FEDInsider

Evolving Technology & Talent to Meet Future Federal Cyber Needs

Agencies and industry are working together to relieve the burden on burnt-out cyber professionals while adopting the tools to keep up with federal cyber requirements.

Contributors:

- **Beau Houser**
  Chief Information Security Officer, U.S. Census Bureau

- **Jeffrey Lush**
  Chief Information Officer, Air University, U.S. Air Force

- **Martin Nystrom**
  Vice President, Product Security, Lumen Technologies

As the cyberthreat landscape constantly evolves and federal networks face increased vulnerabilities with remote workers and outside connected devices, cybersecurity professionals are being stretched thin. They're trying to keep up with new mandates, reporting requirements and complex threat environments while system security alerts pop up left and right. As the war for talent continues and budgets remain constrained, these professionals are burning out.

Government and industry leaders spoke at a recent FedInsider panel to discuss the changing cyber environment, and how to deal with it using automation and advanced security solutions to relieve the pressure on cybersecurity staff. The following are some of the most important aspects of their discussion

The Power of Zero Trust

Adopting a zero trust architecture has become an important component of cybersecurity frameworks in government and industry. At the Air Force's Air University, it helps manage who is accessing what system and why. "That threat of having one person have access to multiple systems or multiple people having access to multiple systems at levels where they can do damage to the environment, it's just a threat that we don't need any more," said Air University's Chief Information Officer Jeffrey Lush. "We are really working very hard to consolidate all of that level of access." With zero trust, Air University is reducing risk by decreasing the number of people that have high levels of access to its systems, and it's developing a process and a budget in order to implement these solutions.

At the U.S. Census Bureau, the true power of zero trust is its access control, and its ability to enable the agency to leverage more tools in its toolbox by getting more granular with user attributes, according to its chief information security officer, Beau Houser.

"We can incorporate more detail around device attributes and we can get to the point conceivably to say, 'to get the access you are talking about, you've got to be the right person . . . and you have to be on the right device,'" Houser said. If that user isn't on the right device from the right geolocation, it is likely an attempted phishing attack or unauthorized user with authorized credentials. "We can stop them and interrupt that kill chain if we incorporate those additional details. It's very, very flexible but sophisticated," Houser said.

Intelligence-Based Cybersecurity Decision Making

Cybersecurity intel has become a key component in cyber defense, especially when typical defenses can fall short. "Intel really brings a whole other aspect to the conversation," Houser said. The Census Bureau has a team of cyber intelligence analysts who understand the nature of the Census' business, the information it handles and its threat landscape. Cyber analysts look at nation state actors, the cyber tactics they're using, why they're targeting certain information and how.

"If we have an actor, say we have a cybercriminal that is targeting PII, obviously that's interesting to the Census Bureau," Houser said. "We want to know exactly how they are doing that as an active event happening on the internet and then we feed that information to our cyber hunters. Our cyber hunters turn that intel into fingerprints and telltale signs of what that looks like within the Census environment."

That intel becomes a proactive monitoring tool for its security operations center. The Census Bureau confirms its environment is clean against those specific attacks. None of that can happen without that intel driving those processes. "Defense in depth is very important," said Houser. "But the intelligence driven model is now becoming the lifeblood of modern programs."

The Burnout of Cyber Professionals

Many factors are hardening the burden on cyber professionals: Advanced cyber tactics, complex cyber threat landscapes, federal cyber-related requirements, requirements around zero trust parameters and more.

"All of us have missed holidays, birthdays or weekends in dealing with threats and outbreaks. This is a difficult job," said Martin G. Nystrom, vice president of product security at Lumen. "You are usually only blamed for what goes wrong and rarely rewarded for what goes right." Along with burnout, this already-difficult industry is also facing a labor shortage and a war for top-tier cyber talent.

In response, Nystrom recommends leveraging application program interfaces and cloud services to build automation tools that can replace burdensome tasks that security operations teams are responsible for. "It can present a more complete investigation in the hands of that analyst," he said. "They don't have to click and click and click in order to find all of the data."

Data can also be automatically collected and presented to the analyst so that they can move a lot faster than they would if they had to collect the data themselves. Then, machine learning can be applied across the data set to discover important bits that may have been overlooked with human eyes.

According to Nystrom, this method, "actually takes these jobs that perhaps at one time might have been a lot of clicking and typing, and are now thinking," he said. "We are respecting the knowledge and education of our staff by presenting a more complete picture to them, automating that workflow so they can do the job and we together can protect America's data."

Transforming Environments to Fit Today's Cyber World

Agencies are focusing on cloud-based services to provide the flexibility and capabilities to improve cyber defense and reduce the burden on cyber professionals. "Implementing stronger cyber controls and using cloud-based services are huge when it comes to removing the workload and making your folks more deployable and more agile," Lush said. In a cloud environment, Air University can deploy secure applications to airmen around the globe in a controlled environment with managed access controls already in place.

At the Census Bureau, cloud is ushering in opportunities to adopt artificial intelligence and robotic process automation by leveraging cloud service providers, Houser said. This can prompt automated detection alerts when there is a suspected unauthorized user.

Improving the performance of security operation centers and turning to DevSecOps are also a part of this transformation. Constant SOC detection and threat hunting is a 24/7 need. And if a threat is found in the data stream, it will be escalated to the top for the more seasoned personnel to investigate.

This requires someone to constantly monitor the SOC, another workforce challenge in today's talent climate. That's where SOC-as-a-service comes in — Lumen can co-manage or outsource SOC services equipped with automation to detect threats in real-time. "The SOC needs to have the time and maturity to be able to look at sophisticated threats... that's why automation and personnel are so key," Nystrom said.

The cybersecurity landscape is not going to get any less challenging for federal agencies, but by following a holistic approach like the roundtable speakers advocated, defenders can begin to level the playing field. And that will go a long way to helping out in the ongoing battle as agencies work to keep their data, users and networks safe from threats.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

LUMEN

Lumen Public Sector
4250 North Fairfax Drive
Fourth Floor
Arlington, VA 22203

(888) 597-2455
Lumen.com/Public-Sector
Lumen Public Sector
@LumenGov