Talos Group

PROTECTING YOUR NETWORK

At Talos, we know that the magic black box and the silver bullet security solutions do not exist. We know that security is difficult and that it requires a new approach, one that empowers our customers to address their security challenges. We strive to weaponize intelligence and build detection technologies to quickly inform and defend our customers.

The digital world is expanding at an unprecedented rate, likewise targets and attack opportunities are expanding equally quickly. To be effective in combating these threats, security experts need to go beyond tracking and detecting, and need to push the boundaries of today's security technologies to work against tomorrow's exploits. Talos takes the initiative to provide the most comprehensive and proactive security and threat intelligence solutions in the industry, which in turn comprises the solid foundation of the Cisco Security ecosystem.

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

WHAT IS TALOS

Talos is Cisco's threat intelligence organization, an elite group of security experts devoted to providing superior protection for our customers, products, and services. Talos encompasses five key areas: Detection Research, Threat Intelligence, Engine Development, Vulnerability Research and Development, and Outreach.

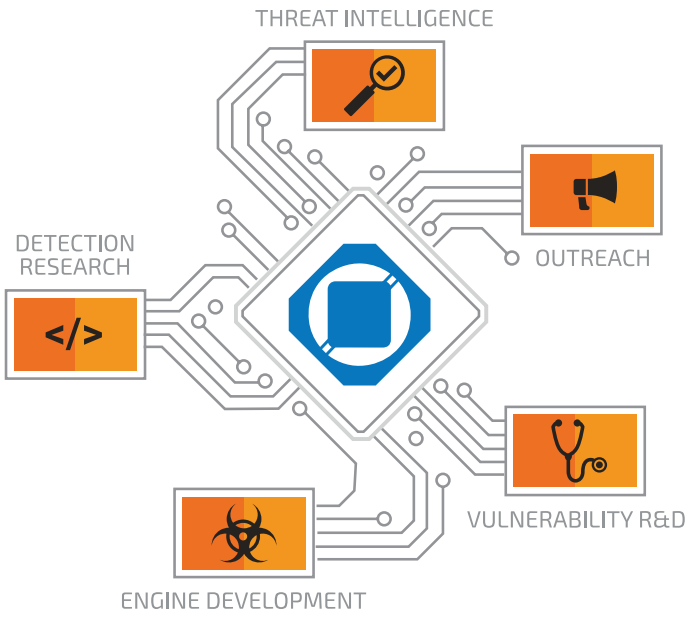
Detection Research consists of vulnerability and malware analysis that leads to the development of detection content for all of Cisco's security products. This includes unpacking, reverse engineering, and the development of proof of concept code to ensure we address each threat in the most efficient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

Threat Intelligence consists of correlating and tracking threats so that we are able to turn attribution information into actionable threat intelligence. By identifying threats and threat actors more quickly, Talos Intelligence enables us to protect our customers quickly and effectively.

Engine Development efforts helps ensure our various inspection engines stay current and maintains their ability to detect and address emerging threats.

Vulnerability Research and Development develops ways to identify "Zero-Day" security issues in the platforms and operating systems our customers depend on. By doing this in a programmatic, repeatable fashion, they identify new methods to find and defend against security issues.

Outreach programs involve researching, identifying, and communicating new trends our adversaries are using to compromise victims.



Talos is comprised of five key areas: Detection Research, Threat Intelligence, Engine Development, Vulnerability Research and Development, and Outreach.

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 IPS (with and without integrated application control), Next-Generation Firewall and AMP (our advanced malware analysis and protection), Email Security Appliance, Web Security Appliance, and ThreatGrid, as well as numerous open source and commercial threat protection systems. Customers gain the unique benefit of the wide range of Cisco security products feeding into the Talos Threat feed. This allows Talos' intelligence and threat research to be deployed in any type of environment to protect any type of asset.

EMAIL SECURITY

It comes as no surprise that Talos has a unique insight into email based threats due to SenderBase© and SpamCop©. The additional perspective obtained through our diverse customer base allows us to address and identify threats with unparalleled speed and agility. Each day we inspect over 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, or 2.3 million blocks per second.

UNMATCHED WEB VISIBILITY

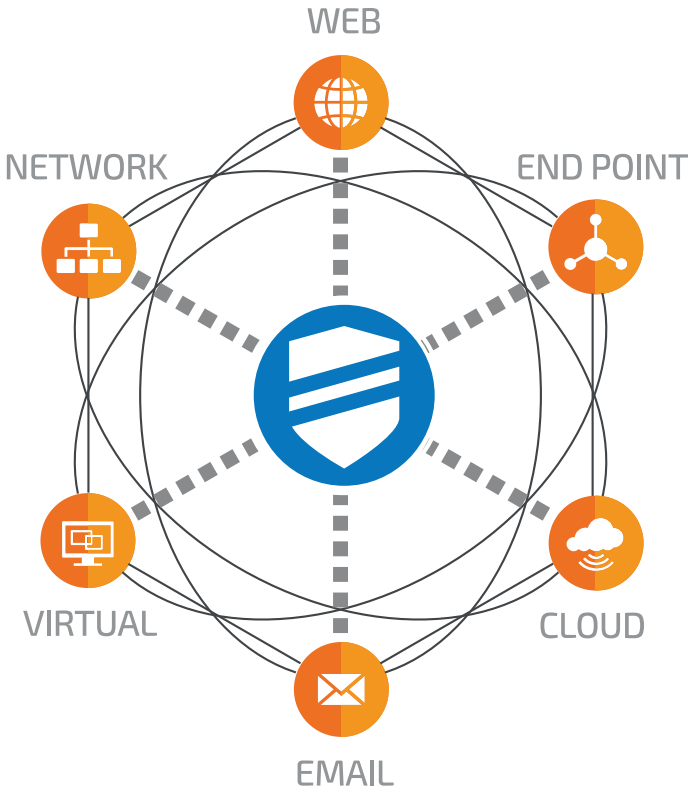
Cisco web security technologies have a reputation for detecting and identifying new and emerging web exploitation techniques. The Angler exploit kit for example compromises users with a success rate of 40% making it one of the most effective ways of compromising users on the internet. Talos has insight into nearly 17 billion web requests each day, drawing on multiple protection methods including our AMP technology to protect our users.

PROVEN IPS VULNERABILITY-BASED PROTECTION

Talos is well known in the industry for its excellence in detecting the myriad of 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. While other vendors claim similar coverage, only Talos has proven time and time again in third-party validation that our detection content is top notch. For the last seven years Talos has led the NSS Labs Network IPS test in detection rate.

ADVANCED MALWARE PROTECTION

Keeping customers safe against the onslaught of malware requires innovative and rapidly advancing detection technologies and content. Additionally, it requires massive amounts of intelligence gathering, reverse engineering, and analytics to wade through this mountain of data and turn it into actionable information. Talos utilizes all of this information to develop malware protections, post-compromise protection, reputation services, and analysis tools to locate threats as they appear "in the wild". These capabilities are driven back into all Cisco's products for protecting hosts, mail gateways, and network



Talos tracks threats across end points, networks, cloud environments, web, and email providing a comprehensive understanding of cyber threats, their root causes, and scopes of outbreaks.

assets — truly protecting customers, Before, During, and After the threat.

COMPREHENSIVE INTELLIGENCE

ACTIONABLE COMMUNITY-DRIVEN THREAT DATA

The core component of any holistic security strategy is solid, actionable intelligence. Over the last 10 years Talos has built one of the most comprehensive intelligence-gathering and analysis platforms in the industry. Through the ClamAV™, Snort®, Immunet™, SpamCop©, SenderBase©, Threat Grid™, and Talos user communities, Talos receives valuable intelligence that no other security research team can match. In addition, through collaboration with users and customers around the globe through our Crete (formerly SPARK) program, Talos is able to detect regionalized and language specific threats as they emerge.

ACCESS TO VULNERABILITY INFORMATION

Talos also analyzes numerous public and private intelligence feeds every day, looking for new threats, and acting on that information in real-time to develop new detection content. In addition, industry partnerships like the Microsoft Active Protection Program (MAPP) allow Talos to quickly and effectively handle new Microsoft and Adobe targeted threats, releasing our detection on the same day as Microsoft patches. This allows our customers to protect their critical assets with network and host-based protection, while they test and deploy these new patches.

EXAMPLES OF TALOS 0-DAY THREAT PROTECTION:

- TALOS-2015-0024 – Total Commander
- TALOS-2015-0018 – Apple Quicktime
- VRT-2014-0301 – Microsoft Windows FastFAT

REAL-TIME MALWARE INTELLIGENCE

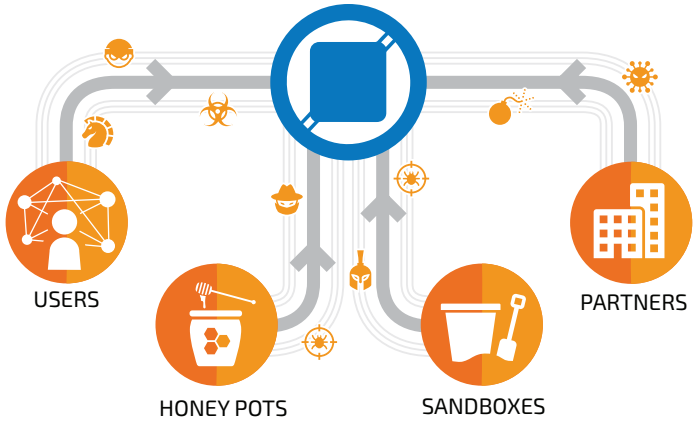
Through compiling data acquired from the millions of users worldwide, along with honeypots, sandboxes, and extensive industry partnerships in the malware community, Talos collects more than 1,100,000 malicious software samples a day. Our advanced analysis infrastructure automatically analyzes these samples and rapidly generates detection content to mitigate these threats on a daily basis. This allows us an amazing insight into the threat landscape and an unparalleled perspective as our adversaries attempts to compromise users.

THREAT RESEARCH

Whether identifying new malware families targeting point-of-sale terminals like PoSeidon, widespread malvertising networks like “Kyle and Stan”, or even threats that pose a risk to core services on the Internet like "SSHPsychos", Talos can be counted on to identify, research, and document their 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 adversaries criminal network, even if they are associated with entirely separate malware campaigns. Cisco customers benefit by having this threat intelligence built into every product.

Additionally this information is shared with the public via blogs, Snort rules, conferences, and white papers. By providing this information to as many people as possible we can help introduce obstacles for our adversaries.



Talos pulls data from millions of users worldwide, honeypots, sandboxes, and extensive industry partnerships, collecting more than 1.1 million unique malware samples a day.

INNOVATIVE DETECTION TECHNOLOGIES

FLEXIBLE DEFENSIVE TECHNOLOGIES FOR DYNAMIC ENVIRONMENTS

The threat landscape has evolved from buffer overflows in network services, to complex client side attacks targeting browsers and files. 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 be quickly adapted to tomorrow’s threats.

ANTICIPATING THREATS

It is one thing to respond to new threats, it is another to protect against new ones. Talos is constantly searching for new vulnerabilities and threats that could affect our customers. When new vulnerabilities are discovered, Talos releases rules to protect against these Zero-Day threats while the affected vendors develop and test their patches. With these protections, Talos customers can control the threat while waiting for protections from their vendors.

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 filtering 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 and 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. Talos has created several programs to help facilitate this task.

INTELLIGENCE SHARING

The Awareness, Education, Guidance, and Intelligence Sharing (AEGIS™) program was created specifically to interact with our 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 to help 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 help protect your network.

The Crete program is a collaborative exchange between Talos and our Customers that provide us with real-world scenarios and traffic, while providing participating customers with leading edge intel.

Talos

Content	URL
Talos Website	talosintel.com
Talos Blog	blogs.cisco.com/talos
Talos Twitter	twitter.com/talossecurity
Talos YouTube Channel	cs.co/talostube
IRC Channels	irc.freenode.net: #snort, #razorback, #clamav
ClamAV Website	clamav.net
ClamAV Blog	blog.clamav.net
Snort Website	snort.org
Snort Blog	blog.snort.org
Talos Rule Advisories	snort.org/talos

INTERACTIVE INFORMATION

Talos keeps in constant contact with our customers through numerous interactive channels. 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. For a list of Talos resources and ways to interact with Talos, see the table below.

KEEPING UP-TO-DATE

Talos is responsible for the entire chain of Cisco detection and prevention, from intelligence-gathering, analysis, content creation, packaging and quality assurance, to end user delivery. Controlling this entire process allows Talos to rapidly deliver industry-leading detection content in the time frames necessary for defending against today's latest threats.

CONCLUSION

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

For Talos customers, these skills and research translate directly into award-winning products and services. Even if you're not a Talos customer, you will reap the benefits provided by Talos' research efforts. With a unique and enduring commitment to an open source model, and a continuing stream of research papers, presentations, blog posts and more, Talos makes high-impact, effective knowledge and tools available to the entire community.

It's a record and a legacy - one that is unmatched in the industry.