Know yourself

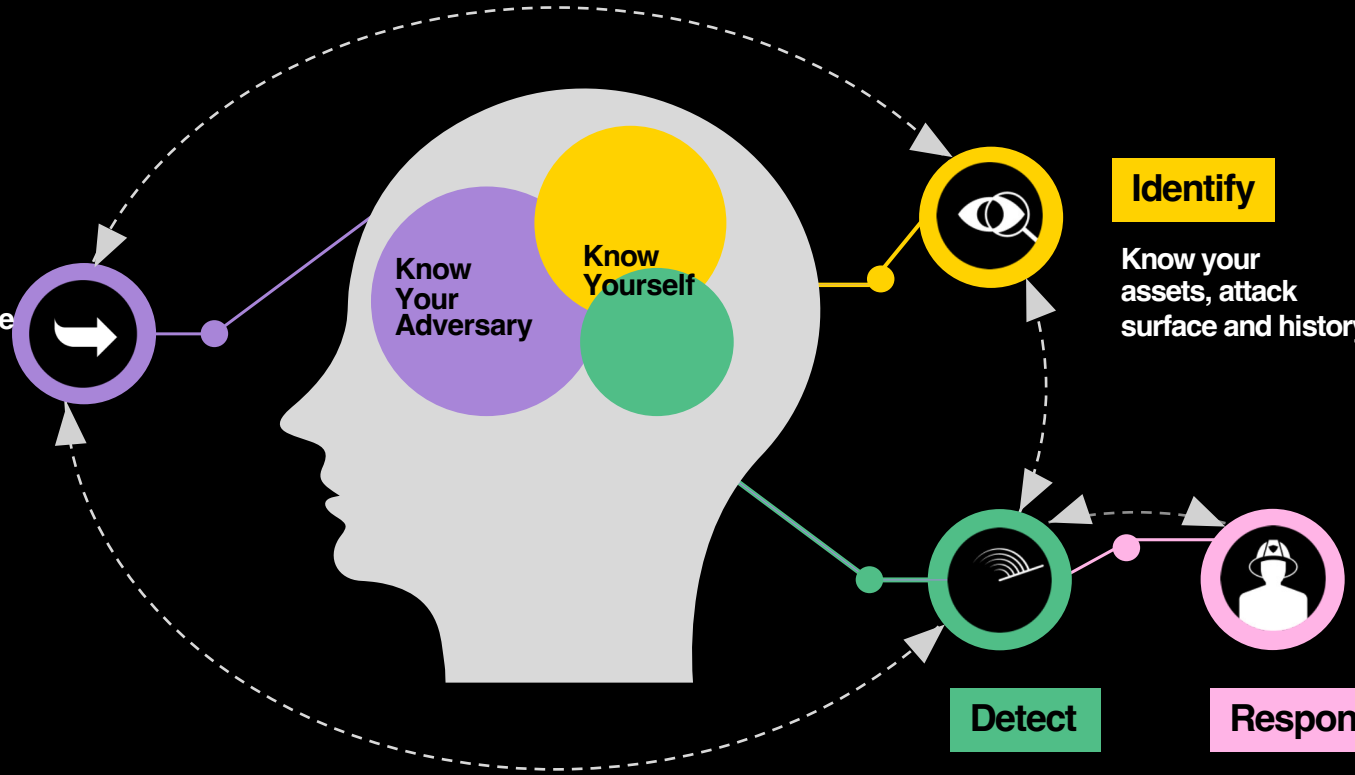
Strategies employed for understanding the attack surface

Grant Paling
Product Manager

orange™ Cyberdefense

Hello!

Intelligence-led security requires two perspectives



Anticipate

Observe the landscape – Vulnerabilities, Threats & Attacks

Identify

Know your assets, attack surface and history

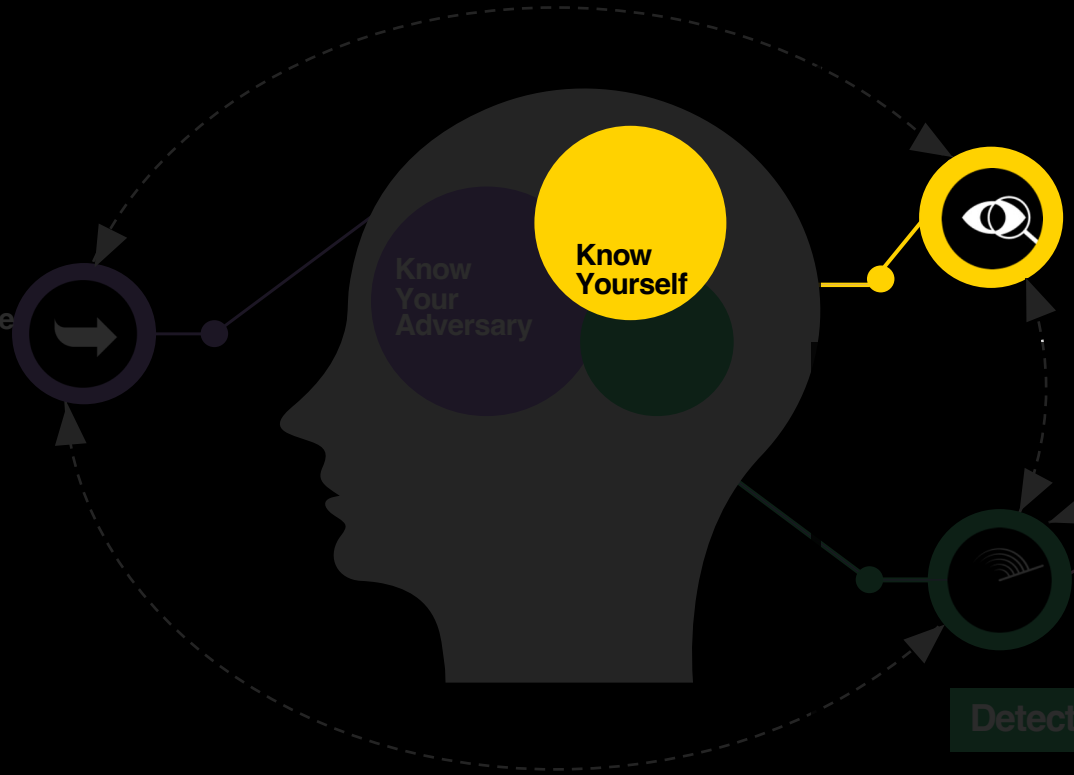
Detect

Detect vulnerabilities & active attacks

Respond

Engage with attacks in progress

The weakest link



Anticipate

Observe the landscape – Vulnerabilities, Threats & Attacks

Identify

Know your assets, attack surface and history

Detect

Detect vulnerabilities & active attacks

Respond

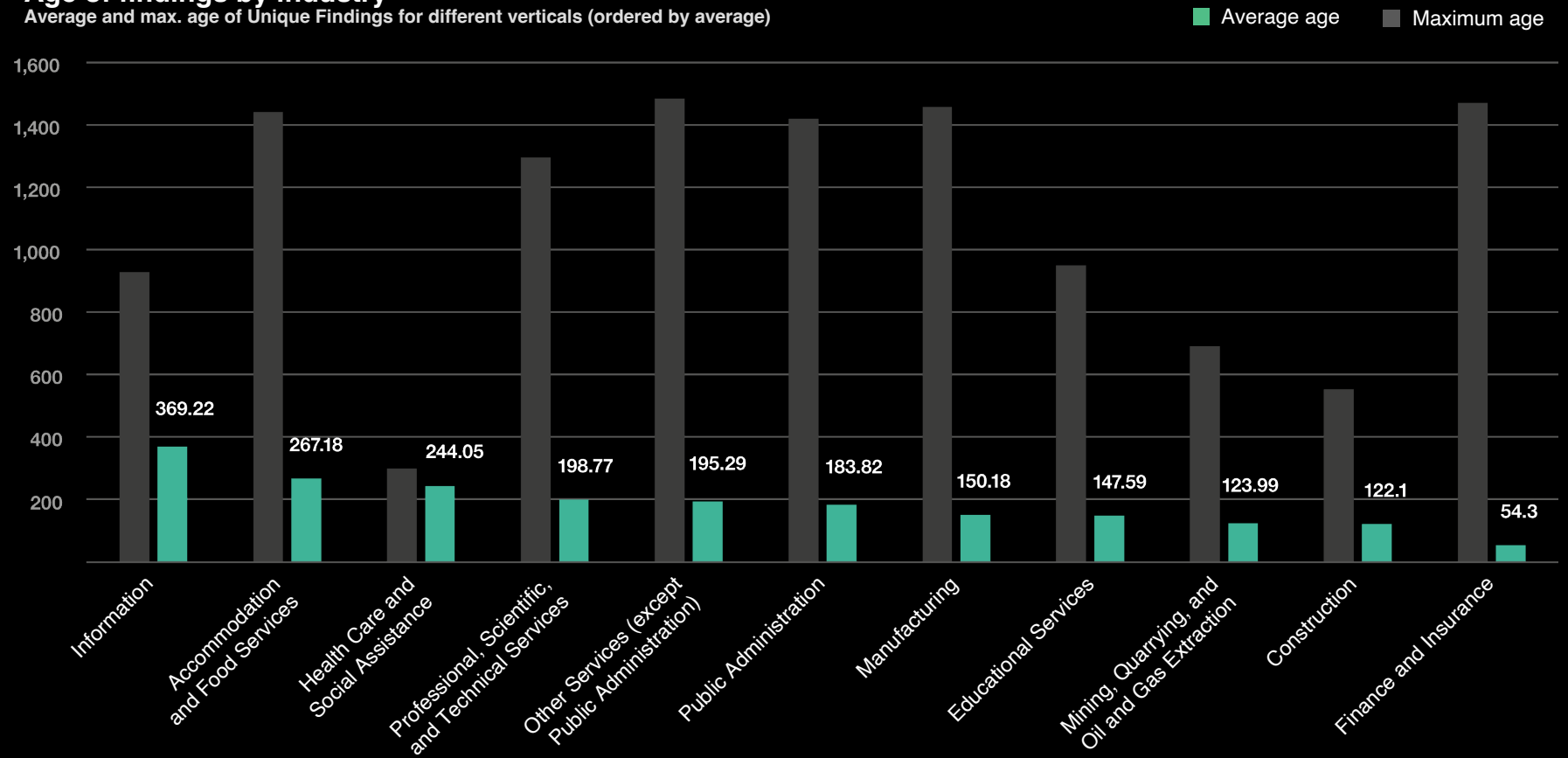
Engage with attacks in progress

Same stuff, different year

The problem is clear, how to solve it is not

Age of findings by industry

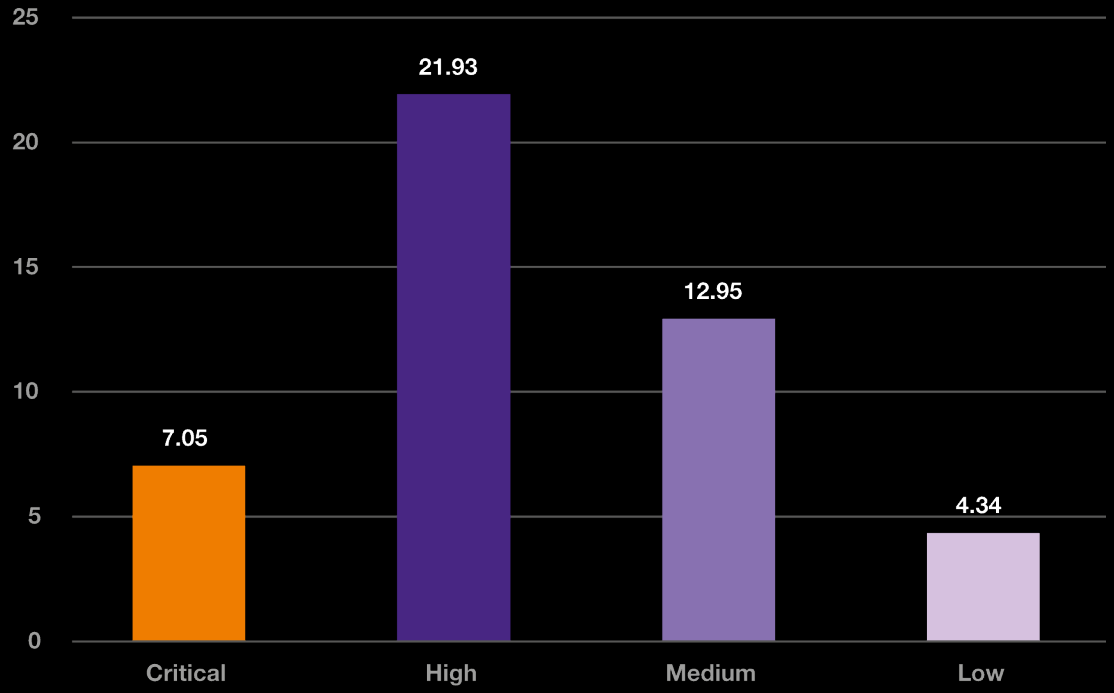
Average and max. age of Unique Findings for different verticals (ordered by average)

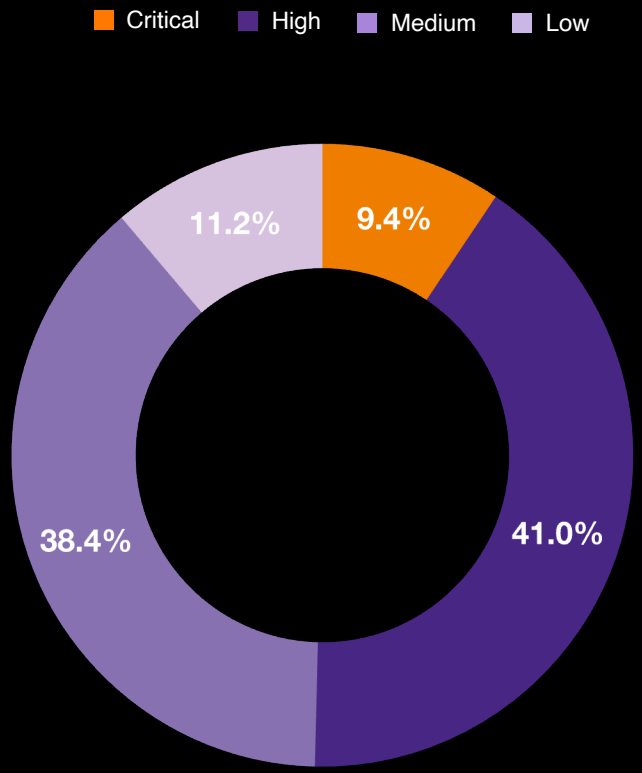


Source: Orange Cyberdefense Security Navigator 2024

Severity of findings

Average findings per unique asset and total severity distribution





Let us sidestep
for a moment…

Orange
Cyberdefense

Incident Response War Story

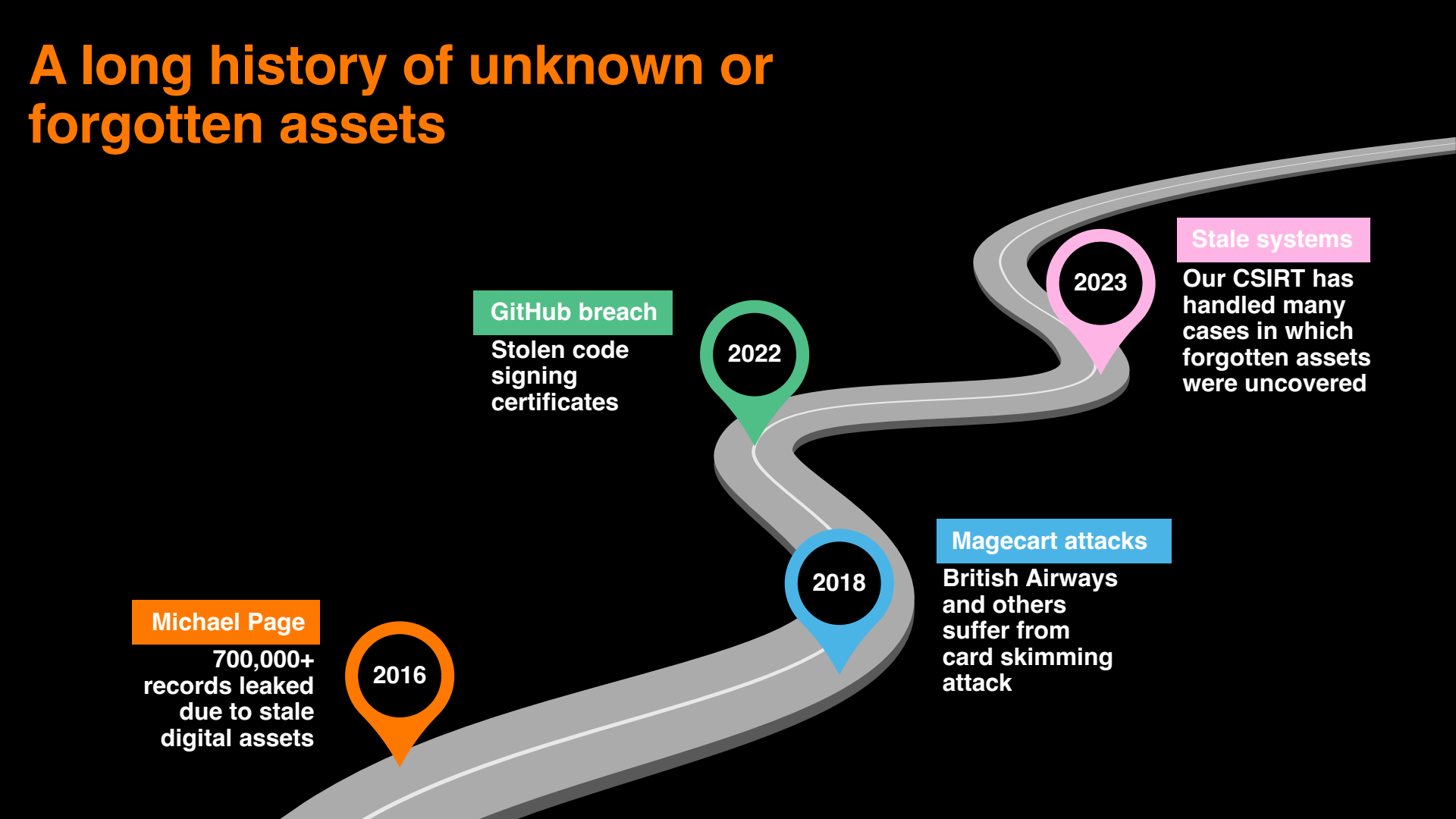
Friday evening just about to pour a beer when….

Case Overview

- Information passed by Interpol from a seized attacker server which contained the output for the clients Active Directory.
- Immediate containment of the affected Domain.
- Cobalt Strike Beacons not one but two on the Domain controllers and servers.
- Found the insecure Citrix gateway that was the initial point of entry.

Cyberdefense

A long history of unknown or forgotten assets



The expansion of the problem

"I don't know what to patch first."

"I don't have a unified view of my riskiest assets."

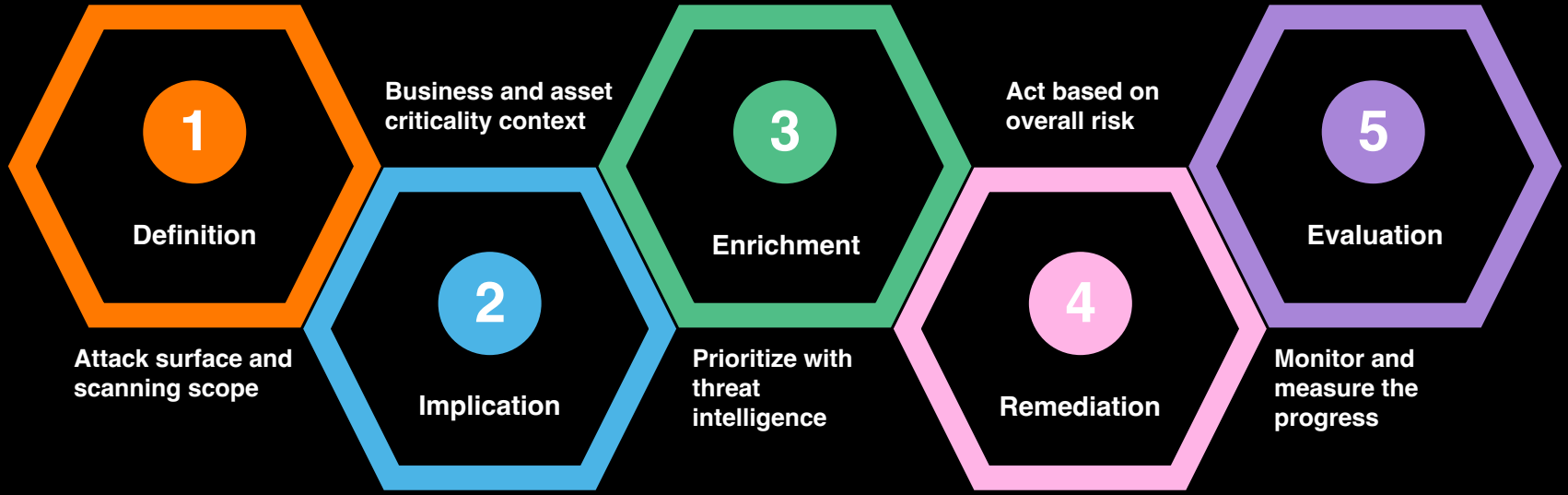
"I'm not even sure I know that I have visibility of all my assets."

Business context and threat intelligence correlated to focus on the real organizational risk

Factors affecting the risk score

Our approach

How to embrace risk-based vulnerability management



30%

What am I going to do?

How should you do it?

Who you think you are, your alias's and your history, … The Full Picture

Scan the internet for Every Asset linked to you

Aggregate and augment to discover your True Attack Surface

Cyberdefense

Inside our Vulnerability Operations Center

Going above and beyond for our customers

Zero-Day for Cisco IoS XE

Remote code execution capabilities, potentially thousands of exposed instances. Massively exploited in the wild.

16/10/2023

17/10/2023

Asset enumerations conducted

Complete threat analysis report pushed out to all Orange Cyberdefense customers. Script developed and run by our CERT to identify exposed devices.

High-risk targets identified

No patch available and 34k devices potentially compromised. Scanning results are shared with customers. Going beyond scanning to ensure the risk was identified and mitigated ***fast***

18/10/2023

Use case - Ivanti

Ivanti Connect Secure VPNs are used for remote work: these software are widely used by large corporations and for extensive usage. In January 2024, the products have been compromised for **espionage attacks** by an advanced **Chinese Nation-state threat actor**.

27 000 exposed assets have been identified when vulnerabilities were published.

Cyberdefense CERT

The CERT Orange Cyberdefense has been able to quickly identify vulnerable assets, scanning internet looking for specific patterns. **670 organizations have been identified** and, from case to case, **notified diligently**.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

DARKReading

The Hacker News

HELPNET SECURITY

Notifications led us to carry out **19 incident response missions**, for customers and non-customers, and **reinforced our position as an expert** within Infosec communities.

Knowing yourself is about balance

Fighting immediate threats
whilst proactively reducing risk

Knowing Yourself

Understanding your attack surface