GovCIO
MEDIA & RESEARCH

DeepDives

Cybersecurity's Future RELIES ON AUTOMATION

INSIDE:

SPONSORED BY

maximus

GovCIO
MEDIA & RESEARCH

From the writer's desk

Sarah Sybert, Staff Writer

Cybersecurity's Future Relies on Automation

The threat landscape is evolving at a speed too fast for humans alone. With more cyber attacks, large-scale supply chain vulnerabilities and advanced ransomware threats, organizations must use automation to keep their security up to speed with the rate of change.

Federal agencies are embracing automation in new approaches to digital transformation. Plus, it's showing promise in helping alleviate the cyber workforce shortage by reducing time consuming manual work. In addition to the growth of attacks, organizations are faced with shortages across the cyber workforce and budget limitations, making automation even more critical to reduce time-consuming tasks and see the greatest return on investment.

Automating systems to detect cyber threats will improve organizations' threat intelligence to better plan and defend against future attacks. By leveraging automation, organizations can easily build automated workflows to expand cybersecurity strategies as the threat landscape shifts. Automation is no longer a reward at the end of digital transformation journeys, but an enabler to mature IT modernization and security.

Table of Contents

Katherine MacPhail, Staff Writer

Nikki Henderson Staff Writer

Automation Drives Cybersecurity Innovation at ICE

The agency implemented 'SOAR' to streamline key security areas.

BY KATHERINE MACPHAIL

In order to keep pace with the growing number of cyberattacks, government can't rely upon its cyber workforce to do all the leg work. Automation is a critical component to effective monitoring and incident response.

"When you look at the latest attacks and the sophistication that the adversaries are using, you can't be successful without implementing some sort of automation," said Rob Thorne, CISO for U.S. Immigration and Customs Enforcement (ICE). "There's such a large amount of event log data that we're collecting, and to have to go through that without automation — you're just not going to be able to stay ahead of the adversary."

Photo Credit: Ar_TH/Shutterstock

From patch management to routine scanning, ICE looks at its cybersecurity tasks for processes that are simple, time-consuming and repetitive to find what might be a good candidate for automation. Automating these processes can help cyber teams identify threats more accurately, understand relative risks and ultimately respond faster.

"The goal is to reduce the load that we have on our already burdened staff," Thorne said. "We want to make certain that they can focus on those risky events that we really want them to focus on."

Thorne said ICE benefited from implementing a security, orchestration,

Rob Thorne

CISO, ICE

automation and response (SOAR) capability. SOAR is a collection of software solutions and tools that allows organizations to streamline three key areas: threat and vulnerability management, security incident response and security operations automation.

In particular, Thorne found SOAR to be instrumental in reducing fatigue. There are massive amounts of data for analysts to parse through, but automation can help pinpoint the highest risk alerts.

"Fatigue is a reality, and we have to deal with that going forward," Thorne said.

Most critically, SOAR has helped ICE integrate its security capabilities; including scanning results, EDR activity and SIEM. This integration initially prompted ICE to adopt SOAR. Automation can drive powerful tools, but those tools ultimately have to enable the people operating them.

"About five years ago, I went out to the West Coast and I sat down with an analyst," Thorne said. "He was walking me through a potential incident that he was working, and he had to cut and paste and log into different systems and move things around and pull data to create a story. And I said, 'Oh my goodness, I can't believe you guys are doing that.' So that's when we started our journey to implement a SOAR product. And it paid off in dividends."

“Fatigue is a reality, and we have to deal with that going forward.”

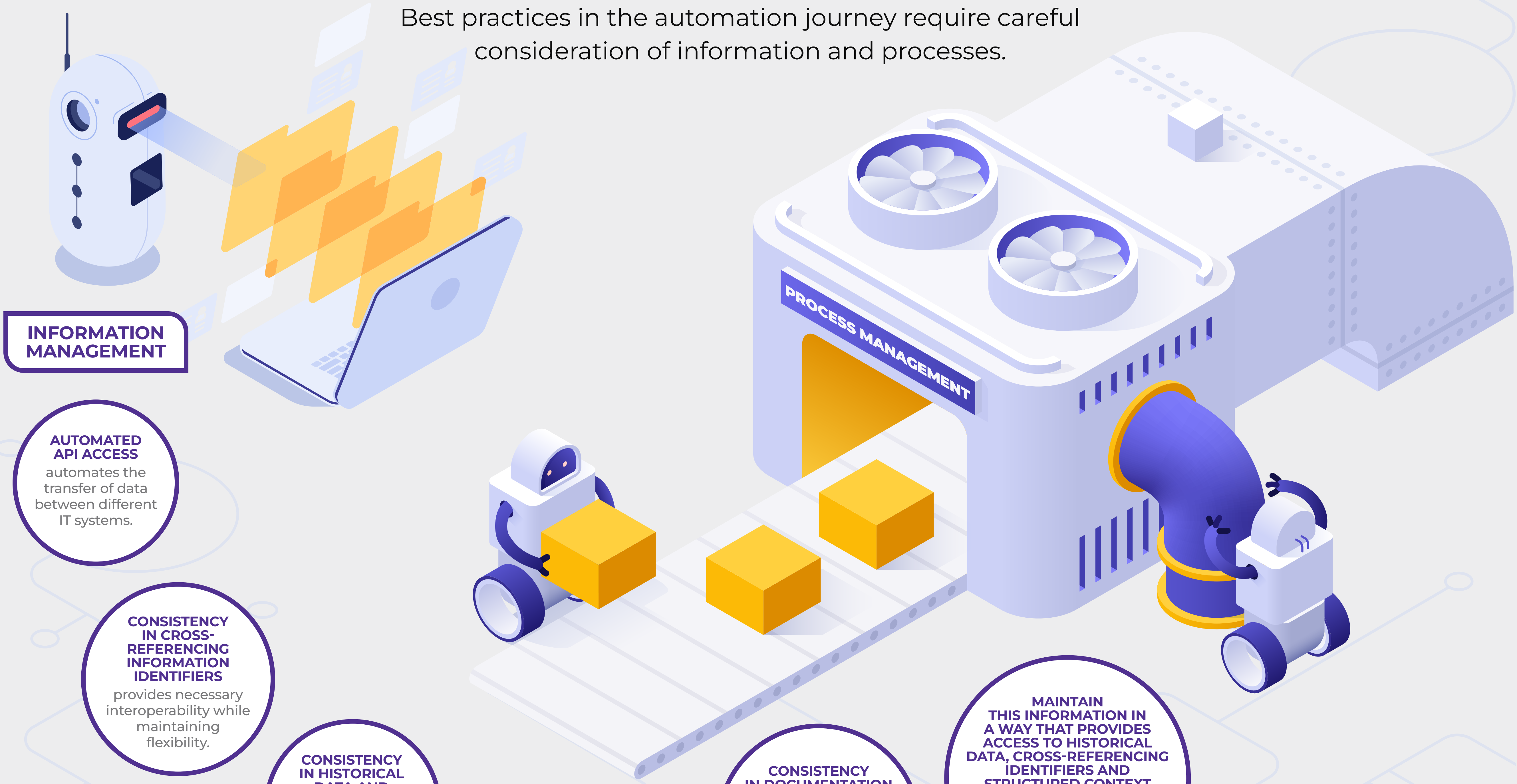
—Rob Thorne, CISO, ICE

GovCIO MEDIA & RESEARCH

DeepDives

The Path to Automating Security

Best practices in the automation journey require careful consideration of information and processes.



INFORMATION MANAGEMENT

AUTOMATED API ACCESS automates the transfer of data between different IT systems.

CONSISTENCY IN CROSS-REFERENCING INFORMATION IDENTIFIERS provides necessary interoperability while maintaining flexibility.

CONSISTENCY IN HISTORICAL DATA AND METADATA enables leaders to make informed operational decisions.

PROCESS MANAGEMENT

CONSISTENCY IN DOCUMENTATION OF CLEARLY DEFINED STAGES OF OPERATIONAL PROCESSES provides greater visibility into the role and functions of systems.

MAINTAIN THIS INFORMATION IN A WAY THAT PROVIDES ACCESS TO HISTORICAL DATA, CROSS-REFERENCING IDENTIFIERS AND STRUCTURED CONTEXT cuts down on siloed information and systems, enabling repeatable and reliable processes.

Source:
Johns Hopkins Applied
Physics Laboratory

PARTNER INTERVIEW

maximus

Detect and Respond to Threats with Intelligent Cybersecurity

Today's advanced security threats require a new tech approach.

Roger Colón, Principal Architect, Maximus

What are some of the changes you've seen in the cyber threat landscape?

Colón The increased complexity of today's IT infrastructures, coupled with increasingly sophisticated tools and attack methods by cyber adversaries, has significantly changed the cyber threat landscape in recent years. As agencies continue to embrace digital modernization to enable remote workforces, cloud services and "internet of things," these modernizations are increasing the volume, velocity, variety and veracity of data being generated. These changes are all creating new pathways for cyber adversaries to exploit, requiring agencies to identify risks faster in order to minimize the attack vector.

For example, Maximus helps our customers by dynamically integrating AI, machine learning and other automation technologies to protect critical assets and data — regardless of where they reside. By shifting from a stagnant to an active, intelligent cybersecurity posture, we are helping our customers become more resilient against today's advanced threats.

(ctd.)

> “To leverage automation to its full potential, agencies should have a contextual understanding of the technology to strategically plan for the successful implementation of automation into their security environments.”
>
> Roger Colón, Principal Architect, Maximus

What are some of the benefits of using automation in cybersecurity strategies?

Colón Automation provides many benefits, but one of the biggest is the acceleration of threat detection, response and remediation. Tools like security information and event management (SIEM) leverage automation to quickly collect, analyze and identify potential threats — automatically alerting security teams to potential risks. To further harness the power of automation, integrating additional security tools, like security orchestration, automation and response (SOAR), provides a deeper level of threat intelligence through the automation and orchestration of threat response and workflows.

For example, Maximus helped a current customer enhance its IT audit program by integrating SIEM and SOAR technologies to automate event log monitoring and incident response, providing a real-time dashboard view of correlated alerts based on risk. This significantly improved its security teams’ threat response times.

How can automation support zero trust strategies across government?

Colón For zero trust to be successful, agencies must continually identify and verify who or what is requesting access to their enterprises. Automation is a critical component in zero trust strategies as it enables agencies to do this dynamically, automating the identification and enforcement of strictly defined policies, rules and processes. With automation, security teams can dynamically scale and adapt — rapidly detecting threats, prioritizing security alerts, and granting or restricting access to critical data and assets. This saves security operations teams significant time and resources, reduces risks of human error and ultimately saves considerable costs.

(ctd.)

Where do you see areas for improvement when leveraging automation for security?

Colón As with many emerging technologies and tools, automation does not provide a one-size-fits-all solution for better cybersecurity. To leverage automation to its full potential, agencies should have a contextual understanding of the technology to strategically plan for the successful implementation of automation into their security environments. This is an area where Maximus is most passionate. We help our customers understand their security postures and strategically identify where automation can achieve the greatest success. By working closely with our customers, we help them prioritize their long-term objectives while enabling immediate success leveraging advanced technologies, such as automation, AI and machine learning.

GovCIO
MEDIA & RESEARCH

CISA, DOE Promote Automation to Help Detect Cyber Threats

Automation has played a key role in helping improve cybersecurity processes, but workforce constraints still hamper efforts.

BY NIKKI HENDERSON

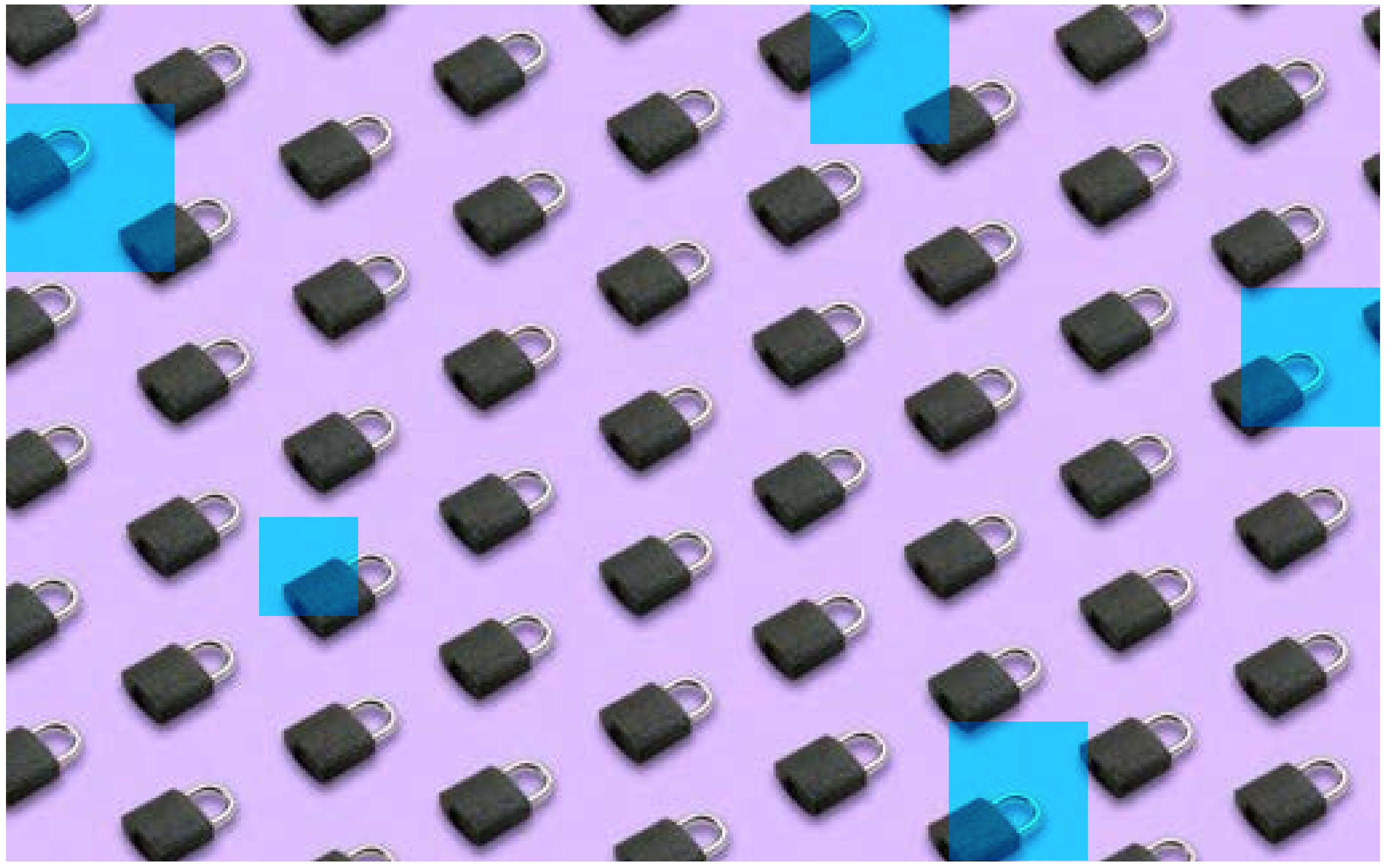


Photo Credit: OlgaKan/Shutterstock.com

Cyber leaders at the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE) believe automation can make dramatic improvements to threat detection and vulnerability management processes at federal agencies, but the cybersecurity workforce shortage still challenges federal agencies' overall cyber health.

According to CISA Tech and Cyber Strategy Lead Daniel Bardenstein, detection is one of several areas where agencies should be placing more emphasis as they try to strengthen their security posture.

"Detection of threats, detection of assets and detection of vulnerabilities. Automation is very flexible. It provides many different ways to get better visibility around what assets and vulnerabilities are so the agency has a sense of what it is that needs to be fixed," Bardenstein said at a recent FCW event.

Once a particular threat has been detected, the next steps are finding out what assets were impacted, who owns the assets, and then identifying the vulnerabilities.

Bardenstein said vulnerability management is often overlooked in cyber strategies, but can be heavily automated to reduce the burden on cyber professionals.

"Process automation across IT systems can make a huge impact and save a lot of people's time to make phone calls or look up other resources," Bardenstein said. "If people in their normal jobs can identify things that they can do all the time and repeat all the time, that is a good place to start automating. Just focus on the processes that people do over and over again."

CISA is also trying to integrate existing technologies to have a common analytical environment, especially within the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program.

"We're also launching EDR — the endpoint detection response effort — and a couple of other host-based initiatives that will provide additional degrees of both detection and automation to departments and agencies to help them

Daniel Bardenstein

Tech and Cyber Strategy Lead, CISA

better stay protected from threats," Bardenstein said.

The SolarWinds, Colonial Pipeline and Log4j software breaches highlight that no organization or sector is immune to cybersecurity vulnerabilities.

According to Energy's Puesh Kumar, director of the Office of Cybersecurity, Energy Security, and Emergency Response, the agency is focused on increasing the visibility of threats targeting critical infrastructure through risk analysis, detection, discovery and mitigation efforts. One thing it's looking at is how to quantify cyber risks.

"We feel it's a foundational thing in terms of how you actually invest in cybersecurity," Kumar said. "We're partnering with NIST to think through cyber-risk modification efforts and how to connect cyber risks to financial risks so we can better invest in this area as a company across the board."

Another project DOE is working on is determining cyber base lines for critical infrastructure sectors.

"In some cases, they will be different for each sector, and there may also be some commonalities where there's an expectation of baseline cybersecurity that we should think about and how do we educate companies of all sizes on that," Kumar said.

Securing software supply chain remains a top priority for DOE. Kumar wants to set common software supply chain security standards across energy sectors to improve cyber postures.

"We're developing a framework for what that can look like for energy systems so that we don't have multiple variations of [software bills of material] and [hardware bills of material]. If we can develop a template, it will make it easier for energy companies, manufacturers and suppliers," Kumar said.

In addition to workforce constraints, Bardenstein said retention and the high volume of data has caused many federal agencies to hit a tipping point as they move IT systems and data to the cloud. He said computers should do what computers are good at, and human workers should focus on more

> **“Process automation across IT systems can make a huge impact and save a lot of people’s time to make phone calls or look up other resources.”**
>
> **—Daniel Bardenstein, Tech and Cyber Strategy Lead, CISA**

challenging work.

“We’re at a tipping point where people are starting to realize that there’s no way we can actually handle all of this,” he said. “A softer skills side of cybersecurity, where automation can often be most valuable to an enterprise, is in the area of a ‘Tier 1’ security analyst where humans take more steps. Tier 1 life is very difficult, there are mental health issues and a lot of burnout, which is not good for the employees or the enterprise that continuously loses talented personnel who try to promote elsewhere to make more money.”

Instead of trying to automate processes all at once, Bardenstein encouraged federal agencies to adopt a “spectrum” approach to automating data and security processes.

“There is a maturity model that you can think about across that spectrum. Enterprises should be thinking about how they can continuously find the right way they need to operate move to a more mature approach to automation in their environment,” Bardenstein said.

CISA is in the process of operationalizing automation to address staffing needs and changes. In a security context, automating identification and detection workflows is a good starting point.

“Most people are concerned about automation when it comes to mitigating actions. Figuring out if something has changed, gathering additional information and presenting it to a user is a much safer place to start connecting those APIs and testing things out,” Bardenstein said. “You can have an identification, detection and enrichment playbook and then have a human in the loop to decide what to do. It’s important to understand where that risk and concern is around deciding what to do and automate everything in front of that and then if applicable everything after that.”

Two years ago, DOE established a fellowship for middle- and senior-level cybersecurity and operations managers from U.S. electricity, oil and natural gas companies to help fill talent gaps in the cyber workforce.

“Let’s bring together power systems engineers and electrical engineers and maybe teach them cyber and then bring cyber individuals to the table as well and have a cross pollination of information so they can all work on this together,” Kumar said.

DOE is also investing in academia to mature cyber workforce development programs.

“Students participate in a competition called ‘Cyber Force.’ They come from all across the country and go to DOE laboratories where their goal is to protect a mock energy company while a red team tries to attack them,” Kumar said. “They learn about cybersecurity and about energy systems and what makes them unique.”

DOE hopes to expand the program to high schools in the future, he added.