FEDERAL NEWS NETWORK

STRATEGIC GUIDANCE SURVEY:

Cyber Threat Intelligence

INSIGHTS ON CYBER THREAT INTELLIGENCE FROM:

- Navy Defense Operations Command
- CISA
- JFHQ-DoDIN
- National Guard Bureau

Brought to you by

Recorded Future®


THREAT INTELLIGENCE
FOR INFORMED ACTION
Elite intelligence tailored to your teams, processes, workflows, and existing security investments. Everything you need to reduce risk faster — without any of the noise.
Federal agencies rely on threat intelligence from Recorded Future to make informed decisions and proactively reduce risk.
Recorded Future®
www.recordedfuture.com

The Biden administration is planning on spending more than $10 billion on Defense Department cyberspace capabilities alone in fiscal 2022. The potential investment is a testament to how important cyber and cybersecurity have become to government operations.

Threat detection is a constantly evolving challenge for all government agencies, and will continue to morph in the future. Navy Defense Operations Command summed up the daunting task agencies face: "Every day, large organizations fend off millions of attempted intrusions from across the internet."

DoD and other departments are harnessing data, artificial intelligence, machine learning, zero trust frameworks and everything else to keep networks safe. Those practices and technologies help inform how contractors work with the government, and how agencies operate within cyberspace.

PANEL OF EXPERTS

Rebecca Siders, public affairs and outreach officer, Navy Defense Operations Command

Brian Gattoni, chief technology officer, Cybersecurity and Infrastructure Agency

Steven Mavica, public affairs officer, Joint Force Headquarters DoD Information Networks

Wayne Hall, media operations specialist, National Guard Bureau Public Affairs

Federal News Network surveyed four agencies about their cyber threat detection habits. This ebook highlights the thought and effort that top government officials put into finding network intruders and keeping them out of vital networks.

Jason Miller
Executive Editor
Federal News Network

Describe some of the ways your organization is using or investigating the use of automated tools to detect and mitigate cyber threats. How, if at all, do you plan to expand the usage of automation in the next 12 to 24 months?

NAVY DEFENSE OPERATIONS COMMAND

The Navy conducts defensive cyber operations (DCO) as a persistent mission executed by Fleet Cyber Command/ Commander 10th Fleet (FCC/C10F). We leverage a wide range of DCO authorities, tools, and best practices on a daily basis. DCO is primarily executed from the Navy's DCO Task Force, Navy Cyber Defense Operations Command/Commander Task Force 1020 (NCDOC/CTF1020). NCDOC also actively partners with the Naval Information Warfighting Development Center to codify and standardize the Navy's processes for conducting DCO through lessons learned, tactical memorandums, and doctrine development.

NCDOC primarily leverages three broad sets of resources to conduct DCO operations: Navy-owned networks, workstations and sensors to provide a massive volume of data that we analyze in near-real time to detect anomalous and malicious behavior. The sheer amount of data we consume in this manner requires us to employ security automation and machine learning techniques to execute DCO operations based on trends and indications that would otherwise not prompt an alert via our Intrusion Detection and Prevention Systems (IDS/IPS). We primarily interact with this dataset through the Security Information and Event Monitoring (SIEM) platform.

Additionally, we made significant strides on End-point Detection and Response (EDR). The Navy has capitalized on a pilot program in conjunction with the National Security Agency (NSA) and Defense Information System Agency (DISA) to utilize Microsoft Defender for Endpoint (MDE). MDE enables us to actively conduct DCO utilizing individual workstation-level telemetry that we are able to gather from the nearly 500,000 endpoints that MDE is currently deployed on across Navy networks. These tools allow us to search for evidence of advanced adversarial techniques, tactics and procedures (TTPs) where standard block-lists and automated alerts won't suffice. We are constantly expanding our defensive cyber sensors to acquire the data necessary to perform this task across the Navy's networks.

Due to the increasing amount of encrypted traffic on the networks of today, automated host-based detection is vital to the defense of a network. As the Defense Department and the Navy move more of our systems into the cloud, automated detection of threats in the cloud environments is critical.

It is worth noting here that we leverage relationships and contracts with industry-leading cyber threat intelligence providers to monitor threat activity. Our access to a variety of proprietary commercial intelligence feeds and datasets provides us with global awareness on attack trends, often before they are attempted against the Navy and DoD. The value of these relationships can't be overstated.

As FCC and NCDOC continue to evolve our capabilities, we will remain focused on how we gather insights from our own environment, how we collaborate with the private sector, and how we leverage the intelligence community. This is a mission we carry out day and night, around the world, and we are incredibly proud of the team that executes these operations on behalf of the Navy.

— Rebecca Siders, public affairs and outreach officer

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA uses automated tools throughout its cyber defense of federal networks and the nation's critical infrastructure. For example, the National Cybersecurity Protection System – better known as EINSTEIN – automatically scans, detects, and blocks threats to federal networks, while CyberSentry provides similar automated protection for private critical infrastructure partners. In other areas, automated tools can tackle the scanning of large cyber ecosystems or handle vast data collection, allowing analysts to use their time more efficiently and effectively. CISA's vulnerability management team is a perfect example of this. They use automated tools to scan for vulnerabilities across the .gov space, which is way too large to be managed effectively and efficiently by humans, allowing their analysts to focus on mitigating identified vulnerabilities.

CISA's technology strategy reflects this dynamic and provides a blueprint for optimizing the use of automation, in order to give our analysts more time to focus on the most challenging and sophisticated problems. In the next year, we're particularly focused on finding ways automation can help us better understand our data needs and improve our data collection. This becomes even more important as we take on the challenge of detecting threats in cloud environments. Automated behavioral analytics, for example, will allow us to tailor the development of tools and data collection directly to the operational needs of the individual analyst. We are currently exploring what personnel, processes and technology are needed to implement this approach, given the scale of CISA's mission and the enormous volumes of potential data available.

— Brian Gattoni, chief technology officer

JOINT FORCE HEADQUARTERS DOD INFORMATION NETWORKS

JFHQ-DoDIN continually seeks ways to use and improve automation to compile and analyze the vast amount of data needed to detect, assess danger and mitigate cyber threats to the DoDIN infrastructure and DoDIN-enabled assets, weapons systems and information. The sheer size and complexity of the DoDIN, coupled with the volume and velocity of malicious activity, reinforces the need for automated tools. There will never be enough resources, specifically time and personnel, to solely use manual processes to counter cyber threats at the scale we face on a daily basis. JFHQ-DoDIN, in conjunction with our DoD, intelligence community and corporate partners, utilizes a wide variety of automated capabilities to support the DoD's defense in depth, in order to defend at the speed of cyber.

Our defenses, layered at the boundary, mid-tier and endpoint, provide a robust capability to mitigate threats based on a variety of signatures and behaviors, which are informed by U.S. government and commercial threat intelligence, as well as data shared by key mission partners. The deployment of security appliances, intrusion detection and prevent systems, host based security, and other sensors allow us to feed security incident and event monitoring capabilities to monitor suspicious and malicious activity at the enterprise level. Again, the volume of activity precludes manual reviews of all suspect activity, and we rely on select capabilities to auto-mitigate activity when possible, and to alert cyber analysts to activity that requires human review.

Flexibility in how and when to use automation is key. It is fair to say that DoD uses a multi-faceted approach that incorporates automation as a main element. Cyber threat intelligence (CTI), derived from classified and unclassified sources, feed automated defensive capabilities at a variety of layers within our defenses. CTI

feeds include wholly automated ingestion of data to feed signature based detection and mitigation capabilities, as well as manual inputs from a variety of sources.

Having the capability to share information internal and external in a timely manner is also important. Automation impacts the speed of sharing. The idea is to have the ability to quickly share operational and intelligence-related information such as indicators of compromise; potential vulnerabilities in processes, software or hardware; trends in adversary behavior and other factors used in monitoring the security condition of the DoDIN. We work closely with U.S. Cyber Command, DoD components with areas of operation on the DoDIN, the DoD Office of the Chief Information Officer, Joint Staff J6, DoD intelligence community, allies/coalition partners, and federal law enforcement agencies and other federal agencies. The command is always looking for ways to improve the ability to share intelligence information and cyber operational information with partners as a way to increase speed of action in protecting DoD's technology infrastructure, the DoD assets such as weapon systems that use the DoDIN, and the information that resides on the DoDIN. There was a time when info sharing was done manually, which was ineffective and inefficient. While there is still some level of manual sharing, automation has helped make progress overall in increasing speed of sharing. Technology, specifically automation tools, have helped significantly improve these info-sharing relationships.

Our efforts over the next 12 to 24 months include several initiatives designed to improve shared situational awareness, increase our ability to see across the entirely of our cyber terrain, and to improve the ability to share cyber threat intelligence internal to DoD and across a variety of mission partners. Other efforts include automating our ability to conduct threat informed analysis of vulnerabilities at speed and scale.

One example includes refining capabilities to provide a common operating picture, fed by a variety of data sources, to provide a fused operations and intelligence picture to facilitate decision-making. Tied to this are efforts to increase our ability to rapidly and accurately see ourselves through better understanding of the DoDIN terrain. CYBERCOM's Unified Platform is key to both of these efforts, and is also critical to our ability to federate access across multiple disparate data sets, improving our ability to employ analytics to monitor, assess and hunt as required. Finally, we seek to improve our ability to quickly and accurately share indicators derived from our analysis to facilitate our partners' ability to harden and defend their networks.

— Steven Mavica, public affairs officer

NATIONAL GUARD BUREAU

The National Guard Bureau (NGB) uses several different security information and event management (SIEM) tools to bring log aggregated data in a meaningful way that varies from being centralized to decentralized analyzing to detect cyber incidents and security issues. Depending on the incident (malware, phishing, denial of service etc.) several tools have been placed at different locations across NGB's networks to accurately identify issues during scanning, as well as lateral movement of data or unknown suspicious activities. We are gradually moving to a big data platform (BDP) to facilitate a one-stop shop for all data from multiple locations. This will enable all security protocols in place to filter and ensure only authorized data is shared and stored.

— Wayne Hall, public affairs and media operations specialist

Understanding the sensitivities of the topic, please describe the current level of automation in your threat detection and mitigation processes. How would you characterize the quality of automated processes versus manual ones? To the extent you have used automated processes, are there any success stories you can share, even in general terms?

NAVY DEFENSE OPERATIONS COMMAND

We use our SIEM capability to aggregate, automate, and accelerate our Cyber Event Reports (CERs) so that our analysts are not spending the majority of their time learning the multiple tools and disparate workflows, and manually creating CERs with low confidence ratings.

Currently, we have full automation of particular CERs that go directly to our incident handling division, and more than 400 queries (a.k.a "Playbooks") automated to set alerts for those who stand watch 24/7/365 on our watch floor.

NCDOC's SIEM capability was custom built in partnership with industry as well as our own personnel to address ongoing issues and problems. We wrote a "success story" focused on the cross-functional team and Enlisted Sailors building the capability and the team we need for cyber defense (see link): https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=13779.

— Rebecca Siders, public affairs and outreach officer

CISA

There's no one size fits all approach, and different parts of CISA have different levels of automation based on their needs. On the one hand, our vulnerability management capabilities rely heavily on automated tools to scan the entire breadth of the federal mission space. On the other hand, threat detection and forensics often require in-depth analysis on previously unknown malware, leveraging a level of understanding and critical thinking that cannot be automated. As a result, automated processes are used to support – rather than replace – manual ones.

CISA's goal is to mature automation across all of its operations, while also better integrating tools and data across the agency. Even in areas where automated tools are used heavily, we still use humans to analyze and contextualize findings, as well as spot false positives or negatives.

Describing "success" in the threat hunting space is difficult because the biggest successes will go unnoticed – it's the threat that never made its way to your network. The most highly touted successes are often reactive, meaning the adversary has gotten through the first layer of defense, and we have discovered it and been able to mitigate its effects. While this is obviously critical, it's not really a good metric of overall success in cybersecurity.

If there's an exception to the rule that our successes frequently go unnoticed, it's in the election security efforts of 2020. CISA led a whole-of-government effort, working with the interagency, state and local governments and the private sector to increase the resilience of the nation's election systems. CISA was able to scan for threats on voting infrastructure in all 50 states, providing key information to analysts and state and local election officials that they could use to protect their network. This is a perfect example of how automation can allow humans to do their work more efficiently and make better decisions.

— Brian Gattoni, chief technology officer

JFHQ-DODIN

Fully answering this question is somewhat difficult due to the wide variety of automated capabilities utilized across multiple tiers of DoD's defenses, and the wide variety of work roles responsible for securing and defending our networks. While we strive to automate as many processes as possible to increase speed and free up resources, many processes require manual review and even intervention to increase accuracy. Automated process can assist with acting on known signatures or indicators, and can be enabled by behavioral analysis capabilities when available. Automated tools can assist with eliminating some of the noise facing analysts by reducing the sheer number of alerts requiring manual review or investigation.

There are a number of examples where cyber threat intelligence has proven its value in bolstering the ability of automated capabilities to defend DoD's networks at speed. This includes robust multi-faceted capabilities at DoD's internet access points, as well as at the mid-tier and endpoints. These defenses are informed by a variety of CTI feeds, including IC provided intelligence data, commercial threat intelligence subscriptions and when required, manual inputs from network or intelligence analysis.

Another success includes the development of a methodology to assist with threat informing DoD's vulnerability management efforts. This effort seeks to assist with prioritizing the mitigation of vulnerabilities based on an evaluation of the threat. While this capability is currently conducted using what we would call semi-automated capabilities, great strides are being made to bring together a variety of CTI capabilities in an automated analytic to increase our ability to monitor and mitigate an ever growing number of known vulnerabilities.

JFHQ-DoDIN developed an open source intelligence team as part of our intelligence directorate to ensure we were maximizing the value of publically available information and commercial cyber threat intelligence. The team receives alerts from a variety of commercial platforms as part of its automated processes. This data is analyzed and then disseminated to the appropriate entity to drive defensive mitigation efforts. When possible, this team uses automated alerts, made possible by a variety of DoD and commercial tools, to provide timely and accurate information to our network defenders. This capability augments traditional intelligence analysis efforts, and enables DoD to capitalize on a wealth of threat information processed by the public, industry and academia.

— Steven Mavica, public affairs officer

NATIONAL GUARD BUREAU

NGB data is being fed into these systems at a pace that the average human being would not be able to keep up with. Currently at every layer of transporting or transferring data we were able to add an automated SIEM tool to assist with movement and protection. Some examples are auto assigning tasks to individuals, keeping a log of all actions happening within the system, faster searching capability and communicating workflows through a management tool vs. requiring an individual to complete step-by-step tasks followed by sending an email or mobile notification at a specified time.

The SolarWinds breach is an example of how automated systems were used efficiently to detect an incident. FireEye was able to detect evidence that attackers entered a backdoor in the SolarWinds Orion business software that distributed malware. This would have been more difficult if it were not for the assistance of automation.

— Wayne Hall, public affairs and media operations specialist

To the extent you can automate certain cyber defense functions, in what ways does doing so free up your workforce to perform more critical tasks that can only be done by skilled people?

NAVY DEFENSE OPERATIONS COMMAND

Automating CERs reduced the time (by approximately 50%) our analysts spent on creating reports manually, increased the number of reports, and significantly increased the quality of reporting.

The time saved enables our analysts and SMEs to develop tailored training for our more junior analysts as well as devote time to training and qualifications in their specific areas of expertise. Additionally, our defenders can spend time applying critical thinking skills to develop more "playbooks" that automatically detect vulnerabilities proactively as emerging threats evolve.

— Rebecca Siders, public affairs and outreach officer

CISA

One unique challenge CISA faces is the size of its mission space – automation is essential to detecting threats and uncovering vulnerabilities for all federal agencies and U.S. critical infrastructure. It's impossible for human analysts to do it on their own.

A primary function of automation today is to enhance the skilled analyst's contribution. Once an analyst detects a threat, they can program a tool to automatically detect and block that threat going forward, and then they move on to hunting for new threats. However, this means analysts are creating tools based on the problems of today, rather than what we may see in the future.

One of CISA's mantras is "Defend Today, Secure Tomorrow," and we're planning to do that in the automation space by taking a strategic, mission-focused approach: identifying core data processes that can be easily automated in order to augment the human analyst. This will integrate automation throughout the operations life cycle, freeing up skilled analysts to tackle more high-risk, high-complexity problems at a national scale.

— Brian Gattoni, chief technology officer

JFHQ-DODIN

From an execution standpoint, automating mitigations and countermeasures is critical to defending in real time. As previously stated, no number of cyber defenders can adequately perform these functions in a manual manner. Automated actions, enabled by reliable cyber threat intelligence, is critical. From an analysis and investigation standpoint, automated capabilities assist with filtering out noise by highlighting suspicious or malicious activity requiring analyst review. Additionally analytics, fed by federated data sets, allow for analysis within a common set of tools, vice having them spend the majority of their time compiling data from disparate sources. Ultimately the goal is to increase the amount of time spent on analysis and investigation, while improving the ability to rapidly share data across a community of interest.

— Steven Mavica, public affairs officer

NATIONAL GUARD BUREAU

The analyst has more time to investigate or look at suspicious activities or alerts, while automation is still assisting in the background ensuring the data is being protected. It helps with incident response time by enabling the analyst to immediately focus on remediating the issue. The tool has the capability to automatically block suspicious activities, and therefore allows the analyst time to review and determine whether the activity is malicious. While the average workday for a person normally lasts several hours, an automated tool is working 24-7, and an automated tool can send an alert anytime.

— Wayne Hall, public affairs and media operations specialist

Discuss your biggest pain points when it comes to increasing your use of automation and/or orchestrating various cyber intelligence tools. How are you addressing those issues, and how would you like industry to help you address them?

NAVY DEFENSE OPERATIONS COMMAND

Coincidentally, the biggest pain points when it comes to automating and orchestrating cyber intelligence tools are also the greatest selling points of the service: it involves massive amounts of data, and that data is usually highly perishable.

We approach these issues with two separate assumptions:

First, we assume that any data point we ingest requires corroboration and validation from at least one or two additional sources. Each cyber threat intelligence provider has its own unique accesses and methods for acquiring that data, and while they perform their own due diligence before sharing insights with customers, false positive rates are still very high. Automation is the most effective and efficient way to evaluate individual data points across multiple disparate sources of intelligence, and we even leverage basic machine learning models to help us extract vetted and actionable intelligence from the noise.

Second, we assume that most of the publicly available cyber intelligence data we ingest is also being exposed to our adversaries in some manner, and therefore is most effectively handled as a "trailing" indicator of compromise instead of a "leading" indicator of compromise. While we still use automation to alert on future events based on cyber threat intelligence, our most effective use cases tend to involve retrospective searches, where we take newly-discovered indicators of compromise and compare them to the wealth of historic data we maintain at NCDOC. This tends to help minimize false positives as well, which allows us to orchestrate more reliable response actions based on our findings.

The cyber security industry is generally in line with our approach.

— Rebecca Siders, public affairs and outreach officer

CISA

Automating threat hunting operations requires consistent streams of trustworthy data, which can be a challenge for CISA, as we face unique constraints to accessing and using data within a fully orchestrated system. There are good reasons for these constraints. For example, CISA can access classified data from its partners in the intelligence community to help detect adversary nation-state activity. However, classified data comes with necessary protections that limit how it can be used in automated tools. Similarly, there are necessary privacy and civil liberties protections that limit what data we are able to access from partners in the private sector and critical infrastructure.

In addition, many of CISA's key cybersecurity systems were developed independently and for different purposes, which hinders orchestration even within the organization. When data and analytic capabilities are fragmented, this limits our ability to adopt automated tools. A core component of CISA's technology strategy is to evolve these existing systems so that they can work together to support an integrated, cross-agency data and analytics environment.

While these two challenges may be unique to CISA, a challenge everyone faces when adopting automated tools is ensuring that the outputs of these tools are effective in providing a comprehensive view that helps analysts answer their real-world questions about cyber risk. Incomplete data or findings that lack context will lead to bad decisions. This is why we're not looking at any single new tool or data stream, but multiple tools and data sources to provide insight into the whole risk environment.

Finally, a broader challenge that affects not just CISA and the adoption of automation, but nearly every organization when it comes to cybersecurity, is the shortage of cybersecurity professionals across both government and the private sector. CISA believes part of our mission as the nation's civilian cybersecurity agency is to raise the cybersecurity bar collectively across the country. We have a number of programs designed to invest in cybersecurity education and inspire Americans from all backgrounds and experiences to enter the field of cybersecurity.

— Brian Gattoni, chief technology officer

JFHQ-DODIN

There are several pain points related to increasing our use of automation and maximizing the value of cyber threat intelligence from all sources. There is no shortage of available cyber threat intelligence information, and in some respects we can be overloaded by the volume of data. For example, increasing the number of indicators deployed throughout our sensors and security appliances will obviously increase the number of alerts received, and the number of automated defensive actions that occur. The downside is that we generally can't capitalize on the full intelligence value of that data due to the overwhelming volume. This drives the need for analytics to enrich subsequent analysis to ensure we do not encourage a "fire and forget" mentality.

There are a large number of commercial vendors providing cybersecurity services which include subscription based CTI data, as well as CTI-enabled services or appliances. While there is some redundancy with regard to these services, there are often unique features or core capabilities that often lead organizations to acquire more than one capability. As a result, DoD and our mission partners utilize a patchwork of capabilities. The disparity can lead to practical challenges such as the inability to share information derived from CTI subscriptions with other DoD or U.S. government organizations. CTI vendors can assist by working with their subscribers to clearly delineate procedures for sharing data derived from their capabilities. We have achieved some success in negotiating with our current vendors to maximize sharing when possible, while protecting the commercial company's business model and contractual equities.

Training related to automated capabilities can be challenging given the number of tools and the variety of work roles associated with their use. While there is training for most DoD or commercially provided tools, access to initial and refresher training can be a challenge, and in some cases the training does not address the particular needs of an organization or individual user.

While many capabilities have worked to adopt common technical standards (i.e. MISP, STIX/TAXI etc.), they are not all intentionally designed with the intent of ensuring data sharing with other platforms. They may provide for output in common formats (i.e. CSV, Excel etc.); however, the movement of data can be problematic given the variety of system classifications, the volume of data / file sizes and other potential challenges. While this is becoming somewhat less of a challenge, interoperability between systems, and the ability to rapidly move data can hinder analyst workflows.

Efforts continue to be made to ensure that cyber threat intelligence data is shared across and between organizations in a timely manner. The Department of Homeland Security Automated Indicator Sharing (AIS) capability serves as a great example of how cyber threat intelligence can be shared across the US government and our partners across the public and private sector. JFHQ-DoDIN, using a DISA provided capability, participates in a two way exchange through an interface with AIS. The intelligence community also manages a repository of indicators for use by appropriately cleared entities. Unfortunately, outside of these two examples, there are very few formalized repositories or sharing mechanisms available that allow the sharing of cyber threat intelligence, such as indicator of compromise, with mission partners outside of the emailing of locally developed spreadsheets. Add to this challenge the various classification levels involved, as well as the proprietary nature of a portion of commercially provided CTI data.

— Steven Mavica, public affairs officer

NATIONAL GUARD BUREAU

The approval process for adding a new automated tool to NGB's networks requires several security technical information guides, testing and compliance that is within DoD's standards and requirements. We have implemented a workflow tool to streamline our process from start to finish.

Industry can assist by ensuring that when a product is being presented for our consideration, it has been vetted through Computer Hardware Enterprise Software and Solutions (CHESS) or any other similar DoD process.

— Wayne Hall, public affairs and media operations specialist

What are your goals to increase the amount of automation you rely on to mitigate cyber threats? Are there any laws, policies or procedures that currently present barriers or challenges to your goals?

NAVY DEFENSE OPERATIONS COMMAND

Whether they recognize it or not, each defensive cyber team in the government or private sector is actually its own best source of actionable cyber threat intelligence. Every day, large organizations fend off millions of attempted intrusions from across the internet. Sometimes, those attacks are from commodity actors looking for low-hanging fruit. Often, hiding among that commodity traffic are clues and warnings on what advanced, nation-state adversaries plan to do next. The more we automatically ingest, analyze, and take action on the wealth of data we generate on our own networks each day, the more effective we will all be as cyber defenders.

This cannot happen at just one or a few organizations simply because no one network is seeing all of the adversarial activity that is occurring. Only by collaborating and sharing that data via trusted communities of interest can cyber defenders hope to stay ahead of the increasingly sophisticated attacks we face. This is absolutely key to automation efforts that seek to take action on the information at our disposal. Policies and resources that help create sharing mechanisms between the government and private sector would aid in this effort tremendously.

The Information Sharing and Analysis Center model that has been supported by the Department of Homeland Security is an excellent example to follow, and additional efforts to rapidly, securely and confidentially share threat indicators would give the advantage back to the defenders, making the internet safer for everyone who uses it.

— Rebecca Siders, public affairs and outreach officer

CISA

One of the core objectives of CISA's technology strategy is to take legacy technology platforms and integrate their data and analytics into one environment that supports automated threat detection and risk analysts across the agency. This environment will support the secure storage and management of data from all of CISA's operations, and enable the development of automated tools that provide analysts with a baseline understanding of risk. This will not only allow us to scale our cybersecurity operations, but it will also allow our human analysts to tackle more complex challenges.

None of what we want to do can be accomplished without the right people and processes, which is why we're looking to expand the number of data professionals in CISA's work force. Leveraging automation effectively requires data experts in a variety of different roles – from data scientists to data engineers to data stewards. We're currently exploring how to find the right talent and ensure they're filling the right roles in order to maximize the operational value of data.

– Brian Gattoni, chief technology officer

JFHQ-DODIN

From a JFHQ-DoDIN perspective, we seek to effectively leverage the use of automated tools, including cyber threat intelligence, to improve our ability to secure, operate and defend DoD's information networks. We seek to do this through several foundation frameworks that we believe are critical to our ability to assure the capabilities required to support DoD's critical missions and functions.

We seek to improve our ability to maintain situational awareness to support decision-making. We must understand ourselves, as well as the adversary. Understanding the cyber terrain, the link to mission essential tasks and functions, and the associated vulnerabilities are foundational to our ability to execute the through a command-centric operational framework for cyber. To meet the expectations outlined in the National Defense Strategy, effective DoDIN operations and defensive cyberspace operations demand the integration of intelligence, operations and cyber disciplines to an even greater extent than DoD has historically operated. This allows Commanders to more fully assess risk to mission and make more informed decisions.

We want to improve upon our ability to conduct threat informed analysis against a variety of threats by leveraging automated capabilities to not only monitor existing threats, but to become more predictive with regard to emerging threats. Building on our analysis to understand the threat, we want to improve our ability to support the warfighter through assessment of the cyber risk to mission. This requires an understanding of the security and defensive posture of critical cyber assets and capabilities tied to combatant command missions, while assessing the intent and capabilities of our adversaries.

Finally, we need to focus effort on the development and integration of capabilities to enable the efforts defined above. The availability of resources and budgetary constraints will always influence the development or acquisition of new capabilities and tools. Setting that aside, we must focus on the disciplined definition of requirements, understand the landscape of existing tools and capabilities, and think towards the future to ensure we do not develop stand-alone capabilities that perform a single function and has no interoperability with other systems or capabilities.

— Steven Mavica, public affairs officer

NATIONAL GUARD BUREAU

Being able to identify and mitigate cyber threats in the least amount of time possible. Streamlining our automation efforts with Navy, Marines, Air Force, other government and civilian entities to reduce mean time to detect and mean time to remediate.

NGB follows the policies, procedures and regulations established by DoD, as well as any barriers or challenges as discussed in the response to question 4.

— Wayne Hall, public affairs and media operations specialist

How agencies can refine threat intelligence through automation

INSIGHT BY RECORDED FUTURE

Stuart Solomon, chief operating officer of Recorded Future

Agency cybersecurity personnel have had to work overtime to secure their networks during the pandemic, as the remote workforce pushed the boundaries outside the traditional perimeter. The attack surface grew exponentially as the majority of end points transferred from offices to peoples' homes. But as legacy security models begin to fail, there is one thing that can help agencies keep up with this changing dynamic: automated threat intelligence.

Threat intelligence ultimately generates decision advantage, and automation helps agencies act at the speed of the adversary while mitigating risk. Threat intelligence has become a big data problem, and the human brain simply can't make the necessary connections between seemingly disparate data points at that scale.

"It was already a big data problem to start with. But prior to migration to work from home scenarios, the data problem was generally inside of a confined space, our logical and physical boundaries were pretty well defined. And so you could put a ring fence of detective controls around it, understanding the pathways that threats would take to be able to create outcomes in a much more predictable way," said Stuart Solomon, chief operating officer of Recorded Future. "As we move both to a work from home scenario as well as the continued migration to cloud environments, we've simply expanded our boundary, we've simply added additional surface to the attack surface. And we've added more data that we need to find that needle in the haystack in."

At this kind of scale, even just gathering the data, much less processing it, requires significant motivation. And then you have to be able to determine whether the data represents a potential threat, and if so, what it might be. The data has to enable a very binary decision.

"Is this a threat? Or is this not a threat?" Solomon said. "Is this something that I have seen before? Is this something unique, or different? Am I being uniquely targeted? Or is this a ubiquitous campaign that I've just been swept up in? Is this something that's going to create an impact that I'm not comfortable with in my environment, or because of my business processes, or because of my responsibilities within my enterprise that I can't live with?"

Each of those questions requires some amount of automation to answer due to the scale, the dynamic nature of the

"As we move both to a work from home scenario as well as the continued migration to cloud environments, we've simply expanded our boundary, we've simply added additional surface to the attack surface. And we've added more data that we need to find that needle in the haystack in."

— STUART SOLOMON, CHIEF OPERATING OFFICER OF RECORDED FUTURE

adversary, and the associated threats. And then you have to take those answers, and turn them into actions, which is the most important part of threat intelligence. This could include writing a firewall rule, blacklisting a series of malicious IP addresses or domains, starting an automated vulnerability scan or proactively setting up a hunting capability.

Another critical component is data sharing. Threats tend not to be unique; they follow patterns based on the outcome they're trying to achieve, and they tend to manifest in specific destructive or disruptive capabilities or scenarios.

"There's generally a threat pattern that can be emblematic of similar threats across other platforms, other people, so intelligence sharing and information sharing is hypercritical," Solomon said. "Look at the Information Sharing and Analysis Centers (ISACs) as an example. The ISACs have spent a lot of time across various sectors of industry focused on the same basic notion, which is there's a collective good that can be gained by understanding attack patterns, vulnerabilities and signatures associated with detecting them earlier on and proactively in their attack life cycles."

In a data-sharing scenario, once data has been normalized so it can be understood by everyone, it can help all participants learn the evolution of a threat pattern and the associated technical indicators. There are multiple components to this type of dynamic as well. Some of the data has to be for human consumption, in order to understand the threat. Some of it has to be for machine consumption, to tune detective controls. And some of it will be perishable, like data on known malicious IP addresses, which are likely to be changed after a certain amount of time.

Most agencies are already using some level of automation, largely in the technical and detective controls layer. Some have moved on to applying automation to their analytical layer, creating correlations. Solomon said the next step is to start applying that automation to building a picture of normalcy, and detecting deviations from that normalcy. And then ultimately, that will lead to automating actions in response to threat detection.

But Solomon added three caveats to the use of automation. First, it can't replace humans. What it can do is move them further to the right in the value stream, and allow them to deal with more complex problems. Second, successful automation requires that good processes already be in place. And third, the most important requirement for automation is a triggering event.

"I think categorically, everyone wants automation," Solomon said. "But doing the basic building blocks to get there requires more refinement on some of the strategies."