TALOS INTELLIGENCE

CISCO SECURITY'S THREAT INTELLIGENCE ORGANIZATION

The digital world is expanding at an unprecedented rate, and attack opportunities are expanding just as quickly.

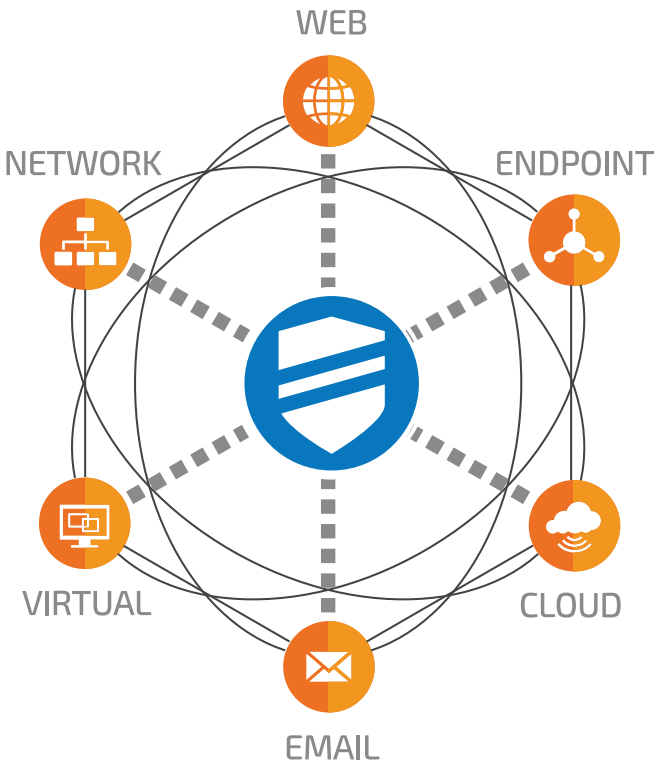
Attackers have unlimited attempts and resources to be effective, so defenders have to win each and every time. To combat these threats, security needs to go beyond tracking and detection to push the boundaries of today's security technologies to work against tomorrow's exploits.

Talos takes the initiative by providing the most comprehensive security and threat intelligence solutions in the industry. Talos provides weaponized intelligence and detection technologies to quickly inform and defend our customers. Our engineers and analysts are working around the world to keep every Cisco Security customer and the security community informed of the current threat environment.

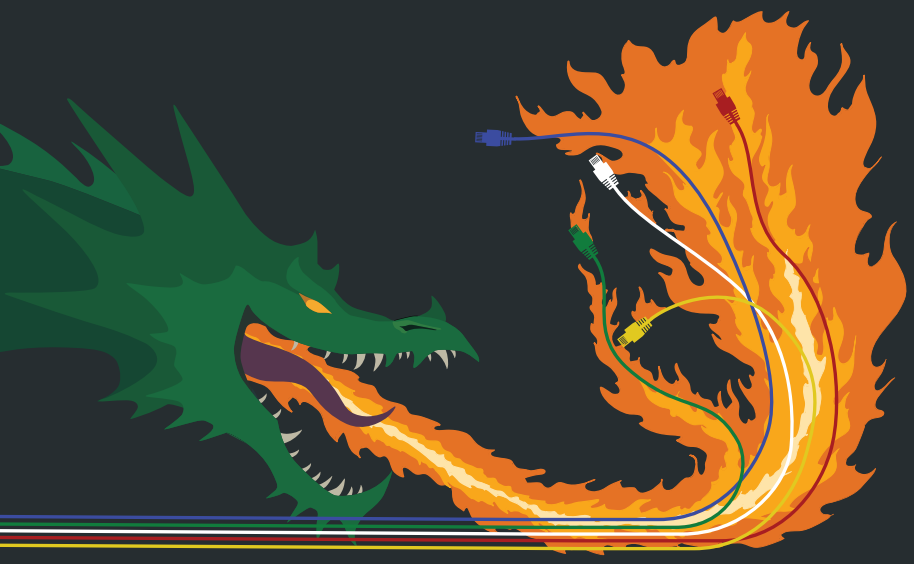
TALOS VISIBILITY

The Cisco Security ecosystem covers email, networks, cloud, web, endpoints and everything in between. Cisco Talos has more visibility than any other security vendor in the world, with the sheer size and breadth of Cisco Security's portfolio and the incoming telemetry from Cisco's customers and products.

This unique visibility delivers us greater context from many data points during an incident or campaign. This, along with other resources such as open-source communities and internal vulnerability discovery, enables Talos to move faster and create more comprehensive assessments of ongoing threats.



Talos' core mission is to provide verifiable and customizable defensive technologies and techniques that help customers quickly protect their assets from cloud to core. Our job is protecting your network.



Talos Out in Front: Nyetya and the MeDoc Connection

The Nyetya ransomware took the world by storm in June 2017, and Talos was out in front with tested coverage, utilizing verified intelligence from Cisco Incident Response. Talos sniffed out the initial threat vector pointing to a destructive and geopolitically motivated attack infecting the supply chain of MeDoc, a tax software. In turn, the attack was targeting companies doing business in and with Ukraine. This intel saved our customers and the general public precious hours of searching for phantom email and maldocs that did not exist. For the full story, visit http://cs.co/nyetya.

WHAT IS TALOS?

Talos, Cisco's threat intelligence organization, derives its name from the Greek giant whose sole purpose was protecting Europa from invaders and pirates. As with our namesake, we are an elite group of security experts devoted to providing superior protection to customers with our products and services.

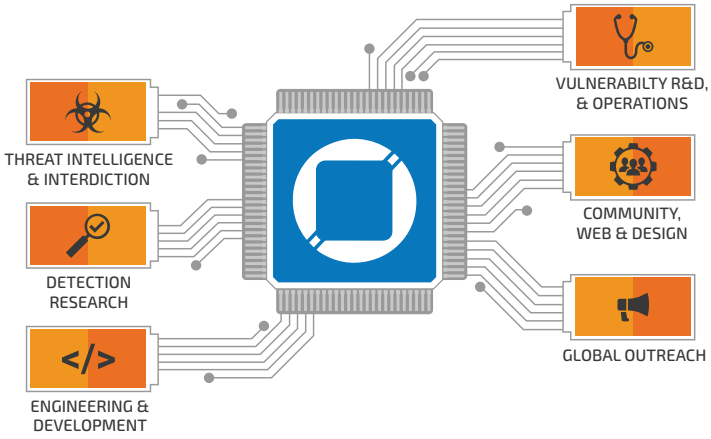
Together with Cisco Incident Response (IR), Cisco Penetration Testing and Cisco Advanced Services, we are able to increase the efficiency and efficacy of our intelligence at Talos. This collaboration drives different data into the overall intelligence stream that Talos uses to create and ship protection to customers. This telemetry gives visibility and context to data, which provides us with unique insight into targeted attacks and advanced persistent threat (APT)-type activity.

Talos encompasses six key areas: Threat Intelligence & Interdiction, Detection Research, Engine Development, Vulnerability Research & Discovery, Open Source & Education, and Global Outreach.

Threat Intelligence & Interdiction handles correlating and tracking threats so that Talos can turn attribution information into actionable threat intelligence. By identifying threats and threat actors rapidly, we are enabled to protect our customers quickly and effectively.

Detection Research consists of vulnerability and malware analysis that leads to the development of detection content for all of Cisco Security's products. This includes unpacking, reverse engineering, and the development of proof-of-concept code to ensure we address each threat in the most efficient and effective way possible on each platform.

Engineering & Development encompasses efforts to ensure our various inspection engines stay current and maintain their ability to detect and address emerging threats. This team is responsible for all the detection content that powers Cisco Anti-Spam, Outbreak Filter, Talos Email and Web Reputation,



as well as many other products. Web categorization and all things SpamCop are also powered by the Engineering & Development team. The team is comprised of developers, QA engineers, security researchers, operations engineers, and data analysts that all work together to develop systems and tools that produce detection content used by Cisco products.

Vulnerability Research & Discovery, & Operations consists of developing programmatic and repeatable ways to identify zero-day security issues in the platforms and operating systems that customers depend on to find and defend against security issues. Our team works with vendors to responsibly disclose and patch more than 200 vulnerabilities a year to reduce potential attack vectors before threat actors can exploit them.

Community, Web & Design leads Cisco Security's efforts in providing the open-source community with new tools for customers and security practitioners to use in the fight against the bad guys. This team also consists of Talos' design and web teams, who create the graphics, websites, white papers and more for the Talos organization and open-source products.

The web team manages the design and features on TalosIntelligence.com, as well as the websites for our other open-source communities and internal tools. The design team is in charge of all of the branding around Talos. Additionally, design assists in the creation of all of Talos' public-facing documents, such as charts, graphics and newsletters.

Global Outreach disseminates all of Talos' intelligence to customers and the global security community. They collaborate on security research with all other research teams within Talos, looking out to the edges of the threat landscape to identify new trends and monitor new and existing persistent threats. The team is stationed globally and communicates findings through customer meetings, conference presentations, the Talos blog, webinars, press interviews, podcasts and local language resources.

SUPERIOR PROTECTION

BREADTH AND DEPTH OF SECURITY COVERAGE

Protecting your network requires both breadth and depth of coverage. While some research teams limit their focus to a few areas, Talos is dedicated to helping provide protection against an extensive range of threats. Talos' threat intelligence supports a wide range of security solutions including Next-Generation Intrusion Prevention System (NGIPS), Next-Generation Firewall (NGFW), Advanced Malware Protection (AMP), Email Security Appliance (ESA), Cloud Email Security (CES), Cloud Web Security (CWS), Web Security Appliance (WSA), Umbrella, and ThreatGrid, as well as numerous open-source and commercial threat protection systems.

Cisco Customers gain a unique benefit with Cisco Security's products. These products directly contribute to Talos' telemetry, which in turn is utilized to provide detection content that can be deployed in any environment to protect all types of assets.

EMAIL SECURITY

Each day, Talos inspects more than 300 billion emails, drawing on layering detection technologies, like outbreak filters and machine learning-based reputation filters, along with Cisco's Advanced Malware Protection (AMP). With all of the features combined, Talos blocks approximately 200 billion malicious emails a day, which equates to approximately 2.3 million blocks per second.

UNMATCHED WEB VISIBILITY

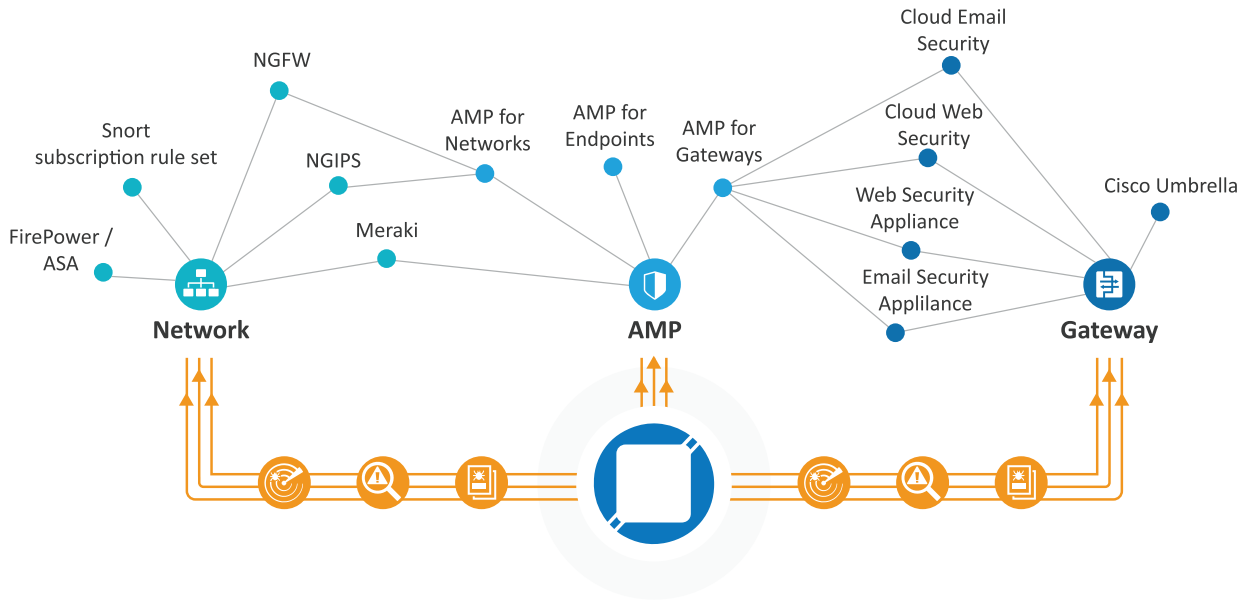
Cisco Web Security technologies have a reputation for detecting and identifying new and emerging web exploitation techniques. Talos has insight into nearly 17 billion web requests each day, drawing on multiple protection methods, including our AMP technology to protect our users.

PROVEN VULNERABILITY-BASED PROTECTION

Talos is well-known in the industry for its excellence in detecting vulnerabilities, exploits and malware that emerge daily. Using high-quality, rapid releases, we keep our customers up-to-date with vulnerability-based protections for the latest threats. Talos has proven this time and again in third-party validation with NSS labs Inc., a leading independent security research agency. We have led the Network NGIPS and NGFW tests in detection rate for the past seven years.

ADVANCED MALWARE PROTECTION

Protecting against the onslaught of malware requires innovative and advanced detection technologies, massive amounts of intelligence gathering, reverse engineering and analytics. Talos utilizes all of this to develop malware protections, post-compromise protection, reputation services and analysis tools to locate threats as they appear "in the wild." These capabilities are included in all Cisco products for protecting hosts, mail gateways, and network assets — truly protecting customers before, during, and after the threat.



Talos' threat intelligence supports a wide range of security solutions including NGIPS, NGFW, AMP, ESA, CES, CWS, WSA, Umbrella, and ThreatGrid, as well as numerous open-source and commercial threat protection systems.

Talos pools data from a variety of sources to create one of the most comprehensive intelligence gathering and analysis platforms in the industry.

COMPREHENSIVE INTELLIGENCE

ACTIONABLE COMMUNITY-DRIVEN THREAT DATA

The core component of any holistic security strategy is solid, actionable intelligence. Talos has built one of the most comprehensive intelligence gathering and analysis platforms in the industry. Through the ClamAV®, SNORT®, Immunet®, SpamCop©, Talos Reputation Center, Threat Grid®, and other Talos user communities we receive valuable intelligence that no other security research team can match. Through collaboration with users and customers around the globe utilizing our Crete program, Talos is able to detect regionalized threats as they emerge.

ACCESS TO VULNERABILITY INFORMATION

Talos analyzes numerous public and private intelligence feeds every day, looking for new threats and acting on information in real time to develop new detection content. Partnerships like the Microsoft Active Protection Program (MAPP) allow Talos to quickly and effectively handle new Microsoft and Adobe targeted threats, allowing us to release our detection on the same day as Microsoft patches.

REAL-TIME MALWARE INTELLIGENCE

Talos collects more than 1.1 million malicious software samples a day by compiling data acquired from product telemetry along with honeypots, sandboxes, and industry partnerships in the malware community. Our advanced analysis infrastructure automatically analyzes samples and rapidly generates detection content to mitigate threats on a daily basis. This provides us with meaningful insight into the threat landscape and an unparalleled perspective as our adversaries attempt to compromise users.

THREAT RESEARCH

Whether identifying new malware families targeting point-of-sale terminals, widespread malvertising networks, or even threats that pose a risk to core services on the internet, Talos can be counted on to identify, research and document our adversaries.

During every investigation, Talos identifies multiple ways customers can defend against threats. We pride ourselves on not only identifying and remediating the issue at hand, but also on identifying all facets of the adversary's criminal network, even if they are associated with entirely separate malware campaigns.

Cisco customers benefit by having this threat intelligence research and protection built into every Cisco Security product. Additionally, we share this information with the public via blogs, Snort rules, conferences and white papers to help create a safer internet for all and help introduce obstacles for adversaries.

INNOVATIVE DETECTION TECHNOLOGIES

FLEXIBLE DEFENSIVE TECHNOLOGIES FOR DYNAMIC ENVIRONMENTS

The threat landscape evolves at a rapid pace, and as attacks change, so must the defensive technologies used to detect them. Talos is constantly working on new detection technologies that push the envelope of today's detection mechanisms while keeping them agile enough to quickly adapt to tomorrow's threats.

ANTICIPATING THREATS

It is one thing to respond to new threats, and it is another to protect against emerging and new ones. Talos is constantly searching for new vulnerabilities and threats that could affect our customers. When new vulnerabilities are discovered, Talos releases coverage to protect against these zero-day threats while the affected vendors develop and test their patches. This means that Cisco customers can control the threat while waiting for patches from their vendors using Talos' zero-day vulnerability protections.

Talos is also actively engaged in locating new malicious websites, botnet, command and control servers, and other malicious sites on the internet. Once located, this information is cataloged and consolidated into comprehensive IP blacklists and URL-altering feeds, which are distributed to our customers as well as shared with industry partners in order to make the internet a safer place.

TRUSTED COMMUNITY

EXTENDING YOUR TEAM

Having a trusted place to turn when the going gets tough is essential to effective security. Without strong communication channels between security teams, response teams, and trusted

partners, it is impossible to stay up-to-date on the latest threats and solve your unique security problems.

Talos believes we should be an extension of your security team. We don't just push information to you, we want to have constructive conversations about your goals and how we can help you reach them.

INTELLIGENCE SHARING

The Awareness, Education, Guidance, and Intelligence Sharing program was created specifically to interact with Cisco customers and partners to help solve custom detection challenges in your specialized environments. AEGIS© puts participating members of the security industry in direct contact with the Talos Threat Intelligence Team. This helps build custom detection content, improve security practices, gather feedback on our products and services, and implement customer improvements to our products. It's just one more way we at Talos help protect your network.

The Crete program is a collaborative exchange between Talos and Cisco FirePOWER customers that provide Talos with real-world scenarios and traffic. This provides the participating customers with leading edge intel, while the data gathered from the Crete program helps us improve threat detection and prevention globally.

INTERACTIVE INFORMATION

Talos keeps in constant contact with our customers through numerous interactive channels. The Talos, ClamAV, and Snort blogs are continually updated with information about the latest threats, how to create custom detection content, and in-depth analysis of the latest malware families.

CONCLUSION

For Talos customers, our skills and research translate directly into award-winning products and services. Even if you're not a Talos customer, you reap the benefits from Talos' research efforts that are provided to the community. Talos produces high-impact, actionable content and tools that are available to the entire community with our unique and enduring commitment to an open-source model and a continuous stream of research papers, presentations and blog posts.

Talos provides a uniquely comprehensive and proactive approach to protecting your network with a history of leadership and success in the security industry. The Talos team members are focused on providing high-quality, customer-driven security research that sets the bar for accuracy and relevance.

Talos

Content	URL
Talos Website	talosintelligence.com
Talos Blog	blog.talosintelligence.com
Talos Twitter	twitter.com/talossecurity
Talos YouTube Channel	cs.co/talostube
Beers with Talos Podcast	talosintelligence.com/podcasts

Content	URL
ClamAV Website	clamav.net
ClamAV Blog	blog.clamav.net
Snort Website	snort.org
Snort Blog	blog.snort.org
Talos Rule Advisories	snort.org/talos