FEDInsider

The Role of Automation in Federal Zero Trust Frameworks

As agencies implement zero trust architectures, they're exploring the use of automation to make processes more efficient and secure.

As federal agencies work to meet the Office of Management and Budget's zero trust mandate to improve cybersecurity, they're also exploring how automation plays a role in a zero trust architecture. The National Security Agency also named automation and orchestration key pillars of zero trust, stating in its final report that, "organizations should employ automation and orchestration methods to address repetitive, labor intensive and predictable tasks for critical functions and access control."

At a recent FedInsider webinar, thought leaders from both government and industry expanded on the role of automation in establishing zero trust and how to keep it up-to-date with agency and user needs.

The State of Automation in Cybersecurity

"Over the last couple of years, there has been a tremendous shift toward generative artificial intelligence. GenAI tools have been added to pretty much everything under the sun, and now we really do not encounter any tools — any systems — that are not somehow AI-enabled," said Donald Yeske, director of the National Security Cyber Division at the Department of Homeland Security.

The DHS is following suit. Yeske said the department is hiring AI analysts, named the first chief AI officer in the federal government, published guidance on the responsible use of AI and more.

Specifically, machine learning is being used in cybersecurity to comb through logs and events, determine trends and patterns, and detect adversarial actions and suspect activities. Automation tools stacked on top of these capabilities take relevant actions in response to events that it can perceive to happen in the environment — like a threat materializing or finding a vulnerability.

AI is also used in security code and risk identification. "You have to think about cybersecurity at the beginning of a project, and generative AI has proven to be tremendously useful for the development of code," Yeske said. "It makes development more approachable, it lowers the barrier of entry and it can accelerate that task."

Still, Yeske stated that DHS has hit its limits with what it can do with AI due to limitations with data and scaling hardware. "What it comes down to is using the right tools for the right jobs," Yeske said.

When it comes to solutions, Michael Hardee, chief architect at Red Hat, said it is crucial to integrate automation into Red Hat solutions at the beginning rather than as an afterthought, or else it probably won't happen at all.

"One of the basic things regarding the value of automation in the security context is

Featured Experts:

- **Don Yeske**
  Director, National Security Cyber Division,
  U.S. Department of Homeland Security

- **Michael Hardee**
  Chief Architect,
  Red Hat

that a manual process can be influenced," he said. "At the core, zero trust is... never trust and always verify." There should be a centralized audit, but there should never be a backdoor when following an automated process. "That's one of the bigger values of removing that manual process from the enterprise," Hardee said.

Building Up a Zero Trust Framework

DHS is preparing to publish its Zero Trust Capability Framework, focusing on its protected surfaces — or protecting the "smallest thing that you can imagine and controlling that. If you lost it, you would lose the mission," Yeske said.

The DHS framework consists of 46 capabilities and is not that different from the Department of Defense's framework. It is compatible with the way the DOD defines zero trust. "We needed that level of objective definition, but we needed it to be more measurable in terms of performance," Yeske said.

The framework also doubles as a design tool, defining capabilities as people, processes and products together, not just technology. "If we define our capabilities that way and manage them that way, the question that is left is: how do I compose those capabilities best to protect my protected surfaces?" Yeske said. That's the next major evolution in zero trust architectures for the federal government, and automation plays a large role in that.

"It is not conceivable that any organization could deploy enough human analysts to do the things that need doing," Yeske said. "Automation is democratizing security operations in a way that allows smaller offices... to do things they wouldn't be able to do otherwise."

Yet automation isn't completely hands-off, Hardee said. When employing autonomous systems, there may be requirements needed that allow people to "break glass" and take action on the models. "We still have a management responsibility there," Hardee said.

"Whether it is standard automation for server provisioning or process automation, there needs to be standard refinements... with the ability to provide improved incidents response so we can rely on automation to take action, and on the human level you can investigate." This provides the ability to scale in order to offload responsibility.

The Long-Term Zero Trust Vision

Security-forward solutions are a non-negotiable. "It is no longer optional for software vendors — and almost every business in the world is a software company — to think about the security of how they build and maintain their software," Yeske said.

The DHS looks at the claims of its vendors surrounding supply chain security and internal practices, and it has a statistical model based on responses from all vendors allowing it to gauge whether or not that it's being told the truth about the practices in operation. "When you come to us, you have to claim certain things about your security and ability to control unclassified information in your context, and we will rely on those assurances and hold you accountable."

For Hardee, the future of zero trust and cybersecurity in government comes down to protecting the surface. "As the clients move to the cloud, there has been autonomy in the program area... the challenge is when you don't patch your system, it will take you offline."

Not being compliant can cause users to be taken off the network, which Hardee said can encourage improvement in processes towards enterprise standards. "Injecting automation into the pillars that we have been provided and the important work [Yeske] and his team are doing designing these capabilities... it's going to give everyone a very good roadmap on what their environments could potentially look like."

And by following that plan and adding automation whenever possible, it will empower defenders to keep their networks and data secure even as the threat landscape also evolves and becomes more challenging. According to Hardee, that is the best possible path forward for security in the future.

FEDInsider

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

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

Red Hat

Red Hat North America Public Sector
100 East Davie Street
Raleigh, NC 27601

(888) RED-HAT-1
infrastructure@RedHat.com
RedHat.com
Facebook.com/RedHat
Linkedin.com/company/RedHat
@Ansible