CSO

SPONSORED CONTENT Telos aws

# Three Steps to Creating Actionable Cyber Threat Intelligence

Unfortunately, enterprise cybersecurity has become a game of reacting rather than preventing. The challenge is that most legacy-based cybersystems are focused on analyzing past warnings and attacks — but the playing field has changed.

Cybercriminals have become more sophisticated. They have learned how to hide in plain sight, avoiding signature-, anomaly-, and behavior-based systems and expertly emulating legitimate traffic. They are hiding in our networks, expanding laterally, and waiting to attack.

To combat these new cyberthreats, effective tech leaders are focused on threat intelligence. In fact, the global threat intelligence market size is projected to grow from $11.6 billion in 2021 to $15.8 billion by 2026, at a compound annual growth rate (CAGR) of 6.5%.

"Our Foundry research shows that cybersecurity is a top concern for CEOs, the board of directors, line-of-business executives, CIOs — virtually everyone in the organization," says John Gallant, enterprise consulting director at Foundry. "The reputational, operational, and financial risks are huge, and there is a growing sense that we are falling farther and farther behind in identifying and preventing threats."

## Hackers are winning the battle of the enterprise

Today's complex security stacks require much more care and handling than those of the past. An enterprise is more likely to get its threat information from multiple entry points rather than a standalone resource, especially as different providers or resources enable businesses to customize their experience. The requirement of securing one perimeter has now become securing many — significantly expanding the threat landscape and reducing overall cybersecurity.

"The sad reality is that enterprises have many, many cybersecurity tools. They are awash in security data, but they are still struggling to keep up with new threats and are fighting from their heels," Gallant says. "Enterprises are reactive, rather than proactive, and that is a real problem, given the pace of change in the threat landscape."

Although enterprises are investing in cybersecurity solutions, the hackers are winning in many cases. For example, according to "Cost of a Data Breach Report 2022," published by IBM Security, the average cost of a data breach reached an all-time high of $4.35 million, an increase of almost 13% since 2020.

> **“It isn’t enough to amass security data and try to parse it all for insights after the fact. We need real-time information on the hacker ecosystem, so we can identify and prevent threats.”**
>
> *John Gallant, enterprise consulting director, Foundry*

In addition, a report from the U.S. Department of Treasury found that U.S. banks and financial institutions processed roughly $1.2 billion in probable ransomware payments in 2021, a new record and almost triple the amount of the previous year.

### Illuminating the hacker ecosystem

This uneven fight already has left many enterprises reeling. For instance, even though the cybersecurity systems of a major power utility didn’t identify attacks on its network, its security operations team was not convinced. It worked with Telos Advanced Cyber Analytics (ACA) and in five days, it located hundreds of successful network breaches from a malicious nation-state-sponsored organization that were previously unknown.

These cybercriminals may have been testing the waters for a long time before choosing the right time to strike. But why didn’t the company’s legacy systems detect the breaches? Because the company depended on past information — this source was malicious before, so block it now — and red flags — this *may* be a threat, this *may* not be. Meanwhile, the attacking nation-state-sponsored organization used sophisticated tools to pretend that it was accessing the network from a local safe site — and not an overseas hidden one. It repeatedly slipped under the radar.

Past behavior and countless red flags are information, not insight. It is too late to do anything, and, even if you did want to take action, you wouldn’t know what action to take. Hence the shift from report-based threat assessment tools to actionable threat intelligence using “fact of” analytics to identify today’s and tomorrow’s threats. Organizations need context at speed and scale to make the data actionable. They need insight to illuminate hacker ecosystems and act rather than react.

“It isn’t enough to amass security data and try to parse it all for insights after the fact. We need real-time information on the hacker ecosystem, so we can identify and prevent threats,” Gallant says. “And we need to continue to learn more about the hacker ecosystem and build our threat awareness and responsiveness.”

### Three steps to actionable threat intelligence

There are crucial actions that enterprises can take right now to increase their visibility into the entire threat landscape. The first step is to contextualize your external threat environment so it is specific to your IT systems and network. Do all the indicators match up? In the case of the power company, it initially did not compare the information such as the location and infrastructure used, with other data sources.

The second step is to analyze the data by using automated analytics to attribute who, what, when, where, and why. You may notice a pattern here: Look for tools and techniques that build on what you have. A powerful capability such as Telos ACA will augment your installed systems by proactively examining your perimeter, but it does not require you to purchase new technology.

Last, once you proactively find the hackers, you need to block them, immediately. Telos ACA not only detects malicious access from one source but also recognizes the related sources that are getting access now or could in the future. All of the bad actors can be blocked.

Threat intelligence solutions such as Telos ACA are critical to your cybersystems and operations. Create actionable intelligence now so you’ll know what action to take — and how to prevent bad actors from striking hard later.

**The best way to learn more about Telos Advanced Cyber Analytics (ACA) is to talk with a Telos cybersecurity expert and develop use cases for your organization. Go to telos.com and complete the “Contact Us” form, and we will start a discussion with you.**