

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

Matt Quinn

Technical Director NE, XM Cyber

Brian Martin

Director of Product Management, Integrity360



#SecurityFirstDublin



A Carbery and IADT Case Study



Attackers Evading Detection, Forcing Reliance on Posture

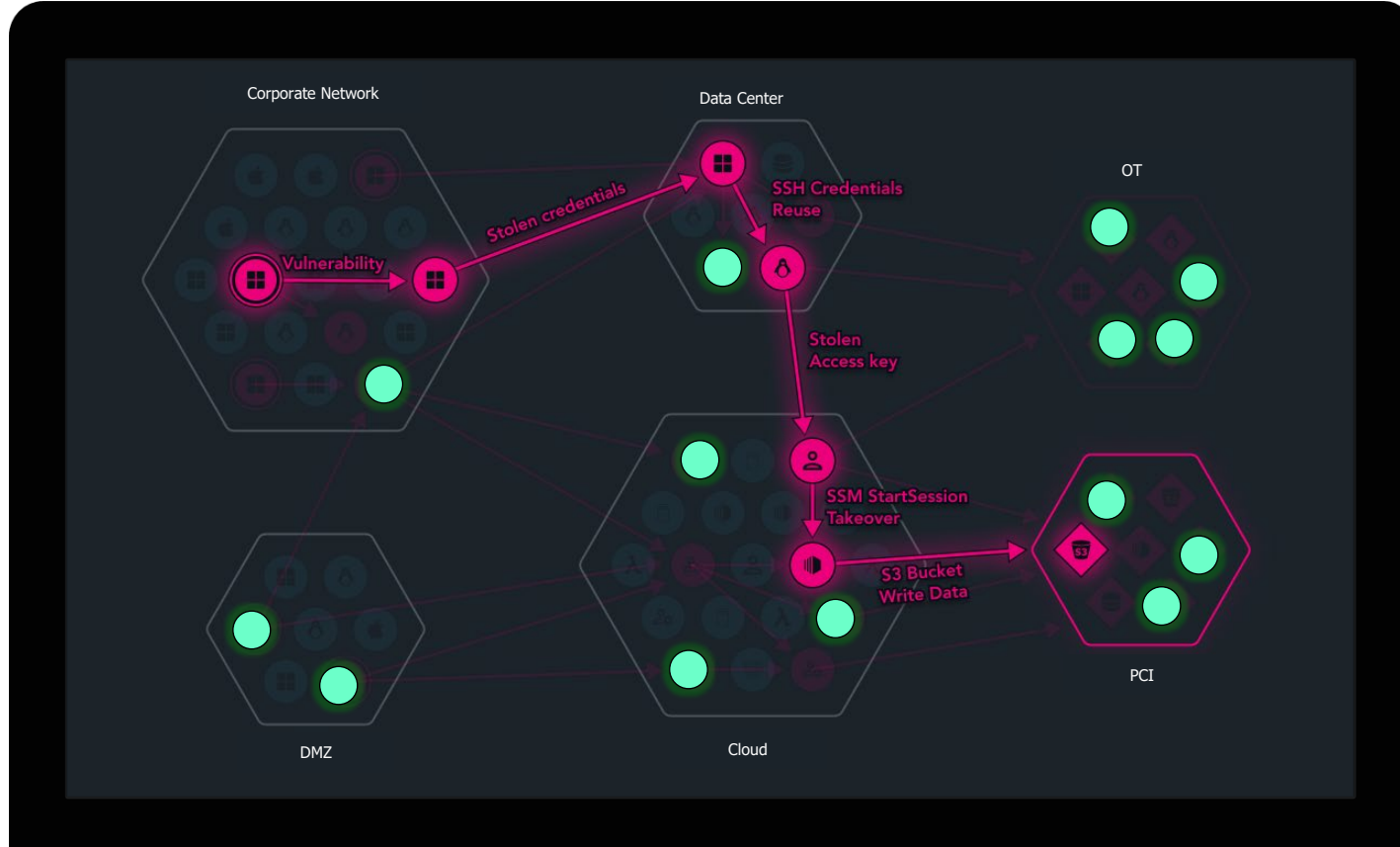


Bypass EDR & other controls

Exploit mix of CVEs, misconfigs & identities

Move laterally across hybrid environments

Gives advantage to attackers



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

 Remediation effort completed

75%

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

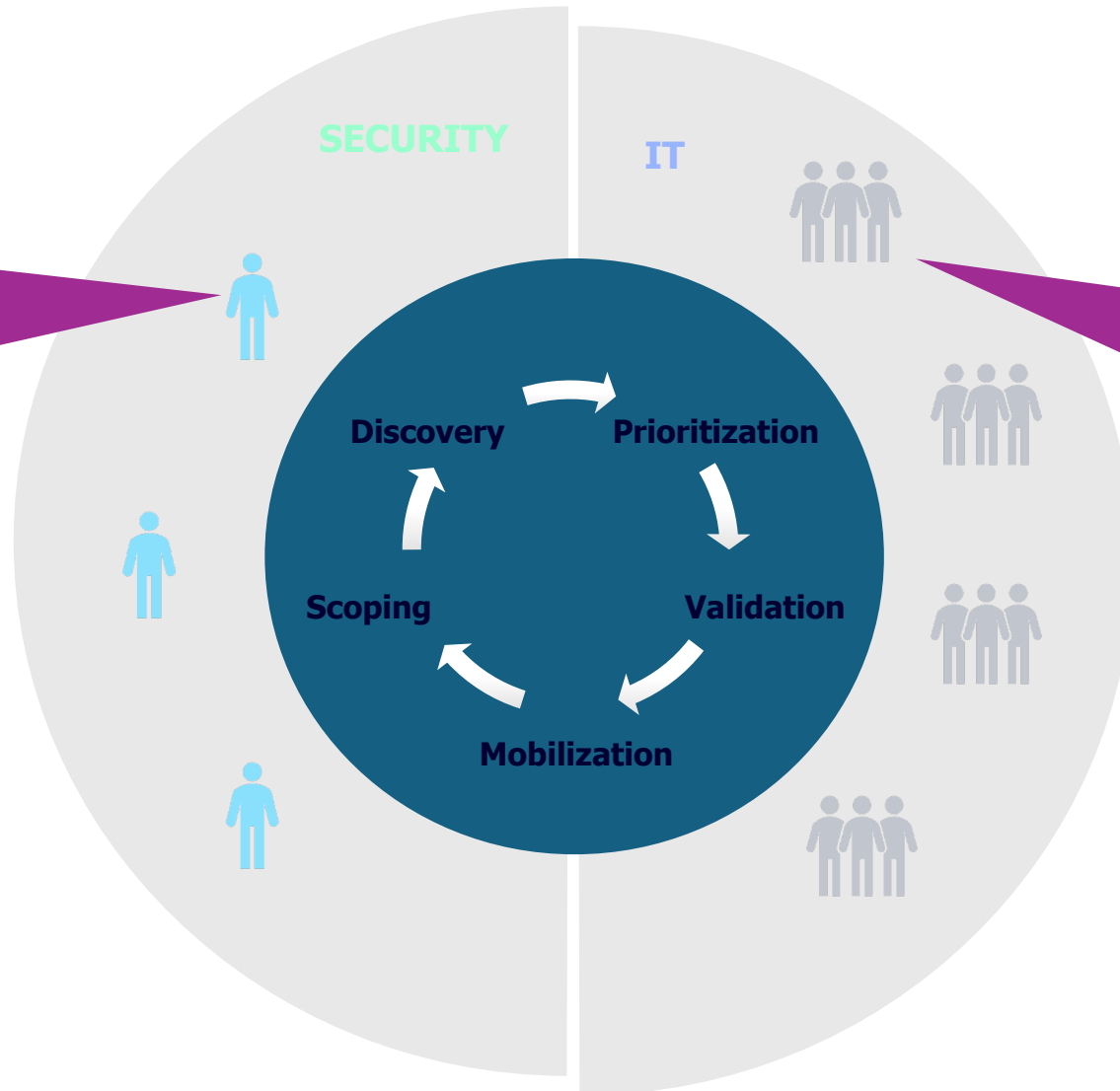
2024 State of Exposure Management Report, XM Cyber




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!



Vulnerability Management

CVEs



- Long lists of only CVEs
- No attack path insight



Red Team, Pen-Test & BAS tools

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



CVEs



Credentials



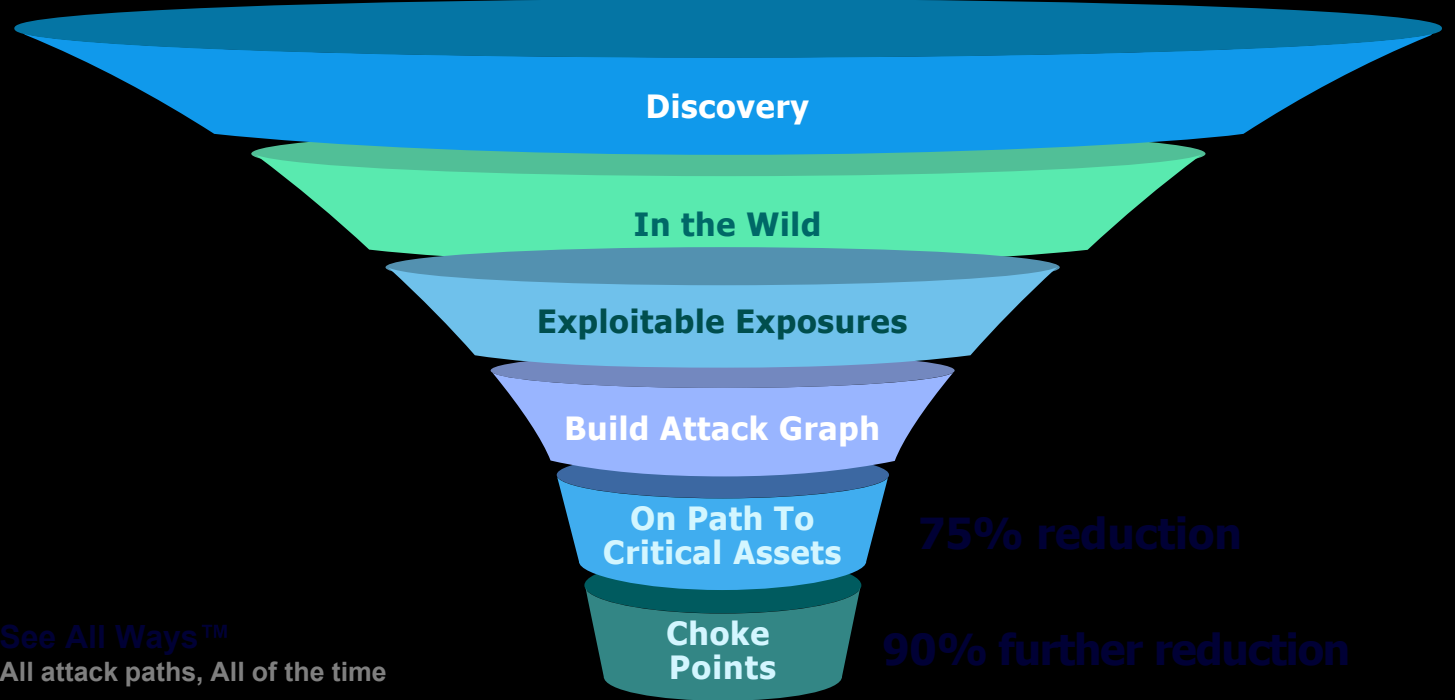
Misconfigurations



Cloud



Active Directory



See All Ways™
All attack paths, All of the time

75% reduction

90% further reduction

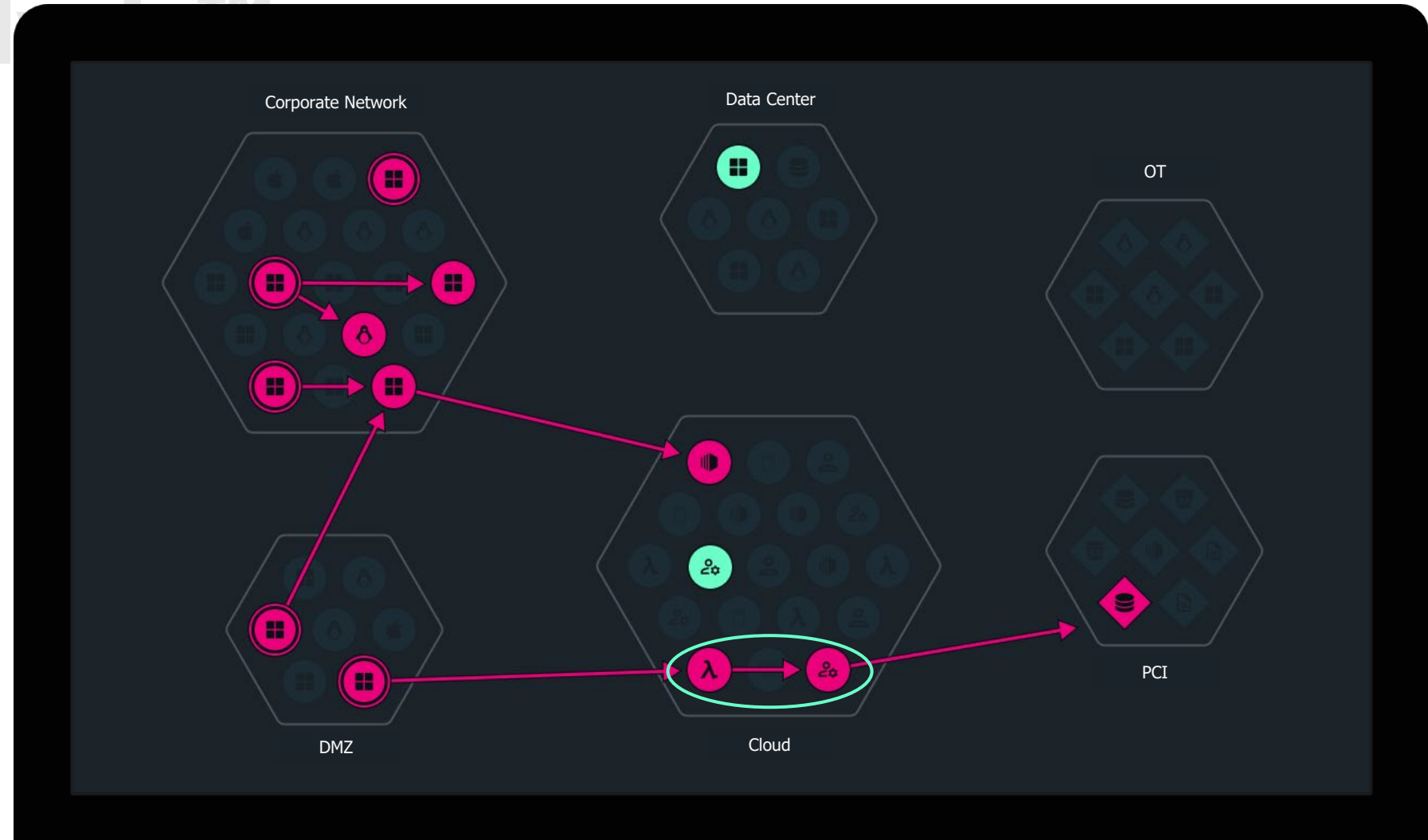
A Smarter Approach – Attack Graph Analysis

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.**



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

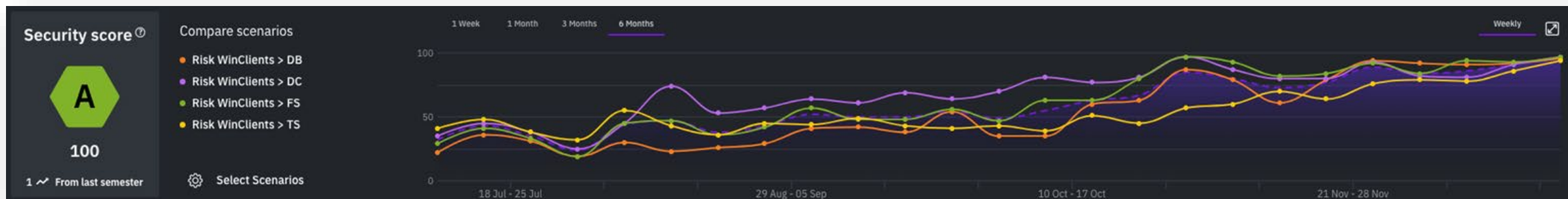
just 2%

of exposures that lie on choke points.

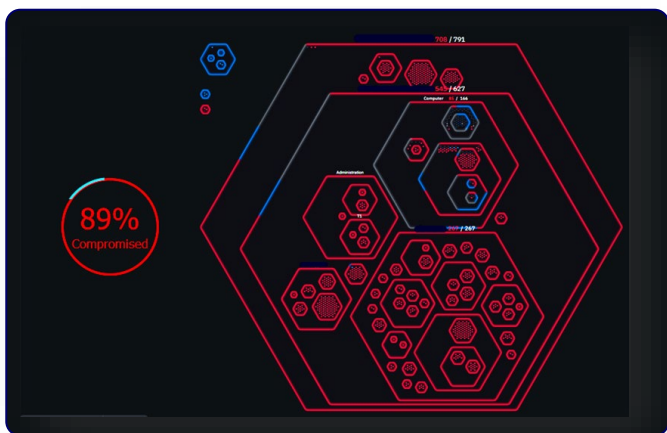
2024 State of Exposure Management Report, XM Cyber

Case Study: Fast, Demonstrable Risk Reduction

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

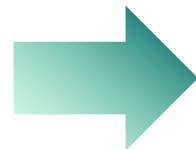


Example step in the journey: Ransomware scenario resolved in 1 day



BEFORE

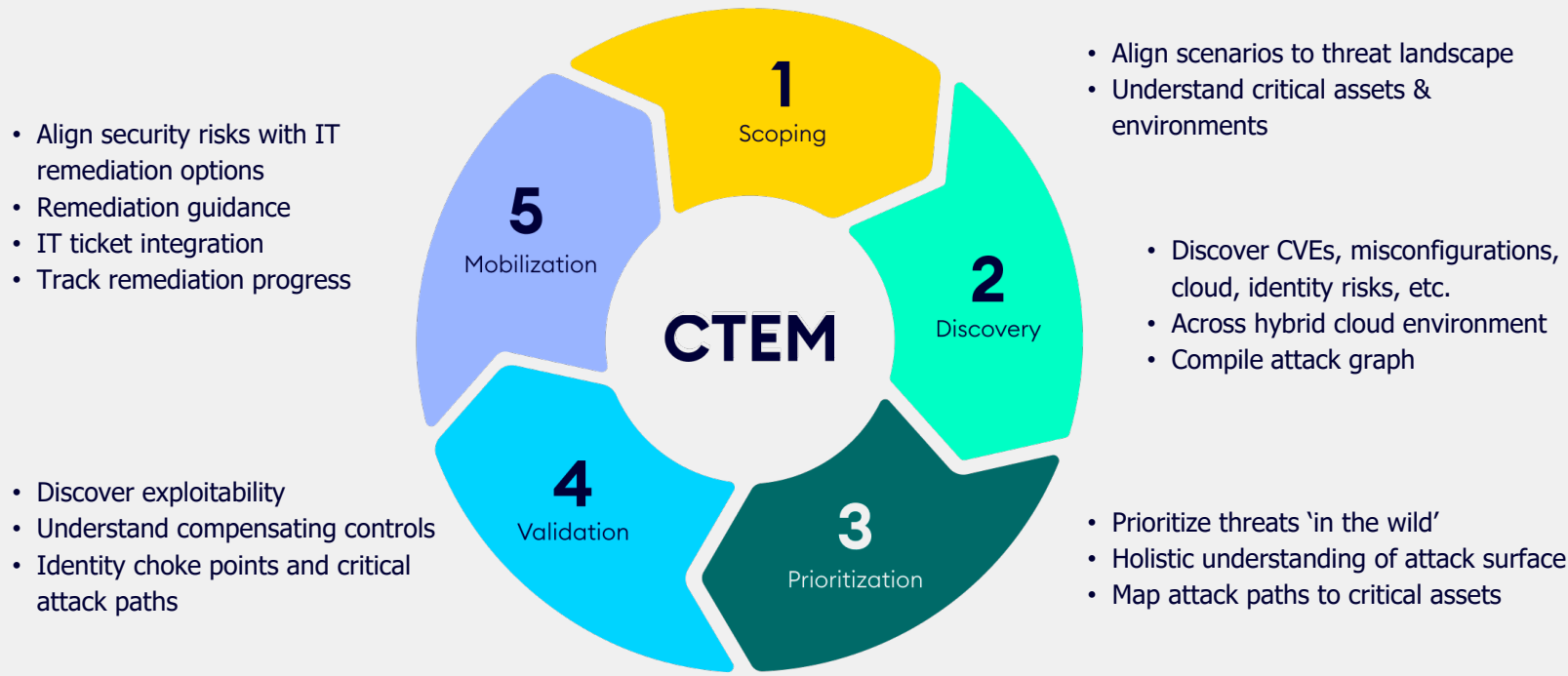
- Choke point on internet-facing file server
- 2 cached privileged credentials
- EDR not running, although installed



AFTER

Operationalize Ongoing Risk Reduction

Enables Continuous Threat Exposure Management



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

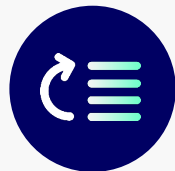
SaaS Delivery & Managed Service

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**

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



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



Q&A

Integrity360
your security in mind

Thank you

#SecurityFirstDublin

#SecurityFirstDublin