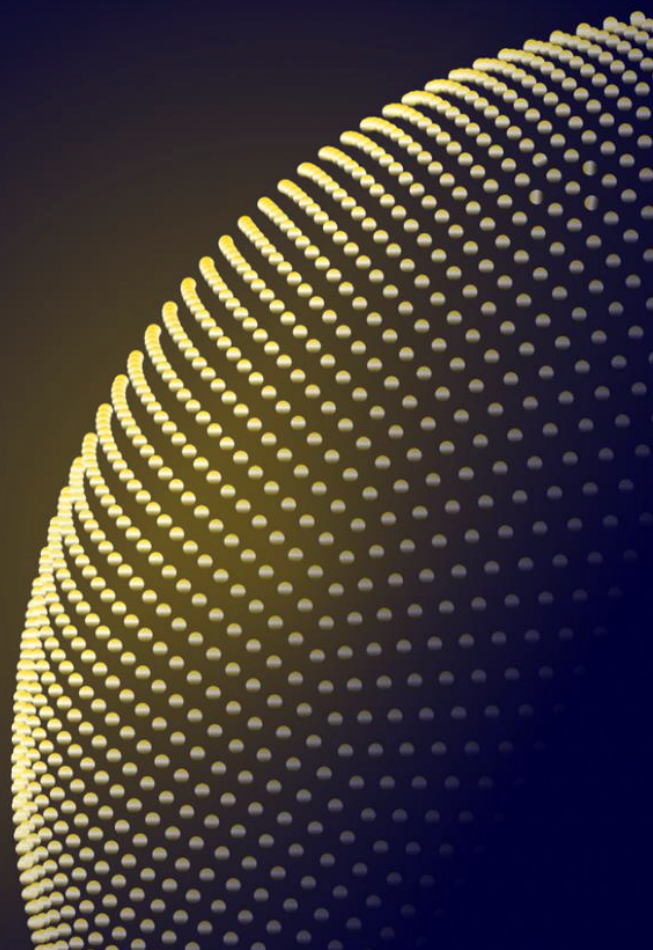
XM Cyber

# Continuous Exposure Management – Why thinking like an attacker is an efficient way to shape your remediation

**Wayne O'Young,** Regional Manager

Wayne.oyoung@xmcyber.com

+61 (0) 407 157 339



# Why Attackers Are Successful

## Real Life Attack Kill Chain

**Not aware of stolen credentials**

**Discovering and fixing high privileged access is not a priority**

**Security controls are siloed and owned by separate teams**

1. Buy stolen credentials
2. Breach VPN via MFA Bombing
3. Find exposed high privileged service account
4. Steal secrets from PAM vault
5. Gain access to all sensitive systems

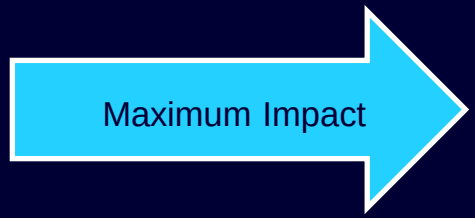

**No vulnerabilities were used here**

**It could have been a whole lot worse!**

XM Cyber

# What motivates the hackers | Threat actors | Adversaries | Cyber Criminals

- Nation-States
- Financial Gain
- Insider Threats
- Hacktivists
- Recognition & Popularity
- Malicious Payback




***The End Goal is to get to the crown Jewels.***
***Understanding what the Crown Jewels are, from a risk perspective, is über important***

# Exposures Go Beyond Vulnerabilities

### Active Directory
- Member of group
- Add Logon Script
- DC Sync

### Identities
- Group membership
- Excessive permissions
- Cached credentials

### Vulnerabilities
- Follina CVE-2022-30190
- PrintNightmare CVE-2021–34527
- Log4j CVE-2021-44228

### Misconfigurations
- Publicly Exposed S3 Bucket
- SMB Signing disabled
- Default passwords

### Security Controls Configurations
- Disabled Endpoint Protection Platforms
- Multi-Factor Authentication not configured
- Outdated signatures

86%

**of breaches involve stolen credentials**
(Google Cloud's 2023 Threat Horizons Report)

**credential issues account for**

60%

**of compromise factors**
(Google Cloud's 2023 Threat Horizons Report)

27%

**Of the top attack techniques involve vulnerabilities and misconfigurations**
(XM Cyber Attack Path Management Impact report 2022))

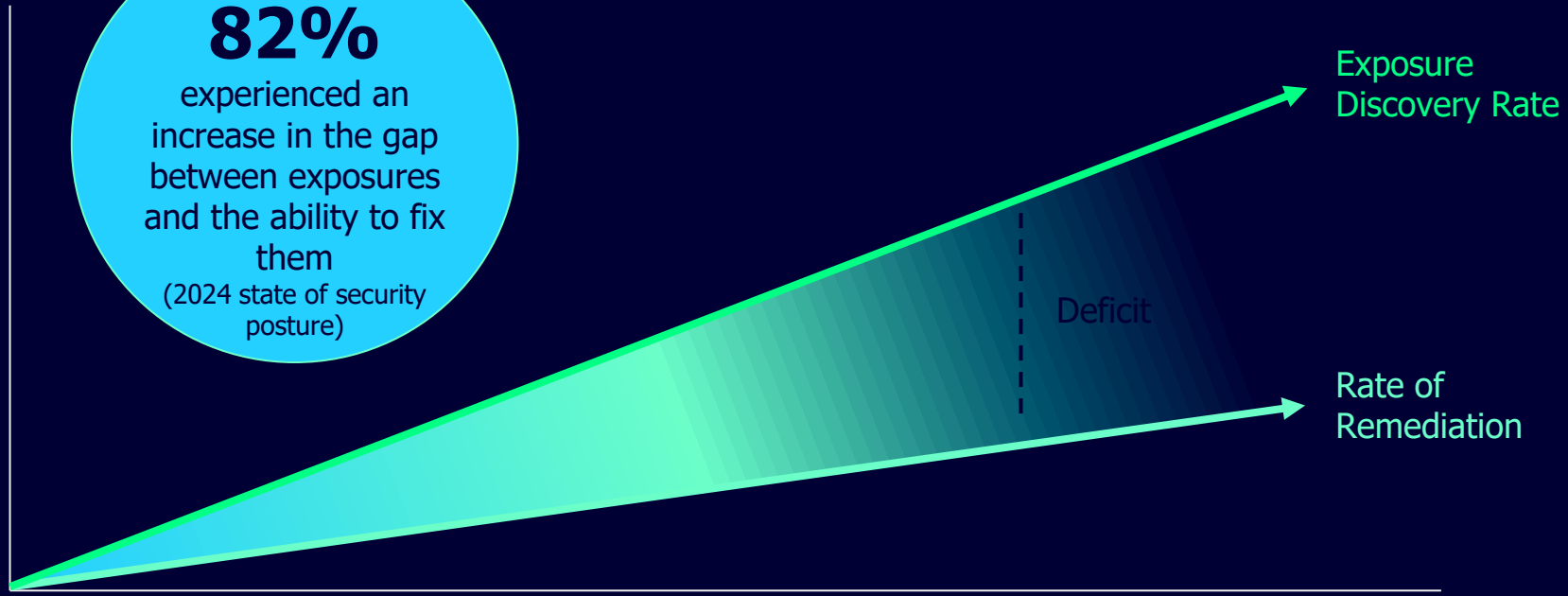
XM Cyber

# The Remediation Deficit

**82%**

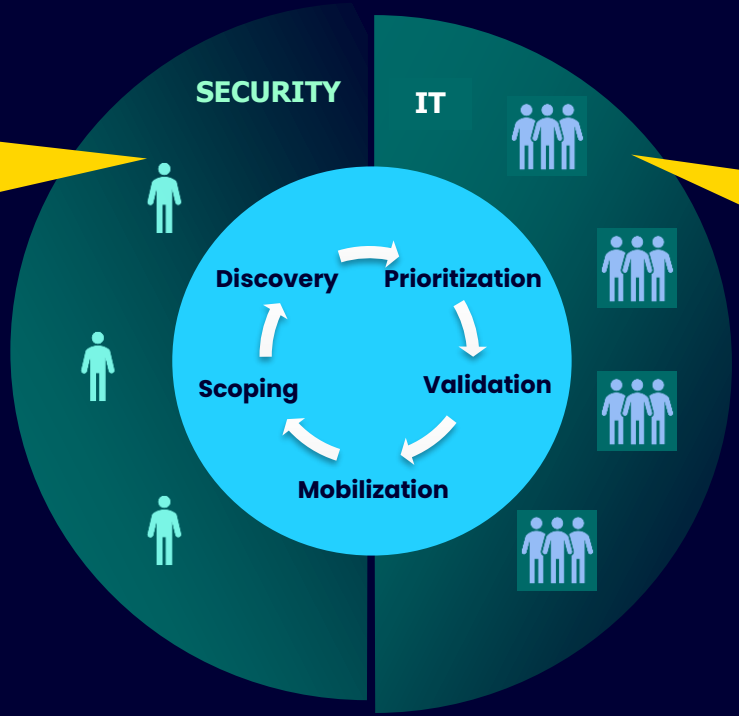
experienced an increase in the gap between exposures and the ability to fix them

(2024 state of security posture)



# Disconnect Between Security & IT

**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!

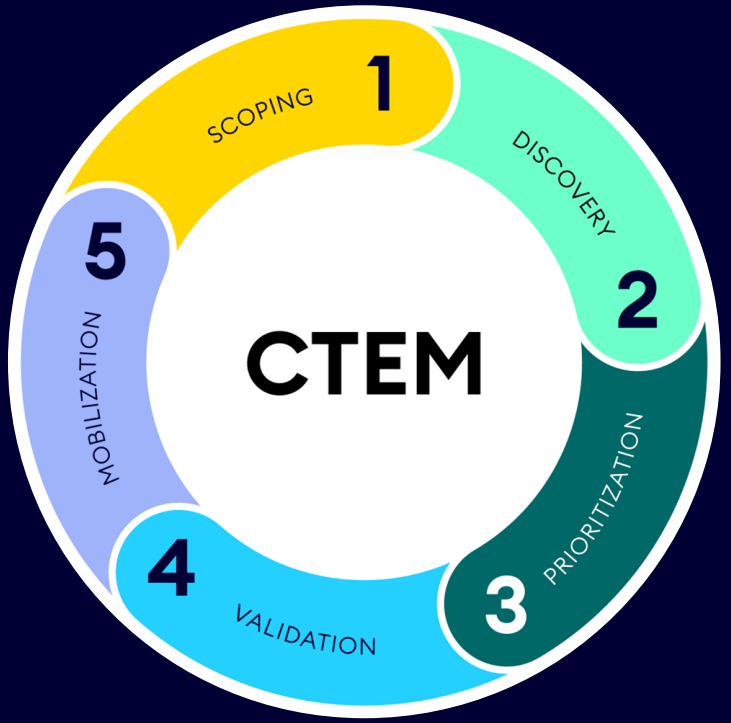
XM Cyber

# What is CTEM?

Continuous
Threat
Exposure
Management

**No. 2 on Gartner**
**Top Strategic Technology Trends 2024**

https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024

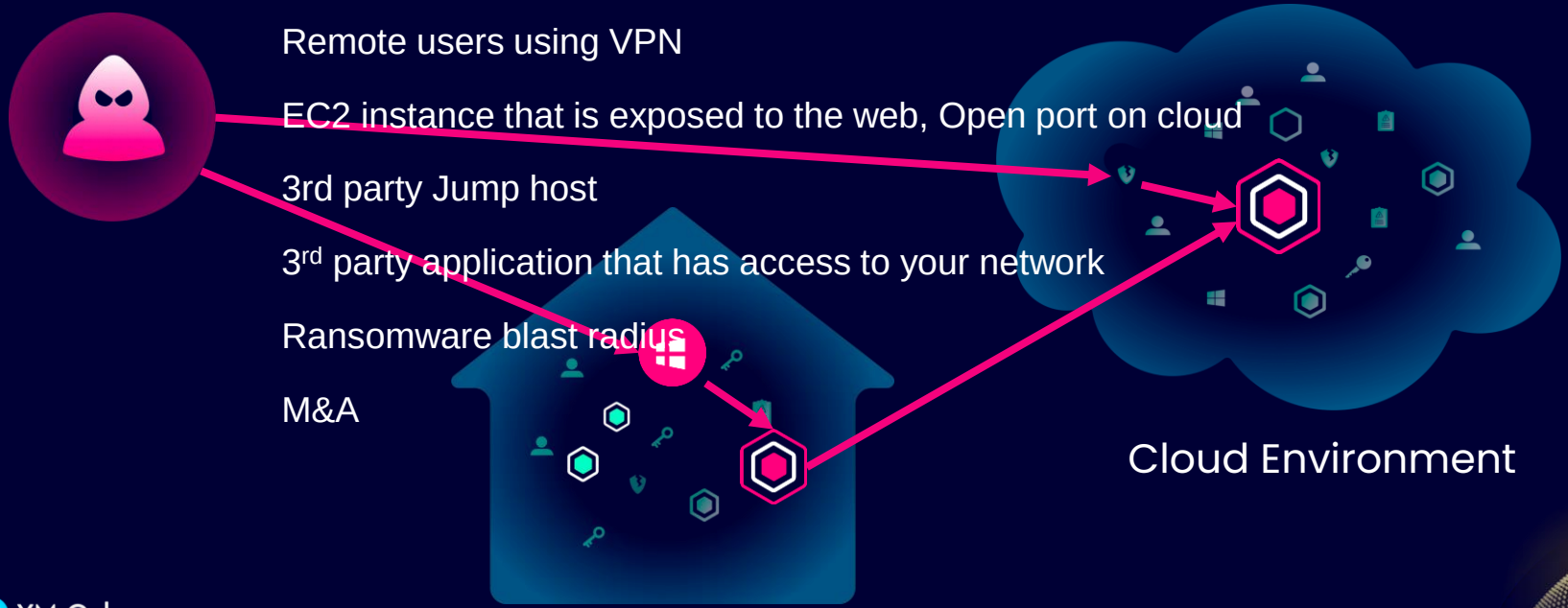



XM Cyber

# Scoping: Define “Business Critical”

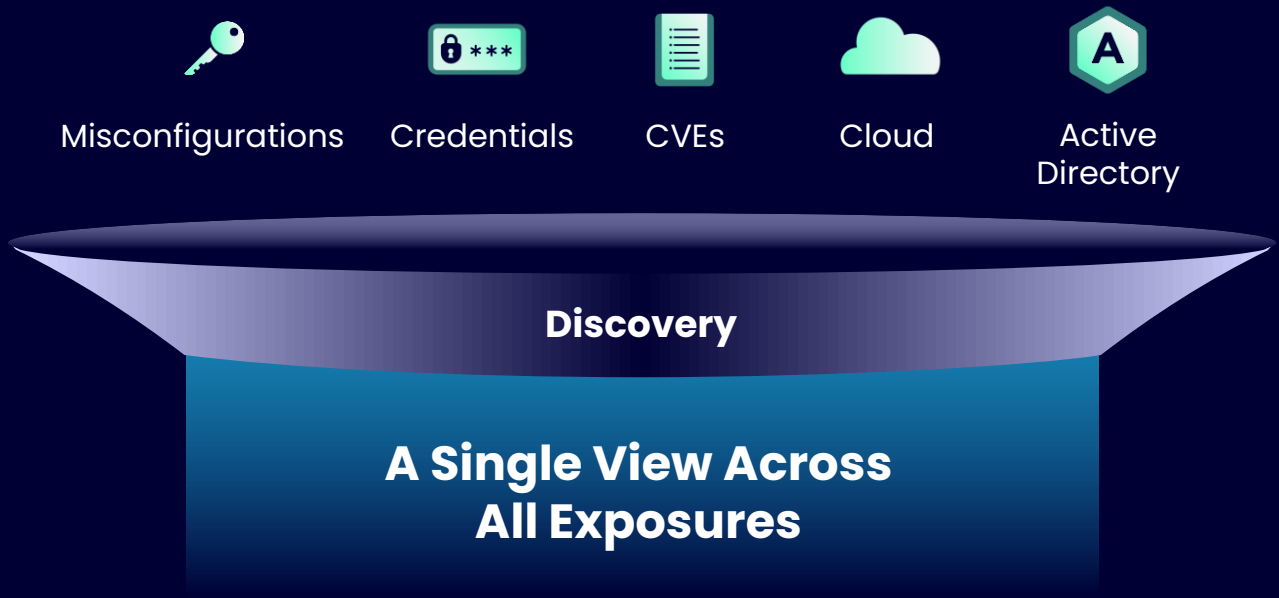

Where Are Your Critical Assets?

What are the most risky Threat Scenarios?




XM Cyber

# Discovery: Where Are You Exposed?




XM Cyber

# Siloed tooling

Source: XM Cyber State of Security Posture Report 2024

## Companies' Processes for Addressing Exposures Across On-Prem and Hybrid Cloud Environments

The responses reveal that, in about half of organizations (47%), separate processes and/or teams are responsible for addressing exposures across on-prem and hybrid cloud environments.

In contrast, 42% of organizations manage exposures holistically, considering both on-prem and hybrid cloud environments as part of an integrated strategy. This means that the majority (58%) opt for ad-hoc or siloed approaches, relying on separate teams and processes for each environment. This puts organizations at a significant disadvantage in effectively combating the dynamic tactics of cyber adversaries, who often operate seamlessly across environments.

This suggests a need for organizations to assess their strategies for exposure management and consider whether a more integrated, holistic approach could enhance efficiency and effectiveness. The data highlights the ongoing challenge of aligning skill sets and tools across diverse environments, emphasizing the importance of strategic cohesion in managing exposures for both on-prem and hybrid cloud infrastructures.

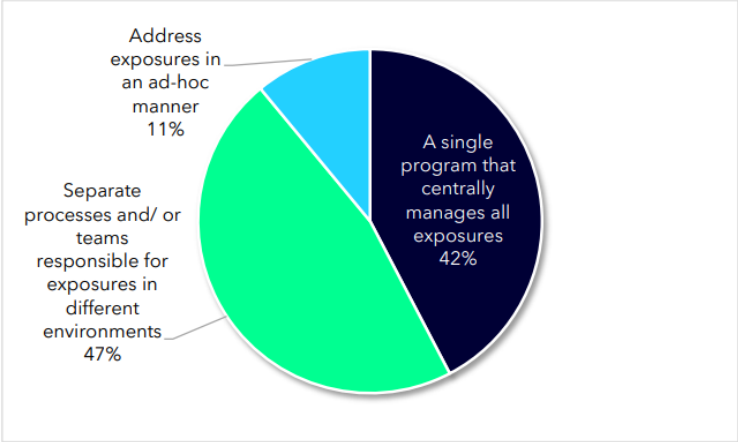
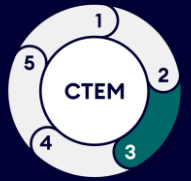



Figure 8: Companies' Processes for Addressing Exposures Across On-Prem and Hybrid Cloud Environments

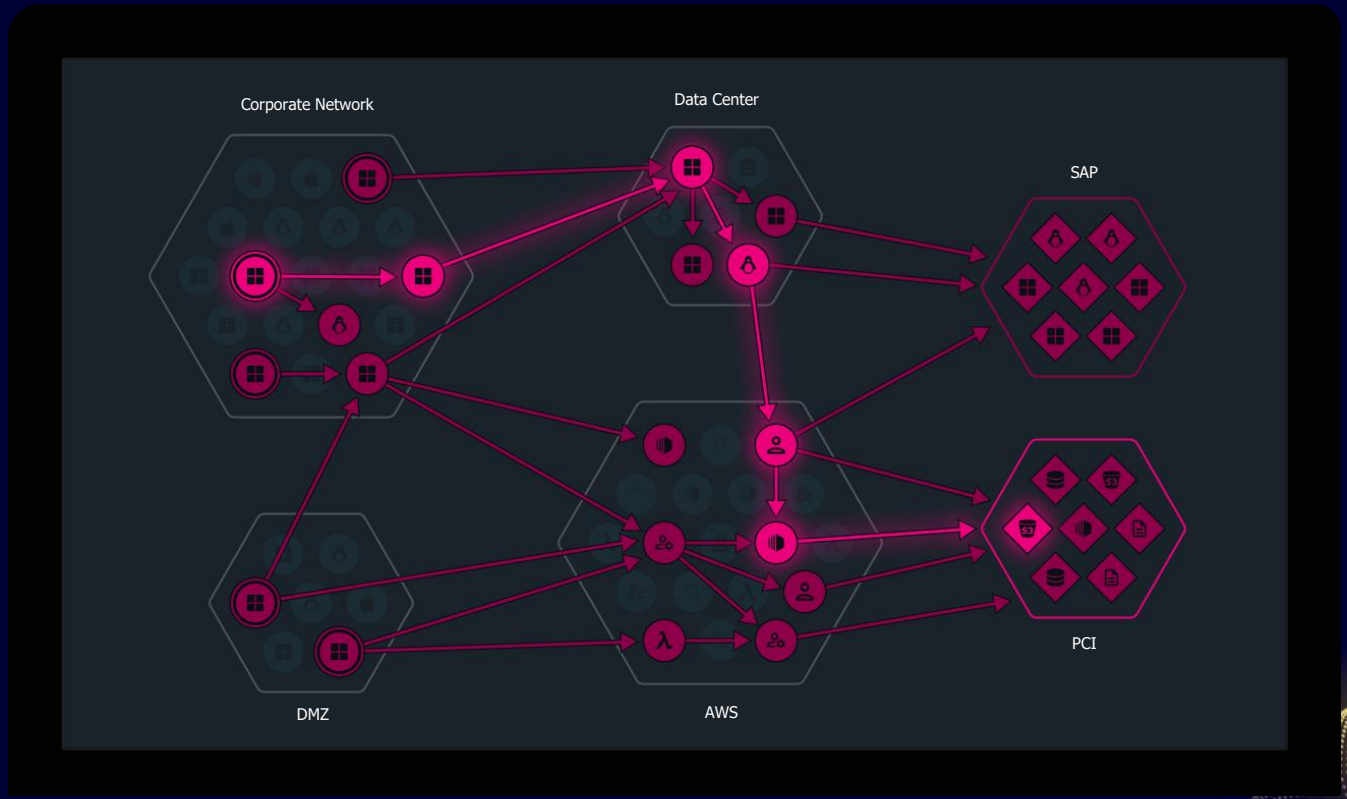
# Prioritisation: Attack Graph Analytics




Consider the whole hybrid attack surface

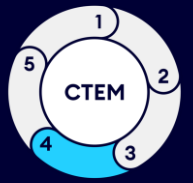
Understand all possible attack paths to business-critical assets

Prioritise Threats in the Wild




XM Cyber

# Validation: Attack Graph Analytics

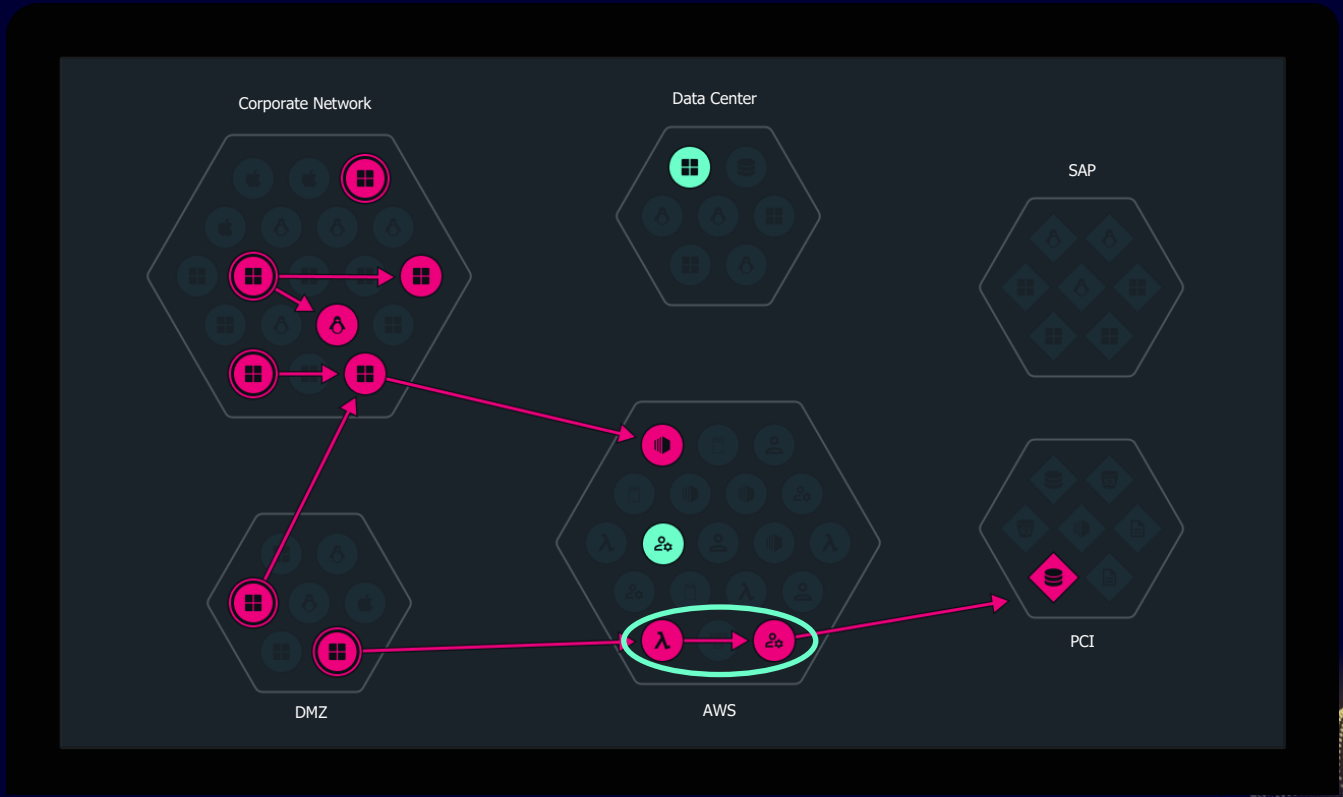



Understand where you don't need to focus

Focus on **Choke Points**, not Dead Ends

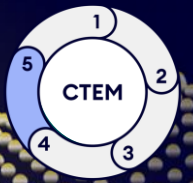
Close remaining easily exploitable attack paths

**Fix Less.**
**Prevent More.**

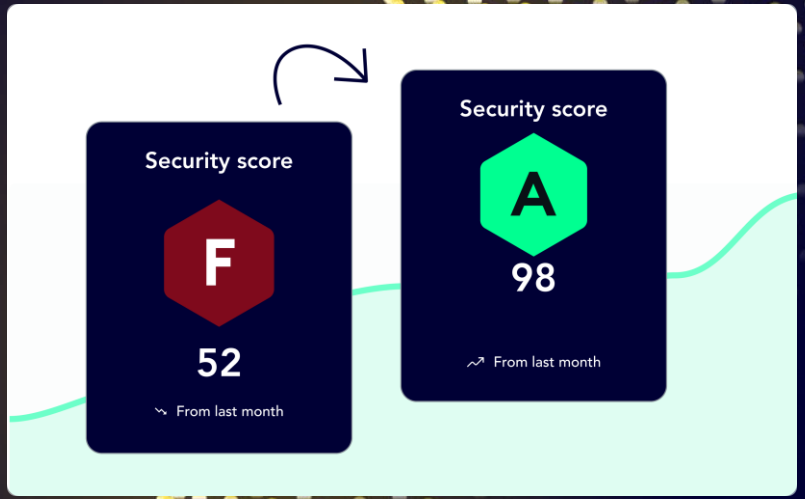



XM Cyber

# Mobilization



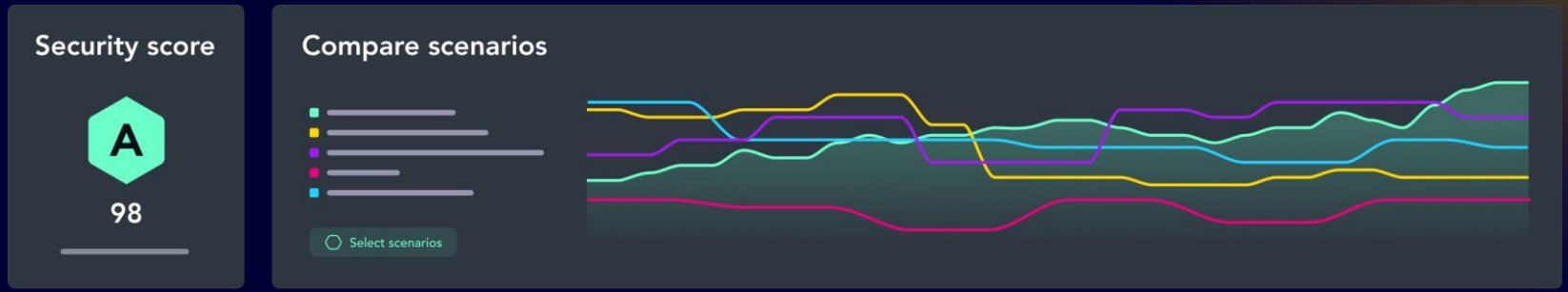

- Justify Criticality
- IT Teams Focus Efforts
- Provide Guidance AND Alternatives
- Integrate with ITSM
- Track Progress




XM Cyber

# Measuring and Reporting


- Measure the ongoing risk of your Threat Scenarios
- Embed within Board Reporting
- As your posture changes, react fast




XM Cyber

# Common Use Cases

**Across Business and Operational Initiatives**

**BUSINESS**

**Digital Transformation & Cloud**

**Connected Supply Chain & 3rd Party Risk**

**Mergers & Acquisitions**


**Cyber Risk Reporting**

**OPERATIONAL**

**Vulnerability Prioritization**

**Ransomware Readiness**

**Network Segmentation and OT Security**

**Efficiency**

XM Cyber

# Outcome = A Winning Proactive Approach

**Prevent High-Impact Attacks**
with Continuous, End-to-end Exposure Management


**Gain Remediation Efficiency**
and Stop Prioritizing Issues That Don't Impact Risk


**Establish a Common Language around Risk**
Foster Security & IT team alignment and improved reporting to the board

XM Cyber

# Thank You.

Stand 20
xmcyber.com

XM Cyber