Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Don't Expose Yourself

A Modern Approach

Brian Martin

Director of Product Management, Integrity360

#SecurityFirstStockholm

Exposure Management

Contents

- What is exposure?
- Types of exposure
- How attackers leverage exposures
- Threat Exposure Management
- Key takeaways

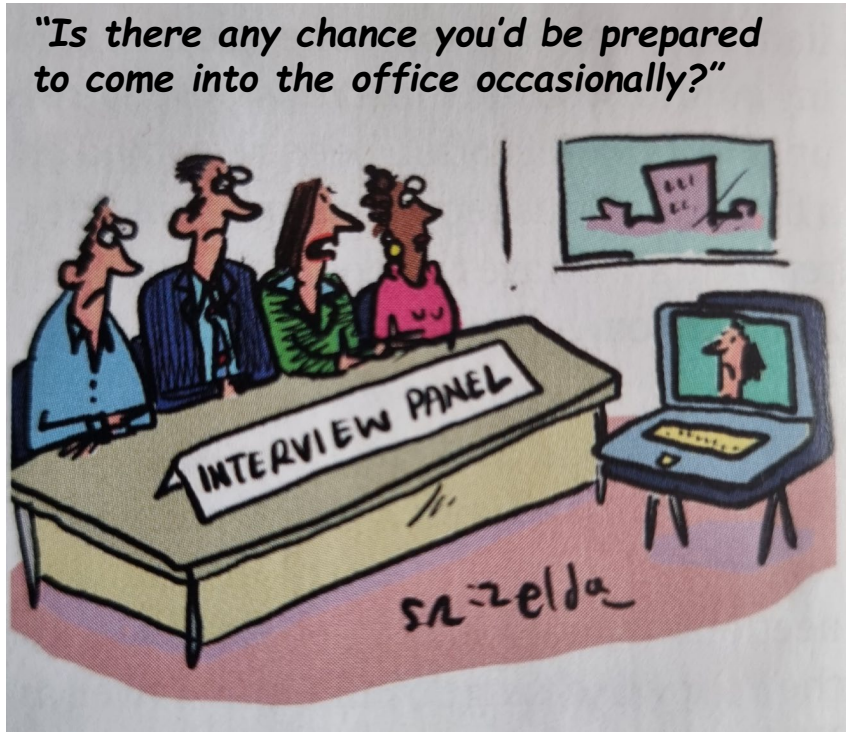
Integrity360
your security in mind

An exposure is anything that may be exploited by a bad actor to achieve their objectives

What is Exposure

Trends exacerbating Attack Surface Exposure

Work-from-anywhere era



March to the cloud continues

Not to mention...

40 Billion

Connected IoT devices by 2025, (+15-20% pa)

19%

Annual growth in OT investment to 2030

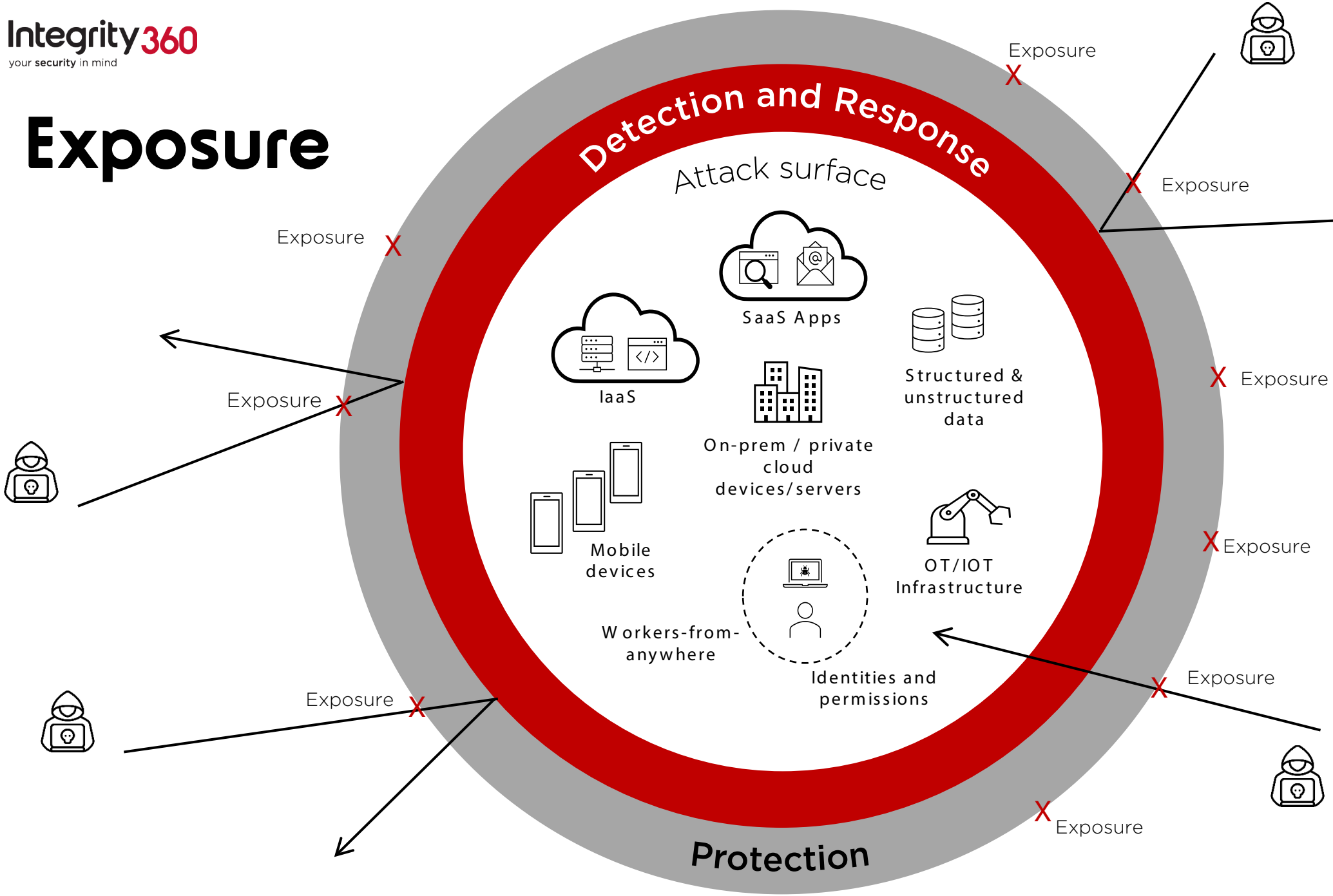
329 million

Terabytes of data generated daily, up to 90% unstructured (+23% pa)

Integrity360
your security in mind

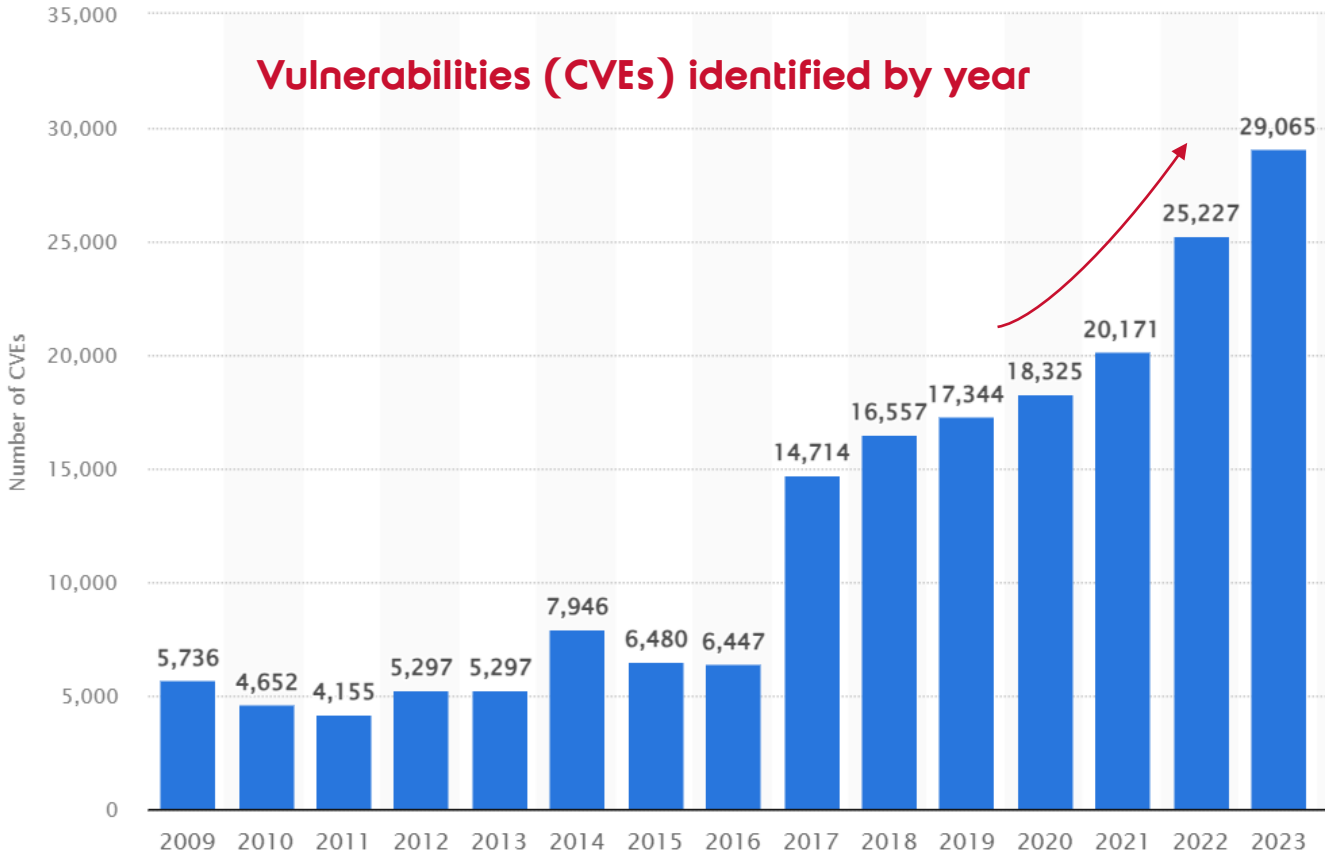
SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Exposure



What is Exposure?

Vulnerability Management as a problem is not going away



Source: Statista.com

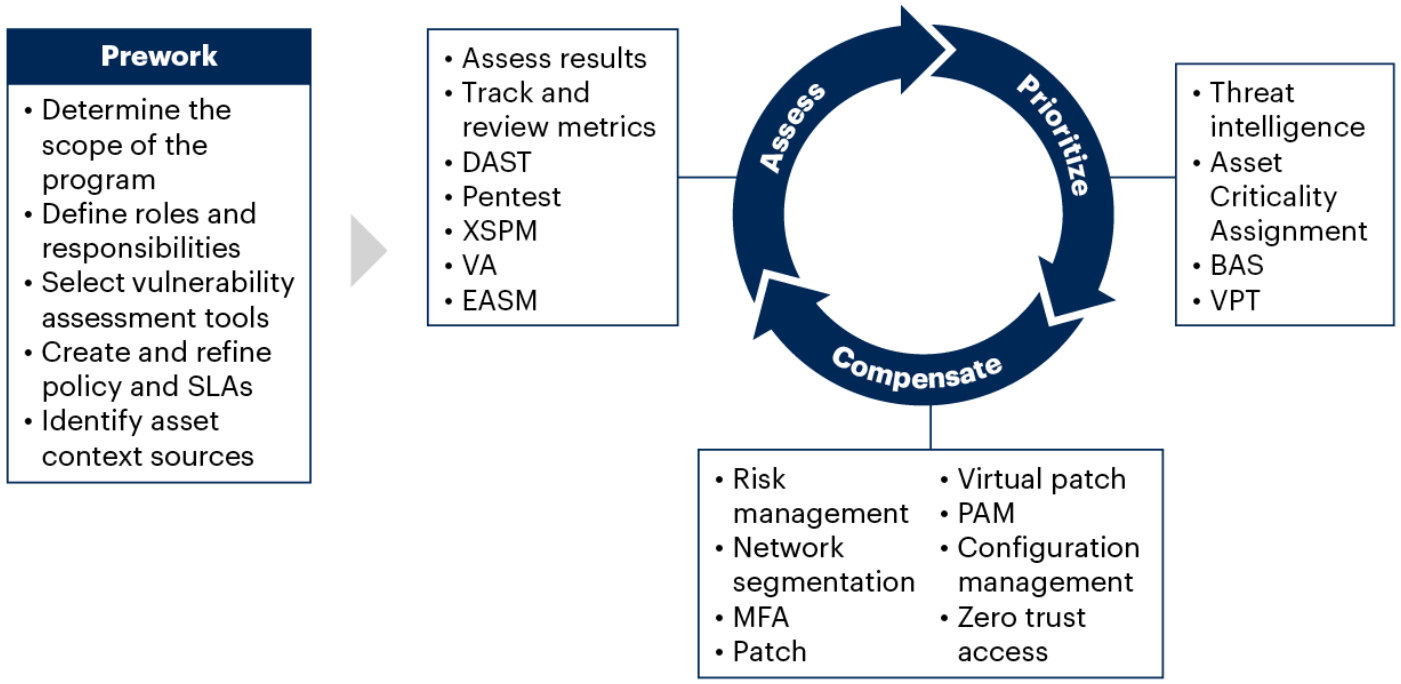
Quick poll:

How many of you find managing vulnerabilities easy within your organisation?

What is Exposure?

Risk Based Vulnerability Management (RBVM)

Gartner's Risk-Based Vulnerability Management Methodology



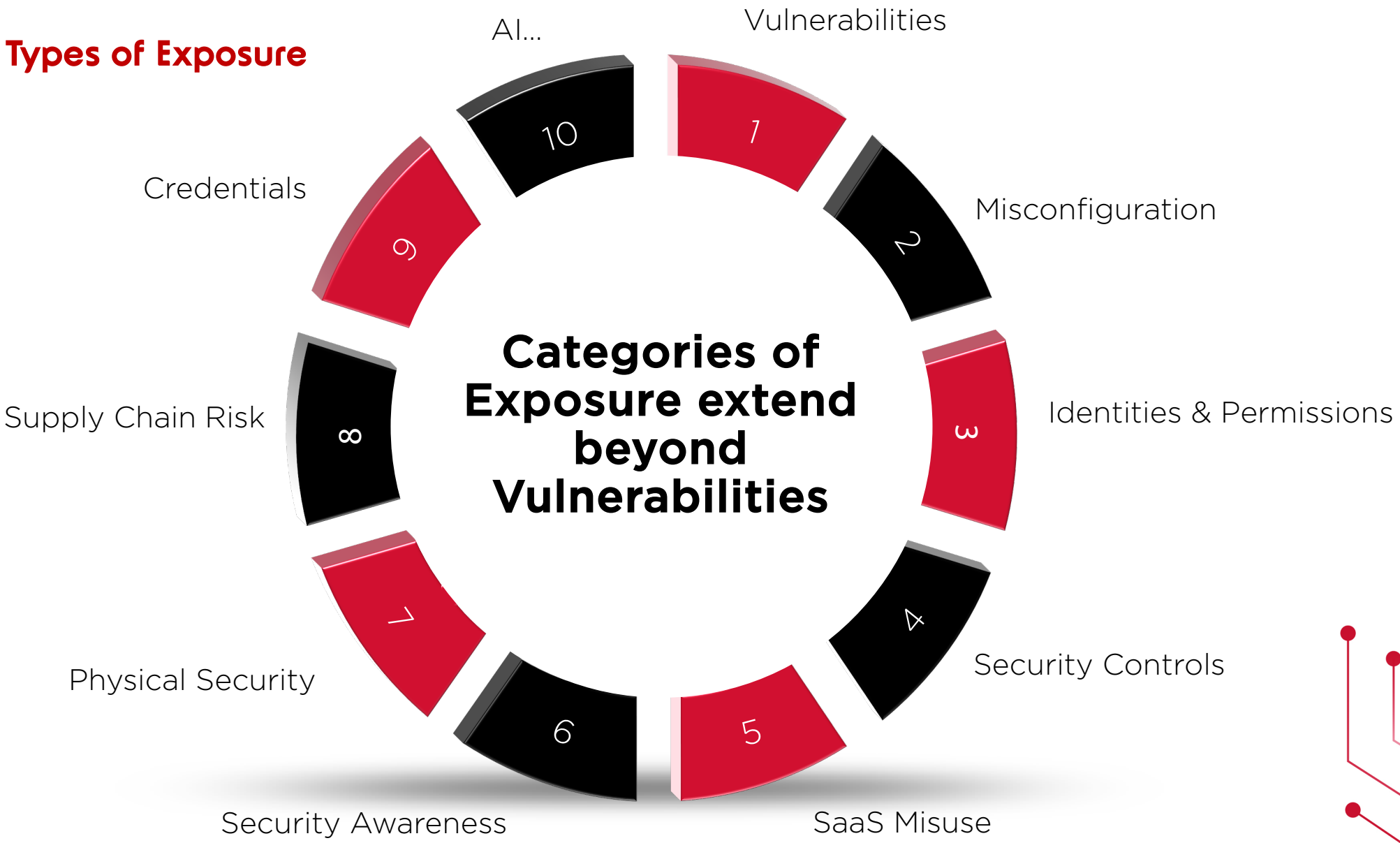
Quick poll:
How many of you have implemented Risk Based Vulnerability Management within your organisations?

"Even taking a risk-based vulnerability management (RBVM) approach might not be sufficient. Fixing every known vulnerability has always been operationally infeasible." - GARTNER

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Types of Exposure



Integrity360

your security in mind

Security leaders must become CEOs

“Chief Exposure Officers!”

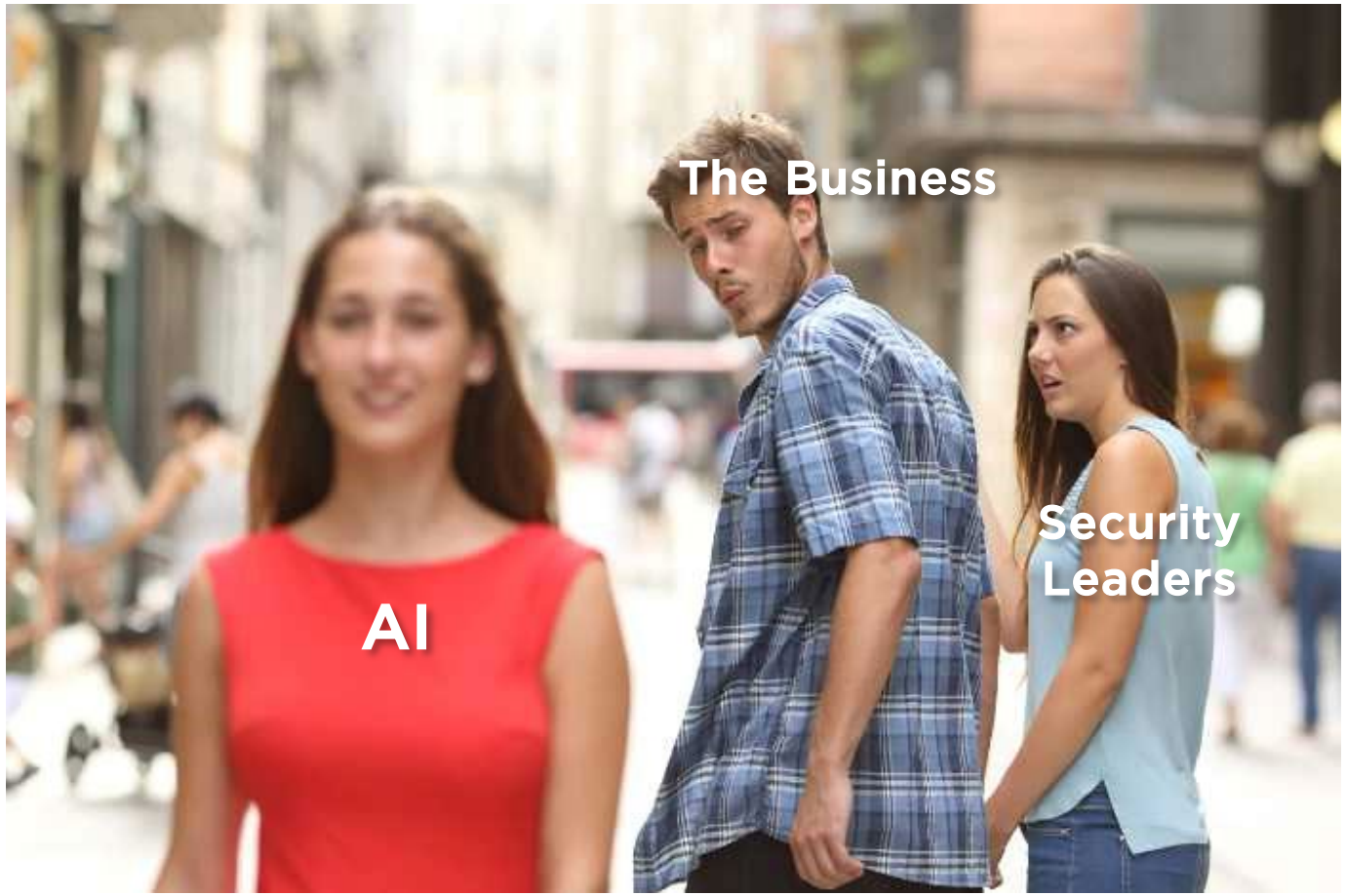
SECURITY FIRST

CYBER SECURITY CONFERENCE 2023

#SecurityFirstStockholm

Types of exposure

AI – threat or opportunity?



The Chief Exposure Officer mindset

AI creates new exposure

- Unauthorised access / Data leakage
- Impact of a breach
- Information governance
- Data classification and labelling
- Access permissions

AI turbo charges exposure exploitation

- Deepfakes & social engineering
- AI-led attack automation
- Advanced phishing at scale

AI-powered security enhancement

- Exposure visibility
- AI-enhanced tooling – rapid analysis
- Copilotization of the SOC
- Natural language queries

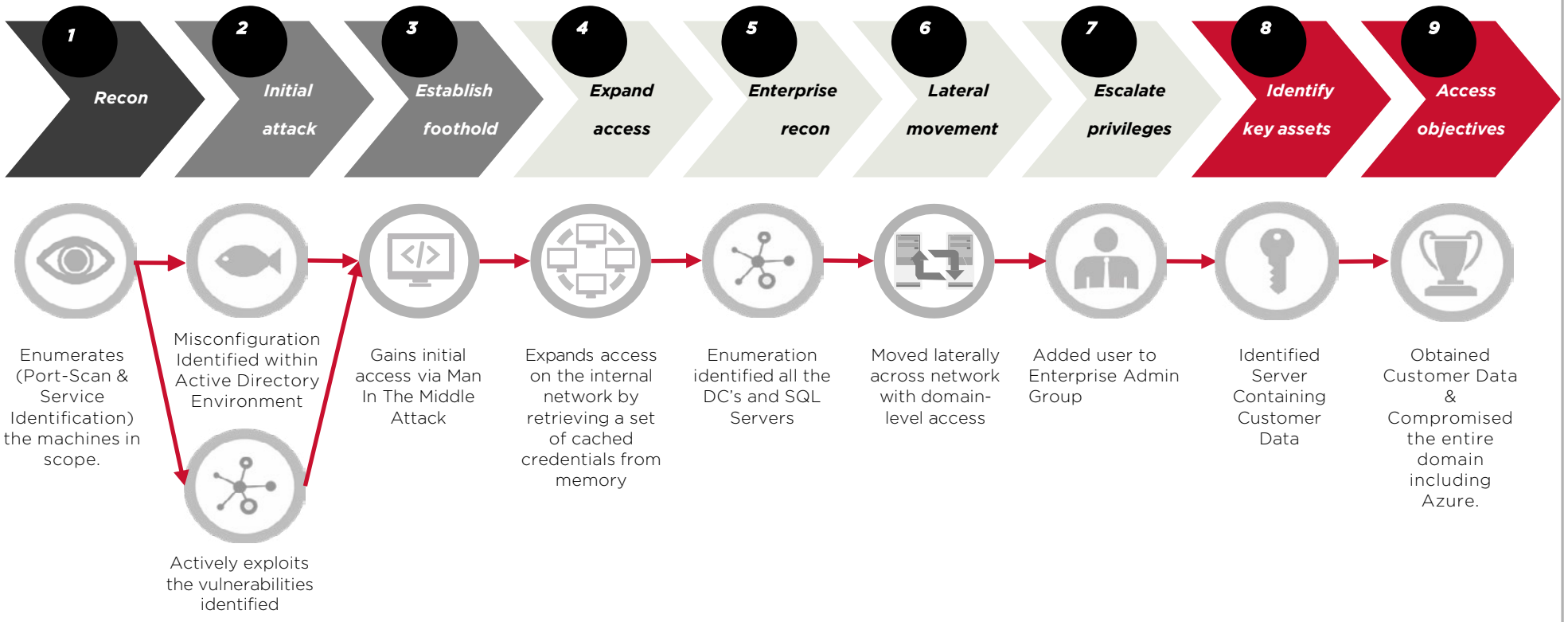
Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

How attackers leverage exposure

Attackers chain exposures to build attack paths

ATTACK PATH



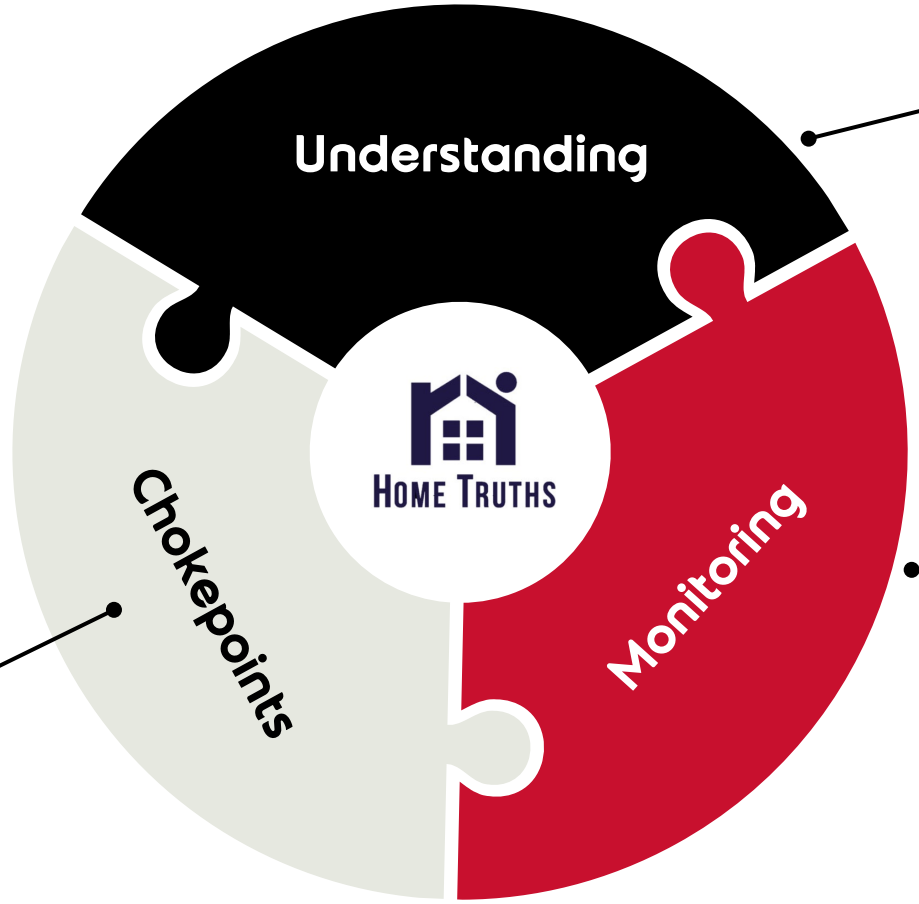
MITRE ATT&CK™

Threat Exposure Management

Home truths about Exposure Management

71%

of organisations do not have sufficient understanding of their attack surface

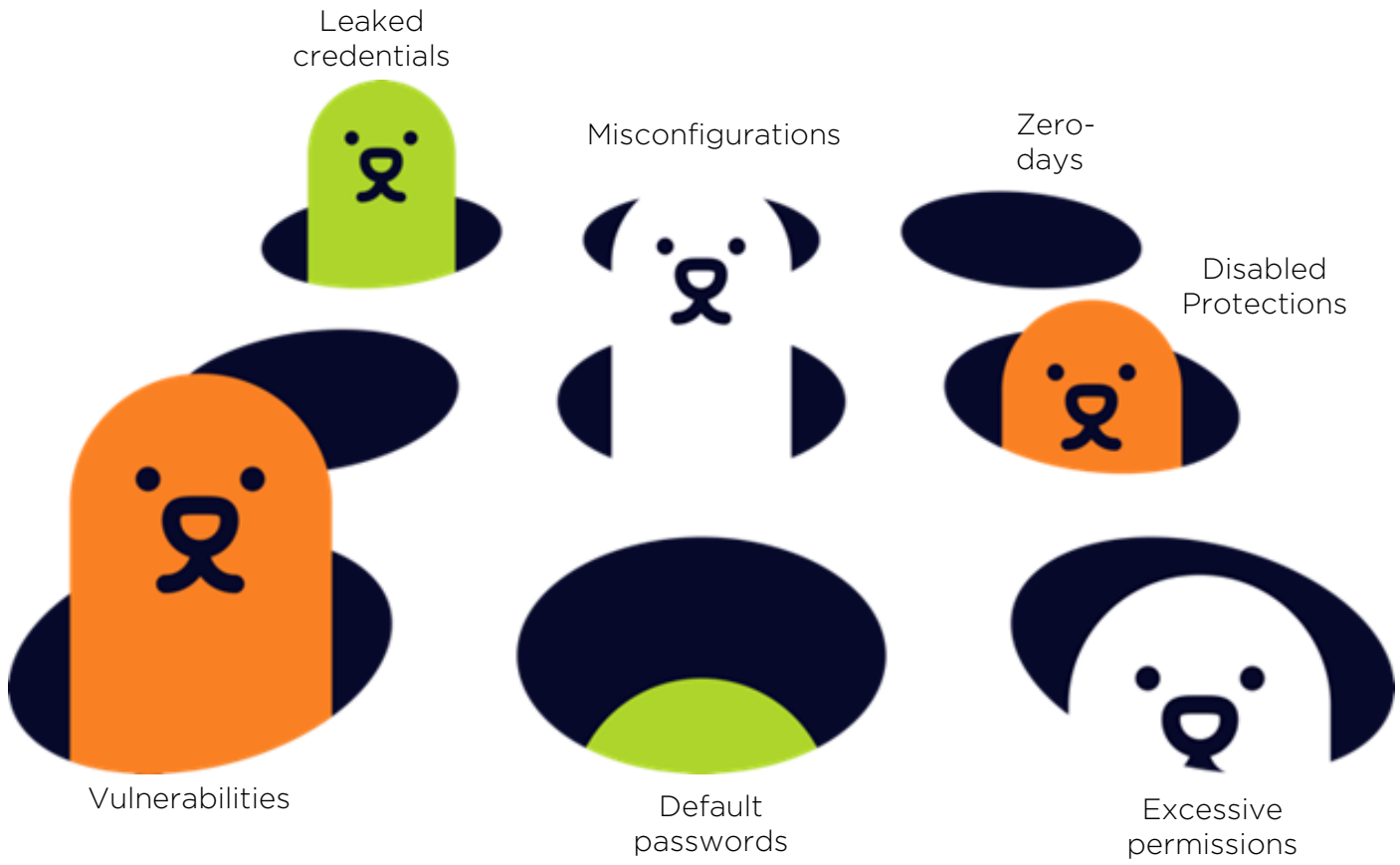


Every organisation needs understanding of their attack surface, exposures, and possible attack paths

Need to constantly monitor for new exposures that open new attack paths

Choking off attack paths will reduce risk

Exposure Management Whack-a-Mole



How do we prioritise remediation of exposures?

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Threat Exposure Management

Risk Management

Traditional Risk Management

RISK = PROBABILITY x IMPACT

Exposure Management: CRITICALITY OF EXPOSURE =

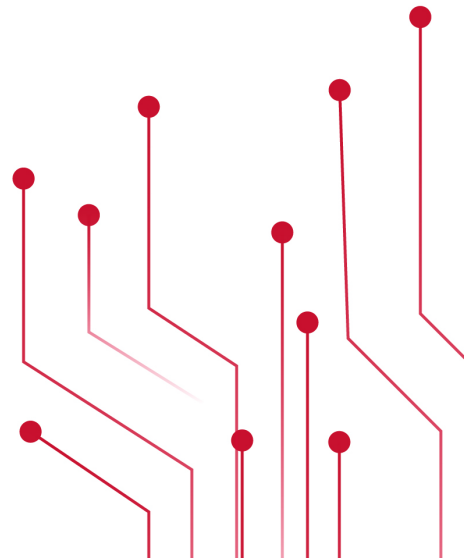
Likelihood of Exploitation

1. Exposure Severity
2. Ease of exploitation – internal/external, requires user interaction, authentication, etc
3. Number of Active exploits available
4. Active exploitation in the wild by threat actors targeting your profile

X

Impact of Exploitation

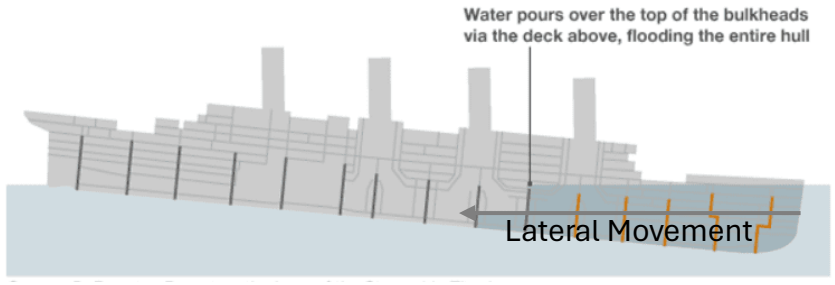
1. Asset criticality
2. Presence on attack path to critical asset(s)
3. Presence on multiple attack paths to critical asset(s)
4. Impact of those critical assets being compromised



Exposure Severity and Asset criticality alone are not sufficient to determine the priority of remediating an exposure

Threat Exposure Management overview

Exposure remediation prioritisation is vital



Bulkheads not watertight

Threat

Invalid no-breach assumption

Exposure

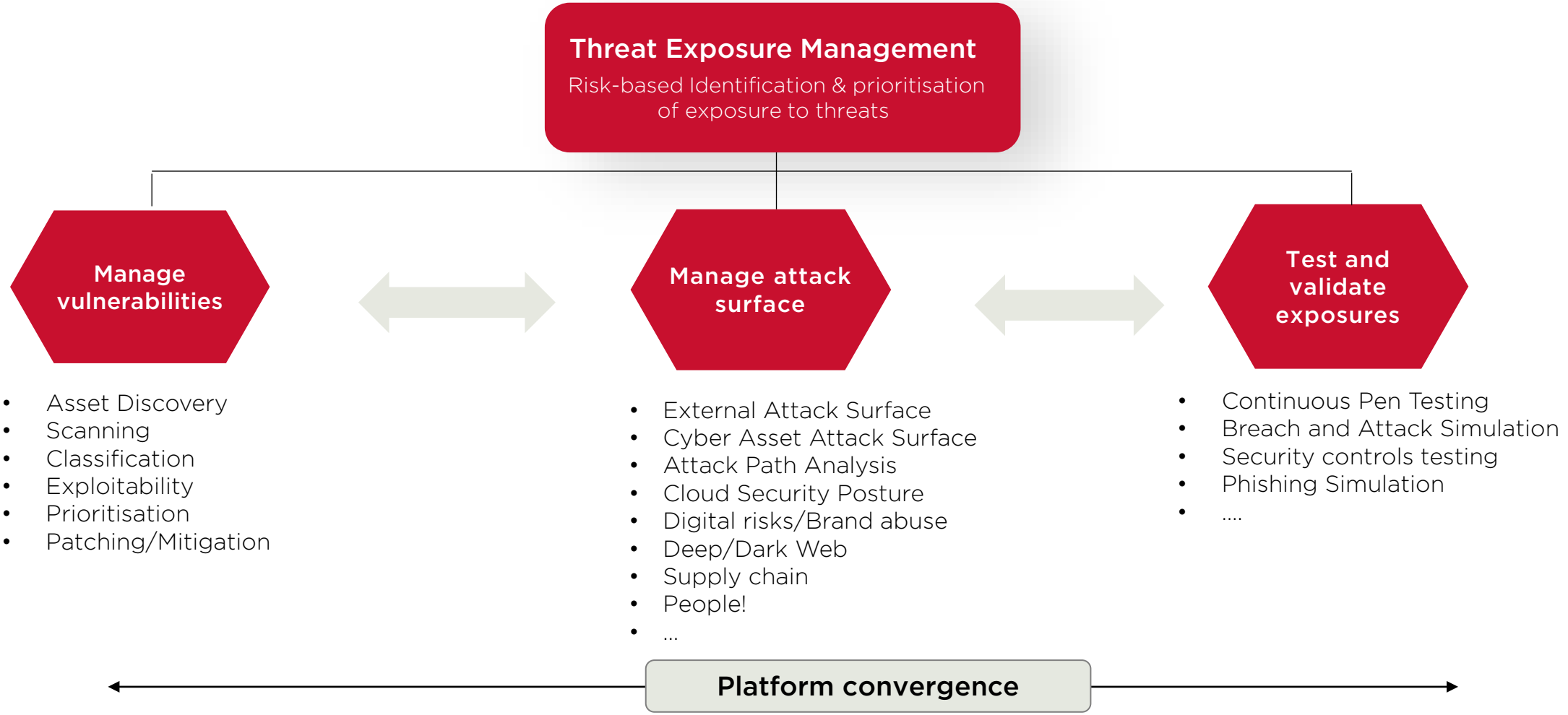
"Someone could trip on these!"

Inadequate response plan

- Nr of lifeboats: 20, places for 1,178 people
- Nr of people on board: 2,209
- Women and children first / Women and children only?
- Titanic survivors: 712
  - 32% of those on board
  - 60% of lifeboat places

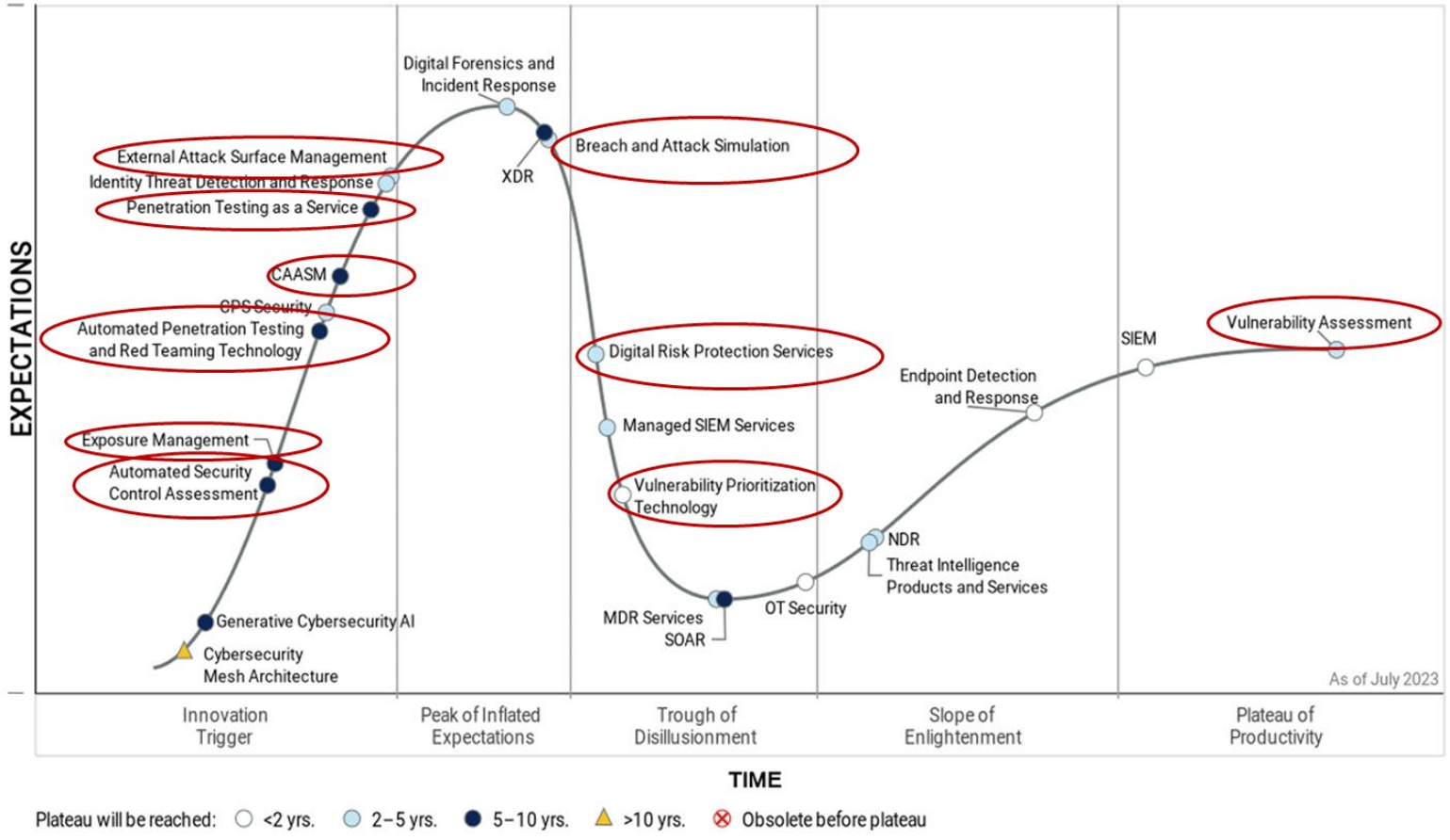
Threat Exposure Management overview

Components of Exposure Management



Threat Exposure Management

Most emerging tech in Security Operations relates to better managing exposures



Mature

- Vulnerability Assessment

Emerging

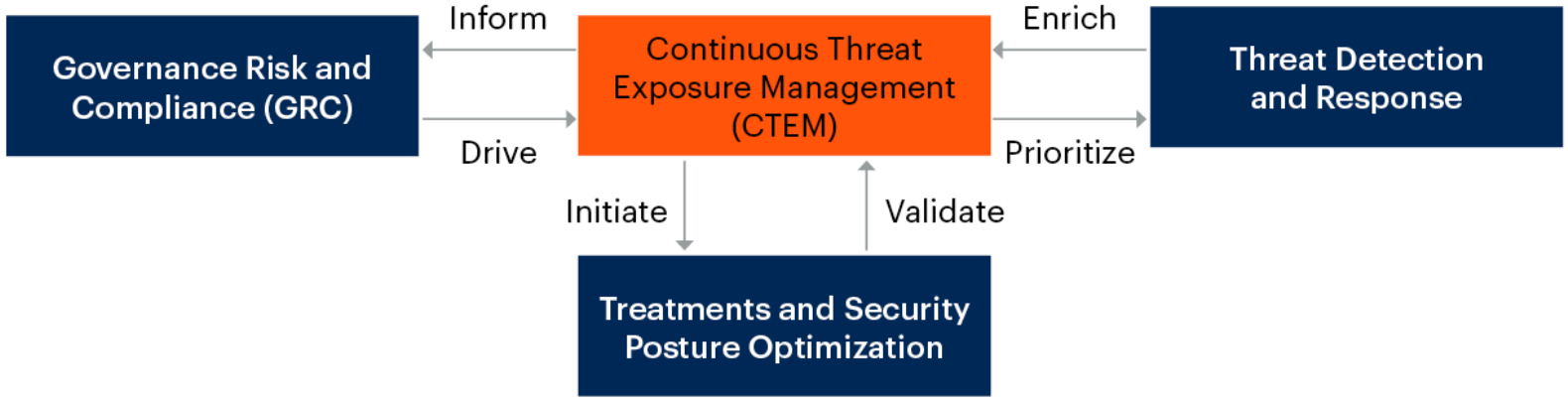
- Vulnerability Prioritisation
- Digital Risk protection
- Testing for Exposures
  - BAS
  - PTaaS
  - Automated PT
  - Automated security controls assessment
- Attack Surface Mgmt:
  - EASM
  - CAASM

- **EXPOSURE MANAGEMENT**

Threat Exposure Management

Continuous Threat Exposure Management

A continuous threat exposure management (CTEM) programme is an integrated, iterative approach to prioritizing potential treatments and continually refining security posture improvements.



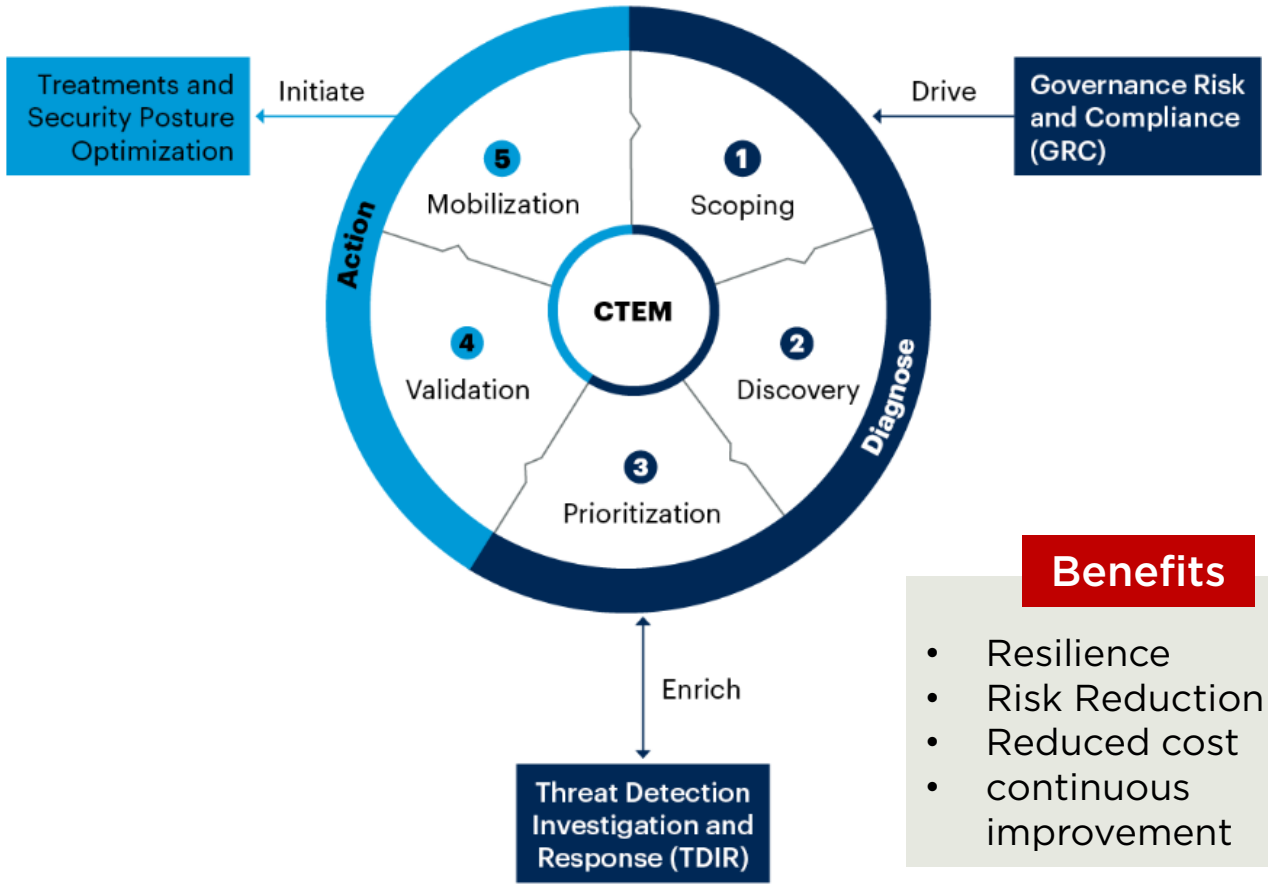
Both the attackers' and defenders' views need to be combined to minimise an organisations exposure to present and future threats

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Threat Exposure Management

The phases of a CTEM Programme



Benefits

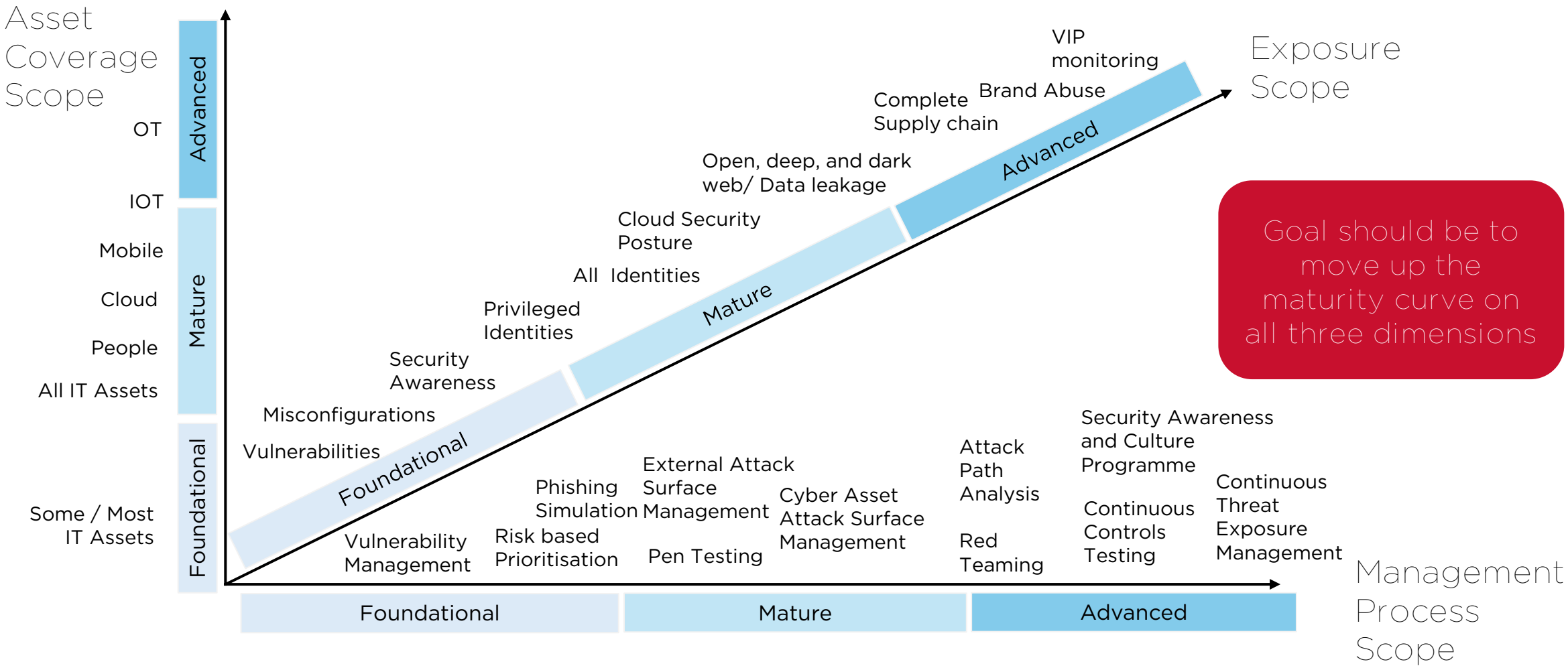
- Resilience
- Risk Reduction
- Reduced cost
- continuous improvement

An effective Exposure Management programme starts with understanding which categories of exposure to include

- **Scoping** (Identifying)
  - Business Critical Assets
  - External Attack Surface
  - SSPM/CSPM
  - Digital Risk Protection
  - Dark & Deep Web sources
- **Discovery**
  - Identify visible & hidden assets
  - Identify vulnerabilities & misconfigurations
- **Prioritization**
  - Based on urgency, severity and risk
- **Validation**
  - Attack success
  - Potential impact
  - Response & Remediation speed
- **Mobilisation**
  - Build a team to address the exposures
  - Confirm the toolset to remediate the exposures

Threat Exposure Management

Sample Maturity dimensions for Threat Exposure Management



Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

> By 2026, organisations prioritising their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach

Gartner

#SecurityFirstStockholm

Key takeaways

- Attackers chain exposures
- Expand concept of exposure beyond vulnerabilities
- Identify full attack surface – Internal and external
- Analyse attack paths and chokepoints to aid remediation prioritisation
- Level up maturity on 3 dimensions: Assets, Exposure categories, and Processes
- Initiate a Continuous Threat Exposure Management programme
- Become a CEO!

Thank you

Integrity360
your security in mind

Thank you

Brian Martin
brian.martin@integrity360.com

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

#SecurityFirstStockholm