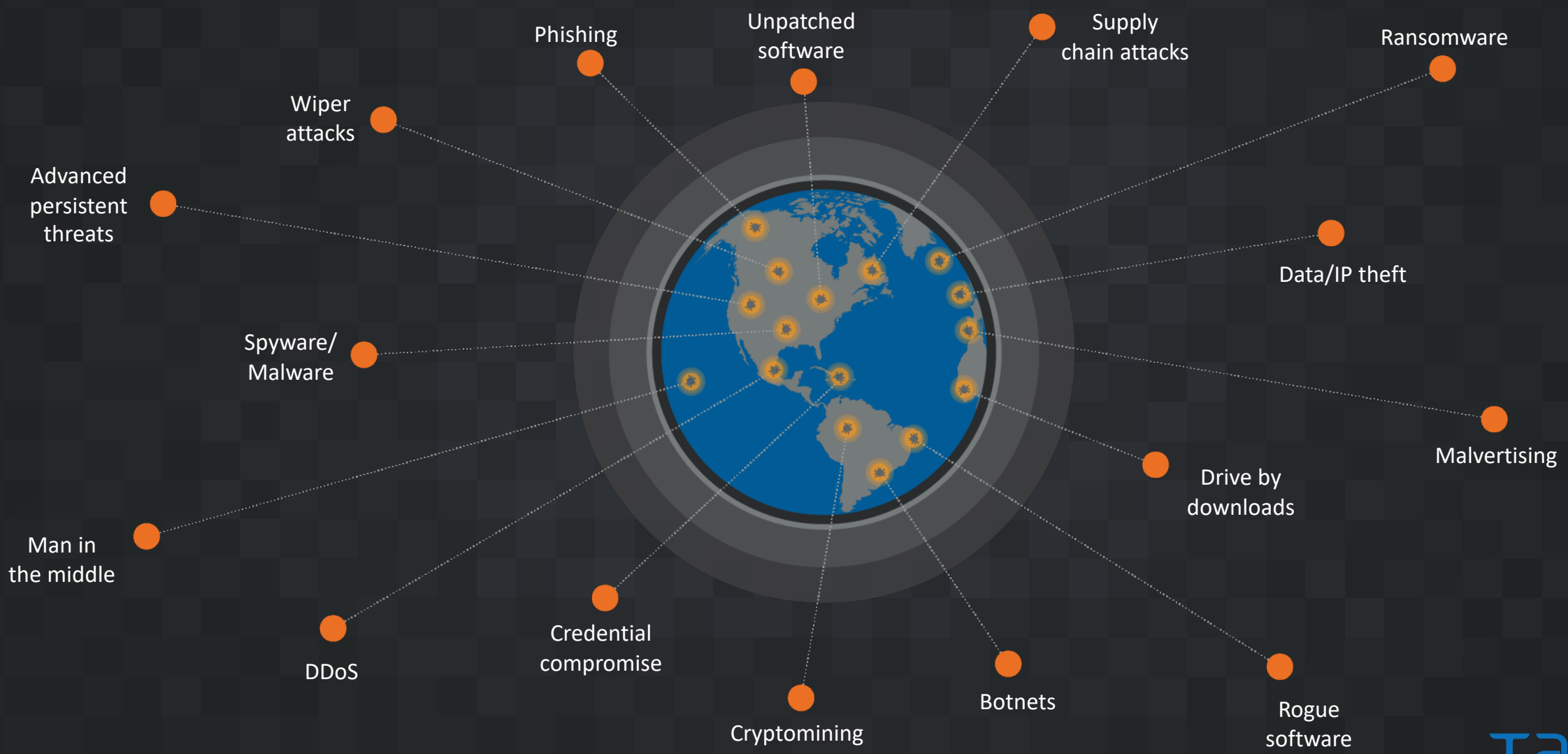
TALOS

Cisco Security Research

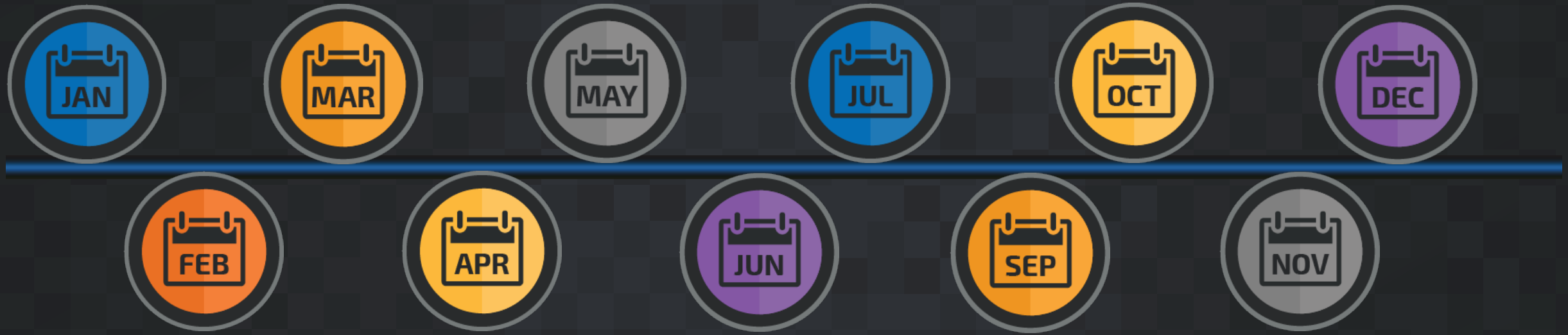
Fighting the Good Fight

Protecting Customers



Talos
Cisco Security Research

2020: The year in malware



JhoneRAT using well-known filehosting to avoid blacklisting

COVID-19 malicious campaigns

WolfRAT targets messaging apps on Android
Astaroth uses Youtube as C2 channel

Ransomware attacks peak, WastedLocker is big-game hunting

LemonDuck botnet with automated spreading capabilities

Xanthe docker-aware miner hit one of TALOS honeypots

Campaign delivering ObliqueRAT as 2nd stage when maldoc executes macro

TALOS takes a look at fingerprint cloning
PoetRAT uses COVID-19 to lure its victims
Zoom vulnerabilities

Highly modular dropper IndigoDrop to spread Cobalt Strike

"Internet did my homework" 😀

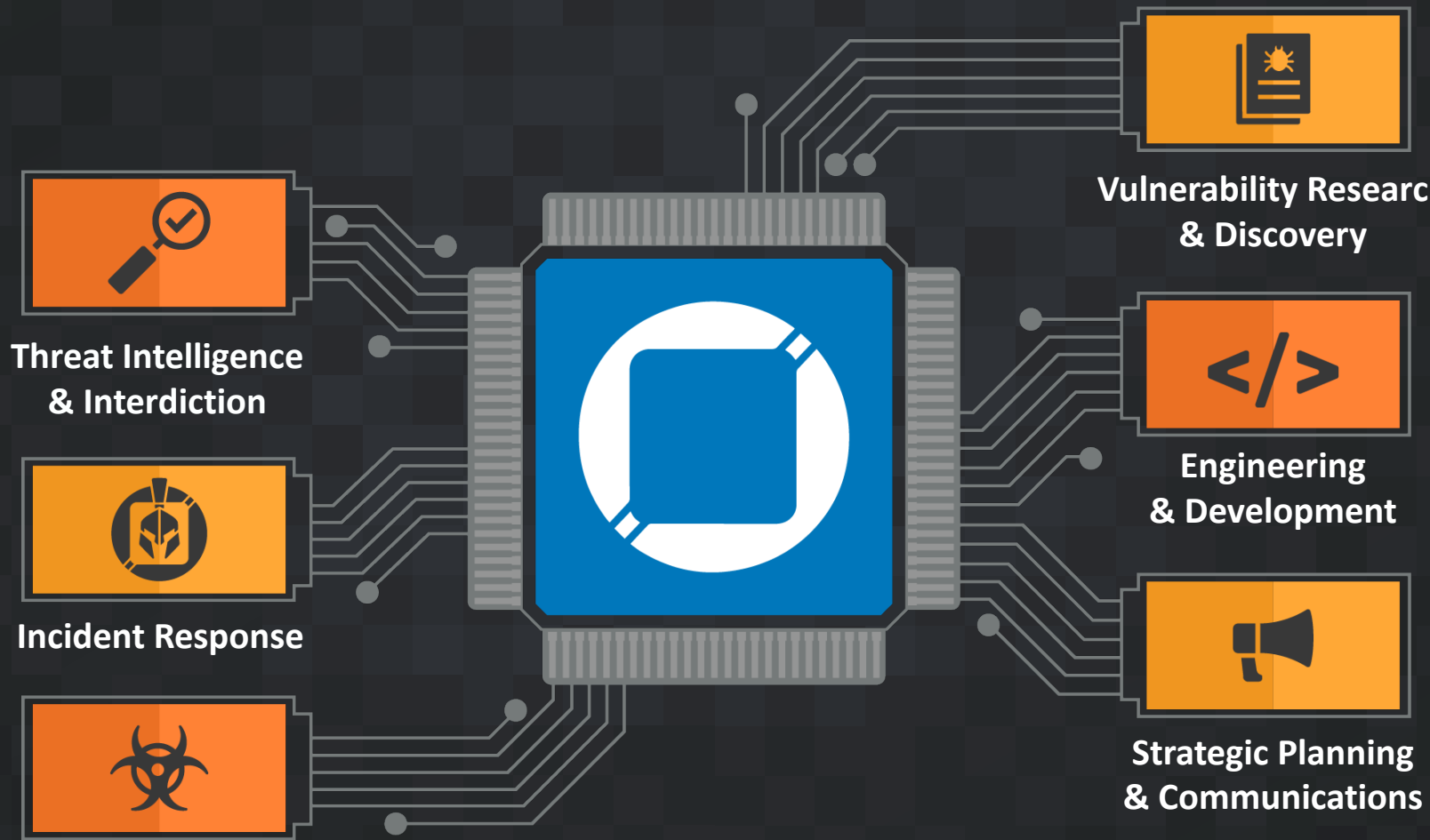
Emotet completes its 2020 comeback with huge Aug-Oct spam volumes

https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2020/09/coverage-strikes-back-cobalt-strike-paper.html

TALOS
Cisco Security Research

Our job is protecting your network

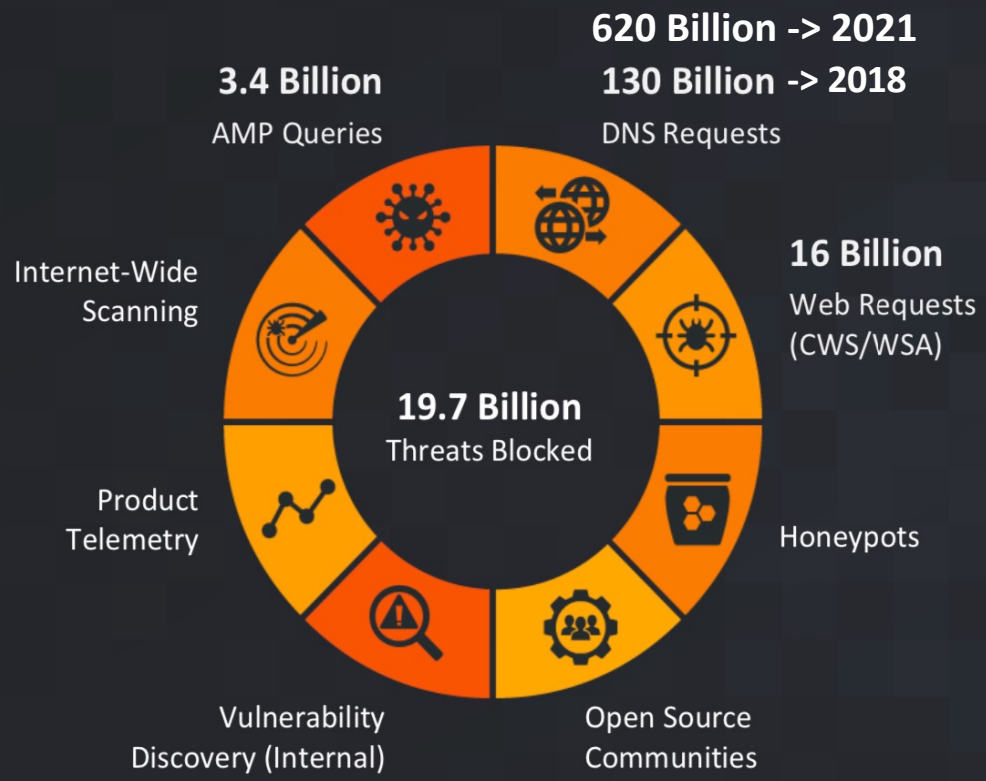
Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



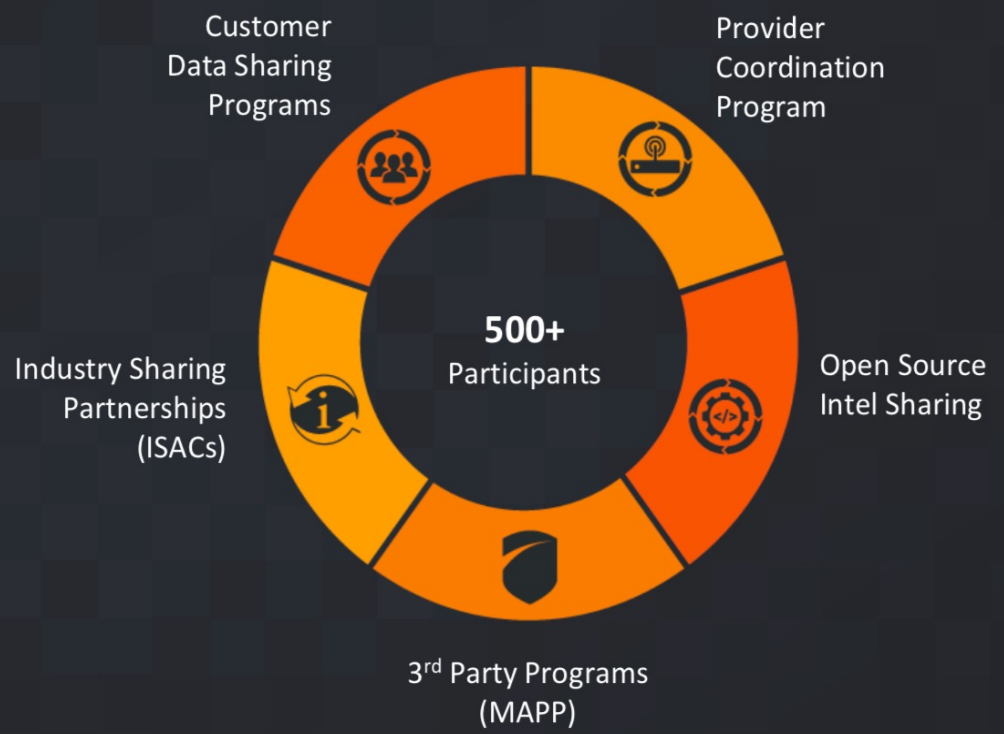
Talos
Cisco Security Research

Daily Intelligence Flow

Threat Intel



Intel Sharing



350+
Full Time Threat Intel Researchers

Millions
Of Telemetry Agents

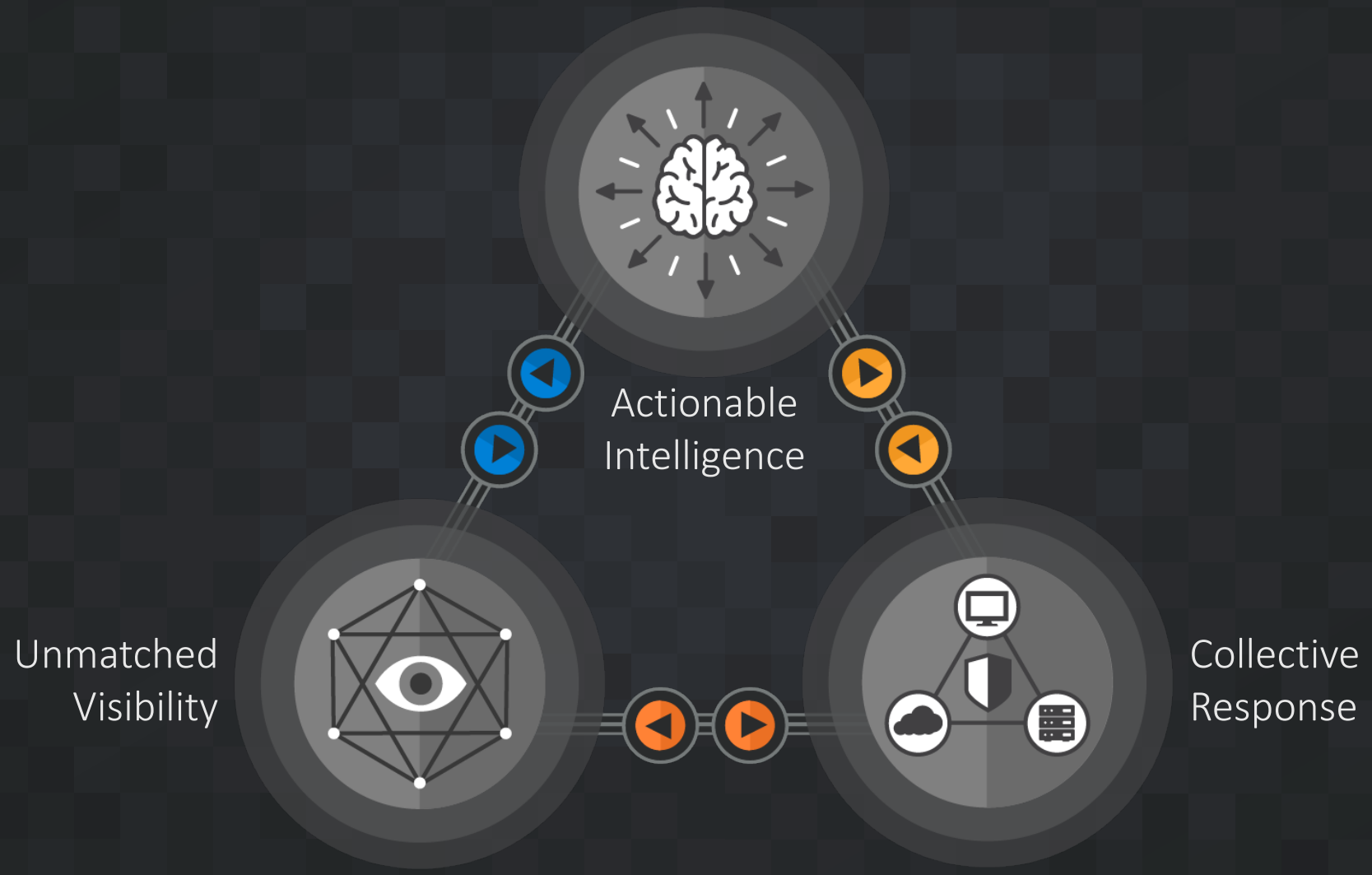
4
Global Data Centers

100+
Threat Intelligence Partners

1100+
Threat Traps

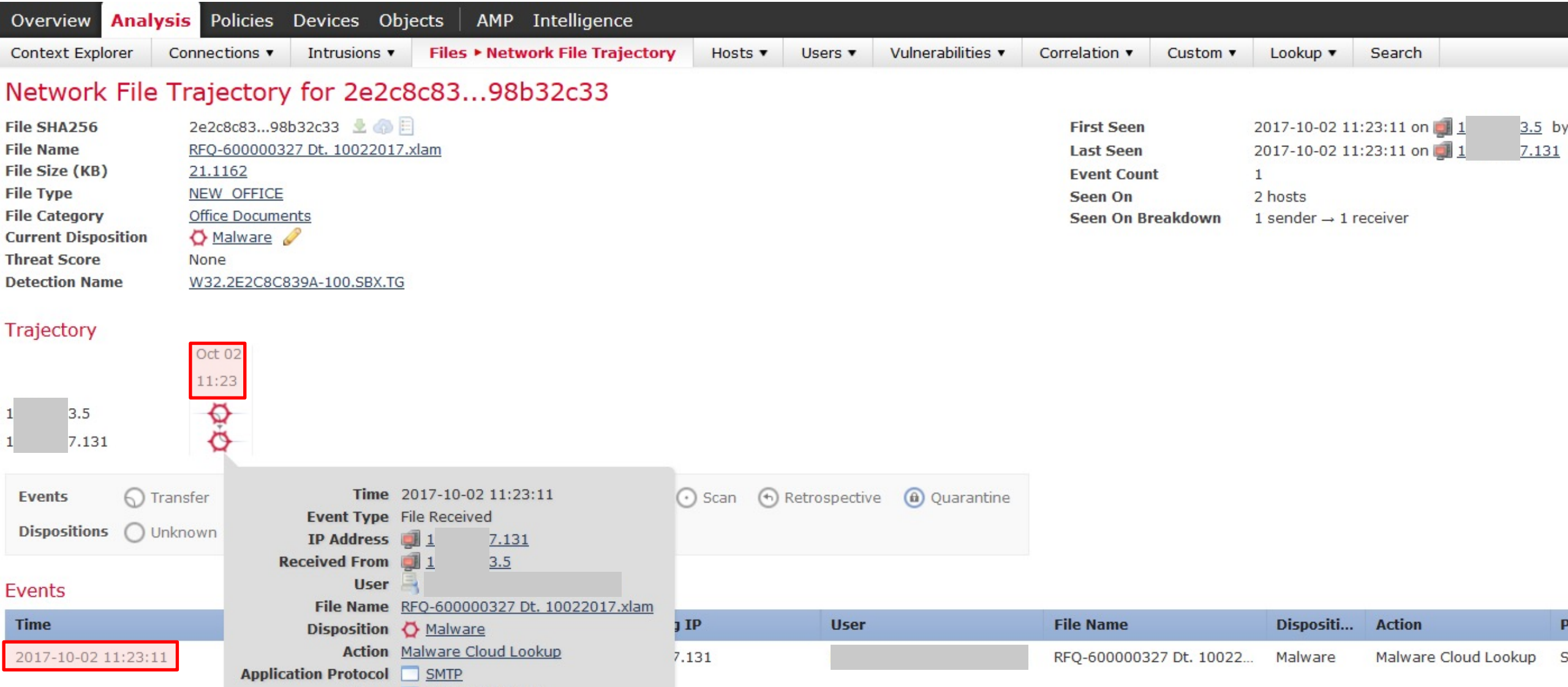
Product telemetry and privacy:
https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet

Why trust Talos?



Talos
Cisco Security Research

Reálna spamová kampaň šíriaca malvér v podobe MS Office dokumentov...



...a TALOS o tejto kapani vedel 2 hodiny vopred

ThreatGRID
Malware Threat Intelligence Platform

ehavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

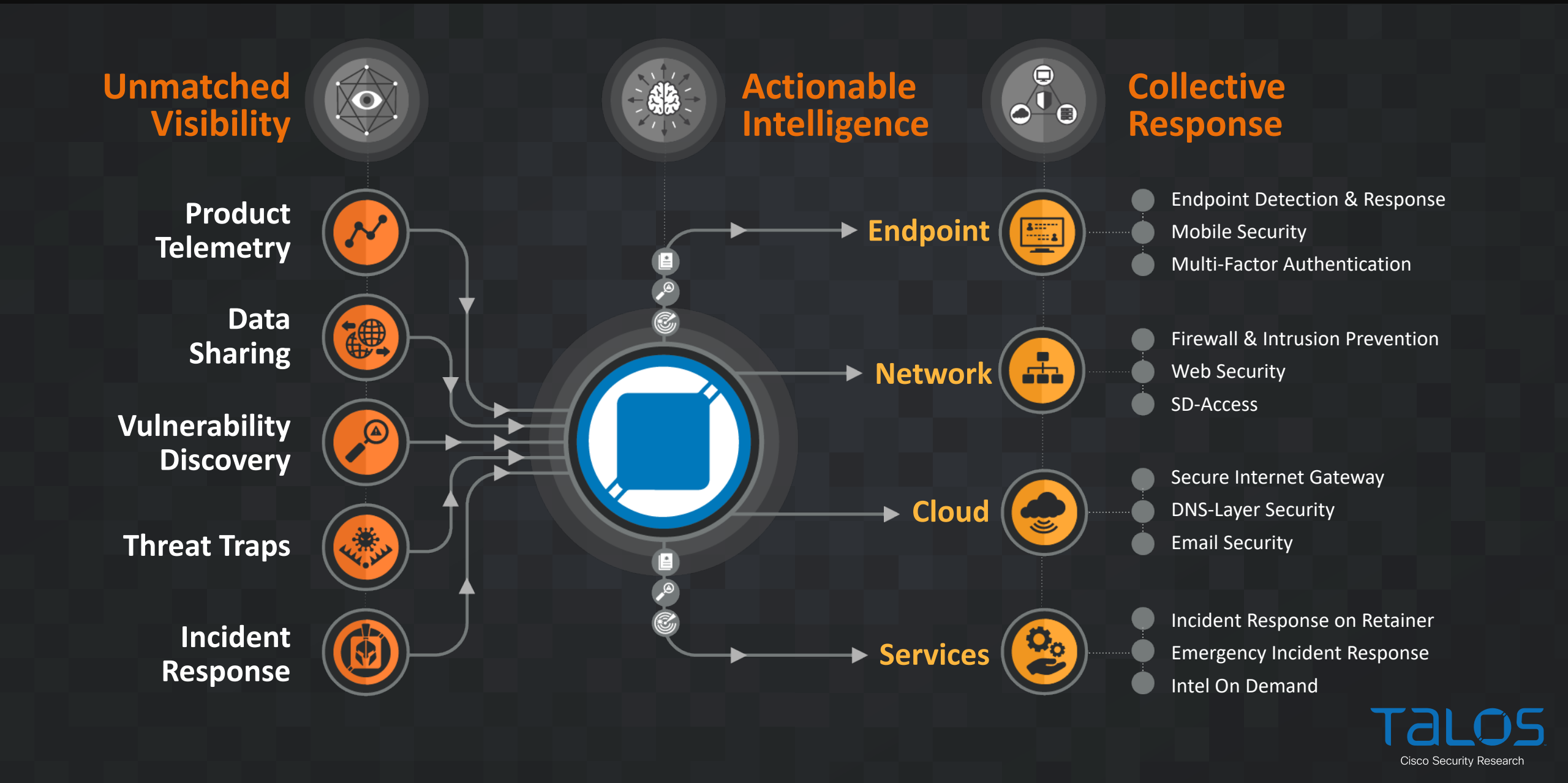
Analysis Report

ID	6869328459ce86e1a056da2232dfcbc6	**Filename**	RFQ-600000327 Dt. 10022017.xlam
OS	7601.18798.amd64fre.win7sp1_gdr.150316-1654	**Magic Type**	Microsoft Excel 2007+
Started	10/2/17 09:27:02	**Analyzed As**	xlsx
Ended	10/2/17 09:33:56	**SHA256**	2e2c8c839a3253dcc30fc57aab04603c602d882fa29f98bfdc27213198b32c33
Duration	0:06:54	**SHA1**	4b3ec9d13241361b4c25a1bbf689d65142e8c8de
Sandbox	car-work-042 (pilot-d)	**MD5**	9da62bf1900241fd29b0513ad7c864de

Behavioral Indicators

Document Created an Executable File	Severity: 100	Confidence: 100
Office Document Launches a Powershell	Severity: 100	Confidence: 100
Document with Random Variables Established Network Communications	Severity: 100	Confidence: 95
A Suspicious Document Containing Randomized Variable Names Detected	Severity: 95	Confidence: 100
Artifact Flagged Malicious by Antivirus Service	Severity: 100	Confidence: 95
Process Hollowing Detected	Severity: 100	Confidence: 95
PowerShell With Encoded Command Downloads Data	Severity: 95	Confidence: 100
A Document File Established Network Communications	Severity: 100	Confidence: 90
Document Launched Utility Application	Severity: 100	Confidence: 90
A Document File Established Direct IP Communications	Severity: 100	Confidence: 90
Registry Persistence Mechanism Refers to an Executable in a Temporary Folder	Severity: 90	Confidence: 100
Office Document Launches a Command Shell	Severity: 90	Confidence: 100

From Unknown to Understood



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

TALOS

Cisco Security Research

Ďakujem