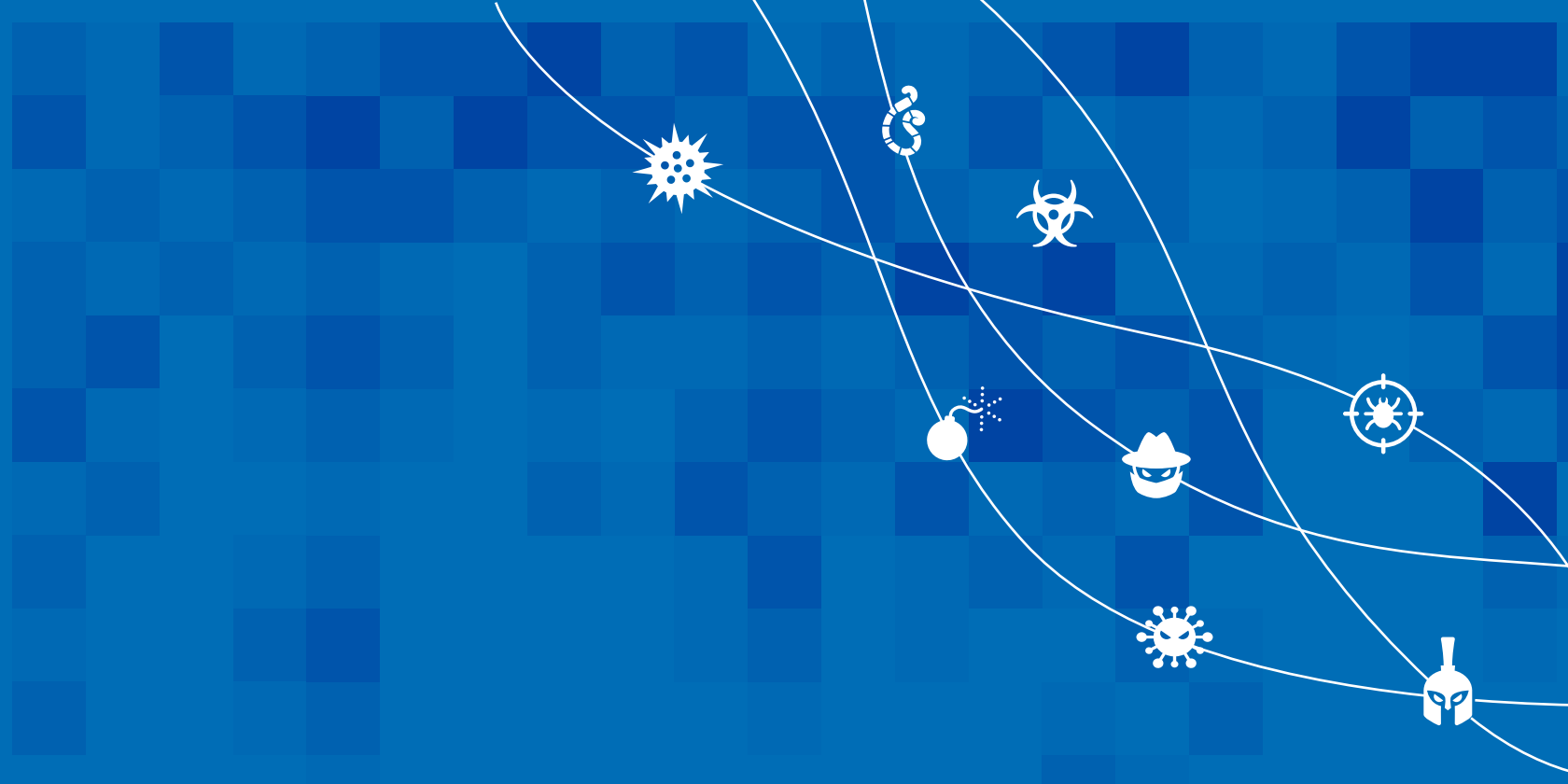


TALOS INTELLIGENCE

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 every time. This requires immense visibility, rapid intelligence, and the ability to respond in-kind and at-scale.

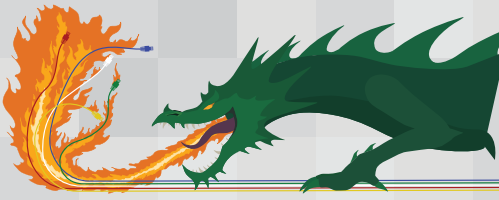
Cisco Talos is one of the largest and most trusted providers of cutting-edge security research globally. We provide the data Cisco Security products and services use to take action. The key differentiator of Talos is our process — seeing what is happening broadly across the threat landscape, acting on that data rapidly and meaningfully, and driving protection. Integral to that process is that Talos has more visibility than any other security vendor in the world and unique capabilities and scale in intelligence. The core mission at Talos is to provide verifiable and customizable defensive technologies and techniques that help customers quickly protect their assets. Our job is protecting your network.

Visibility, intelligence and response

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 the Cisco Security portfolio and the incoming telemetry from Cisco's customers and products.

This unique visibility delivers greater context from many data points during an occurring incident or campaign. This, along with other resources like open-source communities and internal vulnerability discovery, creates a massive amount of threat data. Unique capabilities and scale in intelligence enable Talos to move faster and create more comprehensive assessments of ongoing threats.

A key differentiator of Talos is our ability to respond. With a broad portfolio of protection, responding to threats inside your network is simplified with automatic and configurable updates from Talos. Beyond the perimeter, Talos can take action that few others can to drive collective response on an internet-wide basis.



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.**

Unmatched visibility

If you want to stop more, you have to see more. The modern landscape is made up of all kinds of threats coming at defenders from all possible vectors. Only Cisco Security offers a market-leading, comprehensive portfolio covering IPS, identity, firewalls, endpoint, email, web, DNS and more. That breadth and depth gives Talos immense visibility through product telemetry. However, Talos visibility is not limited to just telemetry. Over 185 industry partnerships, customer feedback, hunting intel, actor tracking, and even forward-looking vulnerability discovery contribute vital intelligence and context. Vulnerability discovery is an essential aspect of visibility that is not easily replicated. Talos is actively finding, reporting, and helping vendors to remove vulnerabilities in software that customers use daily.

Combining market share, key partnerships, and proactive discovery produces threat intelligence with unmatched visibility.

- **The broadest data set:** The Cisco Security portfolio is unique as a broad market leader across NGFW, IPS, Email, endpoint, DNS, and more.
- **Fighting the good fight with the community:** More than 185 intel partnerships
- **Proactively finding trouble before it finds you:** Responsibly disclosing >1 vulnerability every working day

TO STOP MORE, YOU MUST SEE MORE

Protecting your network requires both breadth and depth of coverage — you can only protect where you have visibility. While some research teams limit their focus to a few areas, Talos protects customers from an extensive range of threats. Talos' threat intelligence supports a two-way flow of telemetry and protection across market-leading 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. The breadth of the Cisco Security portfolio enables unmatched visibility across the threat landscape.

INDUSTRY AND OPEN-SOURCE COMMUNITY PARTNERSHIPS

Talos firmly believes the security community wins together — or not at all. Talos is active in more than 185 industry groups and community partnerships. With industry groups like the Cyber Threat Alliance, intelligence gets into the right places faster,

enabling broader interdiction on multiple fronts simultaneously. With the Microsoft Active Protection Program (MAPP), Talos is notified of targeted threats to push coverage simultaneously to patch activity from large vendors such as Microsoft and Adobe. ISAC programs facilitate intelligence and specific insights in targeted verticals. Through collaboration with users and customers around the globe utilizing our Crete program, Talos can detect regionalized threats as they emerge.

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.

PROVEN VULNERABILITY-BASED PROTECTION

Talos Vulnerability Research & Discovery uses a programmatic approach to find more than one vulnerability per working day in a variety of software. When new vulnerabilities are discovered, Talos releases coverage to protect against these zero-day threats while the affected vendors develop and test their patches. Even if attackers uncover those same vulnerabilities while the vendor is patching, Cisco customers have coverage while waiting for the patch.

Actionable intelligence

Unmatched visibility yields a mountain of threat data, the majority of which is related to known existing threats. The challenge is finding the small percentage of malware that is new to the landscape — evolving ransomware, cryptocurrency miners, politically motivated actors, destructive malware and highly targeted espionage activity. Rapidly distilling actionable intelligence from immense datasets involves a high degree of interaction, both human- and machine-driven. Machine learning and AI, overseen by analysts and data scientists, create stronger detection outputs for faster and better results. Those outputs are used by Talos engineers to create protection across vectors and pushed globally as quickly as technologically possible. With a continuous cycle of telemetry and updates across an integrated portfolio encompassing the entire attack continuum — endpoint, network, cloud, edge, data center, desktop, and mobile — Talos provides actionable intelligence that is fast, efficacious, and deeply contextual.

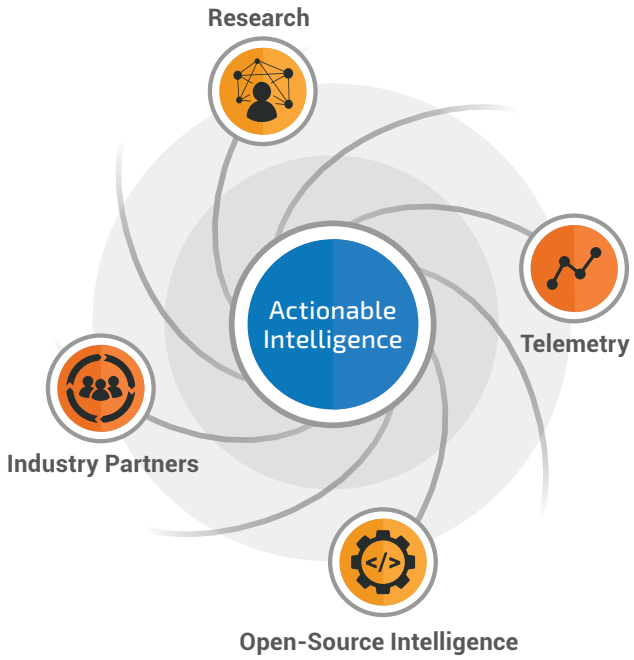
- **Distillation and analysis:** Talos is the largest private threat intelligence and research team in the world.
- **Delivering intelligence with context:** Talos delivers much more than just IoCs with context from telemetry analysis, our research, intelligence resources, and open-source resources.
- **Rapid coverage:** Advanced Malware Protection time-to-detection average of 3.5 hours versus industry average measured in days.

INTELLIGENCE AT SCALE

Over 350 researchers, analysts, engineers, linguists, developers, and other operators work around the clock, around the globe digging deep into threats, tracking actors, creating and shipping detection, and adding deep, meaningful context to threat intelligence. Our advanced analysis infrastructure automatically analyzes samples and rapidly generates detection content to mitigate threats as they happen. The volume of coverage Talos creates and the speed with which it's shipped is made possible by the scale of the organization.

MORE DATA, MORE CONTEXT

The broad spectrum of the Cisco Security portfolio and the varied nature of Talos collection and analysis systems, like honeypots and sandboxes, adds a significant amount of context to incoming threat data. Our industry-leading research and analysis adds invaluable context. Whether identifying new cryptocurrency mining malware, supply chain attacks, or advanced threats that pose a risk to core services and devices on the internet, Talos can be counted on to identify, research and document threats and threat actors.



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 and analyzing the tactics, techniques and procedures of a threat actor.

Cisco customers benefit by having this threat intelligence built into every Cisco Security product. Additionally, we share this information with the public via blogs, presentations, webinars, and whitepapers to help create a safer internet for all and create obstacles for adversaries.

FAST DETECTION AND PROTECTION

Protecting against an onslaught of malware requires innovative and advanced detection technologies, massive amounts of intelligence gathering, reverse engineering and analytics — and speed. Fast time to detection can make the difference between an event log entry and an incident report. Talos malware and vulnerability coverage, post-compromise protection, reputation services and analysis tools are part of Cisco Advanced Malware Protection (AMP).

AMP customers experience median time-to-detection (TTD) of 3.5 hours versus the industry average of over 100 days. "Time to Detect" is defined as the window of time between a compromise and the detection of a threat.

Collective response

Threats move quickly, so providing on-the-fly coverage updates to customers globally is crucial. The principal output of Talos is direct, as-they-happen security product updates. Customers cannot purchase a standalone "threat feed" from Talos. Talos threat intelligence is delivered as tailored, configurable updates for all Cisco Security products across the environment. The sheer breadth of the Cisco Security portfolio combined with the unique capabilities of Talos creates the capability for an unrivaled collective response across potential threat vectors. This collective response capability is augmented by other groups inside Cisco Security, like Cisco Incident Response (IR), Cisco Product Security Incident Response Team (PSIRT), and Cisco Security and Trust Organization (STO). Every Cisco Security device in your environment is another defensive position that Talos builds and maintains around the clock to protect you.

Just as crucial to collective response is the ability to respond to threats that threaten the entire internet. Like its namesake of Cretian lore, Talos can take action that few others can when a major threat arises. Our job is to keep the shores clear of invaders and discourage them from returning. Global service providers, internet governing bodies, and cybercrime law enforcement organizations respond and work with Talos to drive collective response across the internet.

- **Protection across the portfolio:** Every Cisco Security solution present multiplies available protection
- **Responding at scale:** Generating thousands of headlines and oft-cited by government and industry as leading the charge in response to major threats
- Research and open-source efforts provide ongoing response and tools

BETTER LAYERED DETECTION

Talos is continuously working on new, flexible detection technologies across the portfolio that push the envelope of today's detection mechanisms while keeping them agile enough to adapt to tomorrow's threats quickly. Talos works closely with Cisco IR, Cisco Penetration Testing, and Cisco Advanced Services. This increases the efficiency and efficacy of our intelligence at Talos and grants us unique insight into targeted attacks and advanced persistent threat (APT)-type activity. Connecting Talos resources and these front-line services drives rich data into the overall intelligence stream that Talos uses to create and ship protection to customers. Conversely, every Cisco IR engagement involves Talos on the backend, making their results stronger.

RESPONSE AT SCALE

When it comes to responding to an internet-wide security issue or an advanced threat, Talos is no stranger to spearheading the effort. Today, significant threats are often frontpage news. Talos collective response generates a myriad of press mentions and is oft cited by industry partners and global government officials for our capabilities, both sounding the alarm and mitigating the threat.

Responding to threats on this scale with speed, accuracy, and efficacy is made possible by the work of a large organization with diverse expertise focusing intense effort at a critical event. Global service providers and internet governing bodies are vital partners in interdiction efforts. Acting on trusted intelligence from Talos, these partners can affect rapid remediation and often arrest a threat in the wild.

ONGOING ACTIVITIES AND TOOLS

Talos is also actively engaged in locating new malicious websites, botnet command and control (C2) 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 to make the internet a safer place.

This is Talos

Cisco Talos is the threat intelligence organization at the center of the Cisco Security portfolio. Talos derives its name from the Greek automaton whose sole purpose was protecting the shores of Crete 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.

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

Threat Intelligence & Interdiction handles correlating and tracking threats so that Talos can turn threat data and simple indicators into actionable, context-rich threat intelligence. Rapid identification of threats and threat actors gives Talos unique abilities to protect our customers quickly and effectively.

Detection Research conducts vulnerability and malware analysis and creates the detection content for all of Cisco Security products. This includes unpacking, reverse engineering, and developing proof-of-concept code to ensure each threat is addressed in the most efficient, effective, and contextually relevant way possible.

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, Cisco Outbreak Filters, Talos Email and Web Reputation, Web Categorization, SpamCop, and many other products. Comprised of developers, QA engineers, security researchers, operations engineers, and data analysts, Engineering & Development work together to develop systems and tools leveraged by all Cisco products.

Vulnerability Research & Discovery develops programmatic and repeatable ways to identify high-priority security vulnerabilities in the operating systems and common software customers use daily, including platforms like ICS and IoT systems. This team works with vendors to responsibly disclose and patch more than 200 vulnerabilities a year — before threat actors can exploit them — reducing the overall attack surface available. In addition to closing potential attack vectors, this activity allows Talos to maintain skill sets that mirror those of adversaries.

Communities consists of Talos design, education and knowledge management, marketing and media, open-source, and web development teams. Broadly speaking, this team handles the visual, editorial, and public-facing messaging of Talos and our open-source solutions. Design creates the branding, graphics, and visual assets for the Talos organization and open-source products. Education and kKnowledge management handles documentation, policies and procedures of all things Talos. They also interface with Cisco Learning on certifications and courses and internal training initiatives. Marketing and media handles the planning, production and promotion of Talos and open-source research, content, and media efforts. 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. Communities serves as the general public interface to the Talos organization.

Global Outreach disseminates Talos intelligence to customers and the global security community via published research and speaking engagements. They conduct specialized research, looking out to the edges of the threat landscape to identify new trends and monitor persistent threats and work alongside Talos intel and research teams responding to critical events. The team is stationed globally and communicates findings through customer meetings, conference presentations, the Talos blog, webinars, press interviews, and various media outlets.

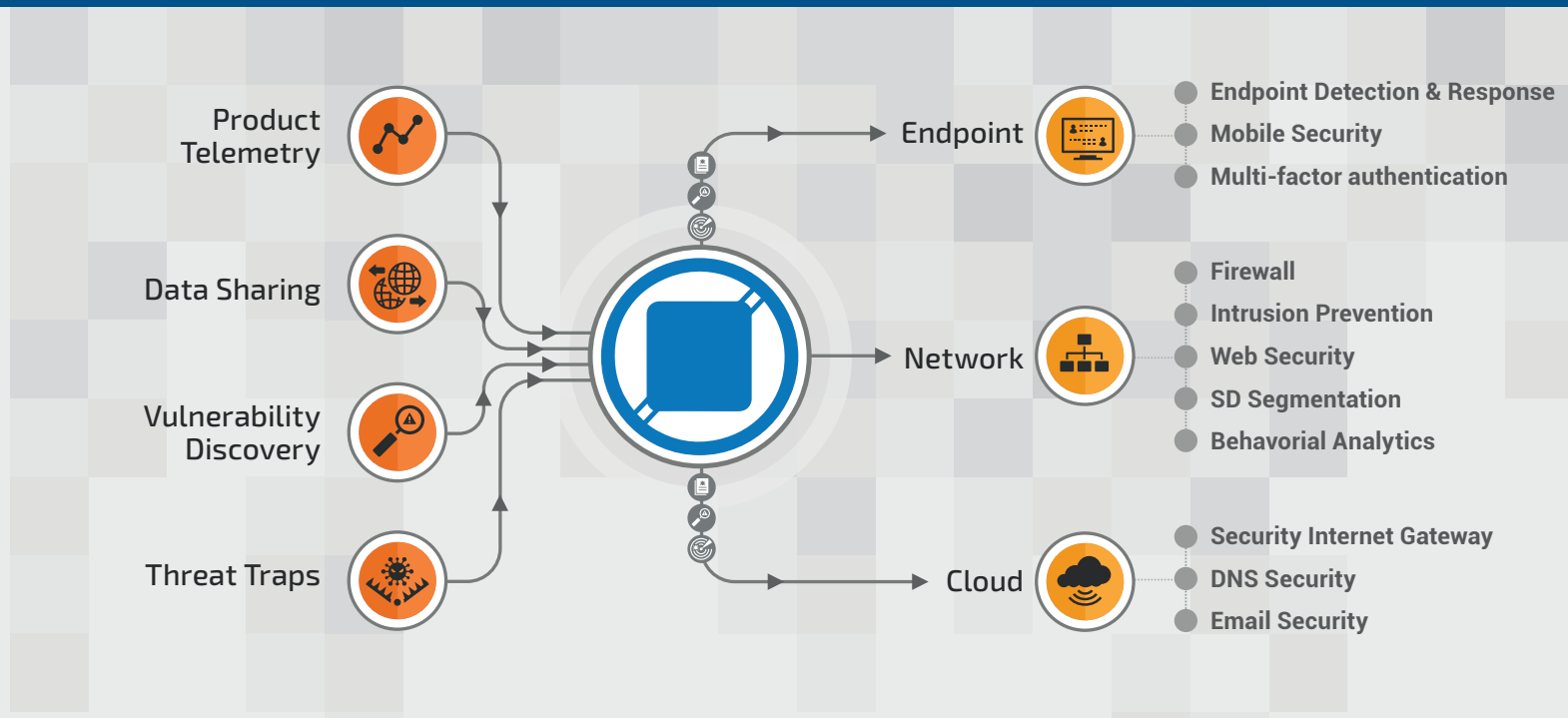
EXTENDING YOUR TEAM

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 at you — we want to have constructive conversations about your goals and how we can help you reach them.

CUSTOMER INTELLIGENCE-SHARING PROGRAMS

The Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) 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 stays in contact with our customers through numerous channels: blogs, social media, press, and podcasts, to name a few. The Talos, ClamAV, and Snort blogs and social accounts serve continually updated information about the latest threats, detection content, and in-depth analysis of the latest malware families. Our popular Beers with Talos podcast offers a decidedly casual and entertaining take on what is currently happening in the threat landscape and security industry.

Conclusion

For Talos customers, visibility, intelligence and response translate directly into better protection. Immense threat visibility from Cisco Security market leadership across the portfolio, coupled with the largest threat intelligence team in the industry enables Talos to deliver better protection. For security practitioners and the internet at-large, Talos research efforts provide high-impact, actionable content and tools. Talos provides a uniquely comprehensive and proactive approach to protecting your network.

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/advisories