March 11, 2020 Leave a Comment

Security

Are You Going About the Talent Shortage Wrong? It’s Time to Stop MacGyvering

We all know the stats. The security workforce shortage is impacting two-thirds of organizations, while the gap – currently at 4 million – continues to grow. Security teams are short-staffed, to the point where a 25% say the inability to keep with the workload is a root cause of security incidents.

The conversation typically focuses on challenges like the growing demand outpacing supply. Forrester even goes as far as saying that much of the problem is “self-inflicted” – and one reason is that employers “expect to hire MacGyver but pay like McDonalds.”

We’re looking at the problem wrong.

In the words of MacGyver himself, “there always seems to be a way to fix things.” But this is the wrong fix.

Yes, the talent shortage is real. But there's another reason why organizations have a shortage of skilled talent. Every new technology added to your security infrastructure not only adds complexity but is resource intensive, not to mention the decreased efficacy in detecting and preventing threats.

So clearly throwing bodies at the problem has not worked here. Talk about a self-inflicted cycle.

The disconnect between technology, people, and processes

We could always count on MacGyver to come up with an ingenious way to solve a problem. In one instance, he took out a flashlight spring to fix a compressor, while saying, "When something's broken, the easiest thing to do is just throw it away and forget about it. But if you step back and take a look at what you've got, sometimes you find a totally different way of making it work."

To apply this idea to security, it's time to step back and take a look at what you have – not just technology but also people and processes – and find a totally different way to make them work. Together.

The appeal of the move from products to platform has flooded the industry with platform solutions that end up integrating two or more products together. These platforms that simply layer technology to deal with your most pressing security concern aren't effectively eliminating the complexity that your teams have to deal with. Adding more technologies may seem like the most straightforward approach to reduce alert fatigue but it's not necessarily the right solution.

You need a platform embedded into your security technologies that empowers your security teams to make decisions based on complete and actionable insights. At the end of the day, the goal needs to be simply to create a seamless, simpler, more consistent experience that allows a threat to be detected in one area of the enterprise and be blocked everywhere else - from the data center, network, and cloud, to email, the web, endpoints, and everywhere in between. We believe that you can do so by leveraging integration, automation, and analytics to ensure that your technologies are working for you.

Making NetOps and ITOps an extension of SecOps

At Cisco, our approach is to bridge technology, people, and processes. We've taken the time to build the mortar into your entire security infrastructure–the new security platform called Cisco SecureX. It doesn't just connect to Cisco products; it transforms your infrastructure from a series of disjointed solutions into a fully integrated environment. This transforms your security teams from business blockers to business enablers empowered to scale and meet the needs of tomorrow.

Instead of telling our customers they need to hire more experts to manage their security solutions, we want to help them mitigate the talent shortage by uniting teams, solutions, and processes into a consistent experience.

To that end, we asked the question: How can we reduce the ITOps and NetOps reliance on SecOps, and stop the bottlenecks these teams create for each other? How can SecOps, ITOps, and NetOps collaborate with unified workflows?

Let's say the IT help desk receives a ticket about a slow-running computer. In a typical organization, the workflow may look like this:

- The technician connects remotely into the server and sees that the process is using up memory, but there's not enough visibility to identify the root cause of the problem.
- Next step is to involve SecOps and NetOps to gain more context. Since those teams don't share context, they may not be able to pinpoint the exact issue either.
- After an hour or more of troubleshooting and working with SecOps and NetOps, the ITOps' answer is to reimage the slow computer.

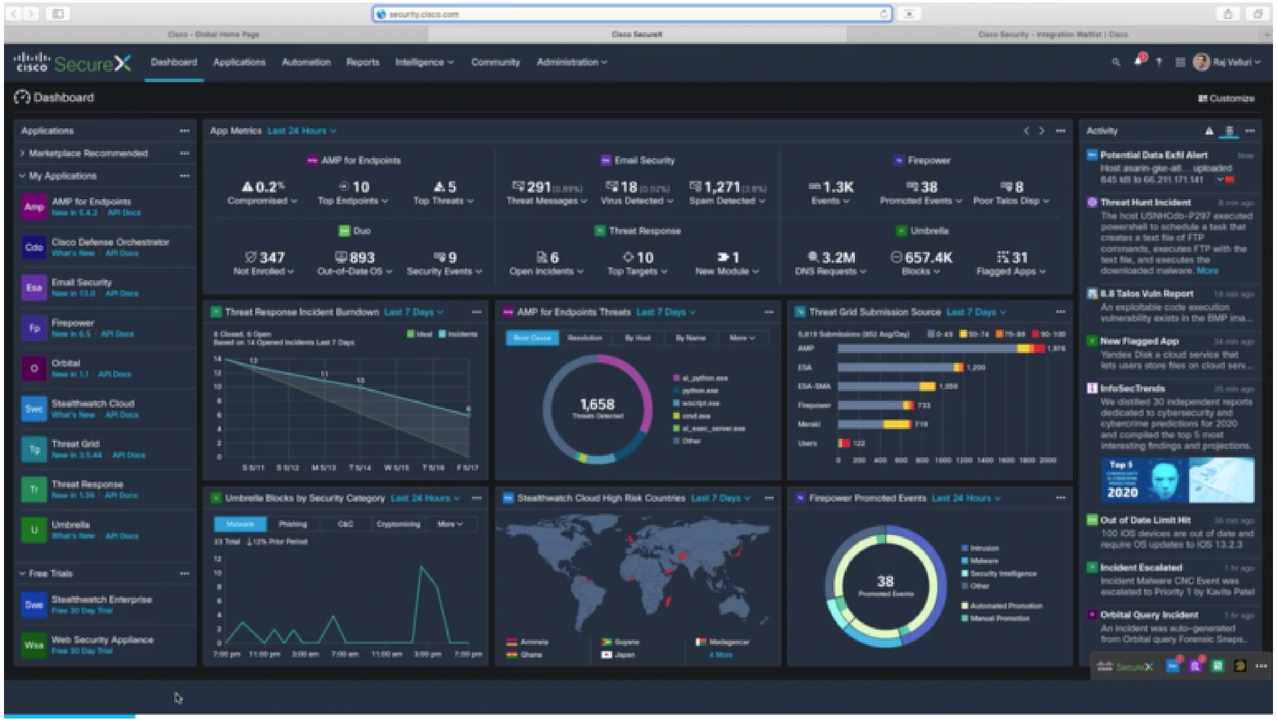
We wanted to break down these kinds of siloes that the teams work in, and at the same time make security more efficient. And Cisco SecureX does just that. At RSA 2020 this year we introduced Cisco SecureX – a new way for users to experience Cisco's Security portfolio. Cisco SecureX streamlines our customers' operations with unified visibility across their security portfolio and provides out-of-box integrations, powerful security analytics, and automated workflows to speed threat detection and response.

With SecureX, this is how the workflow would look like in the same scenario:

- The Security Analyst uses the SecureX dashboard – with access to a list of all users, devices, and apps – to investigate a malicious cryptomining attempt that was exploiting vulnerabilities on your endpoint and server-based applications.

- After identifying the problem, the analyst uses analytics to uncover where cryptomining activity may be occurring in your organization. Armed with a holistic understanding of the threat, the analyst now proceeds to block network connections to web sites known to participate in mining cryptocurrencies and isolates the endpoint host using **SecureX's threat response application.**
- Once he accesses the computer remotely to confirm that the cryptomining app connection was terminated, he simply reconnects the endpoint to the network.

[Watch the Cisco SecureX Overview Video Now]



Potential Data Exfil Alert — Now
Host asarin-gke-all... uploaded 845 kB to 66.211.171.141

Threat Hunt Incident — 8 min ago
The host USNHOdb-P297 executed powershell to schedule a task that creates a text file of FTP commands, executes FTP with the text file, and executes the downloaded malware. More

8.8 Talos Vuln Report — 18 min ago
An exploitable code execution vulnerability exists in the BMP ima...

New Flagged App — 34 min ago
Yandex Disk a cloud service that lets users store files on cloud serv...

InfoSecTrends — 35 min ago
We distilled 30 independent reports dedicated to cybersecurity and cybercrime predictions for 2020 and compiled the top 5 most interesting findings and projections.

Out of Date Limit Hit — 36 min ago
100 iOS devices are out of date and require OS updates to iOS 13.2.3

Incident Escalated — 1 hr ago
Incident Malware CNC Event was escalated to Priority 1 by Kavita Patel

Orbital Query Incident — 1 hr ago
An incident was auto-generated from Orbital query Forensic Snaps...

Cisco SecureX unifies visibility, enables automation and strengthens security

The entire sequence takes just 10 minutes instead of an hour or more, without involving SecOps and NetOps. SecureX provides all of your security teams – SecOps, NetOps, and ITOps personalized views of the same shared context, enabling them to collaborate better than ever before. This means they can more easily harmonize your security policies and drive stronger outcomes.

How SecureX helps mitigate the skills gap

Now, I'm not saying that SecureX solves the talent shortage on a global scale. The reality is that digital transformation, coupled with the growing threat landscape, will continue to place more demand on organizations to hire additional talent.

What SecureX can do, however, is start solving that self-inflicted problem we talked about earlier – the one caused by unnecessary complexities we as an industry have created. With no disrespect to our resourceful hero, we want to stop you from MacGyvering your security with dozens of point tools – and finally close the gap between your technology, people, and processes.

Want to see for yourself how you can do that? Sign up for our SecureX Waitlist and learn more about SecureX here.

Share