How agencies can leverage 'cyber intelligence' to

TRANSFORM CYBERSECURITY OPERATIONS

By CyberScoop | FedScoop | StateScoop Staff

Intelligence drives operations in all matters of national security. But when it comes to government agencies at all levels, from state and local to large Cabinet-level agencies in the federal sector, cybersecurity seems to be one area that needs more relevant, robust and real-time intelligence than ever.

Public sector organizations, like most others, are challenged by the shortage of both trained cyber staff and budget dedicated to cyber. These challenges have made it difficult for government agencies to move beyond a reactive posture where security product alerts tend to drive the cyber team's activities.

Steady staff turnover and an overcrowded vendor marketplace have resulted in operating environments where agencies:

- Have too many cybersecurity tools to manage effectively.
- Aren't able to integrate or fully utilize the tools they have.
- Find their cybersecurity teams are overworked and overly dependent upon tools to alert them to events.

All of this results in an urgent need for IT security teams to consider taking a smarter approach by:

- Focusing on the data and systems that matter most.
- Automating wherever possible, allowing staff to perform more valuable tasks such as threat hunting.
- Implementing security controls that will bring the most protection value per dollar and man hour.

However, the most forward-leaning leaders — whether they are a federal agency executive, a governor, a chief information officer or a chief information security officer — have also embraced "cyber intelligence" as a key driver behind their shift away from a costly, less effective and reactive security posture, toward one that is focused on detecting the specific attacks that their adversaries are using to attack similar victims.

Focusing on what matters most

Cyber intelligence "provides an understanding of who the attacker is, what they are after and how they work. This information is important to know should you become a victim," said Tom Guarente, senior director at FireEye, Inc. "The type of intelligence that you have access to matters most. Intelligence shouldn't only rely on telling you what has already happened elsewhere, but what may be happening today or tomorrow."

The ultimate goal, according to Guarente, is to shrink the time between incident and response. Today, the name of the game is effective and efficient use of time and resources to focus on the actual threats and threat actors targeting your organization.

"Government agencies need assistance in complementing their internal talent," Guarente said. "They have funding challenges and they have heterogeneous environments that fire off an incredible amount of alerts that make it very difficult to be as effective as they want to be. If they can shift to an approach, where they are using cyber intelligence effectively to understand what alerts

matter most, it will allow them to respond in a much more effective manner."

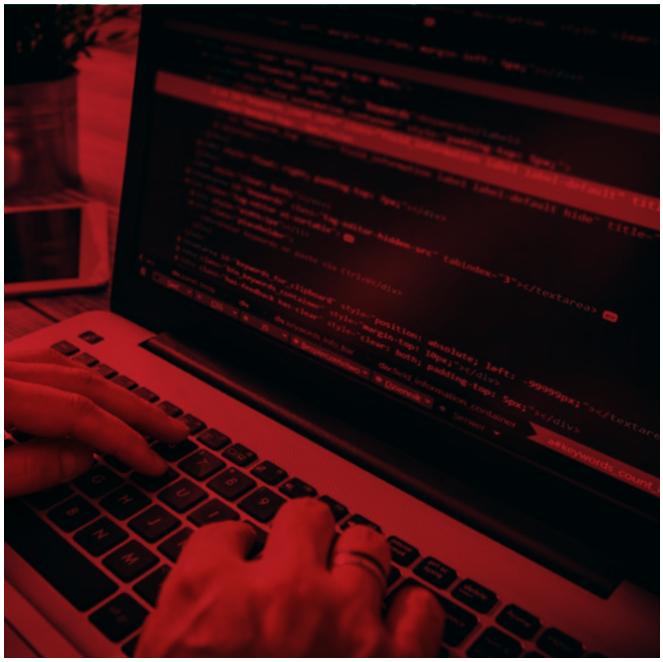
Separating intelligence from awareness

So how does cyber intelligence differ from awareness and how can agencies operate more effectively with it?

Cyberthreat intelligence captures specific knowledge about adversaries, their motivations, intentions, methods and likely targets. It encompasses exactly who is likely to attack you, and precisely what they are likely to do. That's a fundamentally different perspective than simply having awareness of who or what are on your networks.

Cyberthreat intelligence also serves as an essential element in establishing the ability to detect new and emerging threats early on, investigate them quickly and respond to them effectively. Another way to look at it: Cyberthreat intelligence enables organizations to build a proactive cyber operations capability aligned to protect what matters most from those that are most likely to attack you for it.

"All of this means that cybersecurity leaders can leverage effective cyberthreat intelligence to simplify their overall challenges, become more proactive and reduce the overall risk to the organization," said Tom Topping, FireEye's senior director of federal strategic programs and initiatives.



Leveraging intelligence for your organization

According to Topping, there are four key characteristics of cyber intelligence that leaders should be looking for:

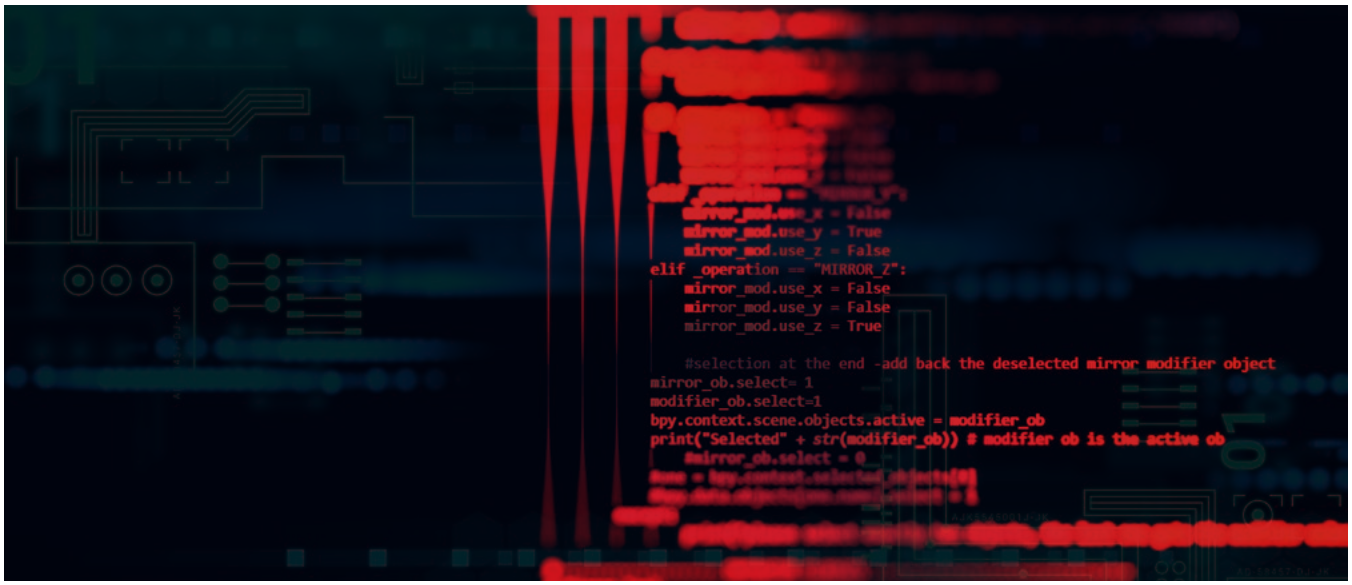
1. **It has to be relevant to your organization.** Not all threat actors are focusing on your organization or your industry. Each industry faces its own specific set of relevant attackers, along with the types of attacks those attackers utilize to achieve their objectives. Additionally, each organization has its own unique set of resources or activities that it must protect.

2. **It has to be timely.** Agencies need to be wary of leveraging old threat data that is just adding to the noise that analysts must sift through. Those evaluating various sources of cyberthreats must ensure that the intelligence is current, especially because cyberthreat actors change their attacks and infrastructure frequently. Hunting for, or blocking, information that is no longer relevant is a waste of scarce resources.

3. **It has to be accurate.** Cyberthreat intelligence enables the ability to focus. But that also means if your cyber team and tools are focused in the wrong direction, false positives will arise, and other attacks can go undetected for too long. Therefore, it's important that the cyber intelligence maps accurately to your circumstances.

4. **It has to be presented in a way that's actionable.** The intelligence must be provided in the formats and methods that are useful to the various components of your organization. When delivered in the most effective manor, cyberthreat intelligence will:

    - Enable executive leadership to clearly understand the risks to the organization.
    - Enable cyber leadership to employ technology and personnel resources in the most effective manner.
    - Enable cyber practitioners to detect, investigate and respond in the shortest time possible.



According to Topping, organizations that do not fully leverage comprehensive cyber intelligence are not utilizing their resources in the most effective manner.

He offers a telling analogy: "It's like an NFL team trying to prepare for a game without any game films to study and no idea who they're going to play," he said. "Leveraging comprehensive cyber intelligence enables the organization to focus on detecting and reacting to the 'plays' that their most dangerous cyber adversaries are most likely to run against them."

"At the end of the day, organizations are not in business to defend themselves. They have a different mission. For cyber, every organization needs to mitigate the right amount of risk In the most effective and cost-efficient way. And that means they have to focus on the threats that matter the most," Topping said.

And focus often comes down to a few simple questions, Topping said. Agency leaders should be asking:

- Is your SOC reacting to events or planning for events?
- Do you know which threat actors are most likely to attack you and why?
- Are your defenses tuned to look for the indicators that your most-likely threat actors will leave behind when they come calling?"

Turning intelligence into advantage

Embracing cyber intelligence also brings strategic advantages to the CIO and CISO, Topping said. When budgets are on the line and resources are at stake, connecting on a personal level matters. Leveraging accurate, timely and relevant cyber intelligence helps CISOs describe security issues in terms that senior agency and political leaders can understand.

"Cyber intelligence facilitates communication from the SOC all the way up to the agency or state leadership," he said. "It helps facilitate discussions about risk management and it helps the leadership appreciate the threat and helps the people on the front line get the budget they need."

Those agencies starting down the path of embracing cyber intelligence are the ones asking for help, seeking best practices and working with partners who understand how to embed threat intelligence into their systems, said Guarente.

"Those which are not there yet typically don't try to go outside their organization," he said. "It generally takes a dynamic leader who is progressive, believes in collaboration, shared experience and working through partnership to start this journey."

Learn more about how to leverage threat intelligence at your agency.

This Tech Brief was produced by **CyberScoop** | **FedScoop** | **StateScoop** for, and sponsored by, **FireEye**.

cyberscoop | fedscoop FireEye