Orange
Cyberdefense

Improve the effectiveness of your vulnerability management strategy

Jesper Madsen – Head of Vulnerability Operations Center Sweden

orangecyberdefense.com

The attack surface continues to grow and diversify…

26 500+

new vulnerabilities in 2023

25000+ in 2022

19000 in 2021

18000 in 2020

80% are patched in +30 days*

* Security Navigator 2023

The attack surface continues to grow and diversify…

…so where do we start?

Context is key

26 500+

new vulnerabilities in 2023

CISA Known Exploted Vulnerabilities

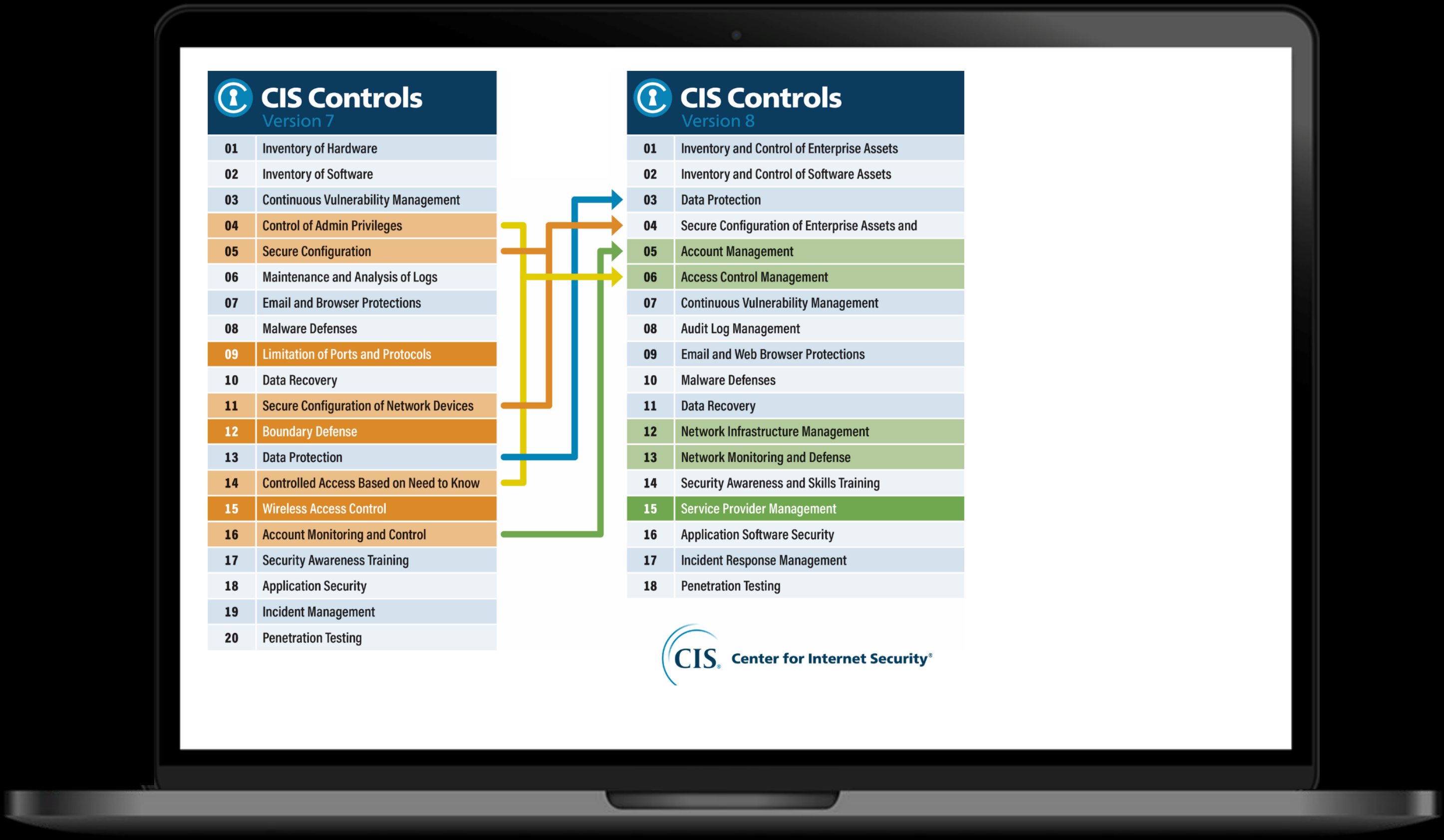
1114

Incident response story

- 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.

“That’s impossible because we don’t have any Citrix…”

Same stuff, different year. Why is this still so hard?



CIS Controls
Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS. Center for Internet Security®

Challenges

- Volume of vulnerabilities
- Prioritization
- Patching
- Resourses
- Complex IT environment
- Lack of visibility
- Threat intelligence
- Organisation culture

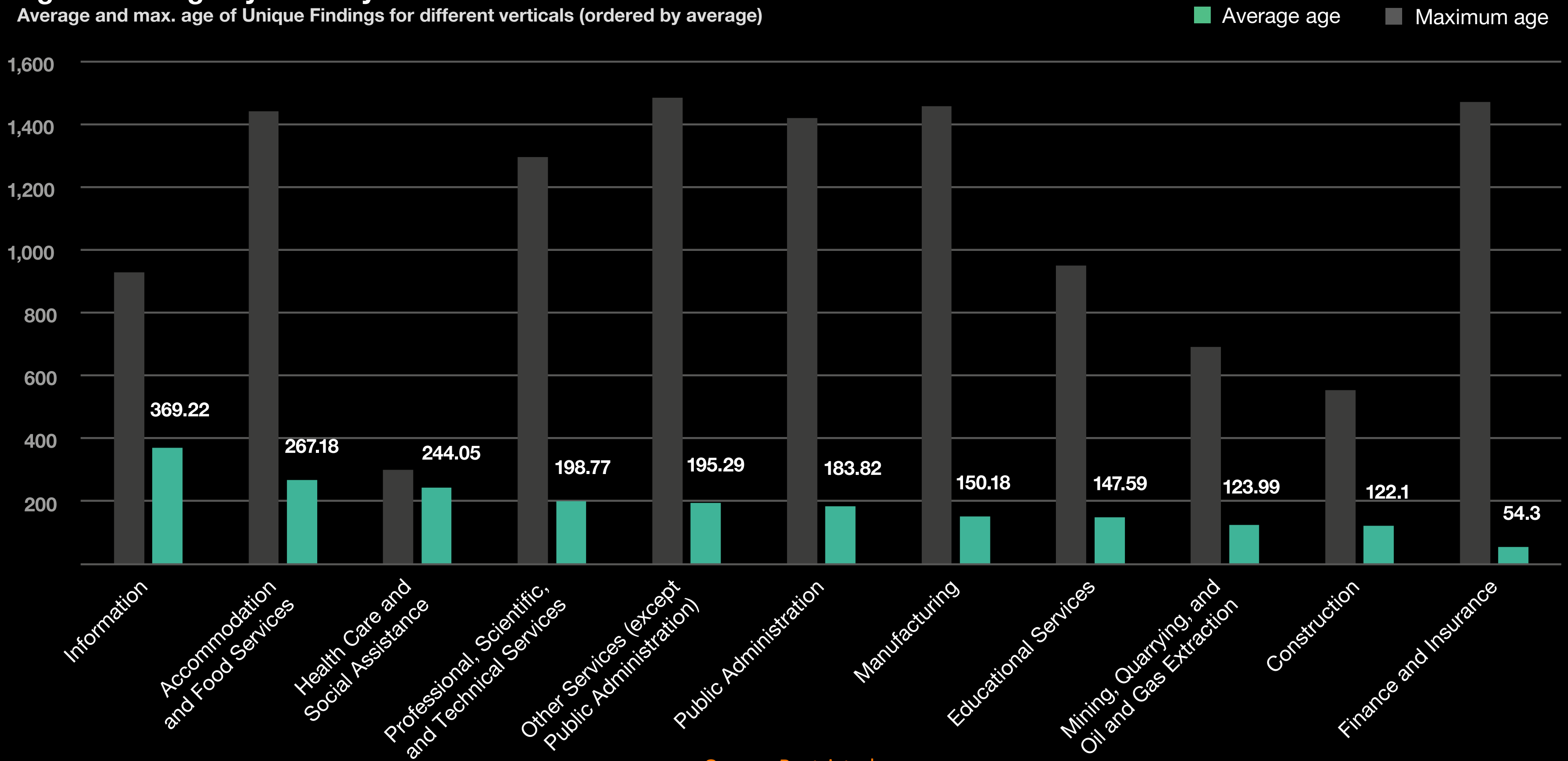
Common misconceptions

- We will find too much if we scan everything – lets start small
- We need to patch all vulnerabilities before we scan again
- Automated patching solves all vulnerabilities
- Vulnerabilities are only ITs problem
- Windows is most vulnerable so let’s run mac and be safe
- The high CVSS vulnerabilities are our highest priority

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)



Orange Restricted

Source: Orange Cyberdefense Security Navigator 2024

Overcoming the challenges

Continuous Asset discovery and Vulnerability scanning

Risk based Prioritization

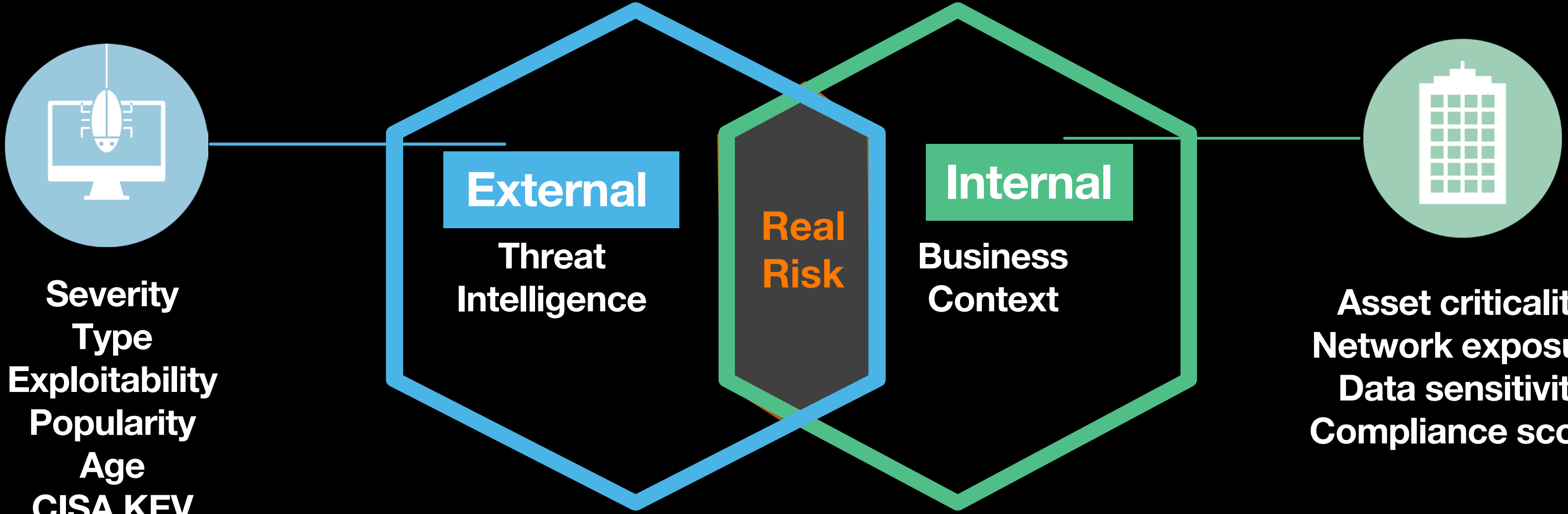
Patch management strategy

Visibility for correct stakeholders

Communication

Threat intelligence

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



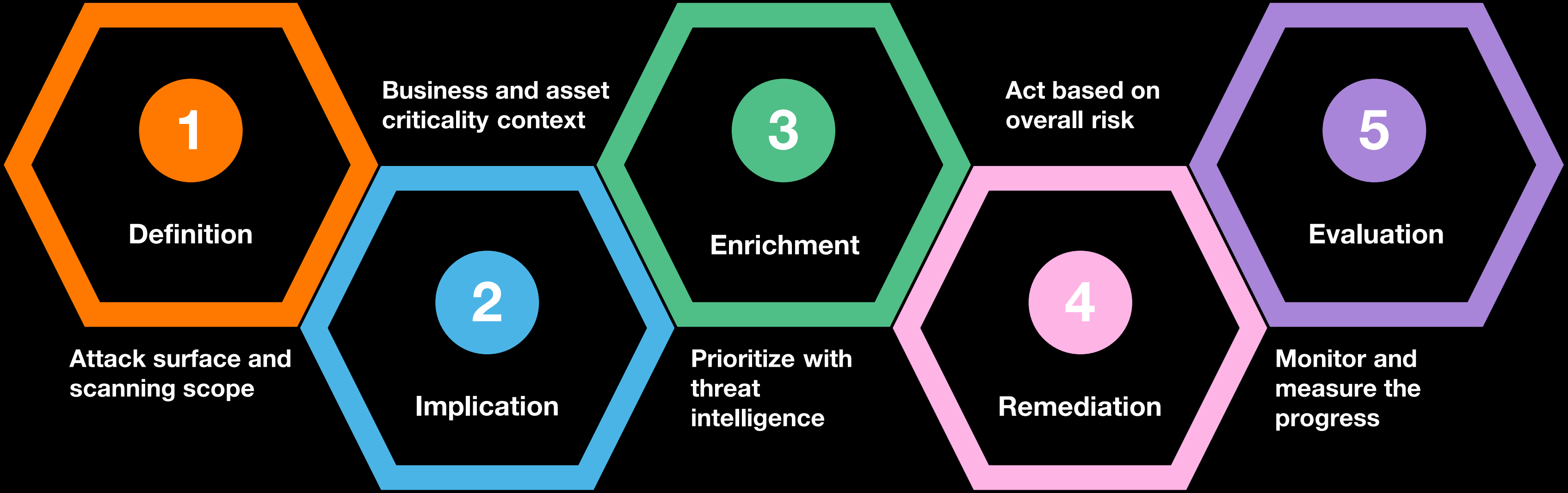
Severity
Type
Exploitability
Popularity
Age
CISA KEV
Prediction - EPSS

Asset criticality
Network exposure
Data sensitivity
Compliance scope

Factors affecting the risk score

Our approach

How to embrace risk-based vulnerability management


1
Definition
Attack surface and scanning scope
2
Implication
Business and asset criticality context
3
Enrichment
Prioritize with threat intelligence
4
Remediation
Act based on overall risk
5
Evaluation
Monitor and measure the progress

Overcoming the challenges

Strategic importance

- Get everyone on board
- The threat is against the organisation
- Advocate for change
- Understanding the risk

Conclusion

Visibility

1

Knowing what you have is half the battle. If you don’t see it, you can’t do anything about it.

Tools

2

Make sure your tools use risk values and combine internal and external factors to help you make data driven decisions.

Remediation

3

Fix your highest risks first. Then work your way down.

It’s never to late to start

4

Even if you have never made a scan, you can still start today, and go fix your top risks regardless of how many vulnerabilities you have.

Check your environment!

SCANNING SCHEDULES AND SCOPE

PATCH MANAGEMENT ROUTINES

ORGANISATIONAL AWARENESS

STAKEHOLDER VISIBILITY

THREAT INTELLIGENCE

Make sure to

Know yourself

Orang Cyberdefense Live

Register as an early bird to seize your chance to **win** one of **5 Shokz** headphones.

SHOKZ

Register as an ealry bird

Orange Cyberdefense