Cyberdefense

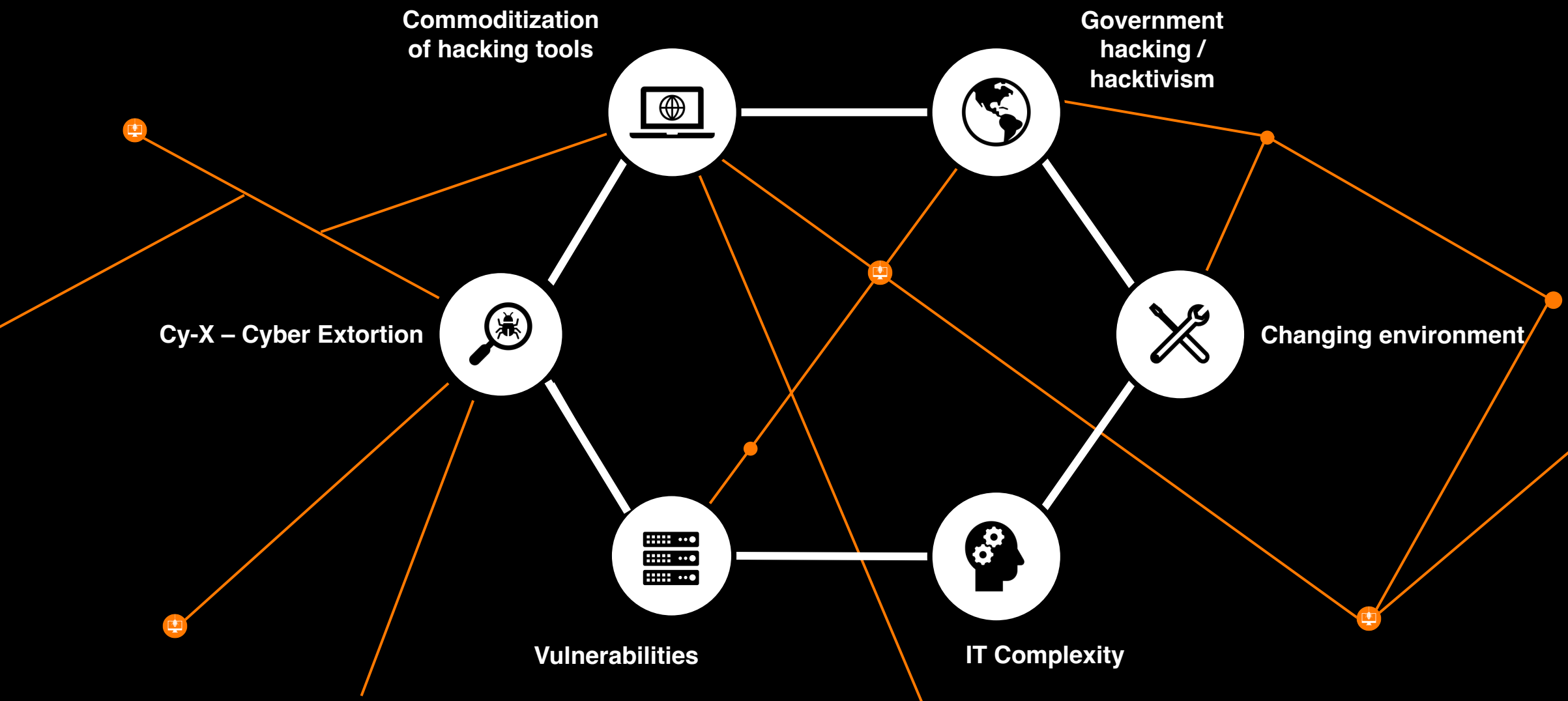
How to detect, prevent & respond

to ransomware attacks and cyber extortion in the current threat landscape

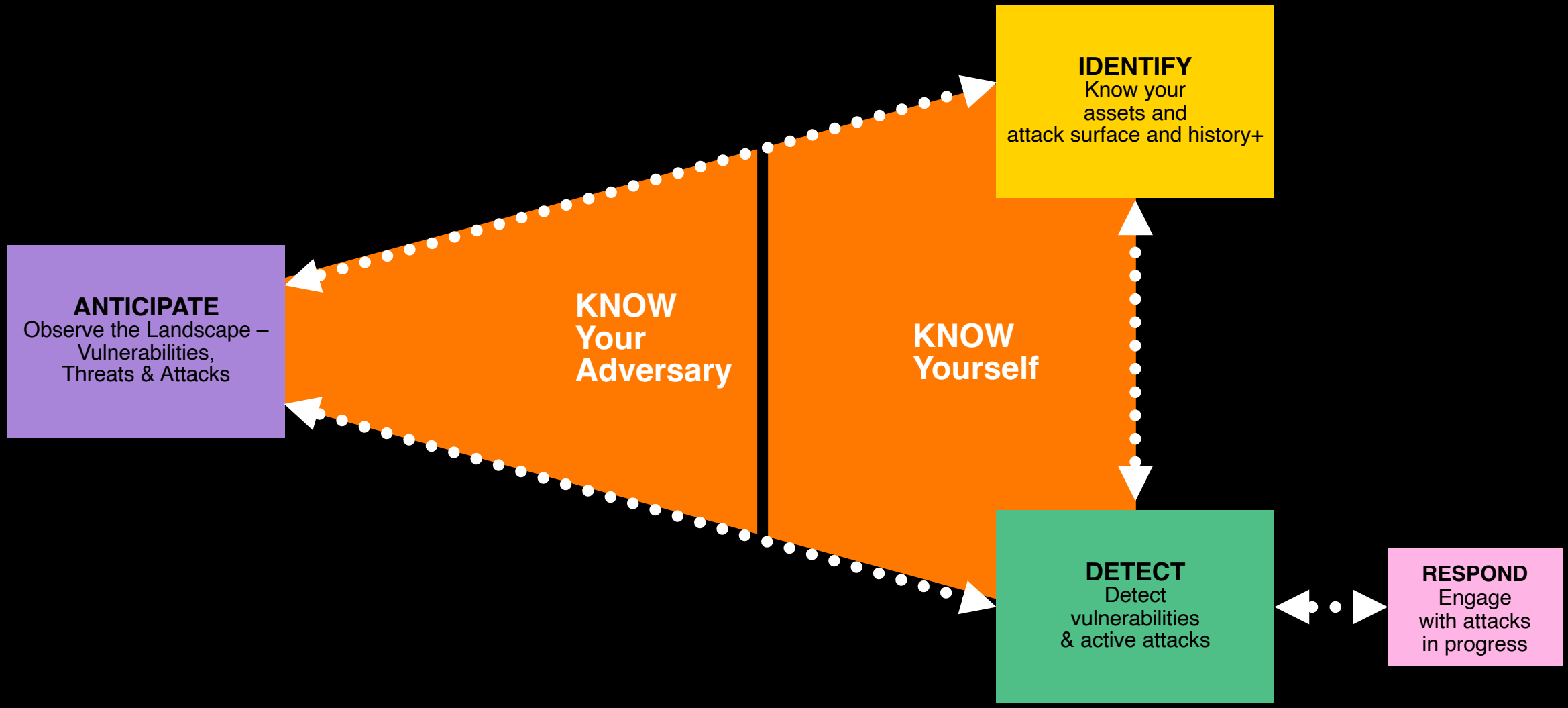

Intelligence-led security is the
compass that guides you

Navigate through the threat landscape

More diversity meaning more complexity



Intelligence Led security requires two perspectives



Challenge

Sophisticated threats, complex solutions, limited resources and expertise.

How to…

… find signals in the noise & stay ahead of threats?

… understanding your actual risk profile?

… focus on real priorities?

… be agile and adaptive?


Our intelligence,
your advantage.

To better navigate, read the changing currents

Our knowledge of the threat

Our research

- Security Research Center
- In house R&D
- Security Navigator
- Epidemiology Labs Reports

Our reach

- Cyber extortion groups
- Cybercriminal underground
- Emerging vulnerabilities
- Attacker infrastructure probing

Our people

- 250+ experts dedicated to R&D and threat research
- 20% of pentesters' time is dedicated to research
- 120+ in our international CERT continuously synthesizing threat intelligence

Our customers

- Quantity: data collected during client assignments
- Quality: diversity of our clients allows us to broaden the richness of our data

…the Intelligence-led approach drives action

Agile, adaptive security to your business in the face of the threat landscape

External

- Assessments
- Vertical specifics
- Business priorities
- Collaboration with law enforcement
- Research & Reports
- Feeds
- OSINT

Internal

Intelligence from our operations:

- MDR services
- Security Research Center
- Vulnerability Research
- CERT intelligence
- CSIRT cases
- In-house R&D

3,000 experts
to qualify, advise, operate, detect and respond

Strategic

- Long-term trends and systemic changes
- Drive security strategy and choices

Tactical

- Real-time intelligence
- Parry threats and mitigate vulnerabilities

Operational & Technical

- Preventive measures
- Precise detection
- Targeted remediation

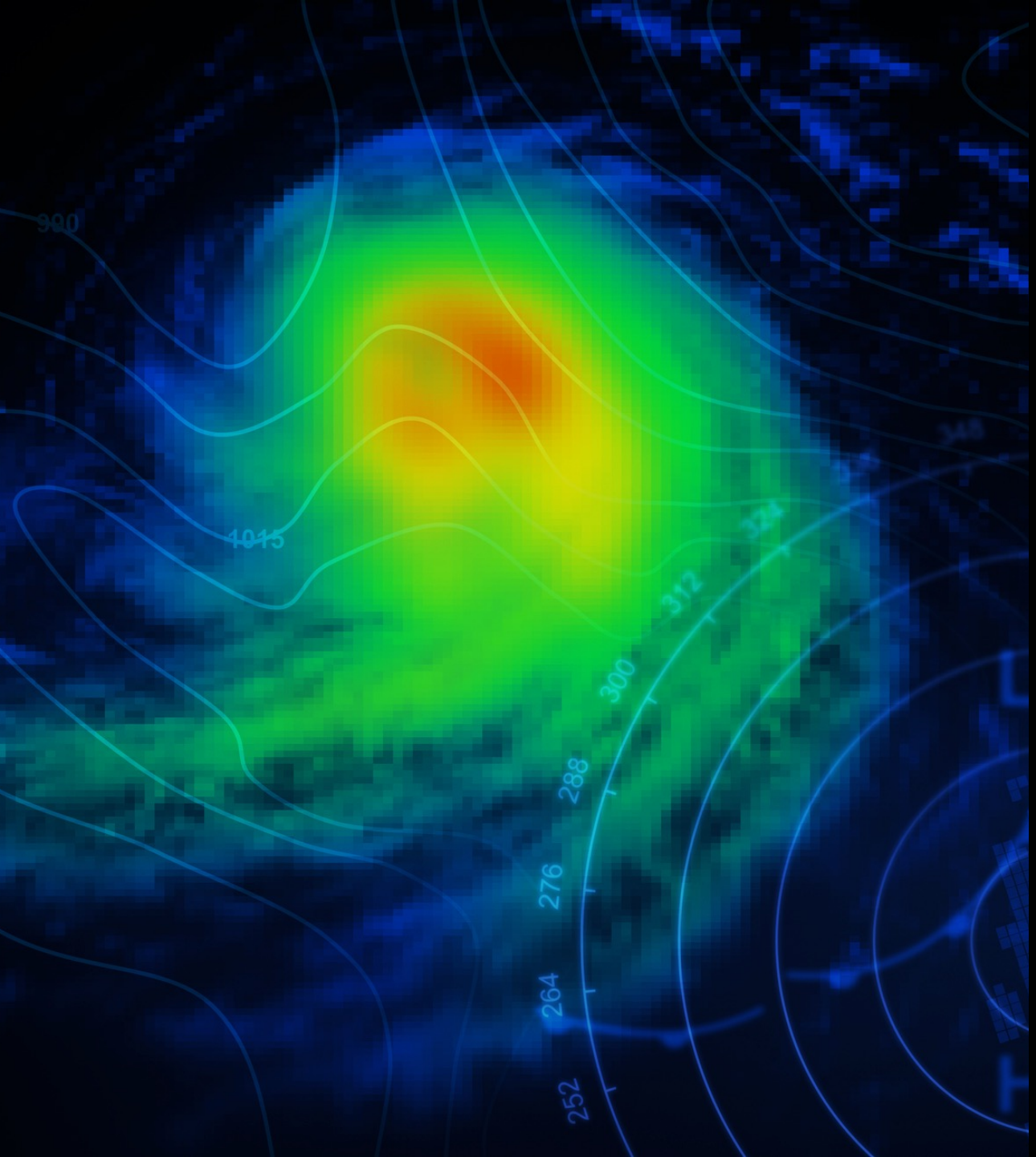
Anticipate
Observe for changes in the landscape and emerging threats

Identify
Create a dataset of assets and vulnerabilities to inform risk analysis

Protect
Take appropriate actions on customers' behalf

Detect
Detect threats in action and update asset database

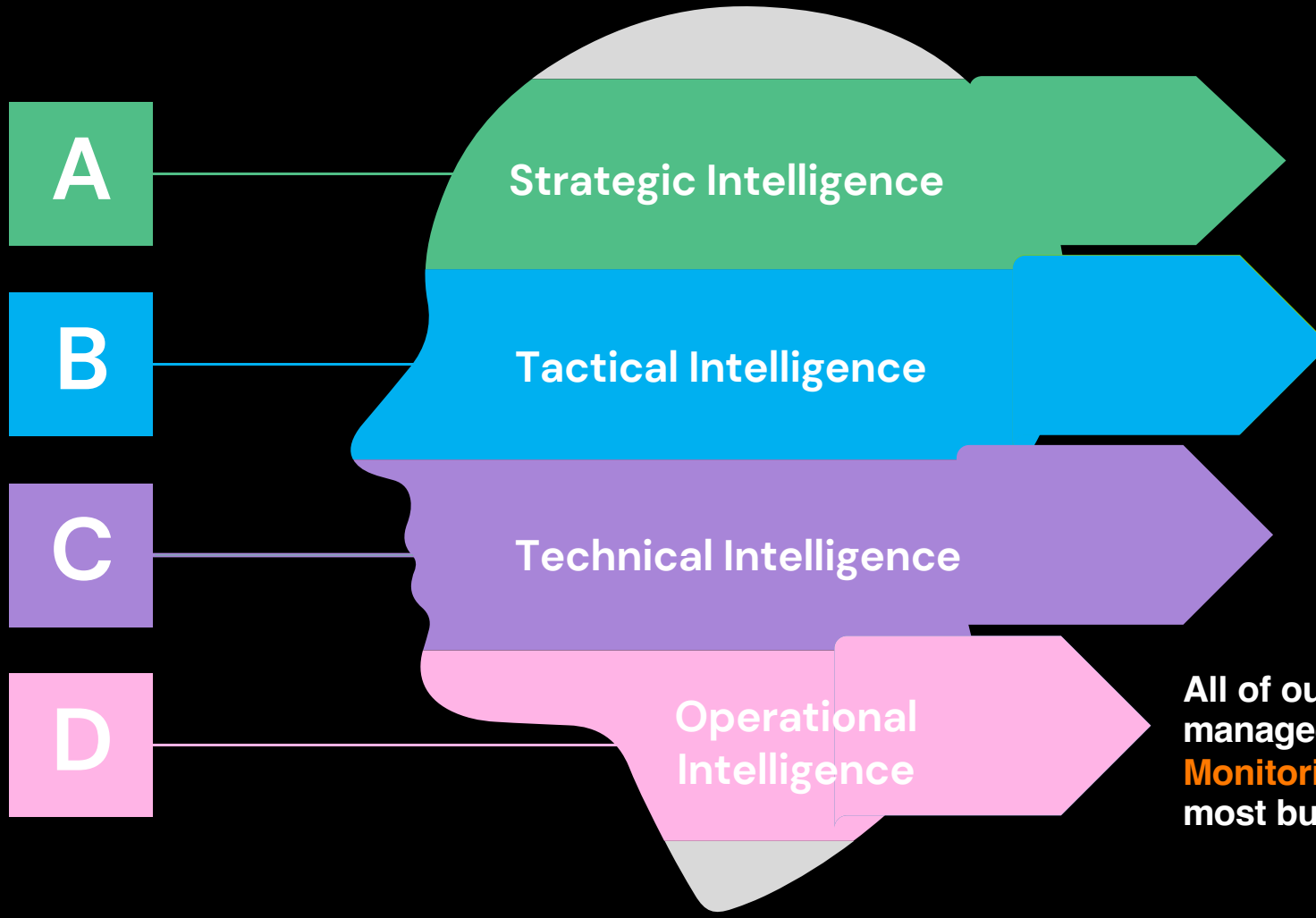
Respond
Targeted investigations and incident response



Get ahead of the storm

Intelligence-led security enables your organization with proactive protection and faster response

So where can we help?



Our **customer portal** delivers strategic intelligence, as well as our Threat Research and AID teams

World Watch and **Managed Vulnerability Intelligence [watch]** deliver tactical intelligence about emerging threats

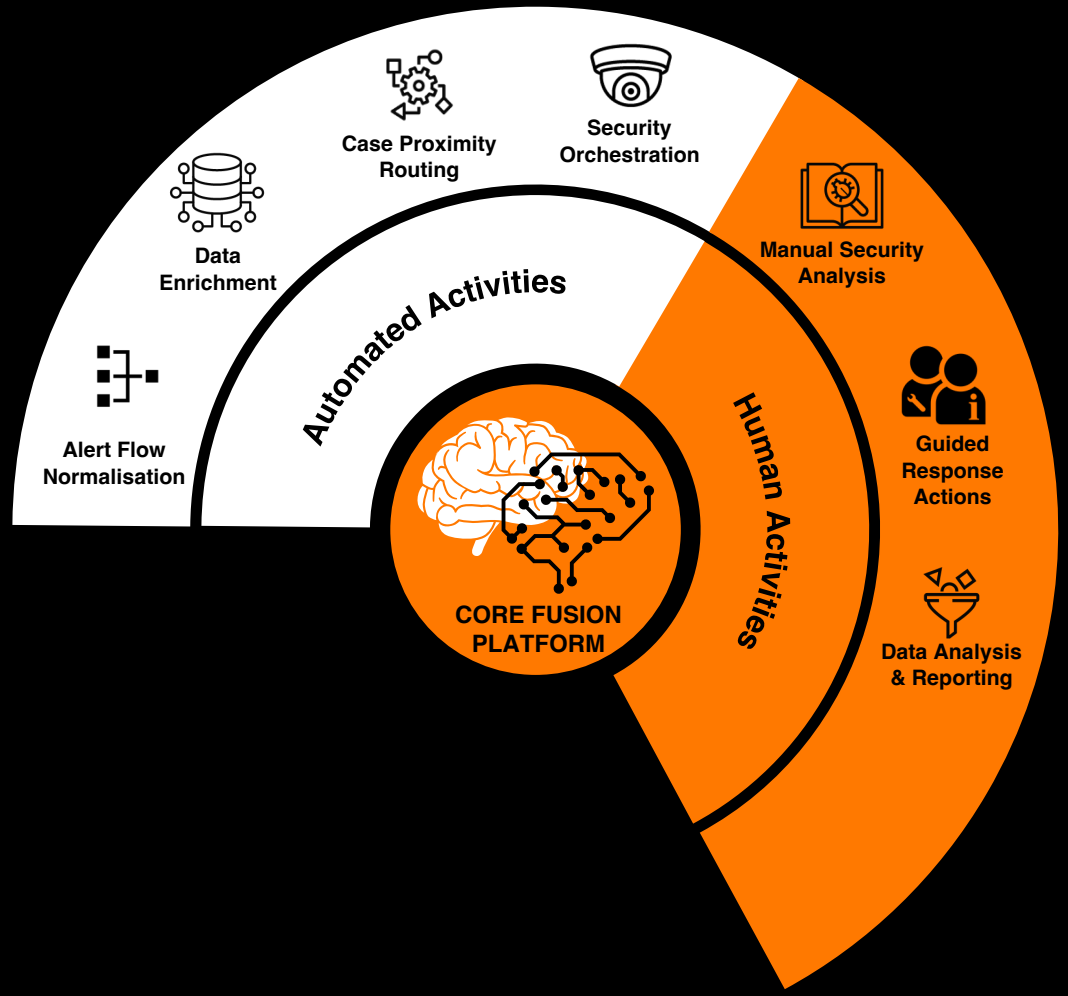
Our **Managed Threat Intelligence [protect]** service feeds high quality technical intelligence continuously into security technologies

All of our intelligence feeds into our global network of managed service hubs and **Managed Cybercrime Monitoring** can provide operational threat intelligence most business just don't have

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?

Tactical Intelligence

Delivering global Tactical Intelligence that drives action

Global OPS

i.e:
Global
VOC

Critical Vulnerability advisories drive proactive scanning from our Global VOC

World Watch

Global Marketing

i.e:
Security
Research

World Watch helps Research Team and Global Marketing to build the Security Navigator as well as monthly updates

Research

World Watch Customers

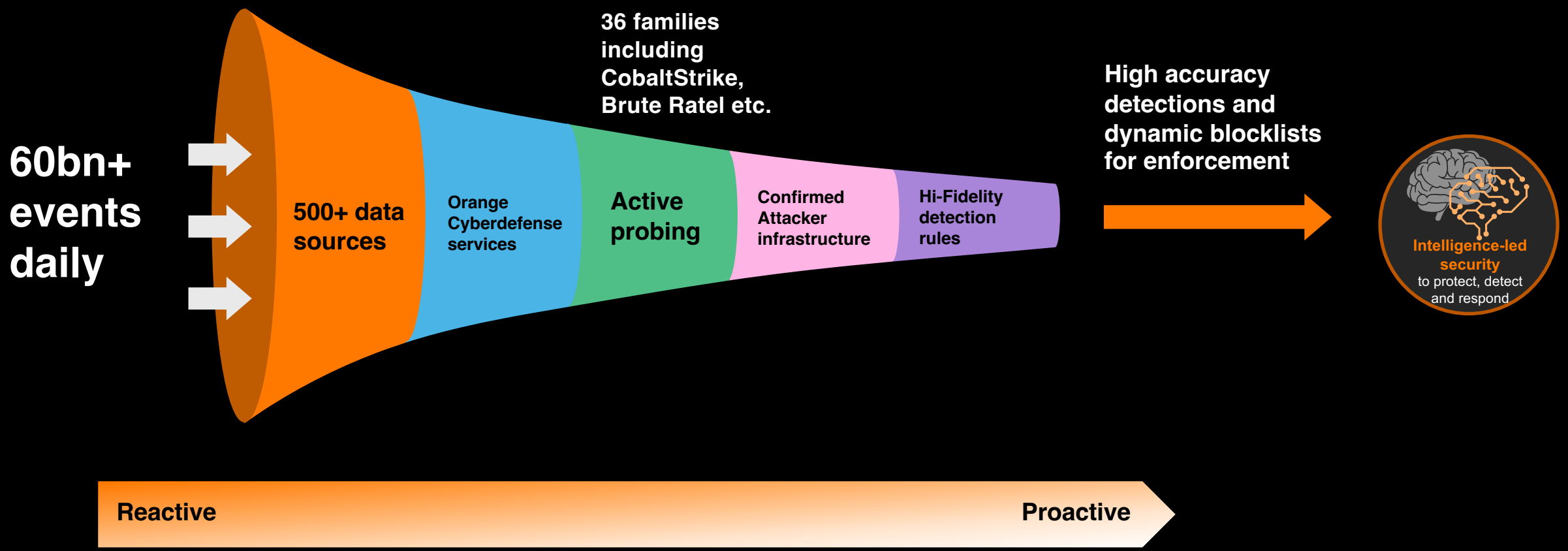
Advisories go out to our Customers regularly and are updated as situations develop

2 May 2024

Technical Intelligence

Orange Cyberdefense advanced intelligence

It is about quality, not just quantity…



Operational Intelligence

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

Collect

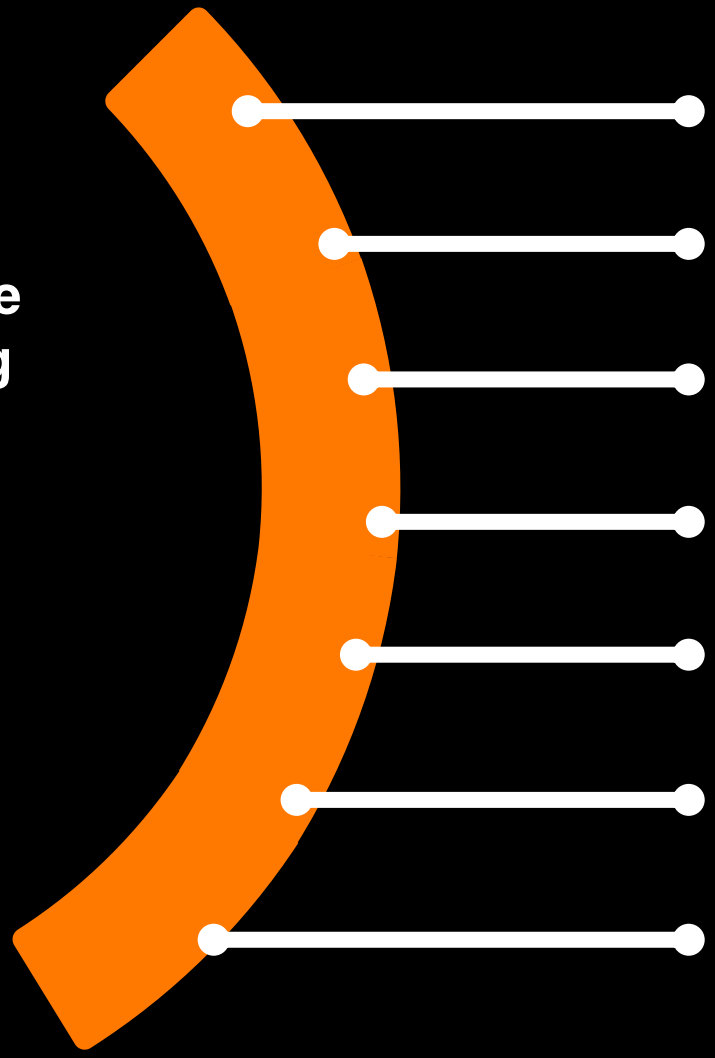
Asset data and intelligence goals

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?

Intelligence-led security in action

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

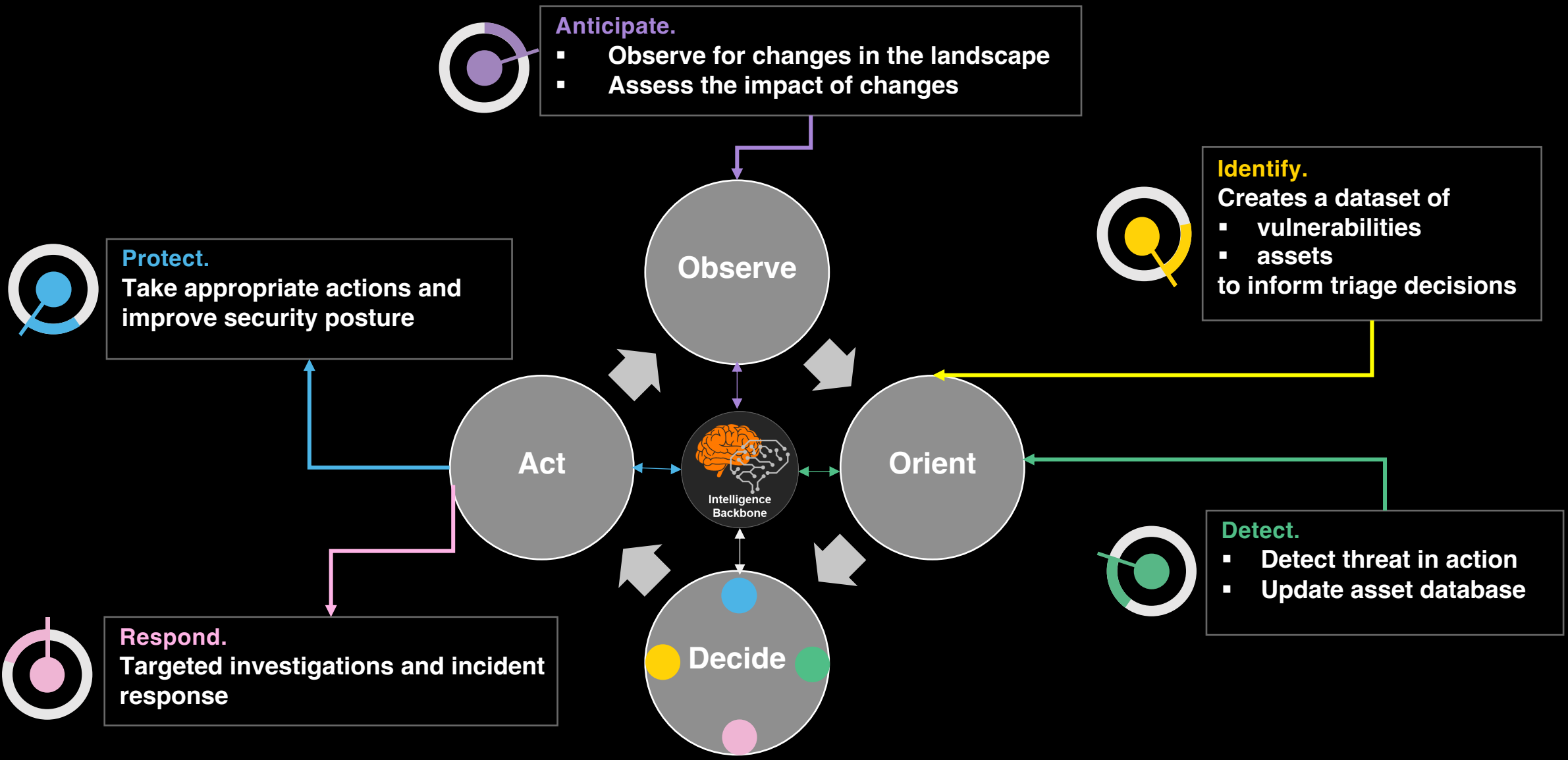
Further compromise prevented and initial breach minimized.

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

Delivering an Intelligence-led approach for adaptive cyberdefense



Together we are stronger.

Our CyberSOC

- Managed Detection and Response operations for Orange Cyberdefense, 200+ people across the world.
- Global team including 14 CyberSOCs.
- Recognised by Gartner in Market Guide for Managed Detection & Response*.
- Highly experienced team including experience in handling Nation State level attacks and processing 50 billion+ events daily.
- Supported by Threat Research and CERT teams, including proprietary Orange Threat Intelligence Datalake and member of programmes such as Microsoft MISA

Member of
Microsoft Intelligent Security Association
Microsoft

* Gartner report October 2021: 'Market Guide for Managed Detection and Response Services'

Our CSIRT is part of the Orange Cyberdefense CERT

- Operating since 2003
- Collaborating with Orange internal CERT
- 60k+ rogue sites taken down per year

- 110+ experts globally
- 24/7 Cybercrime-Fighting team with 20+ intelligence analysts across 3 time zones (follow the sun coverage)
- 10 languages, specialised intelligence backgrounds
- Member of industry-recognised bodies for CERT activities including CREST, TF-CSIRT, FIRST, …
- Partnerships established with vendors / editors, access to private lists, specific communication channels with police and intelligence departments all over the world, specific agreements with internet and Security global organizations (Verisign, Public Internet Registry, ICANN,…)

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CREST
PHISHING INITIATIVE France
VISA DE SÉCURITÉ PRIS ACCREDITED

Our security approach is driven by our knowledge of the threat,
and allows you to make the right decisions.

So you can…

…embed intelligence into your operations.

…align detection and response to key business risks.

…respond effectively and decisively.

…make a step change in maturity.

There are optional tasks as well…

Detecting, preventing, and responding to ransomware attacks and cyber extortion requires a comprehensive approach that combines technical measures, employee training, and incident response planning.

Business Continuity and Disaster Recovery (BCDR Plan):
BCDR practices enable an organization to get back on its feet after problems occur, reduce the risk of data loss and reputational harm, and improve operations while decreasing the chance of emergencies.

Employee Training:
Educate employees about the risks of ransomware and how to recognize phishing emails and other social engineering tactics.

Vulnerability Management & Patch Management:
Keep all software and systems up-to-date with the latest security patches to prevent exploitation of known vulnerabilities.

Access Controls:
Limit user privileges to only those necessary for their roles to prevent unauthorized access to sensitive systems and data.

Data Backup & Recovery:
Regularly backup critical data and store backups offline or in a separate, secure location to prevent them from being encrypted by ransomware.

Security Controls in place
Install and regularly update security controls, such as but not limited to, IPS, network monitoring, network segmentation, endpoint protection, email filtering

Email Security:
Use email authentication protocols like SPF, DKIM, and DMARC to prevent email spoofing and domain impersonation.

Cyberdefense