Raising Agencies' Cyber Intelligence

carahsoft

govloop

Contents

3 Executive Summary

4 At a Glance: The Government Threat Landscape

7 Storytelling With Intelligence-Led Security

8 Prioritizing Cyber Intelligence at the Defense Logistics Agency

An interview with George Duchak, CIO, and Linus Baker, Director of Cybersecurity, DLA

11 Leveraging Zero Trust Against Cyberattacks

12 The Quest for Cyber Intelligence

17 Threat Intelligence: The Context Agencies Crave

18 Explaining Minnesota's Zero Trust Cybersecurity

An interview with Rohit Tandon, CISO, Minnesota

21 Pairing Man and Machine on Zero Trust

22 Best Practices in Cyber Intelligence

24 CDM Approved Solutions From Carahsoft and Our Reseller Partners

25 Understanding DoD's Cyber Hotline

An interview with Kris Johnson, Director of the Vulnerability Disclosure Program, DoD

26 What's Next for Cyber Intelligence?

Carahsoft and GovLoop have partnered to provide this resource around the latest government cyber intelligence initiatives and legislation. The goal is to guide government leaders and stakeholders interested in learning more about procurement initiatives and the solutions available through them.

Executive Summary

Nowadays, most agencies realize they can't avoid thinking about cybersecurity. Whether it is federal, state or local governments, the citizen data they manage is too sensitive to leave unguarded. And public services that rely on that data, such as unemployment benefits, are too important to risk cyberattacks interrupting them.

But what if considering cybersecurity is no longer enough? Nationwide, many agencies are finding their cybersecurity investments don't produce the returns they used to. For instance, strategies such as defending network perimeters have dominated cybersecurity for decades. Yet scores of agencies see diminished results from such measures.

The plot only thickens as modern cyberthreats become more sophisticated. While yesterday's cyberthreats typically lurked near network perimeters, today's version can strike from almost anywhere. Take mobile devices, which have enabled dangers such as ransomware to reach across much larger distances in recent years. And although traditional cyberdefenses cover perimeter defense, they're often powerless against threats emerging from within agencies.

Collectively, these factors are pressuring agencies to evolve or fall prey to risks that constantly change. Unfortunately, increasing agencies' cybersecurity IQ is easier said than done. How do agencies outsmart clever cybercriminals in this era of tight budgets and rising citizen demands?

Cyber intelligence uses behavior analytics, network visibility, and operational and threat intelligence to make agencies smarter about today's threats. Using cyber intelligence, agencies can see their people, processes and technology more clearly. Over time, this information helps agencies make smarter decisions about external and internal dangers. Even better, cyber intelligence can aid agencies by predicting future problems.

If your agency needs a crash course in cyber intelligence, the following guide can be its teacher. Our guide's research, case studies and government expertise can help your agency navigate the minefield of contemporary cybersecurity.

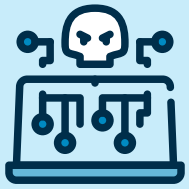
- First, we'll summarize the latest dates, quotes, news and statistics that can help you understand the present cybersecurity environment.
- Second, we'll detail the quest for cyber intelligence by examining relevant concepts such as threat intelligence, network visibility, operational intelligence and behavioral analytics.
- Third, we'll share wisdom from government thought leaders about what's worked – and what hasn't – at their agencies.
- Finally, we'll share best practices for elevating your agency's cyber intelligence before providing the proper context for tomorrow's challenges.

Cyber Intelligence 101 is now in session. Before your agency can master cyber intelligence, let's learn some cybersecurity basics.

At a Glance:
The Government Threat Landscape

5 Cyber Intelligence Terms to Know

The following terms will help your agency grasp basic security concepts before honing its cyber intelligence.



Ransomware

Ransomware is a type of malware, which is any software designed to intentionally damage computers and other technology. Unlike other malware, ransomware threatens to publish or block access to its victims' data unless they pay a ransom. Many law enforcement agencies, including the FBI, recommend against paying ransoms to cybercriminals.

Insider Threats

Insider threats originate from within agencies. Typically, insider threats hurt agencies by handling sensitive assets such as data, intellectual property or personnel records without permission. While insider threats can be intentionally harmful, they can also damage agencies accidentally or through negligence.

Phishing

Phishing is an attempt to obtain sensitive data through deceptive electronic communications. Posing as trustworthy sources such as agency leaders, cybercriminals trick victims using email, social media and other mediums. At agencies, phishing prevention often involves strong cyber hygiene and user awareness.

Zero Trust Cybersecurity

Zero trust cybersecurity centers on agencies automatically distrusting anything inside or outside their network perimeters. Agencies also boost their security by verifying any users or other entities before they access sensitive data or networks. Collectively, these measures help agencies continuously monitor their networks and prevent potential threats.

Artificial Intelligence (AI)

AI features machines demonstrating such human cognitive abilities as learning and problem-solving. AI's possible benefits range from reducing human error to performing simple tasks for people. It could potentially revolutionize multiple fields, including cybersecurity.

5 Federal Cyber Intelligence Facts to Know

$10 billion

was requested in The President's Budget FY2021 for the **military's cyber capabilities** through the Defense Department (DoD).

$1.1 billion

was also requested in the President's Budget FY2021 for the Homeland Security Department's (DHS) **cybersecurity efforts.**

6,500+

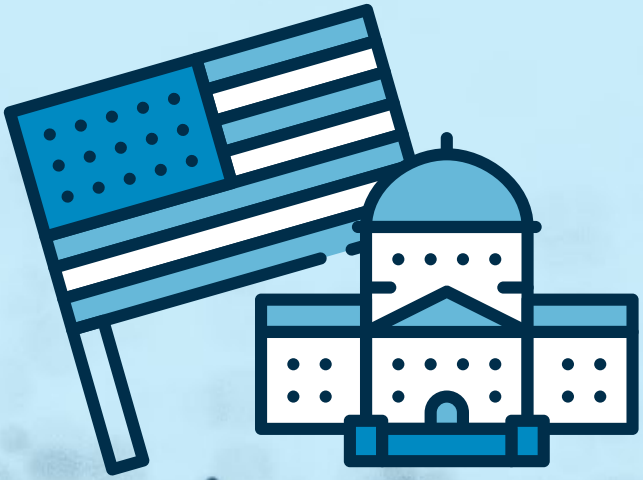
DHS-led **network risk assessments** were requested in The President's Budget FY2021, including assessments of state and local electoral systems.

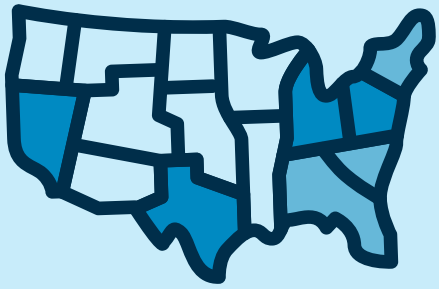
7,000

Nearly 7,000 **malicious domains associated with the COVID-19 pandemic** had been removed by the Cybersecurity and Infrastructure Security Agency (CISA) as of April 2020.

600+

health care partners received **cyber-hygiene scanning** during the coronavirus crisis as of April 2020.





5 State and Local Cyber Intelligence Facts to Know

#1

was where **cybersecurity and risk management** ranked among state chief information officers' (CIOs) top 10 priorities for 2020.

#4

was where **security enhancement tools** such as advanced analytics ranked among state CIOs' top 10 priorities for technologies, applications and tools for 2020.

#7

was where **AI and robotic process automation (RPA)** ranked among state CIOs' top 10 priorities for technologies, applications and tools for 2020. RPA occurs when software creates digital bots for performing repetitive manual tasks.

$76,000

was requested by cybercriminals after a **ransomware attack** against Baltimore in May 2019.

$18.2 million

was the amount, as of March 2020, Baltimore ultimately spent in **restoration costs and lost revenues** after not paying the ransom.


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 proactively reduce risk.
Recorded Future®
www.recordedfuture.com

Industry Spotlight

Storytelling With Intelligence-Led Security

An interview with Allan Liska, Threat Intelligence Analyst, Recorded Future

Too often, agency leaders and cybersecurity analysts seem like they're speaking separate languages. With both sides communicating about cyberthreats differently, getting everyone on the same page is one of contemporary government's greatest challenges.

The wider the gulf between an agency's teams, the more vulnerable it is to external danger. Today's security landscape contains dangers everywhere, and cyberthreats won't wait for agency workforces to unite against them. Agencies that don't speak the same language as their employees and employees that don't speak the same language as their agency leaders will find themselves constantly fighting cybersecurity fires.

Allan Liska, a Threat Intelligence Analyst at the cybersecurity firm Recorded Future, says intelligence-led security — cybersecurity guided by threat intelligence — can align every corner of an agency's workforce. Liska shared three ways agencies can implement intelligence-led security.

1. Learn the same lingo

According to Liska, threat intelligence covers a vast amount of data from multiple sources. Whether it is social media, online forums or something else, that information must make sense to all relevant parties at an agency.

"In order to be good at threat intelligence, you must be able to tell that story," he said. "You need to filter down that data, so it is useful to your agency."

For example, solutions such as those Recorded Future provides can help agencies recognize IP addresses associated with cybercriminals. Using threat intelligence tools, agencies can detect these suspect individuals in places such as digital marketplaces. Analysts can then warn agency leaders about potential tactics — like ransomware — these cybercriminals might use against them.

"It presents a holistic view of everything that is important to your agency," Liska said of threat intelligence. "Recorded Future can help with that translation."

2. Rank the risks

Cybersecurity frequently resembles drinking from a fire hose in terms of understanding every threat. With the variety of perils constantly growing, agencies must separate the alarming from the aggravating.

"It's understanding what an indicator for a nation-state looks like versus a minor annoyance," Liska said. "This allows you to better prioritize which events you are going to go after and stop."

Take unwanted browser plugins. Although obnoxious, ignoring these plugins won't hurt agencies as badly if they overlook known cybercriminals. Distinct problems create distinct warning signs; understanding the telltale signs help agencies better defend themselves.

3. Spend resources wisely

For many agencies, there's no denying their manpower, money and time are limited. According to Liska, threat intelligence can help them use their assets where they are needed most.

"You're not spending money on new security tools," he said. "Instead, you're making existing security tools better. That allows you to get rid of tools that might be redundant or unnecessary."

Fully realized, intelligence-led security gets agencies discussing cyberthreats coherently. It also helps agencies rank their obstacles and the best ways their available tools can overcome them. By making their security intelligence-led, agencies can outwit cyberthreats and focus on mission success.

Prioritizing Cyber Intelligence at the Defense Logistics Agency

The Defense Logistics Agency (DLA) provides more than $42 billion in goods and services annually while supporting U.S. combat logistics around the world. With about 26,000 employees operating in 28 countries, how does DLA monitor cyberthreats?

Increasingly, the answer is cyber intelligence. In an interview with GovLoop, CIO George Duchak and Director of Cybersecurity Linus Baker explained how DLA stays informed about the global threat landscape.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: How is traditional, perimeter-based cybersecurity getting harder?

BAKER: For us at DLA in terms of perimeter-based cybersecurity, in more recent months, across the department – and really, across the federal government – I would say it has probably been an increasing concern outside of DLA more so than inside DLA. It's because of the fact DLA was well-postured. We had been on a course that charted remote work as a normalcy. Our cyber operations staff, mainly our CSSP/CERT – our Cybersecurity Service Provider/Computer Emergency Response Team – they've been postured and executing their monitoring, their response, their incident handling against a robust remote workforce prior to the COVID-19 pandemic. For DLA, it wasn't much of a shift.

One of the things I would tell you is more of a concern than it has been in the past is the large number of endpoints that are seated on our networks today, especially with mass telework becoming the norm over the last few months. Identifying and confirming anomalies and positive, adverse actions has become more difficult. It has amped up our attention on automation, machine learning and robotic process automation and bringing that into the fold to a greater degree across the cybersecurity spectrum. It is almost a must now because of the massive amounts of data to sift through to get to what you're seeking.

DUCHAK: Perimeter security doesn't really protect against the biggest vulnerability that any organization has, and that's phishing. That's something that's very difficult to defend against. We have a good spear-phishing campaign where we'll send out targeted emails to our folks to see if they'll click on things they shouldn't be.

The second thing about perimeter security is you've got to know what's on your network. We're just starting – as well as all of DoD – with this concept of "Comply to Connect." You can't put an unknown piece of hardware on your network. It must be validated. The patching must be up to date. You've got to get a driver's license before you're allowed to drive on the network.

How can DLA improve its threat intelligence?

BAKER: For threat intelligence to be useful, it's got to be targeted towards the mission. There's a lot of backend work that must be done first. You've got to understand the mission. You've got to understand from a strategic perspective how valuable the IT you deliver is. What does it enable? When you begin to target the enabling capabilities, what you deliver as part of the mission, then you can begin to pull out those crown jewels and begin to understand what's important from an infrastructure perspective, down to a business system perspective, down to a sensor that drives some mechanical functions. We're heavily dependent on operational technology for some of our mission. We're talking pipelines, fuel and energy, shipping and refining. Operational technology is key to this.

Logistics operations is what we deliver to the warfighter. Understanding that mission and that cyber terrain, now we can begin to target threat intelligence. That enables me to execute the intelligence preparations for cyberspace that matter to DLA.

That's how I see agencies leveraging cyberthreat intelligence. Otherwise, it's just data that's there, and it is hard to make sense of if you haven't done the work to understand your business or your mission.

Does cyber intelligence give you the best possible information to make an informed decision about something related to DLA's mission?

BAKER: You must prioritize. All threat intelligence might not necessarily rise to the level of other threats. That's why it needs to be targeted.

We've taken steps to prioritize our remediation efforts. We recognize we're not going to be able to swallow the ocean in trying to execute our cyber defense mission where it's most needed. Prioritization is key, and that's how you target threat intelligence.

DUCHAK: Fundamentally, organizations that don't have a threat intel cell behave differently. First, threat intel doesn't equal cybersecurity. Threat intel is more about the who – understanding the motives of the threat actors, what targets they're going after and their behavior. Cybersecurity is more about what to do about it. Having a threat intel cell focuses the mental model at your organization from being reactive to being proactive. You start getting out in front of the threat. If you don't have a threat intel cell, all you're doing is reacting constantly to what someone else is doing to you.

What cyber intelligence lessons would you share with other agencies?

DUCHAK: You must understand your landscape. The reality is we are a target, and we're going to be a target. Part of cybersecurity at any organization is you don't want to spend money on it until you need it. And you don't need it until you've been had, and by then, it is too late. There's always this dynamic tension within an organization when you're trying to fund cybersecurity.

At some point, when do you know you have enough cybersecurity? Is it 10, 20, 30 products? There is a certain law of diminishing returns there. Every agency is in a box in terms of cost constraints and must determine what's the right product mix at their agency. Enlightened leadership understands it does cost money to be secure. What we're securing is national defense.

What's the main takeaway about cyber intelligence?

BAKER: It is the criticality of good, accurate cyberthreat intel and having those feeds consistently available. It is having the cybersecurity infrastructure in place to leverage data and target efforts where they matter most given your business and mission. It is central to your cyber resilience capabilities. It is central to your ability to be proactive rather than reactive. If we're proactive, we can begin to do things before vulnerabilities have propagated across our ecosystems. That's a paradigm shift that's necessary as we go forward.

Trend Micro Cloud One™ Cloud Security Simplified

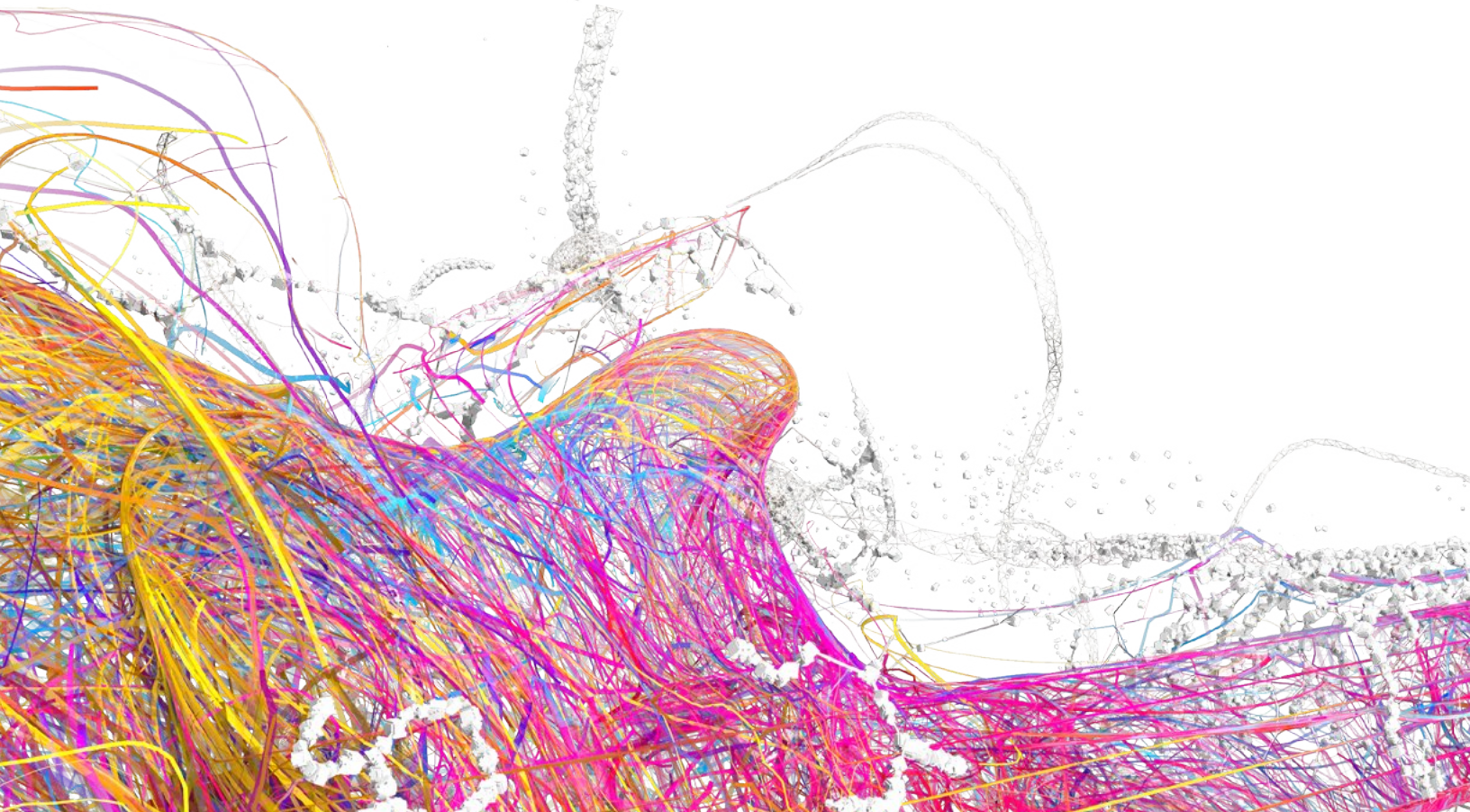
- Automated: Save time, gain visibility. Automated deployment and discovery lead to operational efficiencies and accelerated, streamlined compliance.
- Flexible: Builder's choice. You choose the cloud, the platforms, and the tools, and we leverage our turn-key integrations and broad APIs, freeing you to procure the way you want and deploy the way you need.
- All-in-one solution: One tool that has the breadth, depth, and innovation required to meet and manage your cloud security needs today and in the future.

Discover the beauty of simplified cloud security:

https://www.trendmicro.com/hybridcloud

TREND MICRO™

Real-time discovery and remediation of cloud vulnerabilities and misconfigurations by Trend Micro. **Created with real security data by artist Brendan Dawes**



Industry Spotlight

Leveraging Zero Trust Against Cyberattacks

An interview with Greg Young, Vice President of Cybersecurity, Trend Micro

For decades, agencies have defended their IT by focusing most on guarding their networks' perimeters. While valuable, monitoring the traffic coming and going from agencies' networks is no longer enough. In this new era of widespread telework, cloud and Everything-as-a-Service (EaaS), agencies need greater network visibility than before.

Agencies aren't looking just at the "north-south" of traffic moving inside their network perimeters for threats. **Lateral cyberattacks occur when perpetrators breach agencies' defenses and then move freely "sideways" or "east-west" on their networks.** The modus-operandi of cybercriminals today is to seek a weakly defended element, and then access sensitive data by moving laterally to avoid stronger safeguards.

This protection against lateral movement is what zero trust cybersecurity is all about. By automatically distrusting everything on and off their networks, agencies can enhance their IT security.

According to Greg Young, Vice President of Cybersecurity at Trend Micro, a cybersecurity software provider, zero trust can dramatically elevate agencies' cyberdefenses from their legacy security architectures. Young shared three ways agencies can stop lateral cyberattacks.

1. Create don't trust zones

The older model upon which network security was built created zones with similar trust levels. Young recommended agencies stop assuming everyone and everything in a zone has that level of trust or even belongs there. According to Young, immediately distrusting components can radically strengthen agencies' cybersecurity.

"Zero trust is about having areas where trust is not assumed, and then building up trust based on validation, identification and observation," he said. "Trusting something because of where it resides is a legacy strategy, and it is no longer valid."

Agencies can establish zero trust for their cloud computing environments, networks, servers, internet of things (IoT) devices and more.

2. Recognize human error

Accidents happen, and, in cybersecurity, humans often cause them. People make mistakes even with the best security education.

"People can't be patched," Young said. "There is a limit on how much we can expect them to be involved in security every day and to be flawless." Often, government cybersecurity personnel are bombarded with seemingly unrelated security education information and policies.

Take telework, which has made their homes and offices interchangeable for many government employees. Going forward, agencies should accept and prepare for cybersecurity errors while teleworking.

"Insider threats aren't just rogue people, they are most often unwitting attackers because their credentials or devices have been compromised," Young said.

3. Construct context

According to Young, understanding the patterns and relationships their data have can boost agencies' cybersecurity.

"We've been making too many of our security decisions based on the same small set of security event data," he said. "This limited information is no longer enough. With a greater addressable pool of event data, this can be turned into information that can become security-relevant through associations. You can connect the dots quicker and stop attacks in progress."

Using enterprise software solutions such as the ones Trend Micro, Inc. provides, agencies can improve their zero trust cyberdefenses. Ultimately, clearer intelligence helps agencies make more informed decisions before tackling threats. At their best, agencies can make these decisions automatically.

"Zero trust is about understanding your environment at any given point in time," Young said. "Context is everything."

The Quest for **Cyber Intelligence**

Today, the issue with government cybersecurity isn't thinking about it – it is doing so faster than cybercriminals. Too often, cybercriminals are several steps ahead of agencies on cyberdefenses and weapons that can breach them.

Fortunately, agencies can keep up with the quickest-thinking cybercriminals. Using cyber intelligence, agencies can see the global threat landscape in real time. By detecting cyberthreat patterns, agencies are better prepared to identify, mitigate and recover from them.

At any agency, enlightening cyber intelligence mixes behavior analytics, network visibility, and operational and threat intelligence. Cutting-edge cyber intelligence also combines emerging capabilities and agencywide strategies. In this section, we'll describe four ways agencies can outwit even the craftiest cybercriminals using cyber intelligence.

Augmenting Threat Intelligence With Automation

One of the biggest problems in government cybersecurity is that agencies are frequently *reactive* rather than *proactive*. Instead of waiting for cybercriminals to strike, threat intelligence can assist agencies with moving first.

Robust threat intelligence monitors all potential cyberthreats in real time worldwide. Together, these attributes can give agencies the upper hand over cybercriminals. Threat intelligence differs from cyber intelligence, as it focuses specifically on bad actors rather than security topics overall.

Take a recent cyberdefense pilot program involving the Johns Hopkins Applied Physics Laboratory (APL). In July 2020, APL announced six agencies were joining an initiative involving its automated cybersecurity tool. Participants included CISA; one state agency each from Arizona, Louisiana, Massachusetts and Texas; an agency from Maricopa County, Arizona, as well as the Multi-State Information Sharing & Analysis Center (MS-ISAC).

APL's pilot aims to raise agencies' cyber intelligence using automation. Automation involves machines performing simple tasks with little to no human involvement. Combined with threat intelligence, automation could dramatically change agencies' cyberdefenses.

The pilot's tools, meanwhile, were dubbed the Security Orchestration, Automation and Response (SOAR) suite. The toolset permits agencies to collect data about security threats from multiple sources in nearly real time. After that, it automates agencies' triage response actions so they're significantly faster than the manual version.

Ultimately, APL hopes the pilot will help state, local, territorial and tribal agencies reach three goals:

- Identify key areas where manual tasks could be reduced
- Promote actionable information sharing across agencies at every level
- Identify the orchestration services – such as acting and decision-making – needed to integrate responses to cyberthreats

SOAR isn't APL's first foray into automated cybersecurity. APL previously developed the Integrated Adaptive Cyber Defense (IACD) framework to accelerate the speed and scale of agencies' cyberdefenses using automation, orchestration and information-sharing. DHS and the National Security Agency (NSA) sponsored the framework's creation. Using IACD, agencies could respond to cybersecurity incidents in 10 minutes rather than 11 hours. In some cases, IACD participants were able to implement preapproved cybersecurity responses in one second.

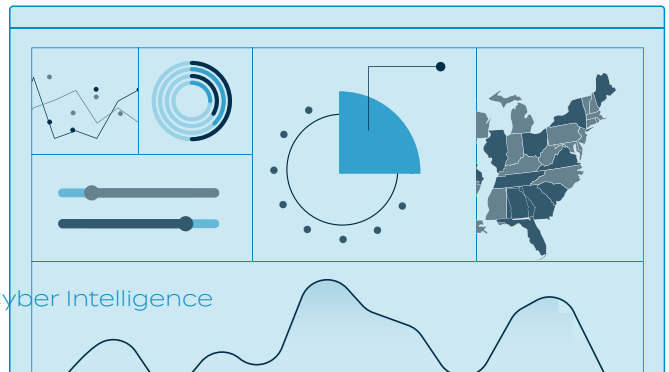
Pilots such as APL's latest effort show the value of playing cybersecurity as a team sport. Rather than go it alone, public and private sector organizations can collaborate on better cybersecurity for all. Adding automation to the mix only eases the burden; while people pursue more complex, higher-level duties, machines take the heavy lifting.

Optimizing Operational Intelligence

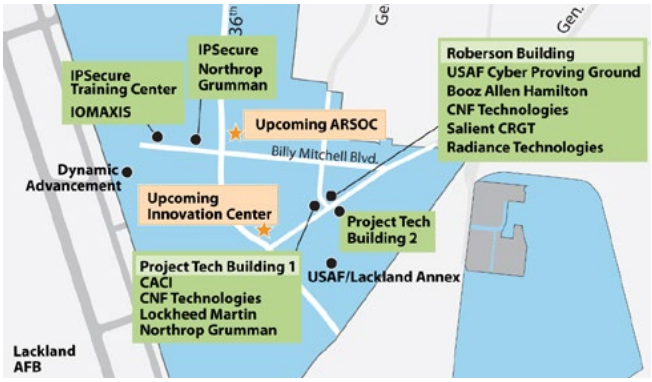
For cities such as San Antonio, Texas, ports can become essential commercial hubs. But ports also have many moving pieces with their critical infrastructure, including energy grids, manufacturing and telecommunications. Subsequently, defending ports requires San Antonio and other local governments to quickly and delicately balance their resources.

Enter operational intelligence. **Operational intelligence provides agencies with insights about their data, events and affairs in real time.** Consider user data – agencies can see who is using their networks when, where and how. Gradually, agencies that rely on operational intelligence can make wiser choices about their cybersecurity – and everything else.

Every mission needs a command center, however, and operational intelligence is no exception. That's where security operations centers (SOCs) come in. SOCs are centralized units for directing agencies' organizational and technical security. In cybersecurity, SOCs usually defend such agencywide information systems as applications, databases and networks.



In June 2020, San Antonio announced its port will host a SOC. Dubbed the Alamo Regional Security Operations Center (ARSOC), the facility is scheduled to launch in early 2021.



Once ARSOC becomes operational, city, port and private sector cybersecurity personnel will simultaneously monitor San Antonio's online activities for potential threats. ARSOC will also strengthen San Antonio's ties with DoD, which already maintains an active presence at the port. Currently, the port houses both the 16th Air Force (Air Forces Cyber) and the 273rd Cyberspace Operations Squadron of the Texas Air National Guard. The two units are involved in regional cybersecurity, and the squadron supports local agencies with responding to cyberattacks.

Potentially, smoother coordination might be ARSOC's biggest benefit to San Antonio. Consider the area's many local agencies. Local agencies frequently lack the same personnel and resources as their state and federal peers to watch for and repel cyberattacks. Connecting ARSOC and smaller municipalities, however, could accelerate resource- and information-sharing for both parties. Eventually, Texas's cybersecurity could be more fortified than before.

Next, the port's board of directors will vote later this year on whether to approve a planned innovation center by ARSOC. Should the center be greenlit, the port will have a technology arena, collaborative spaces and a publicly accessible industry showroom. Together, these features would speed the development of new cybersecurity tools such as AI for the port.

The benefits wouldn't stop there. Upon completing the center, ARSOC and its partners could use it for conducting cybersecurity training and public demonstrations. Consequently, citizens could better understand critical infrastructure cybersecurity and ARSOC's work could inspire similar efforts elsewhere.

With cybersecurity, agencies must often do more with less. Thankfully, operational intelligence programs such as ARSOC can help them work smarter, not harder.

Navigating Network Visibility With CDM

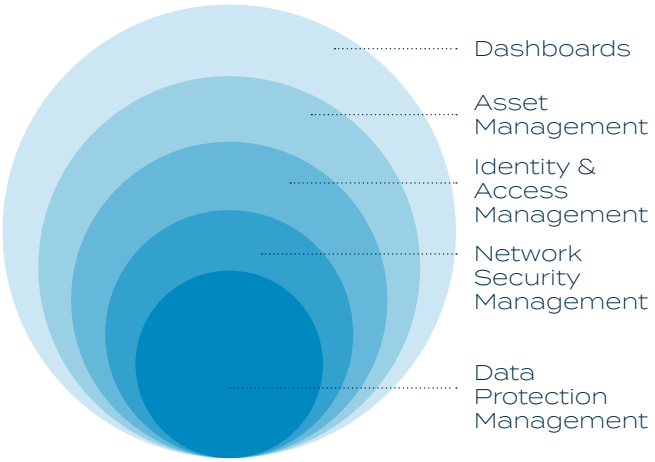
Agencies have spent 2020 dealing with an unprecedented public health crisis: COVID-19. Since reaching America in January 2020, the coronavirus has forced more agencies than ever to work remotely.

COVID-19's reach, however, didn't stop there. As the number of remote workers rose, so did the number of security gaps on their agencies' networks. With the pandemic continuing, the time might be ripe for historically strong cyberdefenses.

The good news is network visibility can help agencies protect themselves during emergencies such as COVID-19 by tracking their data and the networks and users handling it. In turn, these insights can accelerate agencies' abilities to notice and address threats. The resulting vigilance keeps agencies aware of their physical, virtual and cloud computing environments and how traffic flows across each one.

How do agencies get network visibility? Enter initiatives such as the Continuous Diagnostics and Mitigation (CDM) program. Launched in 2013, CDM delivers agencies automated tools to oversee and fix their cybersecurity vulnerabilities. While CDM is a federal program run by DHS and the General Services Administration (GSA), it is also a weapon state and local agencies can wield.

The CDM Program



Broadly, CDM aims to improve agencies' security postures with cybersecurity tools, integration services and dashboards. But network visibility drives CDM forward, including the initiative's four objectives:

- Reduce agencies' threat surfaces
- Increase visibility into the federal cybersecurity posture
- Improve federal cybersecurity response capabilities
- Streamline reporting for the Federal Information Security Modernization Act (FISMA), which requires federal agencies to develop, document and implement information security policies agencywide

Now, the shift to remote work due to COVID-19 has agencies turning to CDM for the network visibility it fosters. For example, network visibility has always assisted agencies with determining which users on their networks are and are not authorized. Since COVID-19's emergence, this capability has only become more crucial for agencies as users work remotely over vast distances. With more people using smartphones and other mobile devices, agencies are under unrivaled pressure to keep their networks secure using programs such as CDM.

With the COVID-19 emergency ongoing, CDM's network visibility is shining a light on vital parts of cyberspace. Take the National Institutes of Health (NIH), which is conducting clinical trials to test coronavirus vaccines and prevention tools. With nations around the world racing to eliminate COVID-19 first, CDM's network visibility can aid NIH with staying alert for potential data thieves. After all, no agency wants to be caught off guard by cybersecurity threats when they're dealing with viruses instead.

Besting Threats With Behavior Analytics

It is easy for agencies to forget that cybercriminals are humans. Like other people, cybercriminals develop and follow expected routines. For agencies, recognizing these behavioral patterns can give them the edge over cyberthreats.

This realization is making behavior analytics increasingly attractive to agencies. **Behavior analytics determines how users act and why and how they might behave in the future.** Using behavior analytics, agencies can predict and prevent cyberthreats with greater accuracy.

Behavior analytics begins with data. Through data, agencies can see how their users normally act. After that, agencies will have what they need to notice and examine any unusual moves their users make.

Picture insider threats, which damage agencies by emerging from within their ranks. Behavior analytics can foil insider threats by exposing their conduct. In some cases, behavior analytics can illustrate when users are accessing sensitive data they normally don't need. In other situations, behavior analytics can catch users wielding passwords that are not theirs. Behavior analytics can point agencies toward atypical conduct, whether accidental or intentional.

Externally, behavior analytics can also shield agencies from threats. Imagine agencies whose users access data across large distances. Behavior analytics can assist agencies with blocking suspicious users from connecting to their network. Sometimes, these efforts involve flagging users from nations known for supporting cybercrime. Other times, they point out when users are relying on unapproved devices. No matter the circumstances, features such as these keep agencies from being caught off guard by cyberthreats.

Combined with AI, behavior analytics can amass even more defensive power for agencies. AI can not only refine the behavioral patterns agencies rely on; it can also relieve government workforces of some burdens. Leaning on AI, agencies can eliminate easy, monotonous tasks such as resetting user passwords for their employees. The workers freed from these responsibilities can then focus on more complicated duties, such as meeting citizens' IT needs.

For evidence, behavior analytics and AI benefit agencies, look at North Carolina. In August 2019, then-CIO Eric Boyette explained how AI was helping state security employees analyze thousands of potential threats daily. Overall, the pairing helped North Carolina tackle the biggest threats immediately.

"With AI, we can narrow the tickets down to a manageable number," Boyette said of North Carolina's cybersecurity backlog.

Agencies looking to beat cyberthreats should explore making AI their force multiplier for behavior analytics. When combined, these tools can help agencies rapidly determine which behavior is worth the worry.

Industry Spotlight

Threat Intelligence: The Context Agencies Crave

An interview with Luke McNamara, Principal Analyst, FireEye

Recently, basic cybersecurity knowledge — such as which attacks are most common — won't always keep agencies' data safe. For scores of agencies, today's threat landscape can change too fast for their workforces.

Fortunately, threat intelligence can prepare agencies for cutting-edge dangers. Threat intelligence adds the context agencies need by focusing on the latest threats in realtime.

According to Luke McNamara, Principal Analyst at cybersecurity solutions firm FireEye, threat intelligence can make the difference between cybersecurity success and failure. McNamara listed three ways agencies can sharpen their threat intelligence.

1. Know the enemy

Agencies are surrounded by cyberthreats. From nation states to cybercriminals, the list of potential pitfalls is long.

McNamara suggested agencies become well-versed in the latest cyberthreats and how they operate. Like nature's predators, many cyberthreats hunt specific prey using unique tactics.

"Threat attribution is understanding what group is conducting an operation," he said. "You understand certain characteristics about their behavior. It can help you focus on the adversaries that matter most."

Take the COVID-19 pandemic. During the crisis, agencies should monitor cyberthreats infamous for stealing healthcare data.

2. Polish cyber hygiene

Across the public sector, many employees are cybersecurity novices. According to McNamara, remedying this requires agencies to teach their workforces more than entry-level cybersecurity.

"The threat actors you need to care about are the ones who know how to social engineer your employees," he said. "The human element on the defender side is incredibly important."

Consider phishing, which often snares innocent victims. McNamara recommended agencies instruct their employees on how to recognize deceptive emails and other phishing techniques.

"It's getting an email and trying to decide whether to open that attachment," he said. "Understanding those tell-tale signs can go a long way."

3. Use threat intelligence intelligently

Threat intelligence doesn't help agencies if they aren't smart about how they use it. According to McNamara, establishing and analyzing behavior patterns can help agencies cultivate stronger cybersecurity.

"It's looking at the full spectrum of adversary activity," he said. "It's everything from the breach to remediation of these threats."

Picture security controls, or the measures agencies take to avoid, detect, minimize or respond to risks. McNamara said closely examining their security controls can help agencies overcome cyberthreats.

"It could be someone that logged in from two different locations," he said as an example of what security controls watch. "It could be a threat actor trying to move laterally into another system. It could be something that detects some sort of privilege escalation."

Ultimately, security controls assist agencies by illuminating every potential cybersecurity adversary. Partnering with security control providers such as FireEye, agencies can track the full spectrum of potentially harmful activity worldwide.

The worst cyber attacks are the ones agencies never see coming. But with quality threat intelligence, agencies can stay alert to where cyberthreats might strike next.

Minnesota Chief Information Security Officer Explains **Zero Trust Cybersecurity**

Zero trust may be generating lots of buzz in the cybersecurity world, but that doesn't mean agencies understand it. At many agencies, confusion surrounds what zero trust cybersecurity is and how it can support their missions.

Minnesota Chief Information Security Officer (CISO) Rohit Tandon said zero trust covers more than cybersecurity tools – it is also a state of mind. Tandon, who is also Minnesota IT Services' (MNIT) Assistant Commissioner, argues zero trust requires agencies to transform not just their technology, but their people and processes.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: What does the global cyberthreat landscape currently look like?

TANDON: The barriers to entry in the cyber domain are not very high. Any motivated actor can develop skillsets by investing resources and capturing knowledge that's already out there. Unlike other types of attacks where weapons require certain tactical research, there is a low effort in the cyberthreat domain. The global threat landscape will continue to have new entrants as actors build strengths and develop talent.

There's this model of a cyber kill chain. It talks about how attackers move from discovery all the way to mission completion, whatever the mission might be. If we build layers of defenses that look at that cyber kill chain, can we identify the mission actions through that cycle before the mission completes?

Another framework is called a MITRE ATT&CK Framework. *(Note: This is the MITRE Corporation's Adversarial Tactics, Techniques, and Common Knowledge cybersecurity framework.)* It concerns the tools, techniques and procedures that cyber attackers build through the journey from beginning to end.

Every actor develops a pattern that they find success doing. Let's compare it to soccer, for example. You've got offense, you've got midfielders, you've got defenders. You play different formations based on how you're built and what your team's skills are. Likewise, cyberthreats have formations for the tools and techniques they use. If those aren't successful, they tend to fall back into the same rhythm of operations.

If I can study those patterns and share that knowledge with peers in my industry, we can then build the right layers of defenses using frameworks like that kill chain or MITRE to address those areas they're strong at and take actions in our domains if they get inside our perimeter.

How can zero trust help agencies' cybersecurity?

It is identity- and context-based access. Users, devices, each thing on our networks needs to have an identity. Based on that identity, you may allow access to certain data that you're trying to protect on that domain. It's about access to critical resources.

Right now, our perimeters contain everything inside. It includes storage, data, networks and many different components. Once you're inside, you're given access to

a broad spectrum. The identity piece allows us to become more granular. I could go as far as determining roles for individuals doing specific jobs and what components they need access to. Then I could limit it to just those components they need for their daily operations.

Cyber actors are looking for that inside access to pivot. They're misusing the identity trust that we have. If I can restrict that trust to just the critical operational needs of that user or device, there are very few insights they'll gain if they misuse that trust. There is very limited data or actions that I'm granting. It's a more secure infrastructure overall by applying the zero trust model.

What does adopting zero trust cybersecurity require?

It's not one solution you buy and plug into your infrastructure, and you're good to go. There are process and expectation changes. There are different layers of technology in how you're embedding it.

It is a long journey, so there's a commitment. Starting out with an identity management and governance administration will help agencies realize the benefits of zero trust faster. That itself is a daunting task that requires continuous investment and setting expectations about access control. It's about how that's going to work around devices and people on your network.

If you start improving on your identity governance administration, you'll be much better positioned when it comes time to understanding what data you want to secure and how you can connect zero trust with that data and identities.

What do you want people to know about cybersecurity?

I'd tie it during the last few months to COVID-19. Technology adoption has been moving at blazing speed.

We've been presented with the chance to build new habits. Remote working is much larger now, and there is a higher presence of workers outside the perimeter than there were inside the perimeter before COVID-19. Leaders and developers have had a roadmap for how to meet tomorrow's cyber needs. That journey may have had a timeline for when we want to adopt specific solutions.

Because of the technology adoption, there's a significant opportunity now to start out in a secure manner. Looking at that journey – which may be a year out – it's time to consider: Is it a year out? Maybe that's something we should be doing tomorrow.

Start looking at your roadmap journey. It might make sense to bring it elsewhere because we are at a different stage of technology modernization.

Home is the New Enterprise Perimeter

How far does your security extend?

LEARN MORE

BlackBerry®

Industry Spotlight

Pairing Man and Machine on Zero Trust

An interview with Rich Thompson, Vice President of Global Sales Engineering, BlackBerry Limited

Since the COVID-19 pandemic began, the number of endpoints to defend has exploded as government employees started working remotely. These endpoints include devices such as laptops, smartphones and tablets, and they are leaving agencies more vulnerable than before. Going forward, the more endpoints agencies have, the more targets they will present to cyberthreats.

According to Rich Thompson, Vice President of Global Sales Engineering at enterprise software firm BlackBerry Limited, agencies aren't helpless against this trend. Thompson gave agencies three pointers for protecting themselves with zero trust cybersecurity, which assumes everyone and everything on IT networks is potentially threatening.

1. Expect human error

Humans are not perfect, and the mistakes they will inevitably make should factor into cybersecurity. Subsequently, expecting missteps can help guard agency resources better.

"Every time you increase friction on the user, they'll find ways around it or not use it," he said of agencies' applications. "If I lock it down, nobody would have access to it, but it would be 100% secure."

Thompson argued a zero-trust, risk-based approach to cybersecurity can effectively balance how employees work with the data their agencies must defend.

2. Turn to zero trust

Zero trust cybersecurity addresses de-perimeterization, or the gradual erosion of network boundaries. With zero trust, users must be capable of securely accessing data from anywhere no matter where it resides. To accomplish this, agencies must assume external and internal threats constantly exist on their endpoints and networks.

"Zero trust is an aspirational goal," he said. "It is the freedom to be productive and secure from anywhere in the world."

Using zero trust, agencies must authenticate and authorize every device, network flow and user accessing their data. Agencies should practice zero trust dynamically, using their latest information about potential security threats.

3. Leverage machine learning

Machine learning happens when computer algorithms "learn" how to perform functions using data. Machine learning can help agencies practice zero trust more efficiently. By analyzing data, these machines can inform security personnel about which threats deserve the most attention.

"Machine learning's greatest gift to the world is to provide data at scale in real time," Thompson said. "The machines can take care of themselves if given the proper data. It's more work than a human can do and on a quicker scale."

Aided by machine learning, humans can make more informed decisions about how to improve cybersecurity faster. For instance, machine learning can alert agencies about suspicious email attachments in real time. Additionally, solutions such as those BlackBerry Limited provides can aid agencies with practicing zero trust agencywide.

"The only way to achieve strong zero trust cybersecurity is with machine learning," Thompson said. "This area of technology continues to grow and evolve, transforming zero trust from aspiration to reality for both security teams and end users."

Best Practices in Cyber Intelligence

Whether agencies like it or not, many cybercriminals are intelligent. Cybercriminals risk severe penalties, so they must outfox their victims, or their activities won't be profitable.

Conversely, many agencies aren't as helpless as cybercriminals may think. Decades of cyberattacks have made agencies wary. Presently, many agencies realize that healthy cybersecurity requires constant IT.

Rising caution has thus made zero trust cybersecurity a hot topic among agencies. Zero trust thrives on two principles: First, agencies must continuously monitor all activities on their networks. Second, they must manage which devices and users can join their networks in addition to when, how and why. A key part of zero trust cybersecurity is monitoring and analyzing network activity, which is also part of thriving cyber intelligence.

If your agency isn't considering zero trust cybersecurity, here are seven tips for embracing it:

1 Fortifying Networks Comes First

Zero trust cybersecurity begins and ends with safe networks. To resist cyberthreats, agencies should assume all traffic is threatening regardless of its location until it has been inspected, authorized and secured.

Another valuable step is segmenting networks, so devices and users can access only the least number of resources required.

The final layer is continuously monitoring traffic for external and internal threats.

In concert, these features help ensure agencies are rarely in the dark about their threat landscapes.

2 Hazard-Proof People, Data and Workloads

Networks may fuel zero trust cybersecurity, but they aren't the philosophy's only components. Zero trust can also apply to agencies' data, people and workloads.

With data, agencies should develop, categorize, manage and secure classification frameworks for their data. Possibilities include high-risk, low-risk or other kinds of data; no matter the data, it should be encrypted in transit or at rest on their networks.

Continuously authenticating and monitoring people, meanwhile, provides better security than simply allowing them unwatched access once.

Finally, enforcing the same security controls for workloads across agencies' various applications enhances cybersecurity agencywide.

Leverage Least Privilege Access Control

Least privilege access control institutes a less-is-more mentality to keep data safe on agencies' networks. By restricting network access to precisely the things devices and users need, agencies can rest assured no one is obtaining materials they shouldn't be.

Recall that many government contractors and private sector employees work for agencies on a temporary, contractual basis. Agencies can restrict when these groups approach resources to business hours.

Tactics such as these provide agencies with sharper details about how their talent is behaving. Furthermore, if an agency's network is compromised, least privilege access control can keep attackers from infiltrating networks elsewhere.

Clean Up Cyber Hygiene

Cyber hygiene encompasses the basics everyone needs to reduce cybersecurity risks. Although there are no guarantees, agencies with vibrant cyber hygiene generally have hearty cybersecurity. As such, teaching their employees cyber hygiene fundamentals is a good investment for agencies.

Regrettably, many government employees aren't familiar with such classic cyberthreats as phishing. Agencies can erase this shortcoming by making education about common security risks frequent and memorable. Well-informed workers prepare for the worst, and they won't fall for tricks cybercriminals love.

Extend Security Beyond Agencies

As 2020 marches on, remote workforces are becoming more prevalent among agencies. More often, the future appears to have employees spread across huge distances but pursuing the same mission.

The truth is this arrangement births potential pitfalls for agencies. Whereas in-person offices predominantly use computers, remote ones may rely more on mobile devices. Soon, agencies will need to include smartphones, tablets, home printers and other tools into their cybersecurity assessments.

Agencies' threat landscapes only expand once the Internet of Things (IoT) enters the equation. IoT networks contain interrelated devices that can connect, exchange and store data. As IoT tools become more widespread, the number of possible flaws agencies must consider will multiply.

Make Connections Count

Most leaders won't admit it, but their agencies go it alone on cybersecurity. Too often, these agencies function as if other organizations can't contribute to their missions. Ironically, this mindset can leave agencies further from success.

Rather than hoard unique information, personnel and resources, agencies should spread the wealth. Not only does this contribute to agencies' individual success, but it reinforces America's cybersecurity posture.

Cybersecurity is perhaps best played as a team sport. The more agencies partner with one another – or the private sector – the more threat intelligence they'll have.

Never Get Comfortable

Agencies should never rest on their cybersecurity laurels. Should they let their guard down, agencies might discover they're not invincible.

So how do agencies keep from becoming easy prey? The answer is nonstop learning. Cybersecurity is an endless quest for knowledge, and there is always room for improvement.

To stay one step ahead of threats, agencies should consistently revisit their cybersecurity training and techniques. Agencies that are always evolving are harder for cyberattackers to strike.

Agencies can also practice this stance with technology. Rather than modernizing once, agencies should frequently upgrade their tools so they're consistently up to date.

CDM Approved Solutions From Carahsoft and Our Reseller Partners

The Continuous Diagnostics and Mitigation (CDM) Tools SIN provides products and services from cybersecurity vendors that enable network administrators to be constantly aware of the state of their respective networks, understand risks and threats, and identify and mitigate flaws at near-network speed.

Each of the following solutions providers have been certified by the CDM program on the approved products list and are available through Carahsoft's reseller partners and GSA Schedule 70, SIN 132-44 (CDM Tools).

Adobe
Akamai
ANOMALI
APPGUARD
APPLICATION SECURITY, INC.
ARMIS
BlackBerry CYLANCE
Bromium
CA A Broadcom Company technologies
corelight
CYBERARK
CYBERSPRINGE
DATAGUISE SENSITIVE DATA GOVERNANCE
DELL Technologies
DIGITALGUARDIAN
druva
Dtex
exabeam
EXPANSE
ExtraHop
f5
Fidelis Cybersecurity
FIREEYE
FORESCOUT
FORGEROCK
Gigamon
GitLab
Hewlett Packard Enterprise
HITACHI Inspire the Next
HYTRUST
IMPERVA
Infoblox FEDERAL
ivanti
Lookout
McAfee
MICRO FOCUS Government Solutions
netskope
New Relic
Nlyte Software
NUTANIX
okta
paloalto NETWORKS
proofpoint
qmulos
Qualys Continuous Security
QUANTUMSECURE part of HID Global
RADIANT LOGIC
Recorded Future
Red Hat
RSA
SafeNet AT
SailPoint
NS2
SAVIYNT
SECURONIX
servicenow
solarwinds government
splunk>
STEALTHbits TECHNOLOGIES
Symantec
THALES
ThreatConnect
THREATQUOTIENT
TREND MICRO
Trustwave Government Solutions
VENAFI
VERACODE
VERITAS
virtru
vmware
Vormetric Data Security
zscaler

For more information, contact the CDM team at Carahsoft at 855-4-DHS-CDM; CDM@carahsoft.com or visit carahsoft.com/cdm.

Understanding DoD's **Cyber Hotline**

Picture the Vulnerability Disclosure Program (VDP) as the hotline for reporting DoD's cybersecurity shortcomings. Nestled in DoD's Cyber Crime Center (DC3), the program makes the philosophy of "see something, say something" digital. At any time, ethical hackers can alert DoD to issues ranging from insecure networks to non-compliance with cybersecurity standards such as FISMA.

VDP Director Kris Johnson said openness and transparency are key to the initiative's success. Since launching in 2016, VDP has connected DoD with private sector researchers eager to strengthen federal cybersecurity. Nearly four years later, VDP shows how agencies such as DoD can advance their threat intelligence through collaboration.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: How does VDP work?

JOHNSON: If we look at DoD and compare it to the private sector, it's technically considered the largest corporation in the world with over 2.8 million employees. That doesn't include all the contracting support. So, it's truly huge. With that comes the largest network in attack surface area. As you add more devices on the network, there are more areas of vulnerability.

At VDP, we look at all DoD's public-facing websites and operate what I call left of boom. That means we operate before an actual breach, incident or exploit occurs on DoD networks. We're considered preventive maintenance. We do that by collaborating with the white hat researcher community – also known as ethical hackers – to discover those vulnerabilities so they can be fixed and mitigated before our adversaries can get to them.

How has VDP helped DoD's overall cybersecurity?

JOHNSON: We needed a front door that was open 24/7/365 to the researcher community to allow them to tell us what they find out there that's broken. We officially launched on Nov. 21, 2016.

A little over three years later, we've discovered 12,925 vulnerabilities. Of those vulnerabilities, 70% are valid and require action on our end. The other 30% don't fall within our current approved scope or could be duplicates or spam.

When these 12,925 vulnerabilities were discovered by researchers, they were unknown to DoD. They're basically about 13,000 gifts that were given to DoD. By fixing them, we've increased cyber hygiene across DoD.

Why is VDP's collaboration with people outside government critical for DoD's cybersecurity?

JOHNSON: We are the largest vulnerability disclosure program in the world per volume and per researchers. When we talk about DoD's relationship with hackers, we always err on the side of openness and transparency with the researchers. That builds trust between DoD and the researcher community.

We've had 1,460 unique researchers across 45 different countries that have participated in our program. At the end of the day, the collaboration between DoD and the researcher community is critical because we need their help to secure the world's largest network. It is tremendously unlikely that DoD will ever have enough military, civilians and contractors to cover every single area of the attack surface. So, all the help that we can get is appreciated.

What's Next for Cyber Intelligence?

Every day, citizens decide whether they can trust their most precious data with agencies. The choice they make depends largely on how intelligently these agencies handle cybersecurity.

In a world where solitary criminals can steal data from continents away, agencies can't afford to make uneducated cybersecurity judgments. At agencies that don't protect delicate data, the consequences are serious: financial penalties, public outrage and declining citizen trust.

Potentially, AI will only complicate this situation. AI's adaptability, speed and smarts make it a promising weapon for agencies. But cybercriminals could also wield AI against the same agencies it helps.

Yet cyber intelligence can help agencies outwit the opposition. Filtered through a zero-trust prism, cyber intelligence can make the difference between security victories and defeats.

Every day, agencies must pick what guides their cybersecurity. With cyber intelligence, agencies can rest assured they're heading in the right direction.

Thank You

Thank you to Blackberry Cylance, Carahsoft, FireEye, Recorded Future and Trend Micro for their support of this valuable resource for public sector professionals.

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the Master Government Aggregator™ for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector. For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

Author

Mark Hensch, Senior Staff Writer

Designer

Kaitlyn Baker, Creative Manager

Carahsoft's cyber intelligence solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, NASPO ValuePoint, OMNIA Partners, and numerous state and local contracts. Learn more at Carahsoft.com/Cybersecurity.

See the latest innovations in government IT from Carahsoft's vendor partners at Carahsoft.com/Innovation.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop