TALOS
Cisco Security Research

Dmytro Korzhevin

# Fighting the Good Fight

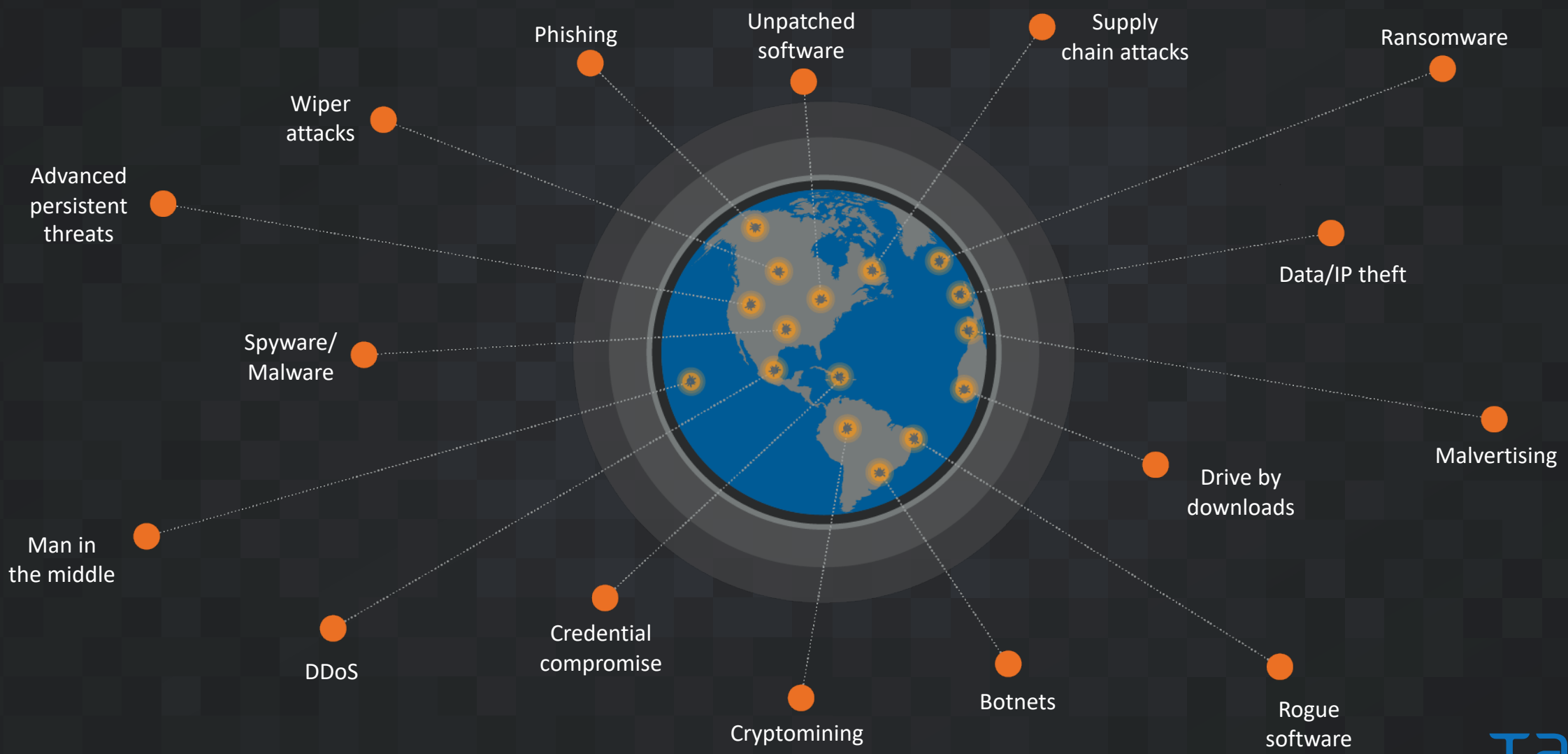
# Cisco Talos

Dmytro Korzhevin
Senior Threat Intelligence Researcher at Cisco Talos

02 November 2022

Talos
Cisco Security Research

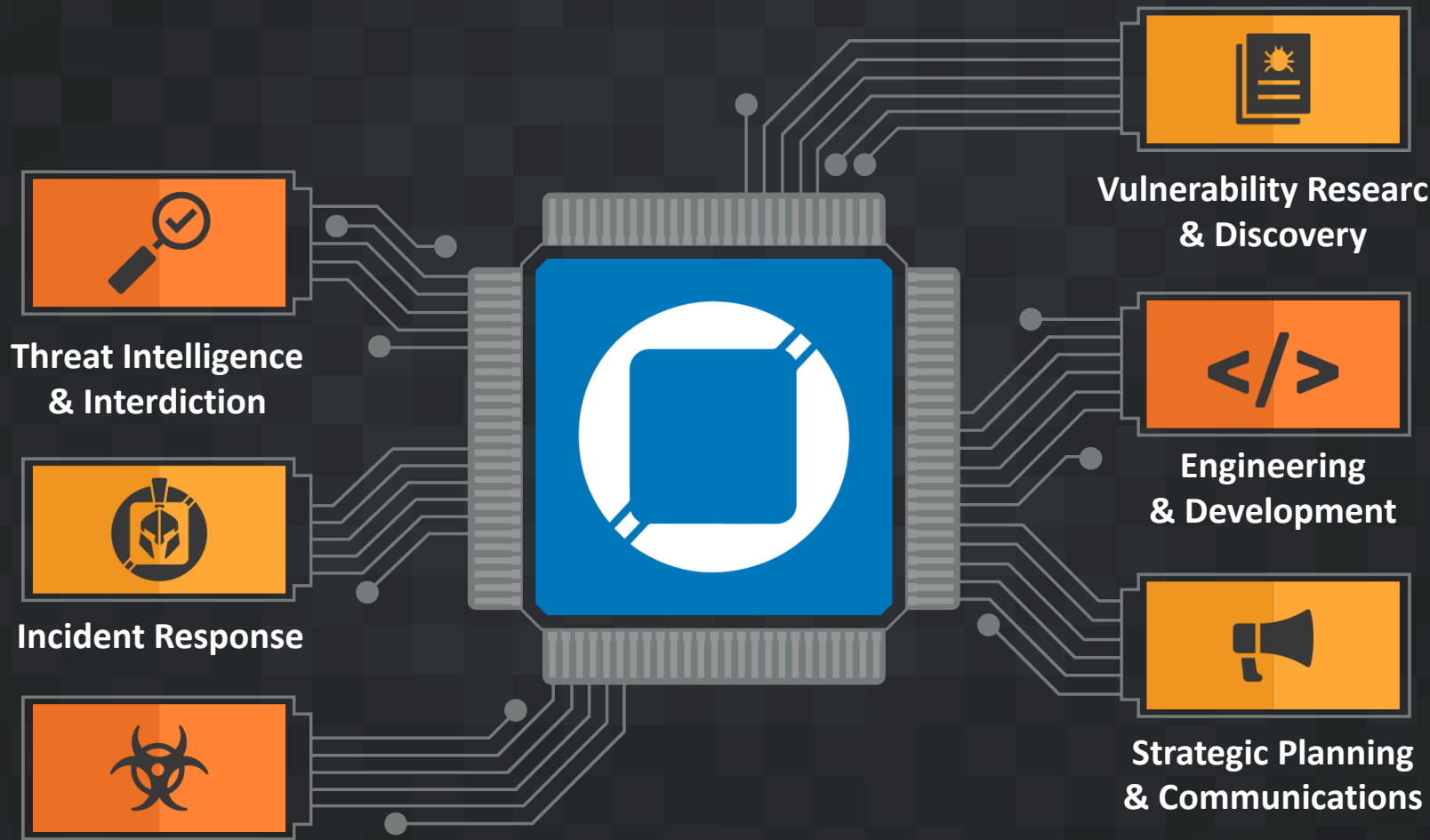
# Protecting Customers




Talos
Cisco Security Research

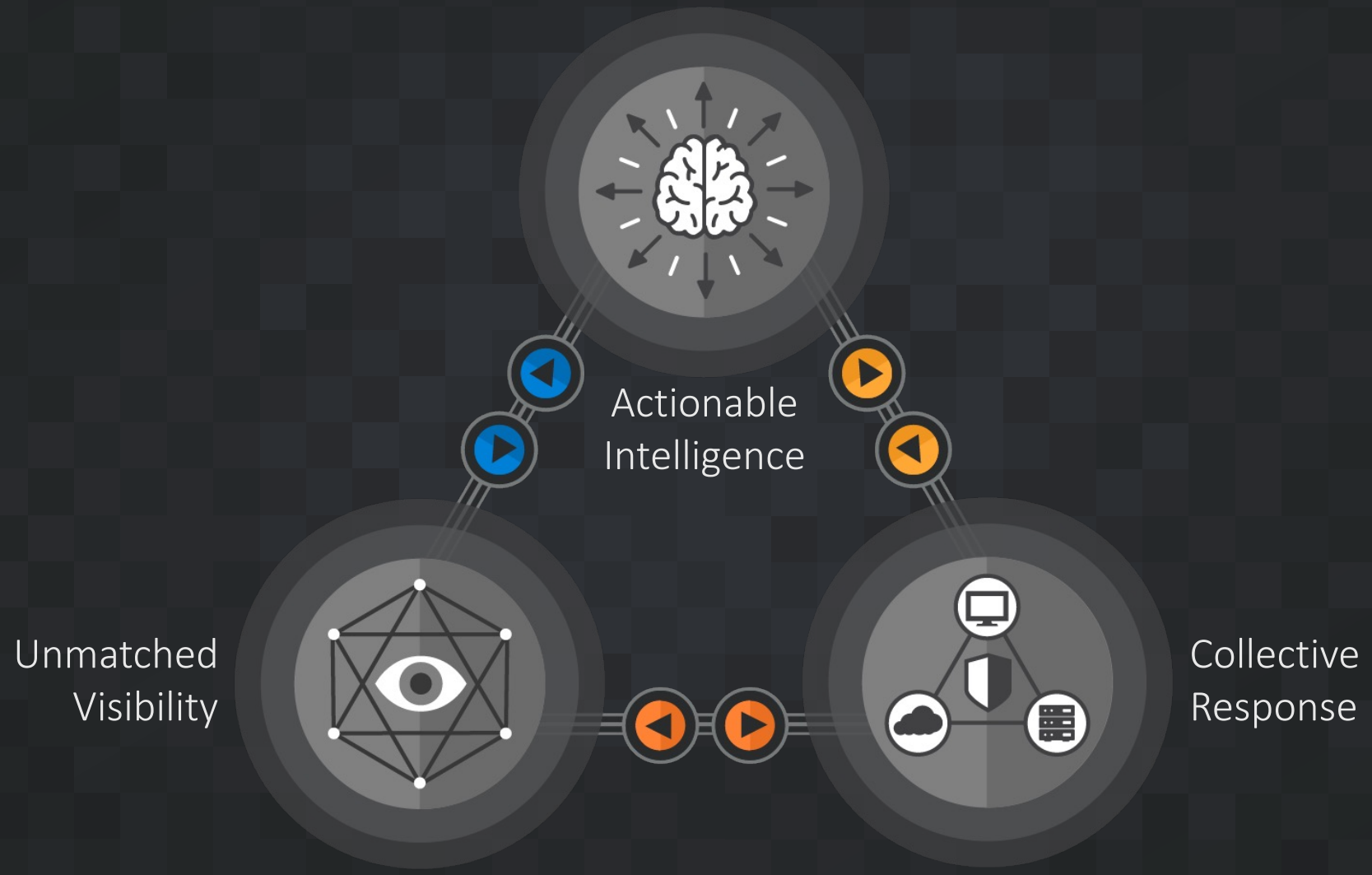
# Our job is protecting your network

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.




Talos
Cisco Security Research

# Why trust Talos?




Talos
Cisco Security Research

# Unmatched Visibility

To stop more, you have to see more.

- The most diverse data set
- Community partnerships
- Proactively finding problems

Unmatched visibility is built on relationships

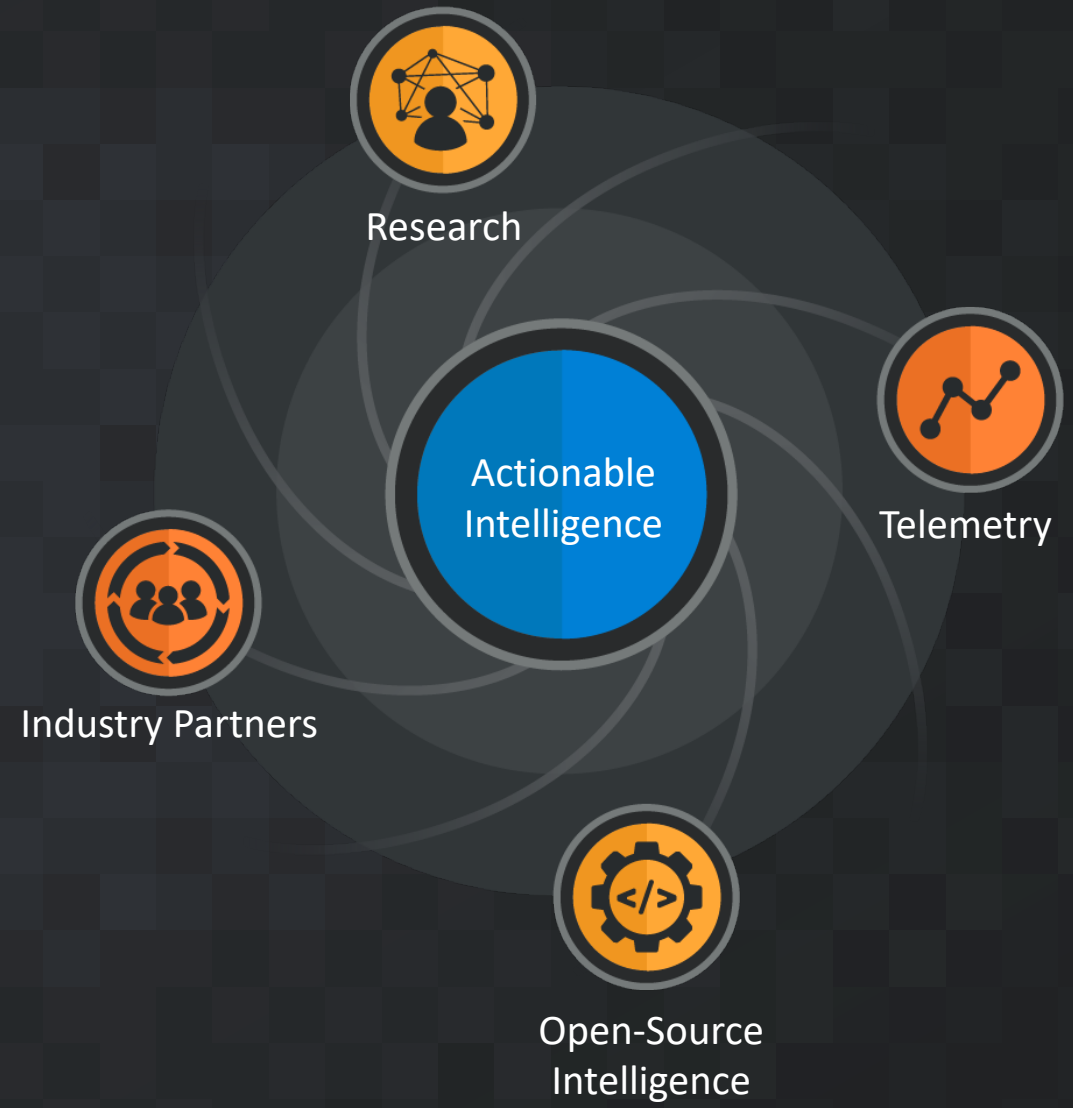

Talos
Cisco Security Research

# Actionable Intelligence

Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

It’s not detect and forget, it’s detect and analyze.




Talos
Cisco Security Research

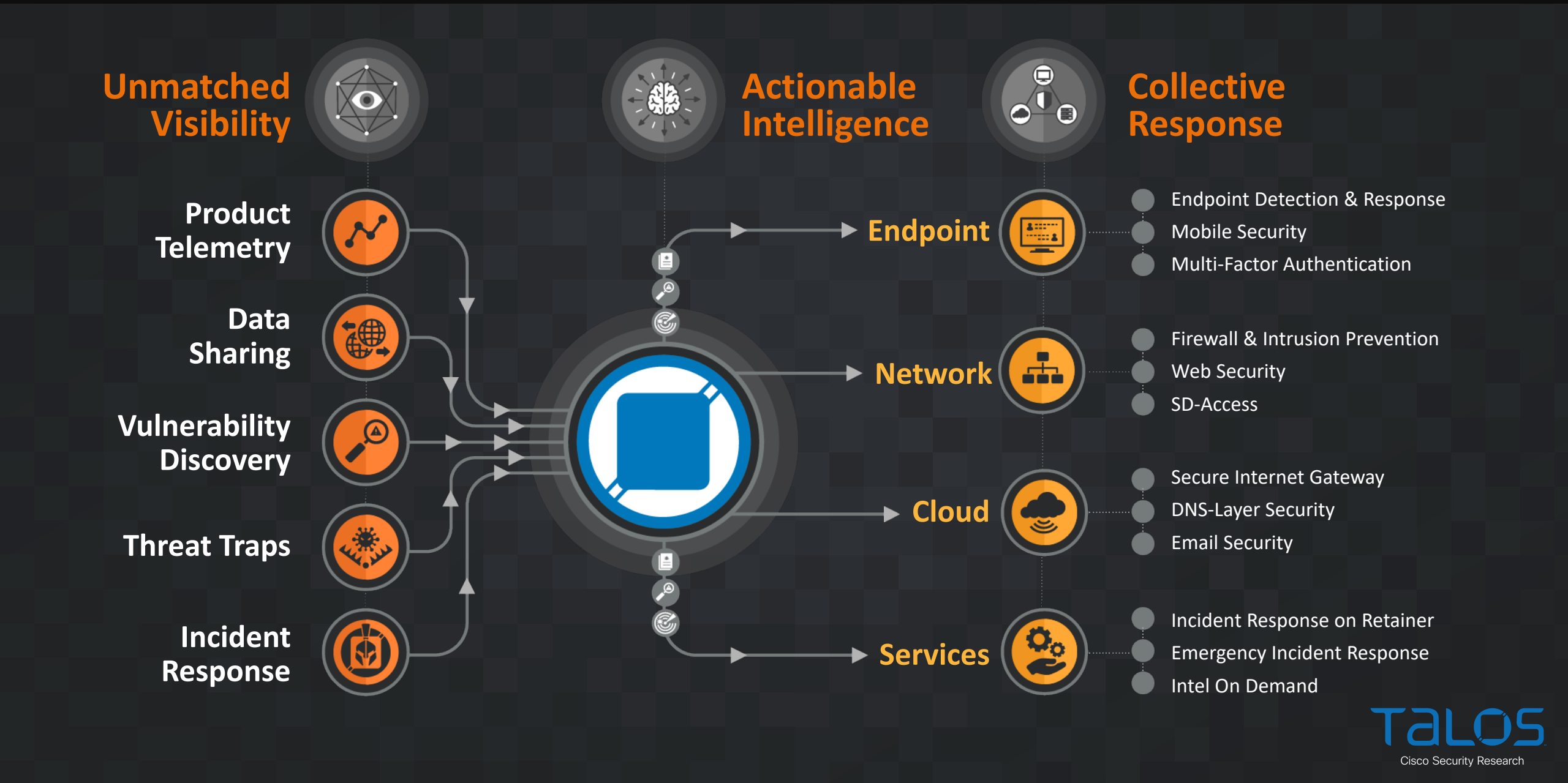
# Collective Response

The ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial

- **Breadth:** See once, protect everywhere
- **Depth:** Response and interdiction drives continuous research
- **Scale:** Delivering portfolio-wide protection, in real-time


Talos
Cisco Security Research

# From Unknown to Understood




Talos
Cisco Security Research

# 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

Talos
Cisco Security Research

# Options to Fit Your Customer's Needs


**Service Level Objectives**
4 Hours by Phone

**Hours**
40 hours


**Service Level Objectives**
4 Hours by Phone;
24 hours in-transit

**Hours**
80 hours

**Travel Included:**
1 Consultant,
up to 3 days


**Service Level Objectives**
4 Hours by Phone;
24 hours in-transit

**Hours**
120 hours

**Travel Included:**
Up to 2 Consultants,
up to 3 days each

## Benefits included in retainer options

- 24x7x365 access worldwide for Emergencies
- Dedicated Talos IR Consultants

Additional Benefits-
- Threat Intelligence Enrichment (Cisco Talos Emergency Intel Bulletins & Monthly Updates)

Tool Access-
- AMP, Umbrella, SW Cloud or Duo*

Limitations-
- If contract hours are under 50 hours in total, only Emergency Services will be available

Additional options are also available within your Enterprise Agreement (EA)

* As needed for ER, Compromise Assessment & at the discretion of the CTIR team

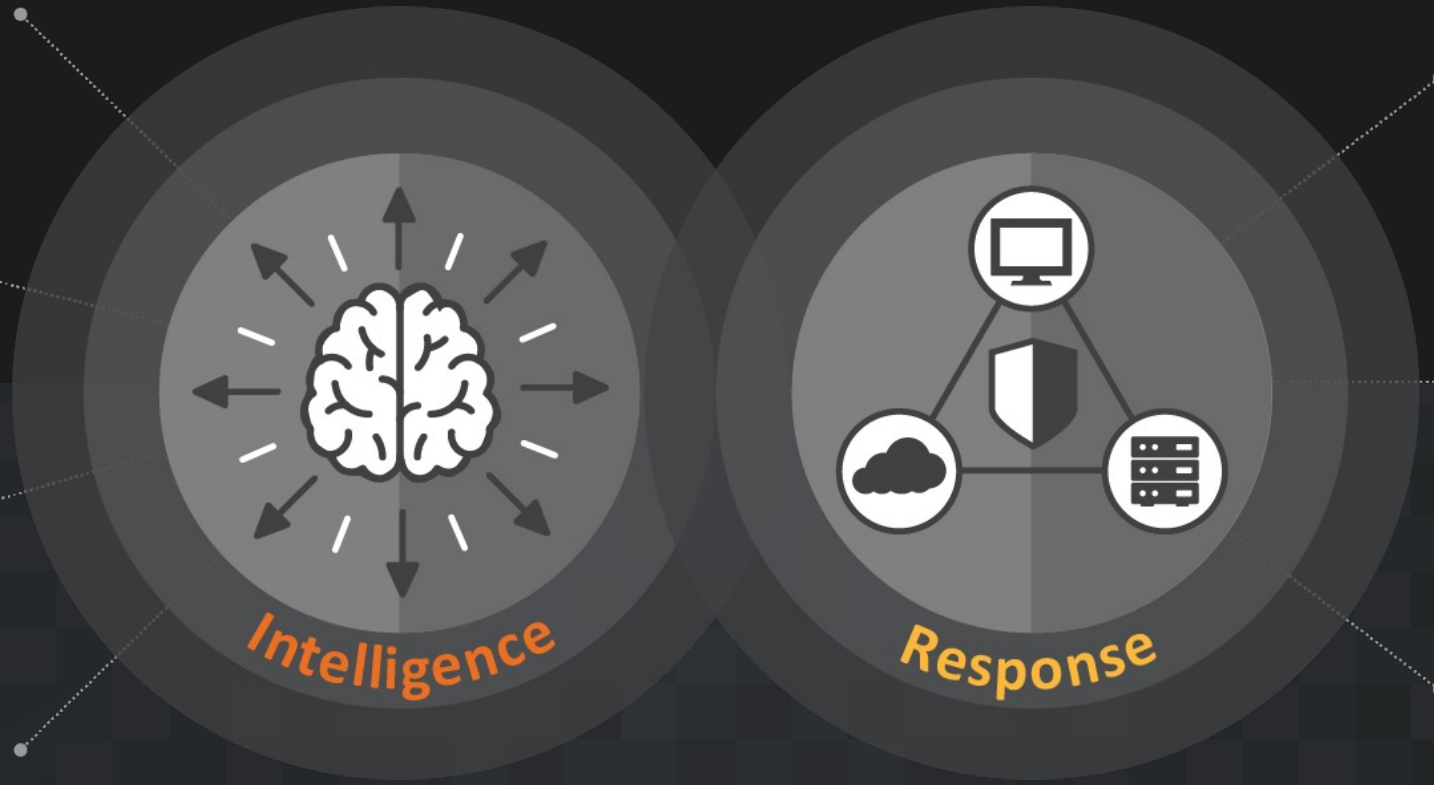
# World-class breadth and depth of Cisco Talos

**625B**
web requests per day

**200+**
vulnerabilities discovered per year

**1.4M+**
new malware samples per day

**30B**
endpoint events per day




**840K**
networks protected

**67M**
mailboxes protected

**87M**
endpoints protected

TALOS
Cisco Security Research

# Reporting Scope

This report covers incident response engagements closed out in Q3 2022 (July, August, September)

It documents the top threats we observed, TTPs, impact, and security weaknesses that facilitated adversary actions

Covers engagements in organizations in a wide variety of industries

Talos
Cisco Security Research

# Observed Trends

Top threat was commodity malware

Top initial vector was exploited or misconfigured public-facing applications

Top weakness was lack of MFA

Talos
Cisco Security Research

# Top Threats

# Commodity Malware

- Comprised 20% of all threats
- Variety of different families
- Looking forward: Ongoing Qakbot activity delivering a variety of threats

**Impact**

Commodity malware is widely available for purchase / free download and used by a variety of threat actors in various stages of their operations to deliver additional threats

# Commodity Malware Families

Qakbot (Qbot) banking trojan

Vidar infostealer

Redline Stealer

Remcos RAT

# Ransomware Families

Conti

BlackCat (ALPHV)

Unknown ransomware variant – amalgamation of other families

# Top Initial Vectors

Public-facing applications and email

## Notable Observations

Adversaries identified and exploited vulnerable or misconfigured public-facing applications

# Actions after Compromise

# Traversing the Network

Post-breach, an attacker may want to internally propagate malware throughout the victim network to infect more hosts

Notable observations:
Leveraging legitimate tools (LOLBins) such as WMI.

# Reaching Out to C2

Reaching out to C2 allows actor to carry out actions post-compromise

Infostealers relying on social media platforms to create C2 addresses

# Other Actions

Establishing persistence

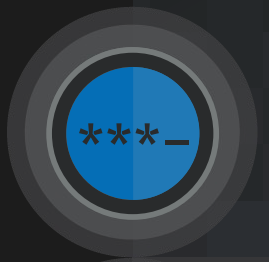
Exfiltration

Evasion

# Top ATT&CK Techniques

- T1078 Valid Accounts
- T1190 Exploit Public-Facing Application
- T1136 Create Account
- T1059.001 Command and Scripting Interpreter: PowerShell
- T1083 File and Directory Discovery
- T1003 OS Credential Dumping
- T1027 Obfuscated Files or Information
- T1021.001 Remote Desktop Protocol
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1056.001 Keylogging
- T1219 Remote Access Software
- T1486 Data Encrypted for Impact

# Recommendations



Instituting MFA!

Centralizing logs

Limiting Windows tools to trusted accounts

Segmenting network

Patching vulnerable systems

Talos
Cisco Security Research

# 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.

Talos
Cisco Security Research

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity