cybereason
A LevelBlue Company

TTP Briefing:

Q4 2025

cybereason
A LevelBlue Company

Methodology

This TTP Briefing is based on threat intelligence collected directly from Cybereason incident response engagements worldwide, which are technology-agnostic, and supplemented with data from a selection of Global Security Operations Center (GSOC) detections. This approach reflects the attack trends, techniques, and procedures that Cybereason is currently seeing in the wild, and provides a realistic view of the evolving threat landscape for our clients.

As we continue to integrate with LevelBlue and expand our threat intelligence to include trillions of events from SpiderLabs, future TTP Briefing editions will include more findings from the unified LevelBlue IR and threat intelligence teams.

Q4 Data Overview

Top 3 Impacted Industries

- Financial Services (17%)
- Legal/Professional Services (15%)
- Manufacturing (12%)

Top 3 Threat Incident Types

- Business email Compromise (42%)
- Ransomware (28%)
- Network Intrusion (Non-Ransomware) (25%)

Top 3 Initial Intrusion Vectors

- Phishing/Social Engineering (52%)
- External Remote Services (18%)
- Exploited Vulnerabilities (18%)

KEY TAKEAWAYS - Q4

EARLIER DETECTION IS LIMITING IMPACT

Organizations are detecting pre-ransomware network intrusions earlier, enabling faster response. As a result, fewer threat actors are reaching the data exfil stage.

EDGE DEVICES REMAIN A KEY WEAKNESS

External remote services, including VPNs and RDP, continue to be targeted, with threat actors like Akira exploiting Fortinet vulnerabilities in recent campaigns.

DIVERSE PHISHING TACTICS PROVE MORE EFFECTIVE

Attackers are gaining access through increasingly varied and sophisticated phishing tactics, including calendar-based attacks.

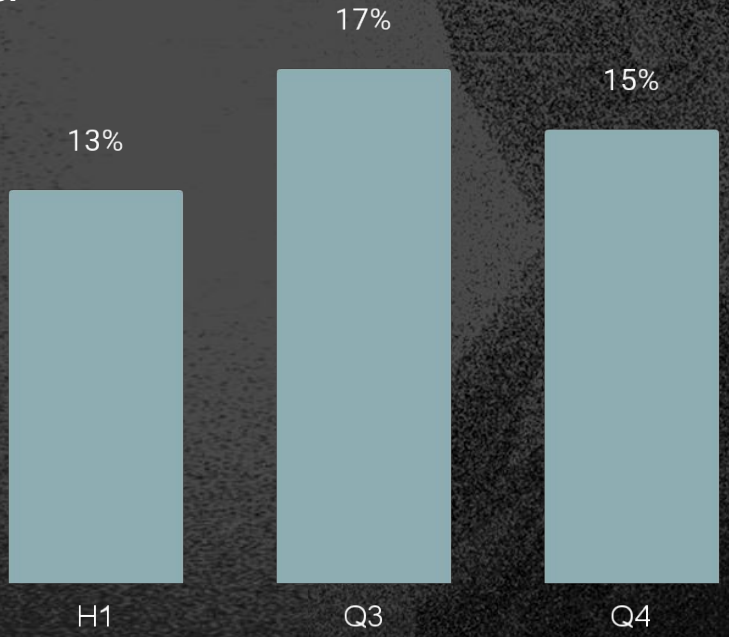
SEO POISONING INCREASES RAT DOWNLOADS

An uptick of SEO poisoning tactics led to an increase in the amount of users downloading Remote Access Tools (RATs) and opening access to their devices.

cybereason

LOLBINs REMAIN A STEADY CONCERN FOR ORGANIZATIONS IN Q4

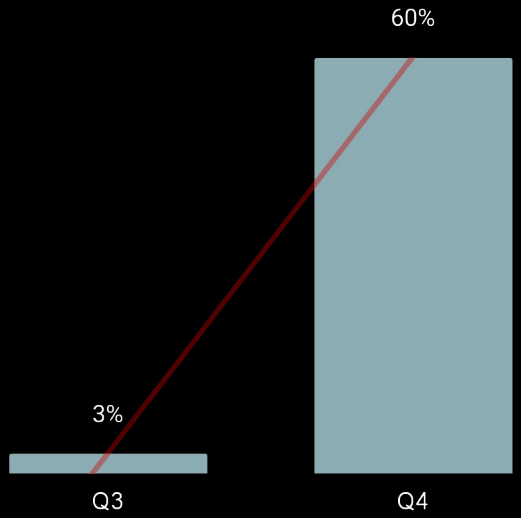
Trusted, built-in system tools let attackers blend in with legitimate activity, evade detection, and carry out attacks without deploying malware.



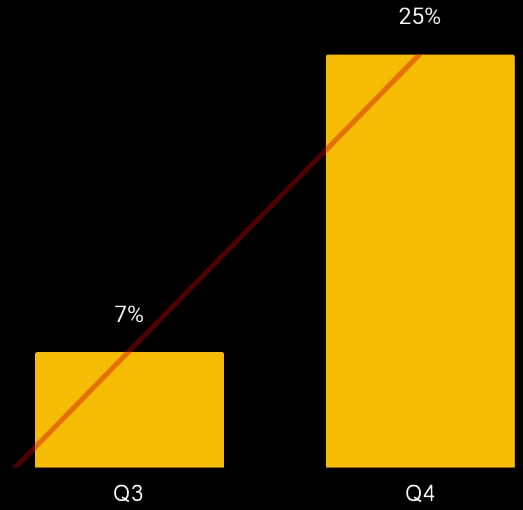
cybereason

SEO POISONING DRIVING RAT DOWNLOADS

Seemingly trusted tools and search results now a primary pathway for deeper compromise.



The use of RATs for privilege escalation jumped from 3% of cases in Q3 to 60% in Q4, enabling rapid asset discovery, lateral movement, and persistence while blending in as legitimate IT activity.

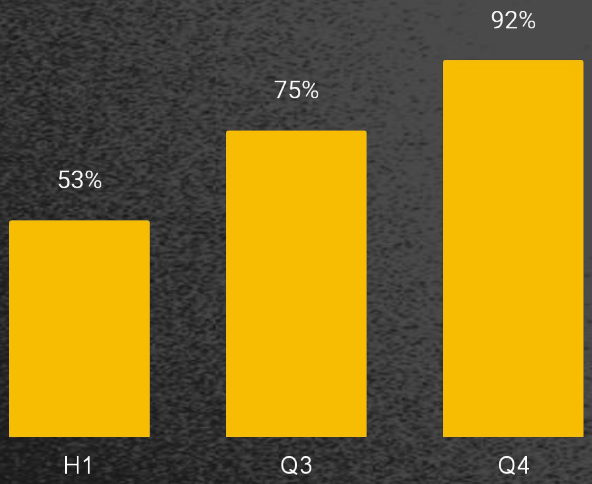


Correlates with a rise in network intrusions, which increased from 7% in Q3 to 25% in Q4.

cybereason
A LevelBlue Company

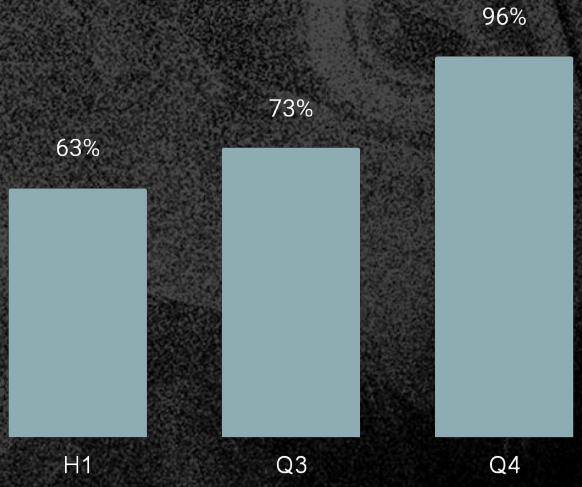
MFA IMPLEMENTATION CONTINUES TO RISE, BUT SO DO BYPASS TECHNIQUES

MFA IMPLEMENTATION



Between Q3 and Q4, we saw organizations more regularly implementing MFA, accounting for a 15+ basis points increase.

MFA BYPASS

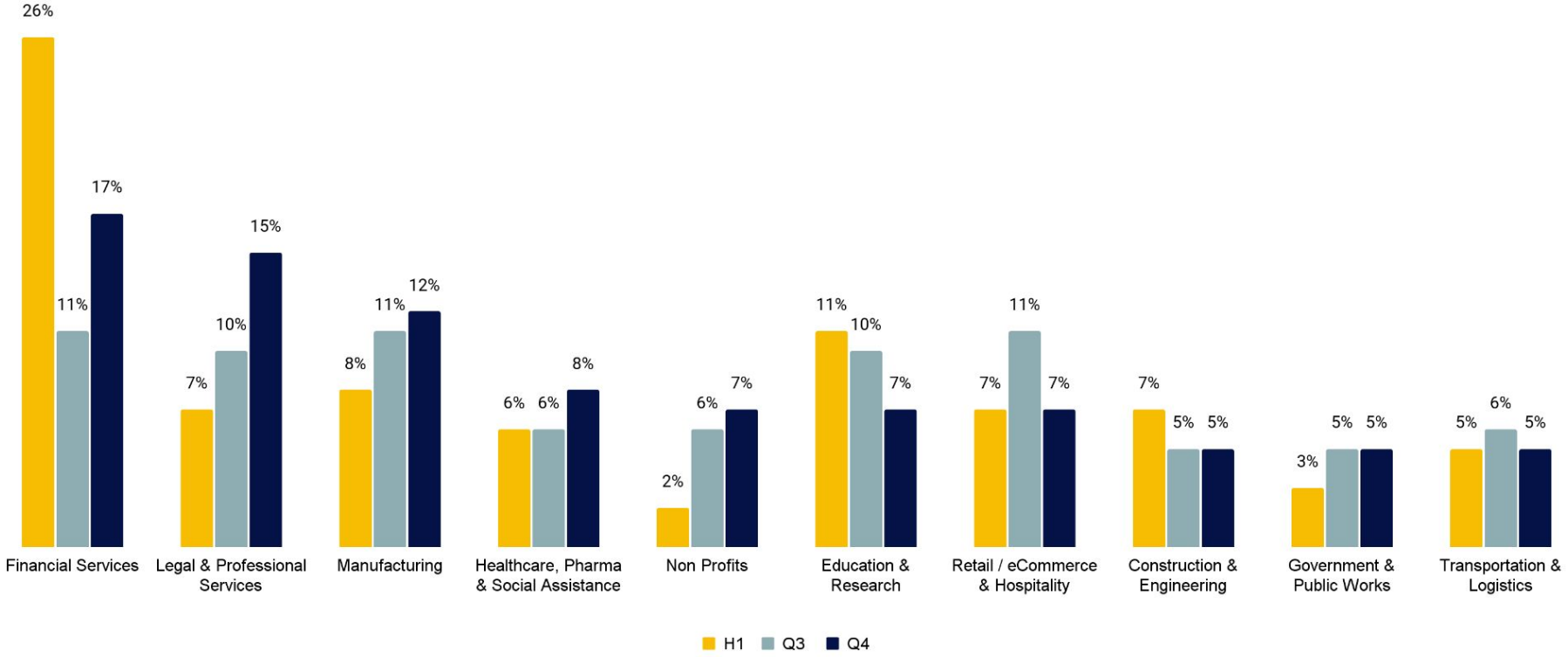


Most companies are still not implementing phishing-resistant MFA, falling victim to readily-available phishing kits and tools that intercept session tokens to bypass MFA.

cybereason

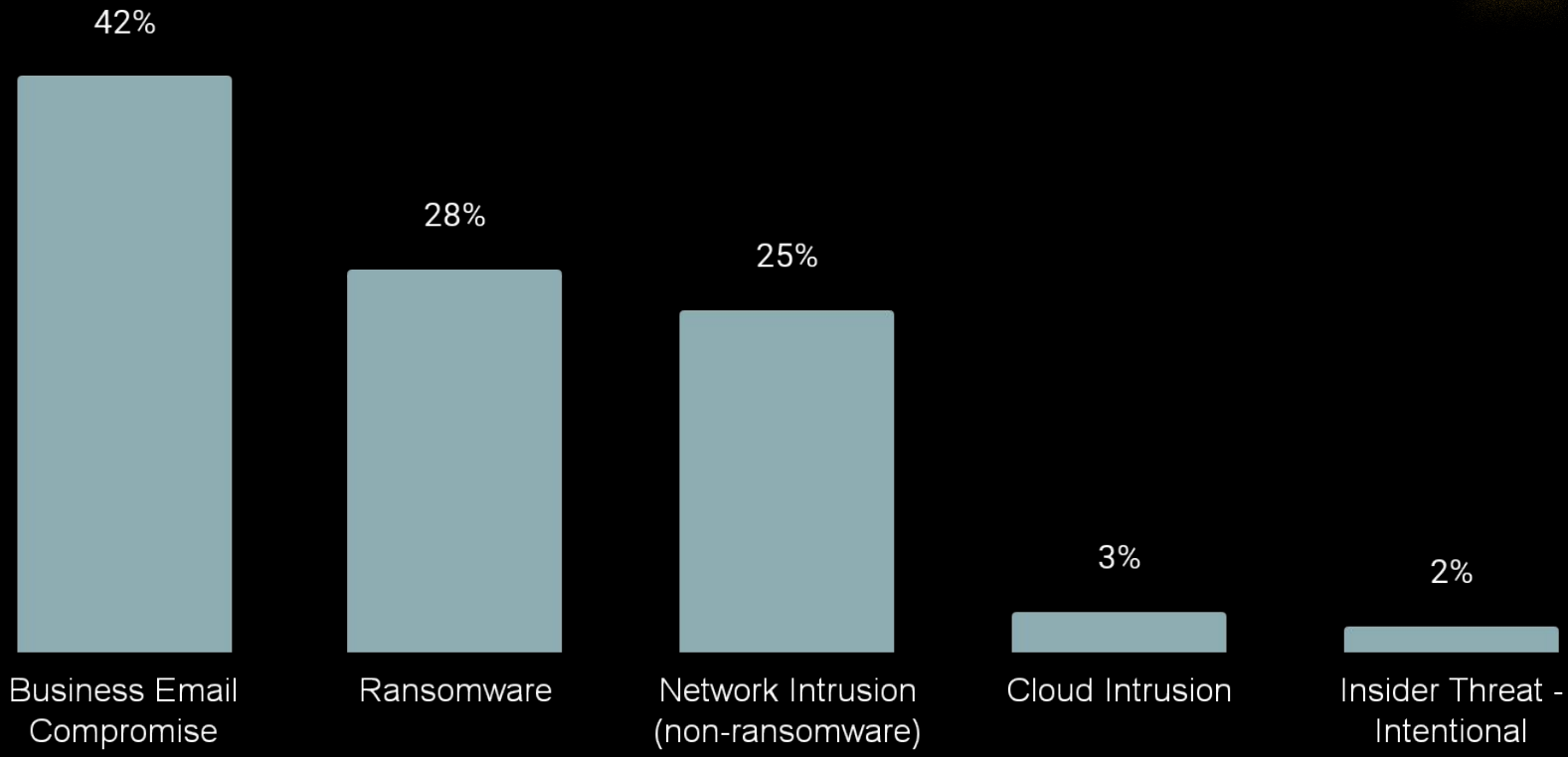
Impacted Industries Over Time

Top 10 impacted industries in Q4 compared to same industries in Q3 and H1 2025



cybereason
A LevelBlue Company

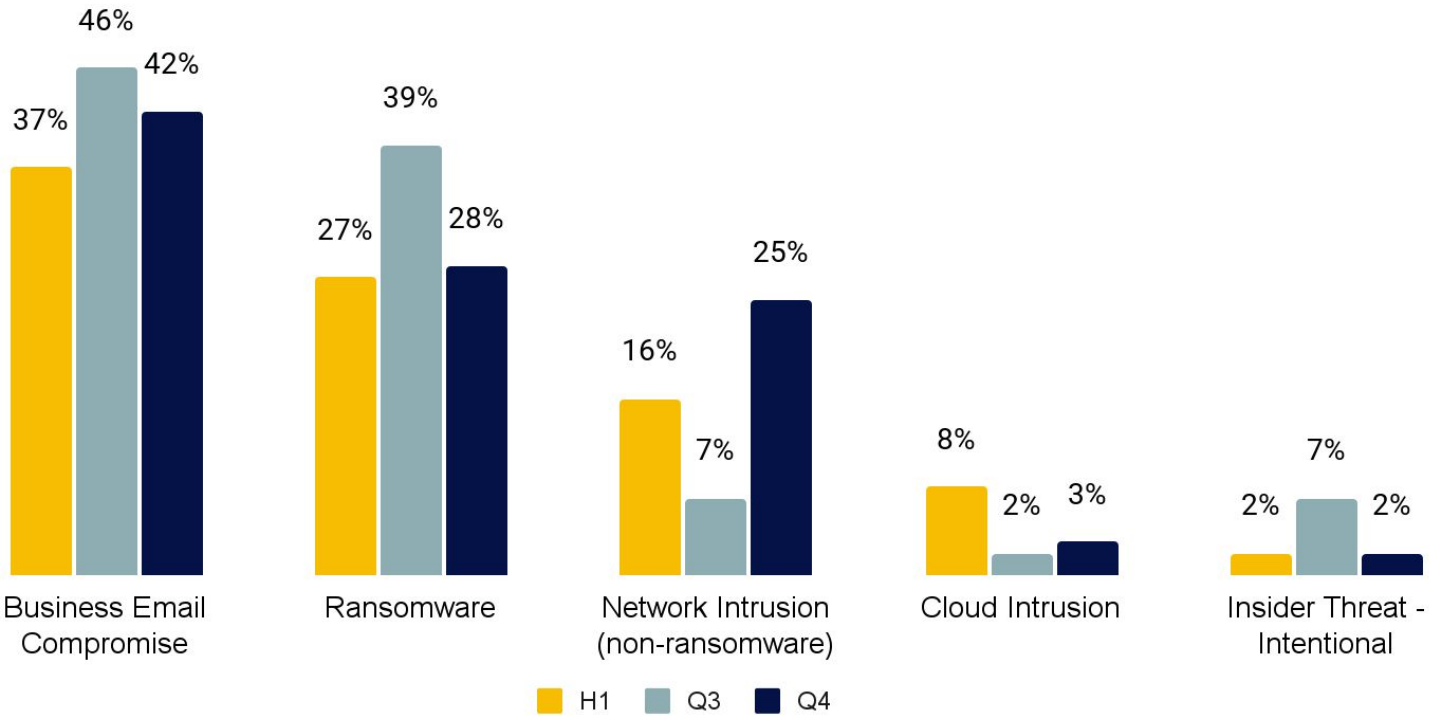
Most Common Incident Types - Q4



cybereason
A LevelBlue Company

Common Incident Types Over Time

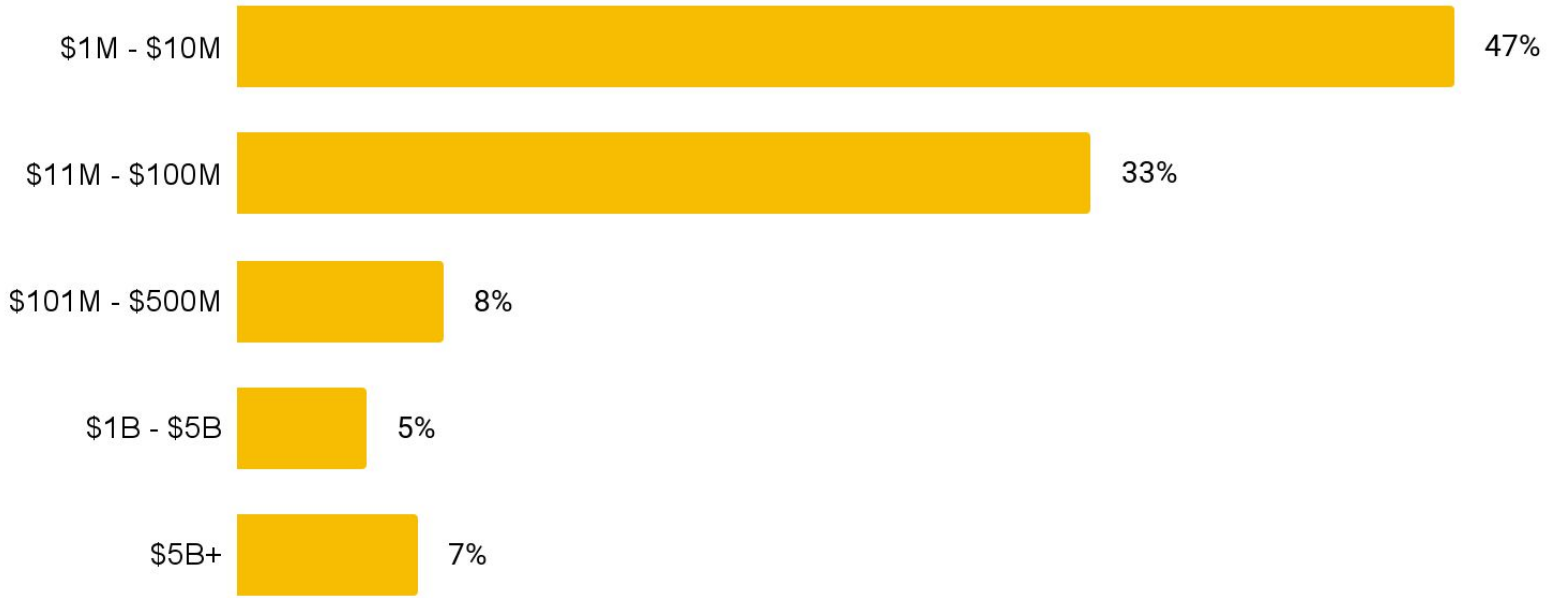
Most common incident types in Q4 compared to same incident types in Q3 and H1 2025



cybereason
A LevelBlue Company

Company Size - Q4

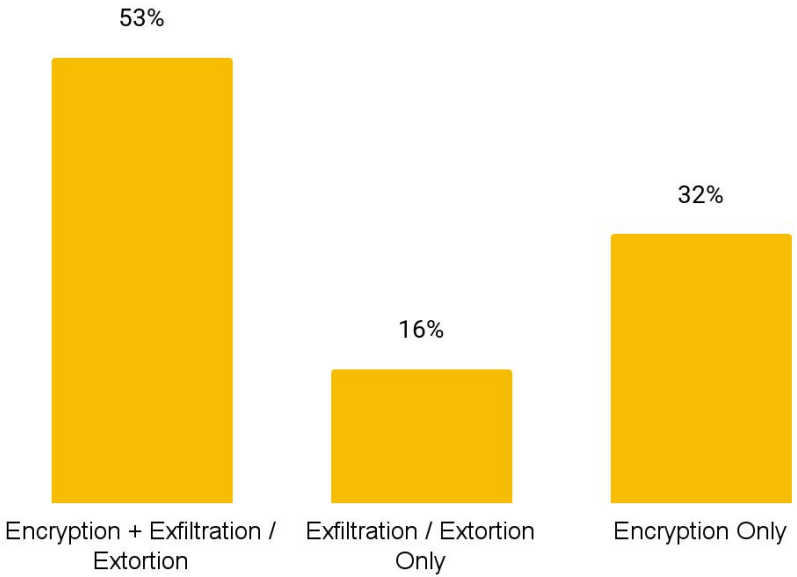
Based on revenue



cybereason
A LevelBlue Company

Ransomware Q4

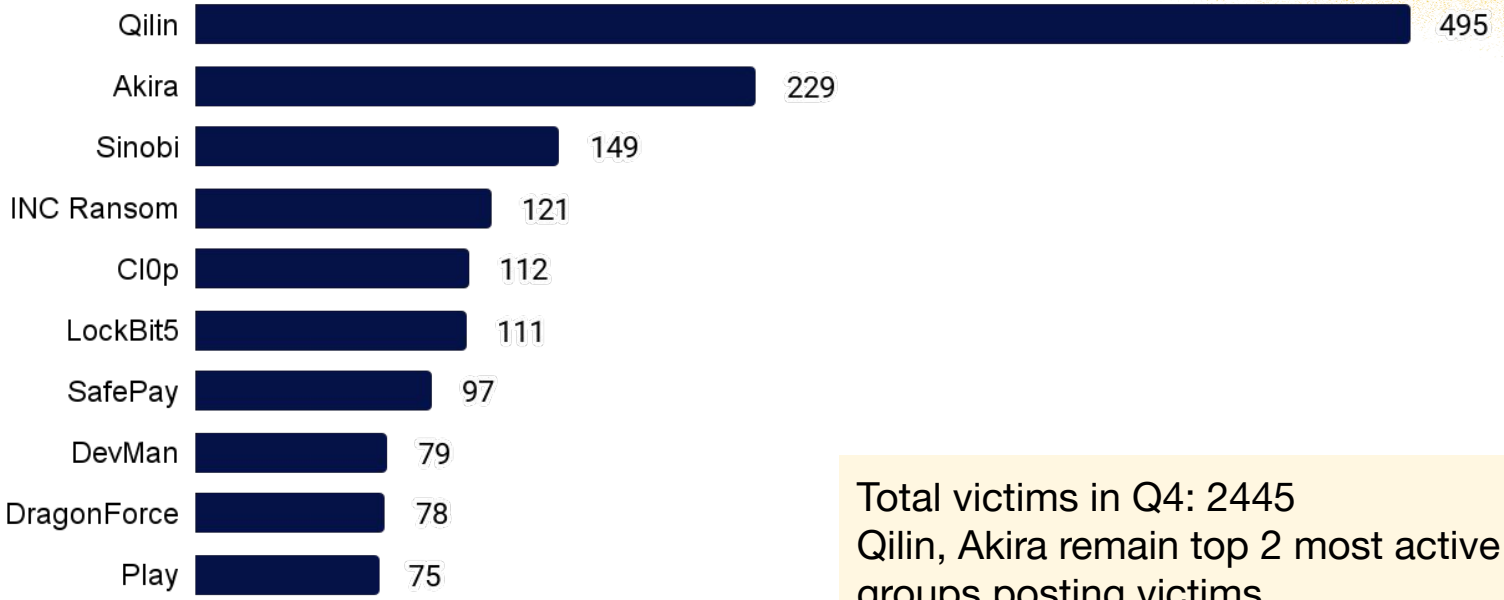
Attack Type Distribution



Top Observed Variants

High Activity:	Others:
Akira	Play
Qilin	Inc
Lockbit	DevMan
	Hardbit
	Cl0p

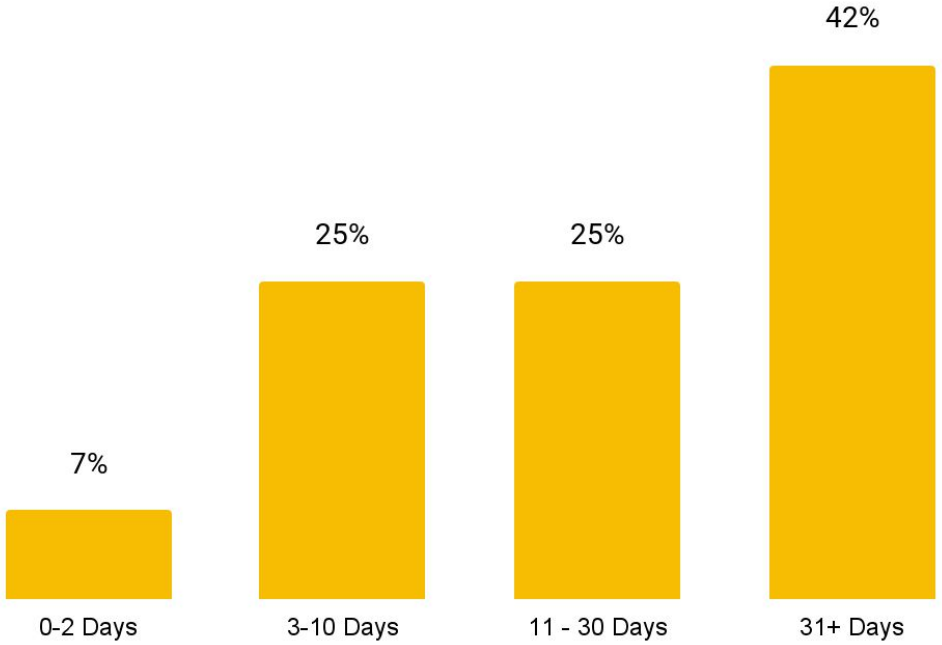
Top 10 Ransomware Shaming Site Publications - Q4



Total victims in Q4: 2445
Qilin, Akira remain top 2 most active groups posting victims

Dwell Time Q4
From Initial Intrusion to IR Kickoff

Measured from the initial date of compromise until Cybereason IR team engagement.



Dwell Time Benchmarks:

0-2 Days: Exceptional

3-10 Days: Above Average

11-30 Days: Below Average

31+ Days: Poor

** Only applies to Cybereason Consulting clients, excludes MDR clients*

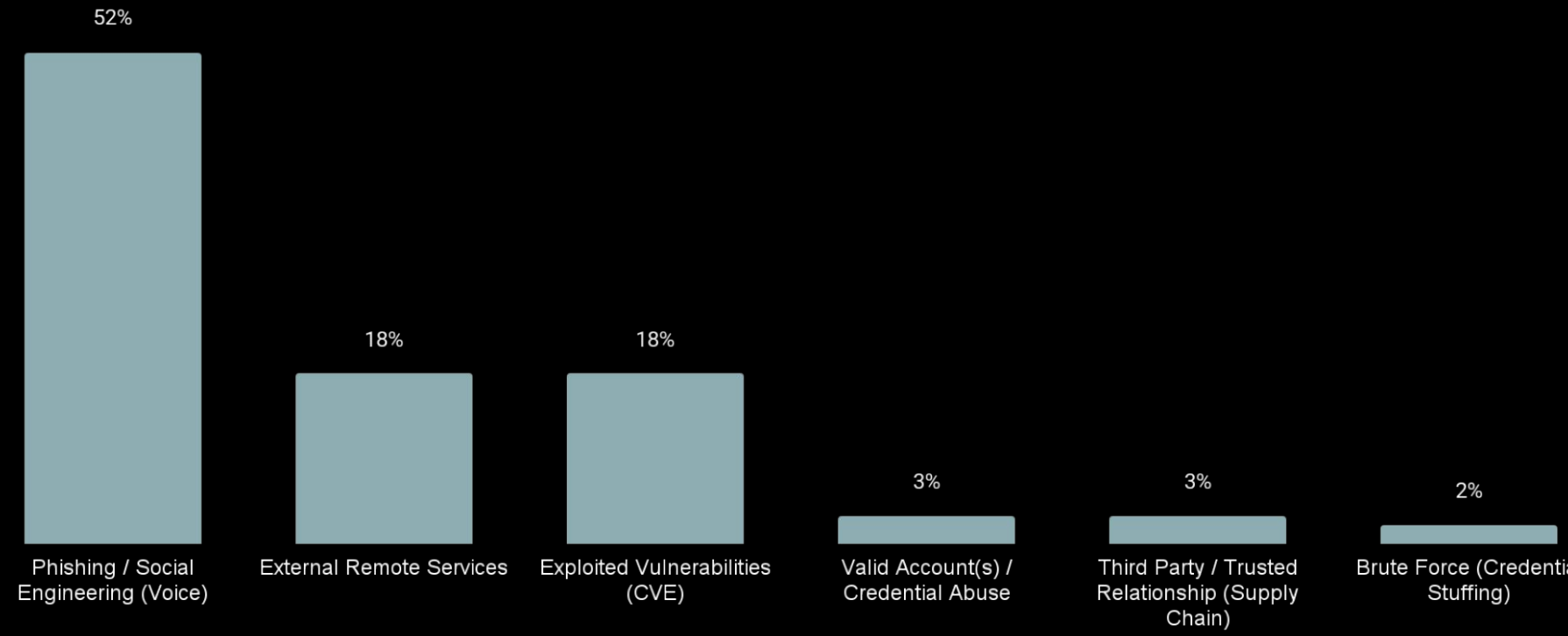
cybereason
A LevelBlue Company

Trends Across The Intrusion Path

Five Stages of Distinct Activity

1 INITIAL INTRUSION VECTOR	2 PERSISTENCE	3 ESCALATION	4 DATA AT RISK	5 END GOAL
• External Recon • Entry vector • “Patient 0”	• Internal Recon • “Where Am I?” • Foothold • Remote Access/C2	• Asset Discovery • Privilege Escalation • Lateral Movement	• View • Access • Acquire	• Encryption • Extortion • Monetize • Business Interruption

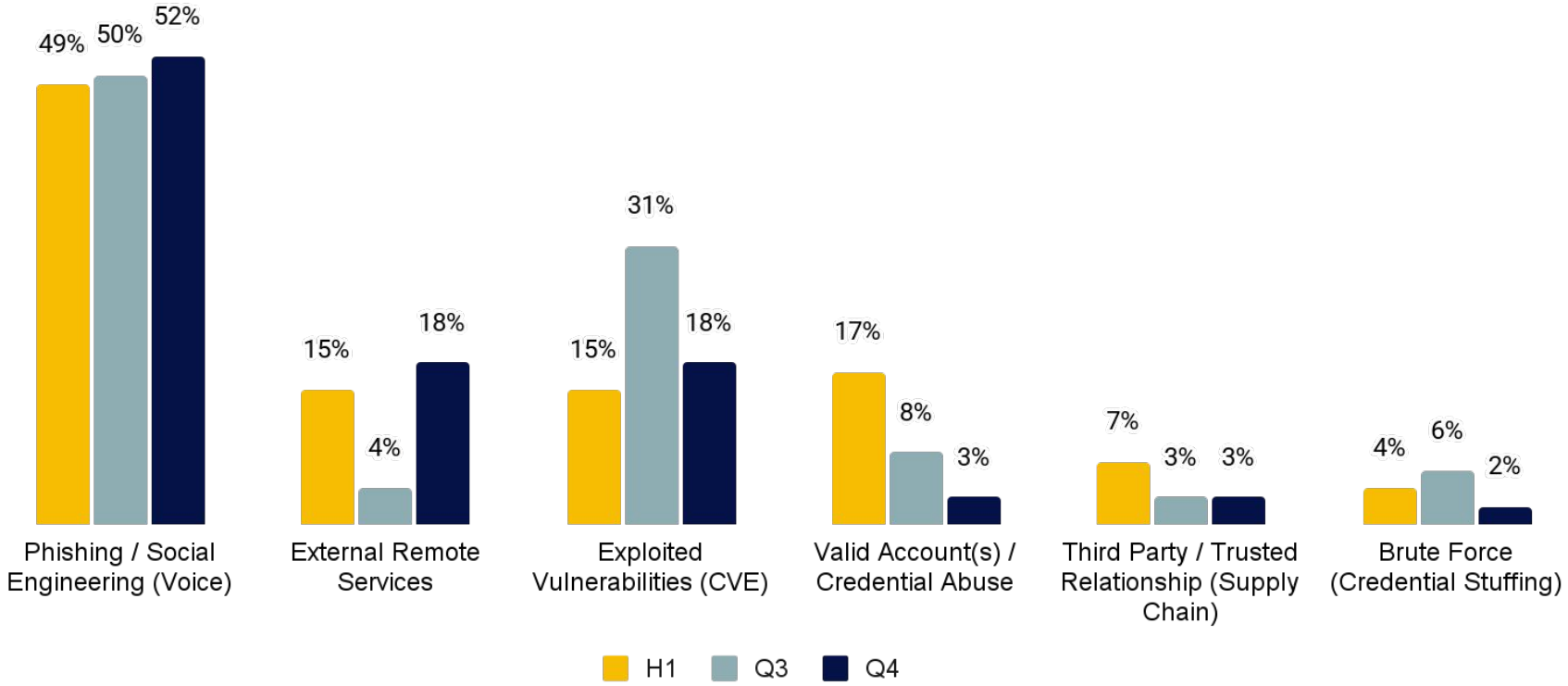
1 - Initial Intrusion Vector - Q4



cybereason
A LevelBlue Company

Initial Intrusion Vectors Over Time

Top initial intrusion vectors in Q4 compared to same intrusion vectors in Q3 and H1 2025



cybereason
A LevelBlue Company

Most Commonly Observed CVEs - Q4

CVE	Impacted Product
CVE-2025-24472	FortiOS Authentication Bypass
CVE-2025-61882	Oracle
CVE-2025-40601	SonicWall SonicOS SSL-VPN
CVE-2024-55591	Fortinet FortiOS
CVE-2024-53705	SonicWall SonicOS SSH
CVE-2024-53704	SonicWall SonicOS SSL-VPN
CVE-2024-40762	SonicWall SonicOS SSL-VPN

CVE	Impacted Product
CVE-2024-21762	Fortinet FortiOS
CVE-2023-39280	SonicWall SonicOS Stack-Based Buffer Overflow
CVE-2023-39279	SonicWall SonicOS Stack-Based Buffer Overflow
CVE-2023-39278	SonicWall SonicOS
CVE-2023-39277	SonicWall SonicOS Stack-Based Buffer Overflow
CVE-2023-39276	SonicWall SonicOS Stack-Based Buffer Overflow
CVE-2019-18935	Telerik UI

cybereason

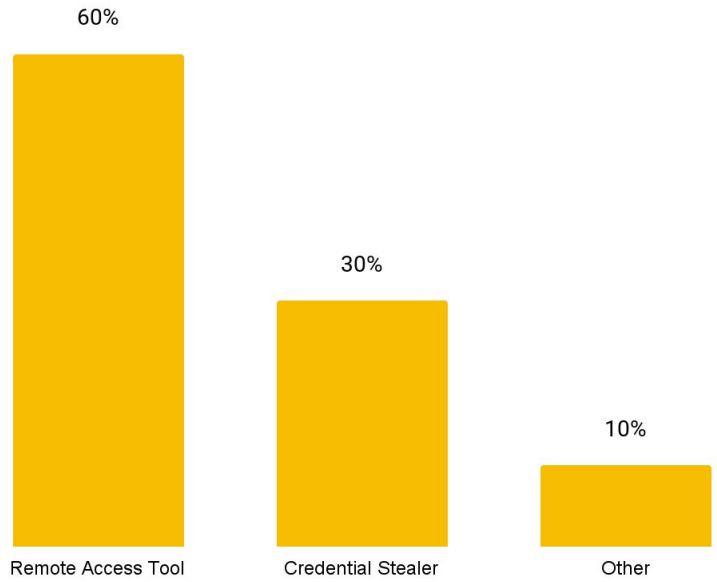
2 - Persistence - Q4

In cases where Persistence was observed, the following Malware/Tools/Techniques were most commonly leveraged

Name	Description
AnyDesk	Remote access tool (RAT)
Netscan	Network discovery tool
Ngrok	Remote access tool (RAT)
Atera	Remote access tool (RAT)
Advanced Port Scanner	Network discovery tool

3 - Escalation - Q4

In cases where Escalation was observed:

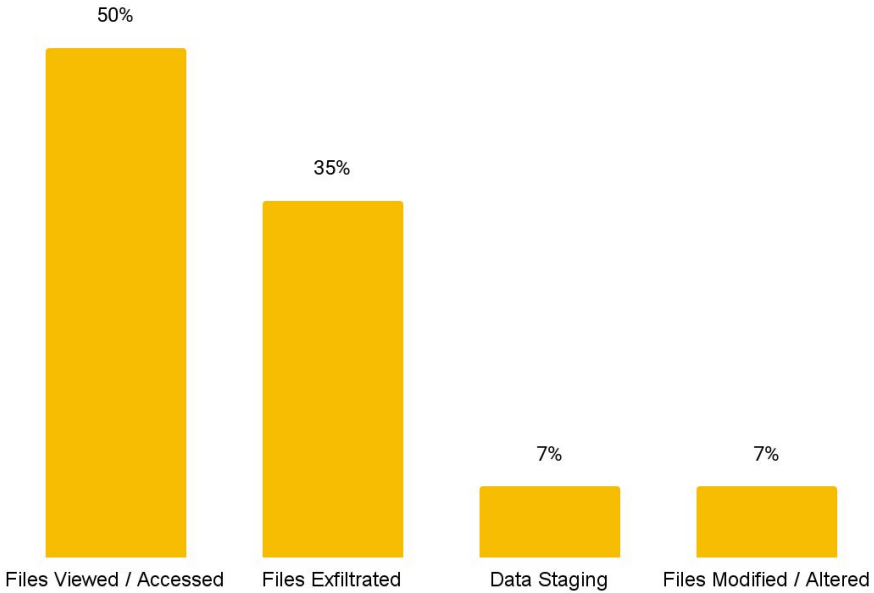


Observed Tools/Techniques used for Escalation:

Name	Description
Mimikatz	Credential stealer
Powershell	Command line
Advanced IP Scanner	Network discovery tool
Psexesvc	Remote management tool

4 - Data at Risk - Q4

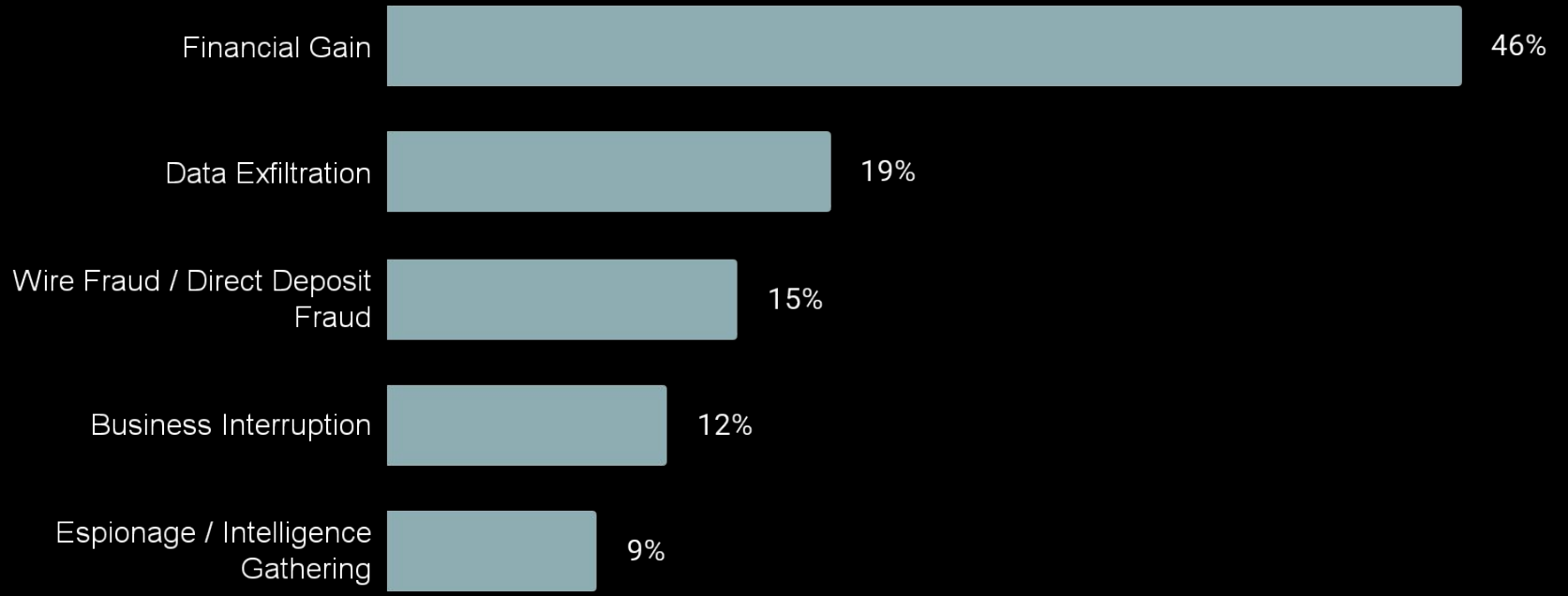
In cases where Data at Risk was observed:



Observed Tools/Techniques for Data at Risk:

Name	Description
WinRar	Software for compressing and archiving files
WinSCP	Open-source SFTP client
Rclone	Command-line program for file management
ezupload[.]io	File transfer service
BitLocker	Data encryption service
FileZilla	File transfer service

5 - Threat Actor End Goal - Q4



About Cybereason, A LevelBlue Company

One team. One mission.

LevelBlue
(AT&T Cybersecurity / AlienVault)

+

SF STROZ FRIEDBERG
A LevelBlue Company

+

Trustwave®
A LevelBlue Company

+

cybereason®
A LevelBlue Company

LevelBlue

Powered by 300+ trusted DFIR experts and frontline threat intelligence, we help organizations anticipate, respond, recover, and harden against threats.

Proven expertise and frontline threat intel

300+
Trusted DFIR experts

2,500+
Cybersecurity professionals

8-9M
Endpoints under management

50+
Approved by cyber insurance carriers and brokers

9000+
Incidents investigated and

1K+
Tabletop exercises orchestrated

Bleeding edge threat intel and vulnerability research via SpiderLabs

200K+
hours of pen tests delivered annually

30K+
vulnerabilities discovered per year

1K+
threat hunts conducted annually

LevelBlue

Anticipate, respond, recover, and harden against threats

Delivering scalable, AI-driven protection across cloud, network, and hybrid environments

Incident Readiness & Response

- IR Plans & Tabletops
- Digital Forensics
- Incident Response
- IP Risk & Litigation Support

Exposure Management

- Pen Testing
- Vulnerability Management
- Scenarios & Simulations
- Threat Intelligence

Cyber Advisory and Transformation

- Strategy, Design and Implementation
- GRC, Assessments and Diagnostics
- Integration and Remediation
- vCISO

Threat Detection, Investigation & Response

- MDR / MXDR / SOC as a Service
- Cyber Threat Hunting
- EDR/XDR/SIEM

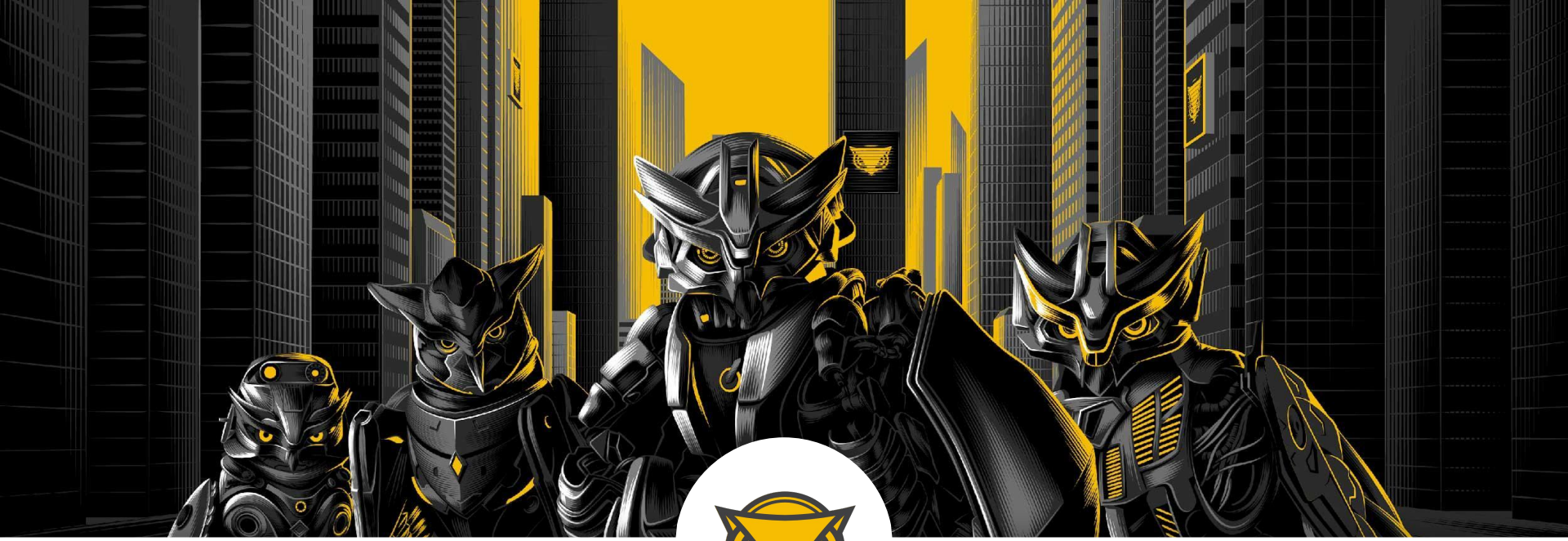
Managed Network Security

- Edge Security
- DDoS Protection
- CDN & SDWAN
- Email Security

Managed Cloud Security

- SASE / SSE
- FWaaS
- ZTNA
- WAAP

LevelBlue



cybereason©

A LevelBlue Company

24x7 expert assistance via response@levelblue.com