Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Moving from Vulnerability Management to Continuous Threat Exposure Management - A Carbery and IADT Use Case

Matt Quinn
NEUR Technical Director, XM Cyber

Brian Martin
Director of Product Management, Integrity360

#SecurityFirstStockholm

XM Cyber

Moving from Vulnerability Management to Continuous Exposure Management

A Carbery and IADT Case Study

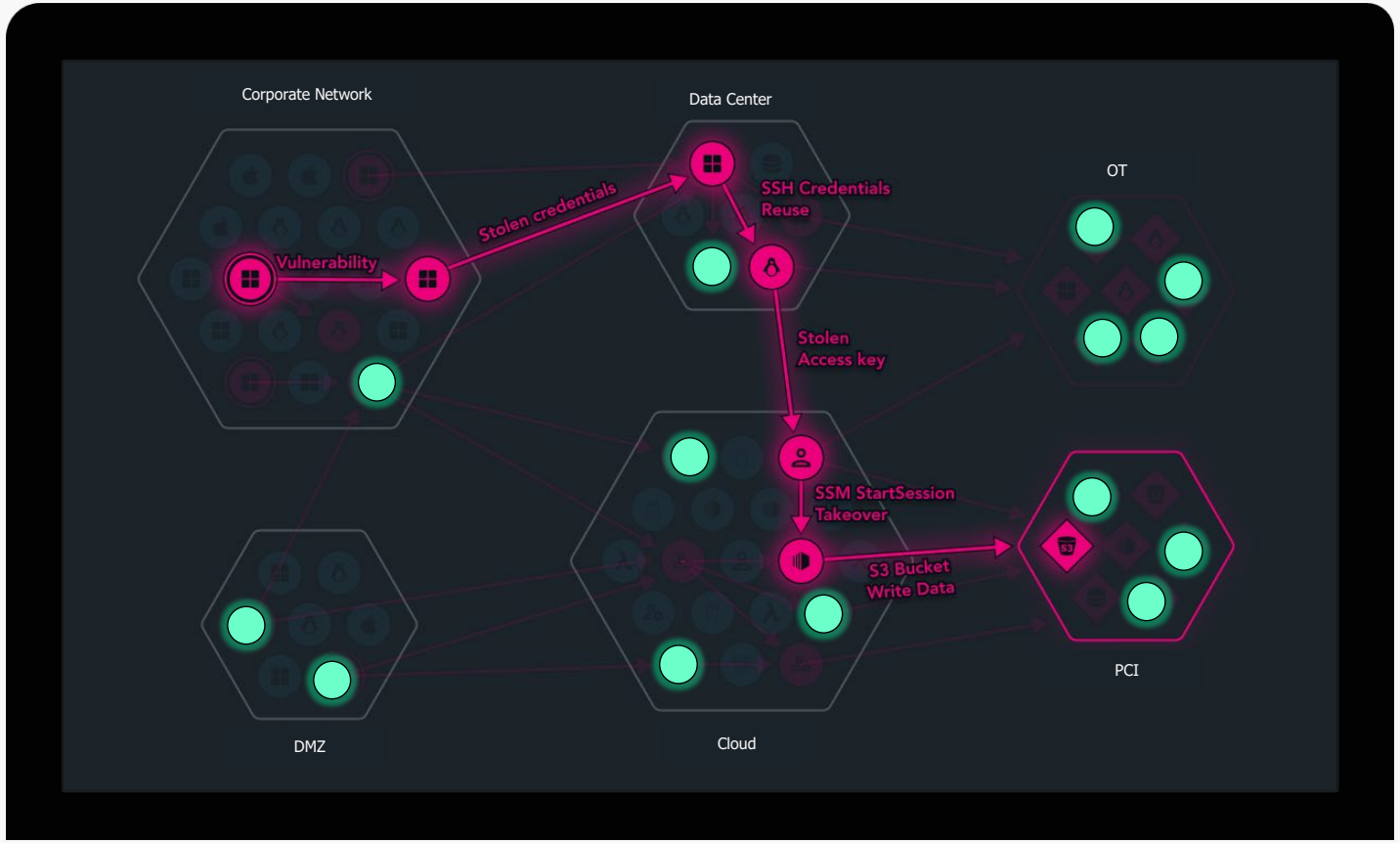
Attackers Evading Detection, Forcing Reliance on Posture

Bypass EDR & other controls

Exploit mix of CVEs, misconfigs & identities

Move laterally across hybrid environments

Gives advantage to attackers



Remediation effort completed

Overwhelming lists of exposures–can't fix them all

Siloed technologies for different environments

Don't know where most vulnerable to attack

Busy fixing the wrong things

75%

of exposures aren’t on attack paths to an organisation’s critical assets… yet organisations are still focusing on fixing these

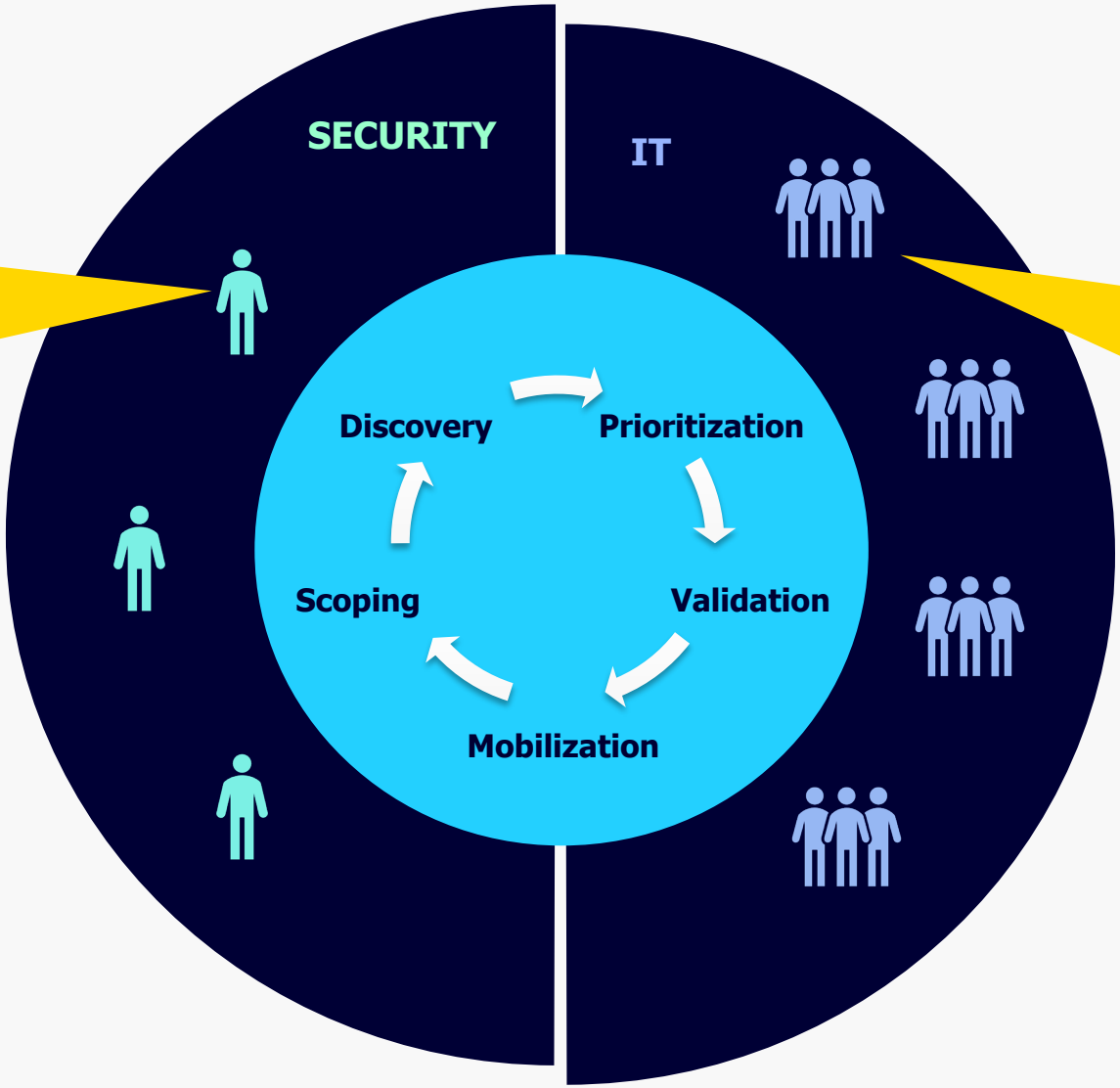
2024 State of Exposure Management Report, XM Cyber

XM Cyber

Disconnect Between Security & IT

Nobody Wins & Unnecessary Business Risk Remains

Security struggles to get IT to complete remediations given lack of clear justification



IT frustrated by never ending and growing lists of tasks that lack clarity on risk impact

- Can't secure business at the pace it's moving
- Highly inefficient and unscalable model
- Problem is getting worse!

XM Cyber

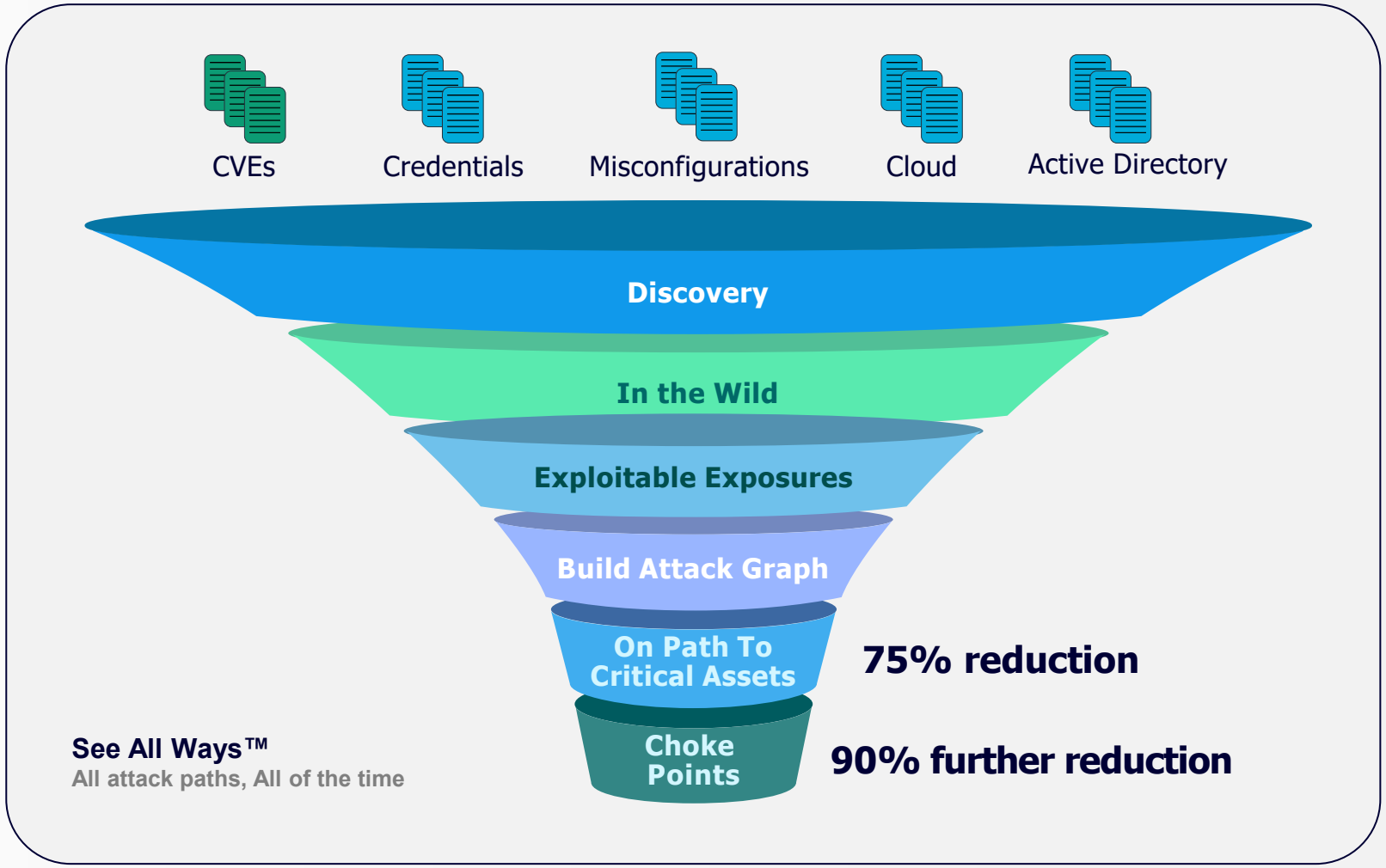
More Coverage, Smarter Prioritization, Fewer Fixes

Automated Discovery of How ALL Exposures Come Together To Put Critical Assets At Risk

- Long lists of only CVEs
- No attack path insight

Red Team, Pen-Test & BAS tools

- Limited attack path insight
- Not comprehensive, continuous or safe



XM Cyber

A Smarter Approach – Attack Graph Analysis™

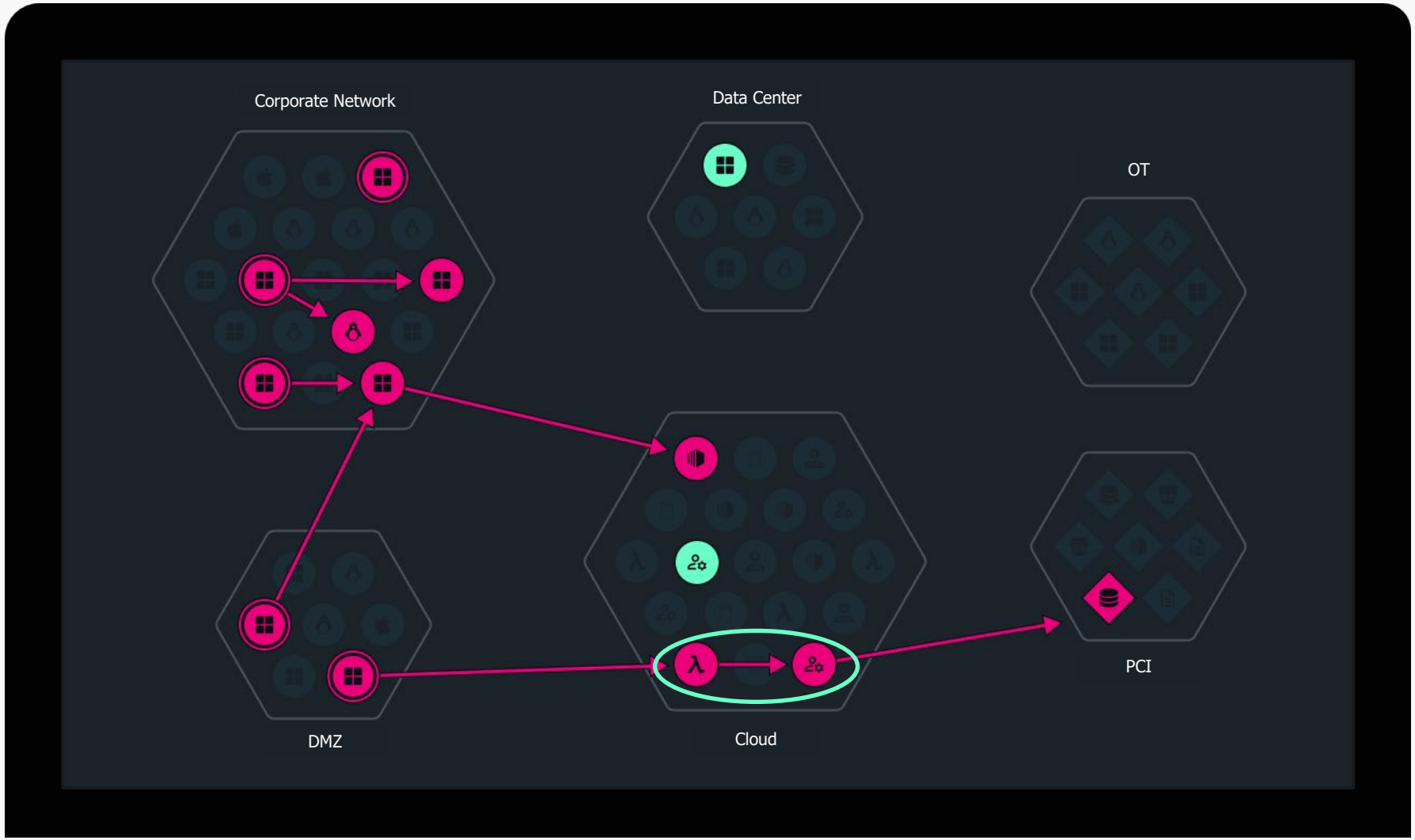
Identify **all attack paths** to business-critical assets

Enable remediation focus on **Choke Points,** not Dead Ends

Provide contextual, **guided remediation options**

Fix Less.

Prevent More.



XM Cyber

Organisations can practically eliminate all attack paths to critical assets by remediating

just 2%

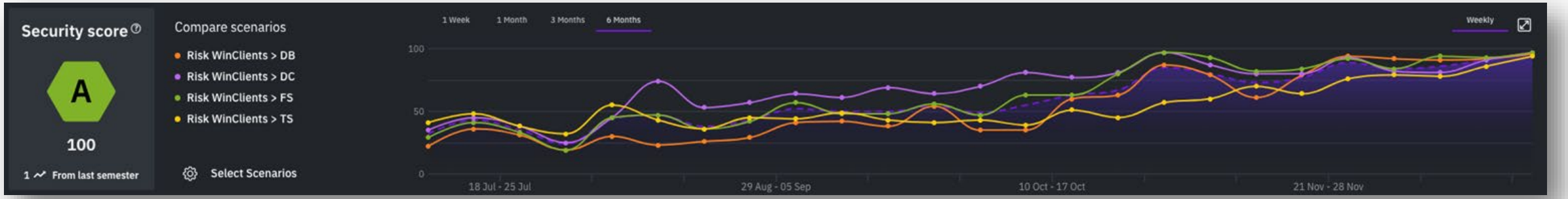
of exposures that lie on choke points.

2024 State of Exposure Management Report, XM Cyber

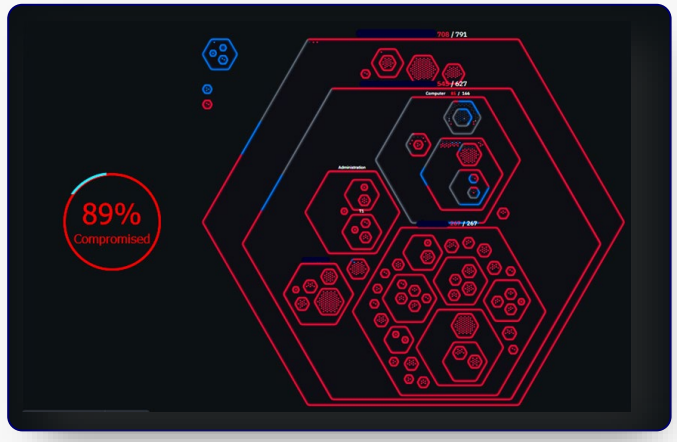
XM Cyber

Case Study: Fast, Demonstrable Risk Reduction

30,000 employee company goes from F (34) to A (100) in 4 months



Example step in the journey: Ransomware scenario resolved in 1 day



BEFORE

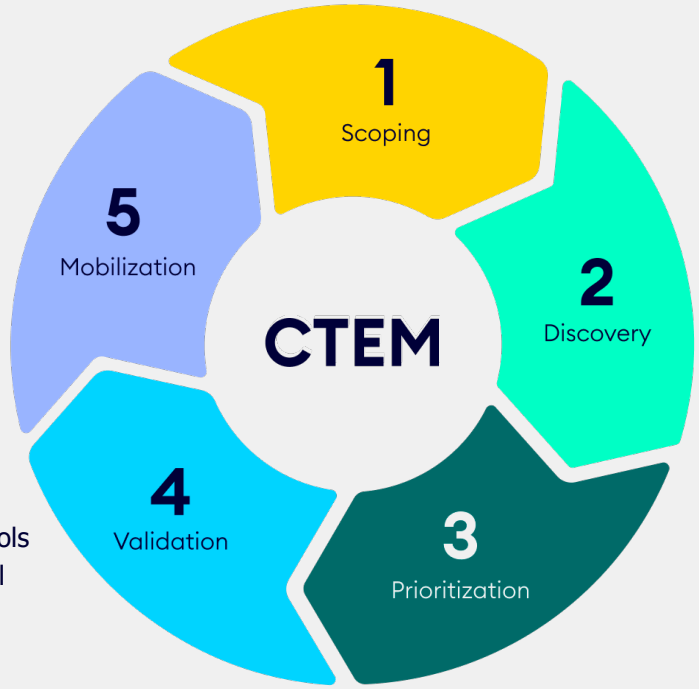
- Choke point on internet-facing file server
- 2 cached privileged credentials
- EDR not running, although installed

AFTER

XM Cyber

Operationalize Ongoing Risk Reduction

Enables Continuous Threat Exposure Management



1 Scoping
- Align scenarios to threat landscape
- Understand critical assets & environments

2 Discovery
- Discover CVEs, misconfigurations, cloud, identity risks, etc.
- Across hybrid cloud environment
- Compile attack graph

3 Prioritization
- Prioritize threats 'in the wild'
- Holistic understanding of attack surface
- Map attack paths to critical assets

4 Validation
- Discover exploitability
- Understand compensating controls
- Identity choke points and critical attack paths

5 Mobilization
- Align security risks with IT remediation options
- Remediation guidance
- IT ticket integration
- Track remediation progress

SaaS Delivery & Managed Service

Enable business to operate securely with a scalable process

Answer "Where are we most vulnerable and what's being done?"

Foster Security & IT team alignment and efficiencies

Free up resources wasting time on the wrong fixes

XM Cyber

Accelerating Security Initiatives

OPERATIONAL

- Ransomware Readiness
- CVE Prioritisation
- SOC Efficiency
- OT Security/ Segmentation

BUSINESS

- Digital Transformation & Cloud
- Cyber Risk Reporting/ Compliance
- Supply Chain & 3rd Party Risk
- Mergers & Acquisitions

XM Cyber

Carbery

Challenge:

- Carbery Group split across Carbery and Synergy subsidiaries in Ireland and US (M&A)
- Risks from IT to OT/Manufacturing (OT)
- Shared infrastructure across the businesses
- On-prem and Cloud environments (Cloud Transformation)
- Agile business, rapidly changing (Continuous)

Solution:

- XM Cyber deployed across On-Prem, AD and Cloud
- Choke Points identified and resolved across on-prem issues between businesses including segmentation
- Risks to Manufacturing eliminated
- Hybrid On-prem to Cloud risks eliminated

Impact / Value:

- Improved cyber resilience to protect manufacturing and intellectual property that are key to keeping Carbery operational
- Measurable reduction in risk

IADT

Challenge:

- Small team looking after a large complex campus environment (SOC Prioritisation)
- Student and Lecturer environments, 2500 students, 350 staff
- 3rd party access (3rd party risk)
- Student medical data

Solution:

- XM deployed across on-prem and AD
- Prioritized choke points based on IADTs most critical systems that keep them running, or have critical student data

Impact / Value:

- Improved segmentation and resilience based on XM Cyber attack simulations
- Eliminate risk from 3rd party access
- Patch and CVE prioritisation based on exploitability, not just vulnerability (CVE Prioritisation)

Key Takeaways

What to consider on your CTEM journey

01 Widen the scope

- Exposure goes beyond CVE
- Look across CVEs, Misconfigurations, AD, Cloud, Network to get a true understanding of posture

02 Look at Cloud from all angles

- "Cloud" is not all Lambda functions and K8s
- Lift & Shift created "double bubble" risks
- VMs exist in Cloud with network connectivity to On-prem
- Domain joined VMs, AWS AD Service
- IAM attacks, Kubernetes

03 Move to Continuous

- Have a process to review issues on a continuous basis, not just point in time
- Create relationships with the different teams that will remediate these issues, and give them context on the risk to operationalise

04 Quick Wins

- Focus on the quick wins that need the least amount of effort for largest reduction in risk
- Plan mid to long term improvements like network segmentation based on your findings, backed by risk

XM Cyber

Q&A

XM Cyber

Integrity360
your security in mind

Thank you

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

#SecurityFirstStockholm