CISCO TALOS: WHERE THREAT INTELLIGENCE AND ENDPOINT SECURITY CONNECT
Insights gleaned from a massive amount of global threat-intelligence telemetry, such as that gathered by Cisco Talos and similar services, can be of tremendous benefit to your organization, especially when it comes to anticipating and preparing for new threats and adversaries.

The sheer breadth of Cisco’s resources, and the dissemination of information pushed out through Cisco’s products and services, the freely available Cisco Talos intelligence blog and Cisco-managed Snort and ClamAV rules, benefit both Cisco’s paying clients as well as the entire information-security community.

But managing that telemetry in meaningful, actionable ways isn’t always easy. Smaller companies with less-developed security programs may require more immediate, practical instruction and advice and may not see as many benefits from tapping into a telemetry firehose. It really depends on whether your firm requires the kind of information that global threat intelligence can provide.

To better understand the challenge and put the telemetry to effective use, one can learn much from the experiences of Cisco Talos, the company’s threat intelligence group. The Talos team gathers intelligence from Cisco’s managed endpoints, networking hardware and software implementations around the world, along with open-source information and a variety of global threat intelligence partnerships. It’s a massive flow of information, explains Cisco Talos Principal Engineer Ryan Liles.

“Cisco has embraced the strategy of security everywhere,” says Liles. “We are building telemetry and data capture into the entire product line in everything Cisco builds, starting at the network level and going all the way to the endpoint.”

That gives Talos immense visibility across hundreds of thousands of networks worldwide, he says, adding: “We get to see all of this data, all of this telemetry. We can use that information to make determinations about new and emerging threat actors, existing threat actors, and the way that they are evolving their techniques to attack individuals, enterprises, and governments.”

Three key points
Talos has a complex strategy to deal with the evolving threat landscape, and it can be distilled down into three key areas, explained Liles and Adam Tomeo, senior product manager covering Cisco Secure Endpoint:

1. **To stop more, you have to see more:**

   Tomeo described this as the aggregation of data from Cisco products that collect information throughout the enterprise, from employees working at home to the data center. “The only people that get more telemetry than us are telecoms,” he said, “because they’re actually the pipes that all the stuff transfers through as it’s leaving the network gear. Talos is one of the largest threat intelligence...
agencies in the world short of being governmental.”

2. **Rapid analysis for greater threat context:**
That massive inflow of data — multiple petabytes of telemetry at a time, according to Liles — is analyzed by Cisco and cross-correlated to quickly notice patterns of behavior, events and file trajectories. That happens not just within one enterprise, but worldwide across Cisco’s vast network of client devices. “Just by the sheer volume of data that we have, we’re able to correlate that and pick out from all of the noise,” Liles said. “We’re able to pick out the pins and needles in the haystack and say this is something that requires one of our hundreds of vulnerability researchers or malware researchers or reverse engineers.”

3. **See once, protect everywhere:**
All the identifiable useful information is then sent out to Cisco client devices worldwide, across product lines, to stop and prevent the newest threats as they appear. “If one person has seen something,” Tomeo explained, “everyone has seen it and can now identify, isolate the threat, and alert the appropriate teams for action.”

Talos has been greatly aided in its mission by acquisitions over the years, including the Snort open-source intrusion-detection-and-prevention platform, the open-source Unix/Linux/macOS antivirus toolkit ClamAV, the email spam reporting service SpamCop and the SourceFire Vulnerability Research Team, which was combined with similar existing Cisco groups to form Cisco Talos.

“Talos as the organization ... kind of evolved from a combination of several groups, starting with the SourceFire VRT acquisition back in 2014,” said Liles. “Talos owns all of the detection content for Snort, which is an open-source platform — again, these are rules and signatures that we make available to anyone who uses this Snort platform — Clam AV, same way.”

**Sharing is caring**
Much of that security content comes in the form of information freely available on the [Talos blog](https://www.cisco.com/c/en/us/about/talos.html). Other outlets include the biweekly [Beers with Talos podcast](https://www.cisco.com/c/en/us/about/talos/podcast.html), the weekly [Threat Source newsletter](https://www.cisco.com/c/en/us/about/talos/threat-source-newsletter.html), the Cisco Talos [Reputation Center](https://www.cisco.com/c/en/us/about/talos/reputation-center.html), the Cisco Talos [community forums](https://www.cisco.com/c/en/us/about/talos/community-forum.html), the Cisco Talos [YouTube channel](https://www.youtube.com/cisco) and [Twitter feed](https://twitter.com/cisco), and a lot of other free software, resources and data made available to the public.

“Talos as the organization ... kind of evolved from a combination of several groups, starting with the SourceFire VRT acquisition back in 2014. Talos owns all of the detection content for Snort, which is an open-source platform — again, these are rules and signatures that we make available to anyone who uses this Snort platform — Clam AV, same way.”

– Ryan Liles: Principal engineer, Cisco Talos

Anyone “can reach out to ask Talos and get responses directly from some of the Talos security analysts, malware researchers, vulnerability researchers, and security
analysts themselves,” said Liles. “We respond directly to Ask Talos queries just to help kind of up the game, up the level of defensive technology worldwide, regardless of the products they’re using.”

**Working with NetSecOPEN and MITRE**

Talos also works closely with testing organizations such as NetSecOPEN, which evaluates network-security solutions, and contributes to both the MITRE ATT&CK framework and MITRE’s Engenuity ATT&CK endpoint-protection evaluations.

“We actually have two groups that are very focused on MITRE internally inside TALOS -- the detection and response group, which we internally call DRG, and then the research and test team,” said Liles.

“Individually, they have team members that work very closely with some of the team leads over at MITRE ATT&CK where we do information sharing between the teams. We pass them indicators of compromise that we’ve seen. We pass them new exploits that we may see, things that they can use to continue to build out the framework.”

(For more on **how Cisco works with the MITRE Engenuity ATT&CK endpoint-protection evaluations**, see the CyberRisk Alliance paper “**MITRE Engenuity ATT&CK: What it is and how to use it for stronger security posture**”.)

Talos tries to be as involved with as many third-party test labs and as many open-source frameworks for security validation and testing as possible, Liles said. The team also works with both government and private entities to share information back and forth and help them to develop the capability to build, test and validate industry-wide security products.

---

**Talos discovery: WhisperGate targeting Ukraine**

For example, in January, Talos spotted a new wiper campaign that resembled NotPetya, the Russian wiper that attacked Ukrainian institutions in June 2017 before spreading around the world.

The new wiper, which Talos calls WhisperGate, “downloads a payload that wipes the MBR, then downloads a malicious DLL file hosted on a Discord server, which drops and executes another wiper payload that destroys files on the infected machines,” according to a Talos blog post that detailed the different stages of the malware deployment, its connections to earlier known malware and its indicators of compromise.

“In gathering up all the intelligence on this, building out indicators of compromise and then publishing detection signatures, detection rules for these types of attacks,” Liles says, “we are proactively and preemptively attempting to protect Western customers from this if [the attackers] decide that they would like to change targets from their current work over in Ukraine to any of the Western countries.”

Other threats noted by Talos recently were opportunistic phishing and malspam campaigns capitalizing on the Ukrainian war with bogus charity appeals and booby-trapped Microsoft Office documents. Although such crude campaigns are often seen after every globally newsworthy event, Liles says there was still value in alerting Talos readers and Cisco customers.

“The reason that these campaigns, routine or not, exist is because they do still work,” says Liles. “There are clearly people out there that are not educated in avoiding campaigns like this. We’ll continue to warn...
about it until we can reach the point where everyone is either aware of it or understands the proper hygiene. In short, we’re going to keep talking about it until it stops working.”

**The challenges of handling all that data**

Organizations that use cloud providing such information isn’t just a matter of hooking up the client and turning on the data firehose. A customer would be overwhelmed by the amount of information coming in, and unless there were some way to separate the signal from the noise, there wouldn’t be much point in getting all that data.

“Incident after incident shows that it’s not just about having the information, but also seeing the forest for the trees and then doing something about it,” says Jacob Ansari, CISO at IT-compliance firm Schellman. “I remember the Target [data breach] incident 10 years ago, and someone in their SOC saw the attack pattern but said that it was indistinguishable from 500 other things they saw every single day.”

It’s very possible, Ansari adds, to have a lot of information and not be able to actualize it to the benefit of one’s customers.

Cisco says it gives its customers intelligence derived from the telemetry, not the feed itself. As a white paper about Cisco Talos threat intelligence states, customers cannot simply purchase a stand-alone telemetry feed from Cisco Talos.

“We want as much telemetry as possible, we want as much data as possible, but we want that data to be good data,” Liles said. “We don’t want to blow up a security analyst’s mailbox or his user interface with tens of thousands of alerts that don’t mean anything.”

It’s not just a question of the sheer volume of the alerts, but the quality of the alerts, Liles said. The data coming in must be sorted and the salient points must be separated out and presented to the customer as actionable intelligence.

“We want to be able to contextualize and correlate what we’re seeing with something that may require human intervention. We want the alerts that we’re popping up to be meaningful,” says Liles. “When we generate an alert, does it tell you what’s going on and does it tell you what to do about it?”

All the intelligence gleaned from Cisco’s telemetry gets plowed back into Cisco software updates, but much of it also becomes public knowledge after it gets posted on Cisco’s Talos blog for anyone to read and act upon.

**Does your firm need this kind of threat intelligence?**

While this kind of threat intelligence may not be appropriate for a company that isn’t ready to receive it, a firm that’s prepared to get threat intelligence on a global scale is one that’s already got the basics figured out.

That’s the ideal security stance you want a firm to have, but it likely doesn’t match the
reality at many smaller and medium-sized businesses, or even sometimes the largest ones.

To understand how well positioned an organization is to benefit from the telemetry firehose, security decision makers must ask:

• Do we have a robust and well-enforced security policy?
• Are we certain that we are updating and managing our endpoints properly?
• Are our organization’s networks monitored and logged?
• Do we regularly update software at the network level and at the endpoints?
• Is our general staff trained to respond to security incidents?
• Does our SOC have contingency scenarios planned out in advance for almost any incident?

If you can’t unhesitatingly answer “yes” to each of these questions, then your organization may have some catching up to do before latching on to the telemetry firehose. In such cases, a huge amount of global threat intelligence may not do much good when your systems are still offering low-hanging fruit to opportunistic attackers.

**Fix the immediate stuff first**

For those who do have catching up to do, where to begin? A lot of organizations may just want to know how the most recent attackers got into the network. To those organizations, it may not matter so much who the attackers are if the means of entrance can be blocked.

“What you want to hear is, ‘You should go fix that,’” says Ansari. “You can get at a lot of that with a smaller amount of information.”

In fact, if you’re not a Fortune 500 company, or you’re simply not at the level where you can receive and act upon threat intelligence, there might be an advantage to going with a smaller cybersecurity provider, Ansari says.

Cisco said as much in a [Talos Intelligence blog post](http://www.cisco.com) March 3 regarding the threat of opportunistic attacks as a result of the Ukrainian war.

“Tech debt, poor cybersecurity hygiene and out-of-date systems and software will have catastrophic impacts on your organization,” Cisco’s post stated. “On the flip side, network segmentation, visibility, asset inventories, prioritized patching and intelligence programs that actively drive changes in your defenses are key to successfully weathering attacks.”

Threat intelligence is only the last part of that overall approach, and it comes after all the other goals have been reached. In other words, being able to handle and properly use threat intelligence is something that may be possible only after the more essential stuff has been taken care of.

If your organization is indeed ready to receive sophisticated threat intelligence, then there are obvious advantages to having access to data from a telemetry feed as large as Cisco Talos’.

“If you’re in a position where you need someone who has that capability, and you’re ready for it, then you can use it,” Ansari says “If you’re in the right state or if you have a very large, widely distributed set of assets that you need to protect, then a global threat-intelligence service could be what you need.”

---

For more information about ebooks from SC Media, please contact Bill Brenner, VP, content strategy, at bill.brenner@cyberriskalliance.com.

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.
Cisco Secure powers security resilience, enabling organizations to protect the integrity of their business amidst unpredictable threats or change. With Cisco Secure, organizations see across the multi-environment IT, anticipate what’s next, take the right action, close security gaps, and get better every day to ensure the success of institutional-wide resilience investments.

More information is available at www.cisco.com