ARCTIC WOLF

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

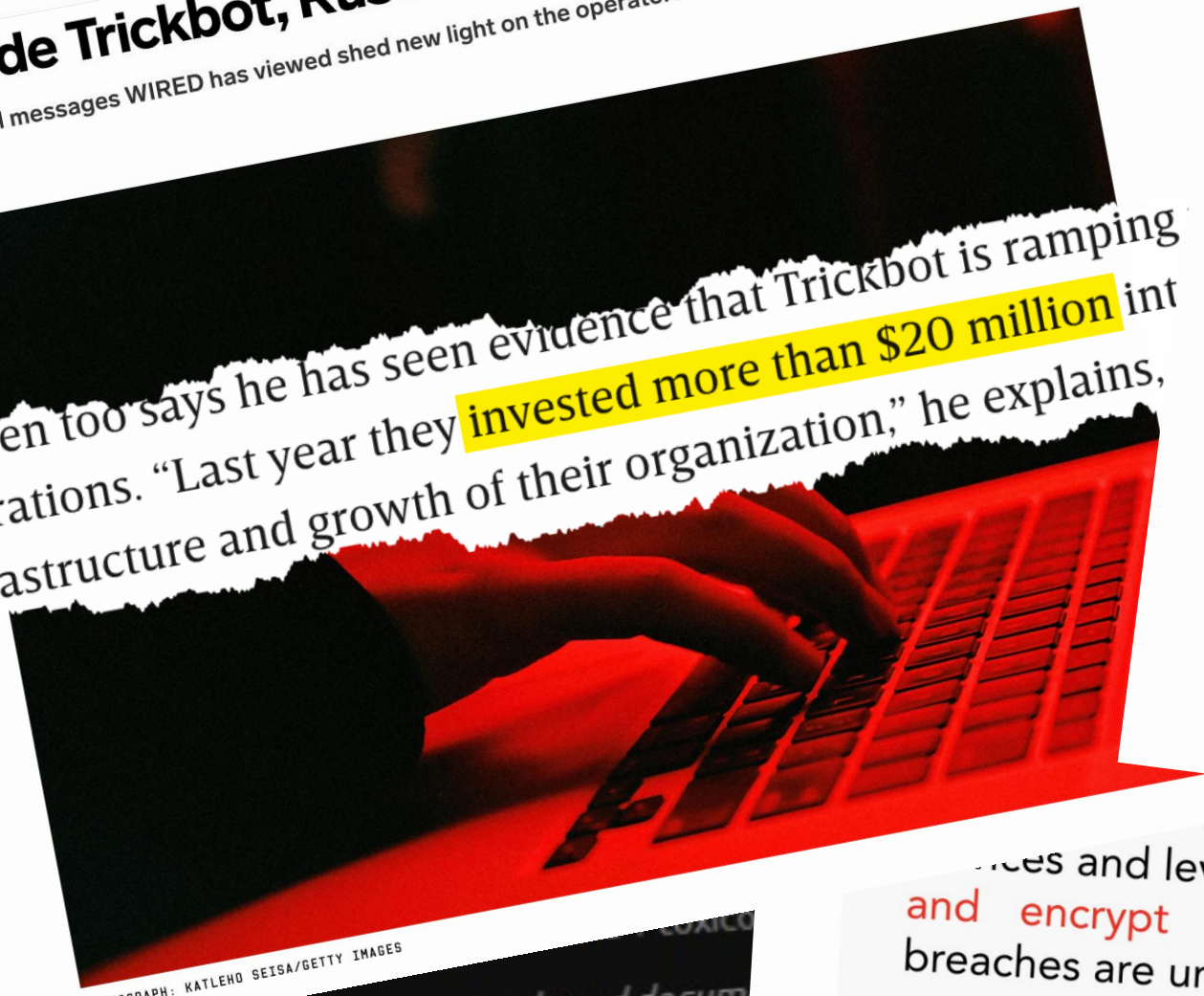
Prepared By:
Jason Monger, Senior PreSales Engineer
Arctic Wolf Networks

Cybercrime e

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 int infrastructure and growth of their organization," he explains,

PHOTOGRAPH: KATLEHO SEISA/GETTY IMAGES

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO

TECH

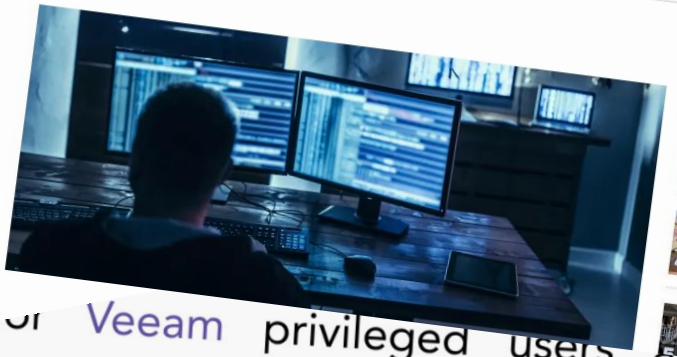
Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'

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

Monica Buchanan Pitrelli @MONICAPITRELLI

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.



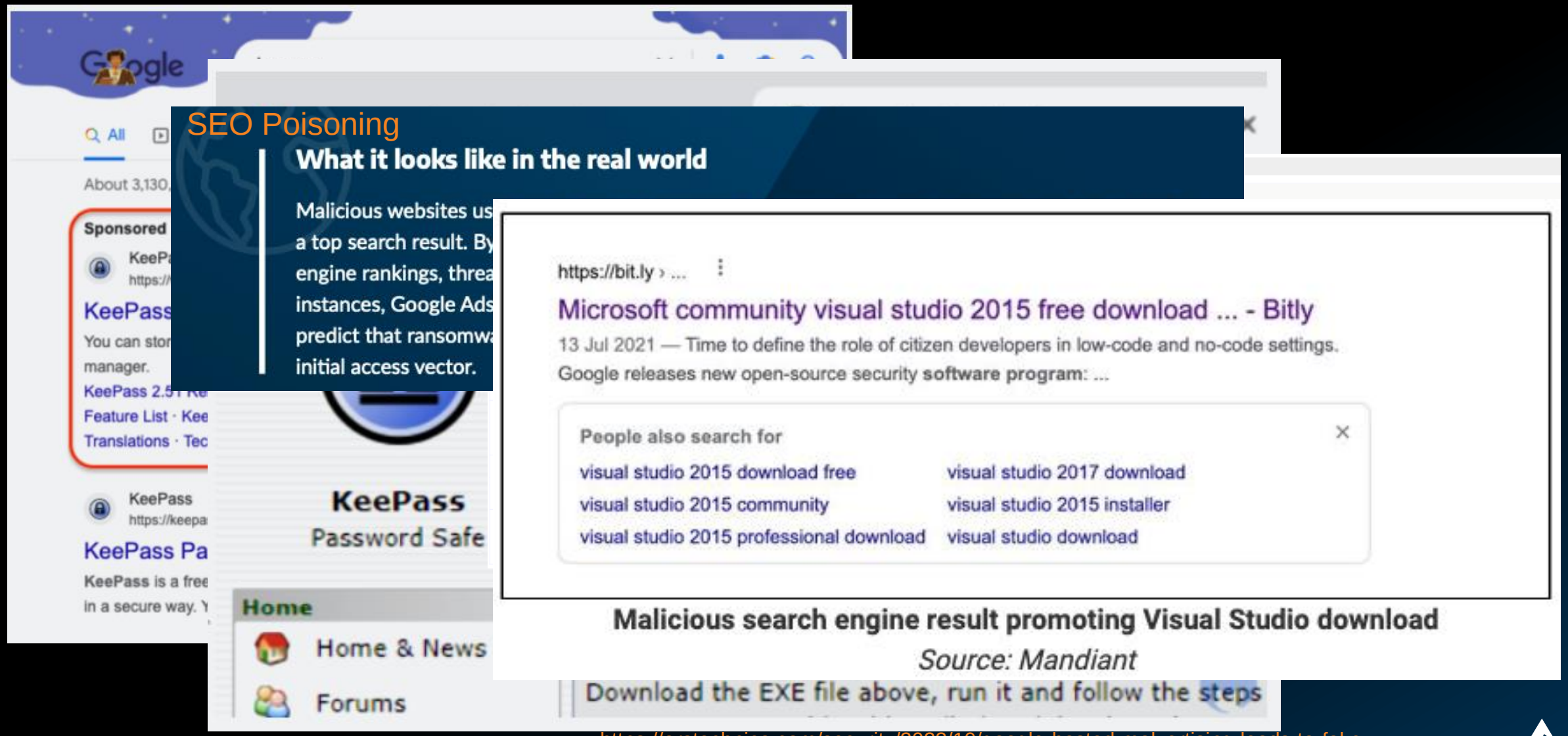
TRENDING NOW

Graduation Night

Veeam privileged users

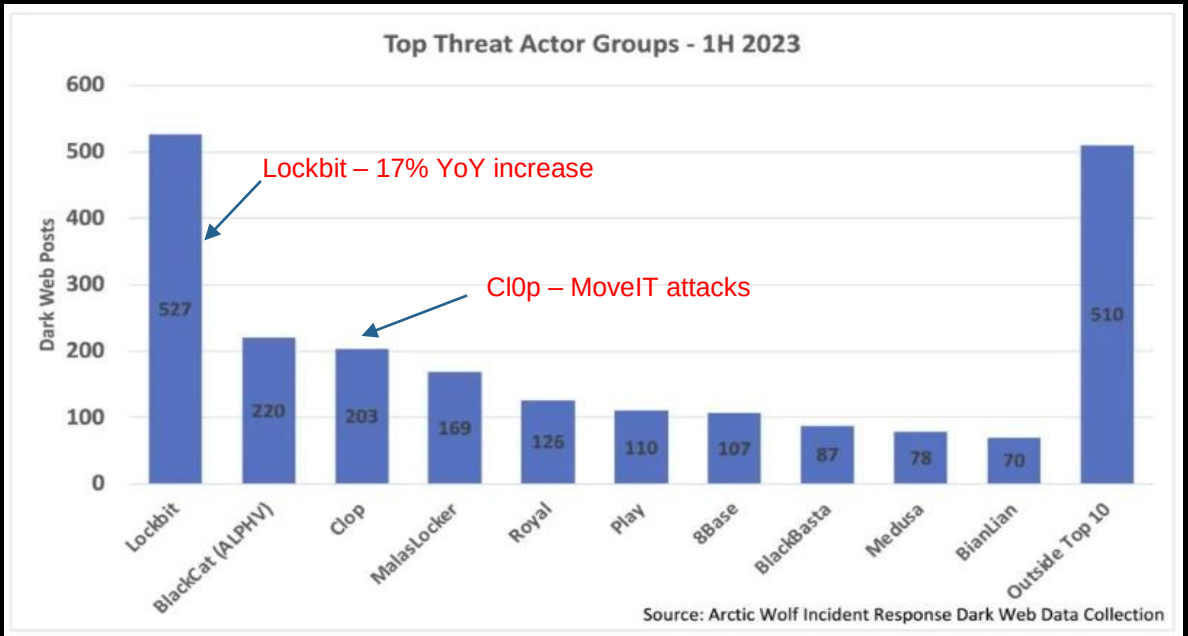
ces and leverages to access, exfiltrate, remove and encrypt backups to ensure ransomware breaches are un-"backupable"

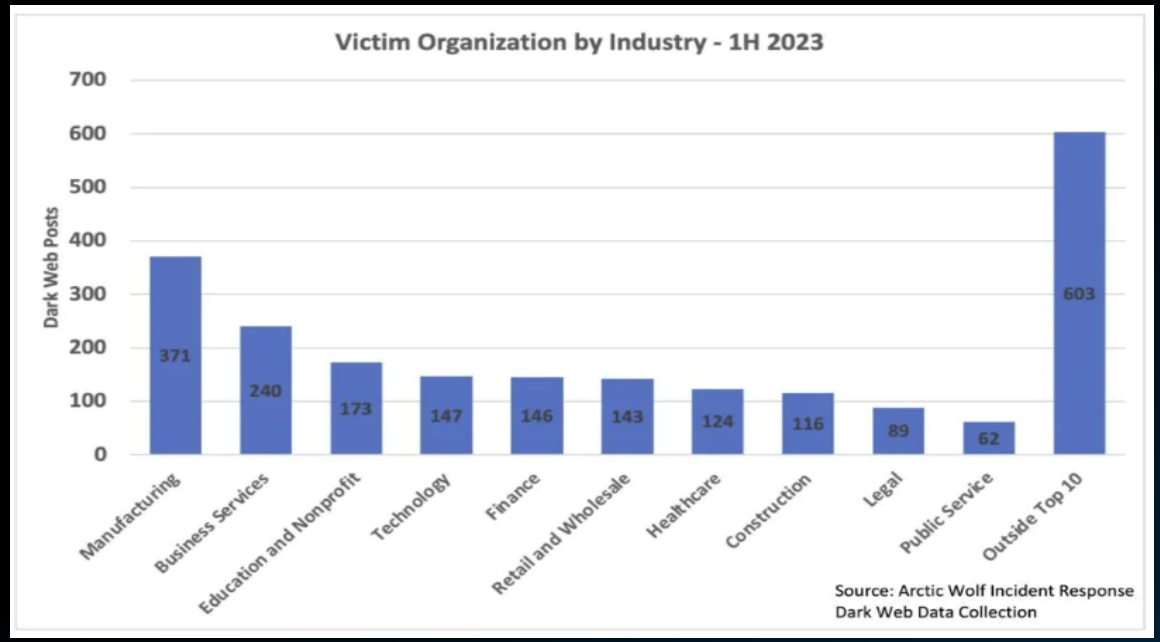
Ever more difficult for end users



https://arstechnica.com/security/2023/10/google-hosted-malvertising-leads-to-fake-keepass-site-that-looks-genuine/

Arctic Wolf Labs - 1H2023 Ransomware Landscape



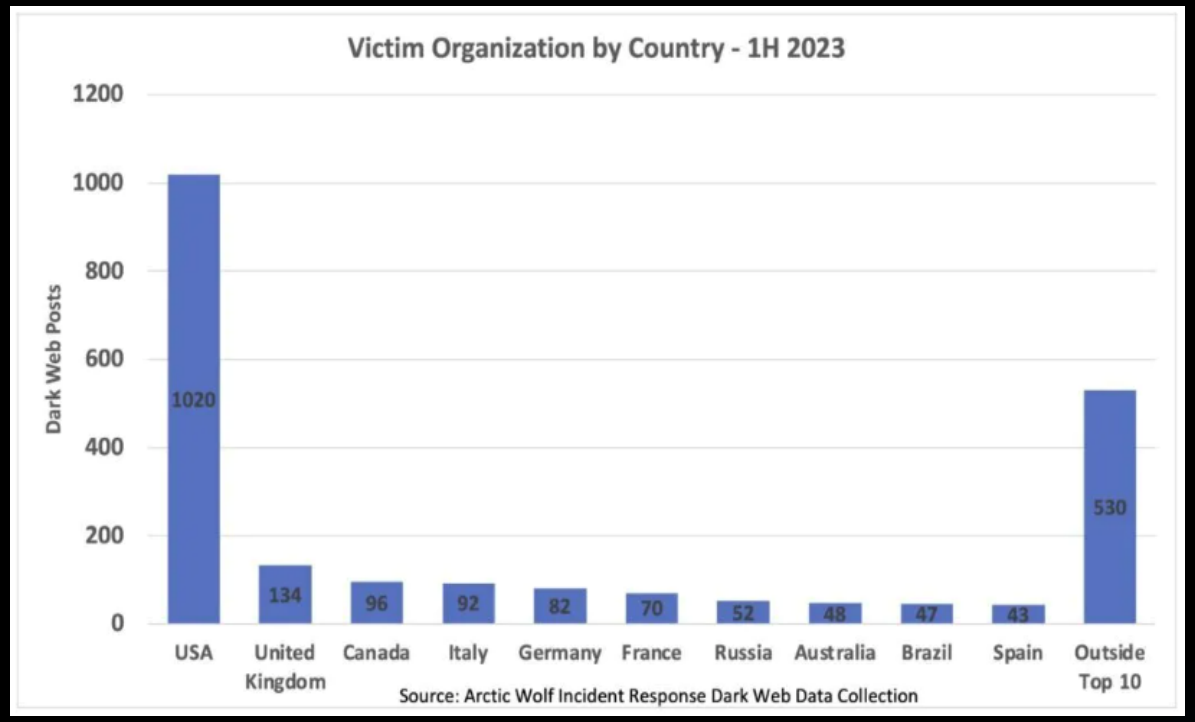


Ransomware attacks growing again
43% increase over 2H22

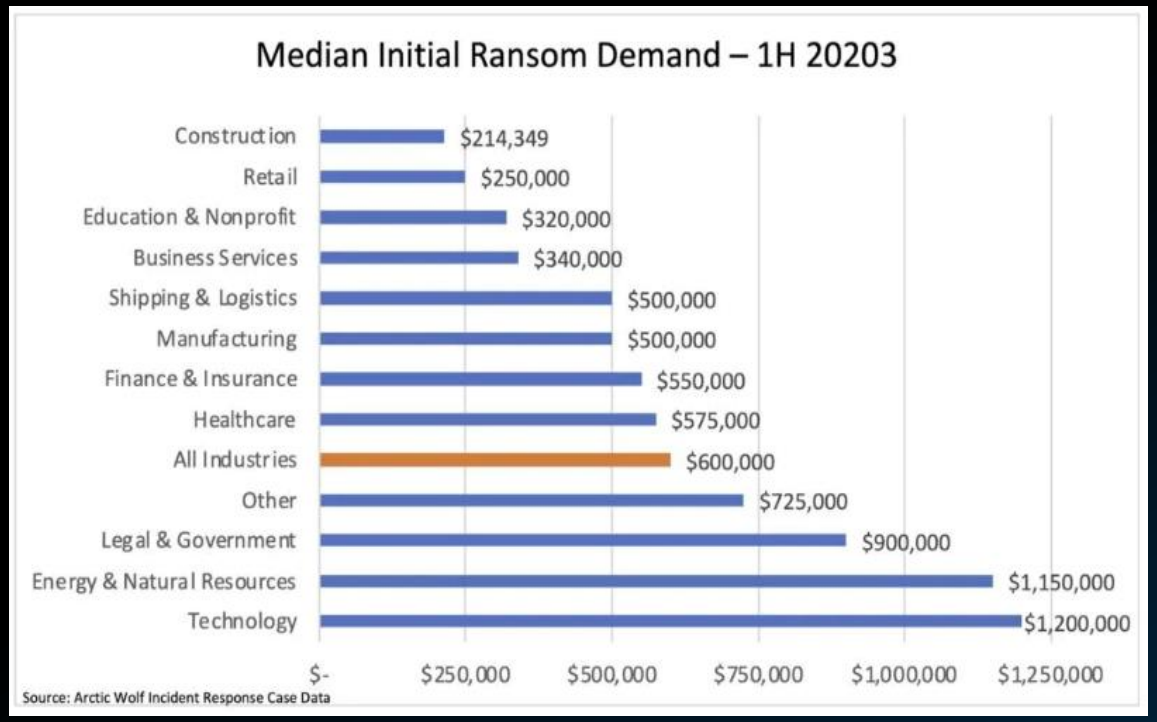
Opportunistic and not necessarily sector specific

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

Arctic Wolf Labs - 1H2023 Ransomware Landscape



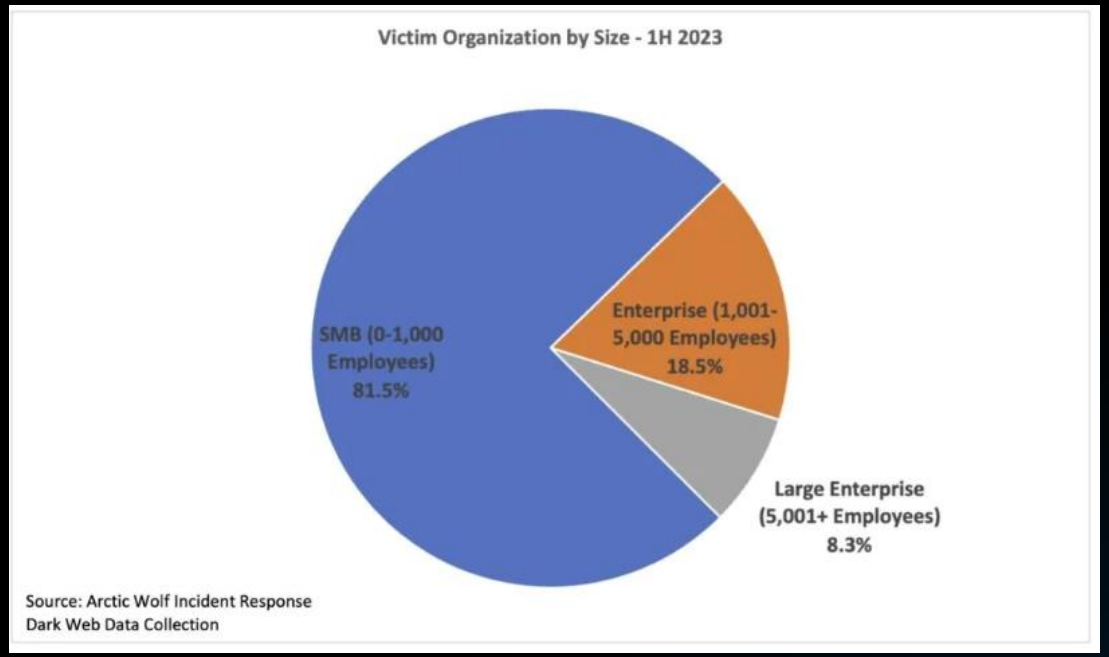
English speaking countries most attacked



Ransom demand is a fraction of overall cost

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

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

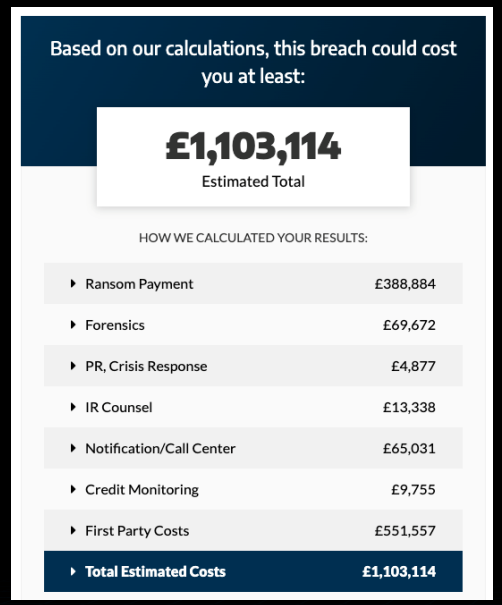
Breached: January 22…	Breached: September 22	Ransomed: Sept 23
Attack using a hacked, trusted **supply chain** computer and account to authenticate into Okta’s systems	Attack by **taking over a user account** by a) compromising the users **personal device** with malware and b) tricking the user into confirming the MFA challenge upon login	Attackers used vishing / **social engineering** on the IT helpdesk

Quantifying Cyber Risk

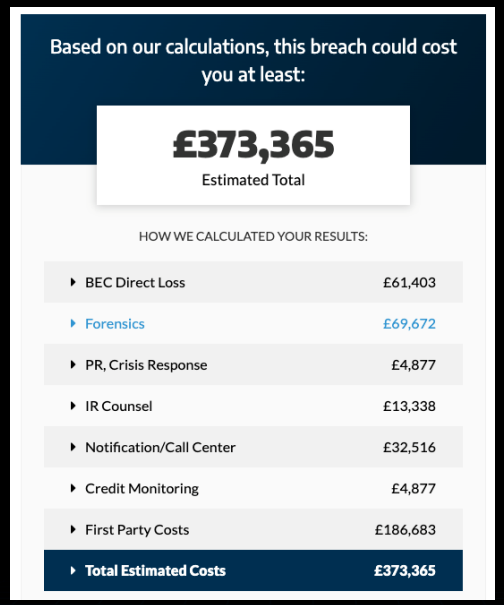
LIKELIHOOD
OF AN INCIDENT

IMPACT
OF AN INCIDENT

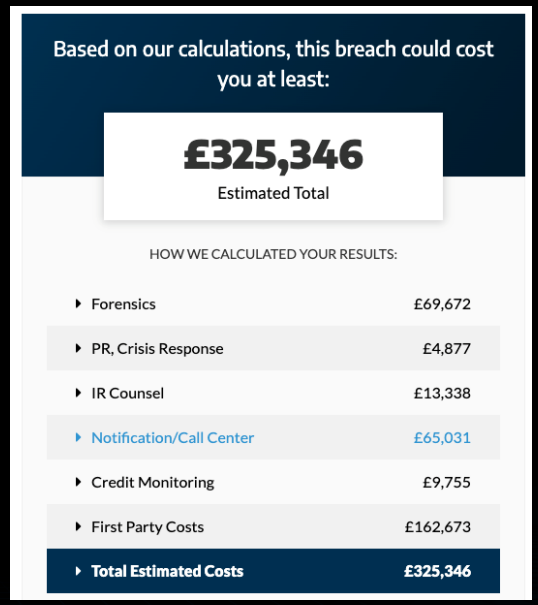
Calculating the cost of an incident



Ransomware
9%



BEC
20%



Data Breach
15%

Breach Scenario:

Ransomware
BEC
Data Breach

Sector:

Insurance, UK

Number of Users

300

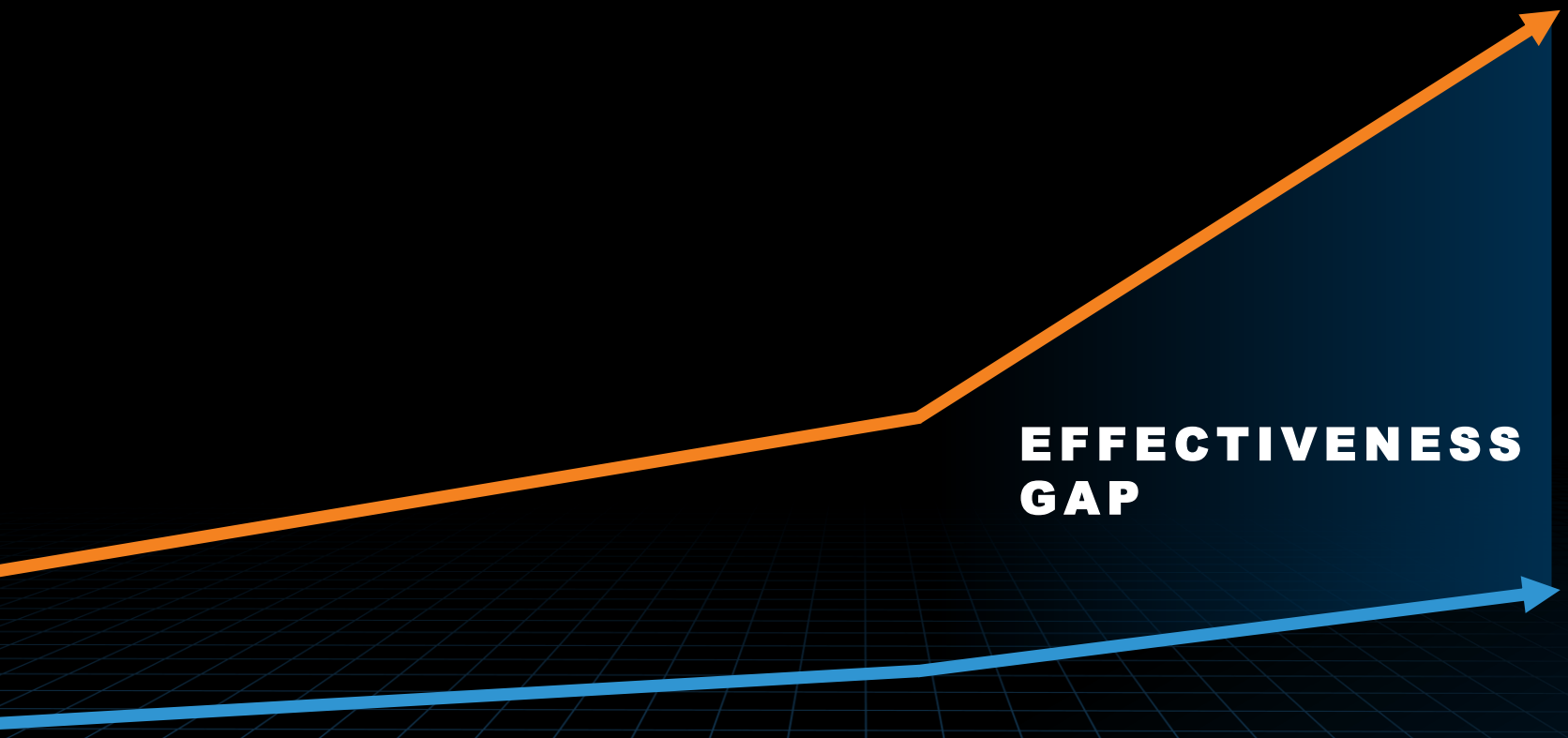
Annual Revenue:

£40m

Total Cyber Risk ~ £1.8m
Combined Annualised Risk ~£223k

https://arcticwolf.com/calculating-the-cost-of-a-breach/

Accelerating Risk



48%
INCREASE
in Cybercrime Losses in 2022

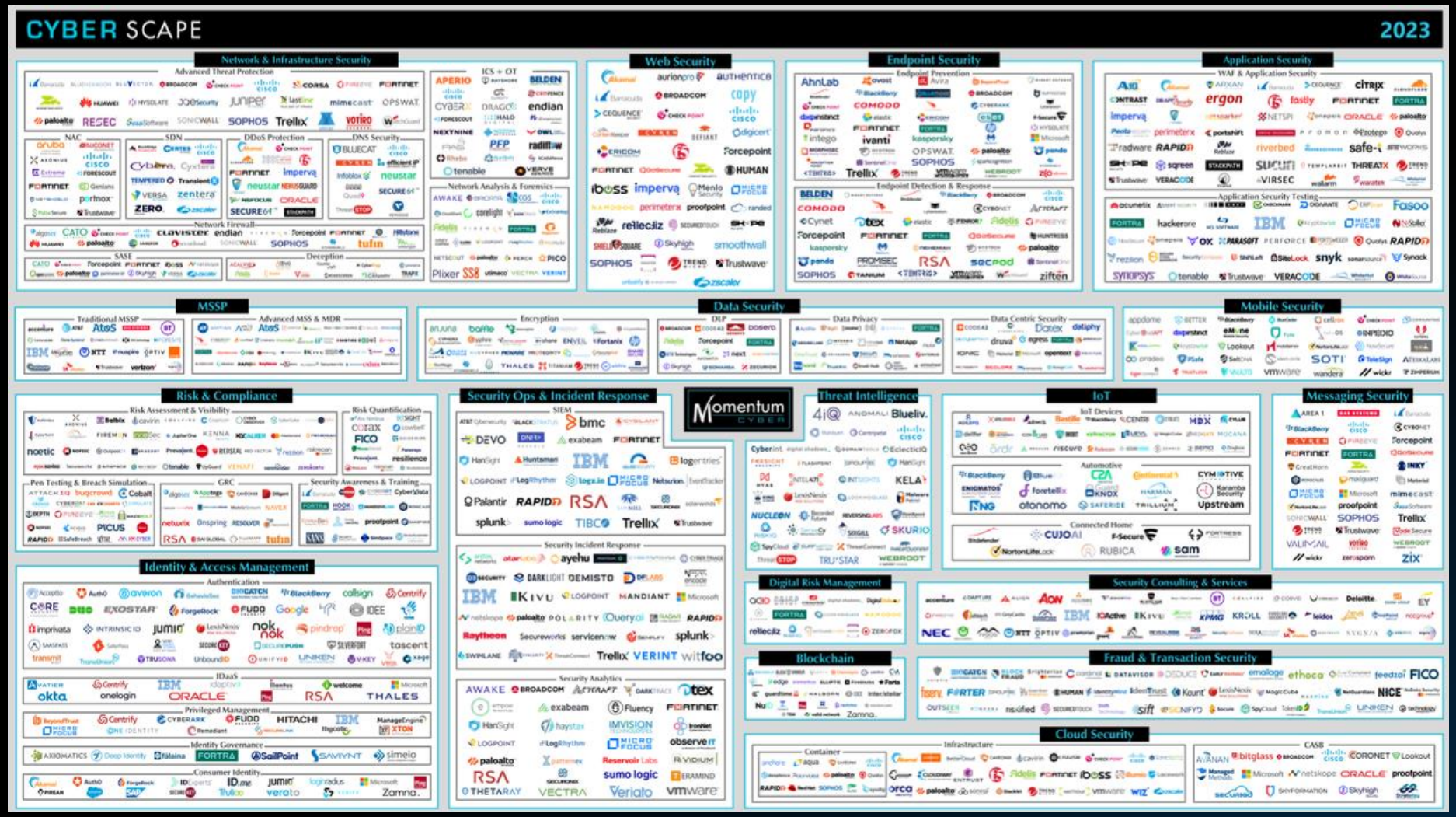
Total Security Companies:
3,377+

Total Security Spend:
$169B

YoY Spend Increase:
11%

Sources: IC3, Gartner, It-Harvest

Cyber Scape



Credit: https://momentumcyber.com/intel/

Security Evolution Drivers

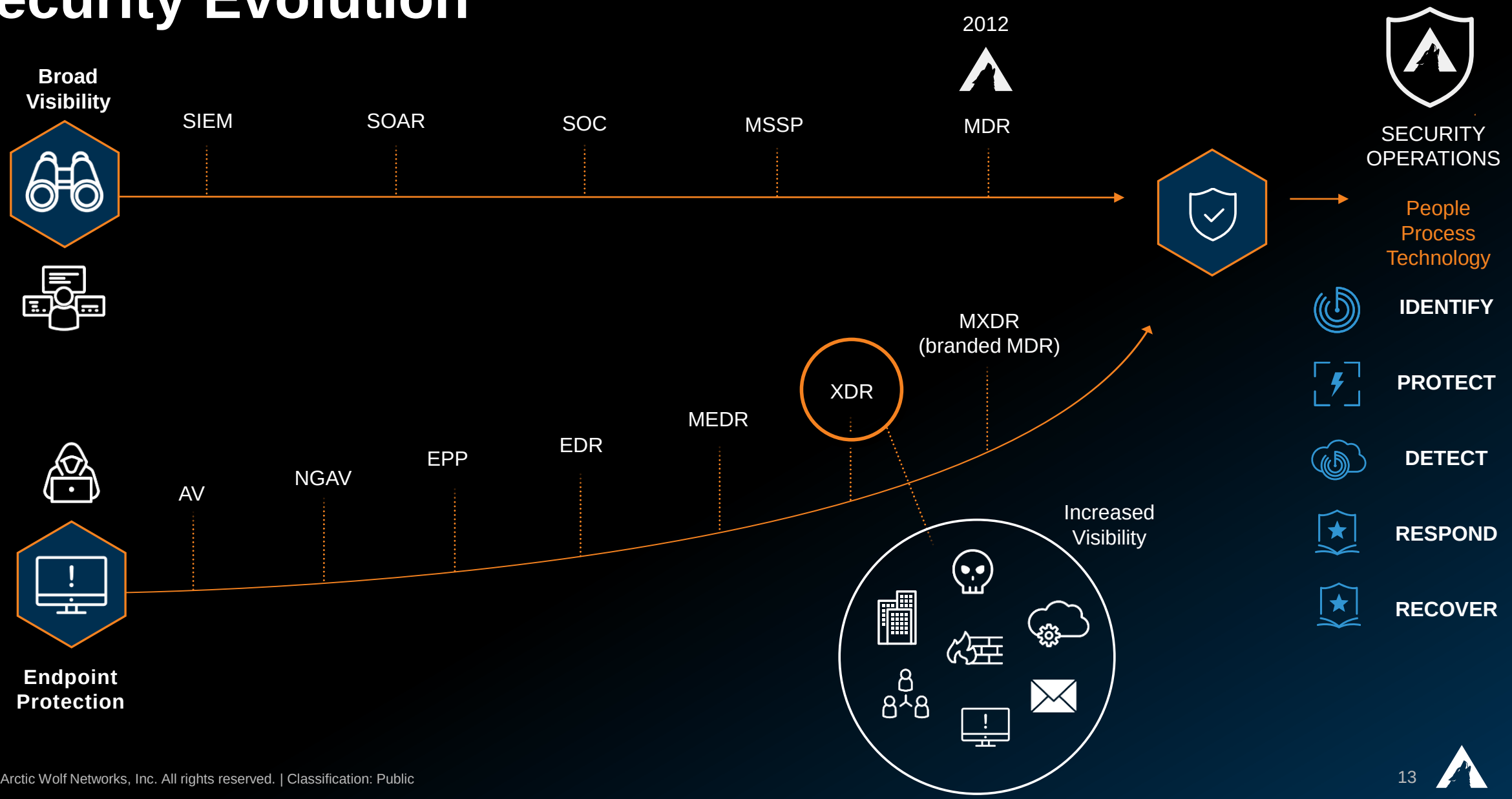
Business Drivers

- 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

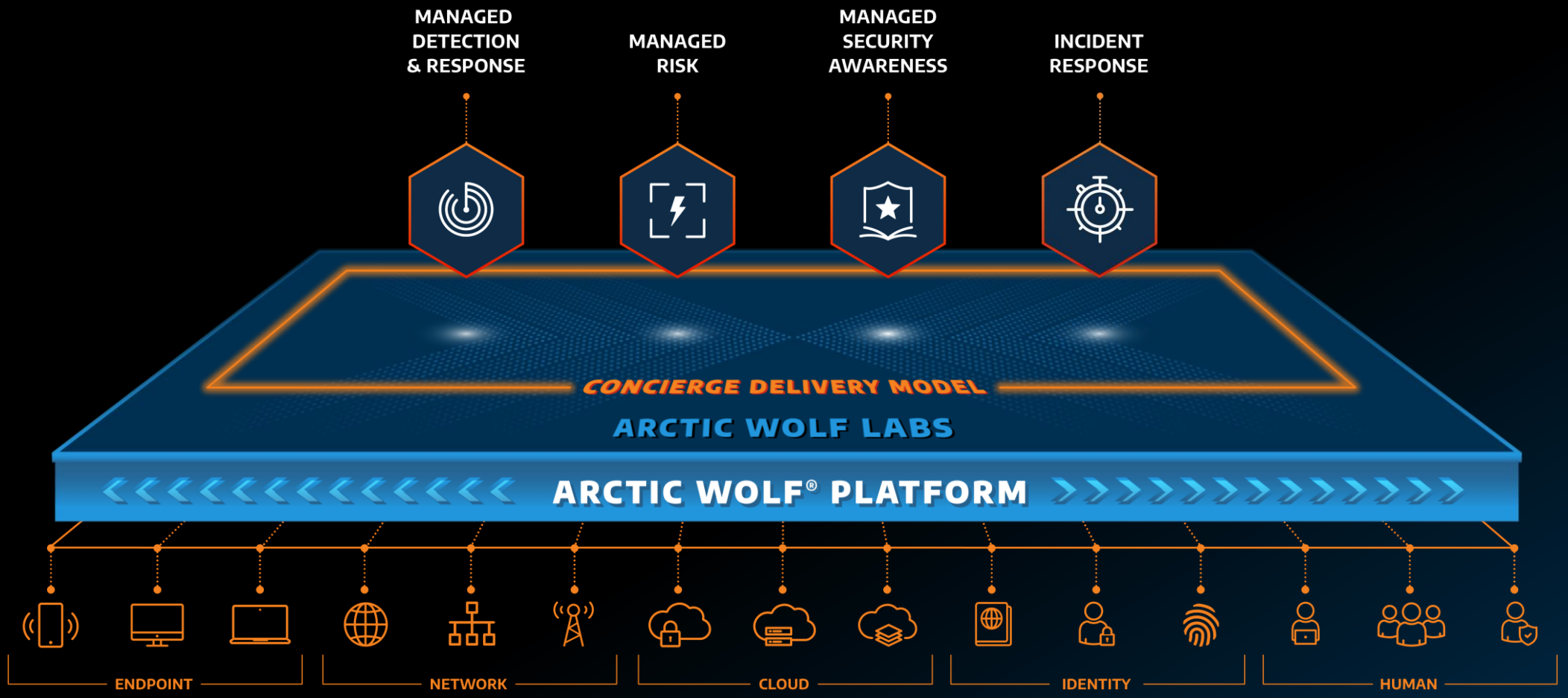
Security Evolution



How to address Cyber Risk

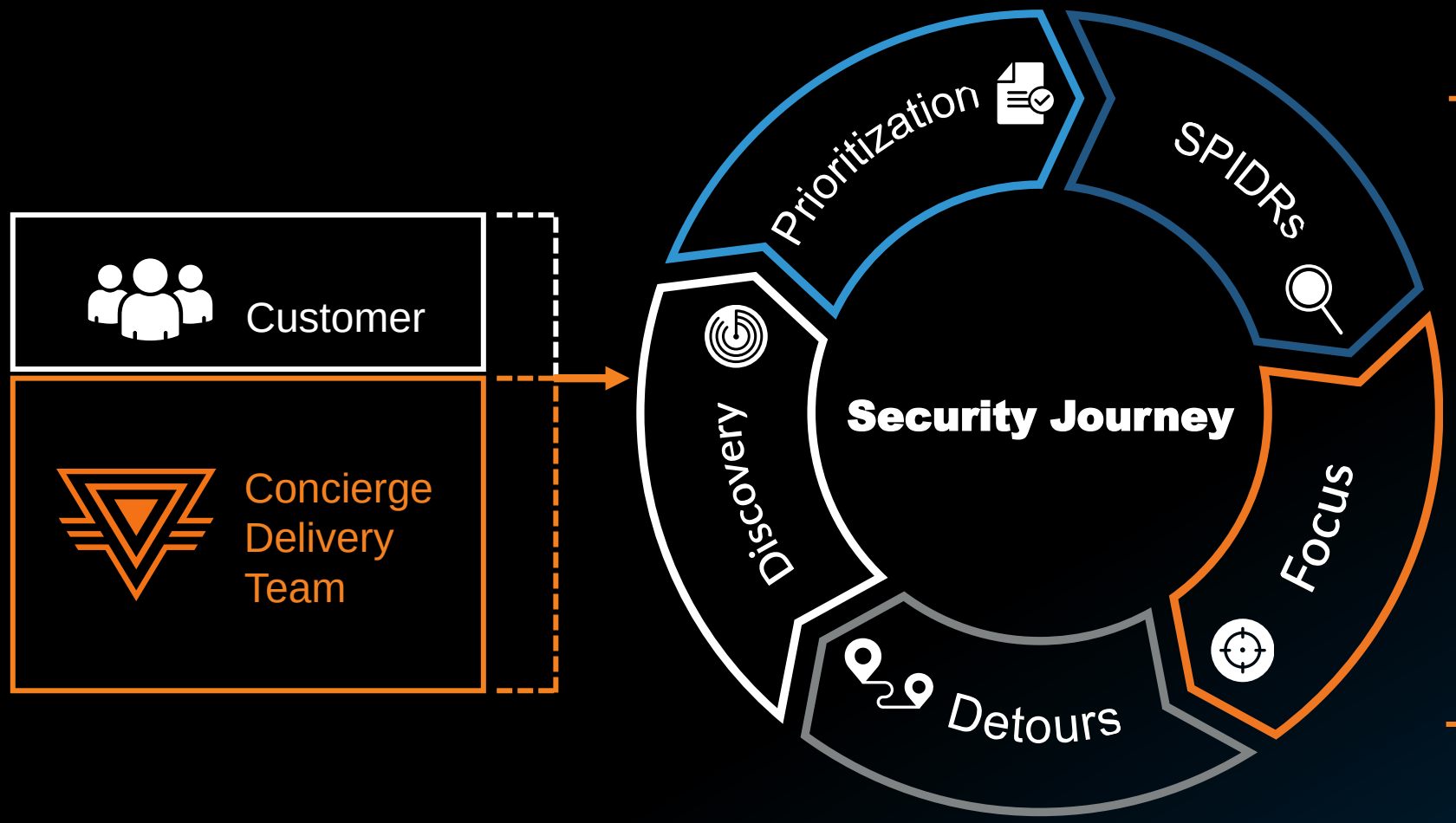
ARCTIC WOLF

Security Operations Cloud



Concierge Security Journey

Proactive security hardening



- Cyber Risk Reduction
- Ensuring Insurability / Compliance
- Fast Time Security Value
- Eliminate Blind-spots

Security Operations

Target State

Security Operations
Effective combination
People/Process/Technology

GAP

Where most companies are today

BASIC

Passwords / AD
Patch Management
Backups

PERIMETER

Firewalls
SPAM / Web Filters
WAF / Proxy

DEFENSE-IN-DEPTH

Endpoint (AV, AEP)
DLP / SSL Inspection
Anti-DDoS / IPS / CASB

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

BUSINESS RESILIENCE

Proactive
Confident
Compliant
Insurable

Thank You

jason.monger@arcticwolf.com

www.linkedin.com/in/jasonmonger/

THE LEADER IN SECURITY OPERATIONS