Securing today and tomorrow – The intersection of intelligence, people and strategy.

Grant Paling
Product Manager,
Orange Cyberdefense

orange™ Cyberdefense

Do you remember me?

Grant Paling

- 17 years in Cyber Security
- I looooooove gangster movies (and all movies, really)
- I also like swimming, running and cycling a long way

Product Management

- Managed Services strategy, packaging and service development
- Strategic consulting services

Grant Paling
Product Manager,
Orange Cyberdefense

What am I going to talk about?

1

Recap:

What did we do today?

2

Here and now:

What do we do with that?

3

The future:

Where can we take it next?

What am I going to talk about?

1

Recap:

What did we do today?

2

Here and now:

What do we do with that?

3

The future:

Where can we take it next?

What did we do today?

Cyber Extortion remains a thriving business model

Successful attempts to catch the bad guys

Proactive about identifying and closing the gaps in a collaborative way

Implementing a consistent approach to security posture

What am I going to talk about?

1

Recap:

What did we do today?

2

Here and now:

What do we do with that?

3

The future:

Where can we take it next?

What am I going to talk about?

1

Recap:

What did we do today?

2

Here and now:

What do we do with that?

3

The future:

Where can we take it next?

3 things…

- Strategy
- Intelligence
- People

3 things…

- Strategy
- Intelligence
- People

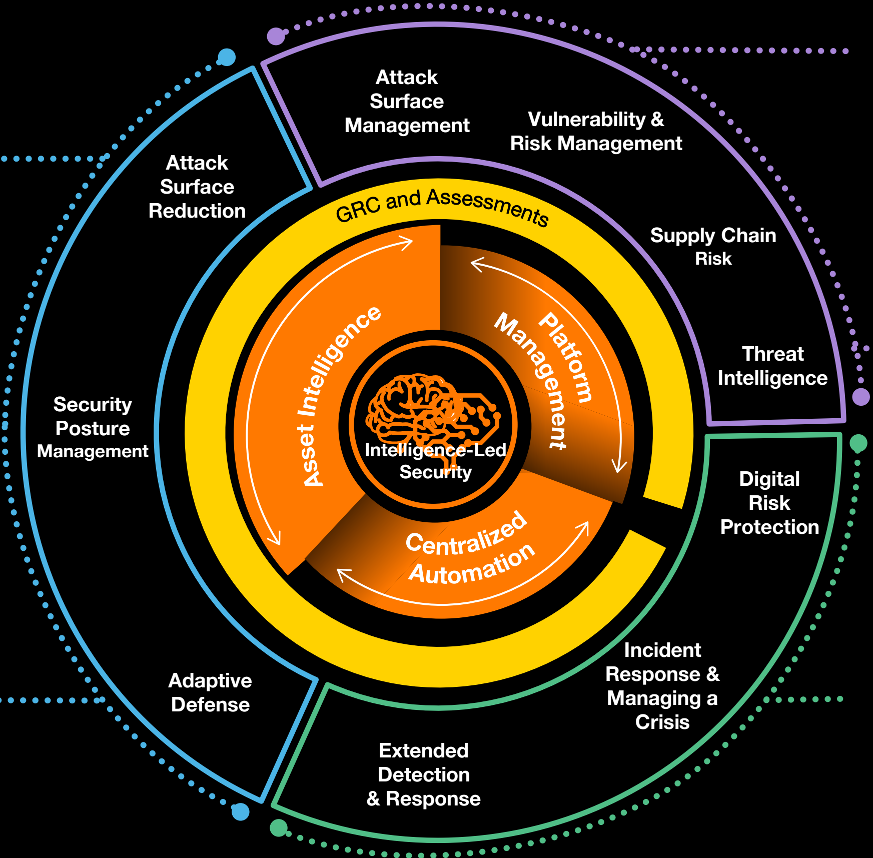
Layers of Defense

One trusted partner

Close down gaps across your attack surface

Continuously monitor and manage configuration

Stop high-risk threats in real-time with ZERO false positives



Identify your exposed digital assets and your biggest risks

Understand emerging threats

Detect and defend against active breaches inside and out

3 things…

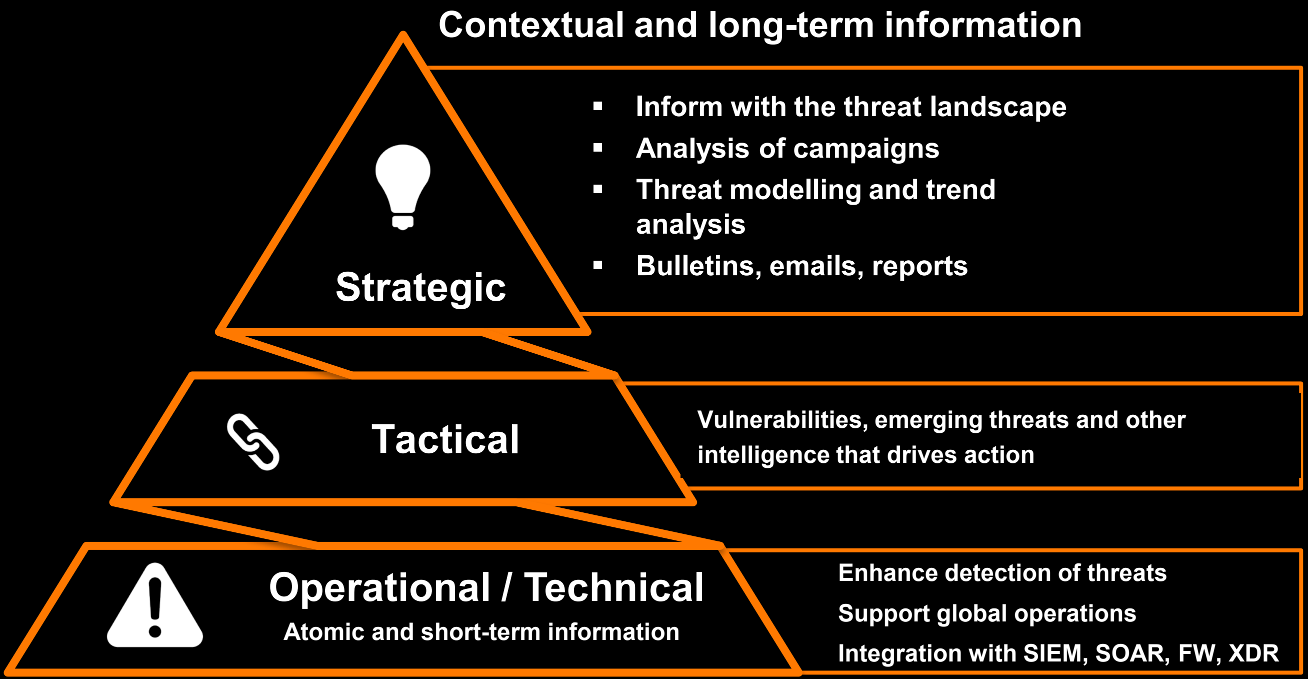
- Strategy
- Intelligence
- People

3 things…

- Strategy
- Intelligence
- People

The Cyber threat intelligence process organizes the data

… to the output



Contextual and long-term information

Strategic

- Inform with the threat landscape
- Analysis of campaigns
- Threat modelling and trend analysis
- Bulletins, emails, reports

Tactical

Vulnerabilities, emerging threats and other intelligence that drives action

Operational / Technical

Atomic and short-term information

Enhance detection of threats

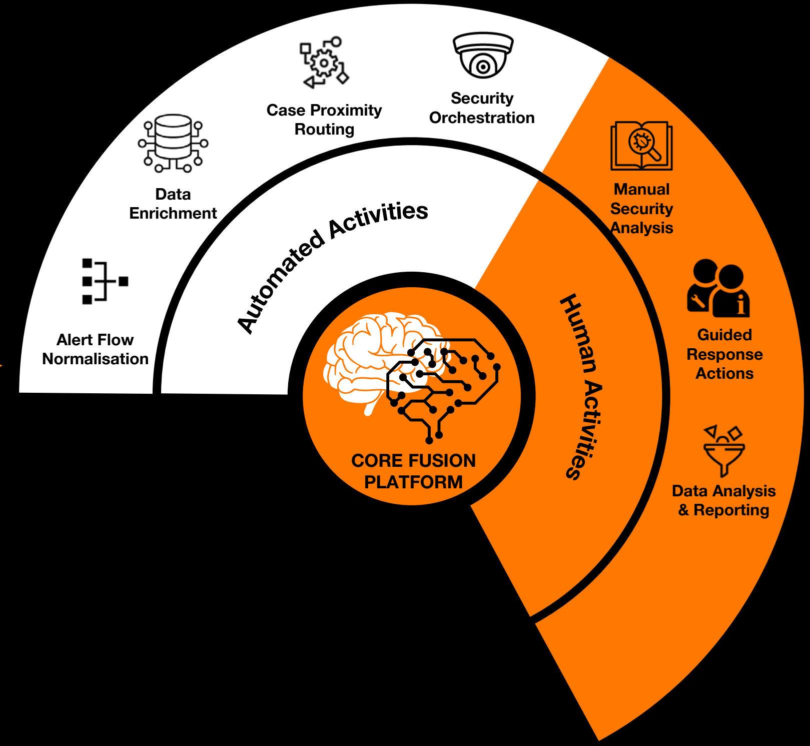
Support global operations

Integration with SIEM, SOAR, FW, XDR

Strategic Intelligence

Delivering Strategic Intelligence through incident classification

Feedback →



VERIS framework

True Positives ✓

- Who was the threat Actor
- What Action did they take
- Which Asset(s) were compromised
- What were the Attributes impacted?
- What phases of the kill chain were observed?

False Positives ✗

- Who caused it?
- Why did it happen?
- What can be done to make sure it doesn't happen again?

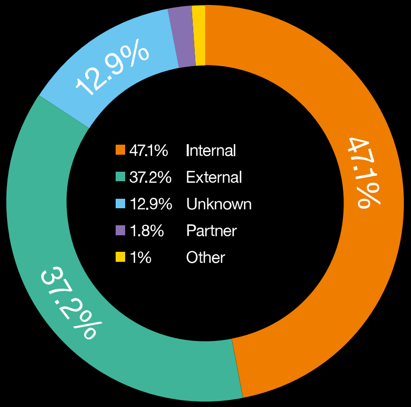
Informing the big picture

Security Navigator: Research-driven insights to build a safer digital society

Security Incidents: Top root causes

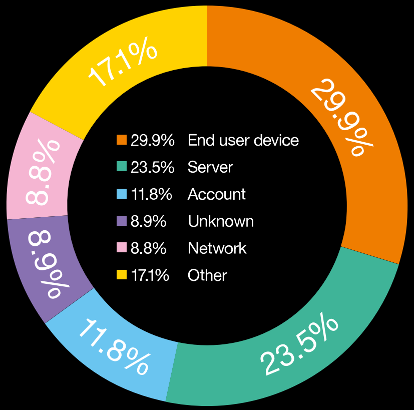
Source: Orange Cyberdefense Security Navigator 2023

Source



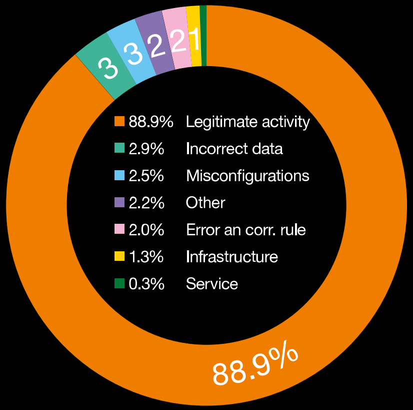
~47% of incidents are caused by internal sources, not external ones.

Target



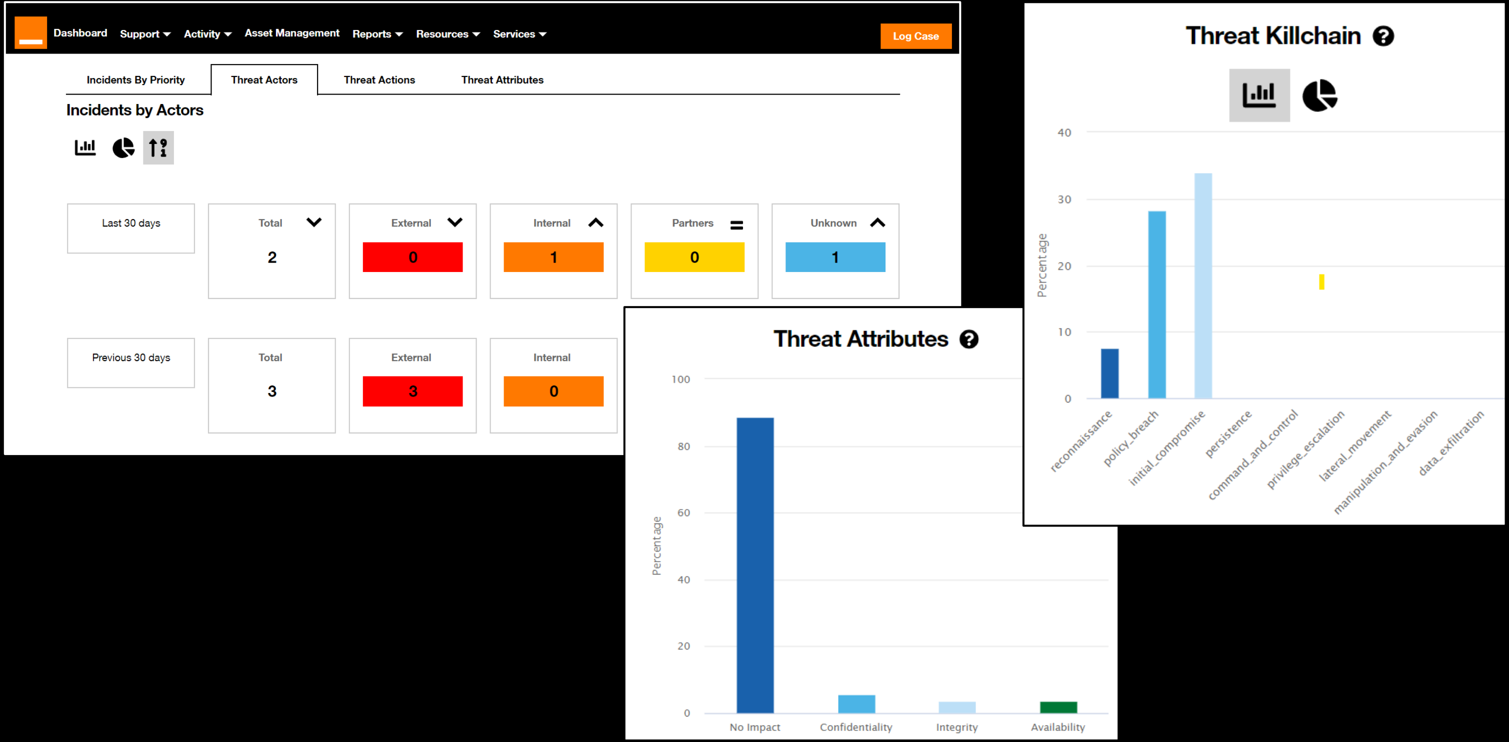
The most targeted resource among our clients are Endpoints (~30%) and servers.

FP type



~89% of False Positives are caused by legitimate user activity.

Delivering your Strategic Intelligence through incident classification



Incidents by Actors

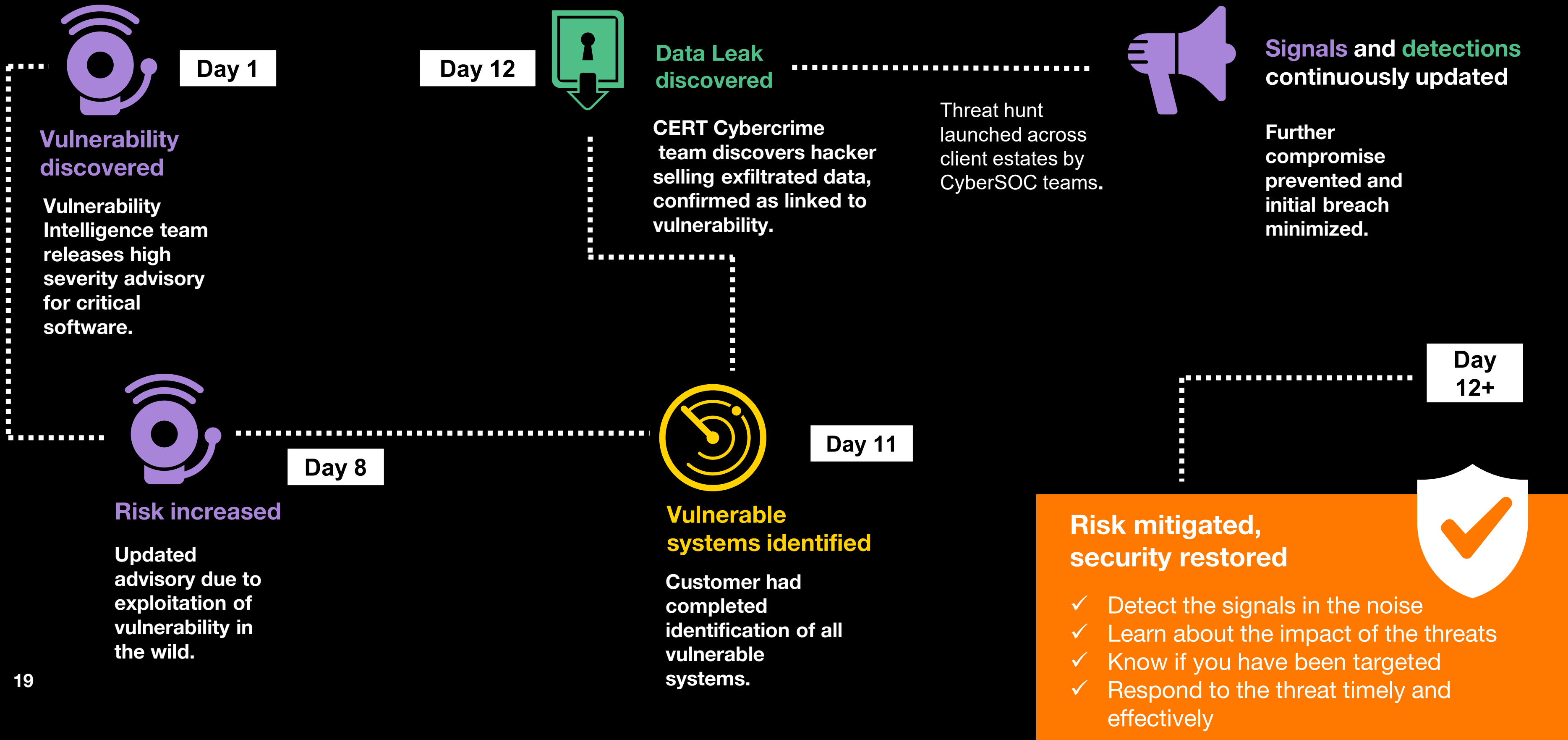
	Total	External	Internal	Partners	Unknown
Last 30 days	2	0	1	0	1
Previous 30 days	3	3	0		

Orange Restricted

Tactical Intelligence

The value-add of a co-ordinated ecosystem

Major software vulnerability



Day 1

Vulnerability discovered

Vulnerability Intelligence team releases high severity advisory for critical software.

Day 8

Risk increased

Updated advisory due to exploitation of vulnerability in the wild.

Day 11

Vulnerable systems identified

Customer had completed identification of all vulnerable systems.

Day 12

Data Leak discovered

CERT Cybercrime team discovers hacker selling exfiltrated data, confirmed as linked to vulnerability.

Threat hunt launched across client estates by CyberSOC teams.

Signals and detections continuously updated

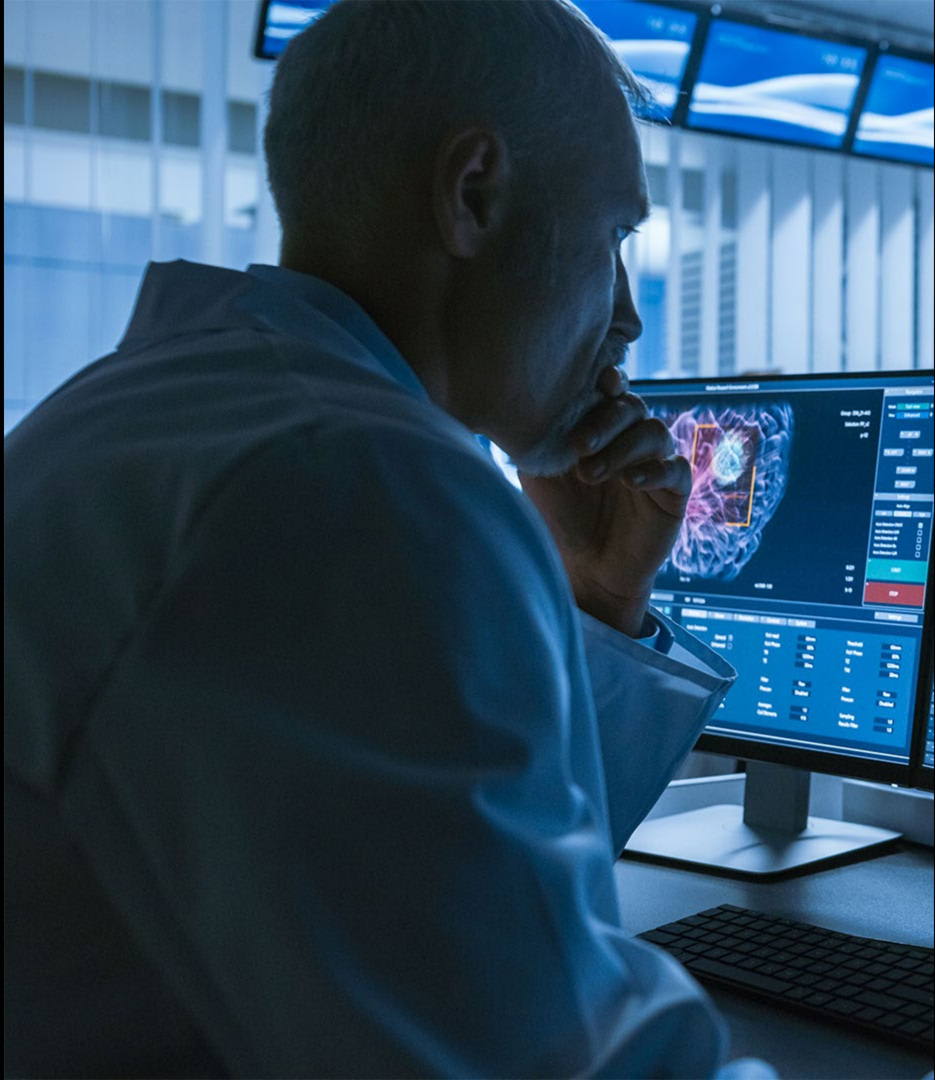
Further compromise prevented and initial breach minimized.

Day 12+

Risk mitigated, security restored

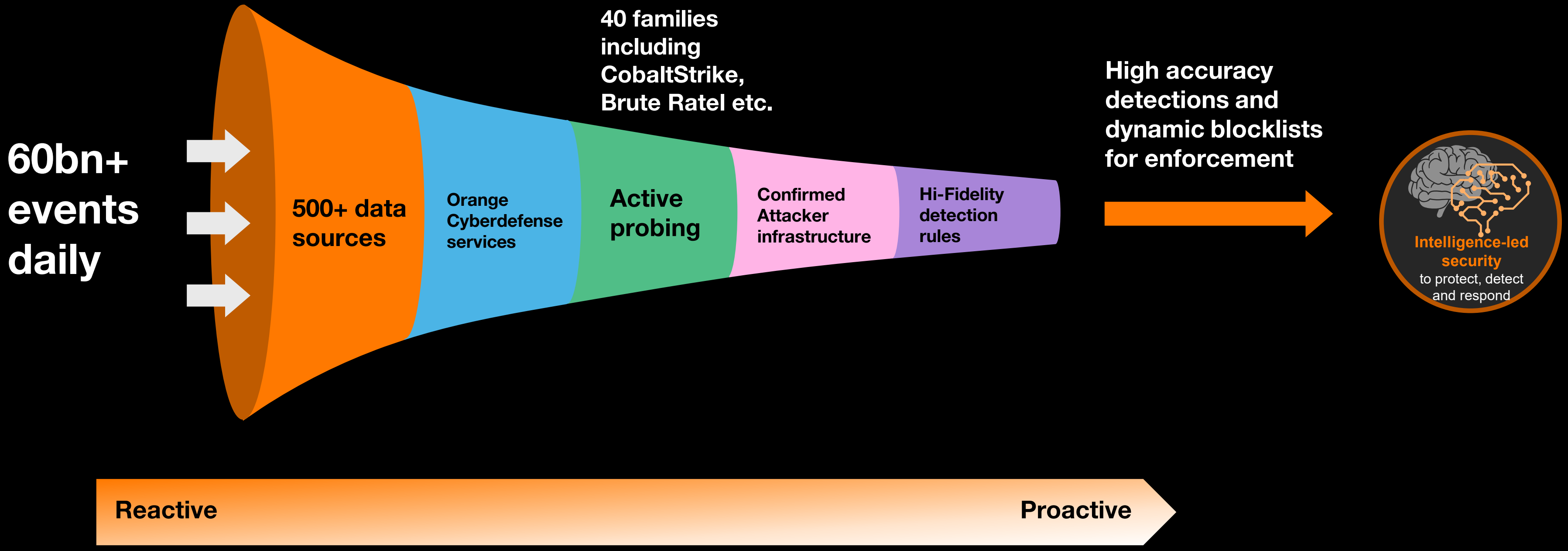
- ✓ Detect the signals in the noise
- ✓ Learn about the impact of the threats
- ✓ Know if you have been targeted
- ✓ Respond to the threat timely and effectively

Technical Intelligence



Orange Cyberdefense advanced intelligence

It is about quality, not just quantity…



60bn+ events daily

500+ data sources

Orange Cyberdefense services

Active probing

40 families including CobaltStrike, Brute Ratel etc.

Confirmed Attacker infrastructure

Hi-Fidelity detection rules

High accuracy detections and dynamic blocklists for enforcement

Intelligence-led security to protect, detect and respond

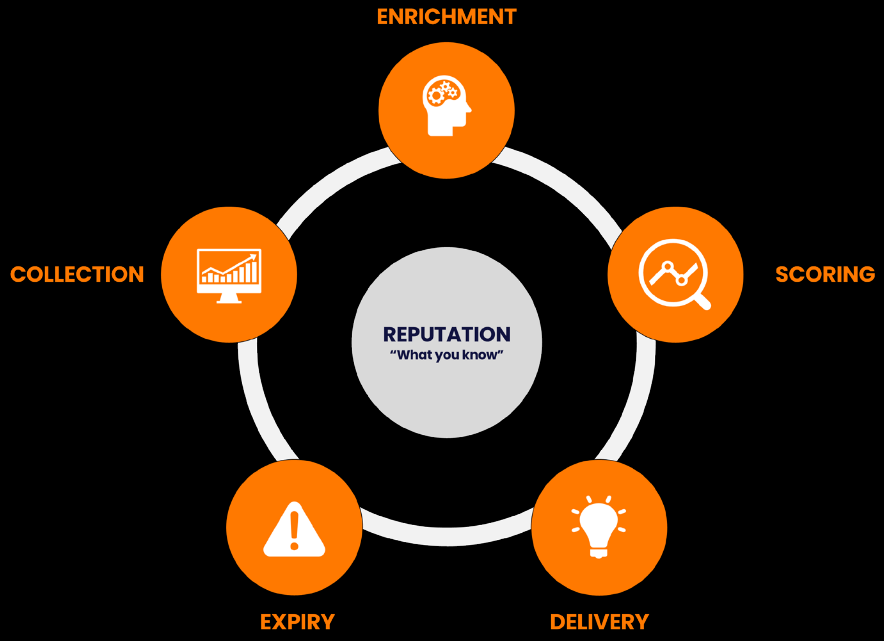
Reactive

Proactive

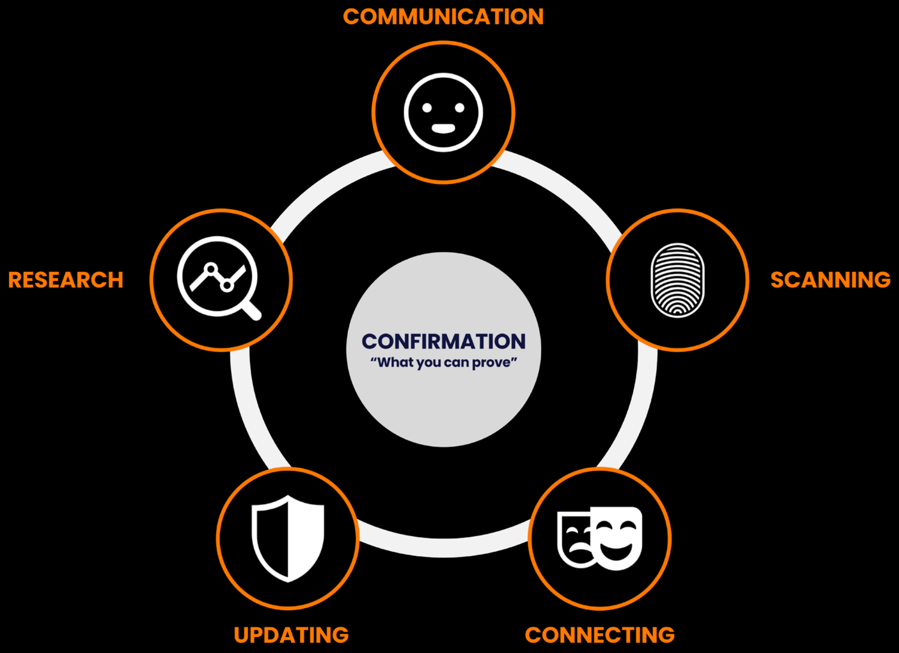
Movie reference!

What's so different?

How can any Threat Intelligence IOCs be 100%?



VS



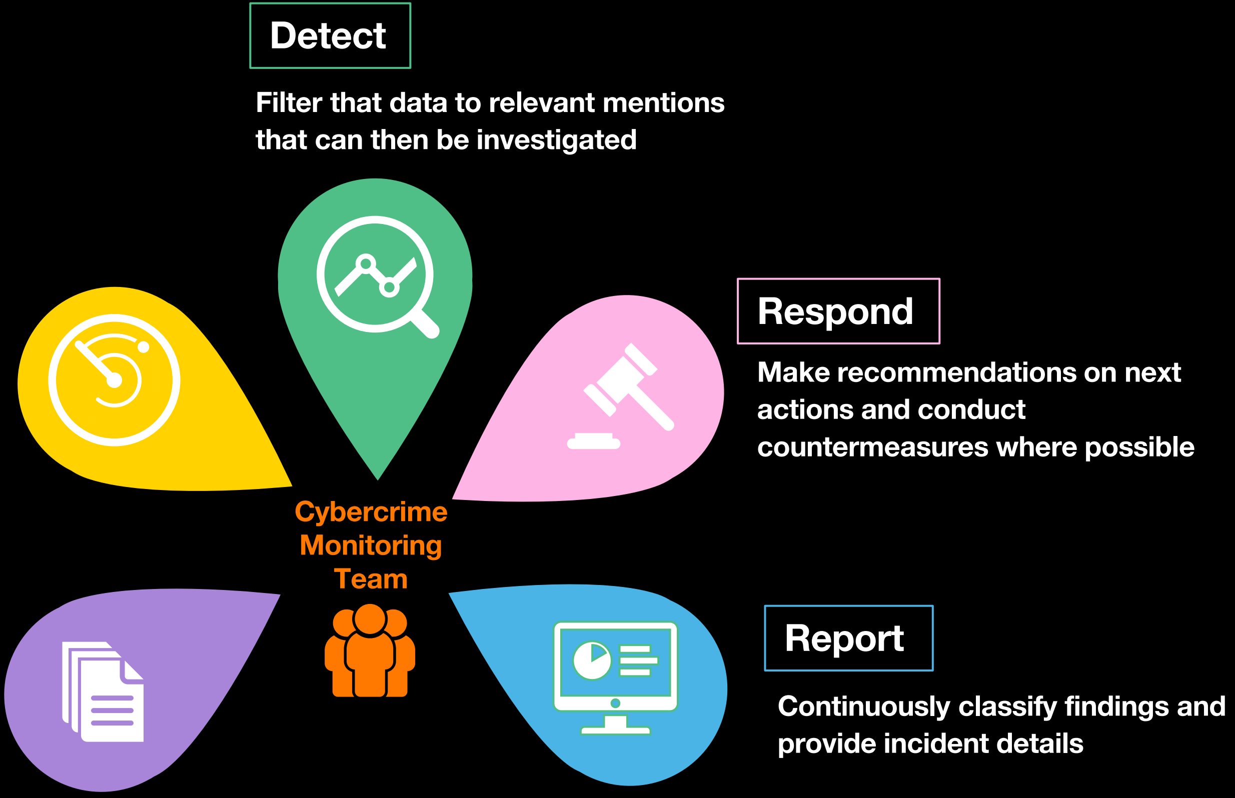
Operational Intelligence

Summary

Stopping advanced attacks is near impossible

- But it can be done by strong MDR players like ourselves
- It is no longer just email, digital transformation increases the scope of attacks
- Education is key

Delivering Operational Intelligence to empower our teams to find hidden threats



Detect

Filter that data to relevant mentions that can then be investigated

Search

Open, Deep and Dark web sources to find mentions of assets in line with goals

Respond

Make recommendations on next actions and conduct countermeasures where possible

Cybercrime Monitoring Team

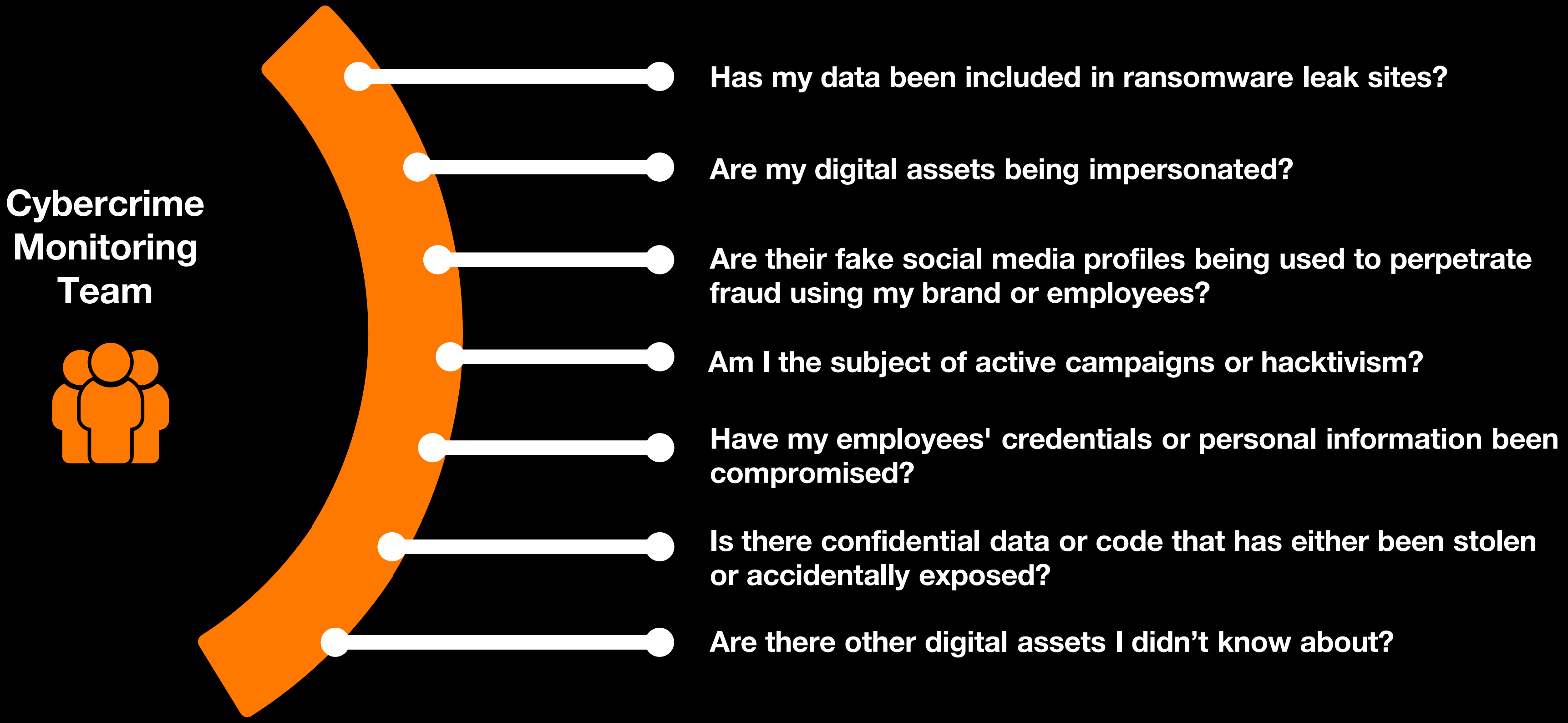
Collect

Asset data and intelligence goals

Report

Continuously classify findings and provide incident details

Delivering Operational Intelligence to find those unknown digital risks



Cybercrime Monitoring Team

- Has my data been included in ransomware leak sites?
- Are my digital assets being impersonated?
- Are their fake social media profiles being used to perpetrate fraud using my brand or employees?
- Am I the subject of active campaigns or hacktivism?
- Have my employees' credentials or personal information been compromised?
- Is there confidential data or code that has either been stolen or accidentally exposed?
- Are there other digital assets I didn’t know about?

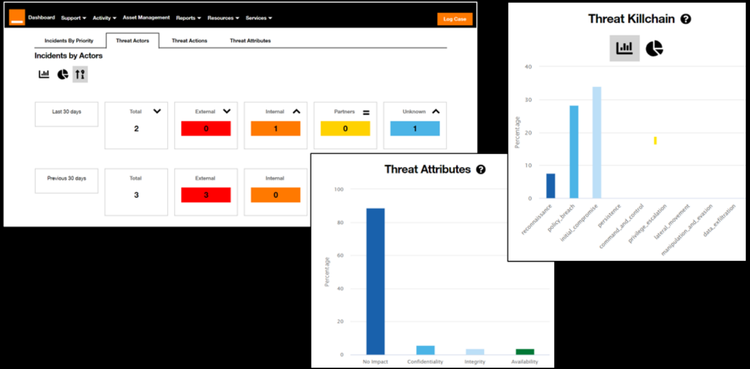
3 things…

- Strategy
- Intelligence
- People

3 things…

- Strategy
- Intelligence
- People

It was the people who made the difference.

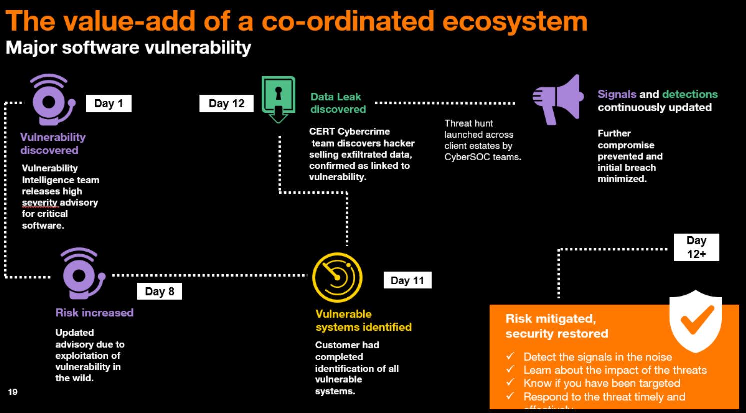


Dashboard Support ▾ Activity ▾ Asset Management Reports ▾ Resources ▾ Services ▾ Log Case

Incidents By Priority | Threat Actors | Threat Actions | Threat Attributes

Incidents by Actors

	Total	External	Internal	Partners	Unknown
Last 30 days	2	0	1	0	1
Previous 30 days	3	3	0		



The value-add of a co-ordinated ecosystem

Major software vulnerability

Day 1 — **Vulnerability discovered**

Vulnerability Intelligence team releases high severity advisory for critical software.

Day 8 — **Risk increased**

Updated advisory due to exploitation of vulnerability in the wild.

Day 11 — **Vulnerable systems identified**

Customer had completed identification of all vulnerable systems.

Day 12 — **Data Leak discovered**

CERT Cybercrime team discovers hacker selling exfiltrated data, confirmed as linked to vulnerability.

Threat hunt launched across client estates by CyberSOC teams.

Signals and detections continuously updated

Further compromise prevented and initial breach minimized.

Day 12+

Risk mitigated, security restored

✓ Detect the signals in the noise
✓ Learn about the impact of the threats
✓ Know if you have been targeted
✓ Respond to the threat timely and

19

Thanks

orange™ Cyberdefense

What am I going to talk about?

1

Recap:

What did we do today?

2

Here and now:

What do we do with that?

3

The future:

Where can we take it next?

What am I going to talk about?

1

Recap:

What did we do today?

2

Here and now:

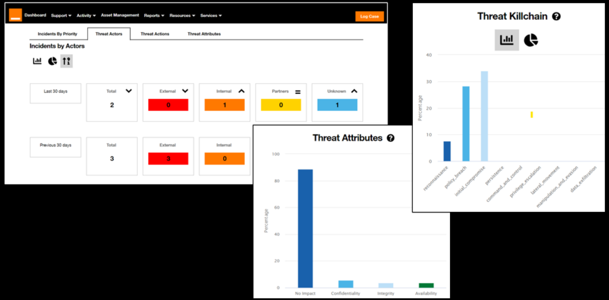
What do we do with that?

3

The future:

Where can we take it next?

Security Incidentology



Incidents by Actors

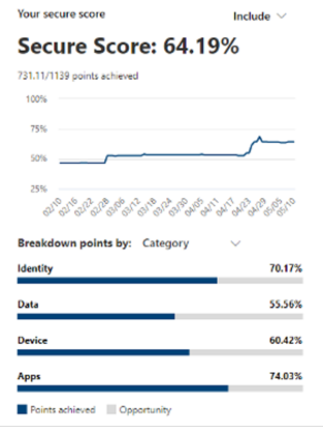
Last 30 days	Total	External	Internal	Partners	Unknown
	2	0	1	0	1

Previous 30 days	Total	External	Internal
	3	3	0

Organizational risk

Benchmarked

Security Posture Analysis


Your secure score

Include

Secure Score: 64.19%

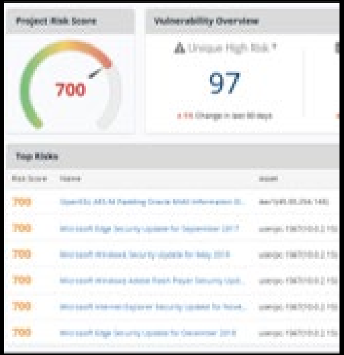
731.11/1139 points achieved

Breakdown points by: Category

Identity	70.17%
Data	55.56%
Device	60.42%
Apps	74.03%

■ Points achieved ▨ Opportunity

Vulnerability Risk


Project Risk Score

Vulnerability Overview

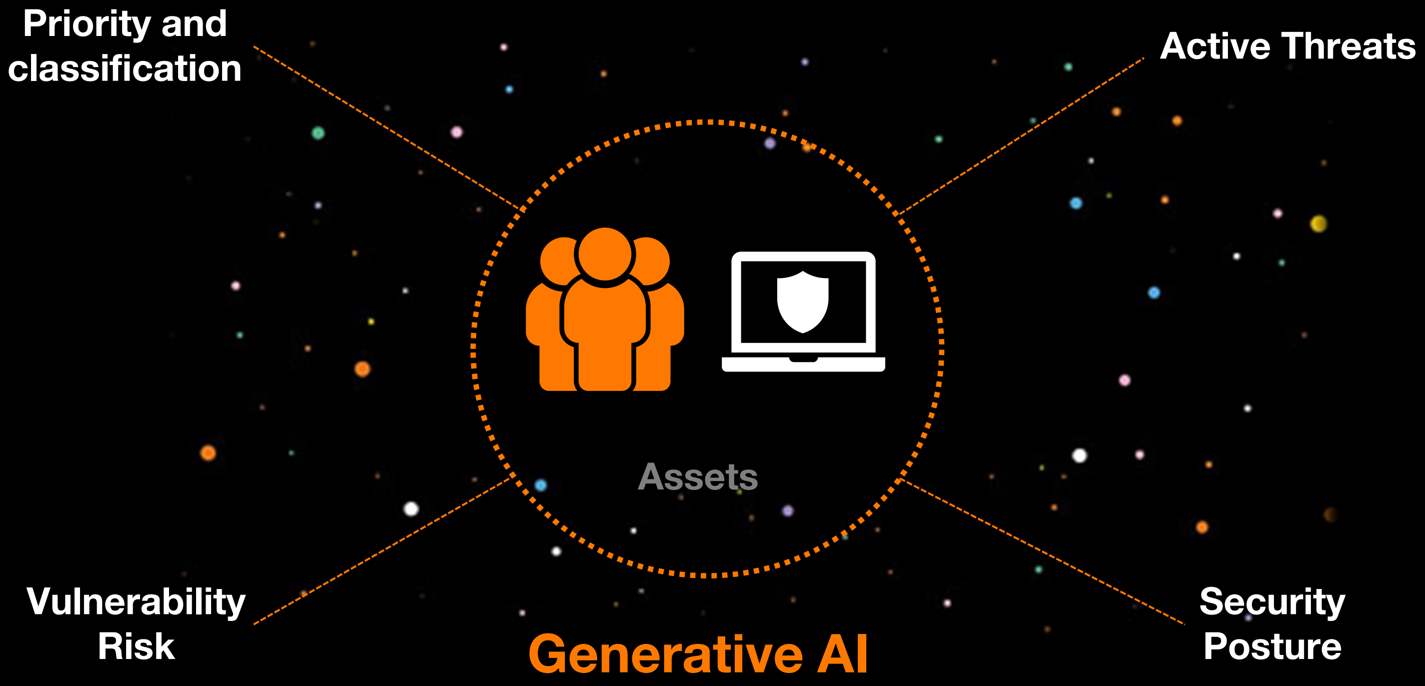
Unique High Risk

97

[illegible] Change in last 90 days

Top Risks

Risk Score	Name	Asset
700	OpenSSL AES-NI Padding Oracle MAC Information D...	[illegible]
700	Microsoft Edge Security Update for September 2017	[illegible]
700	Microsoft Windows Security Update for May 2018	[illegible]
700	Microsoft Windows Adobe Flash Player Security Upd...	[illegible]
700	Microsoft Internet Explorer Security Update for Nove...	[illegible]
700	Microsoft Edge Security Update for December 2018	[illegible]


Priority and classification
Active Threats
Assets
Vulnerability Risk
Security Posture
Generative AI

Key takeaways

We are here to help you accelerate your strategy

By providing a growing level of interconnected intelligence

And through access to one of the largest collections of security experts in the world

Thanks

orange™ Cyberdefense