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

***#SecurityFirstDublin***

## Exposure Management

# Contents

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...

**30 Billion**

Connected IoT devices by 2027

**19%**

Annual growth in OT investment to 2030

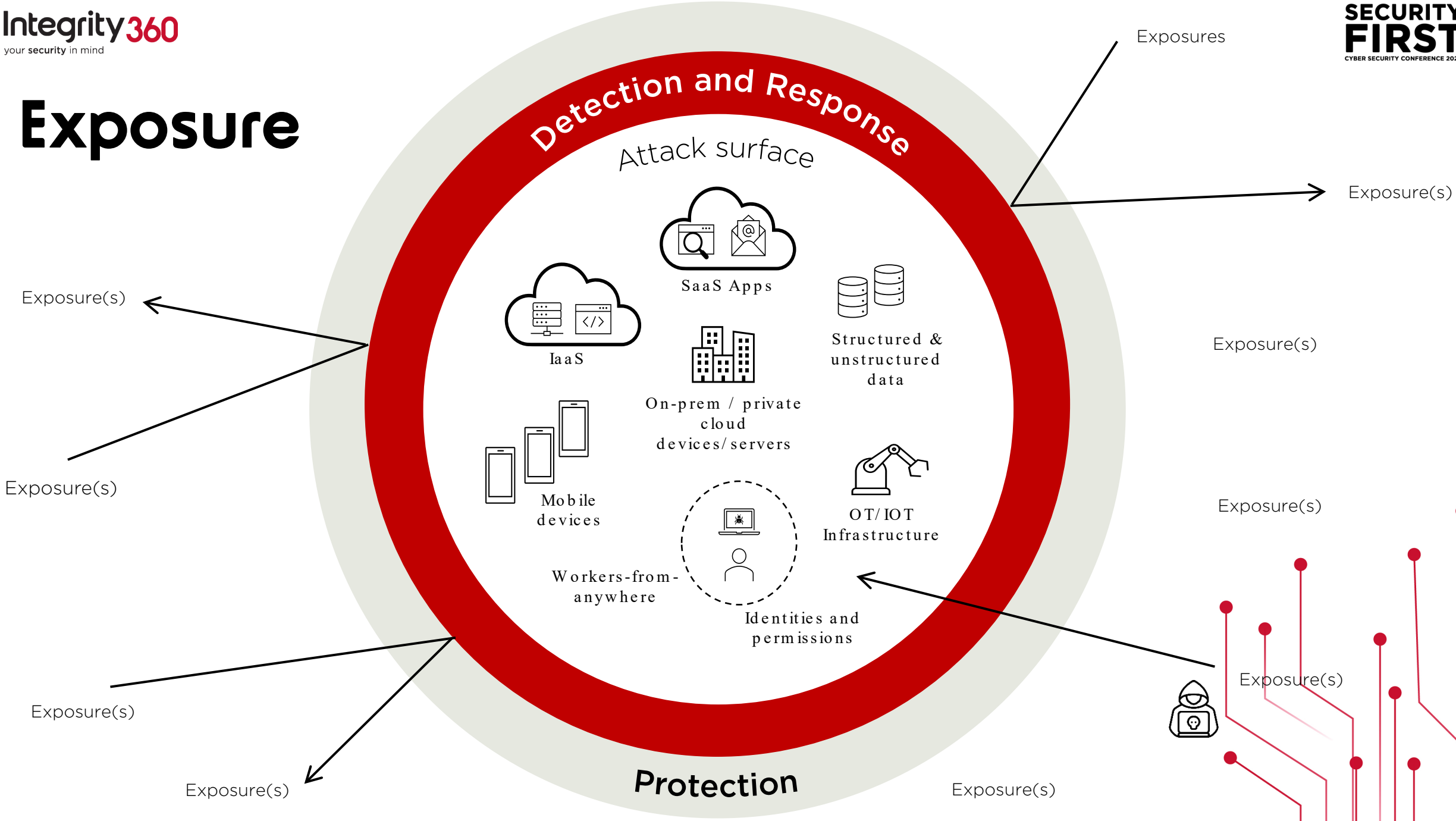
**329 million**

Terabytes of data generated daily, up to 90% unstructured

Integrity360
your security in mind

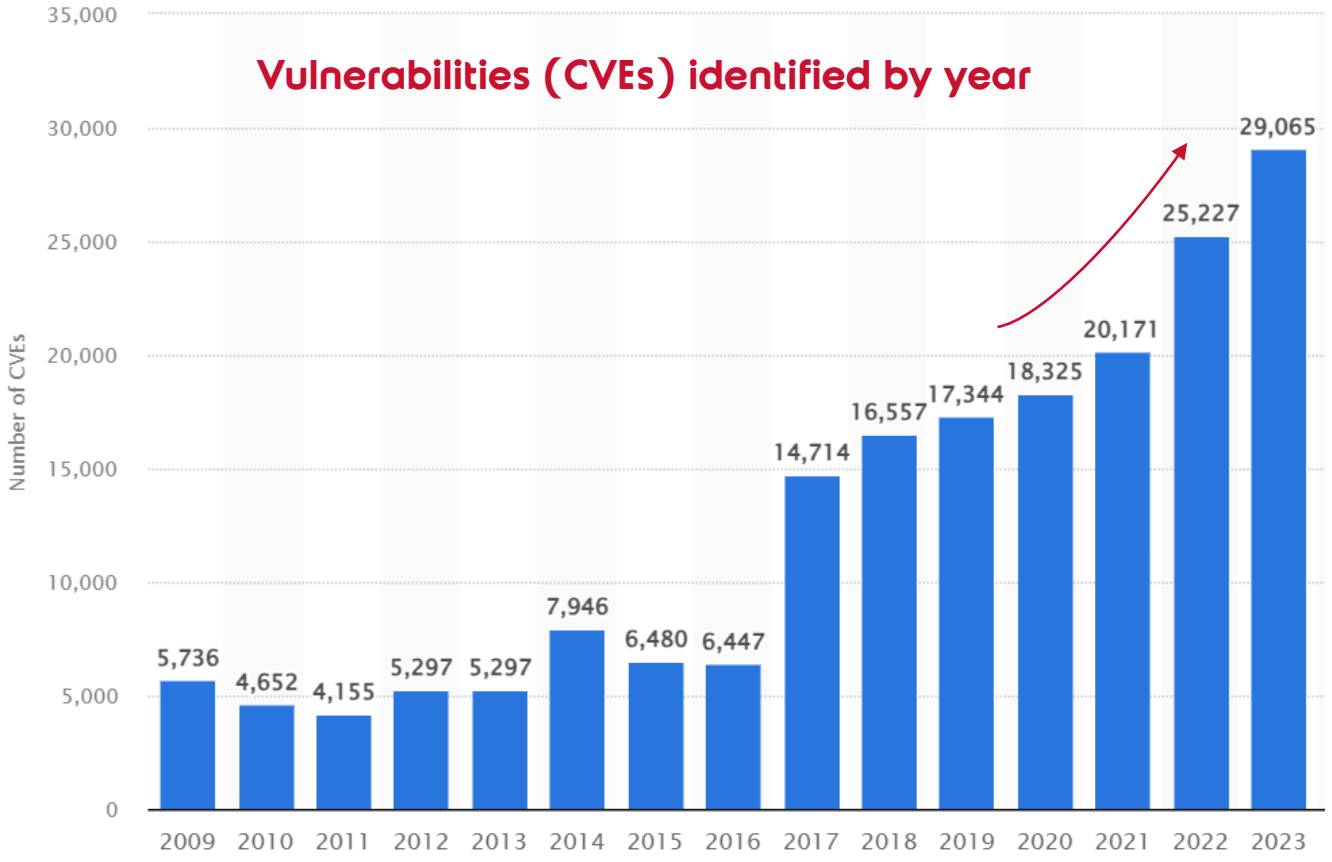
SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

# Exposure



## What is Exposure?

# Vulnerability Management as a problem is not going away




Source: Statista.com

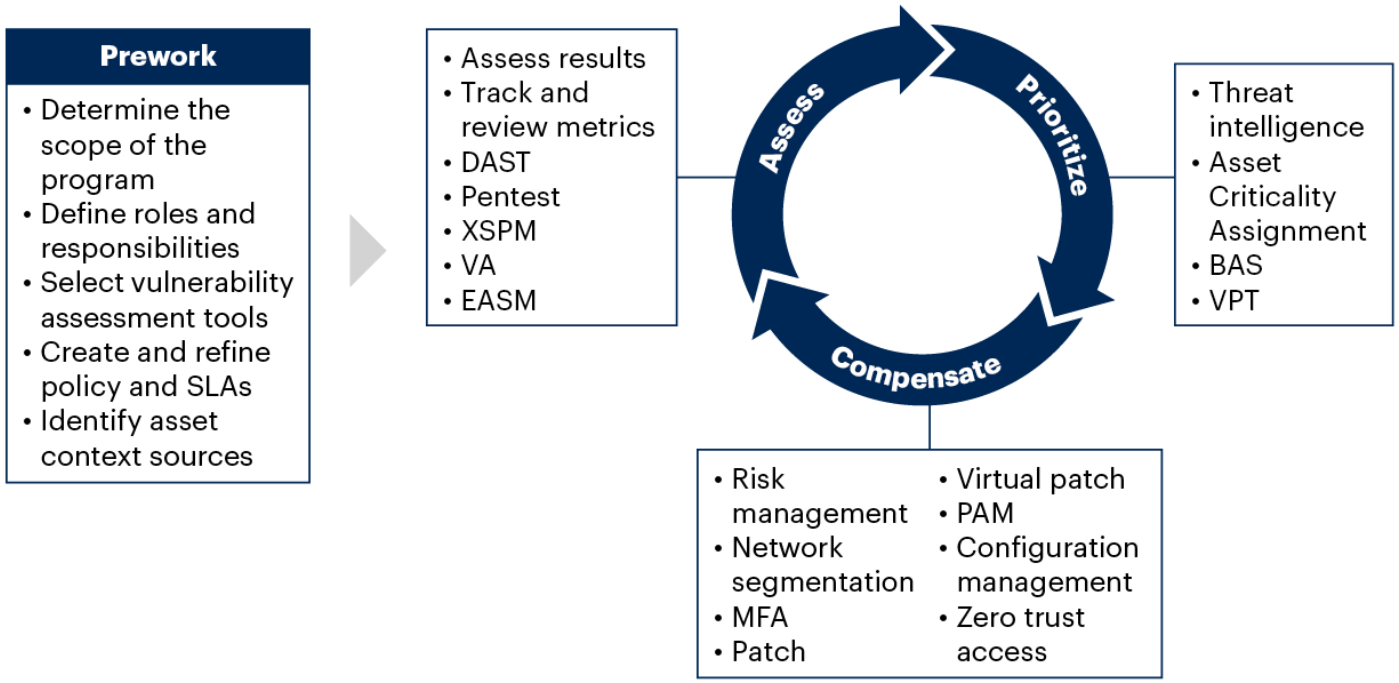
Quick poll:

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**



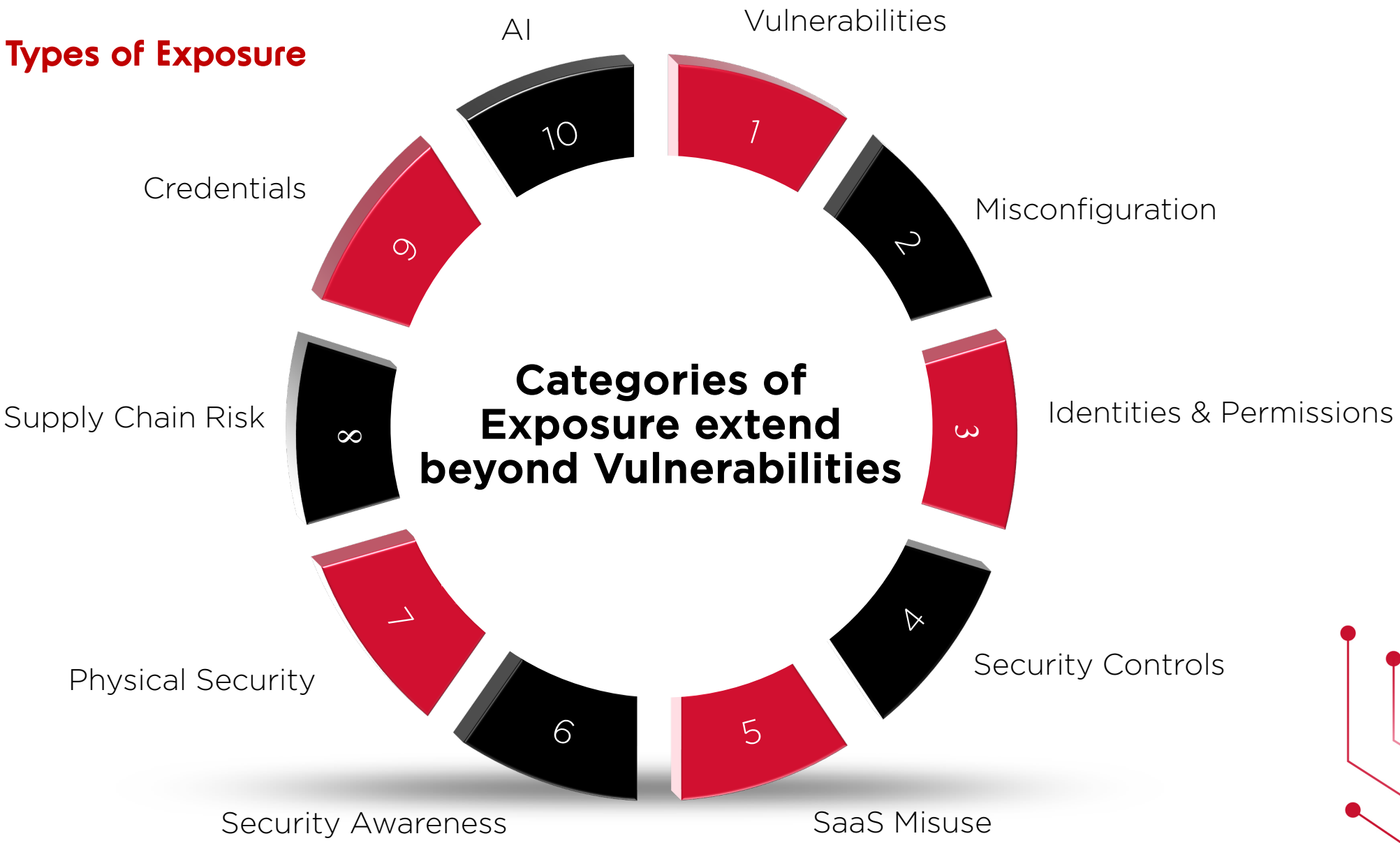

Quick poll:
How many of you have implemented Risk Based Vulnerability Management within your organisations?

"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...

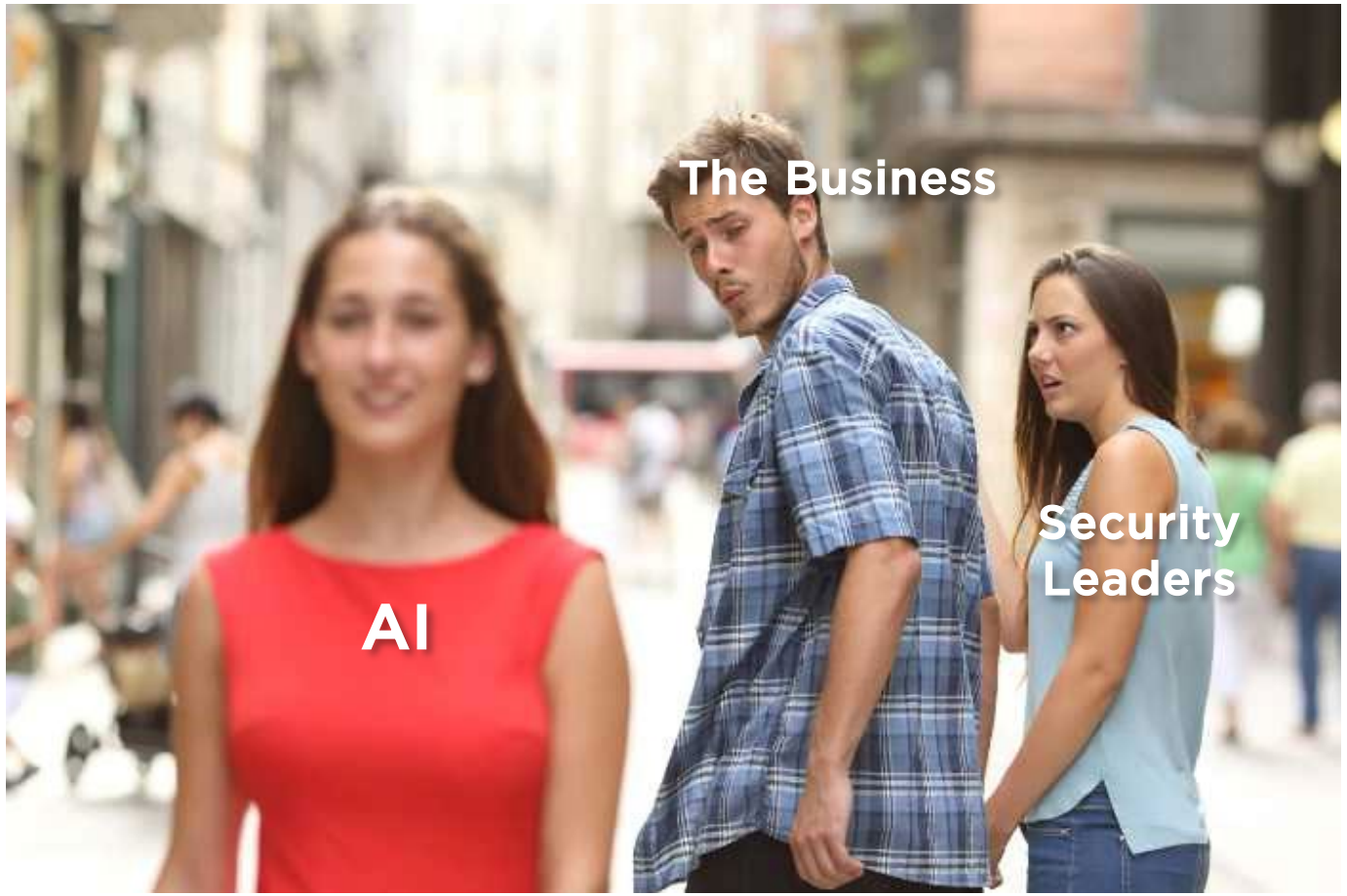
# "Chief Exposure Officers!"

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

#SecurityFirstDublin

## Types of exposure

# AI – threat or opportunity?




## The Chief Exposure Officer mindset

**AI creates new exposure**

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

**AI turbo charges exposure exploitation**

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

**AI offers opportunities to mitigate exposure**

- Exposure visibility
- AI-enhanced tooling
- Copilotization of the SOC
- Organising data to train Security LLMs

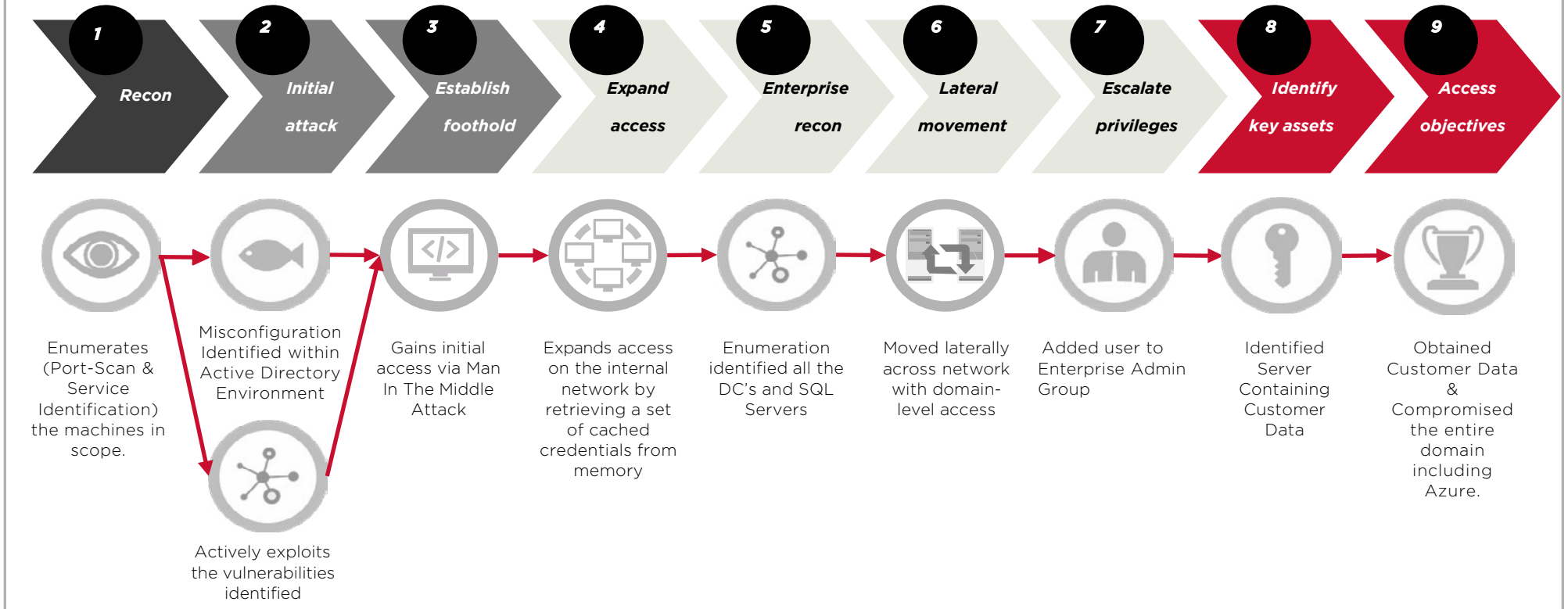
Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

## How attackers leverage exposure

# Attackers chain exposures to build attack paths

**ATTACK PATH**



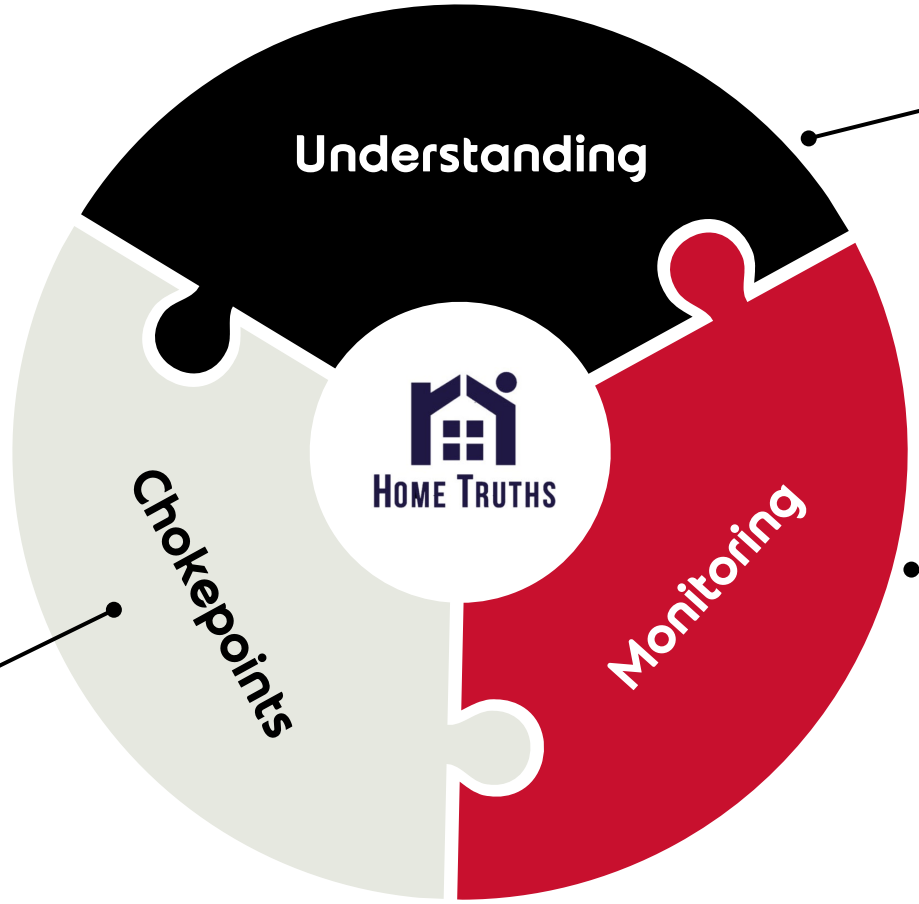

MITRE ATT&CK™

## Threat Exposure Management

# Home truths about Exposure Management

**71%**

of organisations do not have sufficient understanding of their attack surface

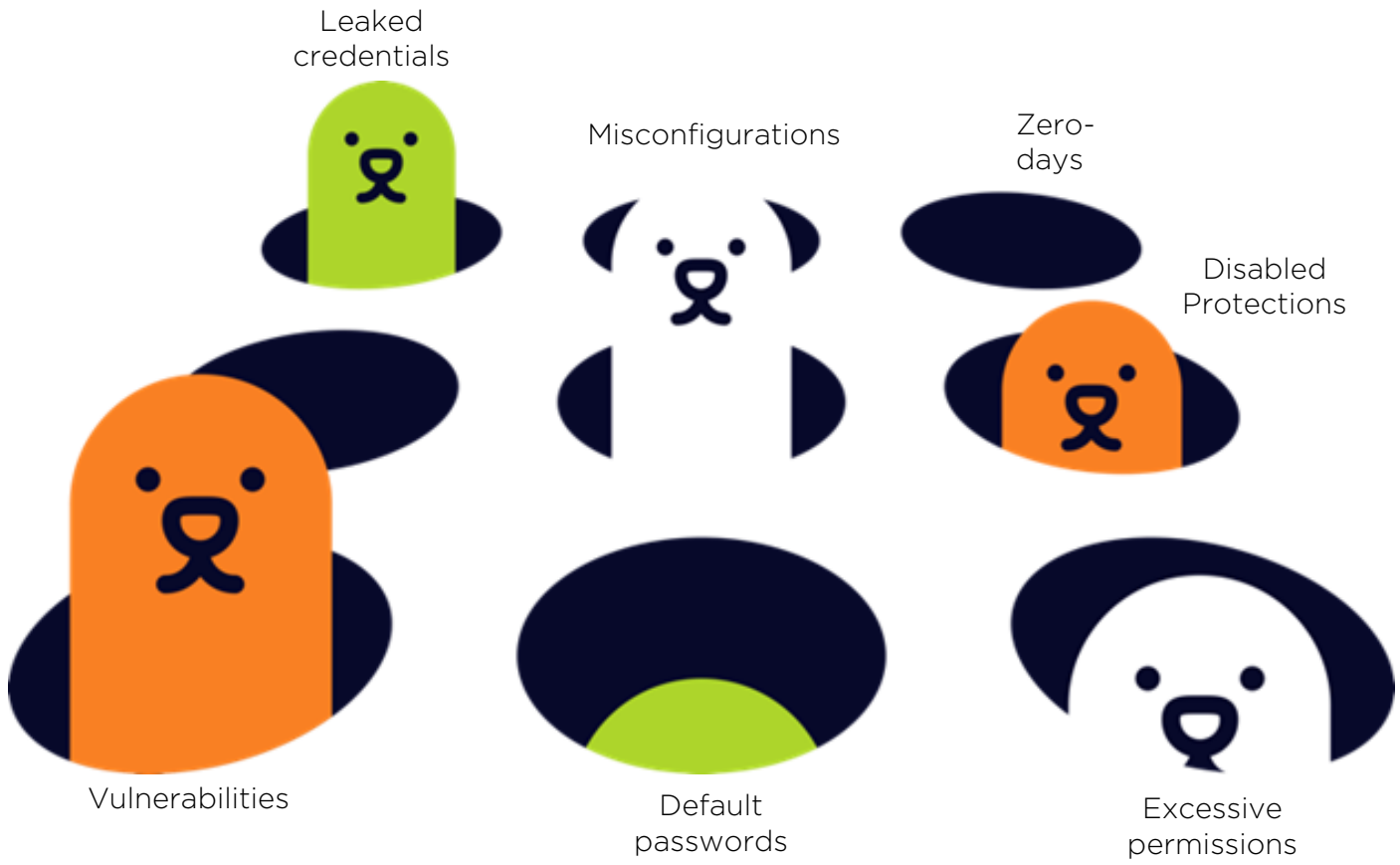



Every organisation needs understanding of their attack surface, exposures, and possible attack paths

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?

## Threat Exposure Management

# Risk Management

RISK = PROBABILITY x IMPACT

Exposure Management

### Factors impacting criticality of exposure

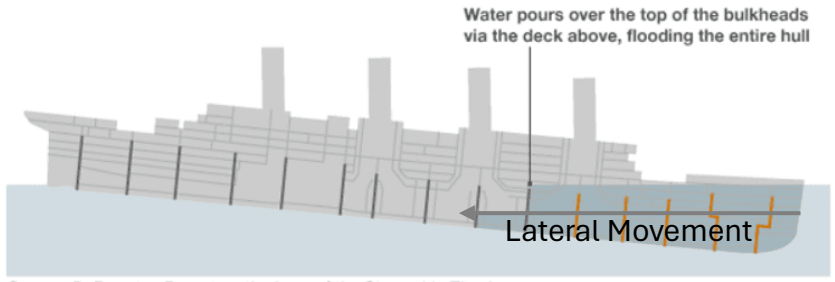
1. Exploitation Impact
2. Asset criticality
3. Active exploitation in the wild
4. Presence in multiple attack paths

## CRITICALITY OF EXPOSURE = LIKELIHOOD OF EXPLOITATION x IMPACT OF EXPLOITATION

**Asset criticality alone is not sufficient to determine the priority of remediating an exposure**

## Threat Exposure Management overview

# Exposure remediation prioritisation is vital




**Bulkheads not watertight**

**Threat**

**Invalid breach assumption**

**Exposure**

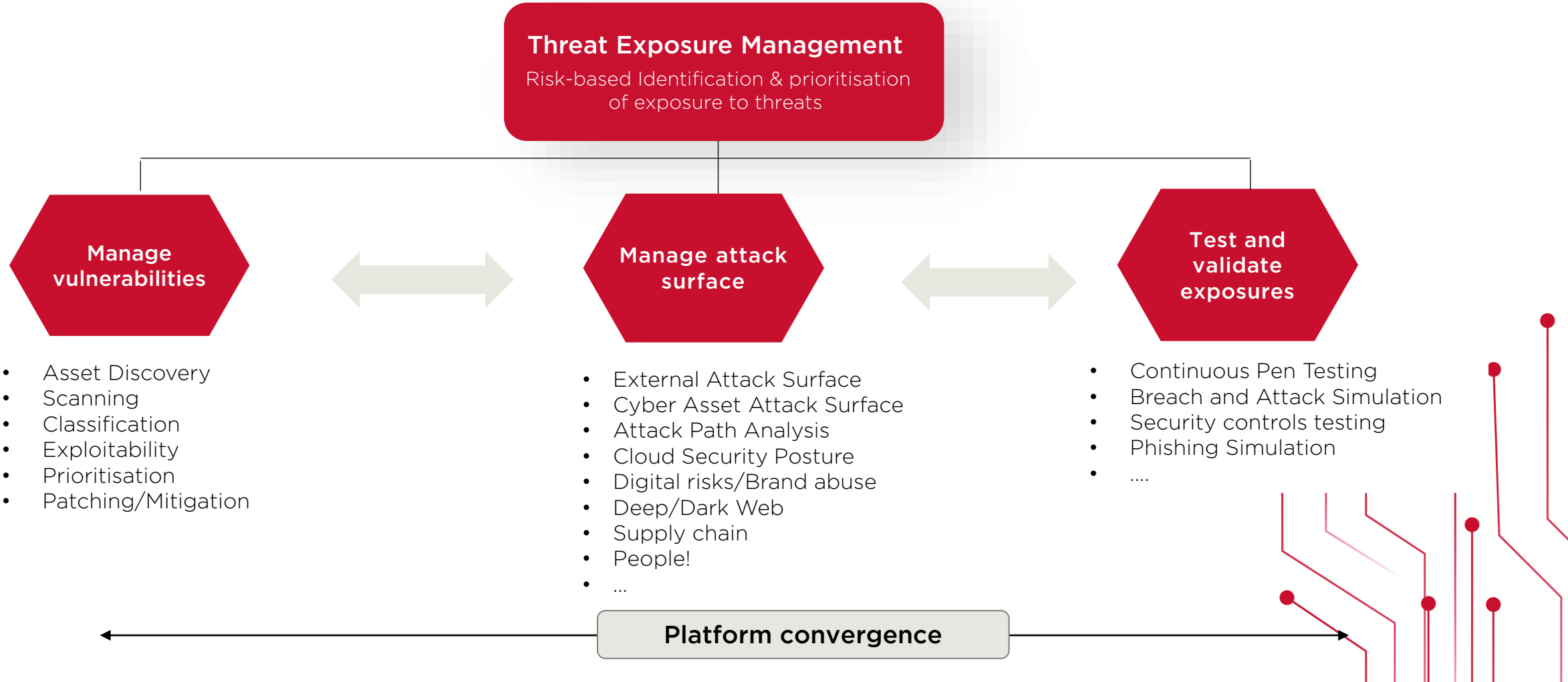

*"Someone could trip on these!"*

### 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

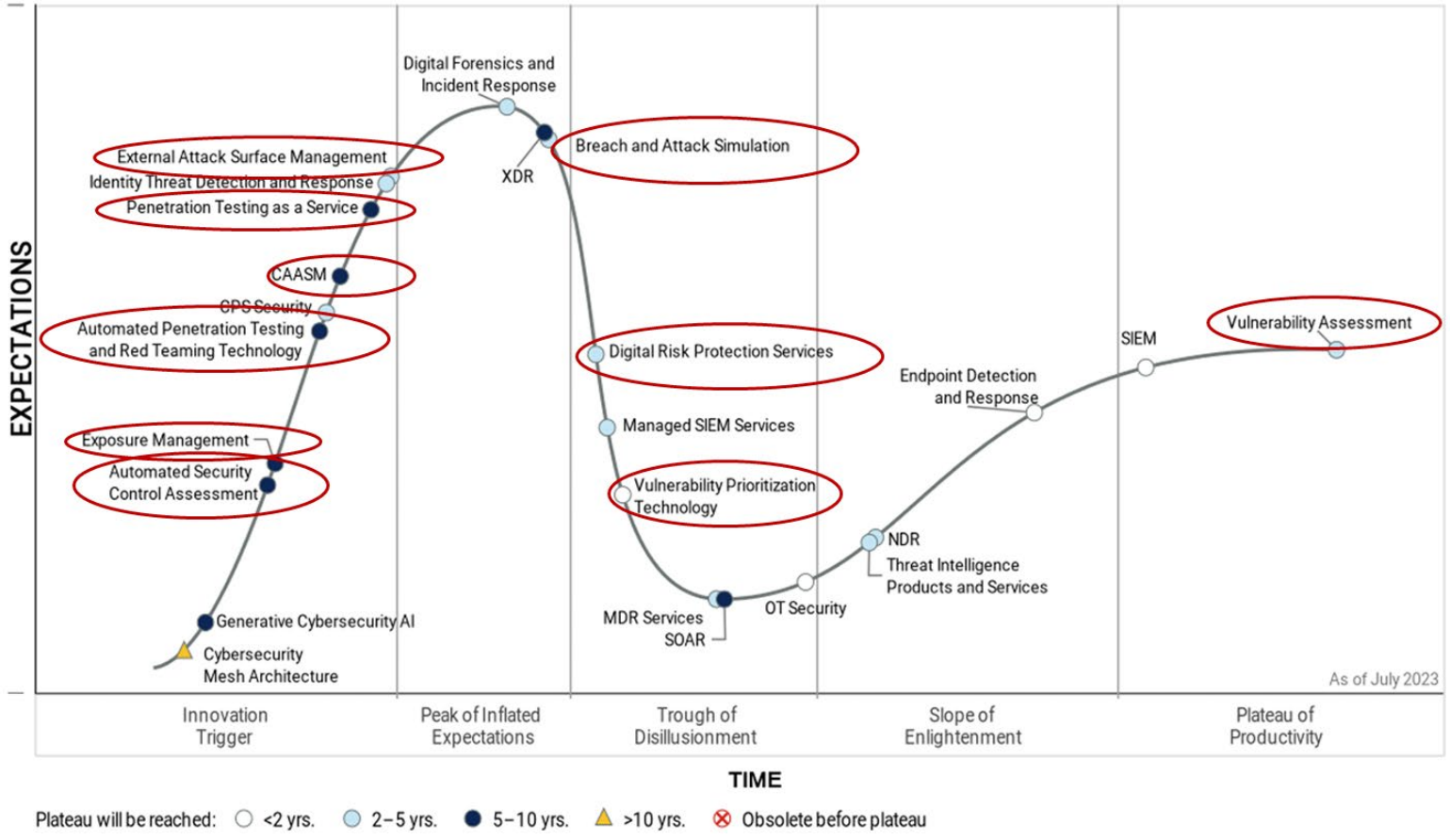
## Threat Exposure Management overview

# Components of Exposure Management



## Threat Exposure Management

# Most emerging tech in Security Operations relates to better managing exposures




**Mature**

- Vulnerability Assessment

**Emerging**

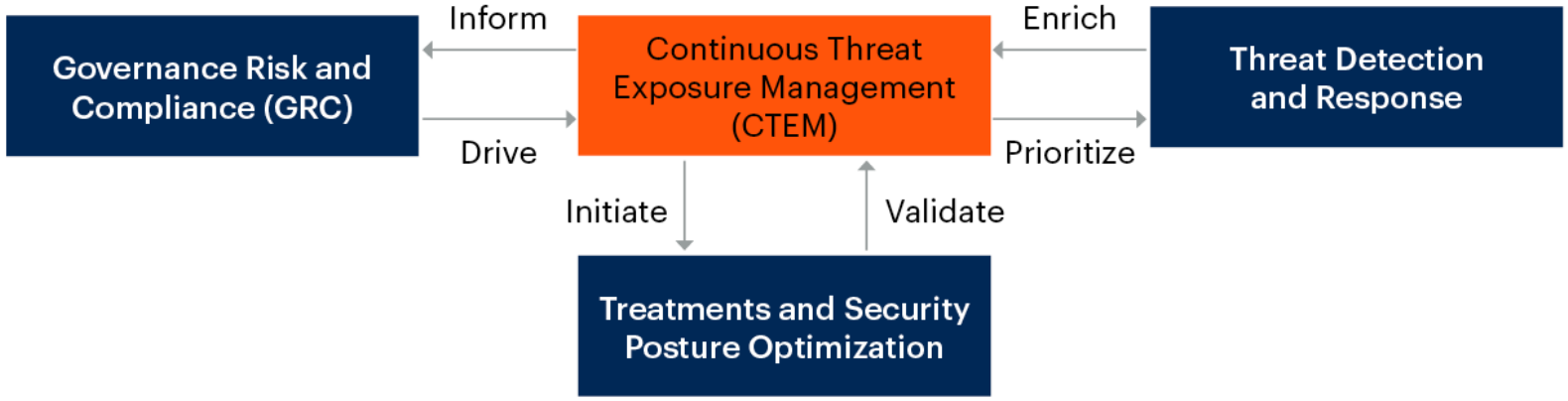
- Vulnerability Prioritisation
- Digital Risk protection
- Testing for Exposures
  - BAS
  - PTaaS
  - Automated PT
  - Automated security controls assessment
- Attack Surface Mgmt:
  - EASM
  - CAASM

- **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.*



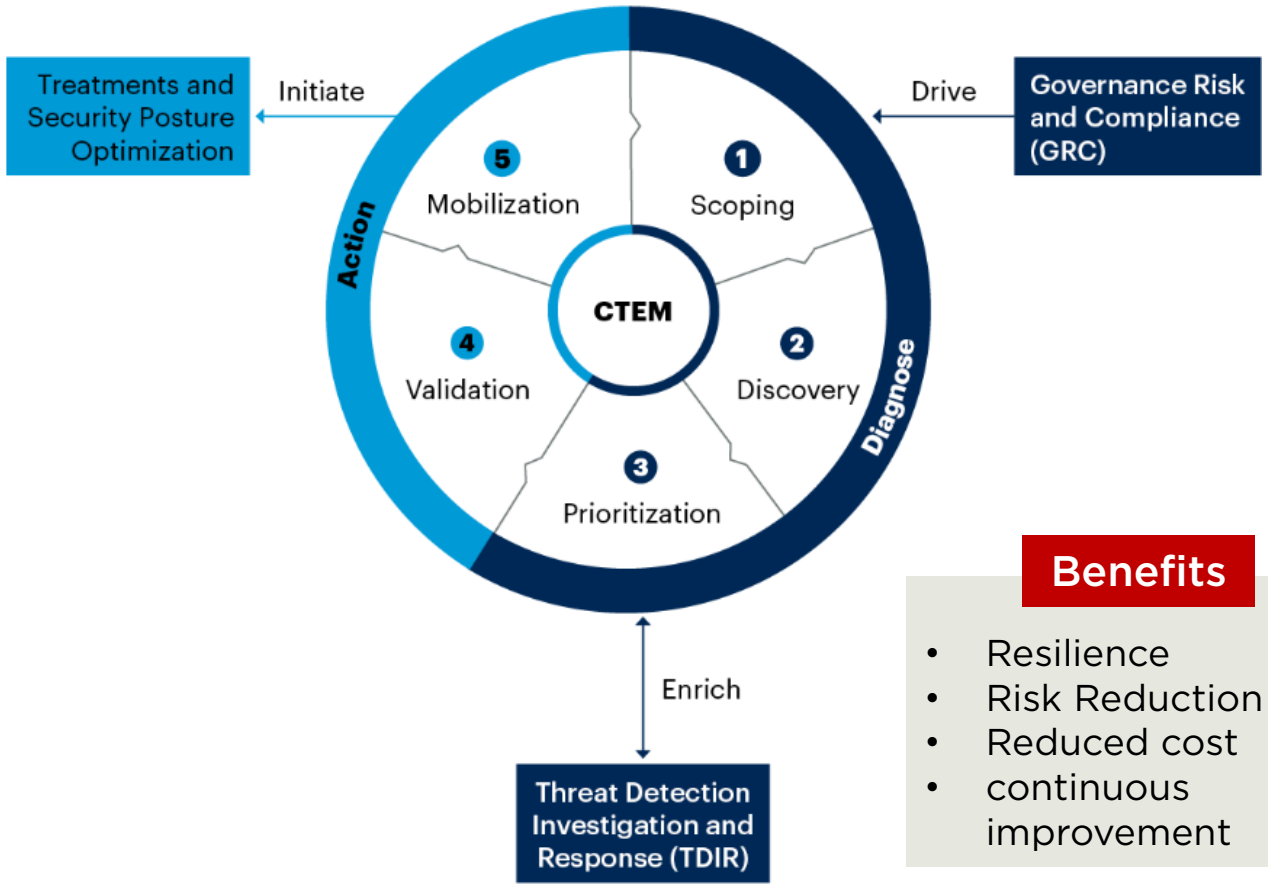

**Both the attackers' and defenders' views need to be combined to minimise an organisations exposure to present and future threats**

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

## Threat Exposure Management

# The phases of a CTEM Programme




**Benefits**

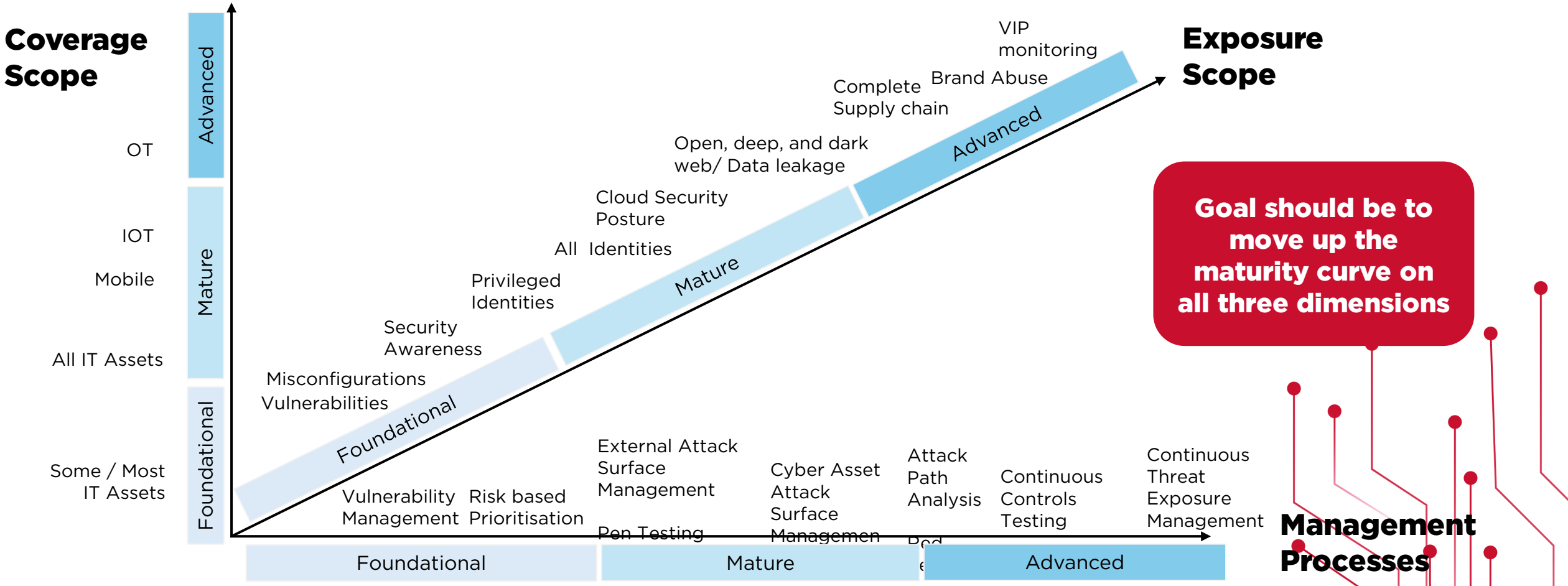
- Resilience
- Risk Reduction
- Reduced cost
- continuous improvement

***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

# Maturity dimensions for Threat Exposure Management

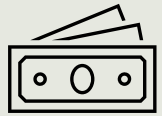



**Goal should be to move up the maturity curve on all three dimensions**

## Threat Exposure Management

# Benefits of Continuous Exposure Management (CTEM)

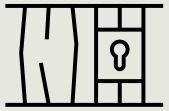
### Risk reduction
CTEM helps prioritise risk reduction actions & optimise resource usage



### Cost optimisation
CTEM allows biggest return on investment on mitigation activities

### Enhanced resilience
CTEM makes organisation more resilient against attack

### Improved prioritisation
Enables focus on business-critical threats, vulnerabilities & exposures



### Response preparedness
Knowledge gained from CTEM can assist security teams detect and respond to threats more effectively

### Continuous improvement
CTEM adopts a continuous process of monitoring, evaluating & enhancing threat exposures

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

# 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
- Implement a Continuous Threat Exposure Management programme

# Thank you

Integrity360
your security in mind

# Thank you

Brian Martin
brian.martin@integrity360.com

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

#SecurityFirstDublin