chain attacks and staff burnout, to say nothing of the constant threats of insider attacks and social engineering — the baseline hurricane, if you will — here is the advice security leaders gave us from this global survey.

01

Seek talent, teach skills

Organizations are already telling us that they're prioritizing efforts to find, train and retain talent. All the traditional efforts in that sphere are important, and recommended. But they're not enough. The field of security analysts is just too small to ever meet the demand, which is why Ryan Kovar focuses on "talent" in its original meaning, not just as a euphemism for "workers."

"You're never going to fill the gaps with the traditional security workforce," he says. "We have to consider alternative candidate pools."

That can include people with experience in non-security IT roles, but Kovar says he looks even further afield.

"We need raw talent, not trained skills," he says. "I've had a lot of luck recruiting people with journalism, HR and creative backgrounds. I just need people with innate curiosity and a talent for synthesizing and understanding data."

People with a degree in the humanities, he has found, can be phenomenal at that — often better than those with traditional computer science degrees.

"I can teach the security analyst role to someone who can synthesize data and communicate it more easily than I can teach someone who just knows how to code in C++."

02

Know your cloud

Nearly eight in 10 respondents told us that CISOs are under pressure to increase their cloud fluency. A significant number also expressed confusion over where security responsibilities between their teams and their cloud providers connect. Everyone from senior security leadership to tier one security analysts needs to understand their hybrid, multicloud environment.

Organizations must dedicate time and training to understand the complex interplay of their public, private and SaaS solutions.

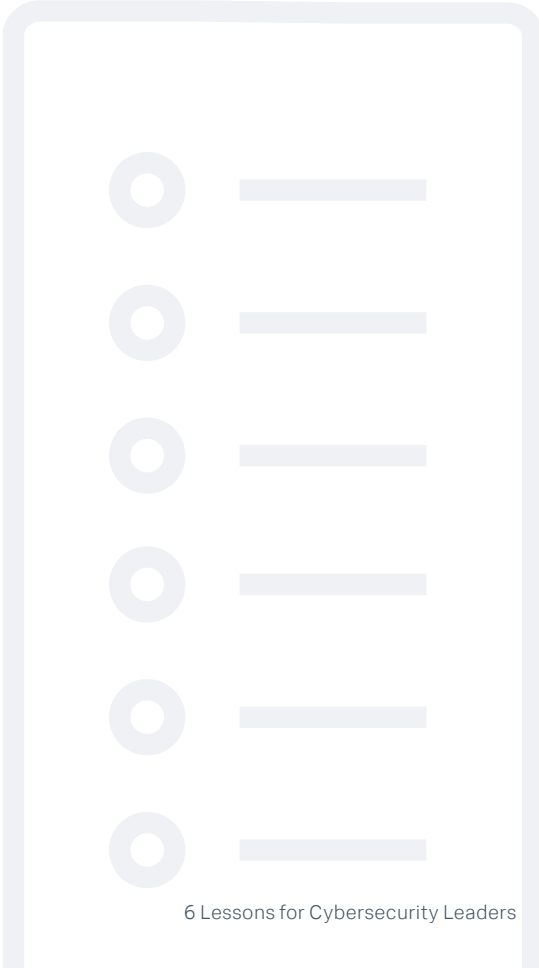
They need the tools and training to securely configure various environments, to manage access and authentication, and to minimize mean times to detect (MTTD) and mean times to detect and recover (MTTR). Many organizations are still in a state of confusion about the cloud, and that's a risk that has to be eliminated through a comprehensive approach to skill sets, tool sets, cross-team collaboration and education.

03

Build an SBOM

We mean really know your cloud. And all your software. Every software organization should maintain — as in, keep relentlessly current — a software bill of materials that lists all software components running in production via software composition analysis (SCA).

"A lot of organizations don't do this yet," Kovar notes. "Thanks to the attention to supply chain attacks, customers are going to begin demanding software bill of materials (SBOMs) from their vendors, and it will quickly become standard."



04

Use automation to enhance human analysts

If we're never going to have enough humans on the team, the solution is to just automate everything, right? Kovar warns that automation can create as many human headaches as it solves.

"Analysts being overwhelmed, and then burned out, is a difficult challenge, and in one sense, automation can make it worse," he says. "The more disparate tools you give someone, the more things they have to do, the more they have to keep up with. That doesn't necessarily help with burnout."

So automate with the intention of liberating your human analysts to do their job better. That can mean fewer tools, not more. It can mean a platform approach that makes it easier for analysts to not only keep up with their tools, but take action on significant events, while the basic stuff is remediated at machine speed. The result should be less sense of being overwhelmed — and less burnout.

"Security people got into the business to solve problems," Kovar says, "not to fill out spreadsheets."

05

Take DevSecOps forward

To the 23% of respondents who haven't gotten around to DevSecOps yet, we say, "Don't delay." To the 2% who aren't even thinking about it, we really urge you to do some reading on the topic. For the vast majority who are already making strides: Keep going.

Our research found that 75% of organizations are using DevSecOps to identify and fix vulnerabilities and to remediate malware prior to deployment, as well as logging code changes for audit and applying runtime API security controls. Add it up, and DevSecOps is helping organizations solve visibility challenges (and keep bad software out of production). Classic DevSecOps benefits.

The next step, Kovar says, is to apply DevSecOps specifically to defending against ransomware and advanced persistent threats.

"A DevSecOps approach helps you consolidate your network defenses to remove inefficiencies," he says. "It's an important step, because adversaries are increasingly combining attack techniques in a way that better exploits our coverage gaps or inefficiencies."

And make sure that your DevSecOps approach covers all software development, not just the official engineering team's work.

"These days, everyone is developing software," he says. "People don't necessarily realize that someone in a Fortune 50 company using Microsoft VBA [Visual Basic for Applications] in Excel might be generating more revenue alone than whole companies at the bottom of the Fortune 1000."

06

Consolidate sprawling tool sets

You need the right tool for the right job, as pretty much everyone's grandfather would say. But a piece of software isn't just a tool waiting in a box. It's an active application that requires monitoring to be effective, a degree of care from which we distill feedback. In that sense, it's more like a pet, and there are only so many of those you can have running around your house before you're mired in chaos. And poop.

Consolidation is about having the right tools for the right jobs, while also making sure that your team can manage the responsibility of care. As with haphazard automation, careless tool consolidation can increase frustration and burnout. Focusing on the necessary set of tools, particularly with a platform approach that can gather multiple inputs on one dashboard, empowers your analysts with information, rather than burdens them with the busywork of checking a million outputs. In the long run, organizations save on maintenance, training and licensing costs, and can put that savings to better uses. At the same time, a smart tool set improves visibility into infrastructure, application performance and security posture.

Want to learn more about how security leaders worldwide are beating ever-rising challenges? Read the full **State of Security 2022** report.

Get Report

splunk> turn data into doing®

22-24412-Splunk-6 Lessons for Cybersecurity Leaders-LS-104