

EXPERT EDITION

Securing the Nation: Deep dive into federal SOCs

Insights from

- CISA
- GSA
- GAO
- Secret Service



A woman with short brown hair and glasses, wearing a white lab coat and a blue lanyard, is smiling and looking towards a man in a blue shirt who is partially visible on the right. They are in a server room with many computer monitors in the background. The lighting is blue and purple.

maximus

Cybersecurity for a Safer Tomorrow

Learn More >

TABLE OF CONTENTS

Why cybersecurity starts in the security operations center	4
How Secret Service's SOC answers data challenges	7
CISA's new plan aims to better align federal cybersecurity operations	10
GSA formalizes SOC framework to distribute incident response authorities	13
How modern security operations centers keep up with emerging threats	16



Joining forces on cyber's literal front line

The security operations center might just be the ultimate nexus for technology collaboration between government and industry.

In this ebook, we go in depth to understand the evolving role of the SOC in helping the government keep its systems, networks and users safe from cyber assaults. It's an assignment that's grown increasingly demanding as the network perimeter has melted away with the expansion of cloud computing and digital services.

One of the things that comes through in the interviews Federal News Network had with IT and security leaders is that these centers are joint endeavors that depend as much on contract teams as on federal employees.

And why is that?

The Government Accountability Office's Jennifer Franks put it this way: "We need fresh thinking, fresh insights. They might have also seen or even helped to implement security controls and infrastructures in other environments that can then help another agency to upskill their

environment." (Read more about GAO's work to inform SOC operations governmentwide on Page 4.)

It's also about the tools that contractor teams bring to the SOC and integrating them appropriately, pointed out the General Services Administration's Bo Berlas. Instead of just taking the approach that Vendor X will bring a certain tool set, "we're really thinking more strategically," he said. "What I mean by that is we provide a shared service to GSA, and GSA provides a shared service to the rest of the government. And I'm focused on making sure that we're effectively integrated and working very closely." (Learn more about GSA's SOC tactics on Page 13.)

To a person, the cyber leaders in this ebook agree on the critical need both to collaborate with contractors but also to make the teams inside their SOC's one. Continue on to find more insights from GAO and GSA, as well as from the Cybersecurity and Infrastructure Security Agency, the Secret Service and [Maximus](#).

Vanessa Roberts
Editor, Custom Content
Federal News Network

Cybersecurity starts in the security operations center

BY MICHELE SANDIFORD

To understand the functionality of cybersecurity at a federal agency, you might start by looking at the organization's security operations center. The SOC is made up of a group of cybersecurity experts that continuously monitor systems and technologies to prevent or respond to security threats in real time.

Think of cybersecurity as the big picture and the SOC as a window into those efforts. SOCs are responsible for keeping the data that government services use to stay in business safe. Over the last several years, there has been an increase in new procedures aimed at protecting the SOCs.

"There's a lot of federal guidance that addresses what is needed to protect security operations centers. And we actually had a report issued December 2023 that looks at federal agencies' information and response procedures. In that, we're highlighting that there's a set of guidance from various entities," said Jennifer Franks, director of information technology and cybersecurity at the Government Accountability Office, on [**Federal Monthly Insights –Securing the Nation: A deep dive into federal security operations.**](#)

There's a lot of federal guidance that addresses what is needed to protect security operations centers.

— Jennifer Franks, Director of IT and Cybersecurity, GAO



"So there was the cybersecurity executive order that really does enhance how government agencies need to secure their cloud-based infrastructures, as well as their agency on-premises networks."

Complexities below the SOC surface

The management of SOCs can also be a bit complicated, like who's in charge and what happens in the case of a security incident. The experts behind the security operations centers in the federal government vary by agency, technology and include both federal employees and contractors.

"The chief information security officers are usually the leaders of security

operations centers, who then directly report to the chief information officers. At some agencies, the CIOs are directly responsible for the SOC. It depends on how the agency is structured,” Franks said. “So when an incident or vulnerability occurs, when something needs to be patched, all of the data owners, the system owners, the business owners, are alerted immediately.”

Franks doesn’t manage the GAO security operations center, but she manages some of the networks that reside in the data operations center. “I do a magnitude of things for the agency. ... I do manage some of the information systems within our network. When the latest vulnerability did impact us, I was able to be at the table immediately for what needed to be done with alerting all of the responsible parties.”

Franks said that protecting critical business services in the federal government requires a menagerie of skills and efforts, including securing cloud-based infrastructures, managing zero trust operations, security event logging and incident response efforts.

“This gets complicated when we think about some of the automated processing that would help us be a little bit more timely in some of our investigative services,” Franks said.

She added that a lot of SOCs lack the skill sets that are now needed, “so being able to provide information sharing services across the various agencies, it will help with some of the visibility that is needed as well as some of the investigative services.”

Finding ways to tackle cyber together effectively

But solutions can introduce new challenges too, she added. Information sharing of incident and vulnerability reports between agencies that use the same productivity tools and services would be one solution to decreasing the amount of time it takes to address a vulnerability or breach, for instance. Yet, Franks pointed out, the risks can vary from agency to agency — sometimes extensively.

“The Department of Defense honestly has its own network and its own set of criteria because of the way it manages more national security, intel-related data, and the classification of their data is so much more sensitive than perhaps the Department of Education,” Franks told the [Federal Drive with Tom Temin](#).

If an agency has more sensitive data that the contractor may not be used to managing, we need to let that contractor know the intricacies and the sensitivities about how we need to manage the data. We need fresh thinking, fresh insights.

— GAO’s Jennifer Franks

“There are times where those entities may or may not want to share information, related data about vulnerabilities that are impacting their environments. But we’re looking at ways that we can do that in the near future, so that we’re not sharing sensitive-related information but at least enough vulnerability-related data that would help those entities as well as others with similar vulnerabilities. That would just help us remediate vulnerabilities a little faster.”

As with the federal government at large, SOCs have to find the right people, and those people need the right training. The mix of employees at SOCs are both federal and contractor, and they all bring necessary knowledge.

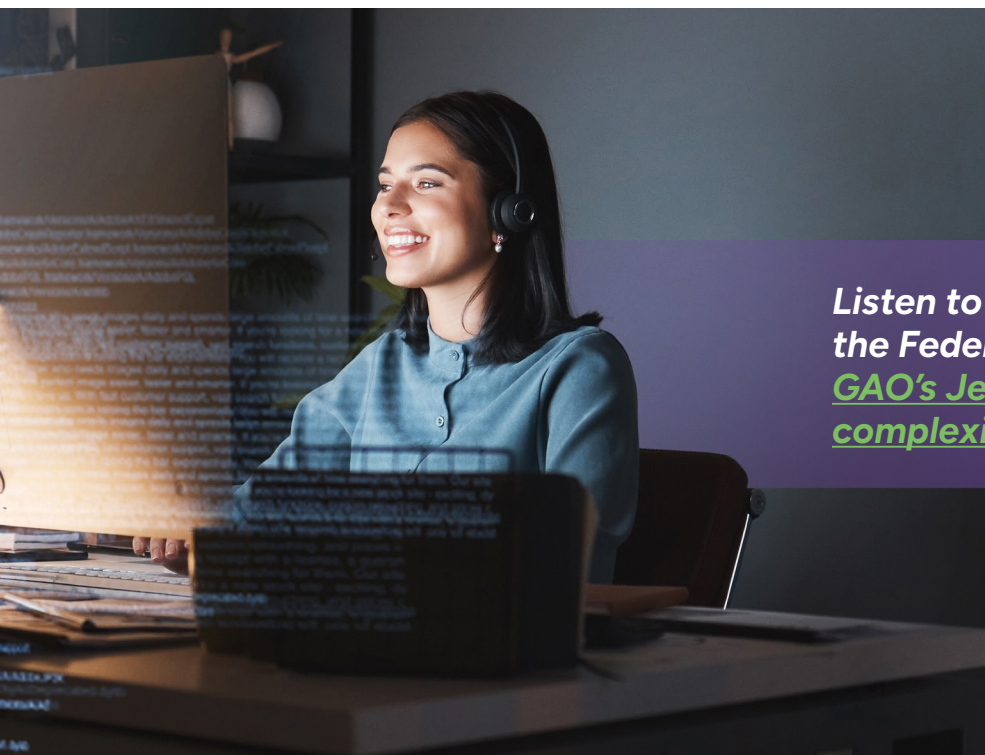
“If an agency has more sensitive data that the contractor may not be used to managing, we need to let that contractor know the intricacies and the sensitivities about how we need to manage the data,” Franks said. “We need fresh thinking, fresh insights. They might have also seen

or even helped to implement security controls and infrastructures in other environments that can then help another agency to upskill their environment.”

Taking a long-haul perspective on cyber

Rule number one of the SOCs is understanding that the job of protecting data is continuous.

“It’s no on person’s fault. If it’s connected to the network, it’s not an if, it’s a when,” Franks said. “A cyber incident, a breach, could inevitably happen. So providing those security control assessments, those risk management frameworks and just having that assessment where you identify all of the likelihoods of events and being ready to respond should an event occur, then you have a plan in place.” 🚀



Listen to the full discussion between the Federal Drive’s Tom Temin and GAO’s Jennifer Franks on tackling the complexities of managing federal SOCs

Tools and training: How Secret Service's SOC answers data challenges

BY DAISY THORNTON

One of the biggest challenges to running a security operations center is the data. Either there's too much for human analysts in the SOC to parse, or there are gaps in the data that create blind spots on the network. But Roy Luongo, chief information security officer for the Secret Service, said that's where having the right tools can help, particularly artificial intelligence.

"One thing I would ask people not to do is be too afraid of AI. Embrace AI. We need to get to a place where AI can be a tool, and as any tool, it could be used for ill or good. ... I think from cybersecurity, AI has the ability to pass through more data faster than a human can," Luongo said during [Federal Monthly Insights – Security operations centers](#).

"I envision a fully trained AI language model focusing on federal cybersecurity data. That's what I want it to learn on. I want it to understand that. And then I want to be able to query it with native language queries versus having to know SQL or KQL or pick-your-query language."

AI is especially useful when it comes to data normalization and minimization, Luongo said. It can handle the massive amounts of data that would overwhelm

One thing I would ask people not to do is be too afraid of AI. Embrace AI. We need to get to a place where AI can be a tool, and as any tool, it could be used for ill or good.

— Roy Luongo, Chief Information Security Officer, Secret Service



human analysts. And AI can reduce that dataset in ways that make it more useful. It can filter out redundant data from dissociated sources and help make indicators of compromise easier to spot.

The right tools for the workforce

But sometimes new tools can be a double-edged sword, Luongo said.

"If I bring in a new tool, I have to understand that the statement of work doesn't say you must supply people that



know X tool. I have to figure out how to integrate that. I have to provide that," he told the [Federal Drive with Tom Temin](#).

"I think a lot of times we forget that we're bringing in the newest and greatest tool, but integration will have our productivity hit. And too many people forget that they want a turnkey solution, which is great, but that doesn't mean all the employees — contractor or fed — are going to be as turnkey as that solution is going to be. So we have to understand that there is an integration period that incorporates the people in that skill set, not just the technology into our solution."

While the CISO will have the final say in what tools will get used in the SOC, Luongo said it's important to listen to contractors too. They're hired as cybersecurity experts; it would be shortsighted not to take advantage of their expertise, he said. They can be a huge resource in providing solutions outside of just filling an immediate cybersecurity need.

The right workforce for the SOC

Luongo said it's also important to consider the certifications contractors have, even if they're certified by the vendor. They're an indicator of potential skill: Whether or not they can apply them, that person at some point demonstrated knowledge, skills or abilities in that particular area.

"When we look at certifications — and we do it both with our government employees as well as with our contracted vendors — what we're really doing is buying down some risk. We're saying, 'Hey, if we start at this certification level, there's a level of assurance that they know certain things, that I don't have to train them,' or not," he said.


"It's really important to understand that that cert is just an indicator. And as part of good workforce development, I need to provide opportunities for people who may not need a cert today but have a career path that may in the future have the opportunity to achieve that cert."

He also said that the specific certification isn't as important as the knowledge or skills it attests to. Although some privilege levels require specific criteria, most of the time there's no advantage in prioritizing a single certification when three or four may fit the bill.

It's really important to understand that that cert is just an indicator. And as part of good workforce development, I need to provide opportunities for people who may not need a cert today but have a career path that may in the future have the opportunity to achieve that cert.

— Secret Service's Roy Luongo

And it's important not to differentiate between federal employees or contractors, Luongo said, outside of the bounds of specific regulations around privileged information, of course. But generally, good privilege access management will take care of that, he said. Otherwise, it's each staff members' role in the SOC that's important.

"If I'm paying a SOC employee, I personally don't want to be limited by the fact that that employee is a contractor or a federal employee," Luongo said. "They're doing a job. They need to have all the tools to do their job, and that includes elevated privileges. I have to provide trust in that person to do that." 

Listen to the full discussion between the Federal Drive's Tom Temin and the [Secret Service's Roy Luongo on identifying the right people and tools for the modern SOC](#)

CISA's new plan aims to better align federal cybersecurity operations

BY DERACE LAUDERDALE

The Cybersecurity and Infrastructure Security Agency is introducing a new strategic approach for 2024. The Federal Enterprise Operations Cyber Alignment Plan will bring agencies together to compare notes on recent cyber incidents and align behind a common path forward, especially for analysts in security operations centers.

"It's important for CISA as we look into fiscal 2024 and really have that strategic outlook of what the future holds. What does the cybersecurity threat landscape look like? It was important for CISA to convene all federal agencies, take an opportunity to walk through what we experienced in 2023 — walk through the major incidents, the cybersecurity issues that we've been dealing with as a community — and work toward an action plan, an operational alignment plan for us to think about what comes next. What's in 2024?" said Michael Duffy, associate director of CISA's Cybersecurity Division, during [Federal Monthly Insights – Security operations centers](#).

"The suite of binding operational directives, for everything from known exploited vulnerabilities to network

management interfaces, down to the asset visibility and vulnerability enumeration, that has been a meaningful shift in the way that we look at cybersecurity defense operations across the enterprise. It's important for us, as we start the new year, to bring that community together, to talk about what we're seeing, the challenges we have and, ultimately, come away with some commitments from them."

Collaborating on cyber across all levels of government

CISA is committed to working collaboratively with state and local governments, election officials and federal partners to manage risks to the nation's infrastructure. The continued evolution of the Continuous Diagnostics and Mitigation (CDM) dashboard to help agencies improve how they manage their cyber environments remains a priority, as does the [Secure Cloud Business Application \(SCuBA\)](#), which ensures agencies are using a baseline of secure workplace and collaboration applications in the cloud.

"The concept of alignment is an important shift in the way that we're approaching

We've seen decreases in the number of KEVs across agency enterprises, and I think that's a really good place to be, as we're talking about reducing the attack surface and moving into more strategic efforts like zero trust.

— Michael Duffy, Associate Director, Cybersecurity Division, CISA



this,” Duffy said. “We designed an operational cyber enterprise plan, which identified all of the areas that we think the federal government, as an enterprise, should be focusing on improvement actions. We had fantastic feedback from chief information security officers and agency teams.”

Taking the pulse of the CISO community

In a survey of CISOs across government, one challenge that emerged for CISA was identifying what else is needed for cyber success within agencies.

“What we heard from agencies was these are bigger than the cybersecurity team,” Duffy said. “When we’re talking about advancing hardening Active Directory or advancing CDM into the next era of

cybersecurity operations, this is more than just a small team of cyber practitioners can handle on their own. This is frankly more than the headquarters CISO shop can handle on their own. This is truly something that will require a whole-of-government, whole-of-federated-agency approach to ensure that we’re successful.”

The known exploited vulnerabilities (KEV) catalog also stood out in the survey as a top priority. CISA recommended agencies monitor the KEV catalog and prioritize addressing vulnerabilities to reduce the chances of being attacked.

“That was eye opening to us. It meant that the binding operational directive was seeing success,” Duffy said. “We’ve seen decreases in the number of KEVs across agency enterprises, and I think that’s a really good place to be, as we’re talking about reducing the attack surface and moving into more strategic efforts like zero trust.”

Ensuring zero trust takes hold

CISA’s Zero Trust Model is used as a reference for agencies to create their zero trust architectures. It seeks to inform agencies in ways to develop implementation plans where CISA can support and generate solutions.

“The federal zero trust managers community of practice is an important step forward for CISA. It was our way to convene all of those agency officials designated as their agency’s zero trust lead. It was important for CISA to say, as we operationalize the next step, the

series of zero trust application maturity model, that we are able to convene that community, have a meaningful dialogue and connect them with each other. This is a community where CISA isn't always the one that has the right level of answer for an agency. They want to speak with their peers. They want to have an open discussion about their challenges. And we're providing that," Duffy told the [Federal Drive with Tom Temin](#).

"We've coupled that with a training program where we are able to provide a standard baseline of understanding for these zero trust managers so they can go into these conversations using the same terminology, using the same approaches and applying the same tricks of the trade — the way that the zero trust managers are considering this challenge at the enterprise level. We're convening, we're training, and we're ultimately ensuring that the federal government has the workforce

they need for zero trust and a sustained effort in zero trust for the long haul."

CISA is also making progress in mobile application vetting, a service it's provided to 15 agencies so far. MAV identifies app vulnerabilities and potential risks, while also allowing agencies to make risk-based decisions.

"It's a great resource that CISA is providing to allow a federal agency to say, 'I've taken every step necessary to secure and configure an application that will ultimately be used by either federal government employees or the public,'" Duffy said. "Our ability to show value in the data that we collect centrally is paramount. I think that there is an understanding that CISA is primarily a partnership organization. We are working with these agencies to secure their environment as much as they are."

CISA isn't always the one that has the right level of answer for an agency. They want to speak with their peers. They want to have an open discussion about their challenges. And we're providing that.

— CISA's Michael Duffy

Listen to the full discussion between the Federal Drive's Tom Temin and [CISA's Michael Duffy on the agency's latest cyber initiatives](#)

GSA formalizes SOC framework to distribute incident response authorities

BY DAISY THORNTON

The General Services Administration has found a unique working model for its security operations center: By focusing on integration of related shared services, it's delivering SOC capabilities more like a product than a service.

This tactic provides greater accountability, transparency and input for stakeholders, while better integrating federal employees with contractors, said Bo Belas, GSA's chief information security officer. Next, GSA intends to experiment with the way it delegates authorities within its SOC.

The agency is in the process of formalizing an authorities framework that dictates what decisions and actions can be taken by an analyst and what has to flow upwards from there. Providing teams the capability to respond to lower-level incidents prevents them from escalating, but some things require the input of the incident commander, the product owner, the SOC director and even Belas. For example, taking any system offline always rises to the CISO level.

"The only exception is when there is a clear and imminent threat and where we have to take a site offline in coordination, and the time that it takes to facilitate that coordination would result in a negative impact to the agency and the program

We follow a one-GSA, one-cyber model. It's focused on achieving unified defense for all our information systems and within the enterprise. We do not like silos.

— Bo Belas, Chief Information Security Officer, GSA



at large, in which case those calls are made directly by me," Belas said on [*Federal Monthly Insights – Securing the Nation: A deep dive into federal security operations.*](#)

That's all in service to the SOC's formalized incident response program, which includes coordination across all the stakeholders, including GSA's legal, client and privacy teams, and its business executives. Belas said that integration has helped communicate more broadly the need for the SOC. GSA has already answered common questions around what

it is, the integrations and tools it uses, and its responsibilities.

The SOC's mission

That allows the SOC to focus on its organizing principles.

"We follow a one-GSA, one-cyber model. It's focused on achieving unified defense for all our information systems and within the enterprise," Berlas said on the [Federal Drive with Tom Temin](#). "We do not like silos. We're all integrated and must act as one. Visibility is something that we do not compromise on. It's required at the agency level versus at the system level. And what that means is every information system must report and integrate into the top-line agency security operations center and deeply, deeply integrate with the corresponding set of cybersecurity tooling."

That's helping GSA meet the requirements in recent cybersecurity regulations, including the cybersecurity executive order and the numerous memos that have followed. But achieving that level of compliance is only half the battle. It's just as important to ensure that compliance leads to actual cyber resiliency, Berlas said. That's why the SOC works within the agency, as well as with the Cybersecurity and Infrastructure Security Agency, to ensure proper interpretation of all cyber regulations.

We live in an age where certification is important, but your ability, your tech ability, is equally — if not more — important. So we don't essentially go through and discount the fact that somebody lacks a certification.

— GSA's Bo Berlas



Finding and keeping SOC talent

Berlas said when recruiting, hiring and retaining SOC personnel, certifications matter, but they're not all that matters. GSA's SOC personnel, an integrated mixture of contractors and federal employees, are all screened for both the standard background checks and for technical prowess.


"We live in an age where certification is important, but your ability, your tech ability, is equally — if not more — important. So we don't essentially go through and discount the fact that somebody lacks a certification," Berlas said.

"We essentially go through and do deep-dive interviews with our teams, ensuring that we're able to have them ask and answer really technical questions that you either know or you don't know. And a study exam-prep-type answer probably will not be able to cut it. And I think that's where we really need to focus based more on skills than we do on certifications. But certifications are also important. They do essentially speak to a certain level of commitment to your craft. And having one, I think, is a sign or indication of that. And it's certainly valued, but it's not the driving factor."

One way GSA's SOC ensures team members have the requisite skills, while also ensuring seamless employee-contractor integration, is by pairing new staff members with existing ones as they're onboarding. That way GSA prevents anyone from falling behind and ingrains collaboration from day one.

Choosing the appropriate SOC tools

Berlas said contractors often bring their own tools along, but GSA maintains the final decision over what tools are used by SOC teams.

"Tooling is always defined at the program level by leadership, by my directors," he said. "Challenges corresponding to the flavor-of-the-day tools presses and creates all kinds of challenges because they're tied to a given contractor with unique competencies or background in a given toolset. We're really thinking more strategically. What I mean by that is we provide a shared service to GSA, and GSA provides a shared service to the rest of the government. And I'm focused on making sure that we're effectively integrated and working very closely with that. Any product service capability that CISA has, I'll be first in line to effectively leverage today." 

[Listen to the full discussion between the Federal Drive's Tom Temin and GSA's Bo Berlas on improving SOC's incident response capabilities](#)

How modern security operations centers keep up with emerging threats

BY TOM TEMIN

Artificial intelligence gives rocket fuel to malicious hackers. That means cybersecurity practitioners had better prepare themselves and their security operations centers.

“Cybersecurity is rapidly changing, and a big introduction is what’s happening in AI,” said Dean Irwin, senior director of cybersecurity at [Maximus](#). “I see that more as an offensive concern for AI, more than the defensive side. It’s making threat actors able to be very sophisticated.”

One way for security operations center staffs to keep up is by requiring continuous training so SOC staff can keep up with the threats they encounter, he said on [Federal Monthly Insights – A deep dive into federal security operations](#).

Irwin, who oversees Maximus teams operating government owned SOCs, added, “We are constantly training and certifying in specific technologies. In one of our SOCs, we have three certifications per employee, which is pretty advanced.”

Cornering AI cyberthreats

AI has revved hackers’ capabilities in several common cyberthreats, Irwin said. Identity theft ranks high among them.

“A lot of surfaces are now in the cloud,” he said, and so the model of moats and perimeter defense no longer applies. “In a cloud environment, it’s all about identity.” Deep fakes, both video voiceprints or even fingerprints, can impersonate an employee or a government official.

AI also powers ever more potent spear phishing attacks, Irwin said. The more information an attacker obtains, the more carefully it can craft an email. The latest technique, Irwin said, is called whaling, where phishing attempts target the top executives in an organization. Such attacks are difficult for tools in the SOC to detect, because the emails arrive singly or in low numbers. Therefore, SOCs must rely not only on signals from detection tools but also on reports from users who receive suspicious emails, Irwin said.

SOC staffs have a third way to get ahead of threats, “what we call CTI, or cyber threat intelligence,” Irwin said. This takes people with knowledge of how to explore

A lot of surfaces are now in the cloud. ... In a cloud environment, it's all about identity.

— Dean Irwin, Senior Director of Cybersecurity, Maximus



encrypted sites invisible to standard browsers, known as the dark web. It is on the dark web that hacker groups discuss their plans and intended targets, Irwin said.

This all makes the SOC a multifunctional blend of human intelligence and technical detection, he said. It's also bidirectional, he said, not looking only for inbound threats but also checking for "beaconing" signals from executables that got into the network undetected initially.

Implementing SOC best practices

When relying on contractor support for SOC, Irwin recommends open communication between SOC staff, the units that own applications and services, and the IT operations staff. He said that in one instance, Maximus people operate the SOC for a system encompassing 60,000 endpoints and 5,000 servers.

Occasionally, the SOC will notice something amiss and contact the system owner.

"So if we say, 'Hey, one of your servers is beaconing out,' they're like, 'No, it's not,'" Irwin said. Because the SOC rarely has the authority to take a system offline, it must have the verification on hand to convince the system owner.

"We have to prove to the system owner that this is actually a compromise and not normal traffic," Irwin said. "They aren't practitioners in the cyber area, so we have to educate them on what happens."

A thorough SOC, Irwin said, will also pay attention to vulnerabilities that arise as systems age, and even analyze legacy code for vulnerabilities.

Irwin outlined three basic components of a SOC, understanding of which will help with selection of an operational vendor:

- The security event information management (SEIM) system. It stays on the lookout for intrusions and attempts.
- End point monitoring. This section is likely to operate a variety of tools because of the diversity of end points – smart phones, notebook and desktop PCs, peripherals, and sensors or internet-of-things devices.
- A data "sandbox" where cybersecurity practitioners analyze log data or malware packages they find, all using the agency's commercial or self-programmed tools.

Irwin said a reliable SOC staff will know and understand the types of modernization an agency is applying to its systems. One type consists of simply shifting workloads from data centers to commercial clouds.

“You’re not improving any of the security, you’re just changing where it runs, where it executes from,” he said.

Or agencies rewrite or refactor legacy applications into modern languages. In such cases, he said, “there’s a big push now for secure software design. And there’s what are called memory safe languages. If applications are written in that language, it’s a lot harder to have a vulnerability.”

Irwin noted that with growing quantities of data undergoing encryption, a SOC staff must be adept at using metadata to analyze traffic to detect abnormalities.

Still another area a skilled SOC staff will understand is provenance of software, what libraries or open source code sets an application was built with. This varies among IoT, operational technology and data processing applications, Irwin said. He said the various cross-currents of technology underscore the need for staff certified in those technologies.

Irwin said, “In fact, we, Maximus, give SOC staff members a little bump of reward every time they get a certification, because we believe that helps show they understand it.” 🚀

There’s a big push now for secure software design. And there’s what are called memory safe languages. If applications are written in that language, it’s a lot harder to have a vulnerability.

— Maximus’ Dean Irwin

Watch and listen to the full discussion between the Federal Drive’s Tom Temin and [Maximus’ Dean Irwin on modernizing the security operations center](#)