



Security Matters Forum Q4-2023

Cyber Security Governance: Latest Trends, Threats and Risks

November 2023

Cyber Threats and Risk

How a holistic approach can mitigate them

Presented To:

Lloyds of London

Prepared By:

Jason Monger, Senior PreSales Engineer

Arctic Wolf Networks

Cybercrime

WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

Inside Trickbot, Russia's Notorious Ransomware Gang

Internal messages WIRED has viewed shed new light on the operators of one of the world's biggest botnets.

Holden too says he has seen evidence that Trickbot is ramping operations. "Last year they **invested more than \$20 million** in infrastructure and growth of their organization," he explains,



PHOTOGRAPH: KATLEHO SEISA/BETTY IMAGES

THE LEADER IN SECURITY OPERATIONS

CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO B

Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'

PUBLISHED WED, APR 13 2022-9:49 PM EDT | UPDATED WED, APR 13 2022-9:55 PM EDT

Monica Buchanan Pitrelli @MONICAPITRELLI

SHARE f t in e

KEY POINTS

- A huge leak of internal documents — thought to be an act of revenge over Conti's pro-Russia stance — revealed details about the notorious hacker group's size, leadership and operations.
- The messages show that Conti operates much like a regular company, with salaried workers, bonuses, performance reviews and even "employees of the month."
- Cybersecurity experts say some workers were told they were working for an ad company and likely were unaware who was employing them.

TV
Graduation Night
UP NEXT | Dateline 03:00 am ET

TRENDING NOW

- 1 A psychological sign of a parent: 'It's a raise your kit
 - 2 The 10 most work-from-home companies in 2022
 - 3 Mark Zuckerberg: like your screen Social media building rela
 - 4 Why China's is shoring up
- EU warns of weapon stockpiles



for Veeam privileged users and leverages to **access, exfiltrate, remove** and **encrypt backups** to ensure ransomware breaches are un-"backupable"

Ever more difficult for end users

SEO Poisoning

What it looks like in the real world

Malicious websites use a top search result. By manipulating engine rankings, threat instances, Google Ads predict that ransomware initial access vector.

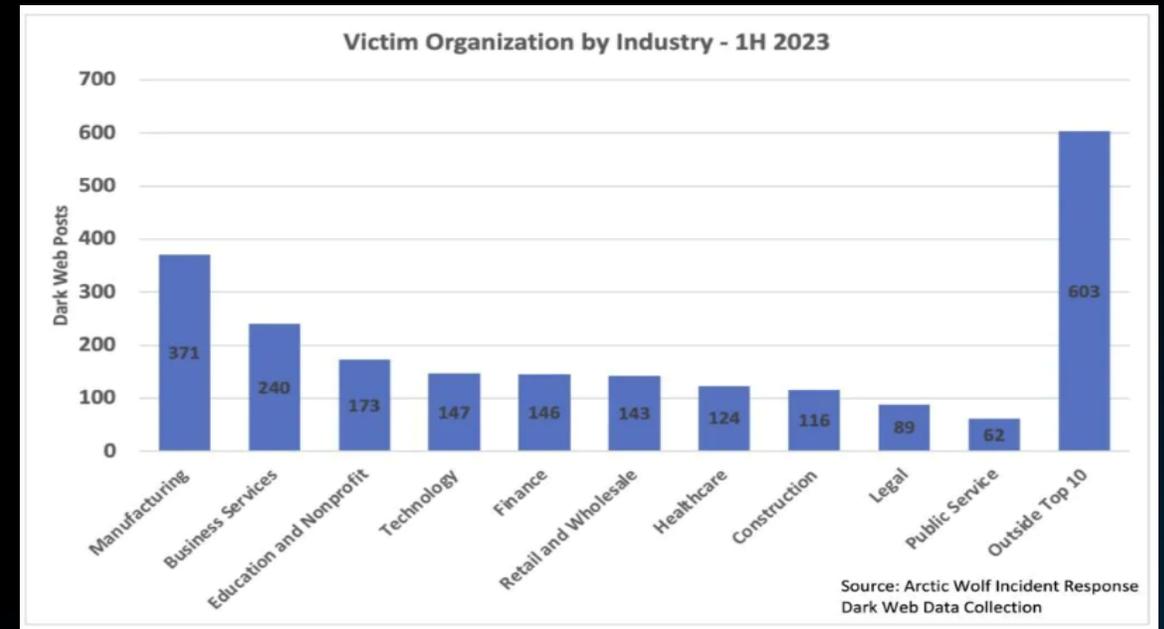
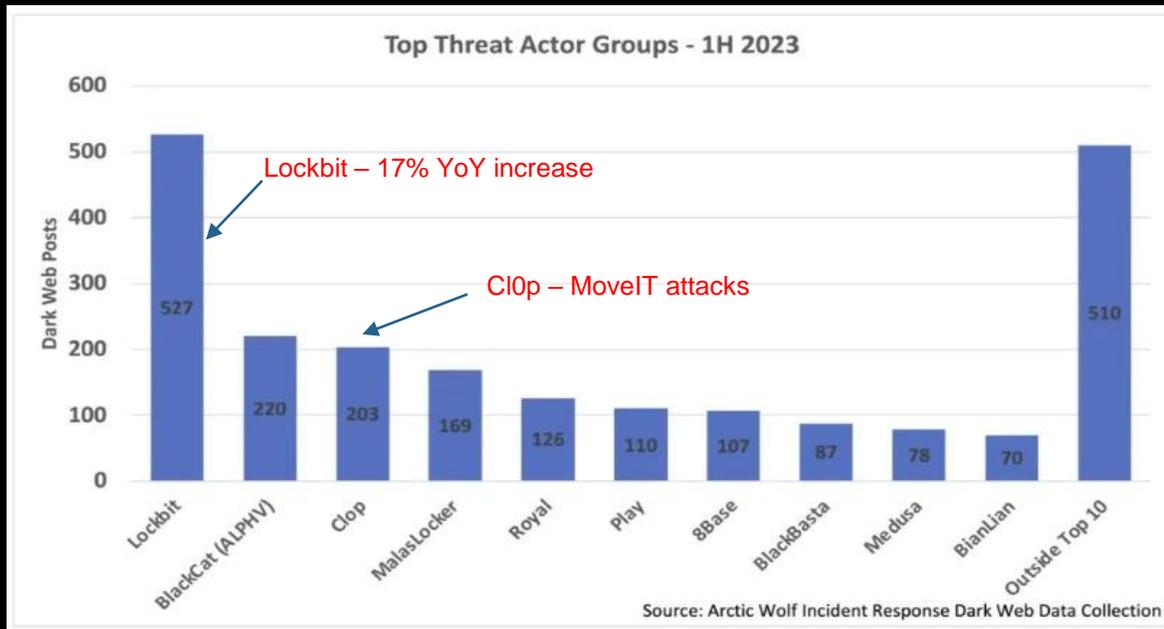
Malicious search engine result promoting Visual Studio download

Source: Mandiant

Download the EXE file above, run it and follow the steps



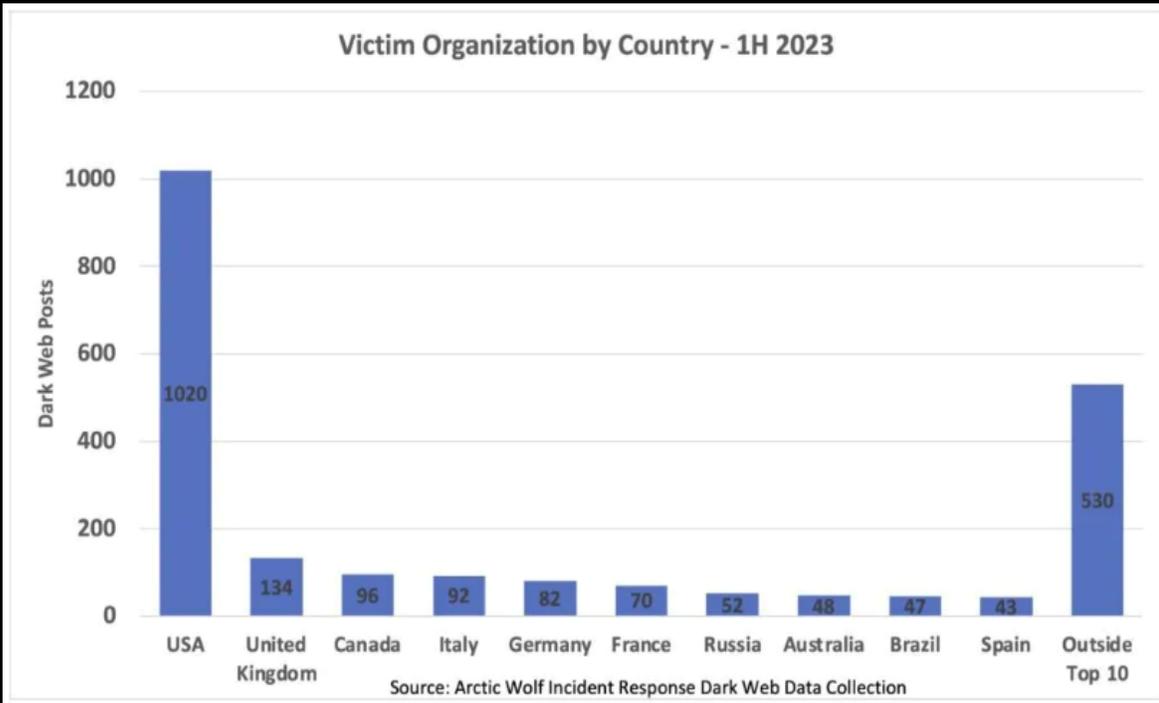
Arctic Wolf Labs - 1H2023 Ransomware Landscape



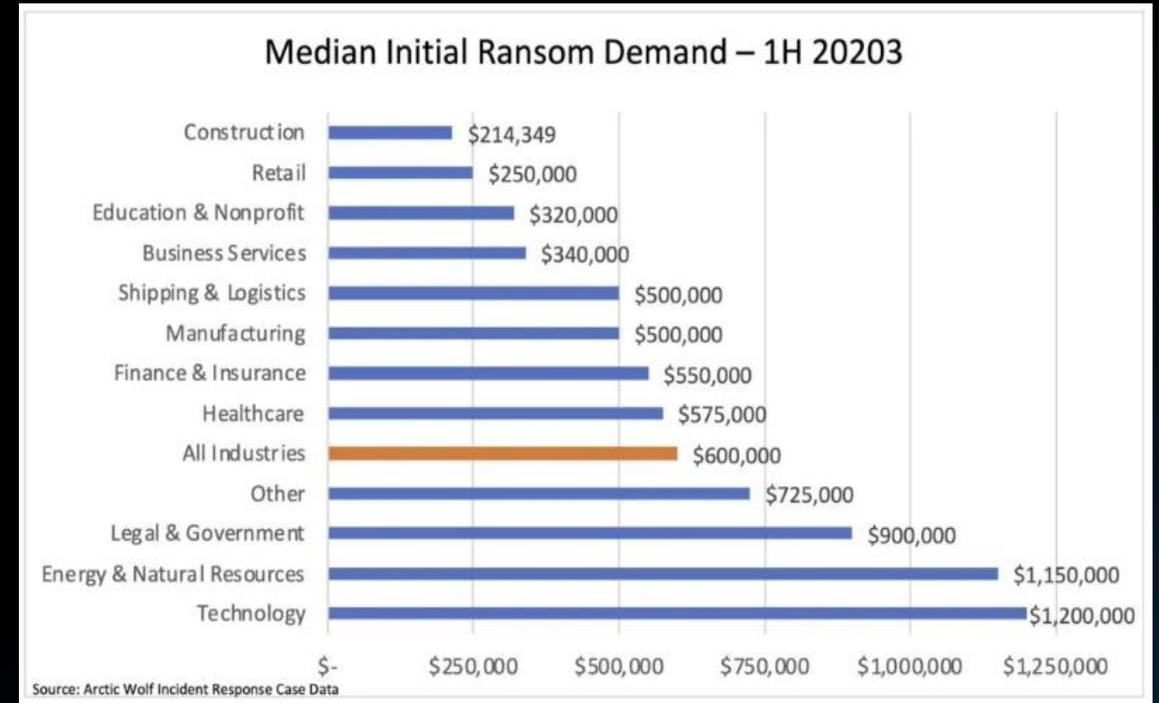
Ransomware attacks growing again
43% increase over 2H22

Opportunistic and not necessarily sector specific

Arctic Wolf Labs - 1H2023 Ransomware Landscape

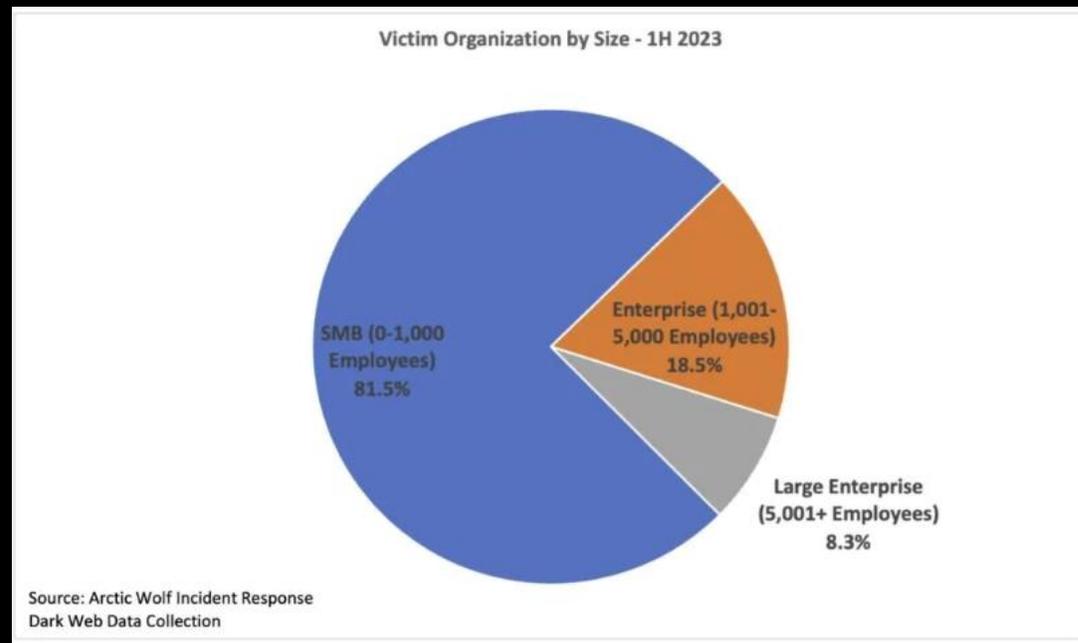


English speaking countries most attacked



Ransom demand is a fraction of overall cost

Arctic Wolf Labs - 1H2023 Ransomware Landscape



<https://arcticwolf.com/resources/blog/1h-2023-ransomware-landscape-overview>



“Missing or bad tools” is **NOT** the reason for many successful attacks: Targeted and untargeted attacks use vectors outside company controls



Breached: January 22...

Attack using a hacked, trusted **supply chain** computer and account to authenticate into Okta's systems



Breached: September 22

Attack by **taking over a user account** by
a) compromising the users **personal device** with malware and b) tricking the user into confirming the MFA challenge upon login



Ransomed: Sept 23

Attackers used vishing / **social engineering** on the IT helpdesk



Quantifying Cyber Risk

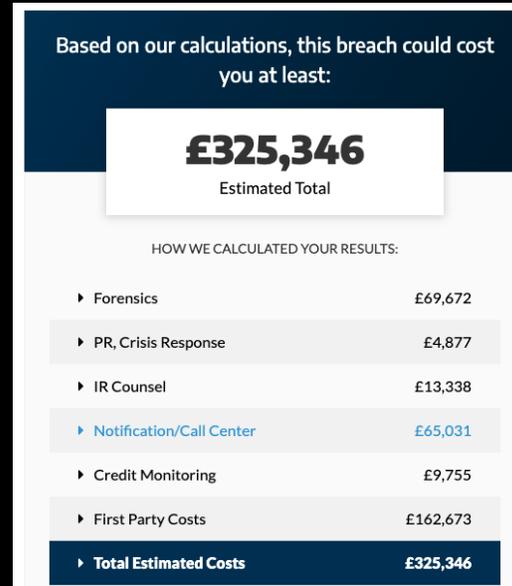
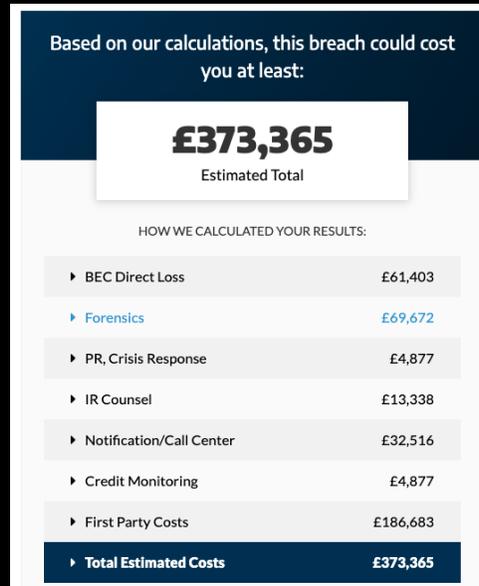
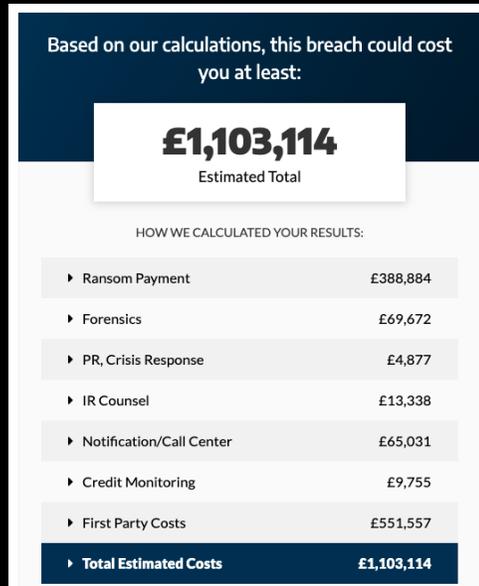
**LIKELIHOOD
OF AN INCIDENT**



**IMPACT
OF AN INCIDENT**



Calculating the cost of an incident



Ransomware

9%

BEC

20%

Data Breach

15%

Total Cyber Risk ~ £1.8m

Combined Annualised Risk ~£223k

Breach Scenario:

Ransomware

BEC

Data Breach

Sector:

Insurance, UK

Number of Users

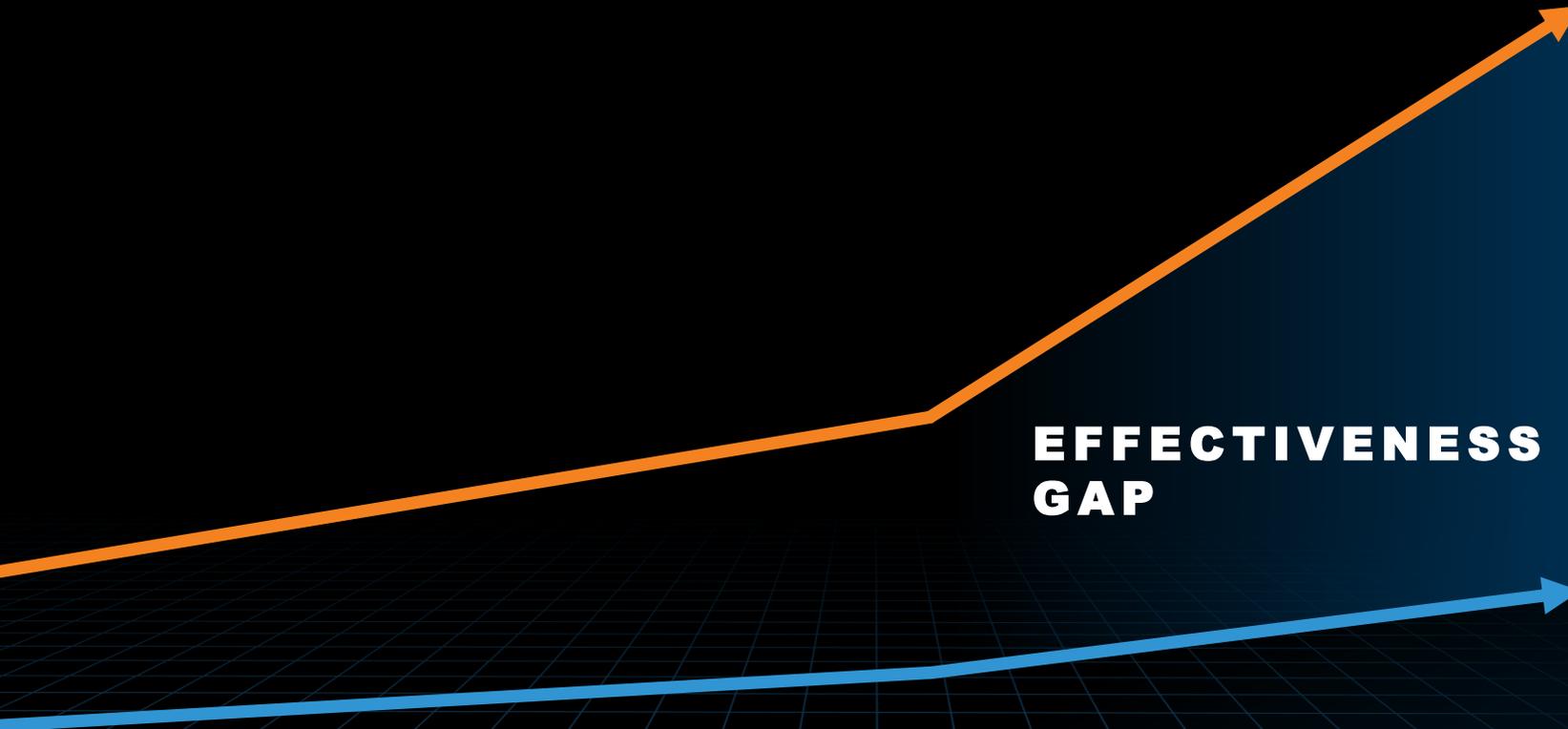
300

Annual Revenue:

£40m



Accelerating Risk



48%

INCREASE

in Cybercrime Losses in 2022

Total Security Companies:

3,377+

Total Security Spend:

\$169B

YoY Spend Increase:

11%



Cyber Scope

CYBER SCOPE 2023

The image displays a 'Cyber Scope 2023' grid, a comprehensive directory of cybersecurity companies. The grid is organized into several major categories, each with a sub-header and a collection of company logos. The categories include:

- Network & Infrastructure Security:** Sub-categories include Advanced Threat Protection, NAC, SDN, DDoS Protection, DNS Security, Network Firewall, and Deception.
- Web Security:** Includes ICS & OT, Network Analysis & Forensics, and Encryption.
- Endpoint Security:** Sub-categories include Endpoint Prevention and Endpoint Detection & Response.
- Application Security:** Sub-categories include WAF & Application Security and Application Security Testing.
- MSSP:** Sub-categories include Traditional MSSP and Advanced MSS & MDR.
- Data Security:** Sub-categories include Data Privacy and Data Centric Security.
- Risk & Compliance:** Sub-categories include Risk Assessment & Visibility, Risk Quantification, Pen Testing & Breach Simulation, Security Awareness & Training, and Security Incident Response.
- Security Ops & Incident Response:** Includes SIEM and Security Incident Response.
- Threat Intelligence:** Includes 4i@ and ANOMAL.
- IoT:** Sub-categories include IoT Devices, Automotive, and Connected Home.
- Messaging Security:** Includes AREA 1, Blackberry, and others.
- Identity & Access Management:** Sub-categories include Authentication, IDaaS, Privileged Management, Identity Governance, and Consumer Identity.
- Digital Risk Management:** Includes OGD and CENTRAL.
- Security Consulting & Services:** Includes AON, IBM, and others.
- Blockchain:** Includes AWARE and BROADCOM.
- Fraud & Transaction Security:** Includes BINGATCH and FICO.
- Cloud Security:** Sub-categories include Container and Infrastructure.

The grid is densely packed with logos from leading and emerging cybersecurity firms. A prominent logo for 'Momentum Cyber' is visible in the center of the grid.



Security Evolution Drivers

Business Drivers

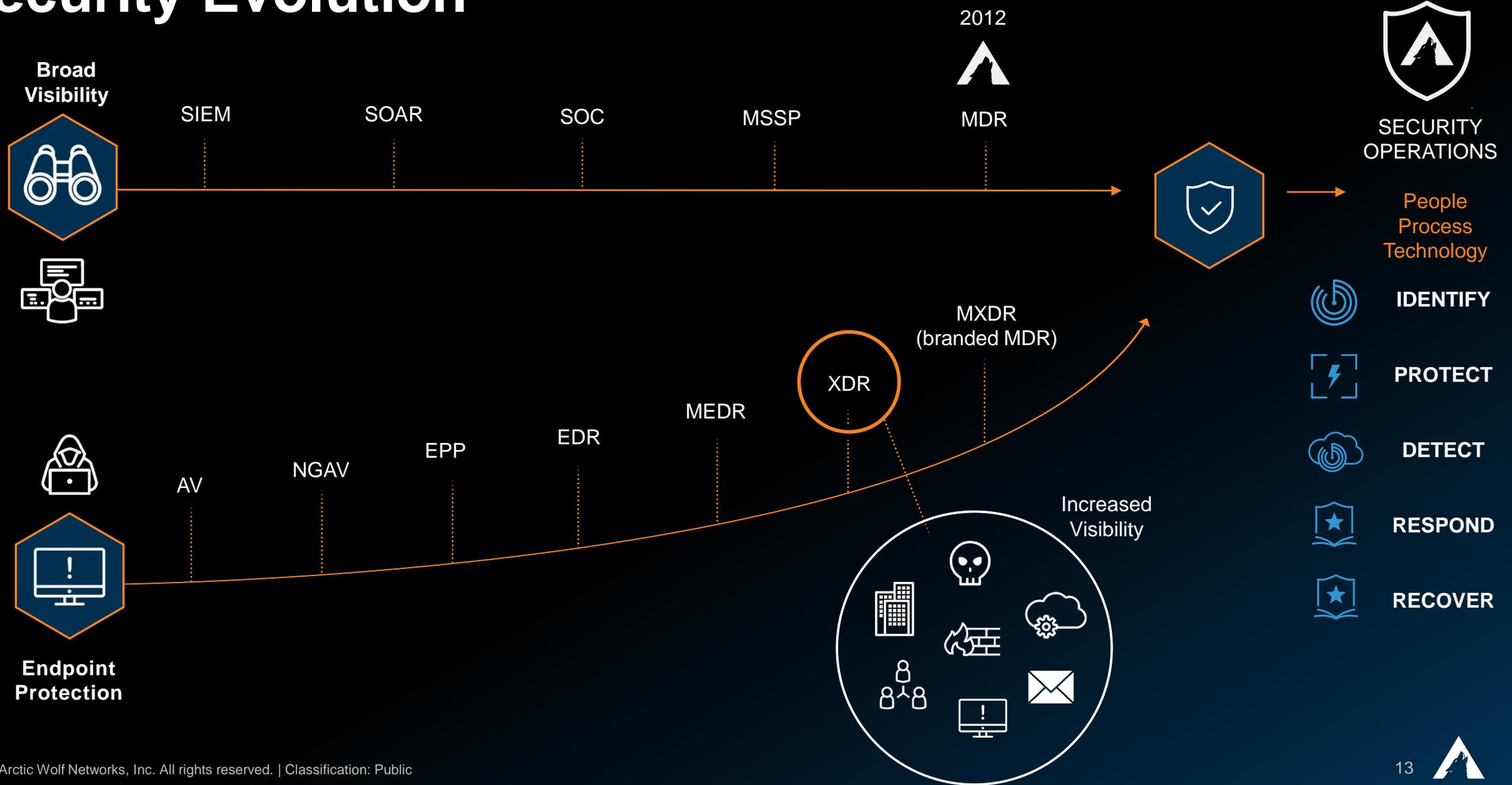
- Digital transformation
- Pandemic / modern working
- Increased cyber attacks
- Board and shareholder accountability
- Supply chain requirements
- Compliance / regulatory fines
- Cyber Insurance

IT Drivers

- Board reporting
- Threat detection confidence
- Scarce expertise
- Lack of resource
- Holistic visibility
- Challenging security budget
- Consolidation of security stack



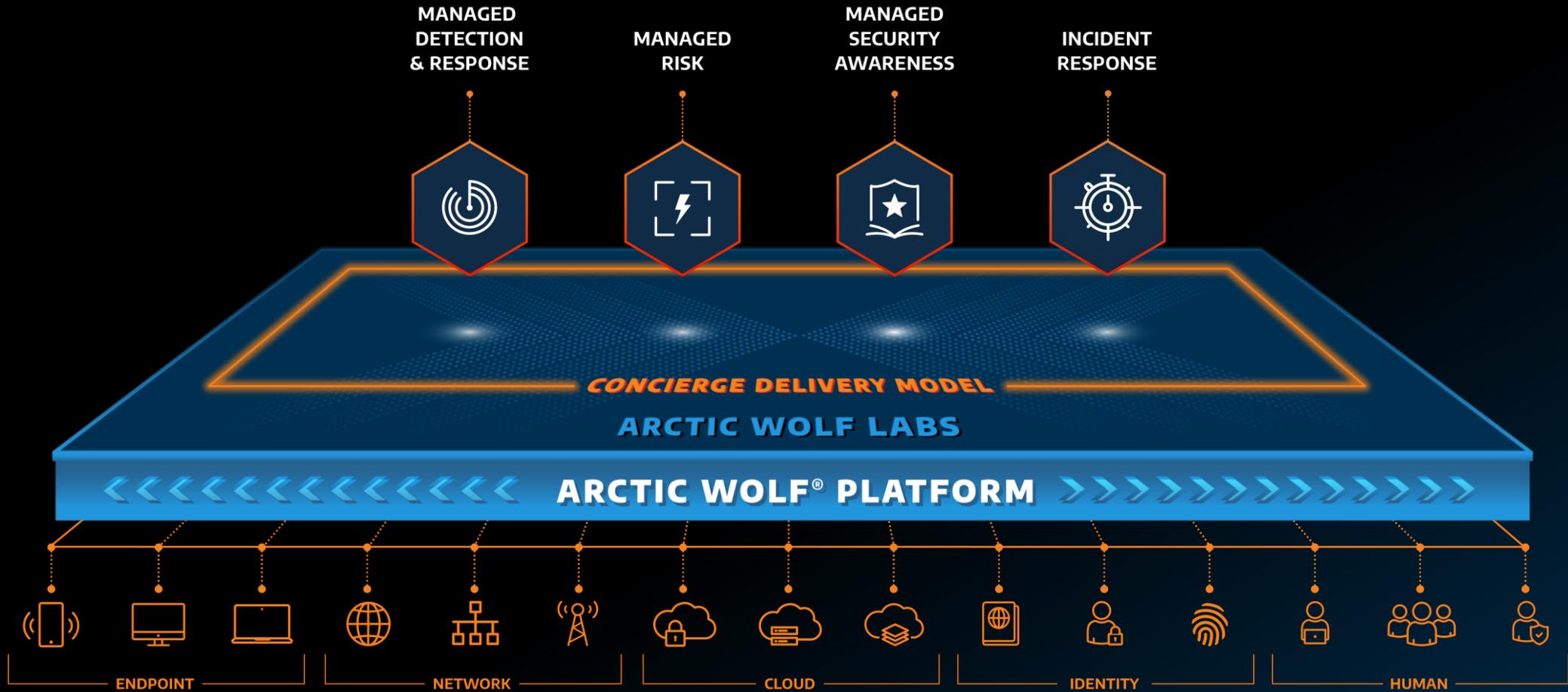
Security Evolution



How to address Cyber Risk



ARCTIC WOLF Security Operations Cloud

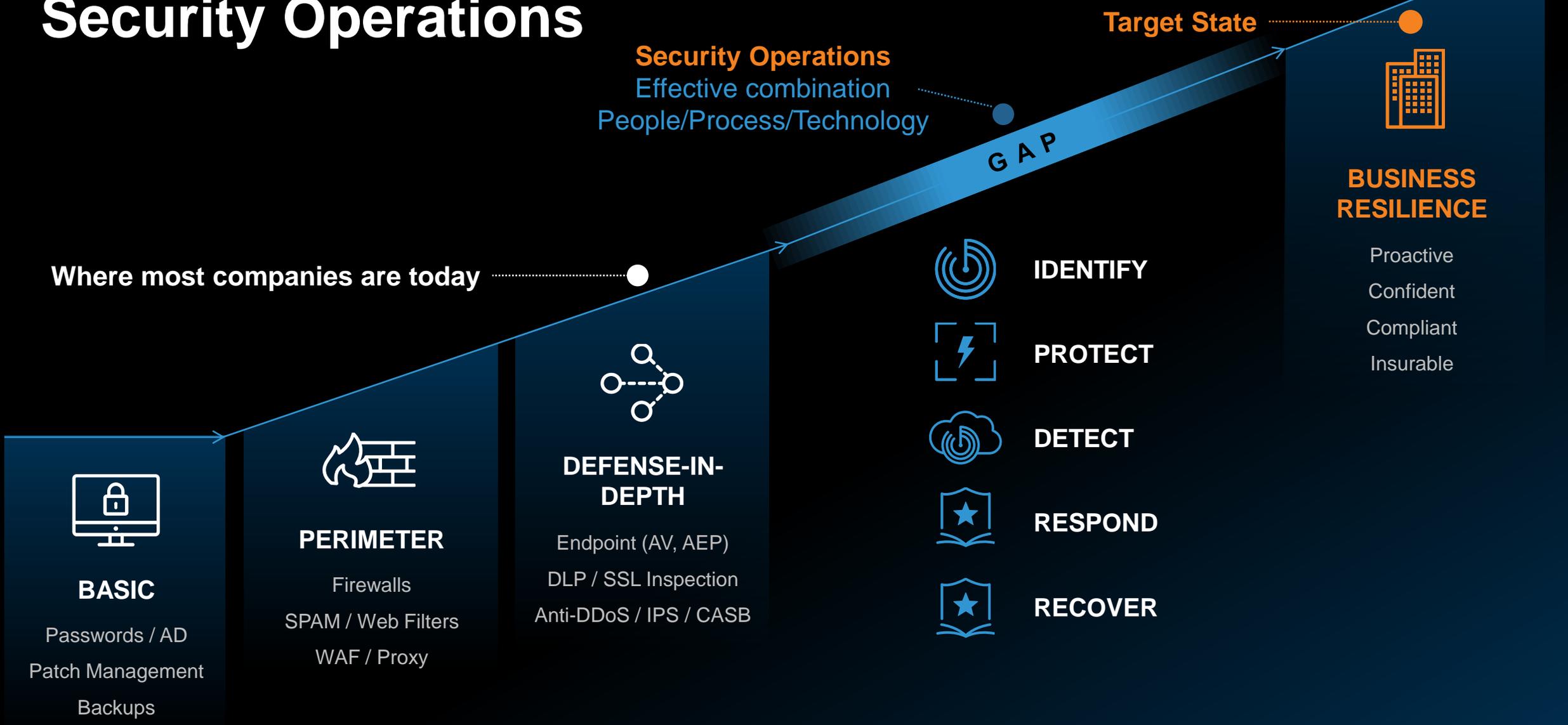


Concierge Security Journey

Proactive security hardening



Security Operations





Thank You

jason.monger@arcticwolf.com

www.linkedin.com/in/jasonmonger/