Orange
Cyberdefense Live 2023

Building Intelligence-Led Managed Services

Knowing you better than you know yourself

Grant Paling, Product Manager

Who is this English guy and who let him in the country?

Grant Paling

- 16 years in Cyber Security in various roles, specializing the last 7 years in Managed Security Services
- Former drama student and master of voices
- Sports fanatic, triathlete and Liverpool FC fan

Product Management

- Managed Detection and Response strategy, packaging and service development
- Global Customer Portal product strategy
- Digital Risk Management product manager

Zwift tag:
GRANT PALING [SDW]

Marginal gains


HEMA
JUMBO VISMA
Better.
HEMA
Bianchi
AGU
UCI WORLD TEAM
JUMBO
VISMA


UAE
Emirates
CELJE

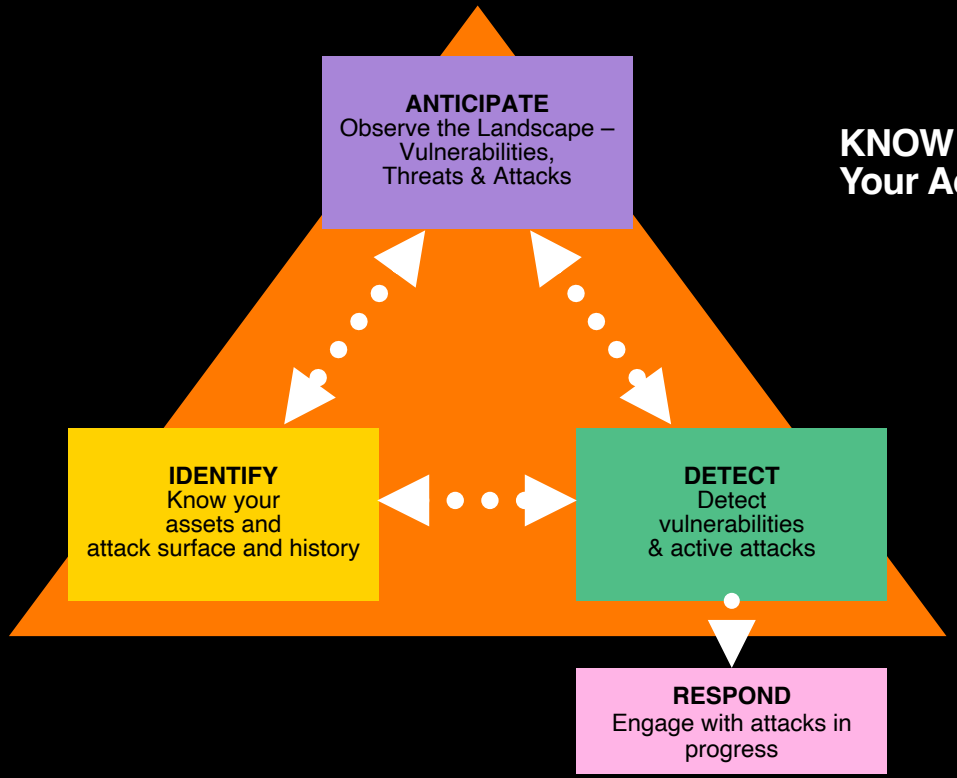
“You can’t win the tour in one day but you can lose it.”

Agenda

- What is intelligence-led security?
- Intelligence-led security in action
- The future of intelligence-led security

What is Intelligence-led Security?

Intelligence Led security requires two perspectives



KNOW Your Adversary

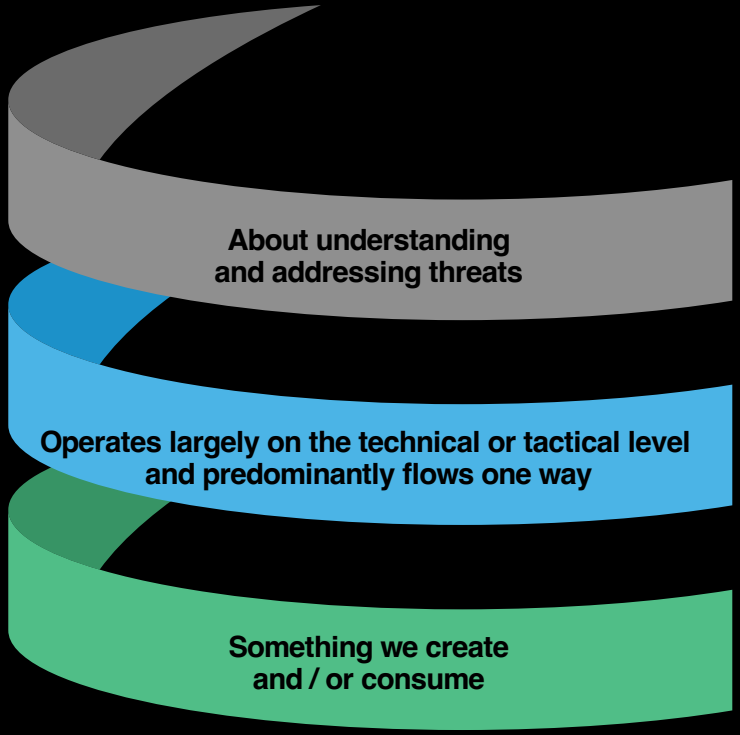
KNOW Yourself

So are we talking about Cyber Threat Intelligence here?

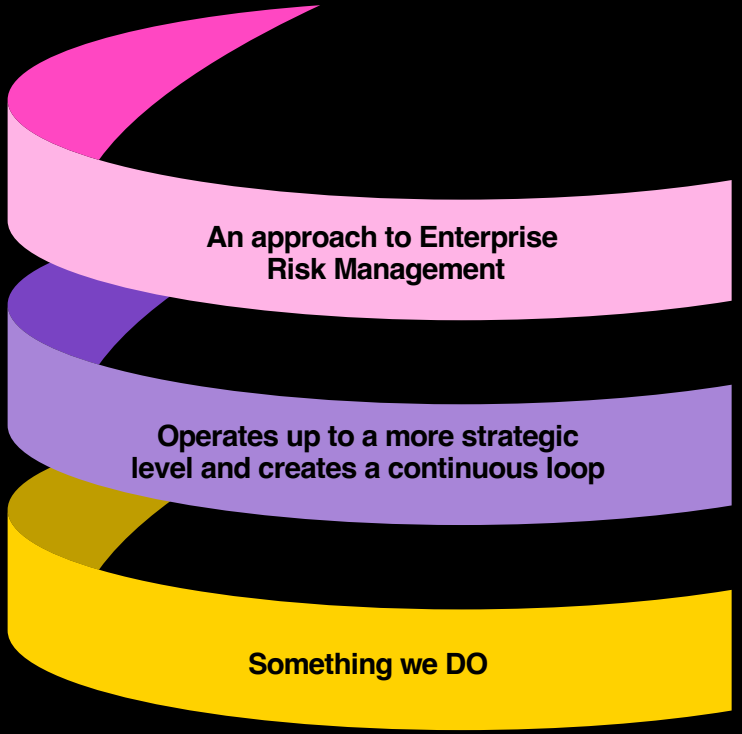
YES!

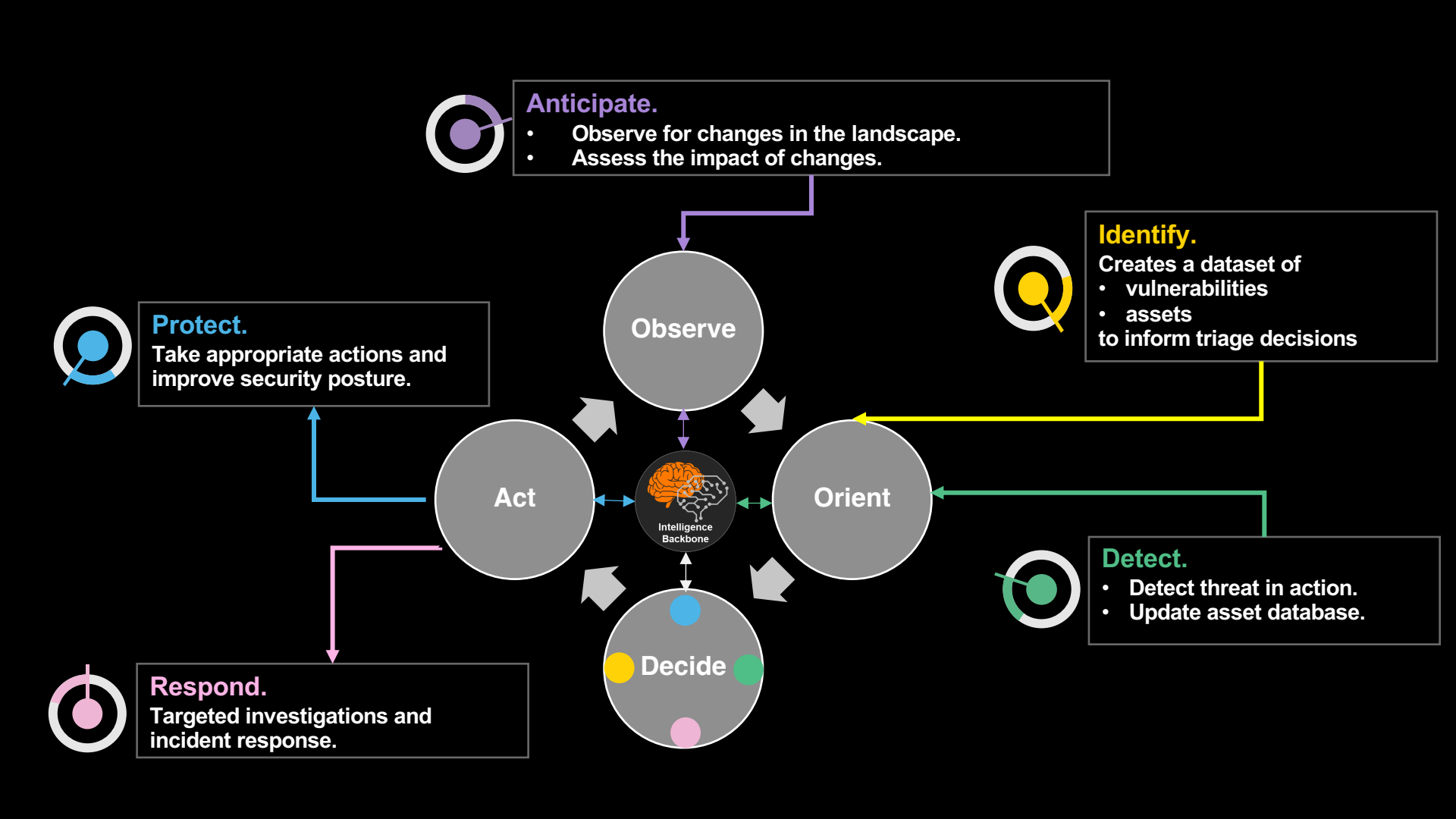
…but NO!

Cyber Threat Intelligence



Versus Intelligence-Led




Anticipate.
• Observe for changes in the landscape.
• Assess the impact of changes.
Identify.
Creates a dataset of
• vulnerabilities
• assets
to inform triage decisions
Protect.
Take appropriate actions and improve security posture.
Observe
Act
Intelligence Backbone
Orient
Decide
Detect.
• Detect threat in action.
• Update asset database.
Respond.
Targeted investigations and incident response.

Intelligence-led Security
In Action


LOG4J

The value-add of intelligence-led security

A timeline of defense for the Log4j vulnerability

Day 1

Vulnerability discovered

Vulnerability Intelligence team and World Watch team releases an advisory.

Scanning set up

Vulnerability scans run for Managed Vulnerability Scanning customers.

Day 3

Vulnerable systems identified

Intelligence team continues to update around affected technologies and exploitation techniques.

Day 4

Rapid analysis

Potential attack vectors analyzed for quick detection.

Threat hunt launched across client estates.

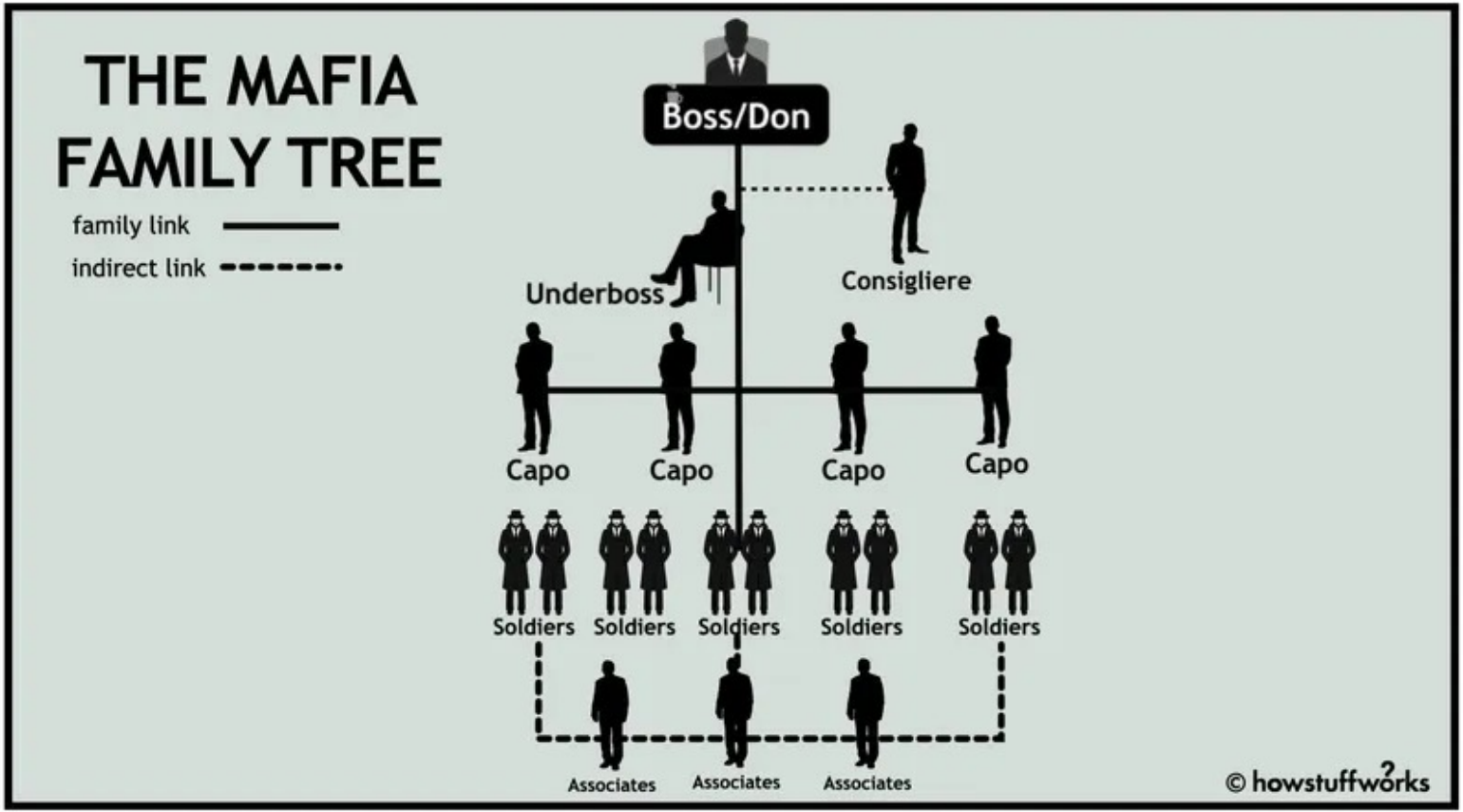
Signals and detections continuously updated

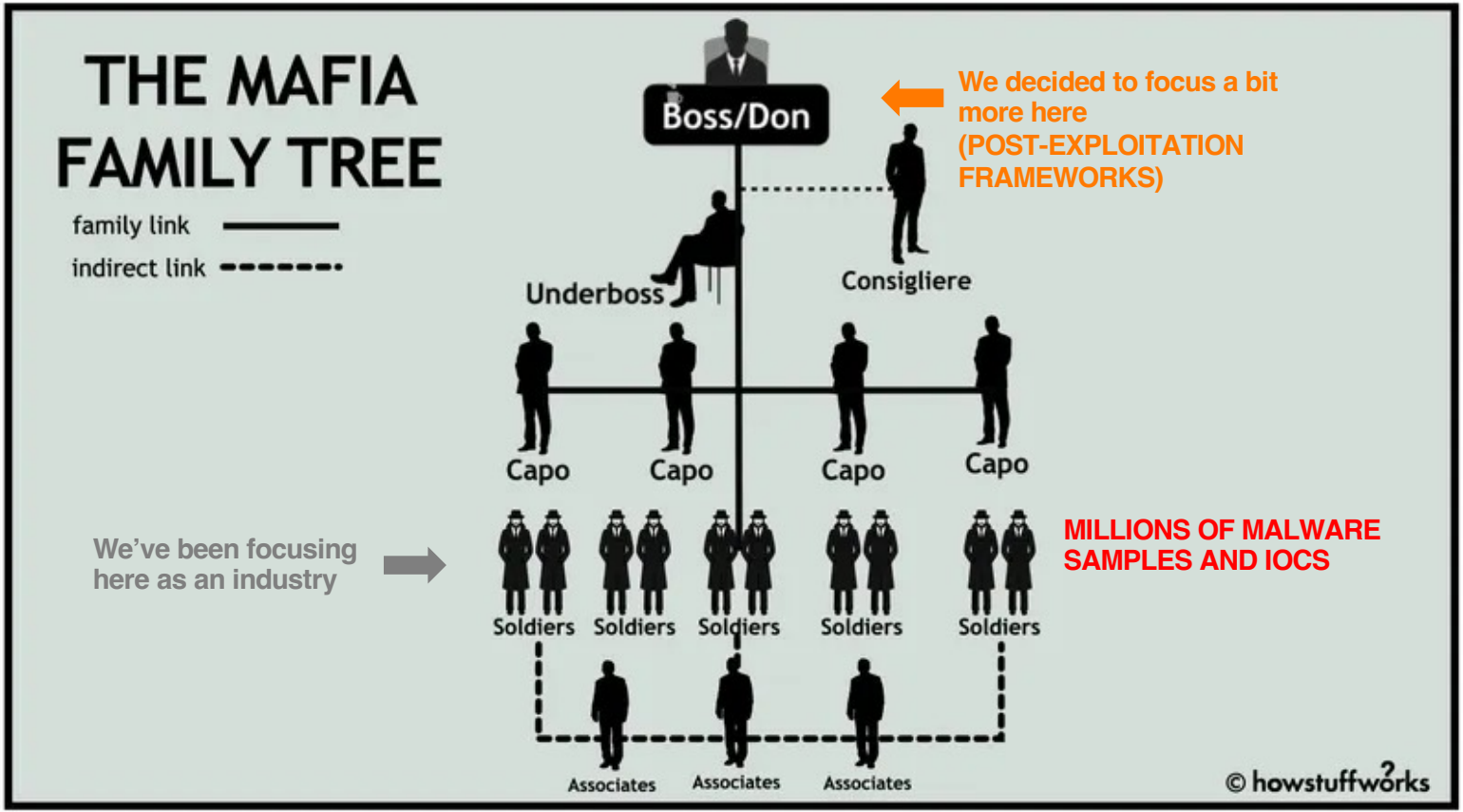
World Watch Signal continuously updated, automatic detections validated and updated

Day 7+

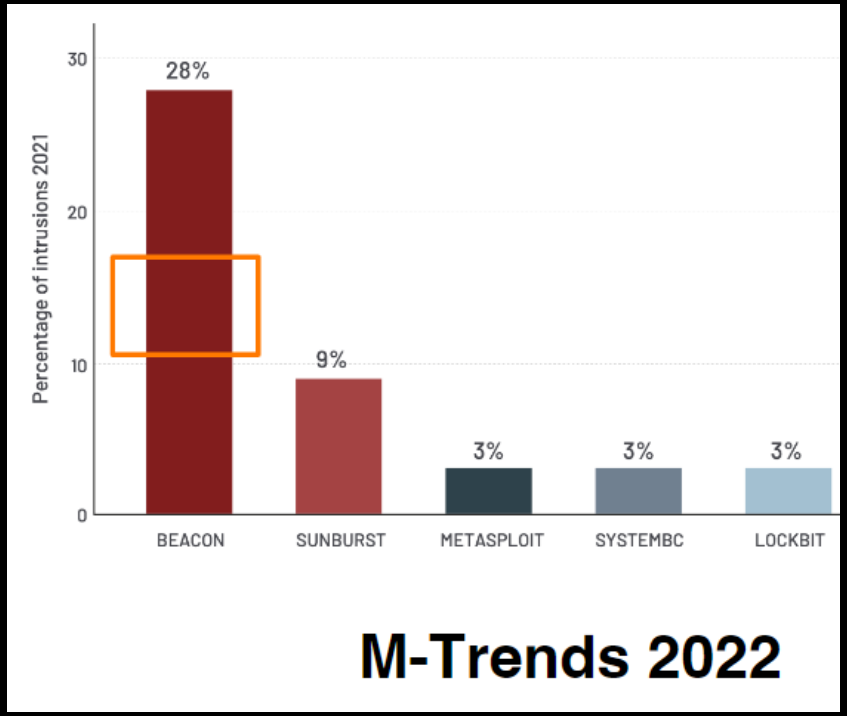
Risk mitigated, security restored

- ✓ 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


THE MAFIA FAMILY TREE
family link
indirect link
Boss/Don
Underboss
Consigliere
Capo
Capo
Capo
Capo
Soldiers
Soldiers
Soldiers
Soldiers
Soldiers
Associates
Associates
Associates
© howstuffworks


THE MAFIA FAMILY TREE
family link
indirect link
Boss/Don
We decided to focus a bit more here (POST-EXPLOITATION FRAMEWORKS)
Underboss
Consigliere
Capo
Capo
Capo
Capo
We've been focusing here as an industry
Soldiers
Soldiers
Soldiers
Soldiers
Soldiers
MILLIONS OF MALWARE SAMPLES AND IOCS
Associates
Associates
Associates
© howstuffworks

Going after the “boss of all bosses”

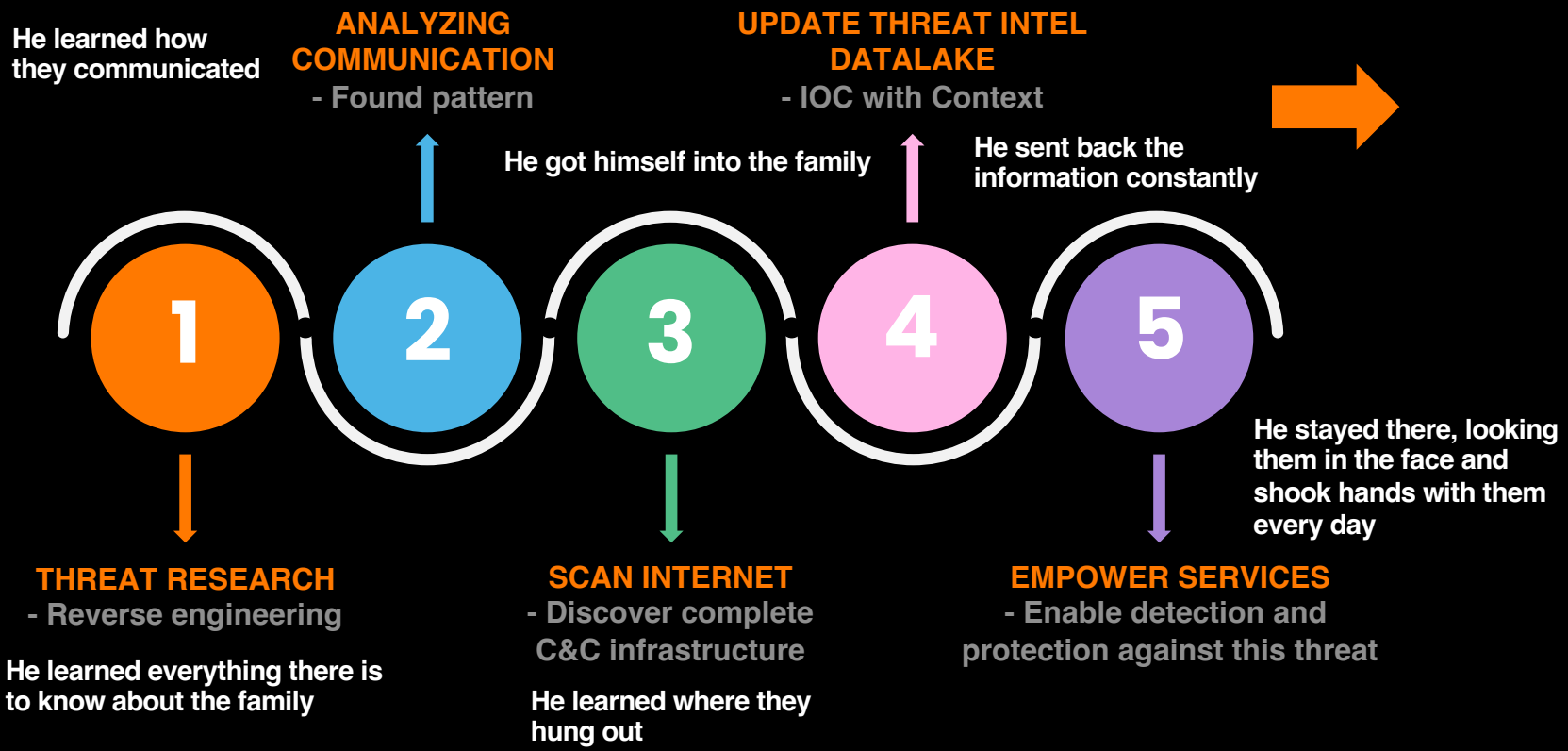


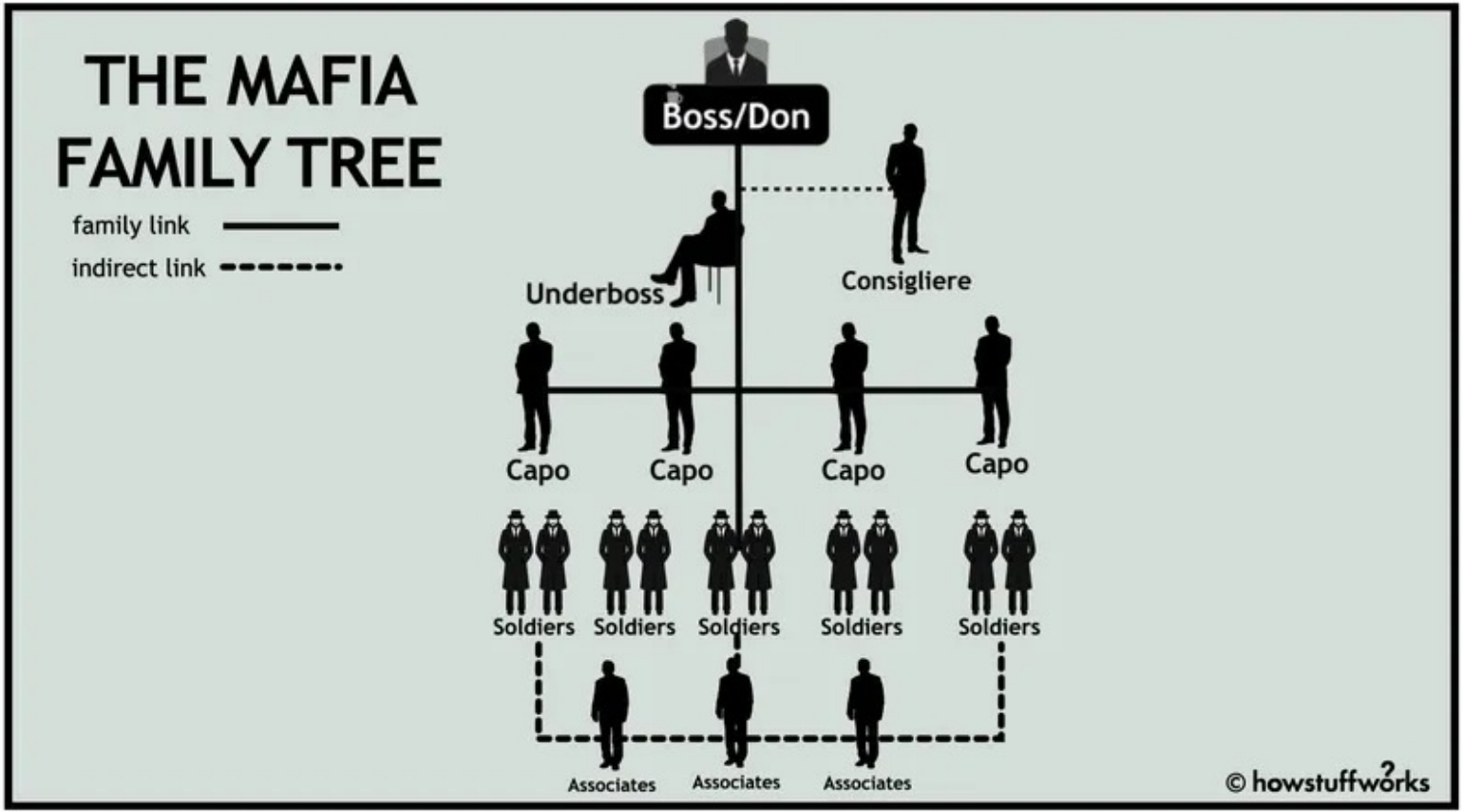
What did Donnie do?

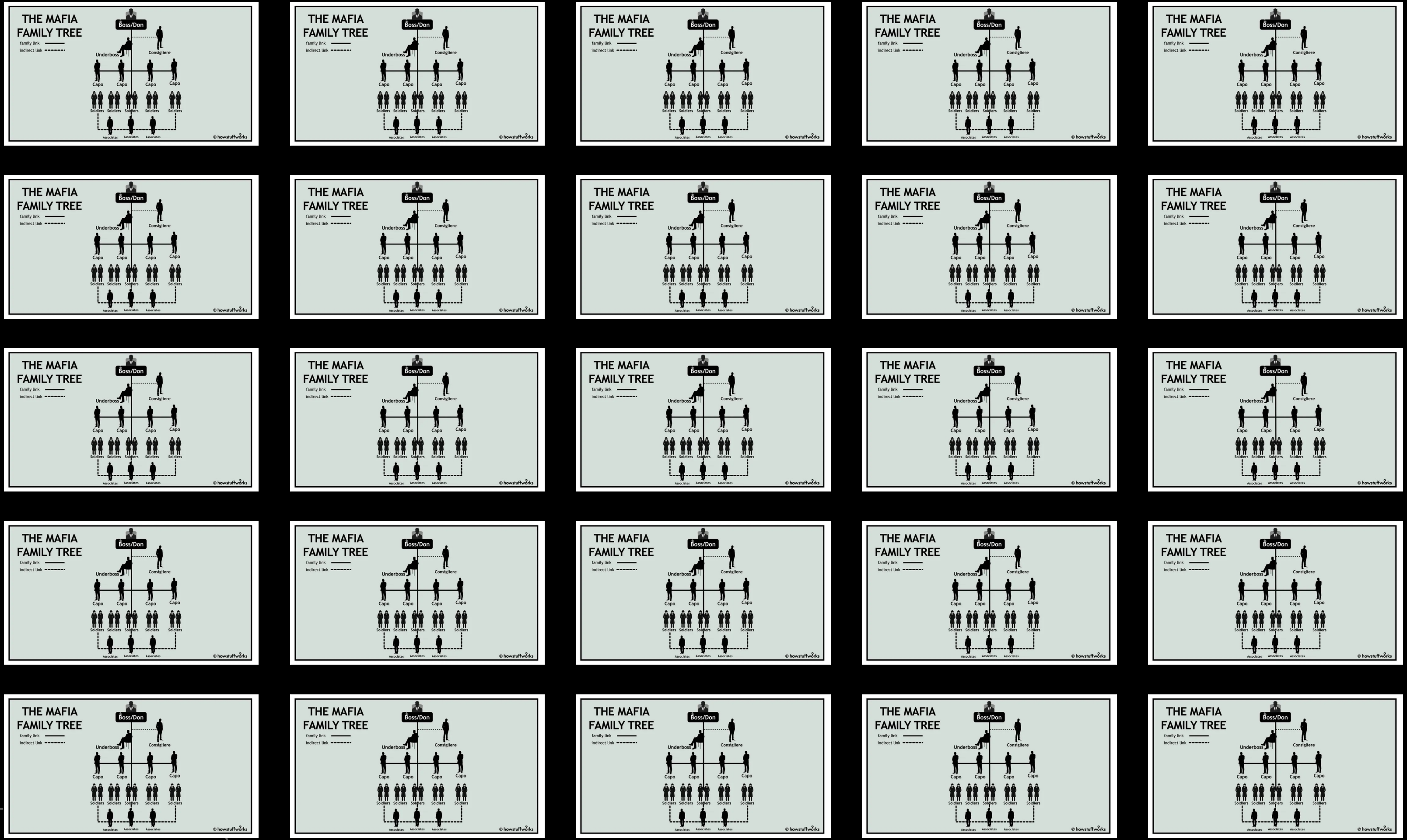
- He learned everything there is to know about the family
- He learned where they hung out
- He learned how they communicated
- He got himself into the family
- He stayed there, looking them in the face and shook hands with them every day
- He sent back the information constantly

Here's the technical version:

Using internet wide scan data to find threat actor infrastructure

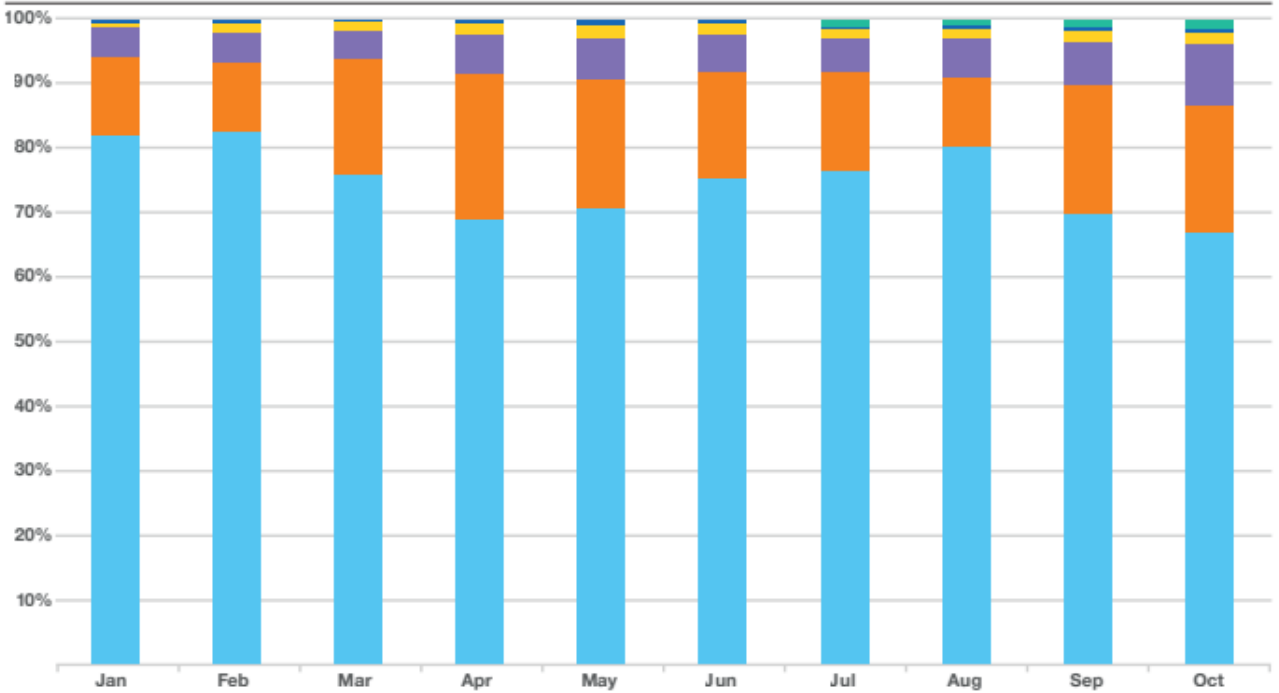



THE MAFIA FAMILY TREE
family link
indirect link
Boss/Don
Underboss
Consigliere
Capo
Capo
Capo
Capo
Soldiers
Soldiers
Soldiers
Soldiers
Soldiers
Associates
Associates
Associates
© howstuffworks


THE MAFIA
FAMILY TREE
family link
indirect link
Boss/Don
Consigliere
Underboss
Capo
Capo
Capo
Capo
Soldiers
Soldiers
Soldiers
Soldiers
Soldiers
Associates
Associates
Associates
© howstuffworks

C&C tools usage

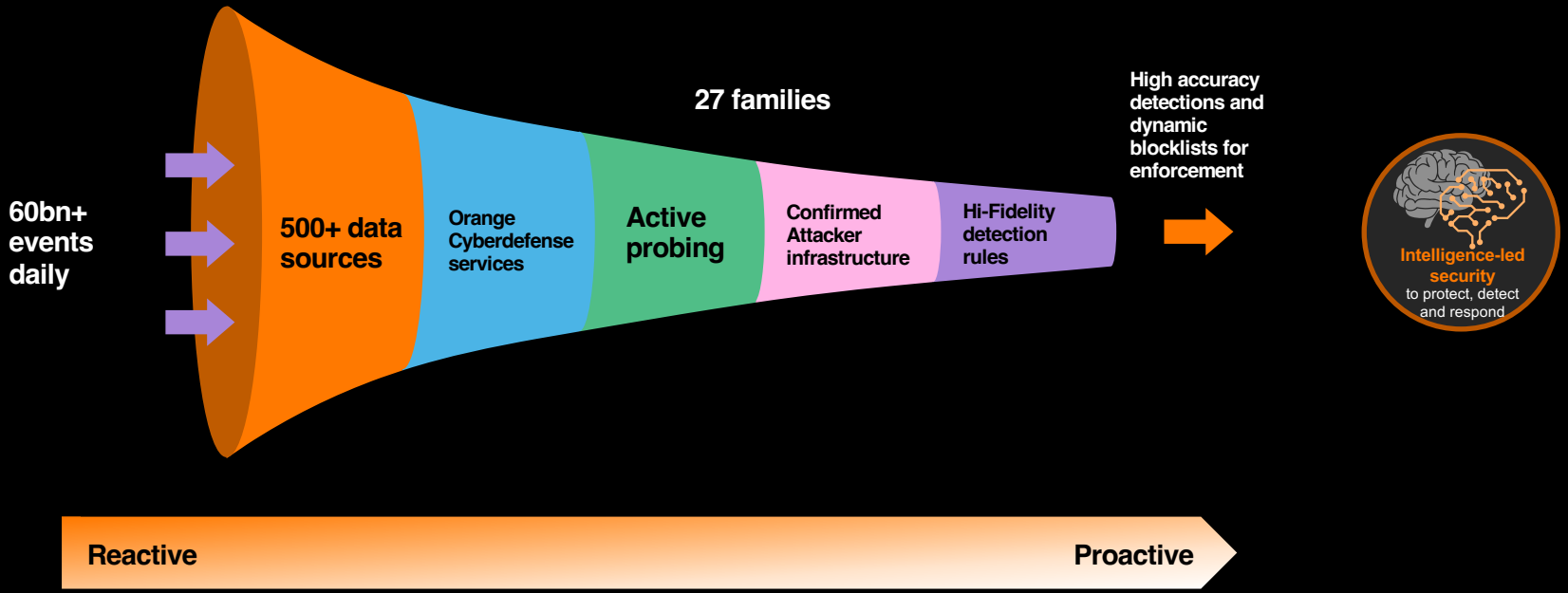
Distribution across C&C Framework Servers detected over time



Source: Orange Cyberdefense Security Navigator 2023

Orange Cyberdefense advanced intelligence

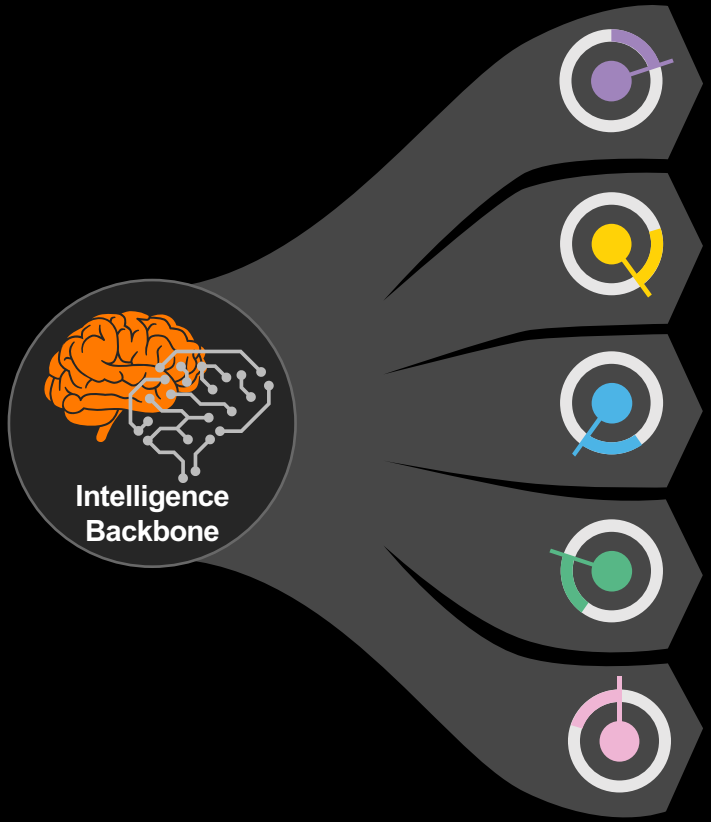
It is about quality, not just quantity…



The Future of Intelligence-led Security

Operational & tactical intelligence-led security

Adopt timely preventive measures, improve threat detection and remediation



Anticipate
Threats you have to face

- World Watch Threat Advisory
- Managed Cybercrime Monitoring

Identify
Risks and weaknesses before hackers do so

- Assessment and Advisory Services
- Managed Vulnerability Intelligence
- Ethical Hacking

Protect
Maintain solutions at the highest standard of security

- Managed Security Services

Detect
High-performance detection

- Managed Threat Detection [xdr]
- Managed Threat Detection [network]
- Managed Threat Detection [log]
- Managed Cybercrime Monitoring

Respond
Targeted investigations and incident response

- Incident Response
- Incident Response Consulting
- Compromise Assessment
- Digital Forensics

Embedding intelligence-led security

Across the threat lifecycle

Managed Workspace Protection

Managed Threat Detection

Managed Cybercrime Monitoring

World Watch

Anticipate

The latest threats, vulnerabilities and breaches to be agile in an ever-changing security landscape

Protect

Utilizing Microsoft 365 Defender to implement attack surface reduction and to continuously improve your secure score

Microsoft Defender and Microsoft Sentinel

Detect

And contain threats that circumvent your protection layer 24x7 and continuously evolve detection capabilities

Microsoft Defender

Managed Cloud Security

Managed Vulnerability Intelligence

Vulnerabilities and incorporate a risk-based approach

Identify

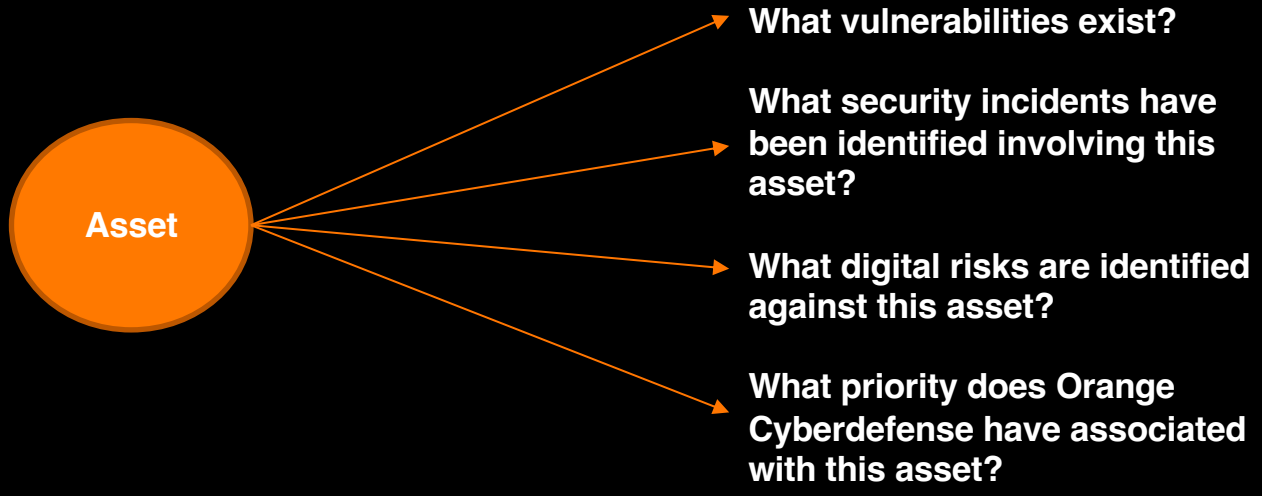
Misconfigurations and potential threats within your public cloud environments

Incident Response

Respond

With confidence, that you have an established and highly skilled team helping you prepare and handle major security incidents

Moving from incident-centric to asset-centric



And from asset to actor – using the “outside-in” view

What vulnerabilities exist?

What security incidents have been identified involving this asset?

What digital risks are identified against this asset?

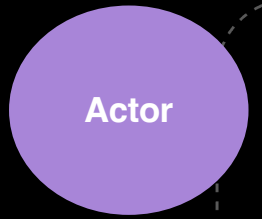
What priority does Orange Cyberdefense have associated with this asset?

How likely are they to exploit them?

How will they do it?

Has the asset been threatened or compromised already?

For whom is it a high value target?



Orange Cyberdefense