Cisco Partner
https://cs.co/1page

Cisco Talos is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts, and engineers. With industry-leading visibility, actionable intelligence, and vulnerability research, they drive rapid detection and protection for Cisco customers against known and emerging threats.

Who is Talos? *(key areas)*

Threat Intelligence & Interdiction handles correlating and tracking threats so that Talos can turn threat data and simple indicators into actionable intelligence.

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.

Engineering & Development ensures 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 Filters, Email and Web Reputation, Web Categorization, SpamCop etc.

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 ICS and IoT systems.

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.

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.

Programs:

Talos Aegis: The Aegis program is available to current Cisco Security Customers, partners and outside agencies or entities with an NDA that would like to partner/exchange information with Talos. Interested parties can reach out to: aegis-interest@cisco.com

Talos Crete: The Crete program is a collaborative exchange between Talos and current Cisco Secure Firewall customers. It provides Talos with real-world scenarios and insights into network threats while providing participating customers with leading edge intel. Crete is offered on a case by cases basis at the discretion of Talos. Interested parties can reach out to: talos-crete@cisco.com

FAQs:

Is Talos an acronym?

No. Cisco Talos derives its name from the Greek automaton whose sole purpose was protecting Europa from invaders and pirates. As with their namesake, Talos is an elite group of security experts devoted to providing superior protection to customers with their products and services.

What is the difference between PSIRT and Talos?

The Cisco Product Security Incident Response Team (PSIRT) is responsible for responding to Cisco product security incidents. Talos, meanwhile, provides the most comprehensive security and threat intelligence solutions in the industry.

How do I buy Talos for my SIEM/random box/etc.?

While Talos does provide a small (1 percent) feed for open-source Snort's testing purposes, they do not offer any sort of consumable threat intelligence feed. Talos intelligence is built into every Cisco Secure product.

Does Talos have an incident response team?

Yes, Cisco Talos Incident Response (CTIR) offers retainers and conducts emergency IR responses.

What is a CUA?

CUA (Cloud URL Analysis) is a URL intelligence generating service that analyses URLs sent to Talos' cloud URL reputation lookup service. CUA integrates existing WBRS information with a variety of different analysis techniques, leveraging internal information and tooling, 3rd party intelligence, and new research techniques.

Resources:

Talos Blog
Talos Podcasts
Incident Response
Threat Source Newsletter

Tools:

Talos Intelligence
IP & Domain Reputation
Email & Spam Data
File Reputation
Software

Social Media:

Talos on LinkedIn
Talos on YouTube

Public page