Orange
Cyberdefense

Ahead of the Storm

How to get ahead of the storm by leveraging threat intelligence

Hans Stevens, Head of Solution Design

orange™

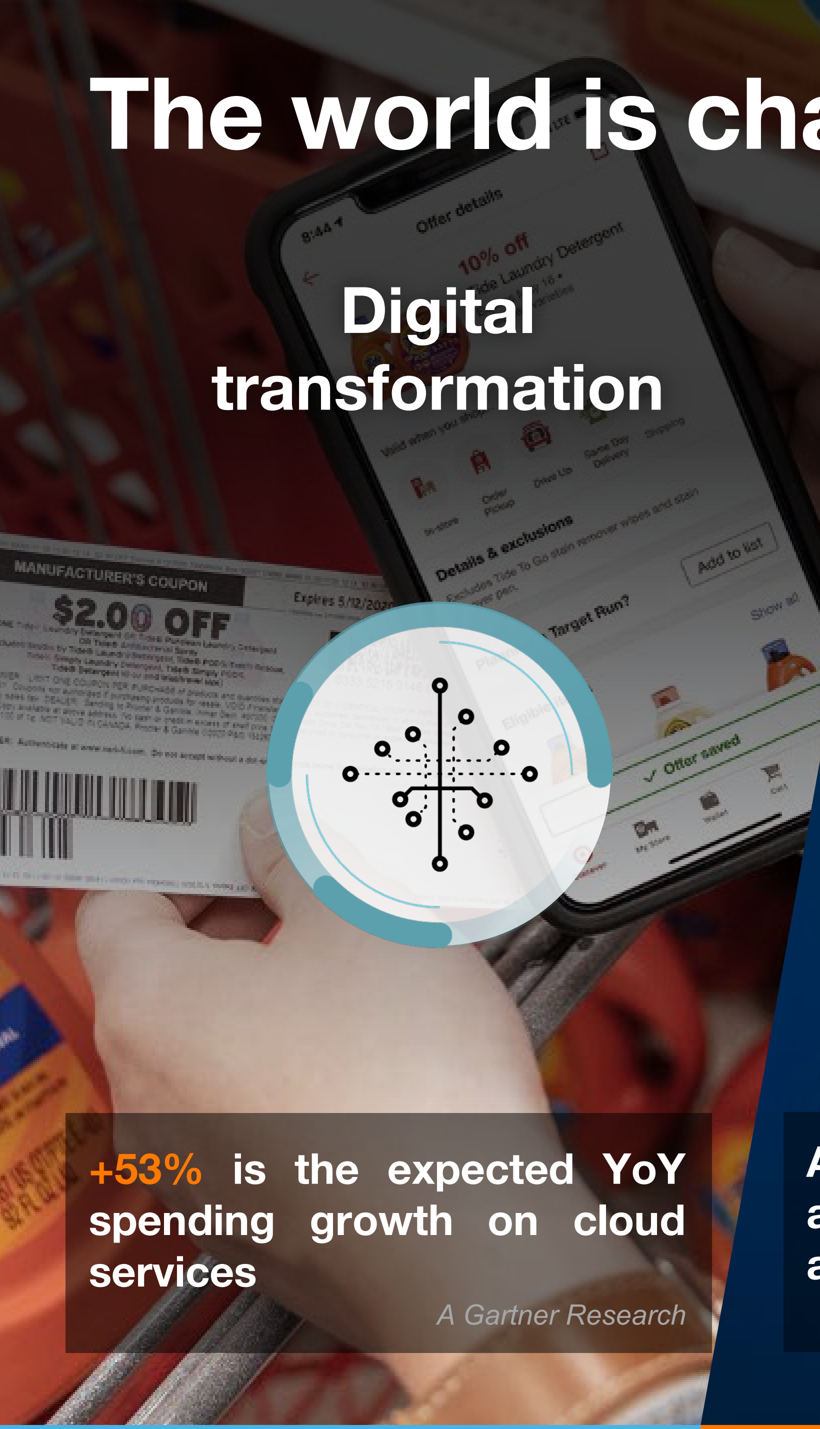
intelligence noun

in·tel·li·gence | \ in-ˈte-lə-jən(t)s 🔊 \

1. information concerning an enemy or possible enemy or an area

2. the ability to learn or understand or to deal with new or trying situations

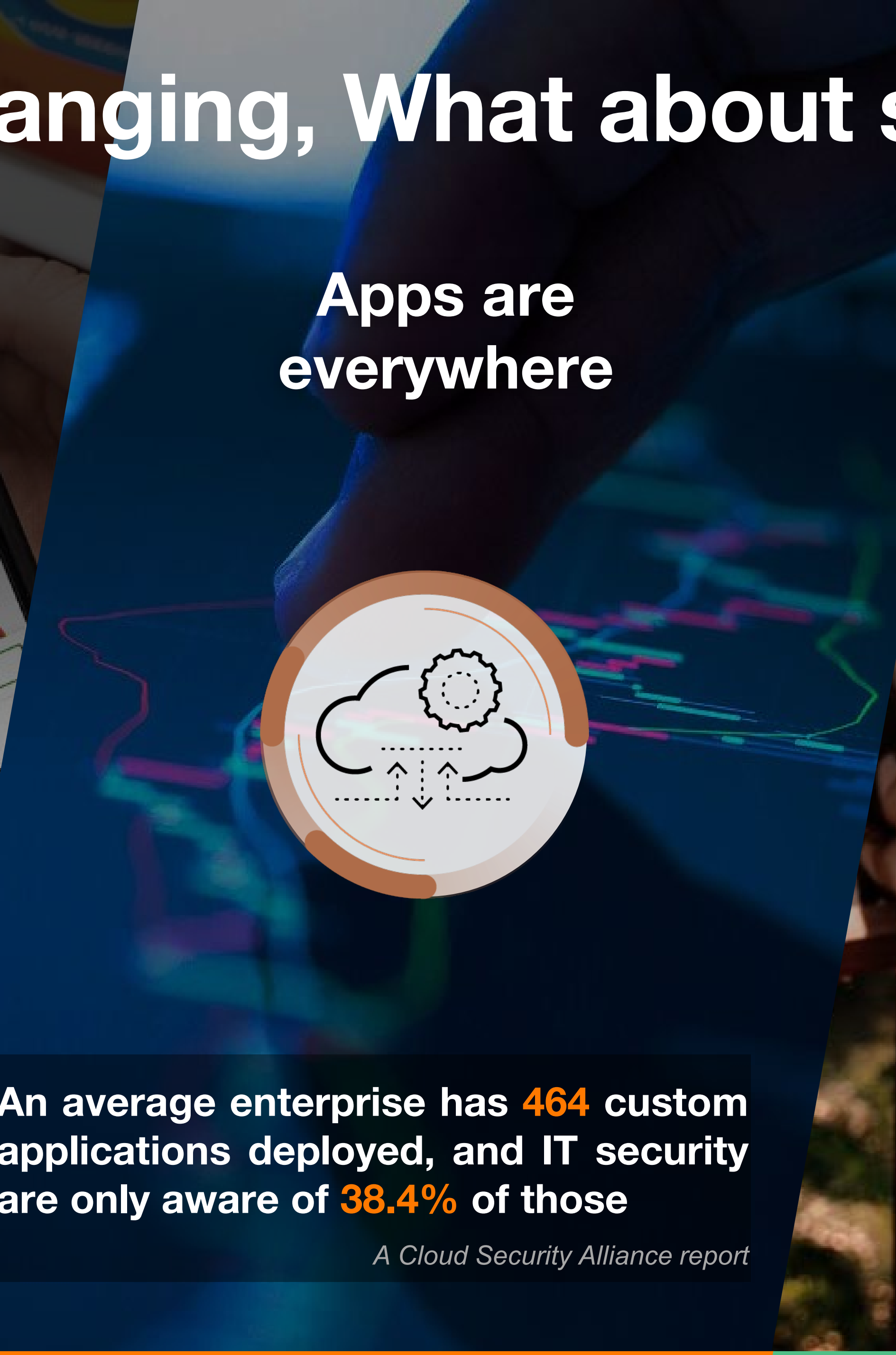
The world is changing, What about security?



Digital transformation

+53% is the expected YoY spending growth on cloud services

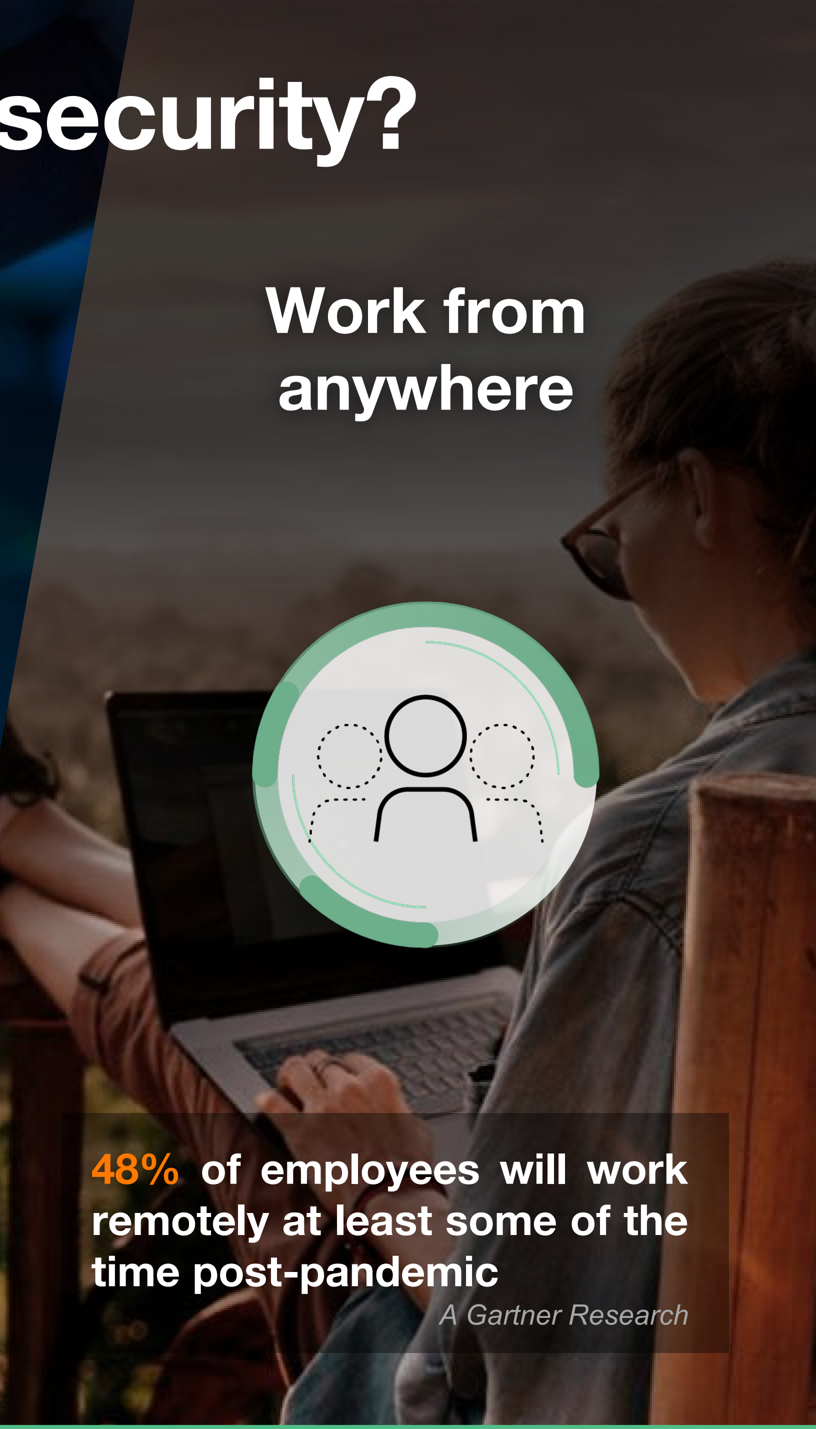
A Gartner Research



Apps are everywhere

An average enterprise has 464 custom applications deployed, and IT security are only aware of 38.4% of those

A Cloud Security Alliance report

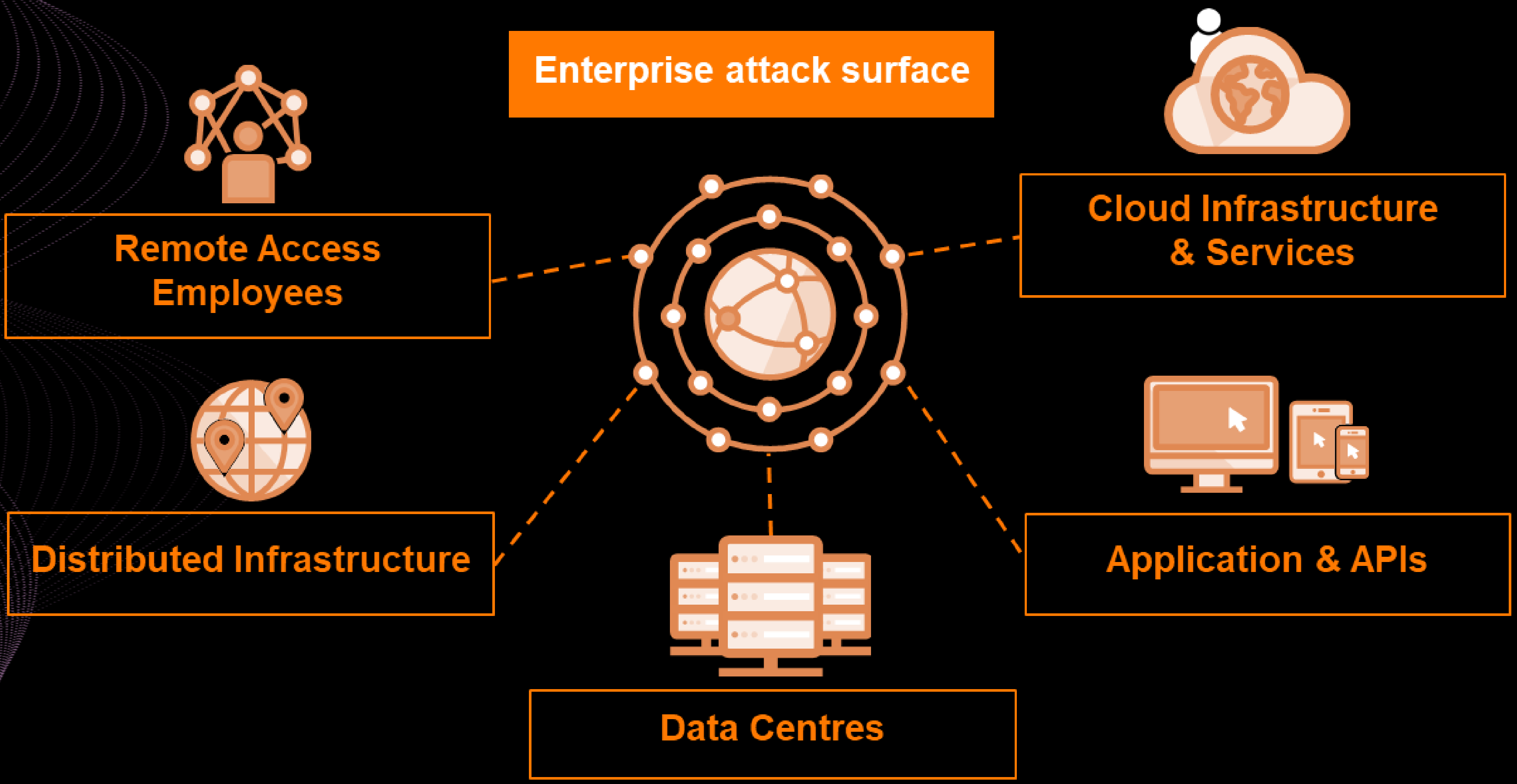


Work from anywhere

48% of employees will work remotely at least some of the time post-pandemic

A Gartner Research

Risk exposure, is it worth the risk?



Enterprise attack surface

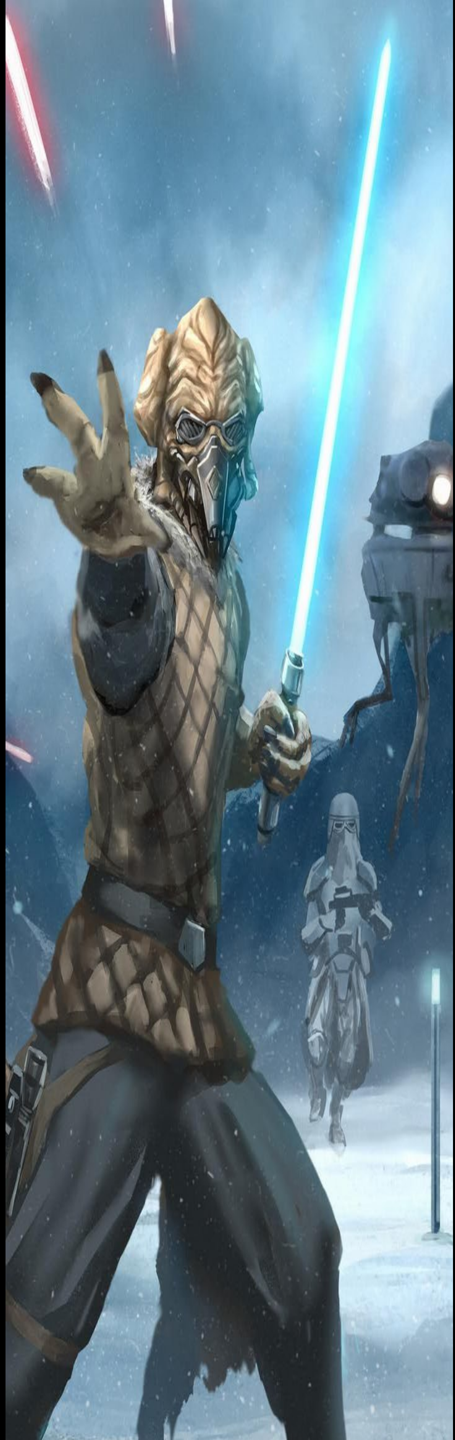
Remote Access Employees

Distributed Infrastructure

Data Centres

Cloud Infrastructure & Services

Application & APIs



As cyber threats evolve, you need to evolve as well

Christopher A, Wray

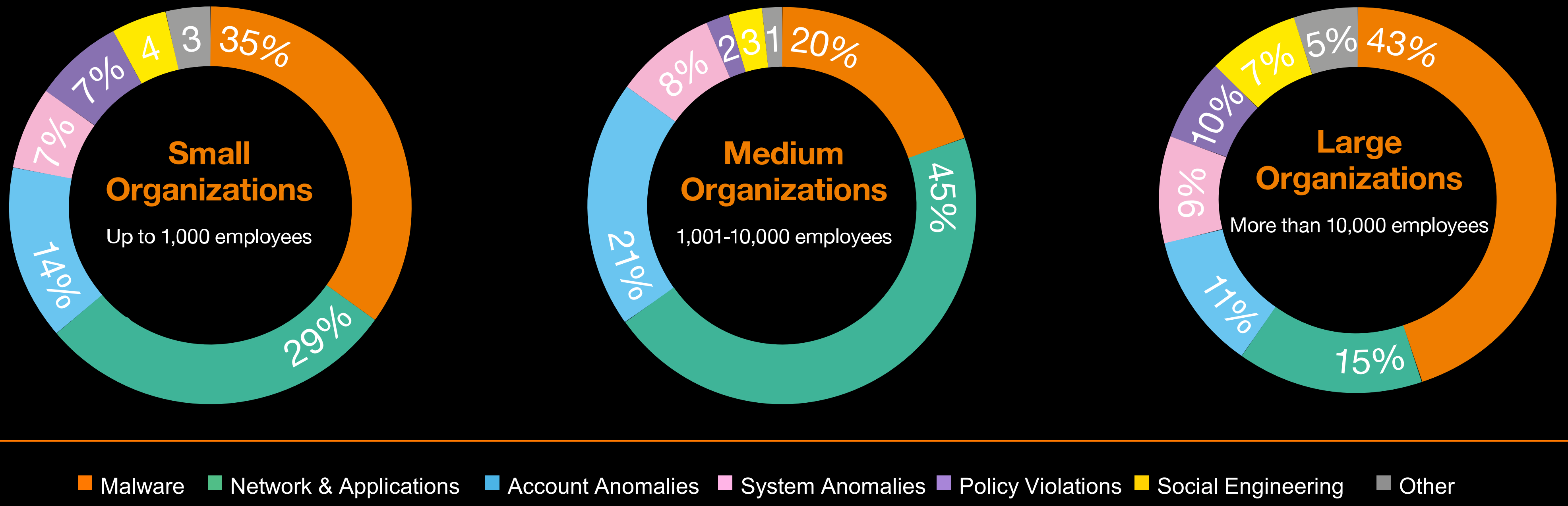
Are you having difficulties managing a growing multi-vendor hybrid IT/OT environment?

“Some are weatherwise,
some are otherwise.”

Being weatherwise to better respond

Security Incidents: Top root causes

Source: Orange Cyberdefense Security Navigator 2022



#1
38% of all incidents

60,000,000,000
Events

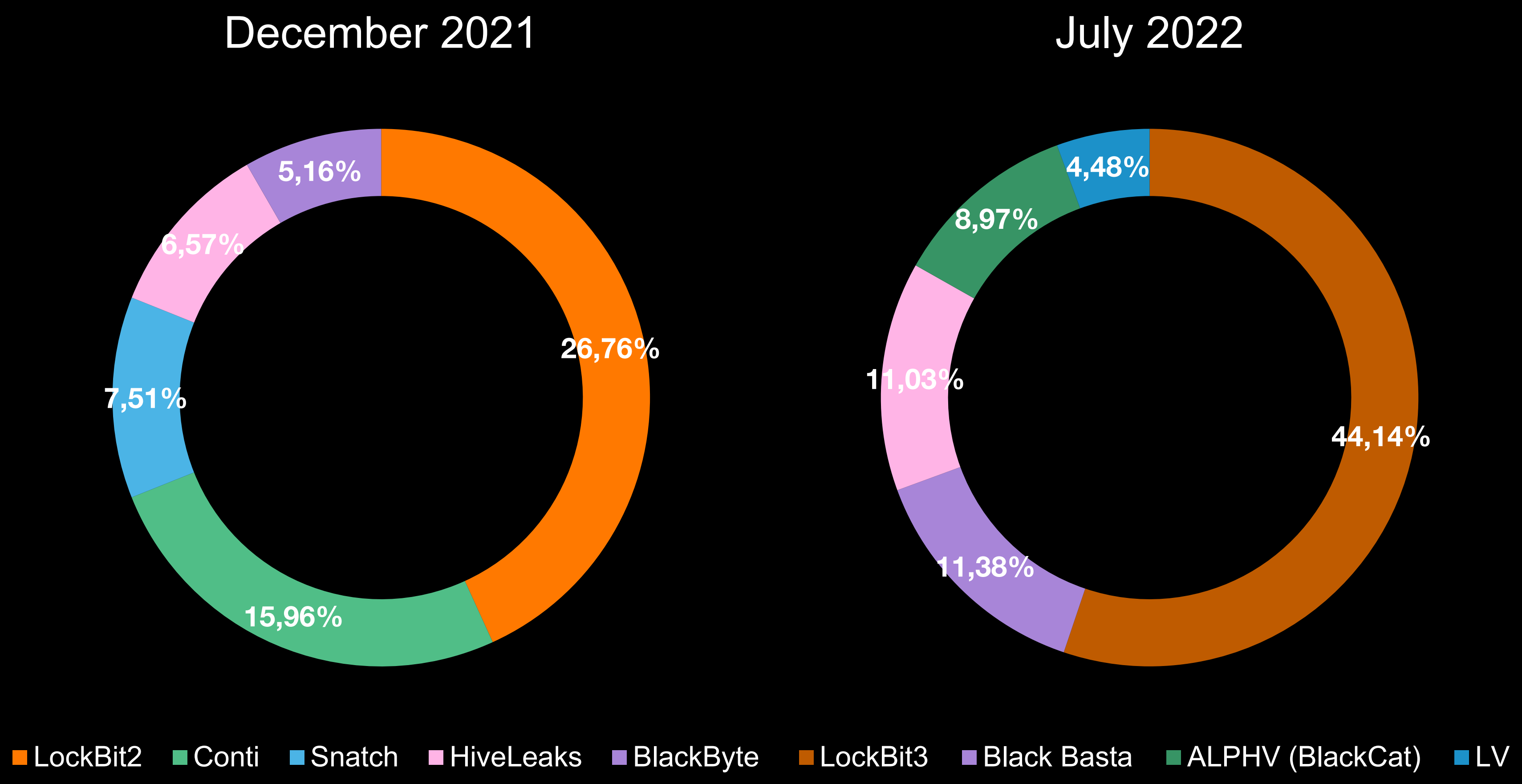
94,806
Investigated Incidents

34,158
Confirmed Incidents (36.03%)

Understanding the climate to continuously adapt

Dark web monitoring: Top 5 ransomware threat actors

Source: Orange Cyberdefense Epidemiology Lab



Conti retired in June 2022, BlackBasta filled in the gap in a short time period. LockBit comes with new malware in June 2022.

New attack tactics, techniques, and procedures are introduced.

Challenge

Sophisticated threats, complex solutions, limited resources and expertise.

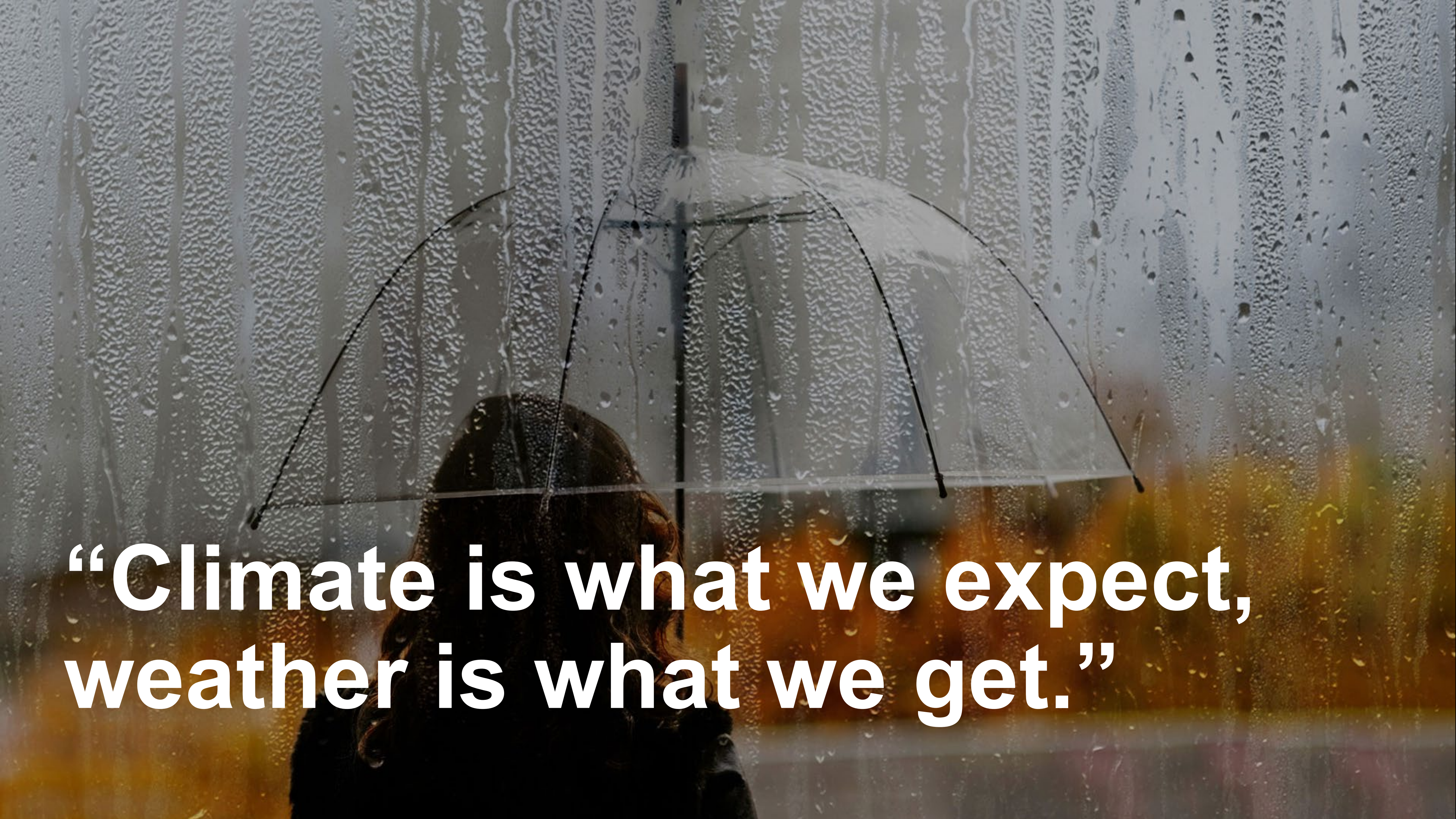
How to…

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

… make best use of security technology?

… focus on real priorities?

… be agile and adaptive?

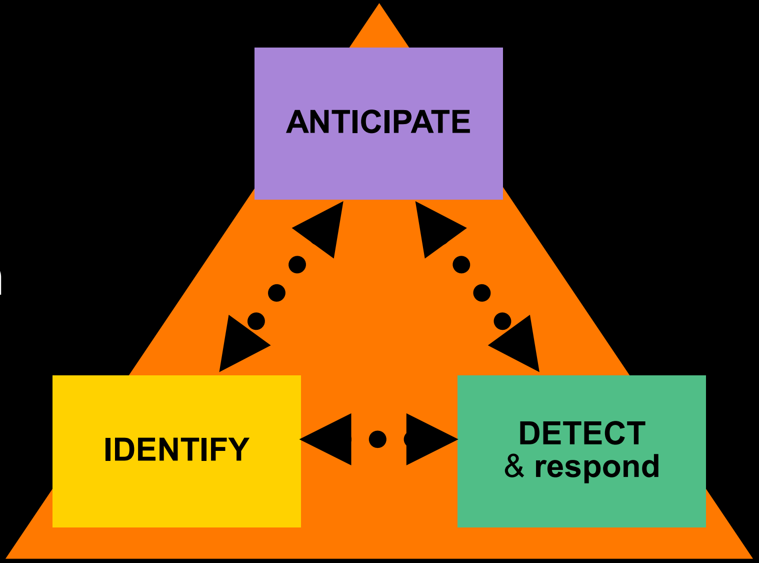


“Climate is what we expect,
weather is what we get.”

Intelligence-led security

Collection, validation, aggregation, correlation and analysis of both internal and external data

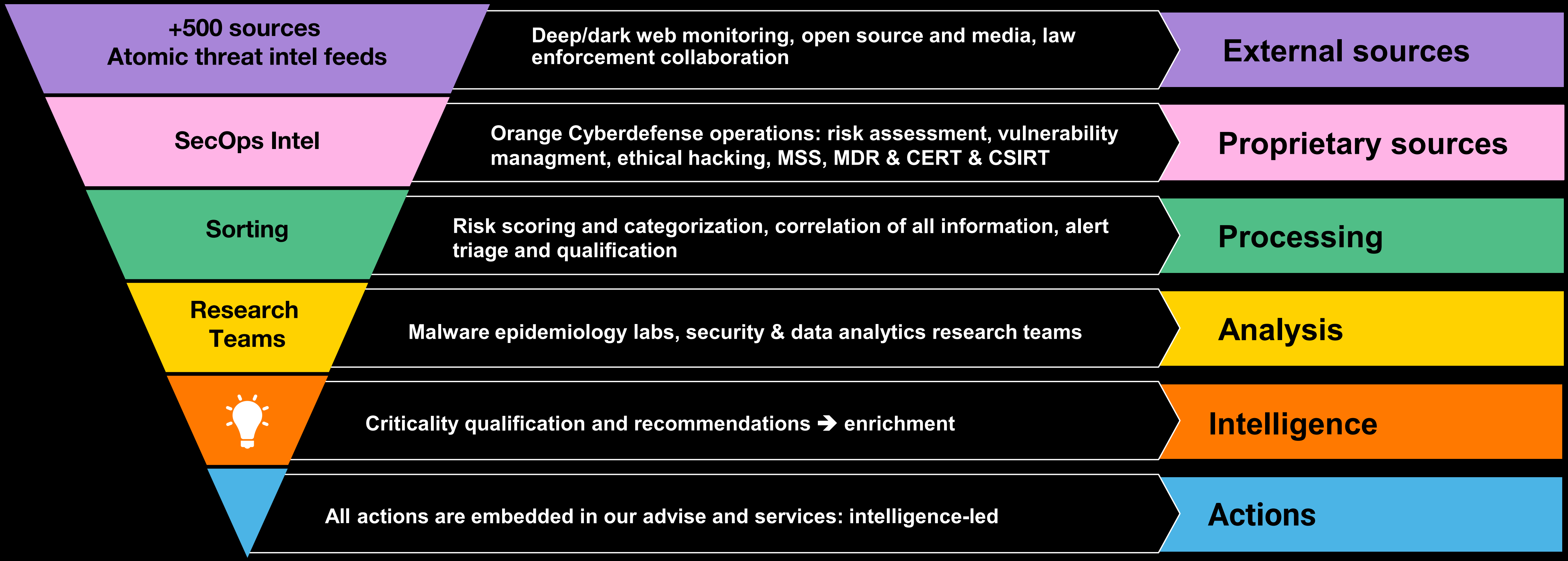
- Collect *diverse* security intelligence
- Correlate that with what's known / seen on the customer estate
- Determine what actions we and the customer need to take in response to intelligence
- Close the loop' to gather additional intelligence to determine how we & our customers are affected.



So that we can be agile and adaptive in the face of a continuously changing threats.

Not all intelligence is made equal

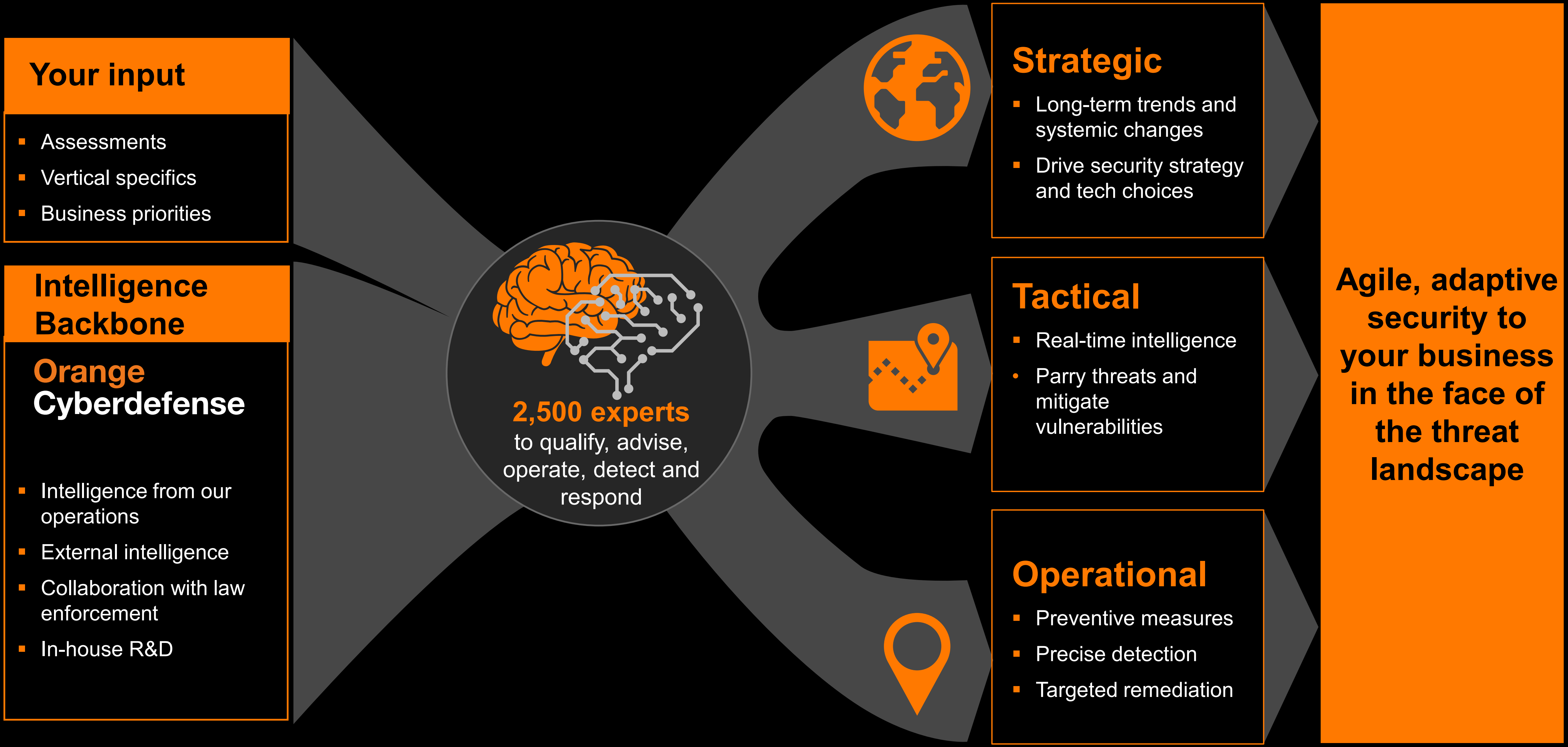
Our intelligence goes beyond IoCs: the path achieving actionable intelligence



+500 sources Atomic threat intel feeds	Deep/dark web monitoring, open source and media, law enforcement collaboration	External sources
SecOps Intel	Orange Cyberdefense operations: risk assessment, vulnerability managment, ethical hacking, MSS, MDR & CERT & CSIRT	Proprietary sources
Sorting	Risk scoring and categorization, correlation of all information, alert triage and qualification	Processing
Research Teams	Malware epidemiology labs, security & data analytics research teams	Analysis
💡	Criticality qualification and recommendations ➔ enrichment	Intelligence
	All actions are embedded in our advise and services: intelligence-led	Actions

Benefit from our intelligence-led security

Better respond to the weather, anticipate and adapt to the climate



Your input

- Assessments
- Vertical specifics
- Business priorities

Intelligence Backbone

Orange Cyberdefense

- Intelligence from our operations
- External intelligence
- Collaboration with law enforcement
- In-house R&D

2,500 experts
to qualify, advise, operate, detect and respond

Strategic

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

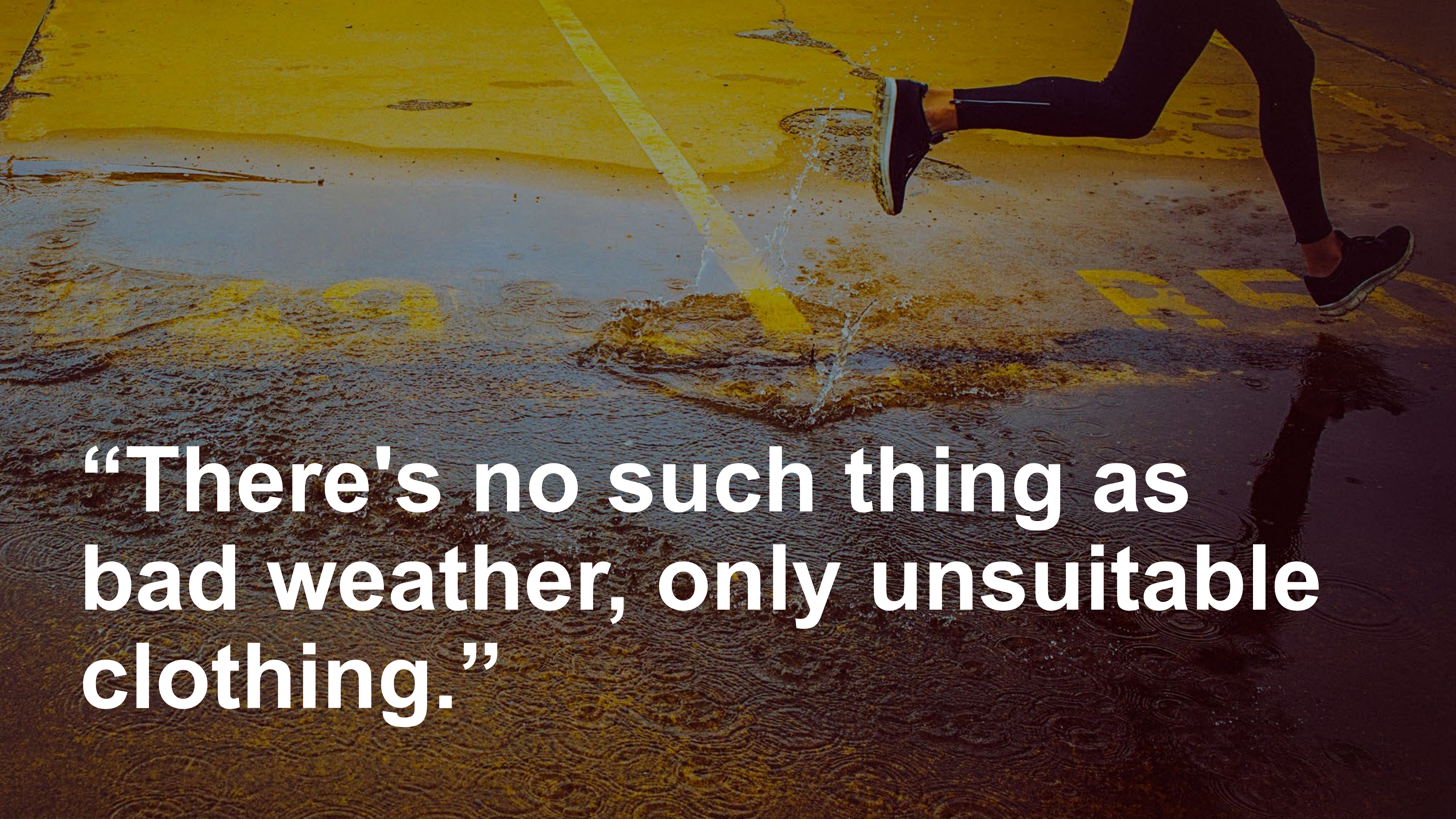
Tactical

- Real-time intelligence
- Parry threats and mitigate vulnerabilities

Operational

- Preventive measures
- Precise detection
- Targeted remediation

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



“There's no such thing as bad weather, only unsuitable clothing.”

Strategic intelligence-led security

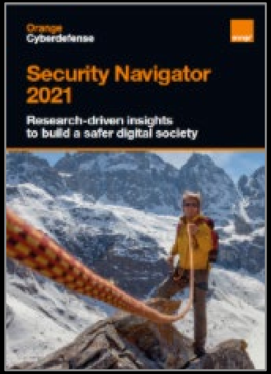
Drive security strategy, roadmap and technology choices

Free insights from our Threat Researchers, available to all.

Orange Cyberdefense

The road to your own SOC

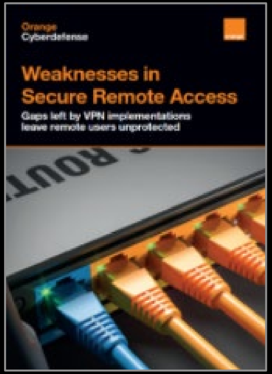
Critical steps you must consider when building your own SOC, regardless of the level of ambition.



Orange Cyberdefense

Security Navigator 2021

Research-driven insights to build a safer digital society



Orange Cyberdefense

Weaknesses in Secure Remote Access

Gaps left by VPN implementations leave remote users unprotected

Orange Cyberdefense

Epidemiology Labs | Threat Intelligence Report

Cybercriminal interest in cryptocurrencies

Date: May 18 (update)

Version: 2.0

Authors: OSINT Unit – Part of the Orange Cyberdefense Epidemiology Lab

www.orangecyberdefense.com

Our security tips for remote work

Use a secure connection [illegible]

Separate professional and personal uses [illegible]

Save your documents [illegible]

Ensure protection of your equipment [illegible]

Be vigilant when browsing the internet [illegible]

Does your workstation behave abnormally? Do you think you have clicked on a phishing e-mail? In case of doubt, don't hesitate to contact the IT support or the Security Team.

Orange Cyberdefense

Epidemiology Labs | Threat Intelligence Report

Potential risks for the pharmaceutical sector

Date: April 6 (update)

Version: 2.0

TLP: White

Authors: OSINT Unit Part of the Orange Cyberdefense Epidemiology Lab

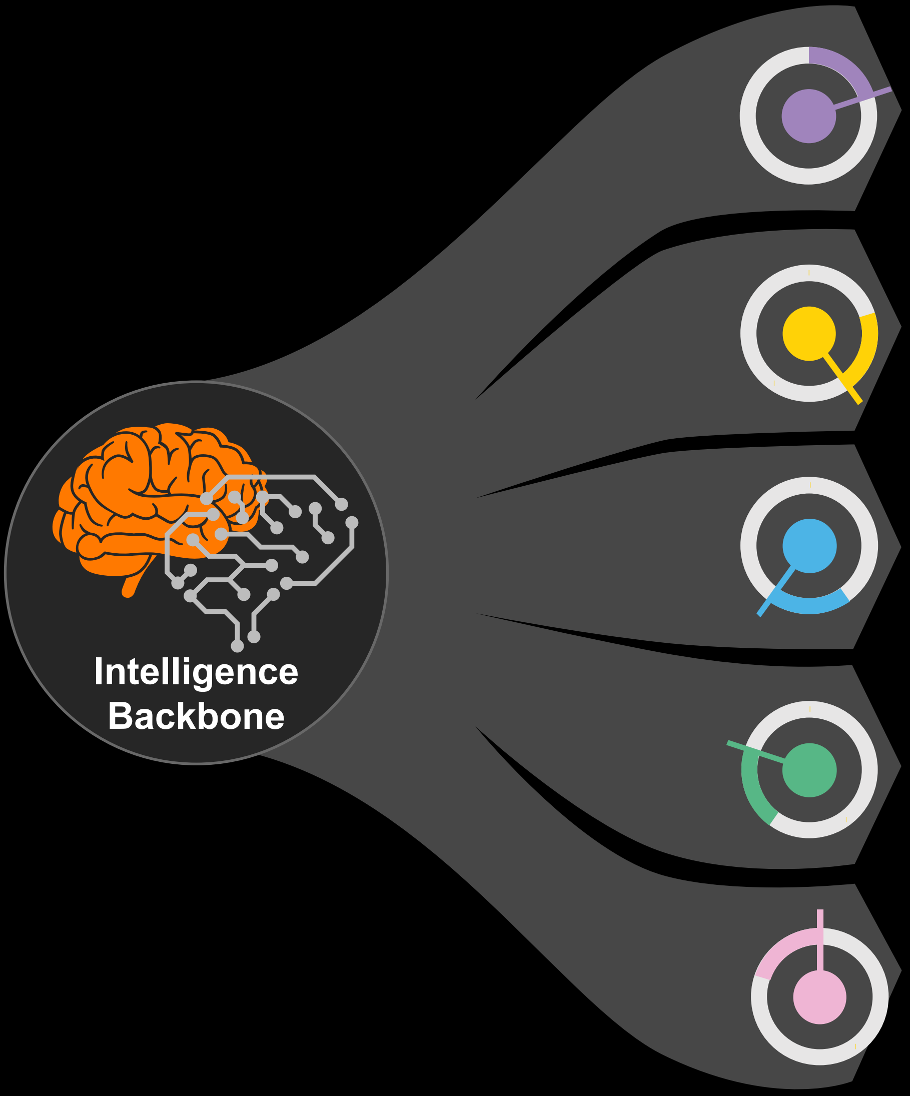
www.orangecyberdefense.com

Assessment and Advisory services:

- Cybersecurity advisors to assess your existing security posture (organizational and technical).
- Consultants to evaluate and improve your cybersecurity strategy.
- Technical experts to advise you on your security architecture.

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 [Endpoint]
- Managed Threat Detection [Network]
- Managed Threat Detection [Log]

Respond
Targeted investigations and incident response

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

Our solution : Managed Cybercrime Monitoring

Managed Cybercrime Monitoring [brand]

Monitoring of web, mobile and social channels.

Managed Cybercrime Monitoring [data]

Proactive identification of potential data exposure across diverse sources

Managed Cybercrime Monitoring [fraud]

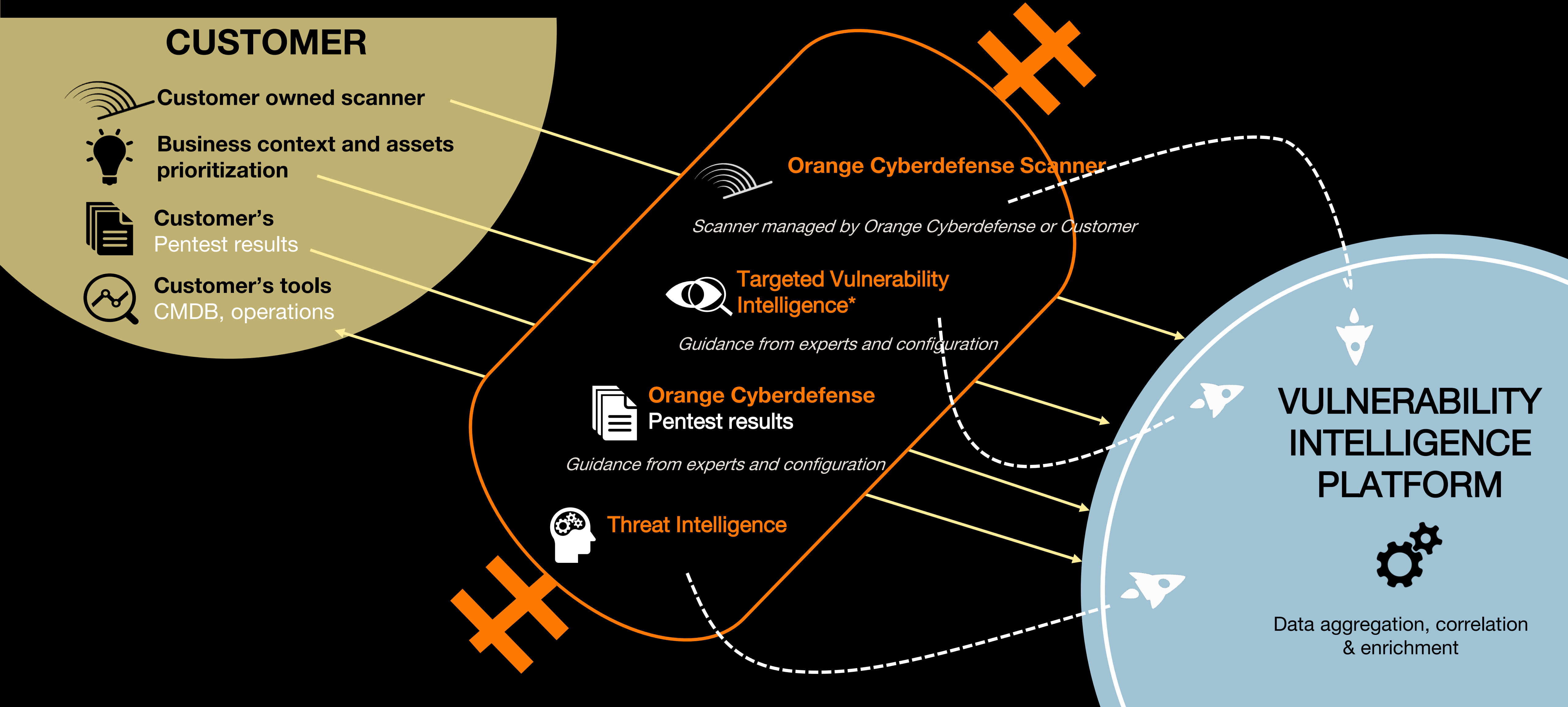
Surveillance of fraudulent activity.

Managed Cybercrime Monitoring [email]

Advanced mail analysis, employee security awareness and IOC collection

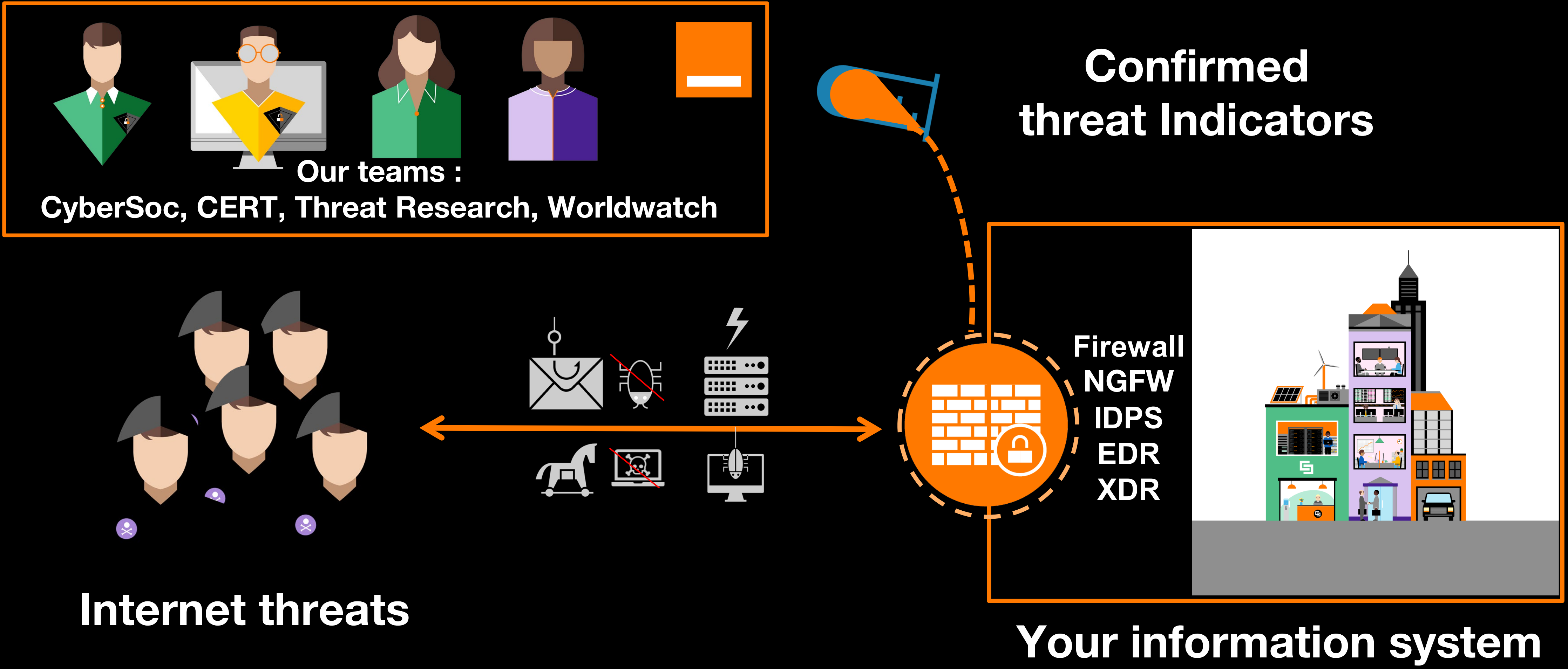
Our solution: Managed Vulnerability Intelligence [identify]

All vulnerability related data consolidated in the Vulnerability Intelligence Platform



CUSTOMER
Customer owned scanner
Business context and assets prioritization
Customer's
Pentest results
Customer's tools
CMDB, operations
Orange Cyberdefense Scanner
Scanner managed by Orange Cyberdefense or Customer
Targeted Vulnerability Intelligence*
Guidance from experts and configuration
Orange Cyberdefense
Pentest results
Guidance from experts and configuration
Threat Intelligence
VULNERABILITY INTELLIGENCE PLATFORM
Data aggregation, correlation & enrichment

Our solution : Managed Threat intelligence [protect]



Our teams :
CyberSoc, CERT, Threat Research, Worldwatch

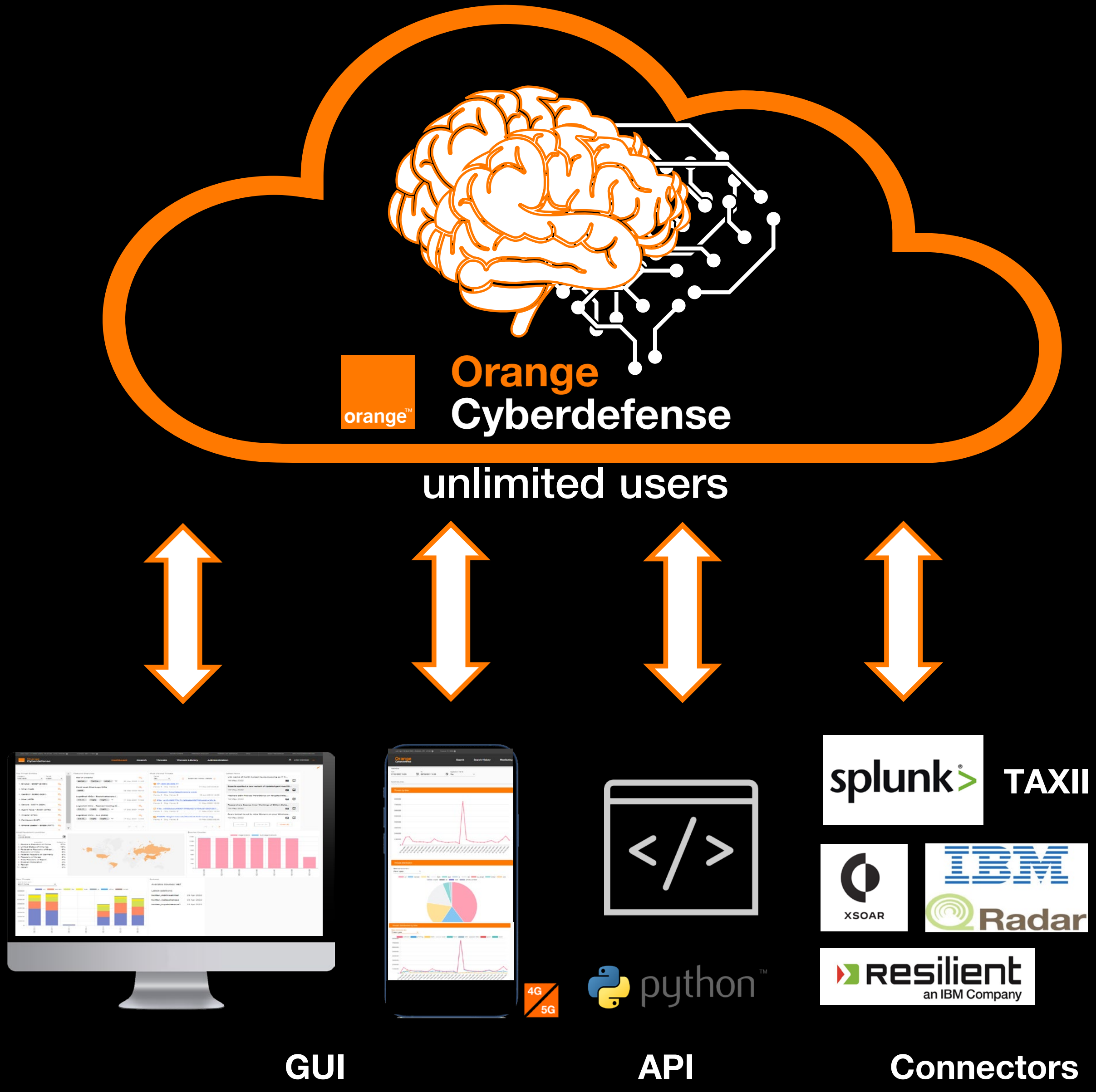
Confirmed
threat Indicators

Internet threats

Firewall
NGFW
IDPS
EDR
XDR

Your information system

Our solution : Managed threat intelligence [detect]



Orange Cyberdefense

unlimited users

TAXII

GUI

API

Connectors

Enhance your detection

- Feed and lookup service for your SIEM, SOAR, TIP
- Alerting service about new threats relative to a vulnerability
- 500 sources, 900 000 new IOC/day, Threat library (TTP, campaign, threat actors, malware, tools)

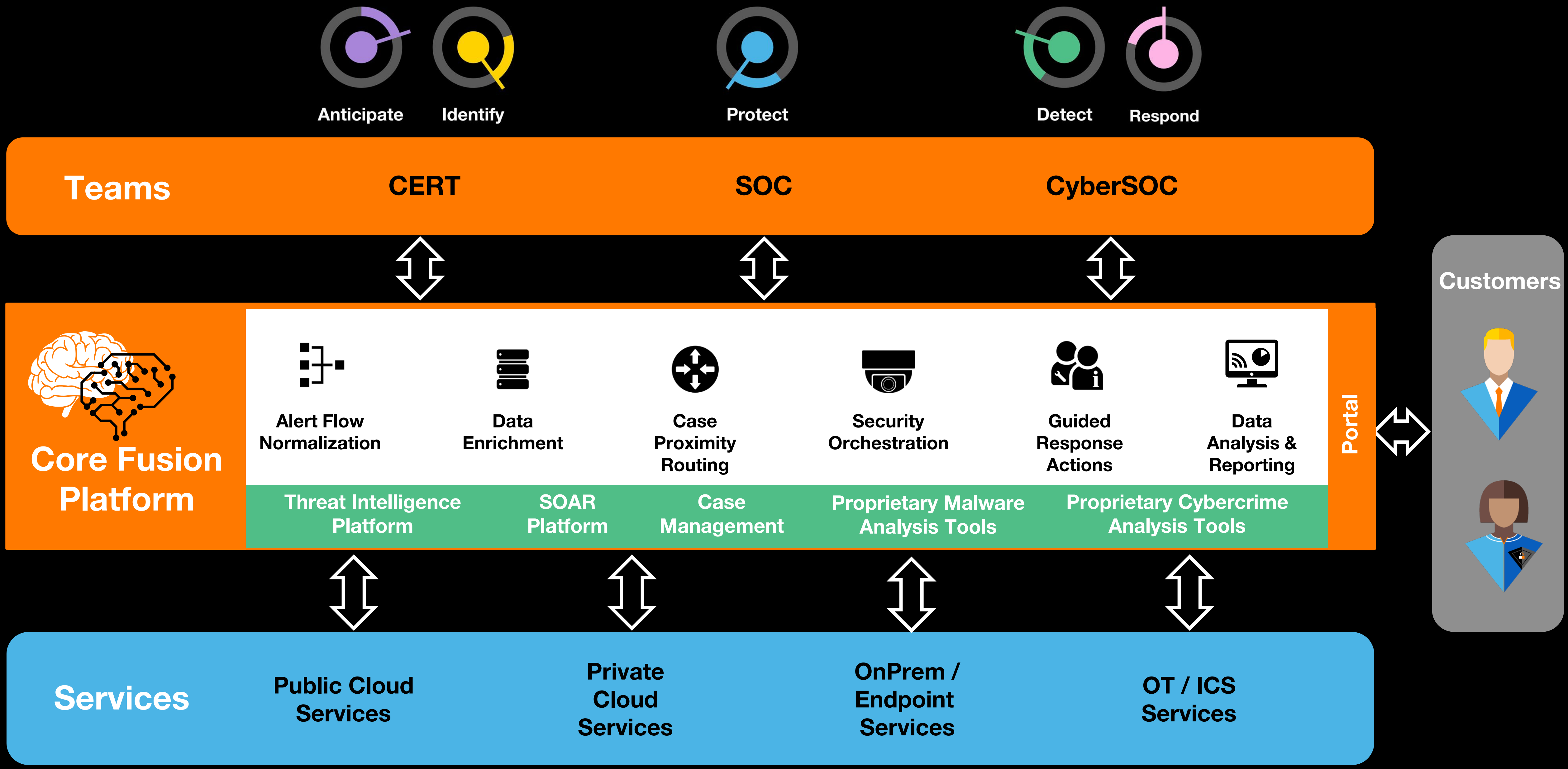
Outsource with confidence your threat intelligence source management

- **Qualified data**
- **Leverage manage service of OCD CyberSOC, CERT (telemetrie, sighting)**
- **Maintenance of sources over the time, Erosion management.**
- **Evaluation of additional sources by CERT OCD.**

Easy to use

- Webapp, API swagger, Command line tool, python SDK, unlimited users.

Operational synergies via Core Fusion



Anticipate

Identify

Protect

Detect

Respond

Teams

CERT

SOC

CyberSOC

Core Fusion Platform

Alert Flow Normalization

Data Enrichment

Case Proximity Routing

Security Orchestration

Guided Response Actions

Data Analysis & Reporting

Threat Intelligence Platform

SOAR Platform

Case Management

Proprietary Malware Analysis Tools

Proprietary Cybercrime Analysis Tools

Portal

Customers

Services

Public Cloud Services

Private Cloud Services

OnPrem / Endpoint Services

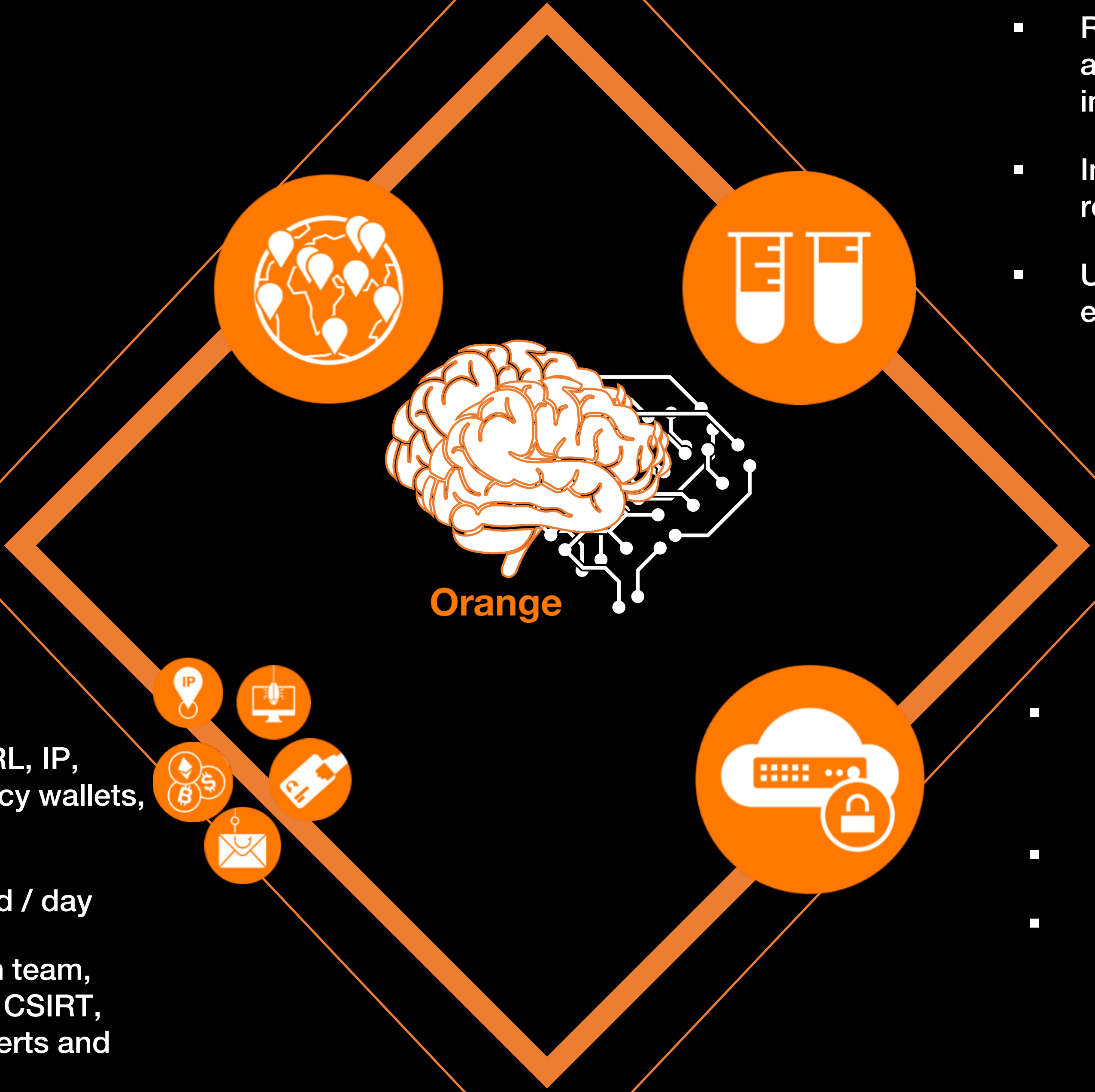
OT / ICS Services

- Orange Cyberdefense feeds
- Orange data
- Public sources
- Commercial sources
- Private/Community feeds

More than 500 data sources

- Raw data is enriched by our tools and experts to get qualified information
- Information is scored & IoCs regularly checked
- Used by our own Cybersecurity experts to assist investigations

Enriched, analyzed, evaluated

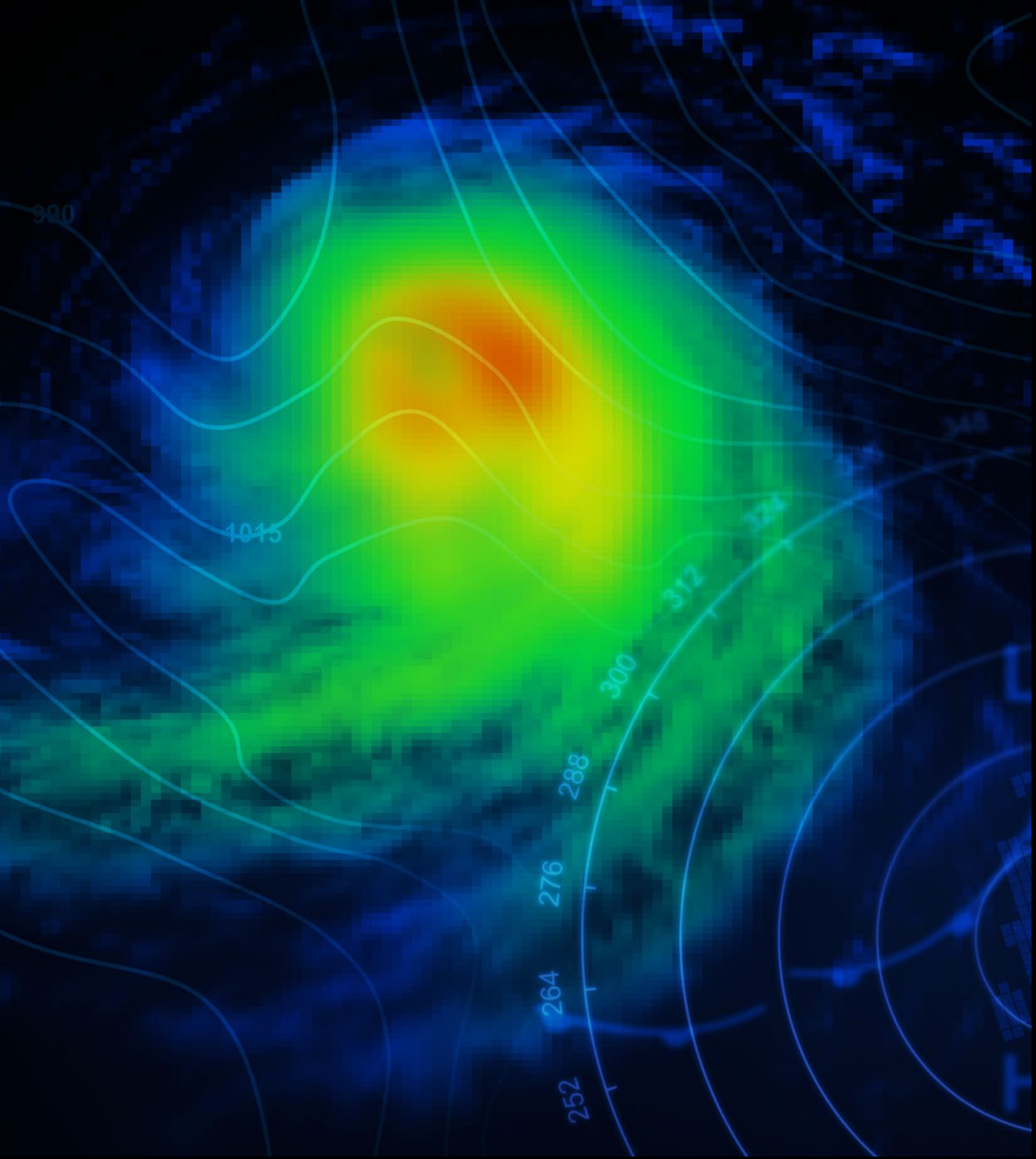


Large and Diverse dataset

- Various data types: email, URL, IP, domain names, cryptocurrency wallets, pasties…
- 2 Millions news threats added / day
- Input from Security Research team, Malware Analysis lab, CERT, CSIRT, Vulnerability Intelligence experts and Security Analysts

Flexible Use Cases

- Integrated into Managed Detection and Response operations
- Available via UI for customers
- Available as curated threat feed to stream into customer protection tools (such as Next-Gen Firewalls, Secure Web Gateways etc.)**

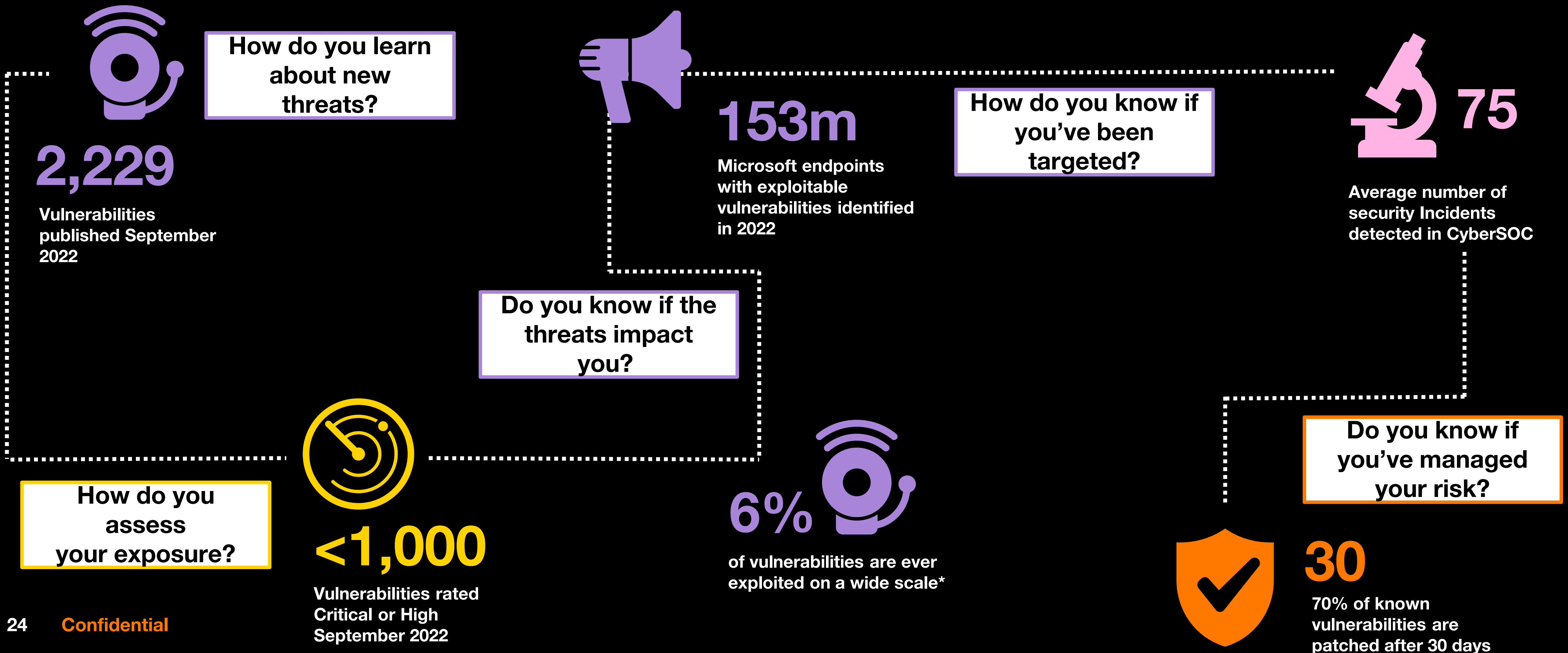


Get ahead of the storm.

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

How do you manage your risk without intelligence-led security?

A timeline of a vulnerability



How do you learn about new threats?

2,229

Vulnerabilities published September 2022

How do you assess your exposure?

<1,000

Vulnerabilities rated Critical or High September 2022

Do you know if the threats impact you?

6%

of vulnerabilities are ever exploited on a wide scale*

153m

Microsoft endpoints with exploitable vulnerabilities identified in 2022

How do you know if you've been targeted?

75

Average number of security Incidents detected in CyberSOC

Do you know if you've managed your risk?

30

70% of known vulnerabilities are patched after 30 days

Source: Orange Cyberdefense Intelligence, Research & Operations teams

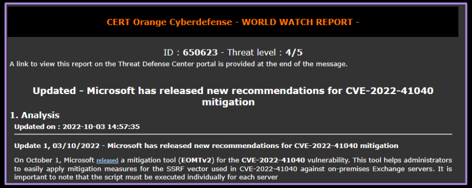
The value-add of intelligence-led security

A timeline of defense for a vulnerability like ProxyNotShell

Day 1

Vulnerability discovered

Vulnerability Intelligence team releases an advisory (WorldWatch Report). CTI collection and share with customers



CERT Orange Cyberdefense - WORLD WATCH REPORT -

ID : **650623** - Threat level : **4/5**

A link to view this report on the Threat Defense Center portal is provided at the end of the message.

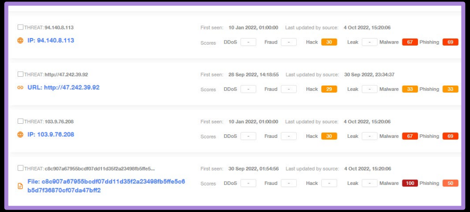
Updated - Microsoft has released new recommendations for CVE-2022-41040 mitigation

1. Analysis

Updated on : 2022-10-03 14:57:35

Update 1, 03/10/2022 - Microsoft has released new recommendations for CVE-2022-41040 mitigation

On October 1, Microsoft released a mitigation tool (**EOMTv2**) for the **CVE-2022-41040** vulnerability. This tool helps administrators to easily apply mitigation measures for the SSRF vector used in CVE-2022-41040 against on-premises Exchange servers. It is important to note that the script must be executed individually for each server



□ THREAT: 94.140.8.113
IP: 94.140.8.113
First seen: 10 Jan 2022, 01:00:00 Last updated by source: 4 Oct 2022, 15:20:06
Scores DDoS - Fraud - Hack 30 Leak - Malware 67 Phishing 69

□ THREAT: http://47.242.39.92
URL: http://47.242.39.92
First seen: 28 Sep 2022, 14:18:55 Last updated by source: 30 Sep 2022, 23:34:37
Scores DDoS - Fraud - Hack 29 Leak - Malware 33 Phishing 33

□ THREAT: 103.9.76.208
IP: 103.9.76.208
First seen: 10 Jan 2022, 01:00:00 Last updated by source: 4 Oct 2022, 15:20:06
Scores DDoS - Fraud - Hack 30 Leak - Malware 67 Phishing 69

□ THREAT: c8c907a67955bcdf07dd11d35f2a23498fb5ffe5...
File: c8c907a67955bcdf07dd11d35f2a23498fb5ffe5c6b5d7f36870cf07da47bff2
First seen: 30 Sep 2022, 01:54:56 Last updated by source: 4 Oct 2022, 15:20:06
Scores DDoS - Fraud - Hack - Leak - Malware 100 Phishing 50

Scanning set up

Vulnerability scans run for Managed Vulnerability Scanning customers.

Day 2

1st Exploit discovered

Intelligence team advises an exploit is available and used “in the wild”.

updates

Signal published & operations take over to protect MSS customers

World Watch report published, and operations teams notified.

Rapid analysis

Potential attack vectors analyzed for quick detection.

Threat hunt launched across client estates.

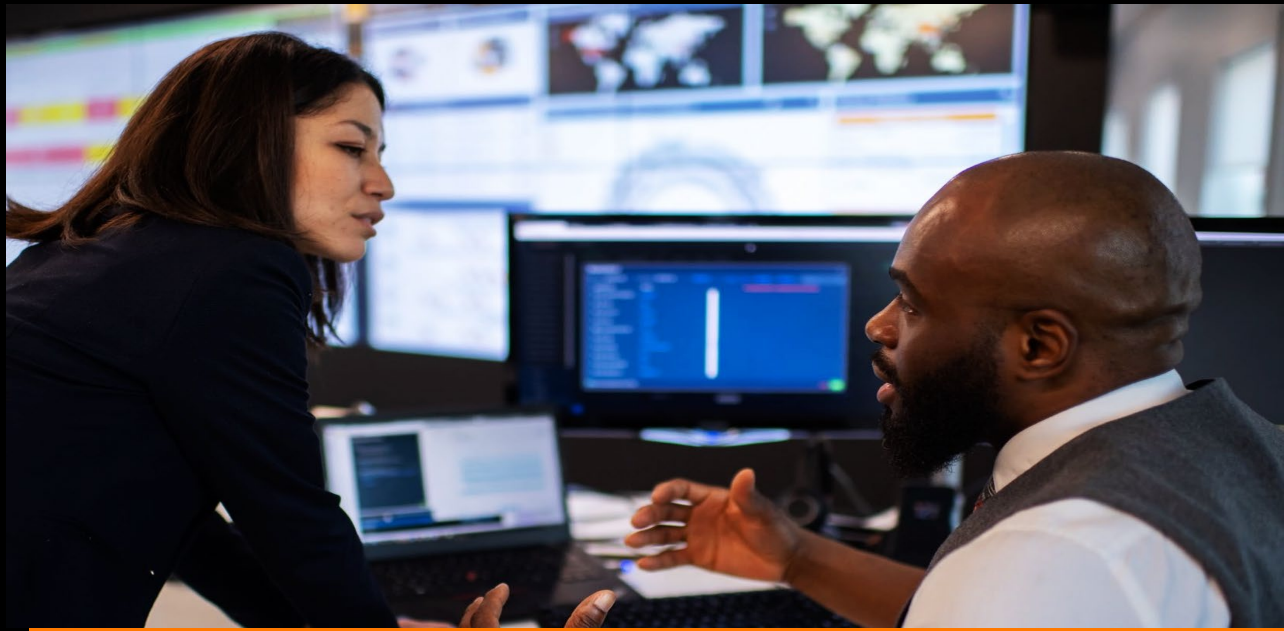
Day 3

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

We enable organization with proactive protection and faster response

- Proprietary threat use-cases, response playbooks and embedded threat intelligence.
- In-house CSIRT / CERT, malware analysis, proprietary 3rd-gen sandbox and Signal Intelligence lab.
- Threat Alliances with key Vendors, Governments and International Organizations.
- Monitoring of IT, OT and Cloud environments



Intelligence-led security for your advantage

Our security approach is driven by our knowledge of the threat,

and allows you to make the right decisions.

So you can…

…demonstrate security ROI.

…adopt appropriate solutions and services.

…accurately detect current campaigns.

…manage relevant, current threats.

Our intelligence, your advantage.

Orange Cyberdefense

Build a safer digital society.