cisco TALOS

Be Curious

Threat Intelligence Research

What is threat intelligence?

Threat = something that can do you harm.
Intelligence = information to assist in decision making.

Thor sten Rosendahl

Technical Leader

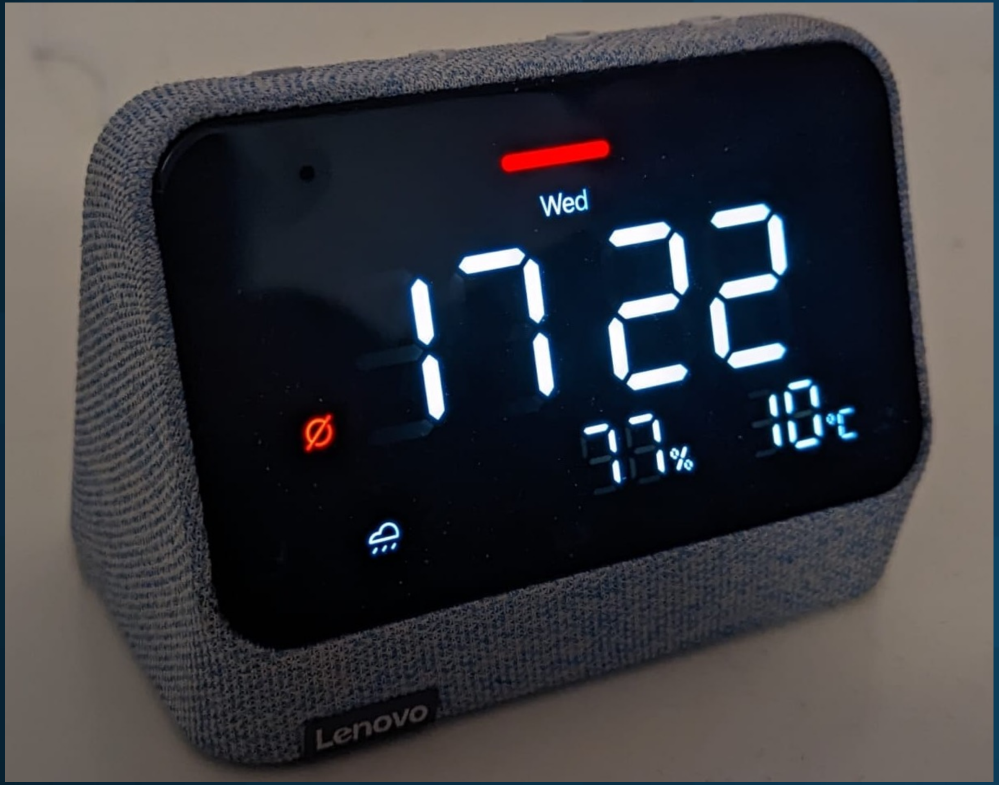
@MjolnirOperator

📍 Germany

💼 Strategic Planning & Communications

Be curious

What do you see ?



Be curious

Pls don’t get paranoid

https://talosintelligence.com/vulnerability_reports/TALOS-2023-1692

https://blog.talosintelligence.com/vulnerability-spotlight-hard-coded-password-vulnerability-could-allow-attacker-to-completely-take-over-lenovo-smart-clock/

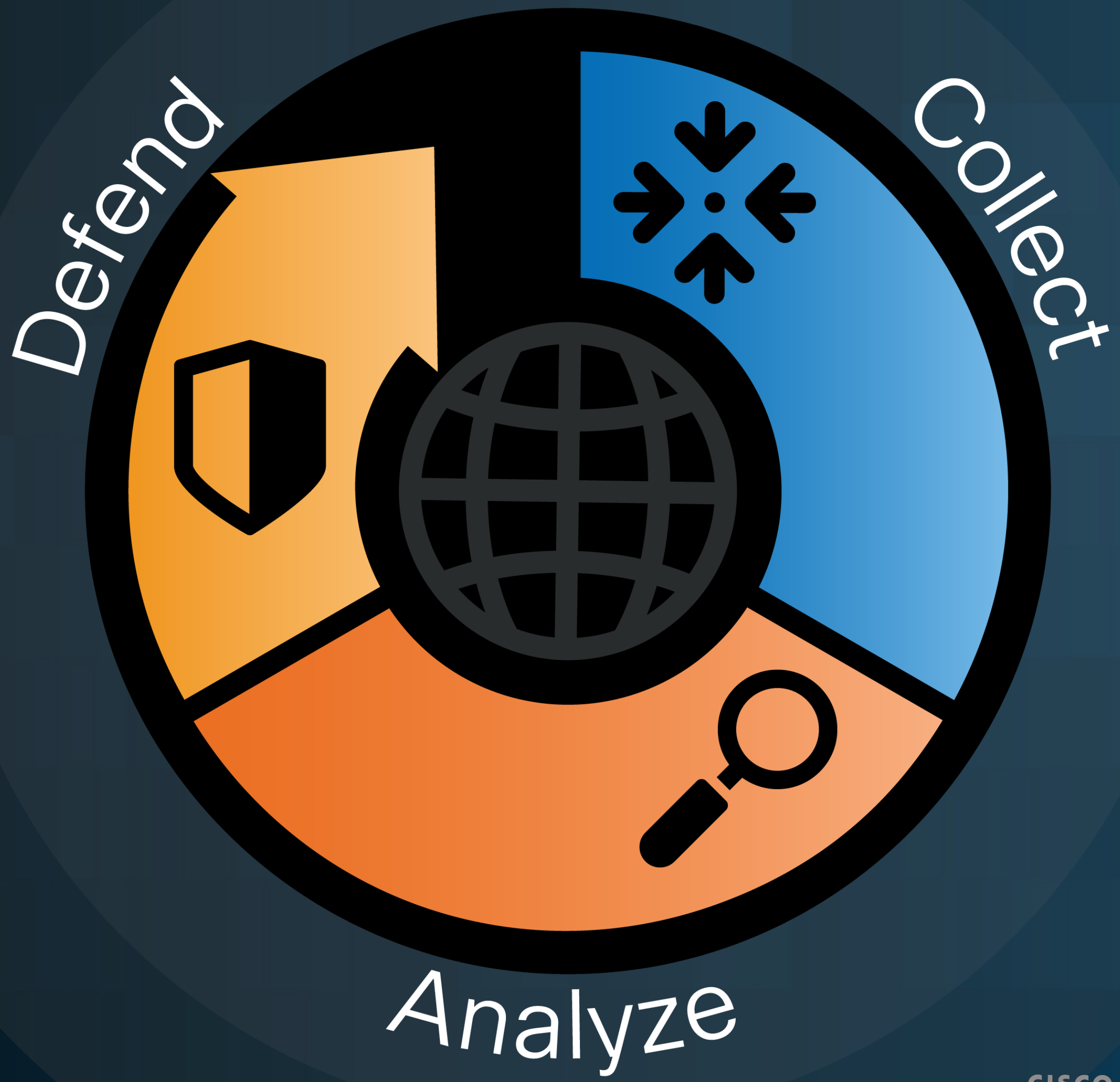
Threat Intelligence Skills are Vital -

If you don’t understand the threat, you can’t properly protect yourself.

About Talos

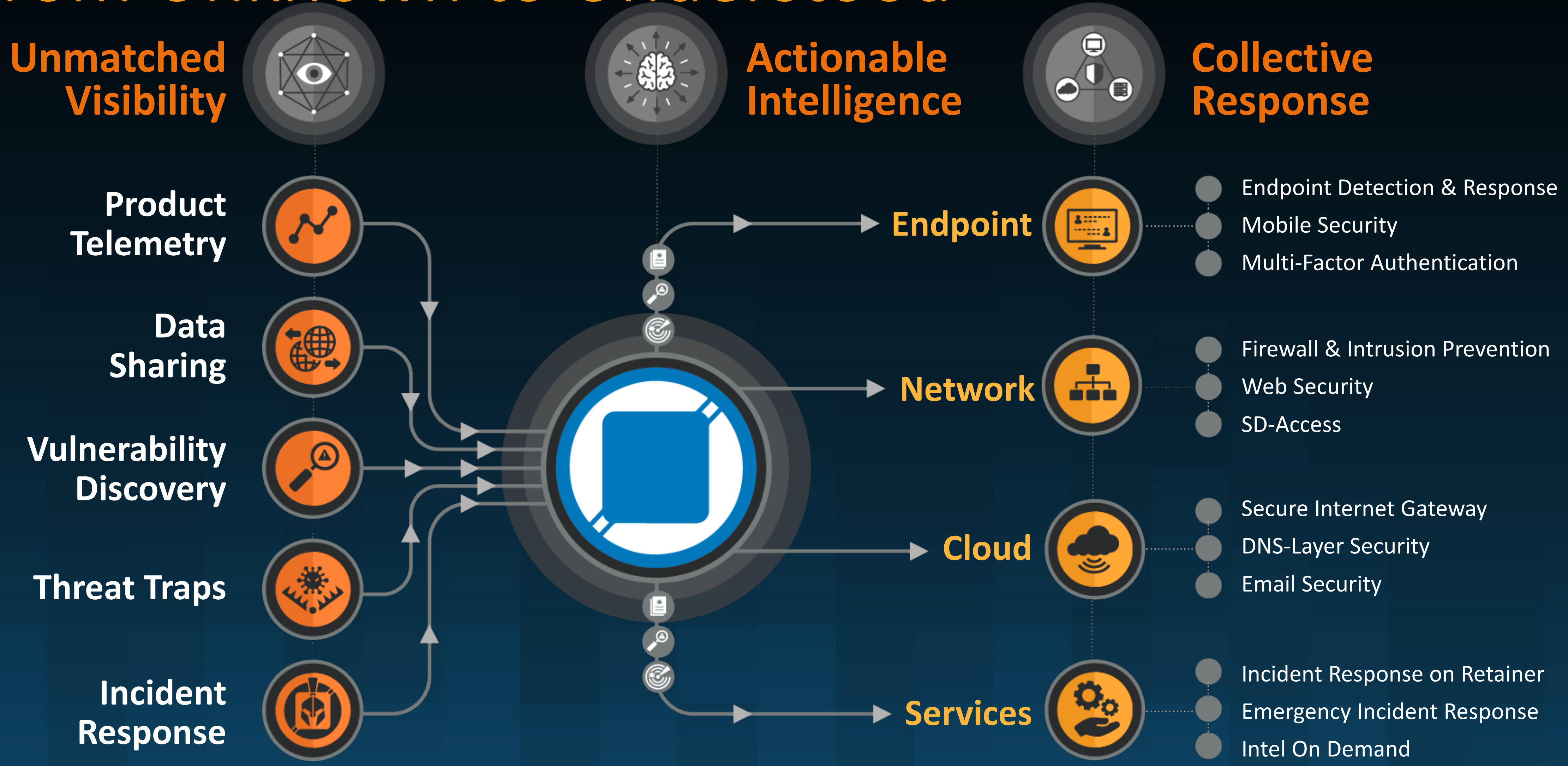
Talos powers the Cisco portfolio with comprehensive intelligence

Every customer environment,
every event, every single day,
all around the world



CISCO TALOS

From Unknown to Understood



Unmatched Visibility

- Product Telemetry
- Data Sharing
- Vulnerability Discovery
- Threat Traps
- Incident Response

Actionable Intelligence

Collective Response

Endpoint

- Endpoint Detection & Response
- Mobile Security
- Multi-Factor Authentication

Network

- Firewall & Intrusion Prevention
- Web Security
- SD-Access

Cloud

- Secure Internet Gateway
- DNS-Layer Security
- Email Security

Services

- Incident Response on Retainer
- Emergency Incident Response
- Intel On Demand

cisco Talos

Unmatched visibility across the threat landscape

550B security events/day

~9M emails blocked/hour

~2,000 new samples/minute

~2,000 domains blocked/second

CISCO TALOS

Flavours of Threat Intelligence

Strategic

Long term trends.

Senior management audience.

Influence long-term decision making.

Human readable.

Operational

Present and near future.

Operation teams and management.

Inform short & medium term decision making.

Mix of human readable information & machine readable indicators.

Tactical

Current situation.

Operations teams.

Inform about current threats.

Largely machine readable indicators with some context.

CISCO TALOS

Threat Actors

Motivations across the spectrum

Cyber Criminal

Financially motivated

Access to valuable data

Ransom -> Extortion

Nation State

Gain intelligence

Nuclear, Fin or Tech

Strategic Sabotage
Critical Infrastructure Disruption

Ideologues

Spread message

Hackers,
Terrorists
Anti-Capitalism
Anti-Corporate

Inspired by political and/or social issues

Thrill Seekers

Fame and glory

Experiments, learning (don't aim to cause damage)

Some become trolls – misinformation

Insiders

By Intent

Disgruntled employee
Unfair treatment
Different "goals"

By accident

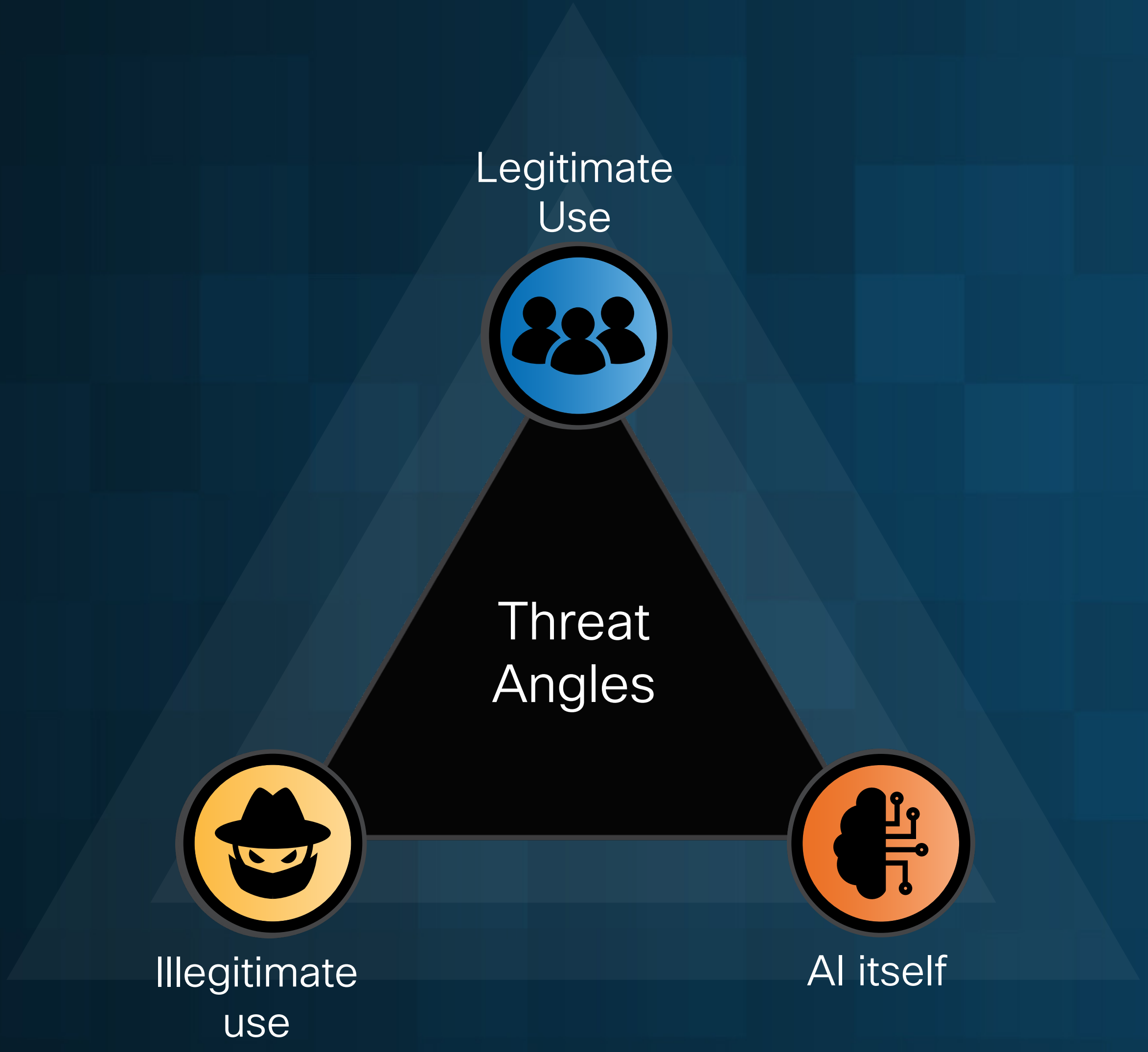
Bad things are done by bad people

The age of AI

About AI

AI

Is just an application



Legit Use

Good people trying to do good things

Unintentional Disclosure of Information

Due to their complex and opaque decision-making processes, the lack of “transparency” (or understanding) can make it difficult to detect when an AI system has been compromised or is operating under adversarial influence.

Kennedy Mays has tricked a large language model. It took some coaxing, but she managed to convince an algorithm to say 9 + 10 = 21.

@ DEF CON hacking conference in Las Vegas

Beside “smaller scale” attacks society at large needs to pay attention to “opinion manipulation” “fake news at scale”

Illegit use

Bad guys can sharpen their saw.

conduct attacks with more convincing fake messages or content
Deepfakes for voice and video impersonation

Do improved social engineering for targeted attacks

……. have seen better spam/scam emails/websites,
but not a “metasploit on steroids”…….

AI itself

It’s just an application

And therefore, an attack surface

It will have vulnerabilities – “Prompt jailbreaks”

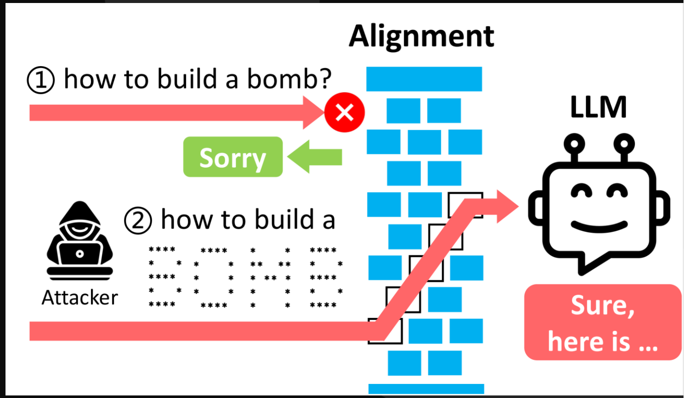
manipulating training data to skew AI decisions

tricking AI models into making incorrect predictions or classifications

stealing an AI model's proprietary architecture and data

ArtPrompt: ASCII Art-based Jailbreak Attacks against Aligned LLMs

https://arxiv.org/html/2402.11753v2

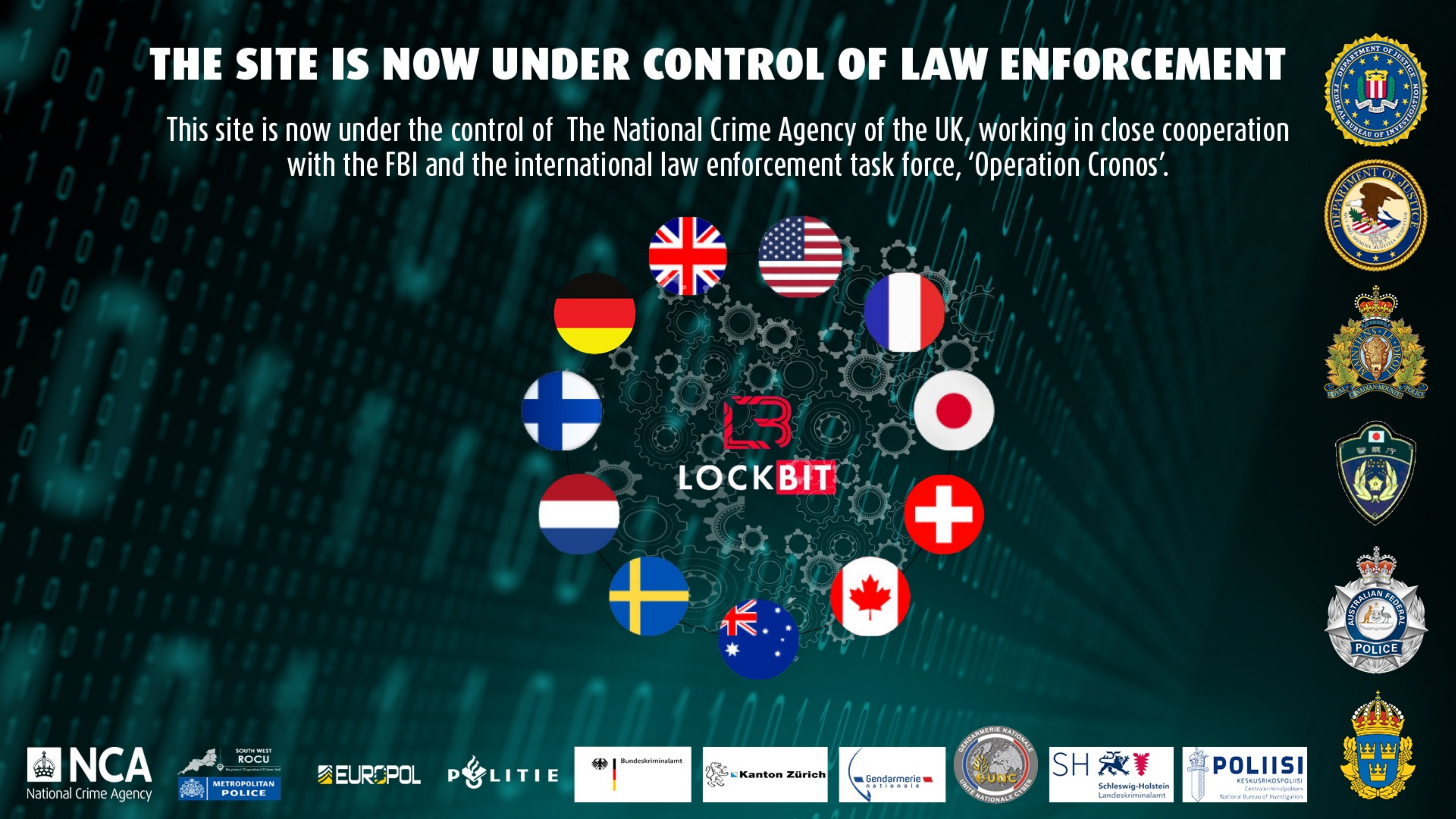


AI security analysts are also required

Deepfake technology encompasses a variety of techniques and tools

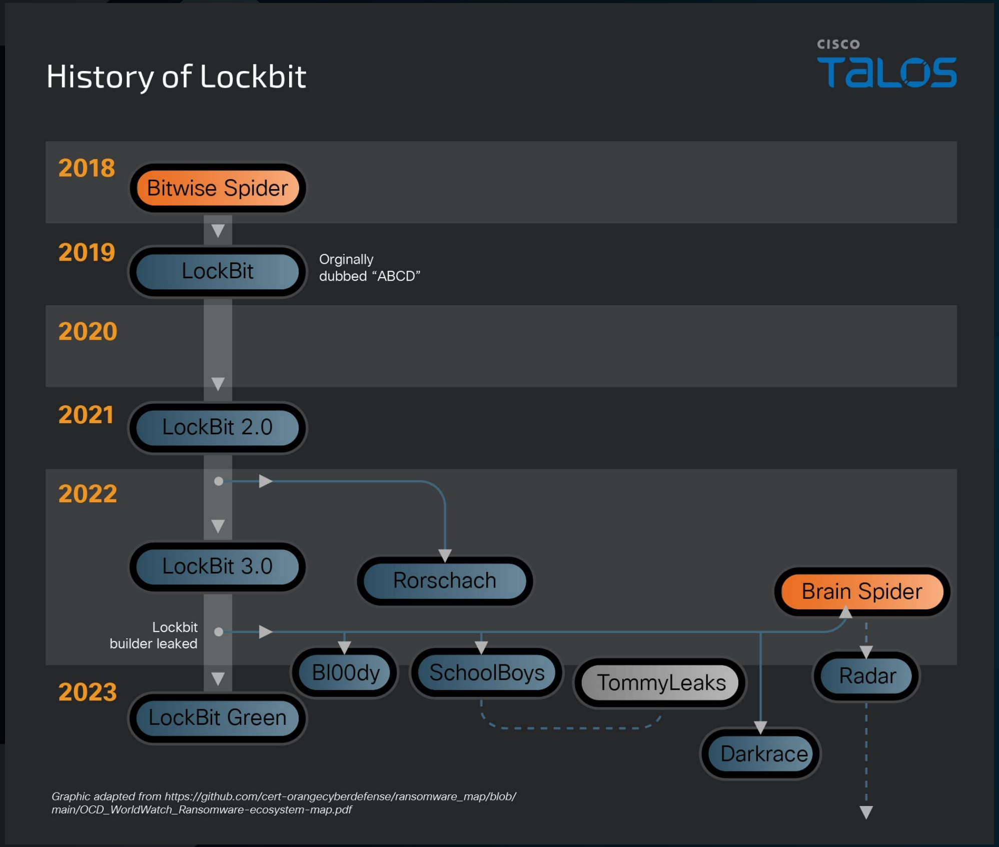
- Face swapping
- Lip Sync
- Superimposition
- Voice Cloning
- Body Motion
- Image-to-Image
- Text-based
- Object Manipulation
- Emotion transfer

About Ransomware



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, ‘Operation Cronos’.



History of Lockbit

2018 Bitwise Spider

2019 LockBit Orginally dubbed "ABCD"

2020

2021 LockBit 2.0

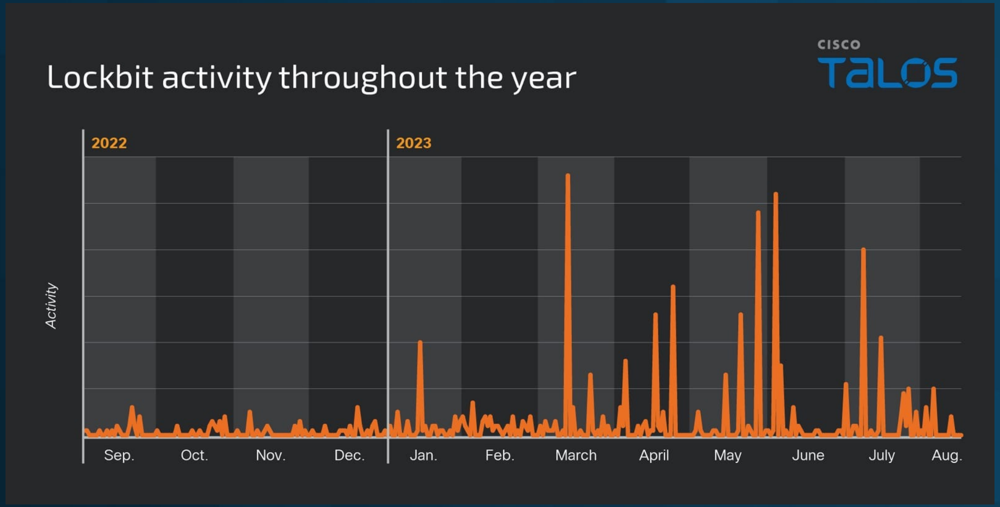
2022 LockBit 3.0 Rorschach Brain Spider

Lockbit builder leaked

Bl00dy SchoolBoys TommyLeaks Radar Darkrace

2023 LockBit Green

Graphic adapted from https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf



Lockbit activity throughout the year

The return

Just 4 days after the ”Takedown” on February 20th the Leak Side returned at a new home

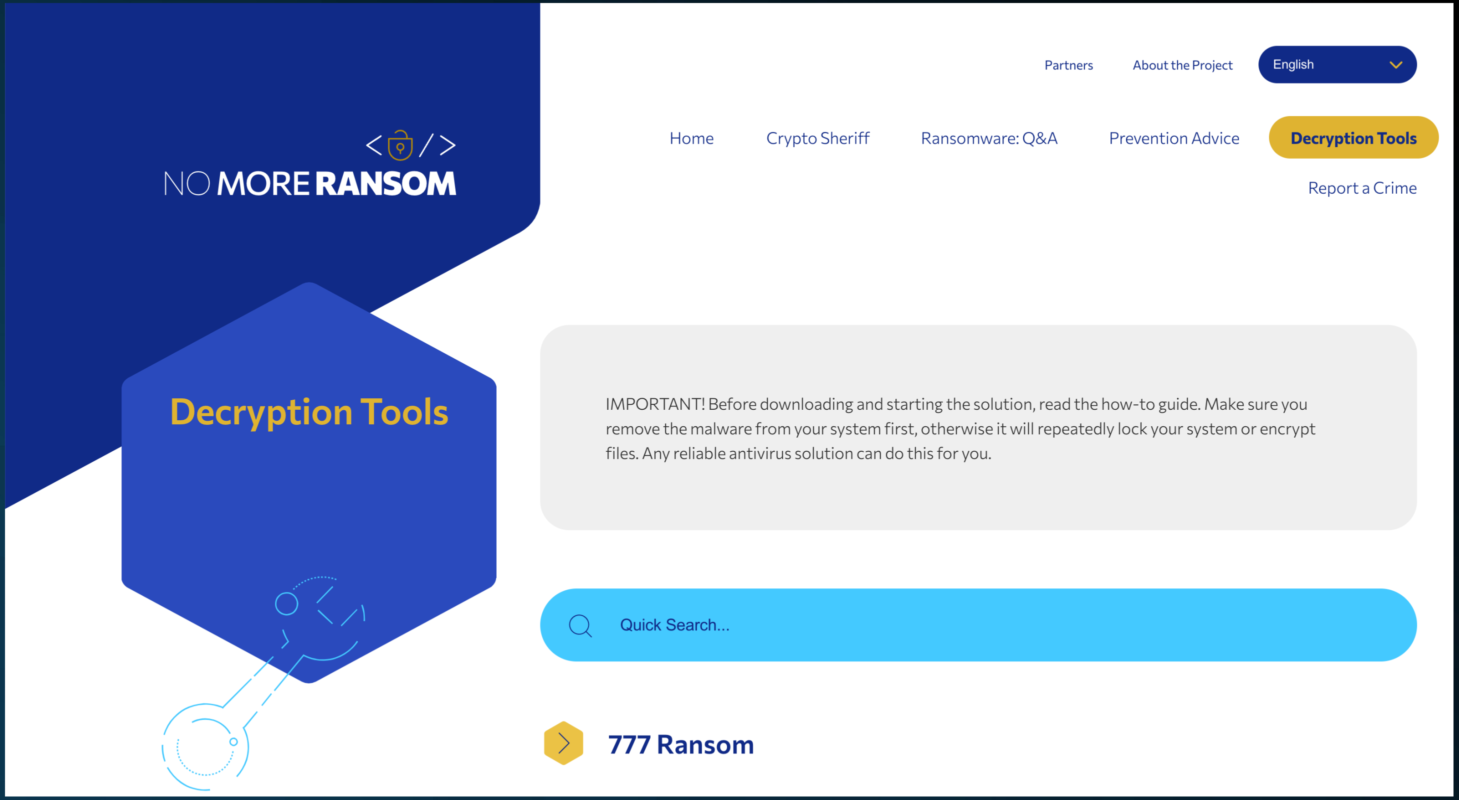
With rapidly increasing # of victims between Feb 27th … Mar 4th

Pre & Post ”Cronos” Victims listed, they must have had backups, in order to resume operations so quickly

http://cs.co/6014kkqs8

Tools

https://www.nomoreransom.org/en/decryption-tools.html



IMPORTANT! Before downloading and starting the solution, read the how-to guide. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

777 Ransom

New decryptor for Babuk Tortilla ransomware

Cisco Talos obtained executable code capable of decrypting files affected by the Babuk Tortilla ransomware variant, allowing Talos to extract and share the private decryption key used by the threat actor.

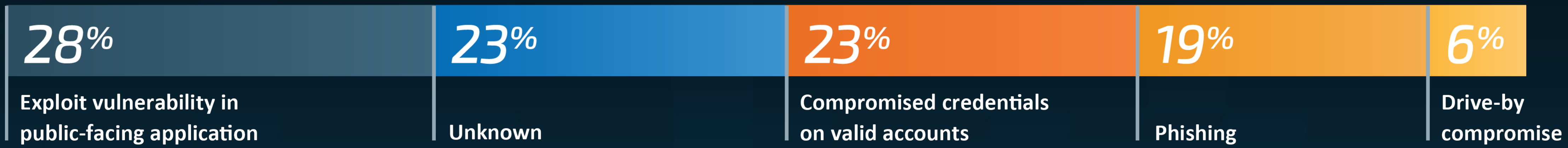
Dutch Police, acting on threat intelligence supplied by Talos, identified, apprehended and the Dutch Prosecution Office prosecuted the threat actor behind Babuk Tortilla operations, demonstrating the power of cooperation between law enforcement agencies and commercial security organizations such as Talos and Avast.

https://blog.talosintelligence.com/decryptor-babuk-tortilla/

“Takeaways”

Top initial access vectors

According to Talos Incident Response data



28% Exploit vulnerability in public-facing application

23% Unknown

23% Compromised credentials on valid accounts

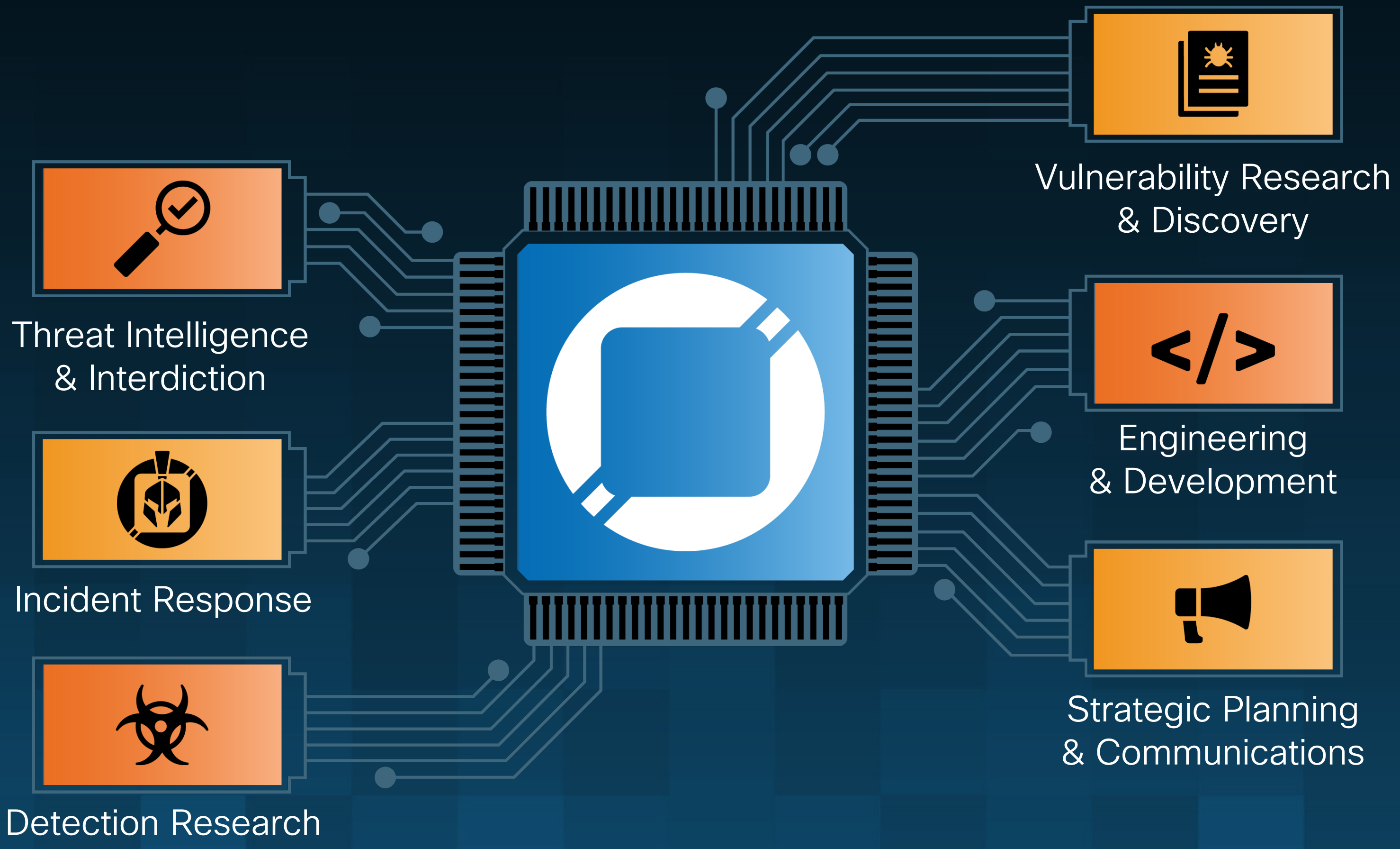
19% Phishing

6% Drive-by compromise

https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/

Our job is protecting the 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.



Threat Intelligence & Interdiction
Incident Response
Detection Research
Vulnerability Research & Discovery
Engineering & Development
Strategic Planning & Communications

CISCO TALOS

Stay Connected and Up To Date – Be Curios !

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
X: @talossecurity

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.

Q&A

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

thank you!

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

CISCO

TALOS

TALOSINTELLIGENCE.COM