A&O SHEARMAN

Threat intel and incident management

Thursday 29 January 2026

Chair

Martin Smith MBE
Chairman and Founder, The SASIG

Host

Ffion Flockhart
Partner, Global Head of Cybersecurity,
A&O Shearman

Agenda for today…

9.30am Registration, coffee and networking

10am Welcome and introductions

10.15am Keynote: Update on the current threat landscape

10.45am Panel: Transformational risk management

11.30am Networking break with tea and coffee

12noon Cloud-Native Threat Intel: From Hidden Blind Spots to Proactive Protection

12.30pm How should industry and regions follow up on the UK Cyber Growth Action Plan?

1pm From Dark Web Leak to IR Fix: Preventing the Next JLR-Scale Disaster

1.30pm Networking lunch

2.15pm Stories from the cyber frontline

2.45pm The Ecosystem of a Cyber Incident

3.45pm Panel: How businesses should prepare for the cyber threats of 2026

4.15 - 5pm Drinks reception

House rules

Respect others
The Chatham House Rule must be universally respected – please do not attribute anything shared today. Phones should also be turned to silent, though you are free to leave the room for calls if needed.

Take part
We welcome questions or comments – don't forget to introduce yourself when you join the conversation. Be sure to make five new friends throughout the day, too!

Give us your feedback
Let us know what you thought of today's event as well as any ideas you have for the future using our short survey – there will be a QR code available today and we'll email you a link.

Get involved
Fancy taking to the stage yourself? Speak to the team or drop us an email. Don't forget to follow us on LinkedIn and share SASIG with your colleagues, too.

Upcoming webinars

AI in Modern SOC: From Theory to Reality
11am, Wednesday 4 February

Getting out of the Perfect Storm: Why It's OK to Step Away
11am, Friday 6 February

Winning the Talent War: Cybersecurity hiring strategies for 2026
11am, Thursday 12 February

Behind the Curtain: Securing Microsoft 365 against cybersecurity threats
11am, Friday 13 February

View the full calendar at www.thesasig.com/events

Upcoming in-person events

Cybersecurity Awareness SASIG: Awareness and Human Risk Management
Tuesday 10 February – London

Scotland SASIG: Resilience & Preparedness – Strengthening Cyber Defences
Tuesday 24 February – Glasgow

Risk and Cyber Insurance
Thursday 19 March – London

What Makes CISOs Buy
Tuesday 24 March – London

View the full calendar at www.thesasig.com/events

Our Supporters and Contributors

A special thanks to our Supporters, Contributors and all the speakers who share their expertise with us.

A&O SHEARMAN

Threat intel and incident management

Thursday 29 January 2026

Chair

Martin Smith MBE
Chairman and Founder, The SASIG

Host

Ffion Flockhart
Partner, Global Head of Cybersecurity,
A&O Shearman

Keynote presentation: An update on the current threat landscape

Ffion Flockhart
Partner, Global Head of Cybersecurity, A&O Shearman

Panel Session: Transformational risk management

Facilitator

Jim Mulheron Board Advisor, Technology Risk Insights

Panellists

Yolande Young CISO, A&O Shearman
Rois Ni Thuama GRC Expert, RT Consulting
David Porter Senior Adviser Emerging Threats, Bank of England

Tea, coffee & networking break

We'll be back at 12pm

Please scan here to give us your feedback on today's event

Cloud-Native Threat Intel: From Hidden Blind Spots to Proactive Protection

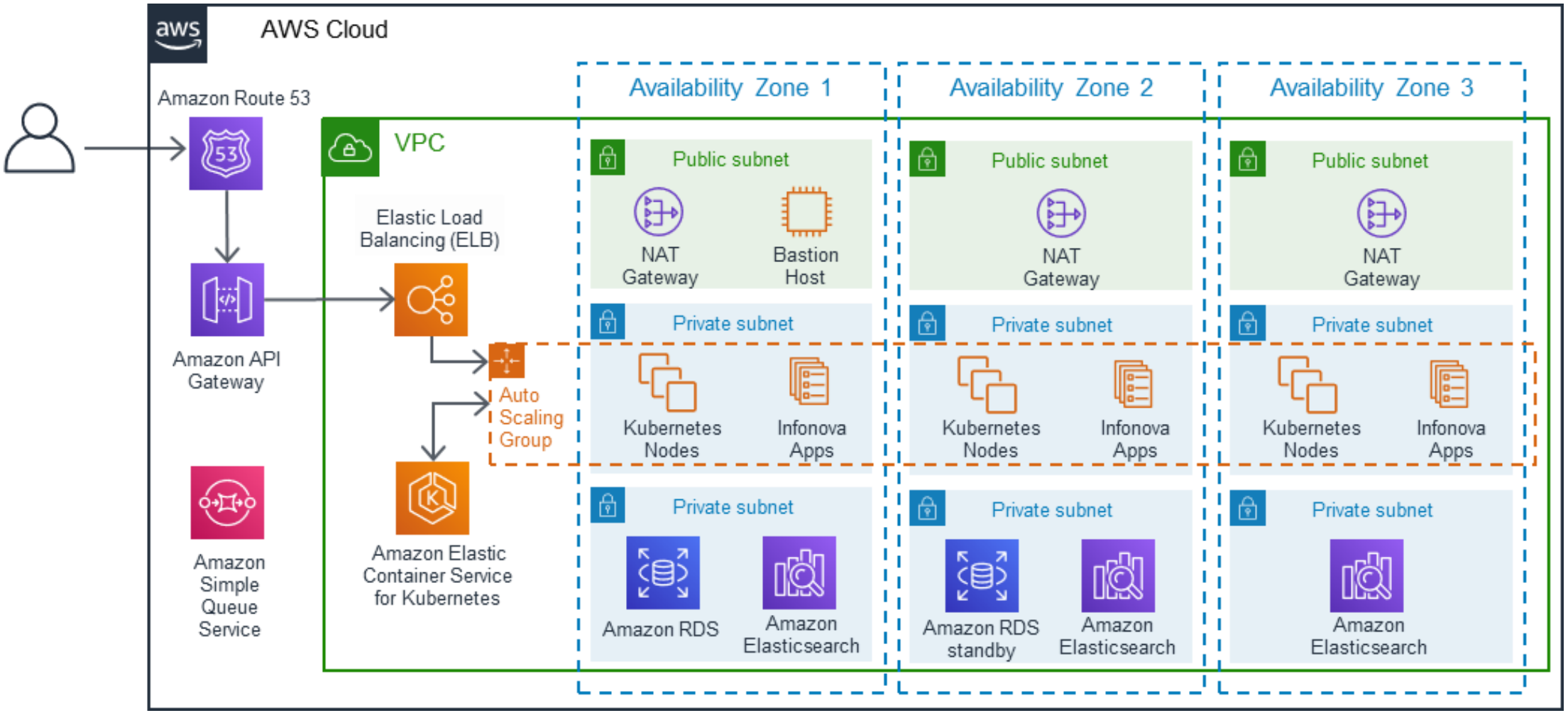
David Greenwood
Cloud Native Security Specialist, Qualys

From Silos to Synergy: Navigating the CNAPP Revolution

David Greenwood

Cloud Native Security Specialist

No longer just somebody else's computer...



The Operational Burden

Alert Inundation:

- 71% of security teams receive more than 500 cloud security alerts per day.

Visibility Gap:

- 52% of IT professionals report limited visibility into their cloud workloads, a significant jump from 35% just two years ago.

Tool Sprawl:

- 57% of organisations use 5 or more separate public cloud security tools.

Alert Fatigue & Human Impact

Ignored Alerts:

- Security analysts are unable to deal with **67% of daily alerts** on average due to volume and lack of context.

Missed Critical Threats:

- 55% of security teams admit to missing critical alerts on a daily or weekly basis.

False Positive Noise:

- Over 40% of all generated alerts are **false positives** that waste valuable investigative time.

The Retention Crisis:

- Alert fatigue contributes to turnover in **62% of organisations**. In fact, 70% of SOC analysts with less than five years of experience leave their roles within three years.

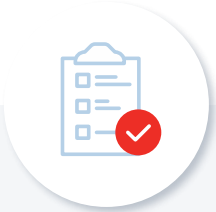
Where does this leave us?

- As of 2025, 82% of all data breaches involve data stored in the cloud.
- Organizations now face an average of 1,925 cyberattacks per week, a 47% increase since 2024.
- 99% of cloud security failures through 2025 are predicted to be the customer's fault, primarily due to misconfigurations.
- Cloud environment breaches jumped 75% between 2022 and 2023 alone. Ransomware incidents saw a 126% increase in Q1 2025

The Major Challenges

Cloud Team

- Remediated Cloud Risks are resurfacing
- **Increased attack surface** generates more findings
- Managing risks in **ephemeral environments** is always challenging.



Compliance Team

- Always **get exception** requests with no concrete plans to remediate
- Unaddressed compliance issues persist for a long duration
- Security Policies are evolving at a later stage

Developers

- **Many security issues** with no context for prioritization.
- Releases are rejected at a very late stage, delaying product rollouts.
- Security concerns are addressed too late in the development process.

Enter the CNAPP

Kubernetes and Container Security (KCS)

Prioritize Risks In Container Environments

Manage Risk Across The Dev Lifecycle

Cloud Detection & Response (CDR)

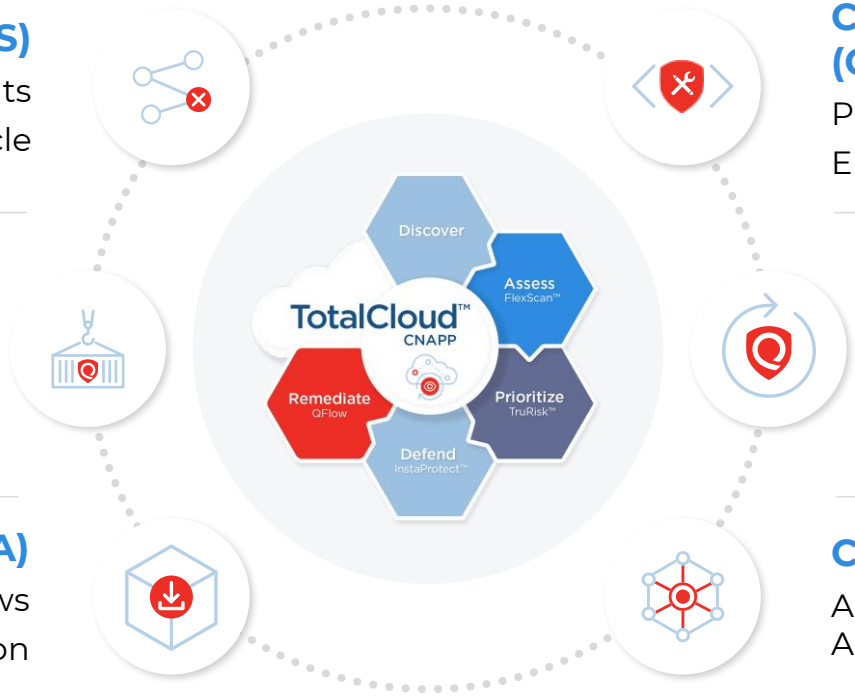
Detect Malicious Threats In Runtime

Respond To Zero-Day Malware

Cloud Workflow Automation (CWA)

Implement Custom Remediation Workflows

Leverage 200+ Playbooks for Remediation



Cloud Security Posture Management (CSPM)

Prioritize Risk With Attack Path Context

Enforce Compliance From Code To Cloud (IaC)

Cloud Infrastructure and Entitlement Management (CIEM)

Manage Excessive Permissions and Identities

Enforce Least Privilege At Scale

Cloud Workload Protection (CWP)

Achieve Full Vulnerability Coverage With Agent, Agentless, Network, and API Scanning

aws Azure Google Cloud ORACLE Cloud

Contextualising the data

Asset Level Risk Score

Complete 360 Context with Threat Intel

TruRisk

TruRisk Score

Correlate signals from many source

Toxic Combination

TruRisk Insight

Visualize Attack Path exposure

Blast Radius impact analysis

Attack Path

Risk Exposures

QualysTruRisk™

Combines Asset Environmental Factors Considers Only

- Active Service/Process
- Attack Path
- Public Exploit
- Public Asset Exposure

Medium	CVE-2023-44487
High	CVE-2020-1147
Critical	CVE-2021-41303
Low	CVE-2023-42282
High	CVE-2025-0411
Medium	CVE-2020-11023

Medium	CVE-2023-44487
Low	CVE-2023-42282
High	CVE-2020-1147
High	CVE-2025-0411
Medium	CVE-2020-11023
Critical	CVE-2021-41303

Qualys Threat DB of 25+ Threat Intel Sources

Qualys Research

Vulnerability Environmental

McAfee, FireEye, packet storm, GitHub, CISA, MISP Threat Sharing, Canadian Centre for Cyber Security, VDE, Reversing Labs, metasploit, GreyNoise, MITRE ATT&CK, Kaspersky Industrial CyberSecurity, Talos, Google, EPSS

- Dark web chatter
- Trending patterns
- POC vs Weaponization
- Easy vs complex exploitation (remote vs local)
- Threat actors associated
- Exploited by Malware, Ransomware?
- Celebrity

100
95
90
80
70
60
50
40
30
20
10

CVE-2023-44487

- POC of Exploit Exists
- Unattributed Threat Actors
- Trending In Mar & Apr 2025
- CISA Known Exploited Vulnerabilities
- CVSS – **7.5** & EPSS – **0.94437**

CVE-2020-1147

- POC Exists and Weaponized
- CISA Known Exploited Vulnerabilities
- Trending in Mar & Apr 2025
- CVSS – **7.8** & EPSS – **0.92695**

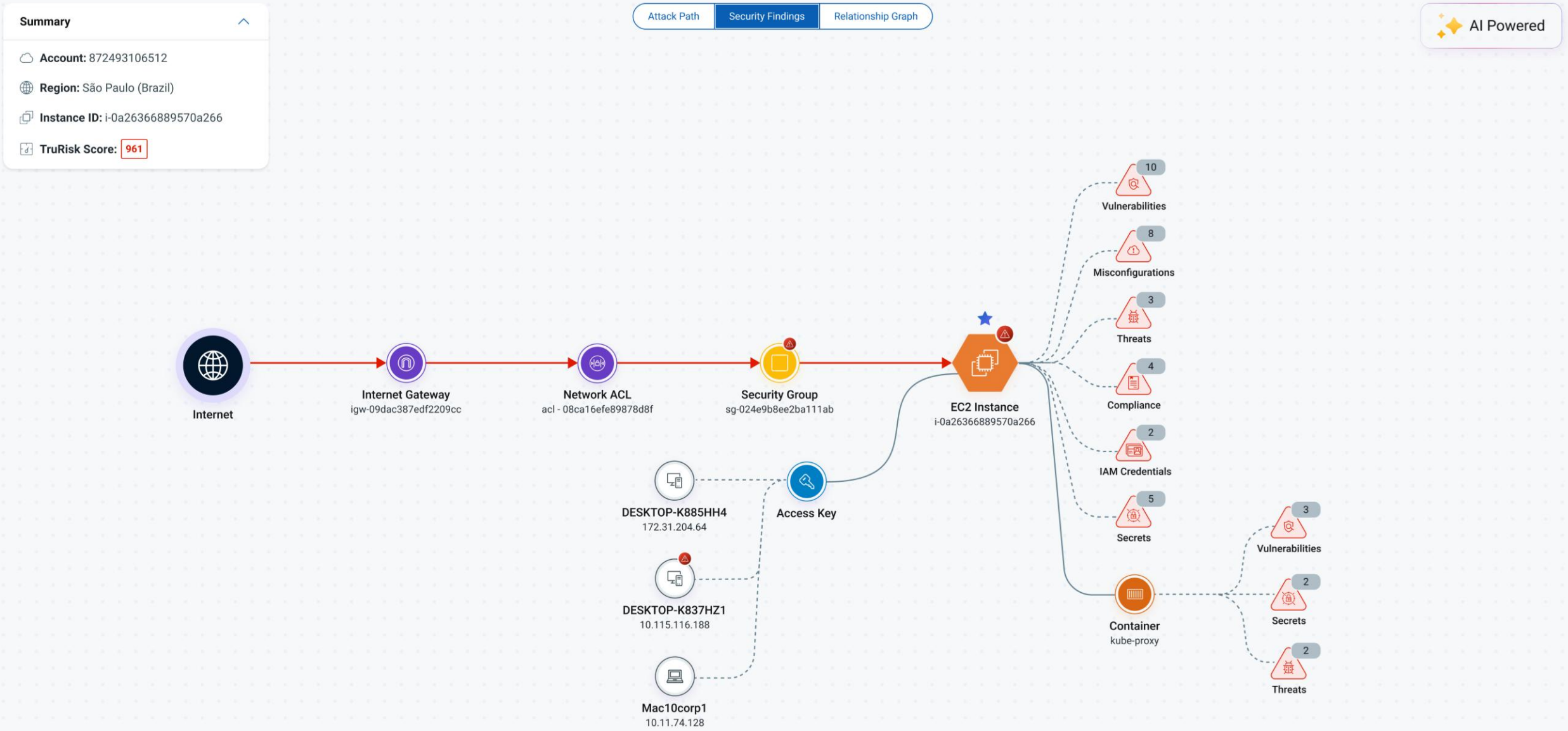
CVE-2020-11203

- POC of Exploit Exists
- Threat Actors – **Emissary Panda, Comment Panda**
- CISA Known Exploited Vulnerabilities
- Trending in Mar & Apr 2025
- CVSS – **6.1** & EPSS – **0.11526**

CVE-2021-41303

- Last Trending in Mar 2025
- CVSS – **9.8** & EPSS – **0.65449**
- CVE Is Not Exploited and No
- Other Significant Contributing Factors Observed

← Attack Path: **Public VMs with critical vulnerabilities and malware, along with risky IAM credentials**



The "Shift Left" Challenge

Shift-Left Security
Proactive Approach

Runtime Security
Reactive Approach

Pre-Deployment

Infrastructure as Code (IaC)

Terraform
Cloud Formation
ARM Template

Repository and Registries

GitHub
Bitbucket
Gitlab

CI/CD

Jenkin
Bamboo

Post-Deployment

Cloud

Instance/Containers/ Serverless/WebApp

Resources

Identities

The Effect of Context

Tool Consolidation:

- Average of 30-40% on licensing costs by consolidating separate CSPM, CWPP, and CIEM tools into a single unified platform.

Time Savings:

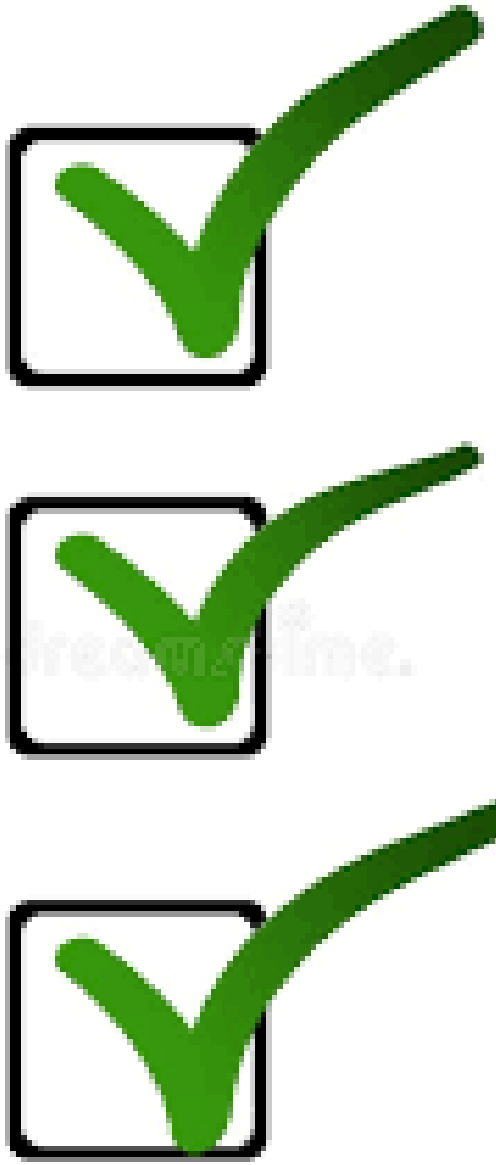
- One major enterprise study showed that a unified CNAPP allowed a single security engineer to manage 5x more cloud workloads than they could using siloed point solutions.

80% Reduction in Critical Alerts:

- Enterprises adopting CNAPP typically see an 80% drop in high-priority alerts by moving from "vulnerability counting" to graph-based context.

90% Faster Mean Time to Repair:

- By identifying the exact "Toxic Combination" teams can remediate threats in minutes instead of days.



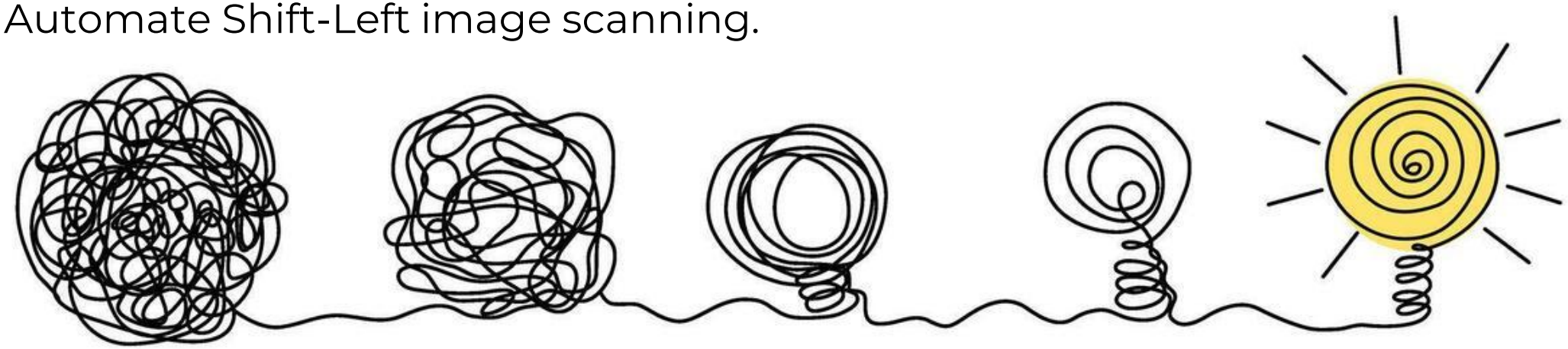
The North Star of Alert Context

Consolidation over Fragmentation

Complexity is the attacker's best friend. Context is yours.

Immediate Actions:

- Map your K8s attack surface.
- Kill "Toxic Combinations" (Identity + Vulnerability).
- Automate Shift-Left image scanning.



How should industry and regions follow up on the UK Cyber Growth Action Plan?

Professor Simon Shiu

Visiting Professor of Cybersecurity, Bristol University

University of BRISTOL

CYBER GROWTH ACTION PLAN

HOW SHOULD INDUSTRY AND REGIONS FOLLOW UP

Simon Shiu

Representing: Alex Greenwood, Chris Hankin (IC), Lisa Kehoe and Martin Sadler

Funded by Centre for Sectoral Economic Perfrmance (CSEP)

bristol.ac.uk

IMPERIAL

CGAP - Focus on ‘UK growth’

Input from
Industry ++


GOV.UK Menu

Home > Government > Cyber security > Cyber Growth Action Plan 2025

Department for Science, Innovation & Technology

Policy paper

A UK cyber growth action plan - final report

Updated 19 September 2025

Contents

Executive summary
1. Introduction
2. A culture for cyber growth
3. Supply and demand
4. Places
5. Futures
6. Strategy alignment
7. Conclusion and next steps
8. Technical annex

Annex: Bibliography and references

Annex: Table of recommendations

Print this page

Presented to Parliament by the Parliamentary Under-Secretary of State for Science, Innovation and Technology by Command of His Majesty

September 2025

CP 1406

ISBN 978-1-5286-5971-0

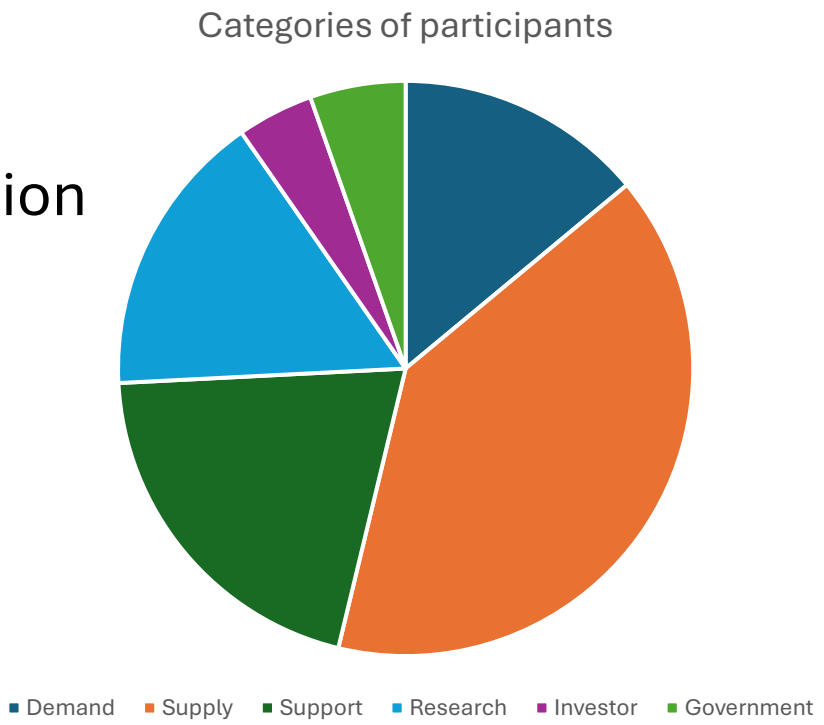
This report is the output from an independent, rapid analysis to provide key insights on the interventions needed to further develop the UK's cyber security sector. Carried out by a team from the University of Bristol and Imperial College London, it builds on the Cyber Security Sectoral Analysis 2025[footnote 1] and the UK government's Modern Industrial Strategy. It was produced in time to feed into the refresh of the National Cyber Strategy.

The authors of this work were supported by and would like to thank the Centre for Sectoral Economic Performance at Imperial College London.

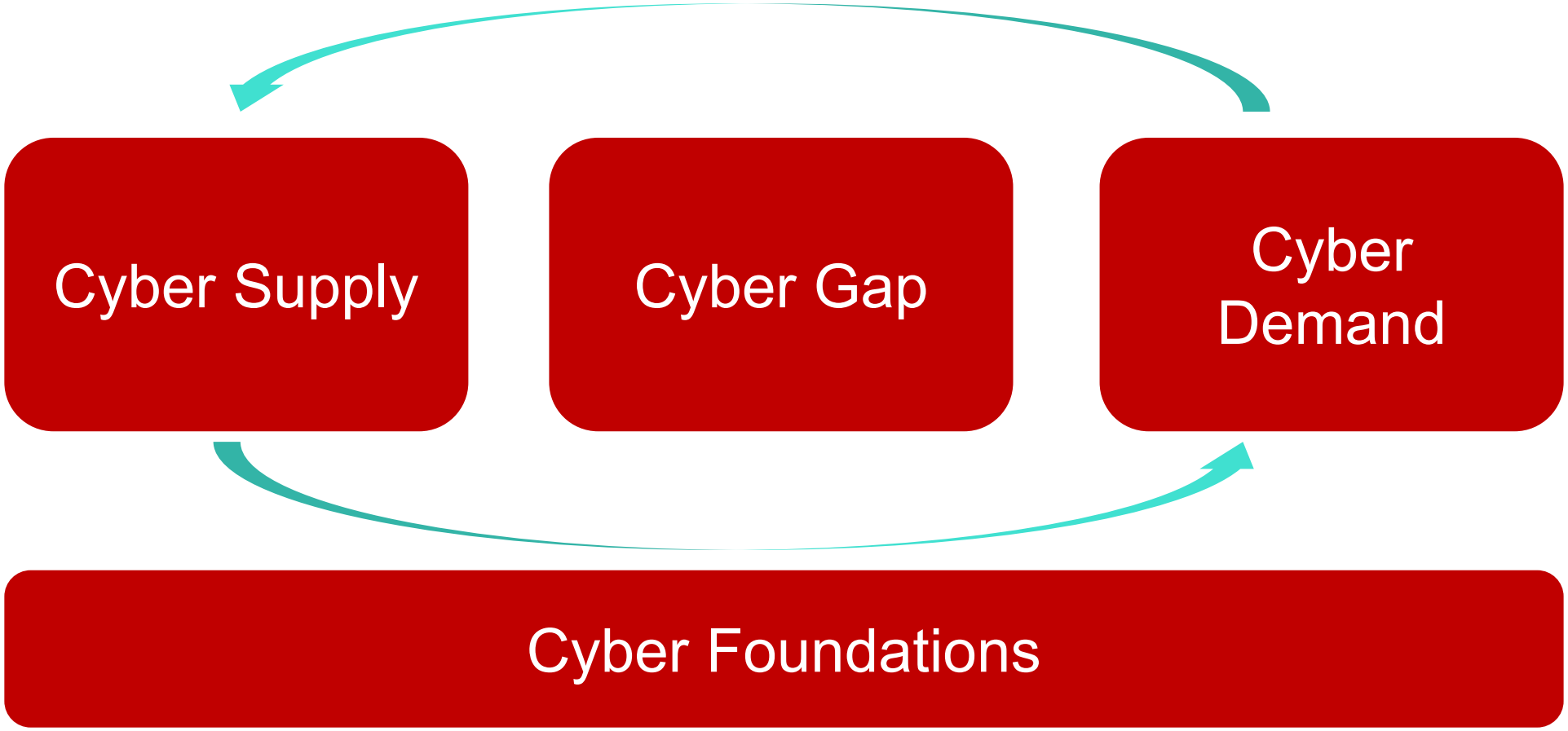
To Influence UK Cyber Action Plan in context of Industrial strategy

Informal Consultation Statistics

- 37 Supply side of Cyber
- 13 Demand side of Cyber
- 19 Support - Trade, Certification & Profession
- 15 Research Institutions
- 5 Government
- 4 Cyber Investors



The Cyber Sector is growing, but so is the Cyber Gap



Recommendations

Culture

1. Support growth journeys
2. Stimulate informed demand
3. Foster public participation in cyber skills & growth

Leadership

4. Appoint a Cyber Ambassador
5. Appoint leaders in places of strength
6. Expand NCSC role

Places

7. Develop futures communities
8. Places to nurture chosen tech areas
9. Places for safe environments

Underlying Principles

The UK cyber sector should act as one team
Growth + Resilience + Value for money

Cyber Growth Action Plan - Reactions

- HMG responding through UK Cyber Action Plan
  - Reinforced by Minister Lloyds first speech on cyber
- Visible industry response positive
  - Several online articles (TechUK, NCC, UKC3…)

Aligning UK demand with UK supply

The UK Cyber Flywheel brings together founders, CISOs, operators, investors, and policymakers for one purpose: *to build a stronger, more connected, more resilient UK cyber ecosystem.*

https://www.ukflywheel.com/
(Next event April 9th London)

CSEP Phase 2 focus on ‘demand and places’

Culture

1. Support growth journeys
2. Stimulate informed demand
3. Foster public participation in cyber skills & growth

Leadership

4. Appoint a Cyber Ambassador
5. Appoint leaders in places of strength
6. Expand NCSC role

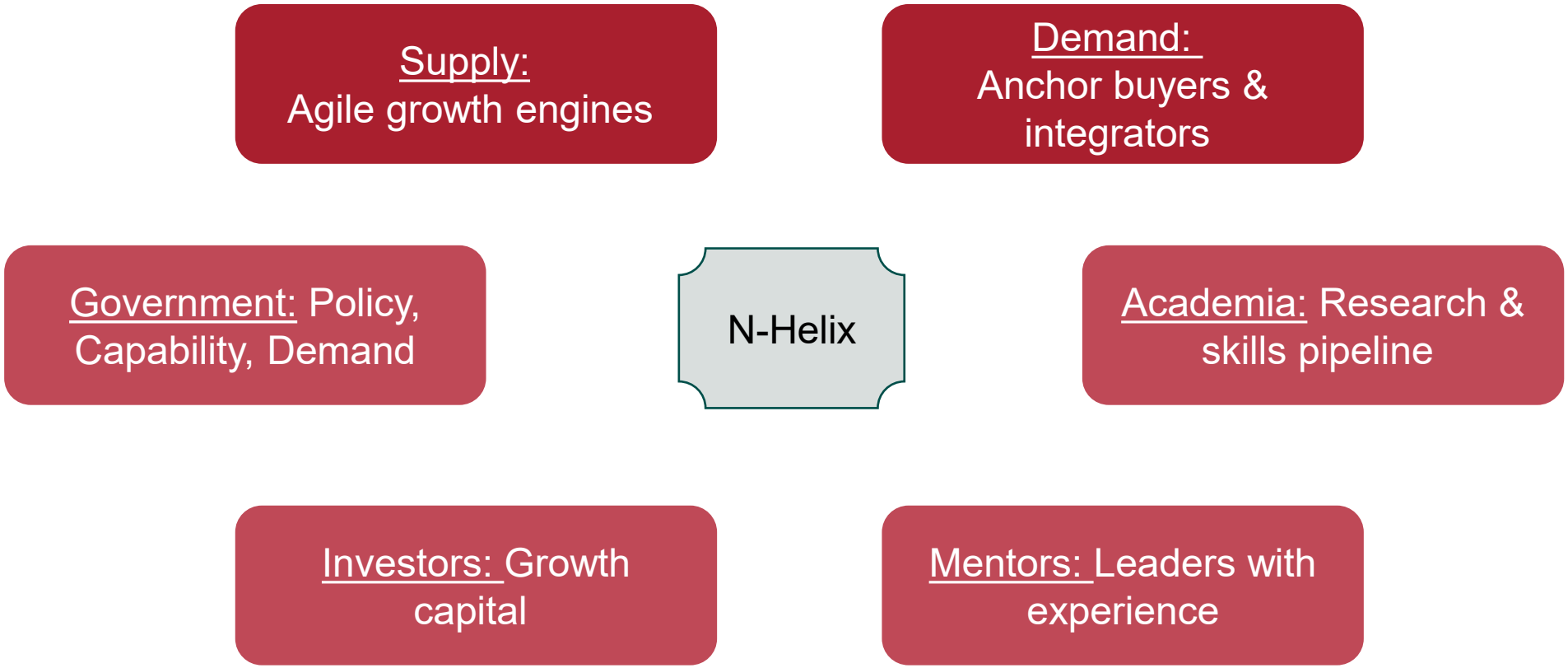
Places

7. Develop futures communities
8. Places to nurture chosen tech areas
9. Places for safe environments

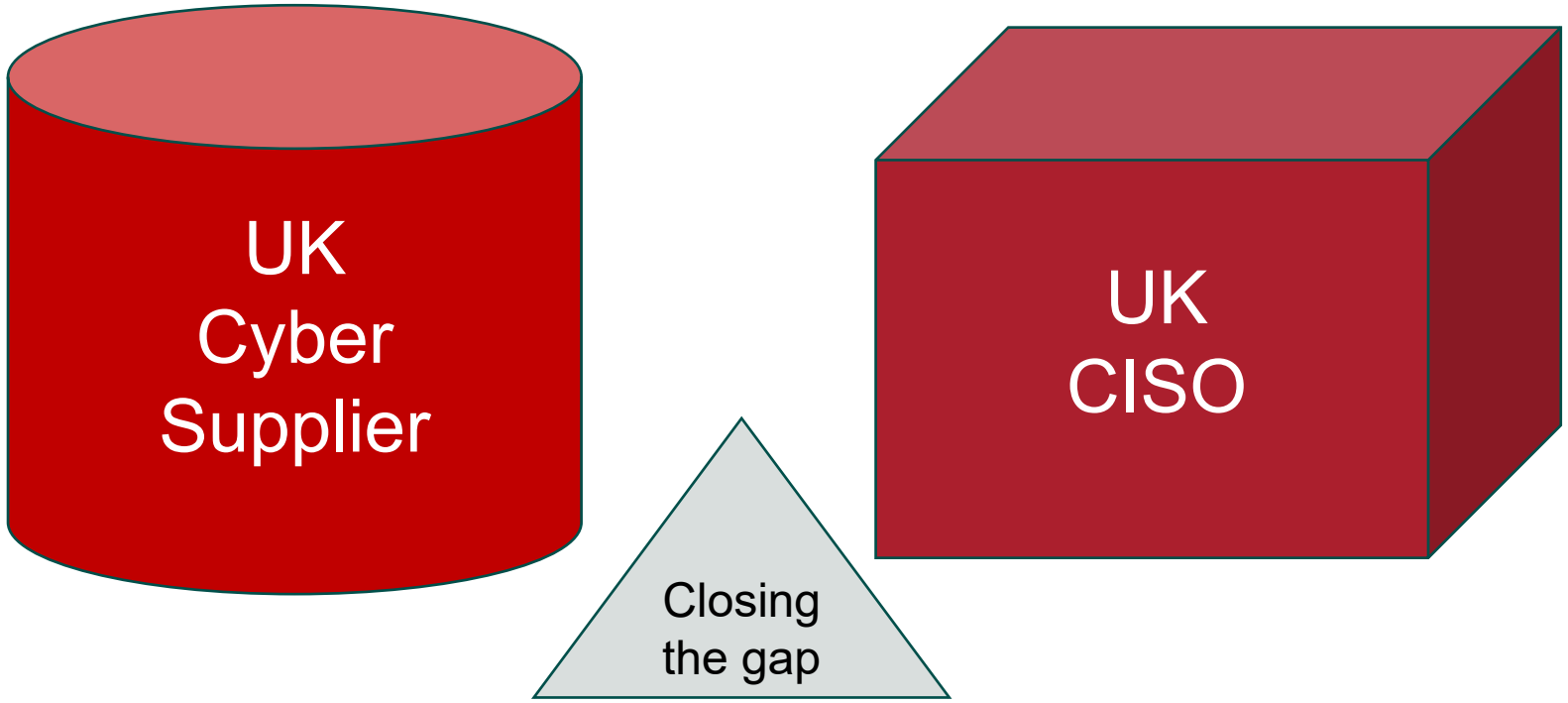
Underlying Principles

The UK cyber sector should act as one team
Growth + Resilience + Value for money

Bootstrapping places for focused growth



Anticipating the innovation challenges



Some starting points:
Areas ripe for growth and resilience

Assured use of AI

Cyber Physical

Tooling for fundamentals

Next Steps

- Please join us at the SASIG event on March 24th to go deeper!
- Please contact me before then too - simon.shiu@bristol.ac.uk

University of BRISTOL

THANK YOU

bristol.ac.uk

IMPERIAL

From Dark Web Leak to IR Fix: Preventing the Next JLR-Scale Disaster

Aviv Gabbay

Senior Sales Engineer, Kela

KELA

sasig

From Dark Web Leak to IR Fix

Preventing the Next JLR-Scale Disaster

Aviv Gabbay
Senior Sales Engineer

29 January, 2025

Agenda

- 2025 Threat landscape recap
- A closer look at the Jaguar Land Rover breach
- Integrating Identity and Brand Protection into IR
- The ROI of CTI

KELA

2025 Threat Landscape

Infostealers, Credentials, Ransomware

KELA

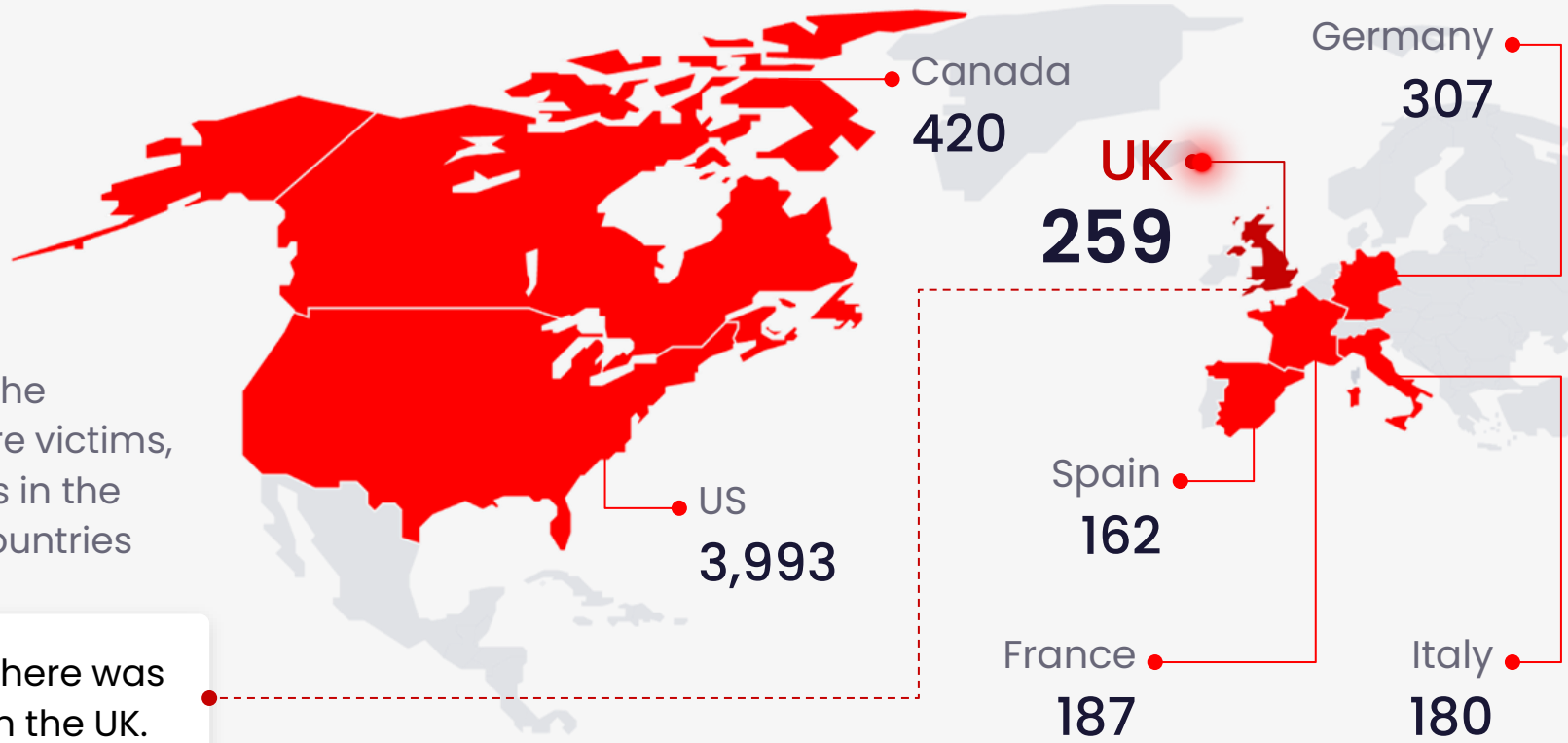
Ransomware & Extortion

The Victims

By Region

The US accounted for the majority of ransomware victims, (~53%) while the UK sits in the top 5 most targeted countries

Compared to 2024, there was an increase of **86%** in the UK.



By Sector

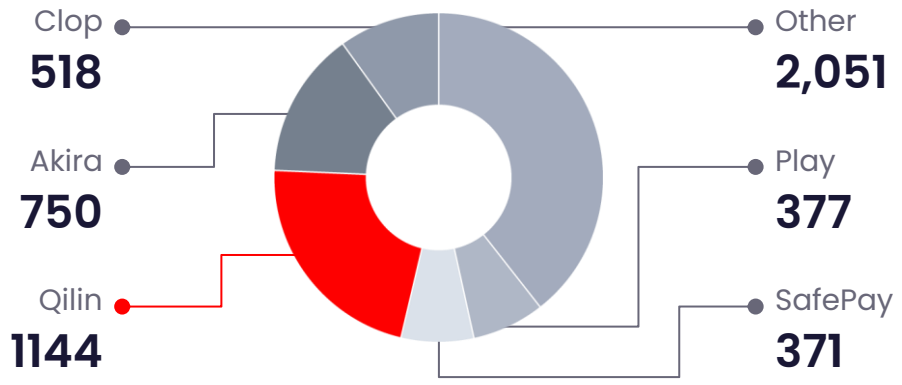
Manufacturing & Industrial Products and Professional Services are the most affected sectors this year.

This is consistent with 2024.

1356	Manufacturing & Industrial Products
1210	Professional Services
705	Engineering & Construction
696	Consumer & Retail
520	Healthcare & Life Sciences
3025	Other

The Actors

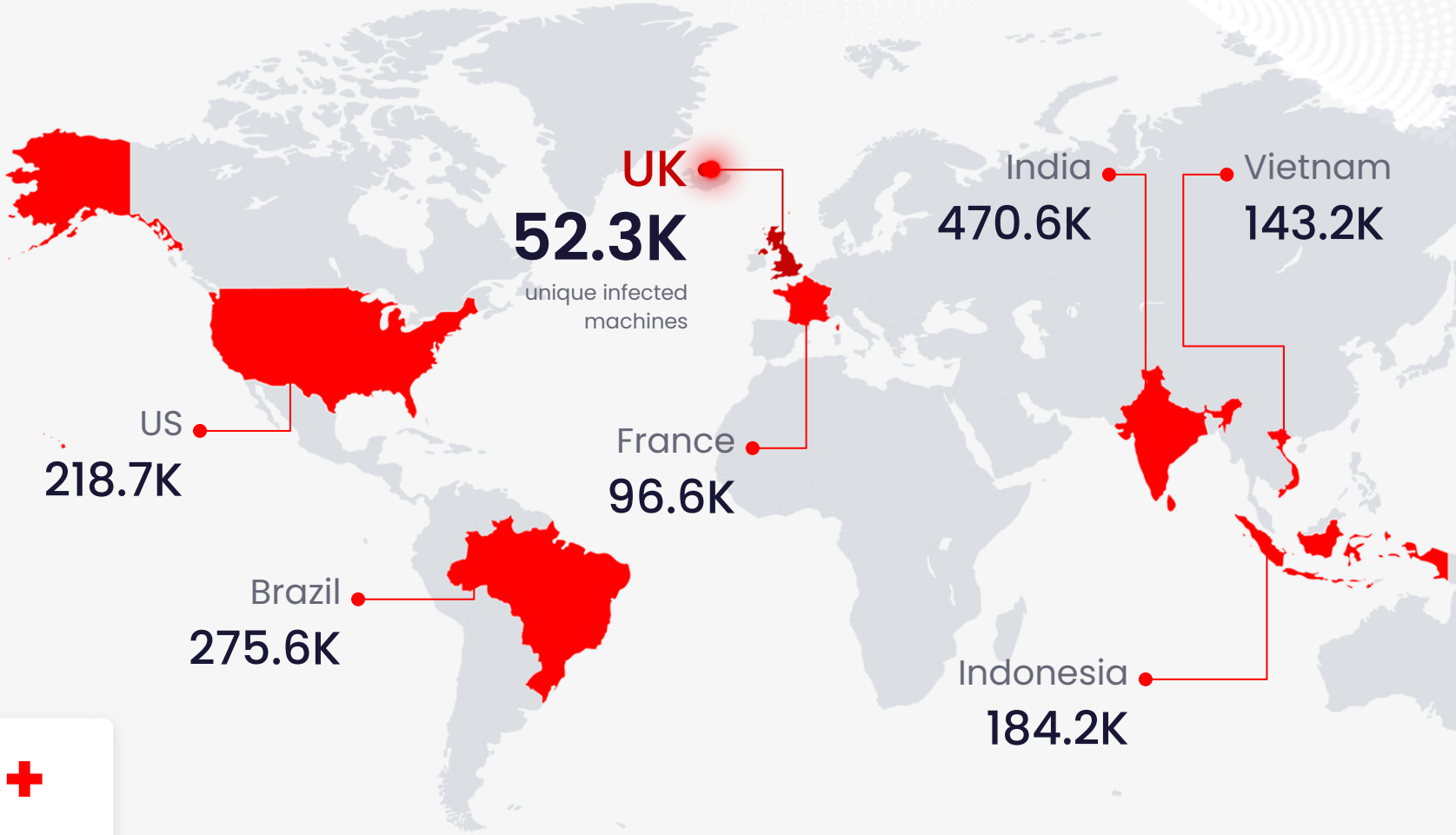
Qilin leads with **1K+ victim claims** (+525% YoY)



The Victims

The countries that experienced the **highest rates** of infostealer infections include:

- India
- Brazil
- United States
- Indonesia
- Vietnam



3.87M
infected devices

2.86B+
credentials

KELA

In 2025 KELA tracked...

3.87M+

machines infected by infostealers

204M+ credentials stolen

3.86B

credentials shared
overall on the dark web

7,547

ransomware victims

42% increase YoY

Attackers discuss
new CVEs within

1–2 days

Intercepting Underground Commerce

Most likely you will be infected, but a larger compromise can be prevented

KELA

Intercept Underground Commerce

Compromised Machines

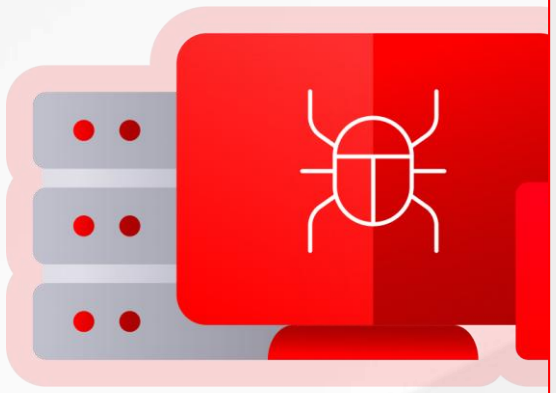
Personal machines, work laptops and others **infected by Infostealers**

- Logins and passwords
- Cookies
- Financial info
- PII
- System details

Monetization Channels

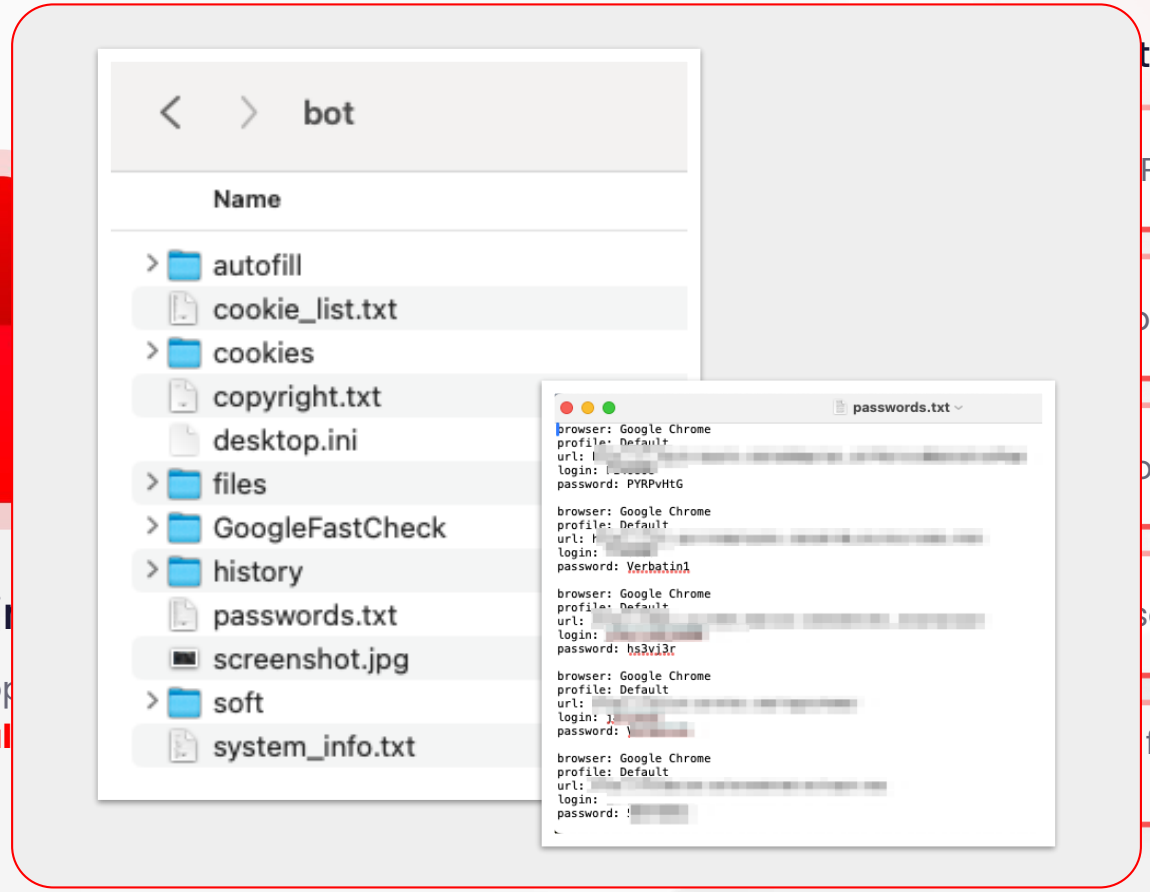
- Private sales
- Cybercrime forums
- Automated markets
- Subscription services
- ULP files on different mediums

Intercept Underground Commerce



Compromised Machi

Personal machines, work laptop
others **infected by Infosteal**



tization Channels

- Private sales
- bercrime forums
- omated markets
- scription services
- files on different mediums

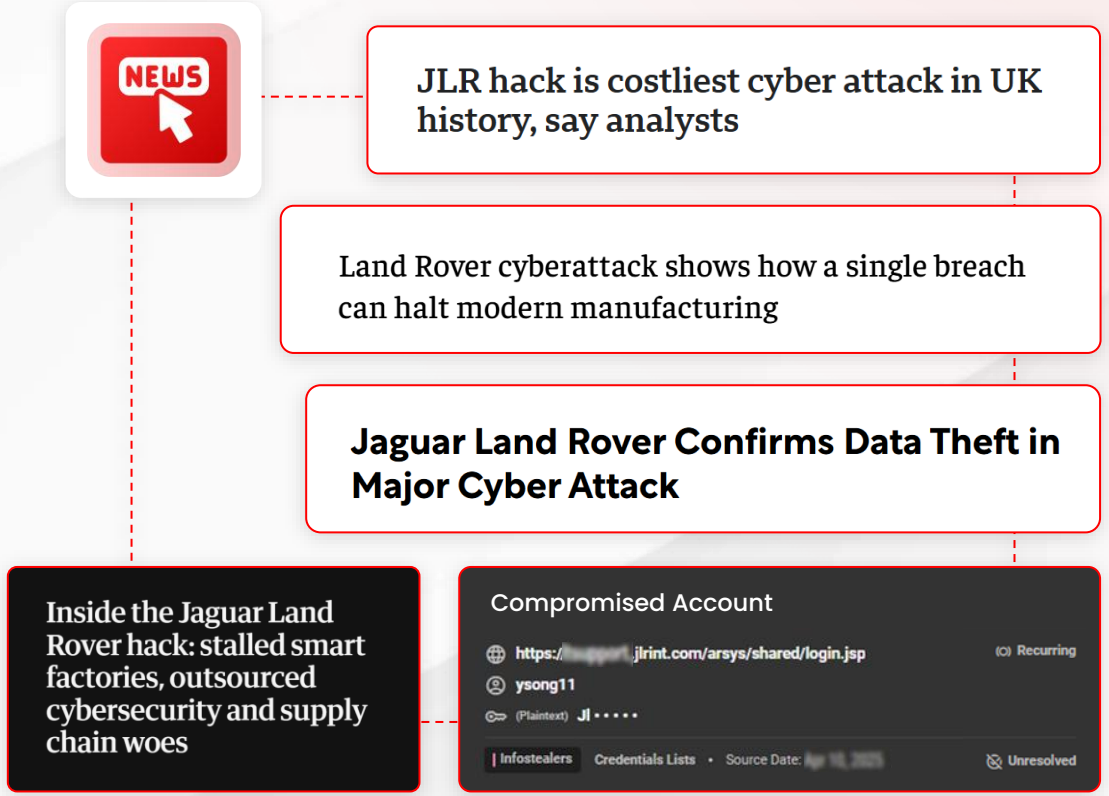
The JLR Breach

KELA

The Jaguar Land Rover Breach

What Happened?

- A massive "digital siege" launched on **August 31, 2025,** which forced Jaguar Land Rover to proactively shut down its global IT systems and halt all vehicle manufacturing.
- Claimed by **"Scattered Lapsus$ Hunters,"** a sophisticated alliance between the groups **Scattered Spider, Lapsus$,** and **ShinyHunters**
- **The group utilized "master keys" — valid employee credentials stolen as far back as 2021 — to bypass modern security layers and move laterally through the network.**
- Hackers exploited vulnerabilities in **SAP NetWeaver** and **Jira** project management tools to leap from administrative IT systems into the **Operational Technology (OT)** that controls the actual factory floor robots.



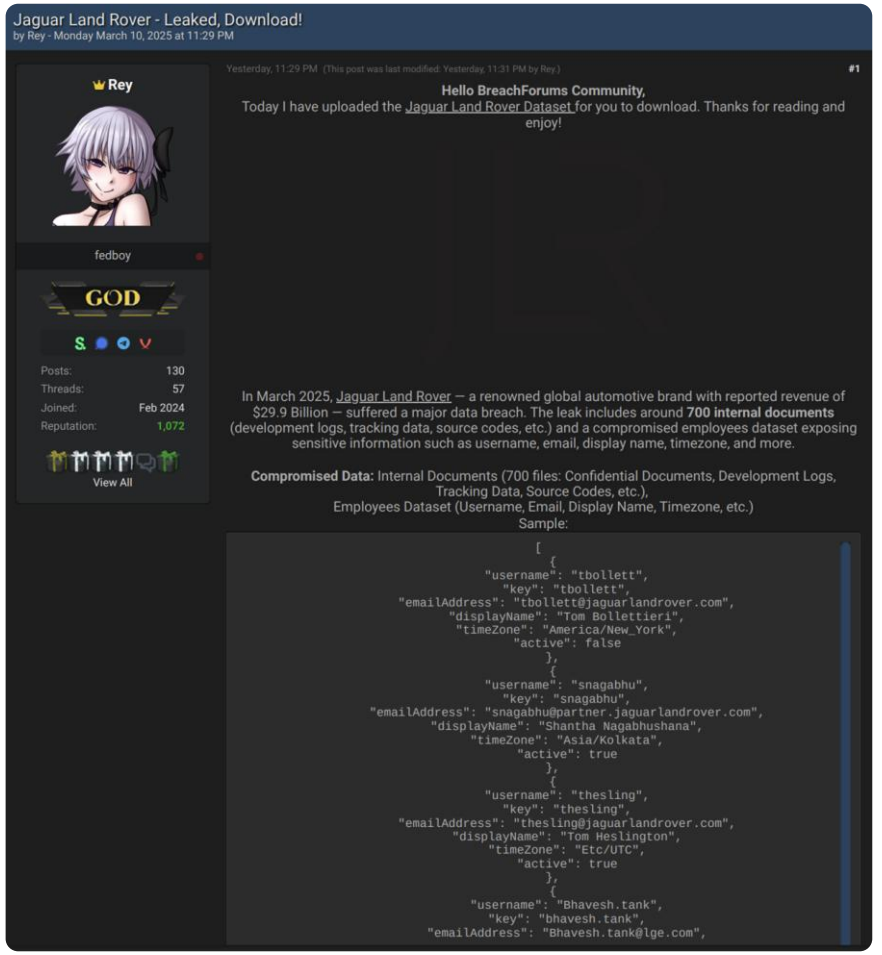
Could this attack have been avoided?

KELA

This was not the 1st JLR breach in 2025

Threat Actor: Rey

- A JLR breach unfolded in **March 2025** on the cybercrime forum **BreachForums.** Initially was listed by **Rey** on March 10, 2026.
- **Claimed data allegedly included:** ~700 internal JLR documents, Development logs and tracking data, source code and Employee information (usernames, email addresses, display names, time zones) - posted **for free download for forum members.**



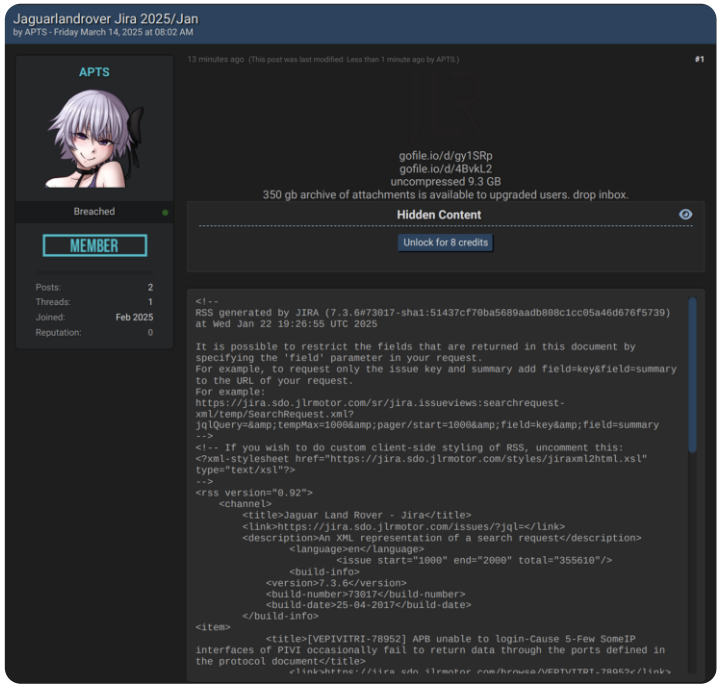
Rey's post on Breached, March 10, 2025, KELA platform

KELA

A few days later…

Threat Actor: APTS

- **Four days after Rey's initial disclosure,** a second threat actor, **APTS,** published a post on the same forum claiming access to Jaguar Land Rover (JLR) data.
- APTS released an **allegedly large dataset (9.3 GB + 350 gb archive of attachments is available to upgraded users. ").**
- Following the publication, **Rey publicly confirmed** that the **initial access vector** was an **Atlassian JIRA account.** Rey stated that the compromised JIRA credentials belonged to an **employee whose workstation had been infected with an infostealer,** enabling unauthorized access to JLR's environment.
- This confirmation aligned with APTS's claims and reinforced the assessment that the breach resulted from **credential theft rather than direct exploitation** of JLR infrastructure.
- The credentials used estimated as stolen back in **2021!**



APTS's post on Breached, March 14, 2025, KELA platform

JLR Timeline

2021

Infostealer infects employee - Credentials Stolen

Once infostealer infects employee machine credentials are harvested and make their way to the underground marketplace

10 Mar 2025

Rey Leaks JLR Data

14 Mar 2025

APTS Leaks JLR Data

2 successive breach posts, both claiming to have used infostealer obtained credentials

Aug 2025

CRITICAL JLR BREACH

Attackers, once again leveraging stolen credentials move laterally to OT environment and cause unprecedented disruption

Could the attack have been avoided?

What could have helped?

- Continuous monitoring of compromised accounts originating from infostealer infections is critical
- No Hacking necessary, Threat Actors are logging in!
    - Revoke access, MFA, enforce password resets, reassess third-party privileges.

? Who else in this story was infected by infostealers.....?

KELA

Who is Rey?

The Rey Case: From Alias to Identity

1. TA emerged in early 2024 as **“Hikki-Chan”,** later changed to **“Rey”**

2. **Initial Activity:**

   Gained attention on **BreachForums** with claims of **high-profile breaches**

   Credibility Issue: Many of the breaches were exposed as recycled leaks

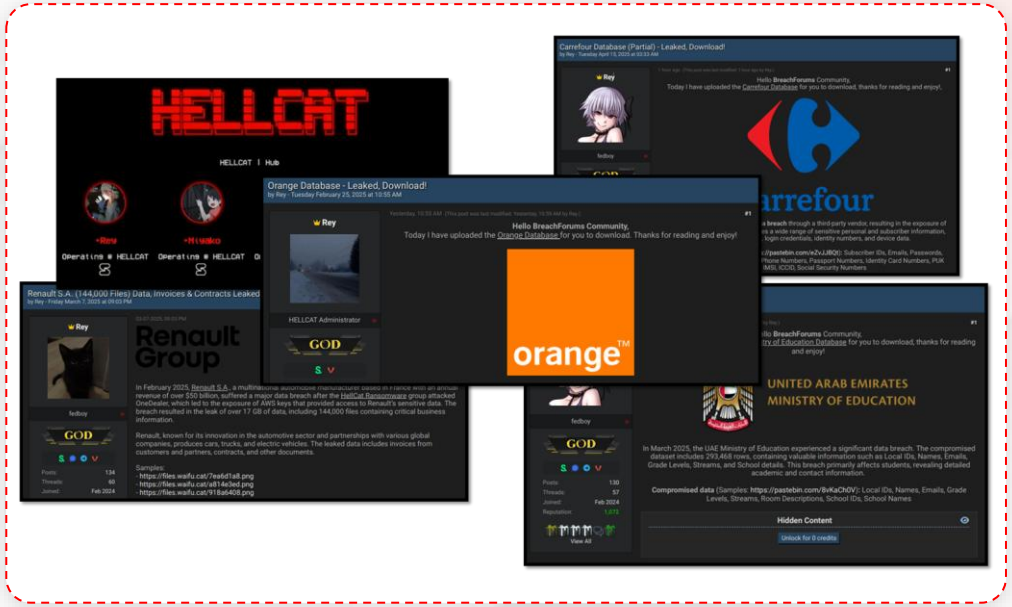
3. **Ransomware Role:**

   Became administrator of the **Hellcat** group

   Victims included Schneider Electric, Telefónica, Jaguar Land Rover

4. **KELA’s Breakthrough:**

   Linked Rey to a young Jordanian named **Saif Khader**

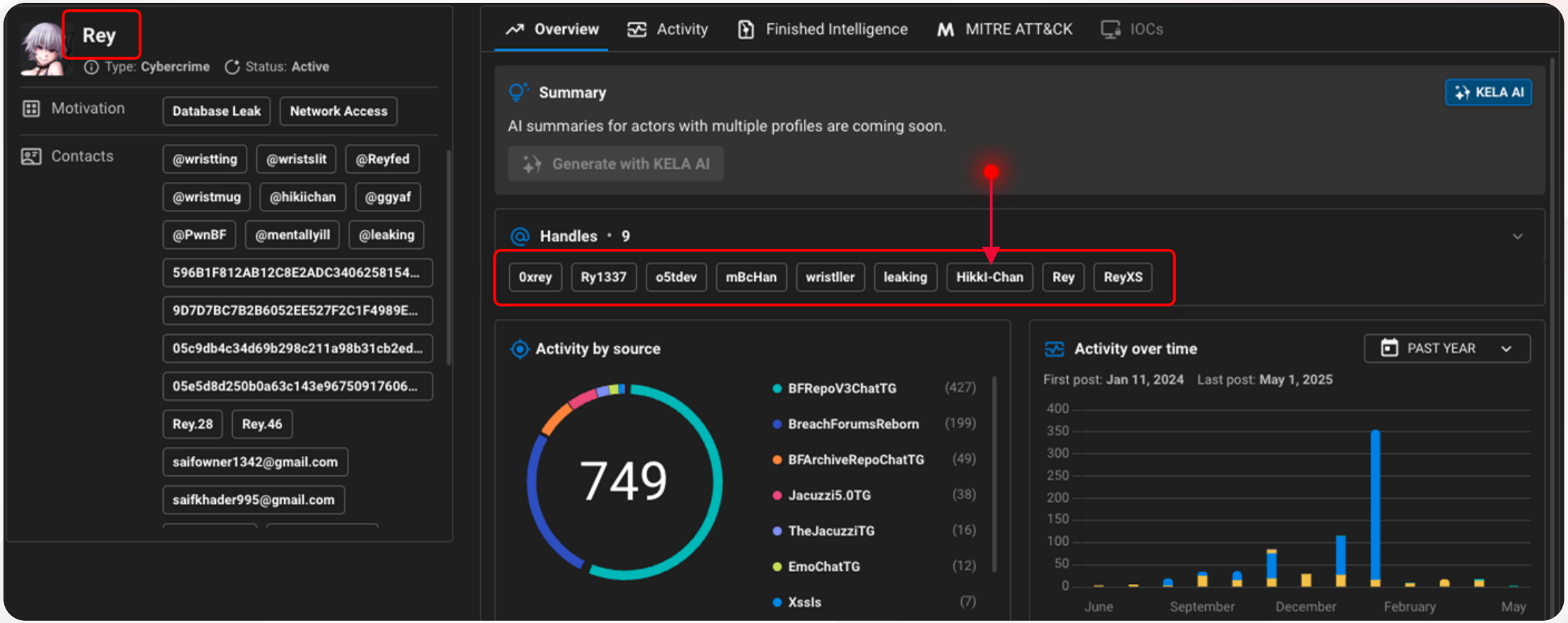


Key Evidence

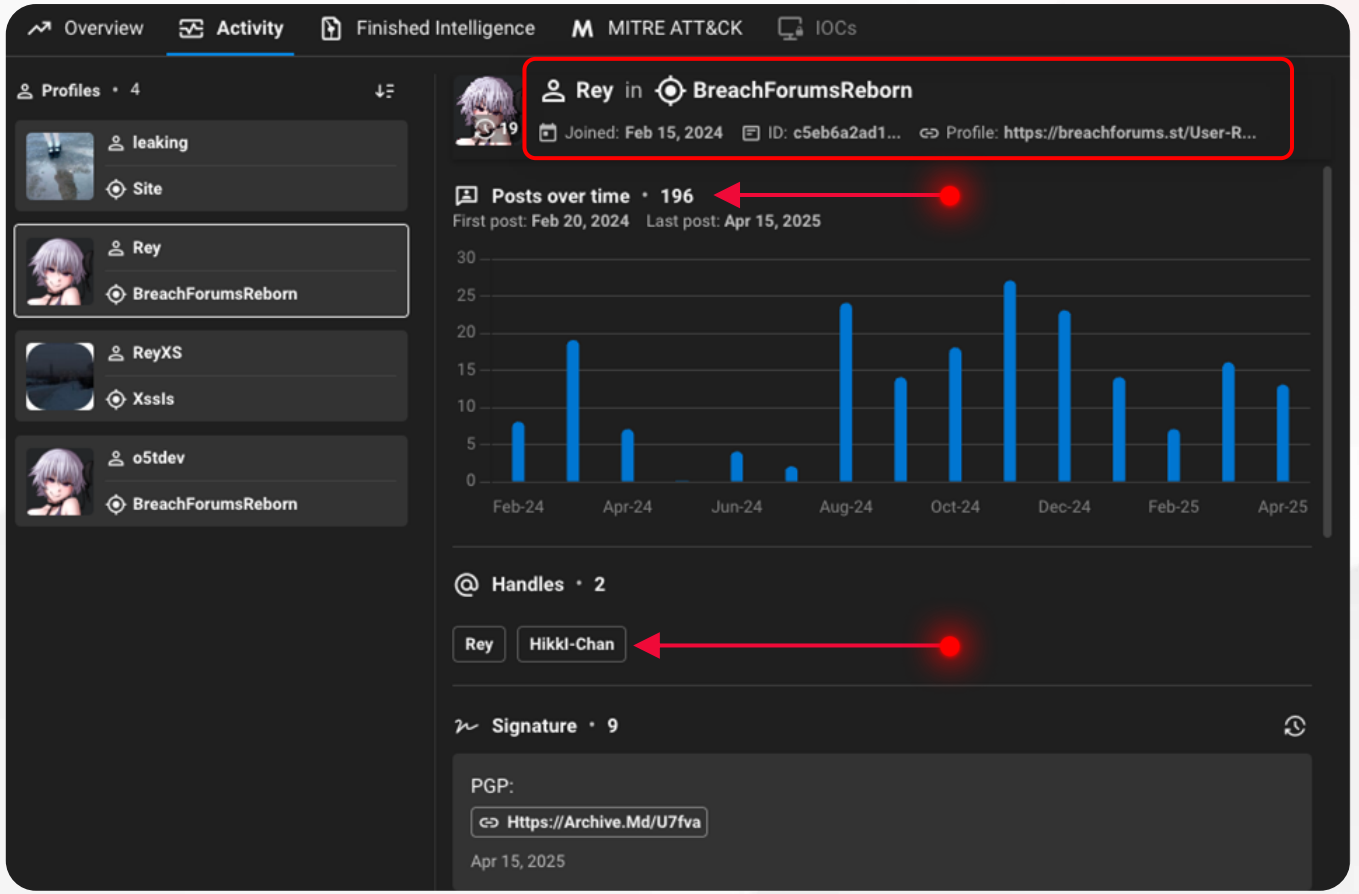
Two infostealer infections on Rey’s own devices exposed **multiple email addresses, online personas**

KELA

Rey monikers on the underground forums

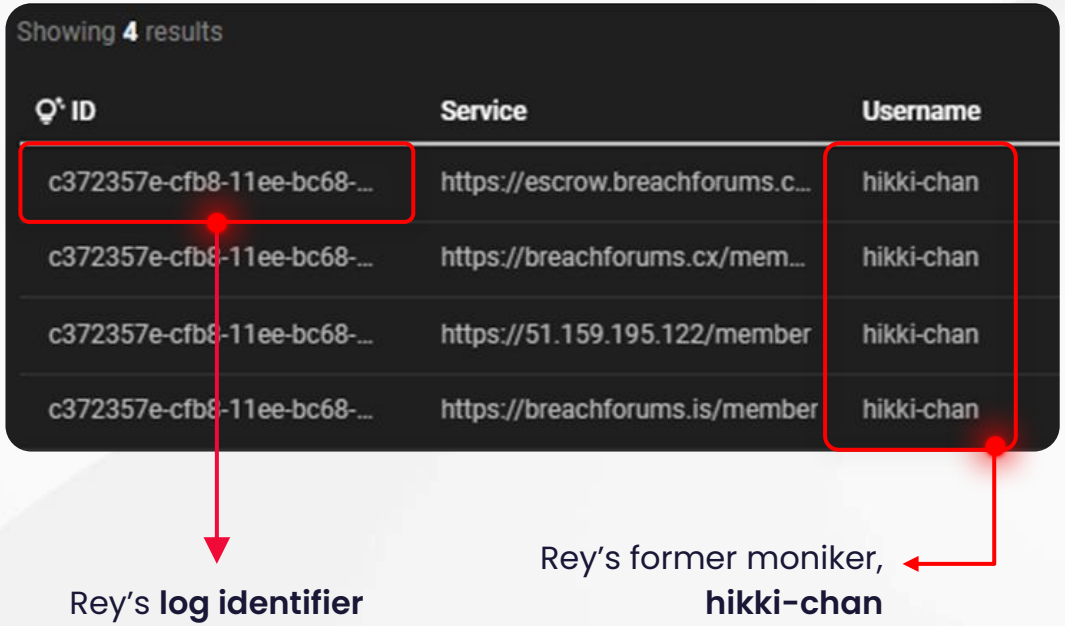


Rey’s activity over time



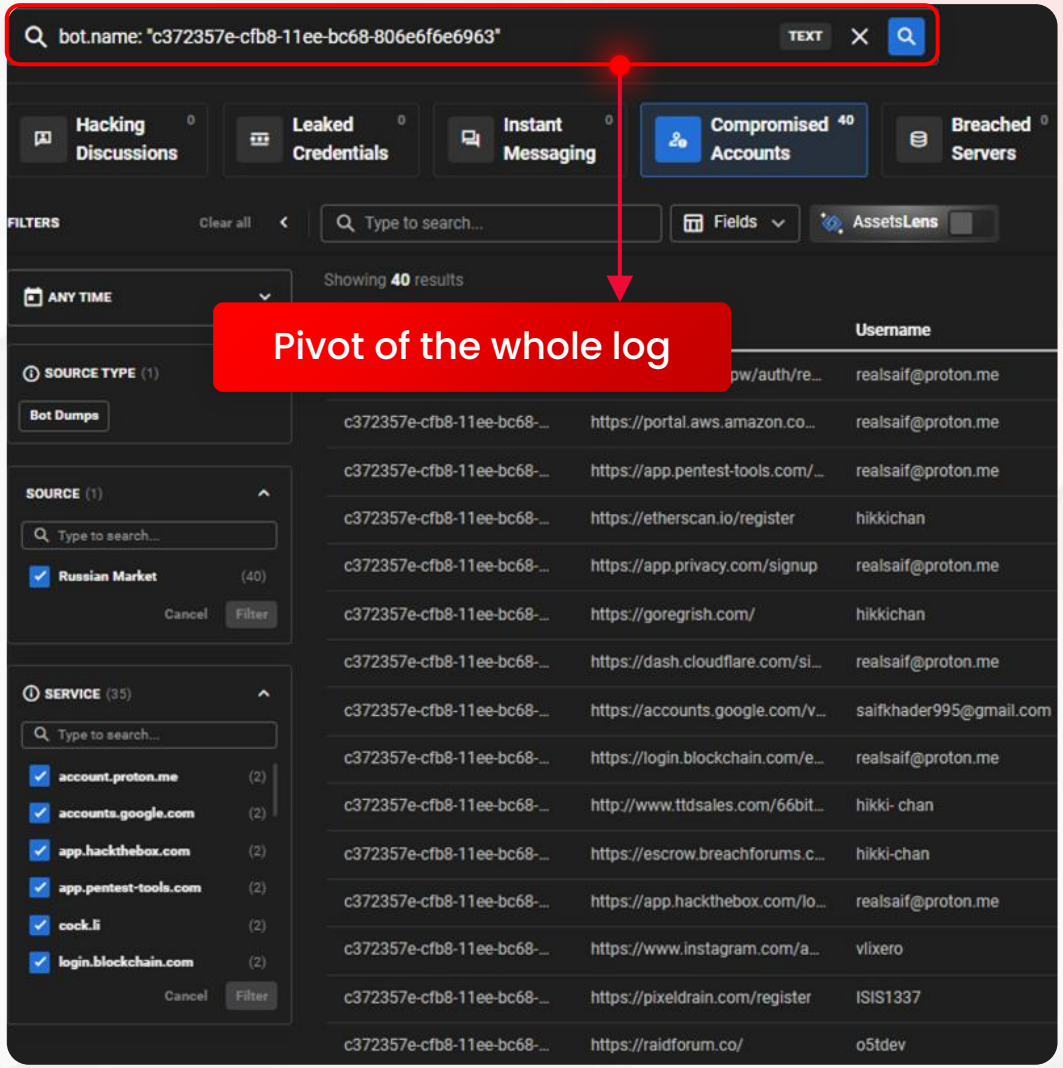
The Pivot Point:

Linking Hikki-Chan to a Leaked Infostealer log



Rey's **log identifier**

Rey's former moniker, **hikki-chan**

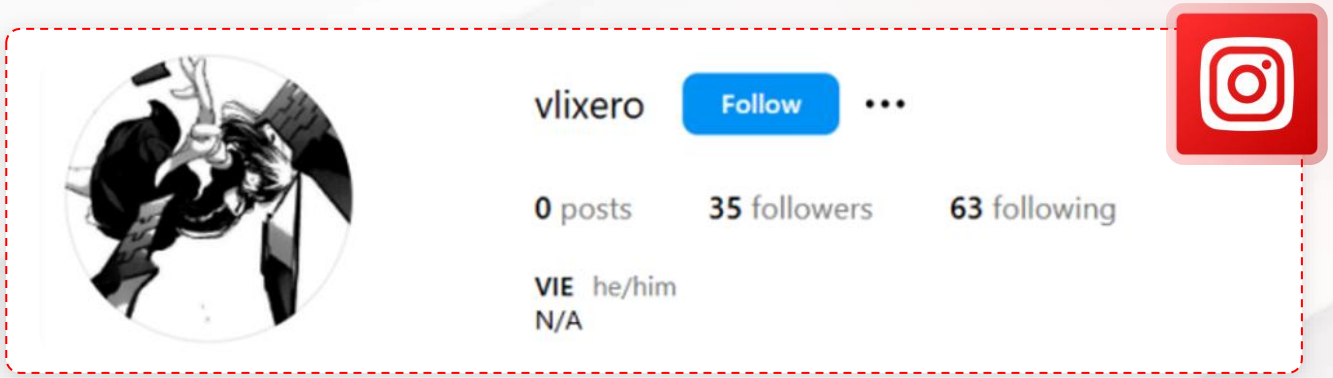


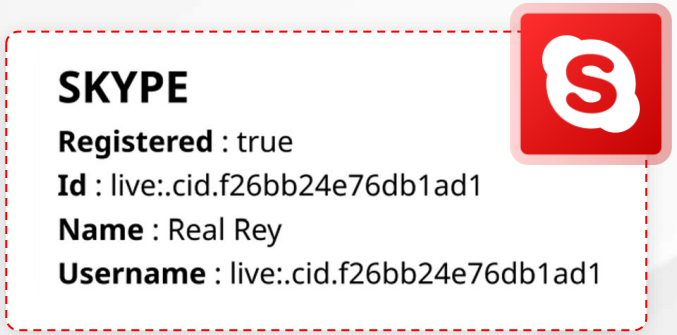
KELA

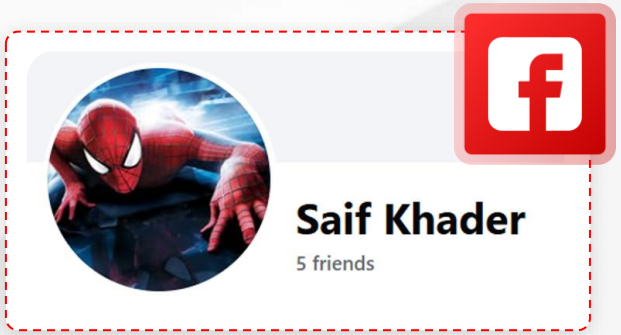
From Shadows to Spotlight:
Rey Is Saif Khader

Saif Khader

16 y.o. Jordanian



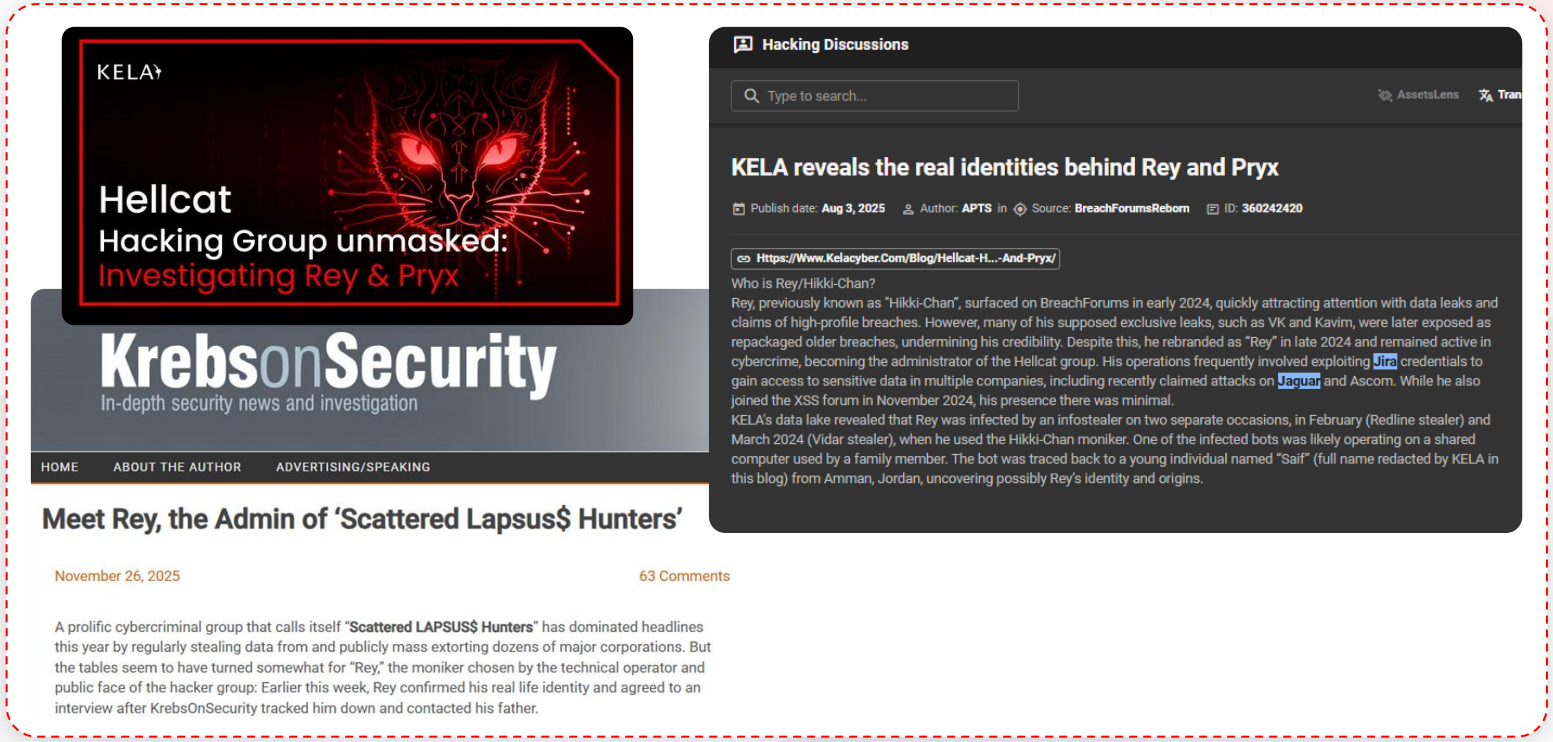




KELA

Closing the Loop

- KELA Published its findings on Rey in March 2025
- Later in 2025 Rey resurfaces as the admin for **Scattered LAPSUS$ Hunters** group, claiming responsibility for the August JLR breach
- November 2025 - Brian Krebs publishes profile on Rey, including an email interview with Saif Khader, reconfirming KELA's findings.

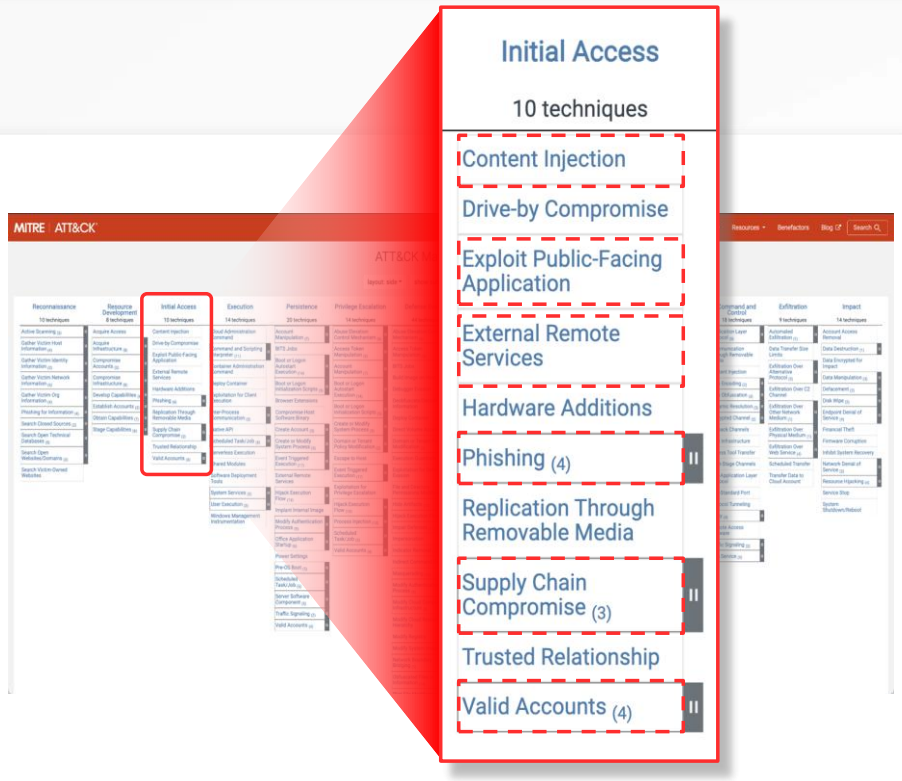


Rey → Scattered LAPSUS$ → JLR Attack

Identity and Brand Protection

Powering the Next Phase of Threat Detection

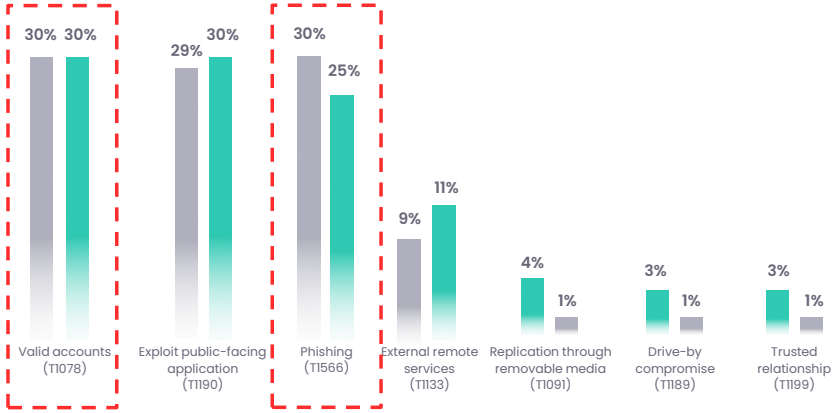
KELA provides solutions preventing the source of up to **96%** of cyber attacks



Top initial access vectors in 2024 versus 2023

IBM X-Force

Top methods used by threat actors to gain access to victim environments



Top initial access vectors X-Force observed in 2024 and 2023.

Sources: IBM X-Force and MITRE ATT&CK Matrix for Enterprise framework

Intercept Underground Commerce

Most likely you will be infected, but a larger compromise can be prevented

Identity Protection

Proactive detection and prevention of identity-related threats

Prevent identity theft and fraud

by safeguarding sensitive data and protecting **employees and customers** from account takeovers.

Intercept compromised credentials

Monitor and detect **compromised assets, identities and services** in real time, enabling swift action to prevent unauthorized access and potential breaches.

Automated monitoring and remediation

reducing the **manual burden on security teams** and ensuring faster, more efficient threat response.

KELA

Demo

KELA

Operationalizing CTI

Proactive detection and prevention of identity-related threats

- **Monitor and Validate CA and Brand**
- **Integrate valid incidents trigger security workflows:**
  - Password resets
  - MFA enforcement
  - Machine quarantining
  - Takedown requests
- **Integrate IOCs and Observable feeds into SIEM/SOAR**

KELA

CASE STUDY

fiverr.

4+ Million
Active users

30 Million
Registered accounts worldwide

Top 300
Websites globally

KELA's Customer Success team worked hand-in-hand with Fiverr's security group to fine-tune detections and automate workflows specific to Fiverr's business logic. The Fiverr team noted that no other threat intelligence provider matched KELA's level of white-glove service and responsiveness throughout setup, deployment, and execution

Brand Control & Takedowns

Continuous dark web and surface web monitoring to uncover impersonation, phishing, and fraudulent monetization of Fiverr's brand.

Identity Protection

Real-time visibility into compromised user and employee credentials to prevent account takeovers.

KELA's Investigate

Deep threat hunting and incident analysis across cybercrime sources to reveal campaigns targeting Fiverr's ecosystem.

Automation & Integration

Direct integration with Splunk and Torq, enabling automatic blocking and takedown actions based on KELA's verified intelligence.

KELA transformed how we protect users at scale, ending manual alert review so we focus on real threats. Onboarding and support have been exceptional - KELA is 'available, responsive, and aligned with our needs.

fiverr.

Framing CTI's Business Value

- Cyber Threat Intelligence (CTI) provides external insight to make internal defenses faster, smarter, and more cost-effective.
- The ROI of CTI is measured by **reduced risk** and **avoided loss,** which is quantified by **lowering the probability** of a material incident and **reducing the impact/cost** when an incident occurs
- A major breach typically costs around $5M USD, and avoiding just one can fund a CTI program many times over.
- CTI generates value through four main pillars:
  - Threat detection and early warning
  - Brand and customer protection
  - Supply chain and access intelligence
  - Compromised accounts and initial access intelligence.

CASE STUDY

The ROI of investing in CTI

One of the largest global insurance suppliers

The overall cost of a ransomware attack for the company in 2024 had the potential of costing over $6Million.

In 2024, KELA found

Over **400 compromised accounts** on sensitive company assets

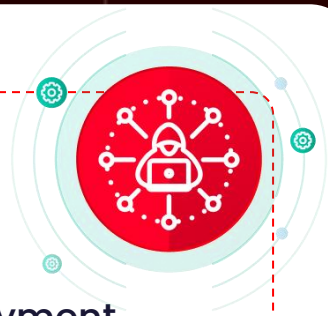
Over **3000 leaked company email addresses,**
>60% of which complete with passwords

From the above KELA identified that **14 pairs** of credentials were specifically vulnerable and able to facilitate **illicit access to company systems.**

Putting ransomware payments aside and taking only recovery costs into account, adding a **risk factor of 10%,** the saving from avoided attacks amounts to

$3.82 Million!

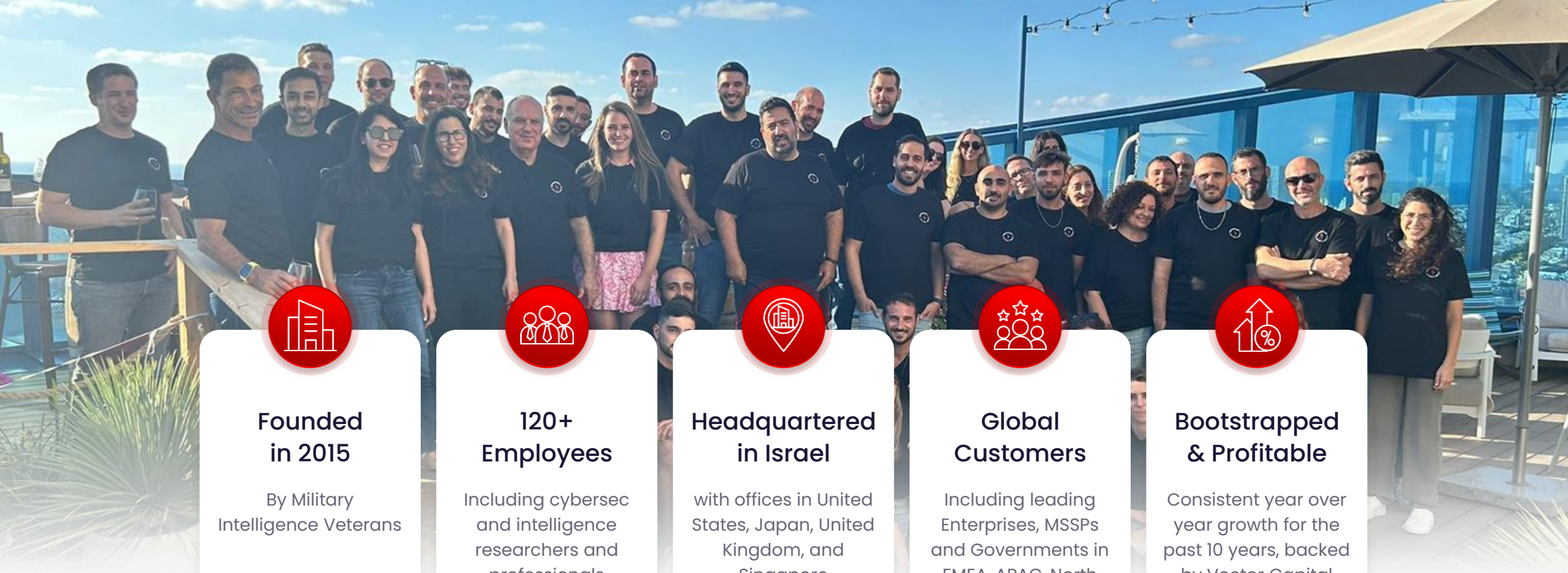
The State of Ransomware



Average ransom payment has risen to $3.96M
(x2.6 increase from 2023)

The **mean cost to recover** from a ransomware attack is **$2.73M**
(~$1M increase from 2023)

$2.73M avg. recovery cost × **14** exploitable credentials × **10%** Risk = **$3.82 Million**



Founded in 2015

By Military Intelligence Veterans

120+ Employees

Including cybersec and intelligence researchers and professionals

Headquartered in Israel

with offices in United States, Japan, United Kingdom, and Singapore

Global Customers

Including leading Enterprises, MSSPs and Governments in EMEA, APAC, North America, and LATAM

Bootstrapped & Profitable

Consistent year over year growth for the past 10 years, backed by Vector Capital since 2018

5.0 ★★★★★

In The last 12 Months,
As of 10 Sep 2025

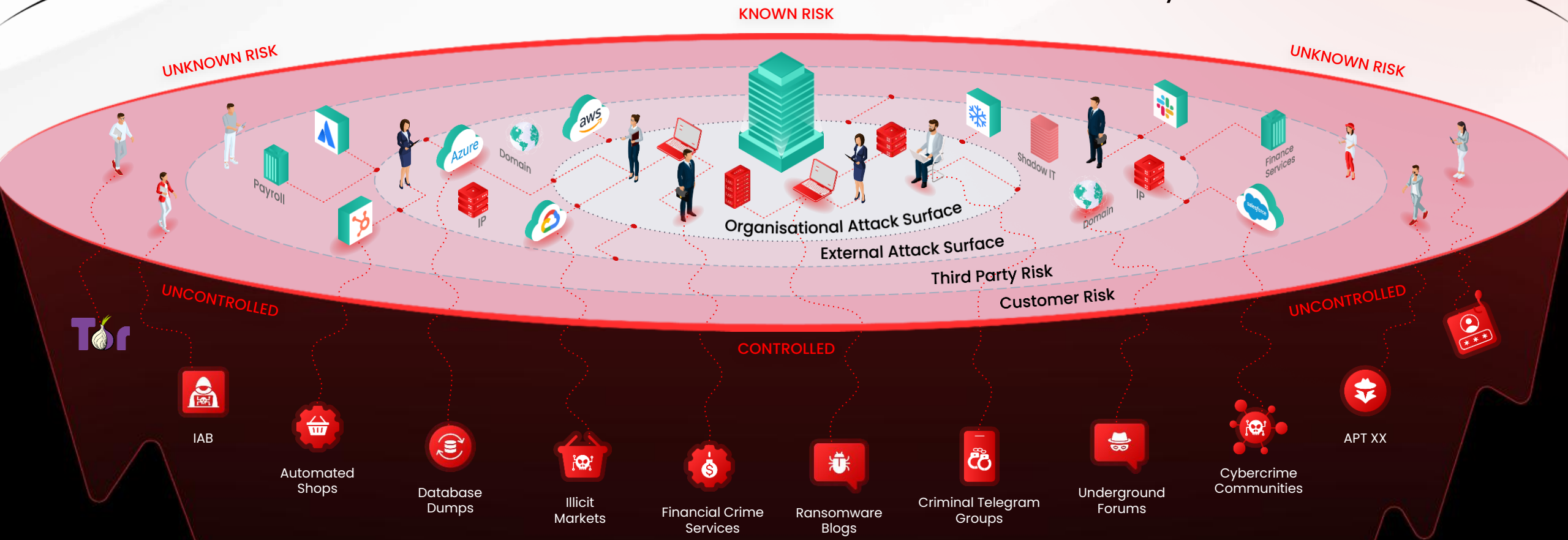
Gartner Peer Insights™

KELA

KELA

External Threat Exposure Reduction

- CTI
- DRPS
- EASM
- BAS
- TPRM
- GenAI Security



The Underground Cybercrime Network

KELA

KELA

Thank you!

www.kelacyber.com

Networking lunch

We'll be back at 2.15pm

Please scan here to give us your feedback on today's event

Case Study: Stories from the cyber frontline

Marcus Harewood

Senior Associate, A&O Shearman

Steve Hadwin

Counsel, A&O Shearman

The Ecosystem of a Cyber Incident: The evolving threat landscape

David Brown

Principal Security Consultant, NCC Group

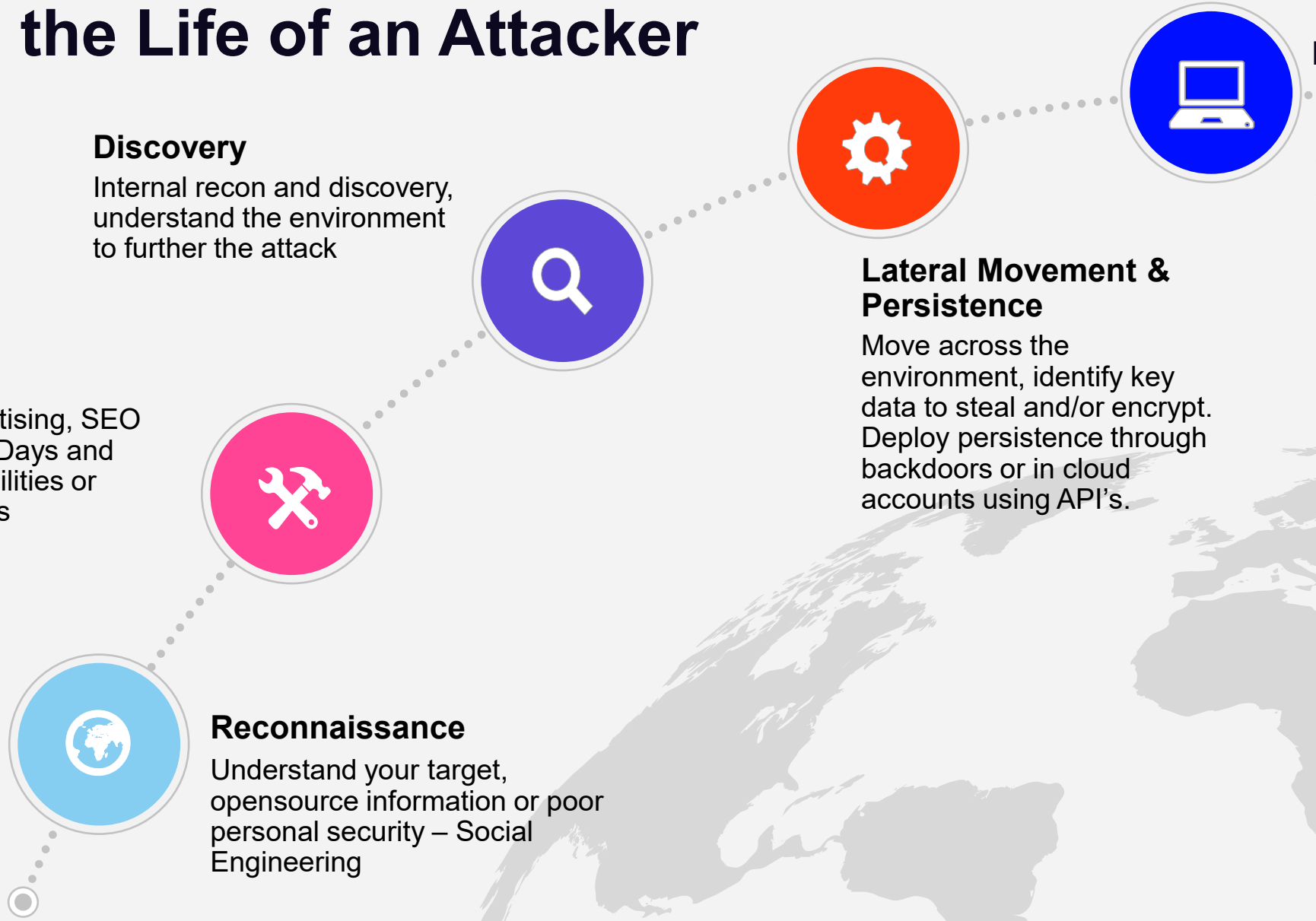
The Ecosystem of a Cyber Incident:
The evolving threat landscape

David Brown
Principal Security Consultant (DFIR)
NCC Group

Agenda

- A day in the life of an Attacker
- Technical Tactics
- Social Engineering
- Threat Intel Trends
- Best Practices

A Day in the Life of an Attacker



Reconnaissance

Understand your target, opensource information or poor personal security – Social Engineering

Initial Access

Phishing, Malvertising, SEO poisoning, Zero-Days and general vulnerabilities or misconfigurations

Discovery

Internal recon and discovery, understand the environment to further the attack

Lateral Movement & Persistence

Move across the environment, identify key data to steal and/or encrypt. Deploy persistence through backdoors or in cloud accounts using API's.

Exfil & Impact

Steal and encrypt data for extortion – sell creds and data (IAB)

Technical Tactics

How are they evading detection?

Initial Access

- Phishing/Vishing
- Drive-by Downloads
- Malvertising
- Supply Chain Compromise

Persistence

- Remote Tools
- Living-off-the-land
- Valid Credentials
- SIM Swapping (Hijack a phone number)

Privilege Escalation

- Session Tokens
- Credential Dumping
- Over Permissive Cloud IAM Policies

Social Engineering

- Deepfakes/AI
- Authority and Urgency
- Human Curiosity

Living Off the Land

- Legitimate Tooling
- Fileless Malware
- Native Admin Tools
- Blend in

Evasion

- Leverage over permissive accounts
- Abuse Token Lifetimes
- Lack of SIEM detection
- Create backdoors – Noisy Audit Logs

Social Engineering

Facing Off the Deepfakes!

Outlook

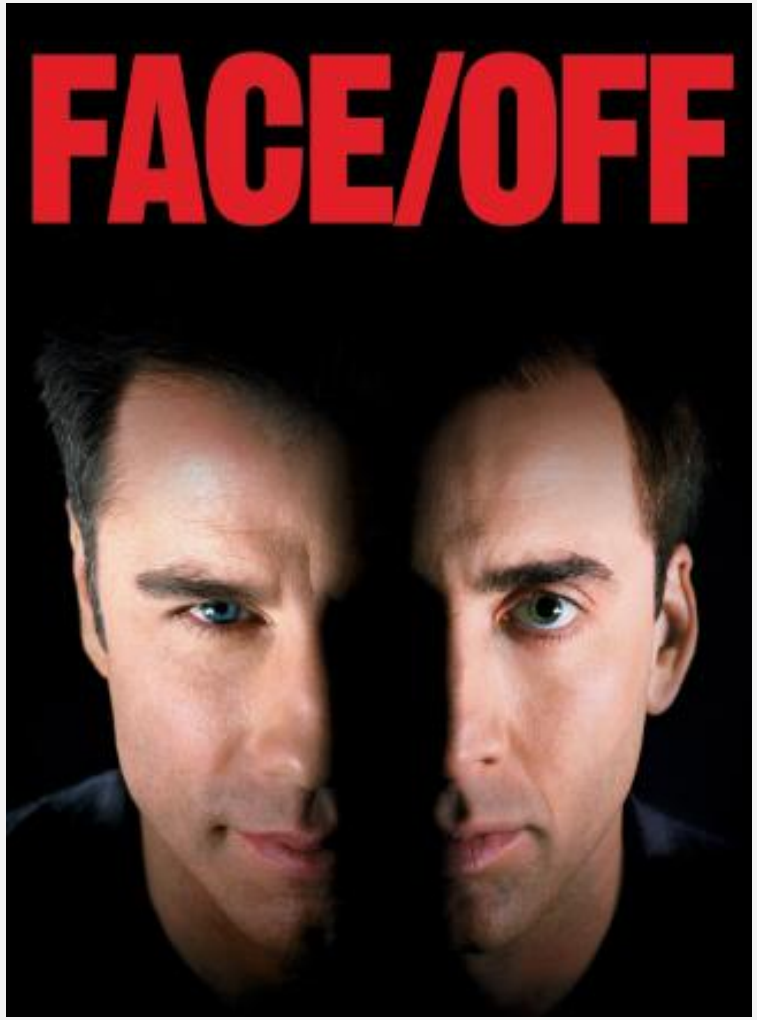
Exponential increase on Deepfake phishing attacks – 18 months (Estimated 3,000% rise in 2024)

Gov Led Action - Paris AI Action Summit

- US Vice President emphasises the need to avoid hindering innovation

Advanced Social Engineering

- Fraud – North Korean IT workers, Financial motivation primarily
  - Integrate fraud detection with deepfake detection efforts
- Espionage – Data, data, data – Impersonation to scrape sensitive data
- Phishing – Emails, Messages, Voice calls/messages
  - Greater consistency and context of messages – no longer visible mistakes, impersonation of key people



Threat Intelligence Trends

Emerging Challenges for All Sectors

Industry Specific Threats

Focused targeting

Industrials continues to be the hardest hit sector with the majority of attacks. However, no sector is being spared from legal to healthcare there is very limited bias from Attackers.

The biggest industry concerns should be OT with significant convergence between IT and OT. With greater focus, are we truly prepared?

Nation State Vs OCGs

Global Landscape Changing

Threat Actor groups converging in tactics yet their intentions are very different, with geopolitical motives driving one and financial gain driving the other.

Criminal groups have become more aggressive and less predictable in their targets predominantly due to the number of groups now in play.

Third Party Risk

Targeting the Supply Chain

Attacks are increasingly opportunistic third parties and supply chains being hit due to weaker defenses allowing attackers to pivot to larger organisations due to converged systems.

Also the scale of our trust in big business, do we truly understand the data being stored?

Best Practices

Preparing and Defending Against Threats

Technical Controls

- Security Architecture (Zero Trust)
- Endpoint Detection
- Phishing Resistant MFA
- Principle of Least Privilege
- Network Segmentation

User Awareness

- Bespoke Role-Based User Training
- Policy Alignment
- Risk Based
- Best practice - NIST / CIS Control 14

Incident Readiness

- Incident Response Planning
- Incident Playbooks
- Aligned to Industry Best Practice

Threat Hunting

Proactive Hunts based on Threat Intelligence to ensure value. Focus on MITRE Tactics not Techniques.

Awareness Programs

Don’t just focus on phishing consider more general elements including current trends i.e. SEO poisoning. Focus your programs on your industry risks through the use of Threat Intelligence.

Testing & Exercising

- Gold (Strategic)
- Silver (Tactical)
- Bronze (Operational/Technical)
- Advanced Exercising
- Offensive Testing

Rumsfeld Score of Cyber Resilience

$$Rs = \frac{[kA + uA]sD^{\gamma} * (u \uparrow \tau * kV + uV) - u\beta * Ł}{i + [(uR^3) * uCMT + uS] - (k + u\xi)}$$

k = known knowns

u = unknown unknowns

A = Assets and Important Business Services

$\uparrow \tau$ = ever increasing threats

sD =Security Debt

V = Vulnerabilities

β = Back-ups

Ł = Lessons learnt from previous incidents

i = Investment

R = Ransom, Reputation, Regulatory fines

CMT = Crisis management training at Gold, Silver and Bronze levels

S = Internal and external stakeholders

ξ = Supply Chain

*This is a joke NOT a real formula do not calculate your resilience using it.
TimR - NCC Group

Questions

Panel Session: How businesses should prepare for the cyber threats of 2026

Facilitator

Yolande Young CISO, A&O Shearman

Panellists

Ffion Flockhart Partner, Global Co-Head of Cybersecurity, A&O Shearman
Nick Palmer Technical Director, International, Censys
Anderson Lunsford CEO & Co-Founder, BreachRx

End of meeting

Please join us for a drinks reception

Please scan here to give us your feedback on today's event