Securing Your Environment with Automation

Highlights from the Federal Law Enforcement Summit

MISSION BRIEF

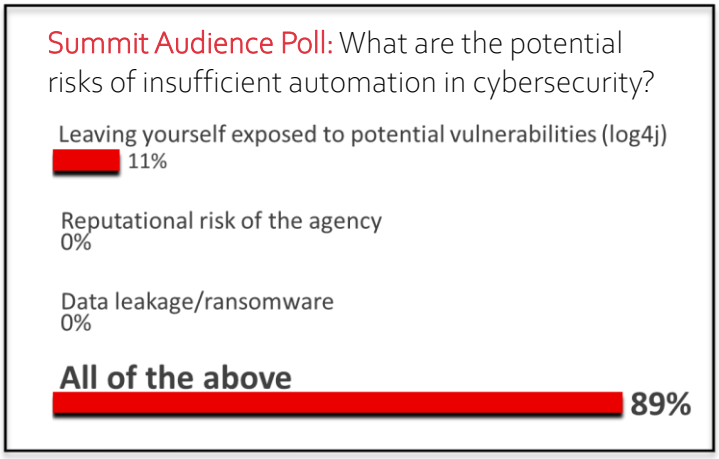
During a recent virtual law enforcement summit hosted by the Advanced Technology Academic Research Center (ATARC), in partnership with Red Hat and Carahsoft, federal government leaders discussed opportunities and challenges when using security automation to enable Zero Trust architectures.

"I think, therefore I automate," Bill Kirkendale, the *Chief Information Officer* for the Courts Services and Offenders Supervision Agency for the District of Columbia, quipped in the opening remarks of a multi-agency panel conversation on the use of security automation in federal law enforcement agencies. Automation is implicit in achieving Zero Trust. Network capabilities and hacker sophistication is far too great for humans to keep up with cybersecurity without the use of automation tools. Automation helps agencies meet Zero Trust mandates while creating efficiencies in both business functions and service delivery.

> *I think, therefore I automate."*
>
> Bill Kirkendale
> *CIO*, Courts Services and Offenders Supervision Agency for the District of Columbia

There are a vast number of tools and technologies available that support business process automation, but agencies often face challenges with proper and efficient integration. With minimal executive guidance on cybersecurity best practices, and sporadic assistance from solution providers, many agencies feel overwhelmed by the need for automation and the number of offerings available. Kirkendale noted that, "it's not as easy as buying one tool to automate processes and creating security. The challenge is to connect many aspects to create a holistic picture of what is going on with a system."

The importance of connecting systems, networks and processes through automation is a recurring theme amongst panelists. In an audience poll question, 89% of respondents agreed that not having sufficient automation for cybersecurity could potentially be costly in exposure to vulnerabilities, reputational risk to the agency and data leakage and ransomware threats. Further conversation explored the integration of automation in data security, identity verification, risk management and mobile security, and the importance of maintaining a skilled workforce.



Automating the Agency Mission

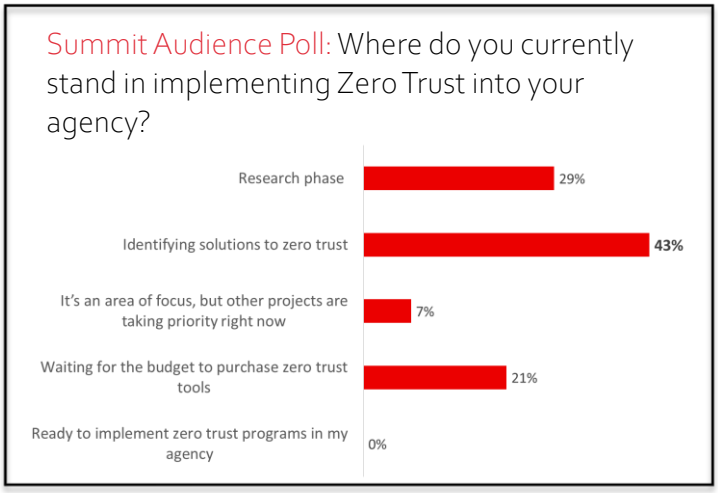
The administration's Fiscal Year 2023 budget allocates $11 billion toward civilian cybersecurity spending, an 11% increase from the year before[1], indicating shifting priorities to bolster security postures throughout the government. Additionally, a recent survey of public sector respondents found that 32% already use automation tools in some way in their work. 67% say that these automation tools reduce stress among security personnel, while 70% say automation helps security personnel focus on critical vulnerabilities[2].

As the federal government continues to prioritize cybersecurity, security automation is becoming increasingly critical. United States President Joe Biden's Executive Order on Zero Trust included a section on automating security responses, a process

[1] https://www.cybersecuritydive.com/news/biden-2023-budget-cybersecurity/621264/

[2] https://gcn.com/cybersecurity/2020/02/government-revs-up-it-security-automation/291165/

OMB calls a 'practical necessity' for both business needs and data protection. In just the last few years, process automation technology has advanced quickly. Agencies are incorporating intelligence automation more frequently to improve business processes such as machine learning, image recognition and natural language processing. As process automation continues to advance, agencies will be able to apply these more easily to security challenges and DevSecOps. This is an imperative in today's IT landscape as there are now more than 600 known exploited vulnerabilities – and that number is still rising.



The U.S. Department of Homeland Security (DHS) relies heavily on automation to achieve national security goals, to meet Zero Trust mandates and improve business processes. Eric Sanders, *Chief Information Security Officer* with the Office of Intelligence and Analysis at DHS, notes that the agency uses automation to assess new capabilities quicker and to automate more simple, repetitive tasks in order for personnel to focus on larger, high-stake issues. Many panelists mentioned that automation helps their agencies achieve service delivery and deployment goals by bringing more services to the end users with ease.

Automating Security Tools

Reports show that organizations use anywhere between 10 to 40 different security tools at a given time[3]. Sebastian Dunne, *Principal Solutions Architect* at Red Hat, shared that using that many disparate tools not only has a budget impact, but can result in a diminishing return on those technology investments. Another challenge is in the number of skilled IT staff required to administer and maintain each system. This can be particularly problematic when security tools operate in separate teams without cross-system or cross-team collaboration. Dunne emphasized that successful automation of security must occur enterprise-wide across silos and disparate teams.

When asked about the role of vendors pushing new tools onto agencies as a contributing factor to the rising number of tools in use, Dunne shared that some technology manufacturers, such as Red Hat, emphasize a more holistic solution integration approach to help agencies achieve business goals. Eric Sanders with DHS added that while most federal agencies face budget challenges that can often prevent the integration of new solutions, the primary focus agencies should take is understanding the operational context of a given system in relation to a new tool.

Having a strong understanding of the operational context of a given system including existing gaps in technology, infrastructure and the potential risks and vulnerabilities associated with incorporating a new tool, is the only way agencies will know if the solution will be effective. While there are many automation technologies available, agencies must first have a real-time understanding of their security posture and Zero Trust mandates. This process can take time to not only gain a full understanding of an agency's needs, but to also ensure the existing workforce can make the necessary updates and changes to their environment.

> *"We look at Zero Trust as a strategy and an enabler to modernize our network and get the latest and greatest technology to our law enforcement officers. Our mission space wants technology to be agile. They want to have data at their fingertips, whether they're in the office or out in the field."*
>
> Rob Thorne
> *Chief Information Security Officer*, ICE / DHS

Skilled Workforce

Rather than viewing automation as another tool to incorporate, Red Hat's Sebastian Dunne postulated that automation should be considered a resource for developers rather than a burden.

[3] Summary of Gartner's Top Security and Risk Trends for 2021

If automation is integrated correctly, metrics should indicate that IT personnel has more time to work on higher level issues.

However, as Eric Sanders notes, hiring people with correct skill sets is challenging, especially when agencies allow technology capabilities to come before the expertise of security personnel. Agencies often play catch up to secure a skilled workforce capable of operating new tools after initial integration. Not only is the recruitment of a skilled workforce challenging, but also retaining those high-level IT security professionals.

Moderator Jason Miller quoted a statistic that 86% of all cybersecurity postings attract fewer than 10 applicants today, and hiring would need to increase by 41% to meet all job openings. Because there is chronic understaffing of security personnel, it is more critical now than ever to integrate automation in cybersecurity efforts and emphasize the cultural shift required to foster a common understanding of security goals while implementing a successful Zero Trust strategy.

Data Security and Identity Verification

All speakers agreed that automation is implicit in Zero Trust. For agencies to meet the 2021 Zero Trust mandates, automation must be incorporated to some extent, whether through multi-factor authentication (MFA) or federated identity. For government agencies as large as DHS, Sanders suggested that achieving Zero Trust must be approached from an enterprise perspective, particularly if it involves the cloud.

> *I see automation playing a huge role in identity and access management."*
>
> Eric Sanders
> *Chief Information Security Officer*, I&A / DHS

Dunne agrees that automation must be incorporated early and at every stage, particularly when moving data to the cloud. He argues that if agencies are not automating as data is shifted to the cloud, the full value will not be realized. The same holds true with Zero Trust and the basis of verifying and validating individual users. He notes the only way to verify every individual's identity is for all aspects of a system to be configured the same way and speaking the same language. And the only way to achieve this is through automation.

Michael Epley, *Chief Architect and Security Strategist* at Red Hat views Zero Trust from the perspective of individualizing access controls for every user and resource that agencies interact with. Agencies must make new access decisions each time, which is turning the traditional security model on its head. Previously, agencies relied on implicit trust where users are authenticated once or have access to a system by connecting to the Internet via a corporate network. Agencies can no longer rely on implicit trust for complete security. Instead, users must be verified with every new interaction. Automation plays a critical role in making Zero Trust not only acceptable to users, but also possible for system-to-system and non-person interactions within those systems.

As Rob Thorne, the *Chief Information Security Officer* at Immigration and Customs Enforcement (ICE), DHS, notes, "There's really not a universal agreement on exactly what Zero Trust means or how to implement Zero Trust itself. It really depends on your environment… and the amount of funding that you have." For ICE, Zero Trust is a strategy to enable modernization of networks and law enforcement technology. The agency has quickly been able to move away from inflexible capabilities, such as virtual private network (VPN), and towards a secure service edge methodology. For ICE to achieve its mission, technology needs to be both agile and secure.

Risk Management

When agencies evaluate risks to systems, applications and supply chain, automation and data-based decision making can help balance and mitigate these threats. Automation adds a sophisticated level of security for certain classified data to maintain high levels of privacy. It also provides real-time visualization of existing and potential risk to help accelerate defense response times. Unfortunately, due to current lack of embedded automation in their security strategies, there are many scenarios when identity can be compromised.

Automation is and will continue to play a large role in identity and access management (IAM). Ensuring that only trusted users are in classified systems was a priority in terms of automation in the past, but the reality is that Cyber Threat Actors (CTAs) get continually more sophisticated. Sharing domains opens agencies up to external threats from lower-level environments. As Throne points out – once threat actors breach a perimeter, they can then move laterally within an organization. Automating Zero Trust and monitoring security at this level is what will protect networks and agencies from the increased sophistication of attacks.

By automating certain aspects of security, security personnel are free to identify higher level vulnerabilities. Dunne states, "...the sooner we are able to detect vulnerabilities and then automate the remediation of those vulnerabilities...we're closing that window where our systems are the most vulnerable." He continues, "...automation can help with risk management and our overall security posture." Not only is automation capable of identifying vulnerabilities, but also existing exposures that if not identified quickly can have dire consequences.

Mobile Security and Zero Trust

Historically centric to traditional networks and personal computing, the federal government's cybersecurity focus is shifting to mobile security. Vincent Sritapan, a *Section Chief* within the Cybersecurity Division of the Cybersecurity and Infrastructure Security Agency (CISA), believes that mobile technology is a prime candidate to help get to Zero Trust faster, because unlike traditional networks or even cloud, mobile devices run on networks that agencies do not control.

Special consideration should be given for Zero Trust in the mobility landscape due to factors like app isolation and micro-segmentation. Because of the ubiquity of mobile device architecture and configuration, automation is used often in mobile devices to build high confidence through application security testing, mobile application vetting, workflow automation and automation's integration in mobile threat defense. Despite major platform providers building many Zero Trust protections into mobile devices, they still pose different attack vectors over cellular or traditional WiFi networks, which render mobile devices particularly vulnerable to lateral attacks.

Red Hat's Michael Epley agrees that the intersection of lateral movement and mobile devices demonstrates why agencies need Zero Trust to continually reauthorize devices. Even if the device itself isn't compromised in the application or the network, another component on the device or even the user could be. It's important not to rely on the device boundary, network or Wi-Fi connection as the primary means of isolating that device from agency enterprise systems. Attackers look for the weakest link as a way into an enterprise, so when considering the role of Zero Trust in mobility, there are several ways to incorporate improved security practices on devices. Sritapan offers examples like a device enrollment program to ensure that the security of the device builds confidence, enforcing configuration management policies through Mobile Device Management (MDM) and building it into workflows to allow for and deny listings through application testing.

Government employees want the same experience and capabilities on a mobile device, as they get on their work computer, but that presents significant security challenges. By incorporating Zero Trust into mobile security, users will have a more cohesive experience regardless of location. Another challenge agencies face when implementing Zero Trust in mobile security is the orchestration of security automation with traditional networks, because mobile security ecosystems often operate independently of one another.

Getting Started with Security Automation and Zero Trust

The best approach to security automation is to just start somewhere. Dunne encourages agencies to, "Just get started. Automation is one of the few IT projects where you don't have to 'go big or go home'. You can start right now and use automation as a point to start solving problems."

> *Just get started. Automation is one of the few IT projects where you don't have to 'go big or go home'. You can start right now and use automation as a point to start solving problems."*
>
> Sebastian Dunne
> *Principal Solutions Architect*, Red Hat

Eric Sanders from DHS agrees, adding that agencies should begin automating processes at a lower risk level and let personnel focus on higher-level activities. Sanders ends by emphasizing the priority of integrating automation into existing processes, so agencies have a real-time understanding of potential risks and vulnerabilities associated with any new tools. ICE's Rob Throne suggests a risk-based gap analysis approach to decide what tools and capabilities are in place today, and how tools could be integrated into existing processes to meet Zero Trust mandates. Regardless of approach, automation should be embedded into each agency's strategy to help support a mature infrastructure and build out the Zero Trust capabilities critical in today's evolving threat landscape.

Learn more how Red Hat can help with automation solutions and public sector support.