Today's threats demand faster response, tailored strategies

As attacks accelerate, federal agencies are turning to intelligent analytics as a defense.

Cybersecurity is a war on multiple fronts involving a vast range of potential threats and vulnerabilities. They can be internal, whether intentional or inadvertent; and external, from lone individuals, organized endeavors by adversarial nation-states. The commonality on the front of every cybersecurity war are data and analysts.

With the high volume of data coming in and the finite resources available to federal agencies, "we have to find a solution that's not just about workforce. We have to be able to out innovate and outthink our adversaries," said Roy E. Horton III, Noblis' cybersecurity senior manager.

Speaking at a virtual workshop cosponsored by Noblis and FCW, Horton said these challenges are also opening space for opportunity. "Convergence, all of these things coming together—automation, the need for AI and ML—drives us toward changes," he said. "Seeing the alert come in and then responding is no longer an effective way to do business. Now we have to know why that alert came in, what it means, and the impact for the network. Our analysts can't get to those questions if we don't have a good automated system to help them discern the volume and velocity of data coming in."

Noblis is a nonprofit science and technology strategy organization dedicated to creating innovative, forward-thinking technical solutions that serve the public interest—in an environment of independence and objectivity. Noblis works with a wide range of federal entities, and its research program is driven by agency missions. The September event, *Cyber Analytics at Mission Speed,* featured speakers from cybersecurity stakeholders across the federal government.

The volume, velocity and variety of cybersecurity threats are quickly out pacing standard-issue threat detection solutions. Federal agencies must manage and stay ahead of these ever-shifting threat vectors and the obfuscation of threat origins and intentions—and they must manage this in a workplace in which security perimeters have expanded drastically to accommodate a remote workforce. Add to this the rising amount of data collected, organizational silos, workforce limits and issues around trust in information and organizations, and agency missions seem increasingly difficult to achieve.

For NASA, the exponential increase in data volume resulted in bringing more automation and AI to data so that humans could focus on providing insight and value, said Karim Said, CISO at NASA headquarters. NASA has historically been a highly decentralized agency, with partnerships across government, the private sector and NGOs, and it deals with massive amounts of data and sprawling networks.

Rather than looking at cybersecurity in large-scale transformative actions, The NASA CISO said, the most important and beneficial changes and the ones that have the greatest payoff are iterative and incremental, not always glamorous. "I don't want to draw attention away from actual mission successes occurring at NASA. … Cybersecurity is a support organization and we'll be working tirelessly behind the scenes," he said.

Balancing human resources and technology investments is not a new challenge, but the speed at which the cyberthreat landscape changes and

Article Source: Cyber Analytics at Mission Speed | September 2, 2020

presents new attack fronts has moved cybersecurity to the top of priority lists.

Chet Wall, technical director, 688th Cyberspace Wing, U.S. Air Force, cited a 2019 report indicating that a nation-state actor could achieve compromise and lateral movement in a network in 18 minutes 49 seconds—noting that this time has likely decreased by at least a few minutes in the subsequent year.

"We have to be improving as our adversaries are improving their techniques against us," Wall said. "If the adversary is at 18:49, we have to strive for 18:48."

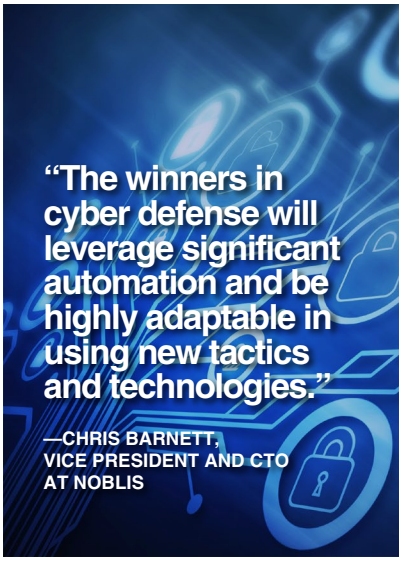
For the FBI, technical electronic data is part of every investigation whether cybercrime or not. "The volume and content of raw data, how to process that data via machine or applications, is the paramount focus of most analysis at mission speed," said Valerie Cofield, deputy assistant director, Cyber Capabilities Branch, Cyber Division, FBI.

As cyber has become a top priority, Cofield said, the agency is leveraging its unique authorities and its commitment to both mission and engagement. "We can't counter adversaries on our own," she said. As an example, she pointed to the strategic reorganization of the National Cyber Investigative Joint Task Force with the goal to assess risks and combat threats more effectively. Changes include new partnerships and stronger communications to integrate operations and intelligence across agency lines.

"It is crucial to understand the distinction between raw data and actionable intelligence," she said, and technology alone is not the solution. With the scale of data that goes into threat analytics, the FBI is working to adapt its workforce and workplace culture for a more data-centered approach.

"Mission speed requires human actions and decisions," she said. "At the end of the day, people make the determination about intelligence value."

Kyle Forsyth, a cybersecurity engineer with Noblis, explained that many federal agencies and other organizations have the same issues with triage, sifting through data and pulling from multiple tools—and when they do get to something, then trying capture how they got there in order to be able to get there again.



Rather than framing resource allocation as an improper balance between people and technology—an either/or mindset—the relationship can be restructured as one based on alignment and alliance. This can be accomplished by adopting a workflow solution that has analysts make more informed decisions regarding cyber threats, but without adding barriers between the analysts and the data.

Most analysts no longer directly access data and are using visualization tools that depend on data, Forsyth said. "Different organizations need to see things in different ways."

A tool like Artemis, the cyberdefense workflow solution developed by Noblis that helps analysts make more informed decisions regarding cyberthreats, removes the need for analysts to know specific languages.

"Queries are done through the enrichment engine, and you're able to connect to those data sources directly," Forsyth said. "The engine within Artemis captures the steps that it takes an analyst to get from point A to point B, and all of the information they receive within that. The engine can also look at those queries and decide what steps to take away from the manual process and introduce it in a more automated fashion." Having these things in place, he said, can accelerate time to action for an analyst, allowing them to be more effective.

"We've helped prioritize for rapid searches, to sift through a lot of data and get results very quickly, sometimes within milliseconds of return," Forsyth said. In addition to users getting the information they need quickly, this direct access also allows introduction of some open source tools so organizations can use resources they already have.

Forsyth said leveraging automation to free up your workforce requires fast automated tools, like Artemis, so analysts have the time and capacity to analyze this new information in the cyber warfare age.

Noblis VP and CTO Chris Barnett summarized the key points from the event: "The winners in cyberdefense will leverage significant automation and be highly adaptable in using new tactics and technologies," whether for information warfare techniques, implementing zero trust architectures, measuring outcomes and tracking metrics, or broadening communication and collaboration in the service of cybersecurity. "We're constantly investing in our research and solutions to make data science capabilities accessible to analysts, enabling mission speed," he said, highlighting that across the enterprise it is important, "always to be innovating to stay ahead of the adversary." ■