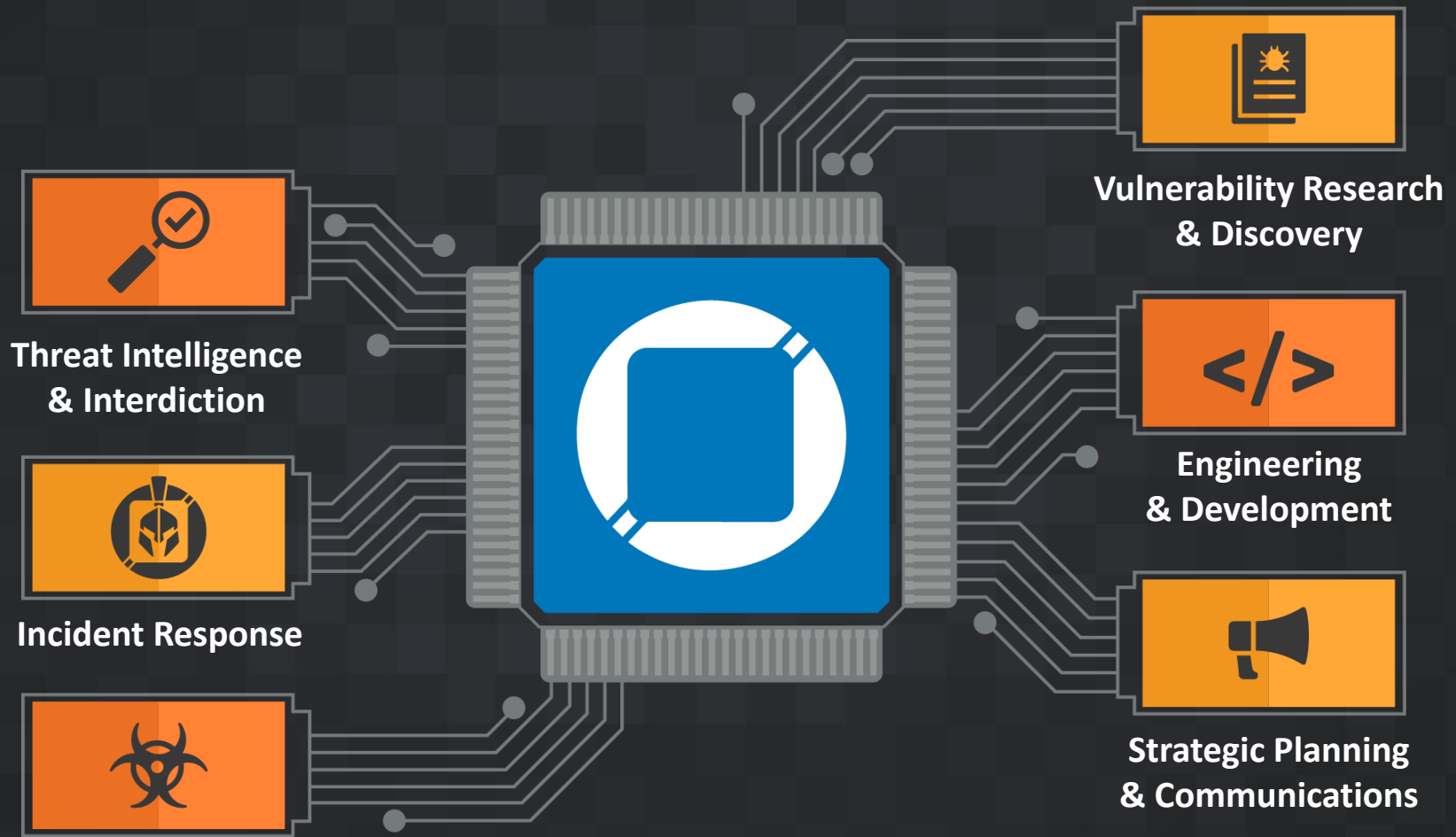
Cisco Talos Incident Response best practices.

Dmytro Korzhevin,
Cisco Talos, Senior Analyst

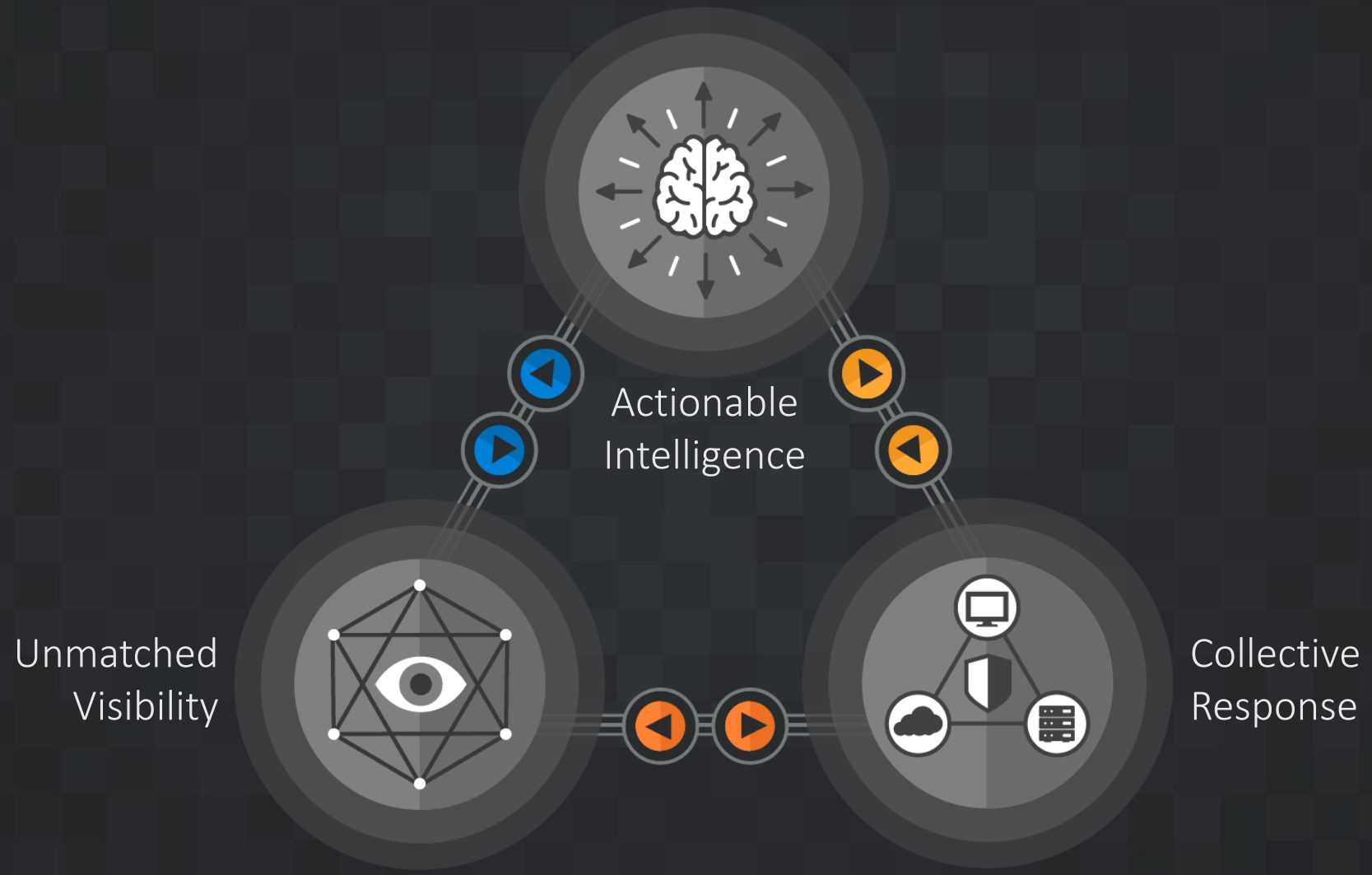
Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



cisco | Talos

The Talos Difference



cisco | Talos

Changing Nature of Threat Actors

Criminal Actors

Groups and individuals motivated by profit or personal agenda.

APT / State Sponsored Actors

Military units & intelligence agencies financed and directed by the state.

State Tolerated Criminals

Criminal threat actors working with some state instruction.

Fellow Travelers

Amateurs inspired by state information loosely instructed by the state.

State Backed Criminals

Criminal threat actors working partially under state direction.

Mercenaries

Specialist services provided by the private sector, but financed and directed by the state.

cisco | TALOS

Advanced persistent threats

Engage in a variety of activities, including espionage, intellectual property theft, and deploying destructive malware.

Russia

- Most active in 2022
- Track several actors: Turla, Fancy Bear, Gamaredon
- Focused mainly on Ukraine, NATO countries

China

- Targets a wide range of industries for economic espionage and intellectual property theft
- Track Mustang Panda and Deep Panda
- Known to exploit current events

Iran

- Primary goal of intellectual property theft and espionage
- Track Muddy Water
- Have observed a plethora of backdoors and post-exploitation tools used

North Korea

- Data theft, financial crimes, and disruptive attacks that back national security objectives
- Track Lazarus Group
- Adept at exploiting vulnerabilities and custom remote access trojans

cisco | TALOS

2022 Year in Review

1. If it works, its being used
2. Innovation and division in the ransomware community
3. Increasing use of dual-use tools and living-off-the-land binaries
4. Advanced Persistent Threat (APT) activity

cisco | Talos

Talos Incident Response Retainer Services

http://cs.co/CTIRDescription

Core

Emergency Incident Response

Intel on Demand

Preparing

IR Plans/ Playbook

IR Readiness Assessments

Training

Tabletop Exercises

Cyber Range Training

Hunting Adversaries

Compromise Assessments

Threat Hunting

Simulating Adversaries

Red Team

Purple Team

cisco | Talos

Talos Blog

https://blog.talosintelligence.com/

Talos Blog

Talos

Software Vulnerability Information Reputation Center Library Support Incident Response Careers About

FEATURED

DECEMBER 14, 2022, 08:12

Talos Year in Review 2022

We expect this data-driven story will shed some insight into Cisco's and the security community's most notable successes and remaining challenges. As these Year in Review reports continue in the future, we aim to help explain how the threat landscape changes from one year to the next.

BY CISCO TALOS

2022YIR YEAR IN REVIEW

JANUARY 19, 2023 08:01

Following the LNK metadata trail

While tracking some prevalent commodity malware threat actors, Talos observed the popularization of malicious LNK files as their initial access method to download and execute payloads. A closer look at the LNK files illustrates how their metadata could be used to identify and track new campaigns.

JANUARY 12, 2023 07:01

How to instrument system applications on Android stock images

By Vitor Ventura This post is the result of research presented at Recon Montreal 2022. Two slide decks are provided along with this research . One is the presentation showing the whole process and how to do it on Google Play Protect services. The other one is a workshop on how

JANUARY 10, 2023 12:01

Increasing trust, commitment, and predictability during a remote incident response

In this blog post, Cisco Talos Incident Response (Talos IR) presents some of the key benefits of remote IR support and offers a list of recommendations for working on a remote incident.

FEATURED CATEGORIES

THREAT ADVISORY
THREAT SPOTLIGHT
VULNERABILITY SPOTLIGHT
THREAT SOURCE NEWSLETTER
MICROSOFT PATCH TUESDAY
THREAT ROUNDUP

View all categories

THREAT SOURCE NEWSLETTER
All the security news you need to know

JANUARY 19, 2023 16:01

Talent retention and institutional knowledge go hand in hand. Both are critical to ensuring the security of your network environment.

VULNERABILITY SPOTLIGHT

JANUARY 19, 2023 15:01

Dave McDaniel of Cisco Talos discovered this vulnerability. Cisco Talos recently discovered a cross-site scripting (XSS) vulnerability in Ghost CMS. Ghost is a content management system with tools to build a website, publish content and send newsletters. Ghost offers paid subsc

cisco | Talos

Stay Connected and Up To Date

Spreading security news, updates, and other information to the public.

White papers, articles & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
Twitter: @talossecurity

Instructional Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

cisco | Talos


CISCO
TALOS
TALOSINTELLIGENCE.COM