cybereason

TTP Briefing:

Q3 2025

cybereason

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.

Q3 Data Overview

Top 3 Impacted Industries

- Financial Services (11%)
- Manufacturing (11%)
- Retail/eCommerce & Hospitality (11%)

Top 3 Threat Incident Types

- Business email Compromise (46%)
- Ransomware (39%)
- Insider Threat - Intentional (7%)

Top 3 Initial Intrusion Vectors

- Phishing/Social Engineering (50%)
- Exploited Vulnerabilities (31%)
- Valid Accounts /Credential Abuse (8%)

cybereason

KEY TAKEAWAYS - Q3

LOLBIN USAGE INCREASES, HINDERS DETECTION

Usage of Living off the Land Binaries (LOLBins) increased in Q3 as threat actors see higher success in evading EDR and Antivirus detection by leveraging native or pre-approved tools.

NEARLY ¾ OF BEC ATTACKS BYPASSED MFA

Though we saw a higher rate of MFA implementation in Q3, attackers bypassed MFA in over 73% of business email compromise (BEC) incidents using modern phishing kits and token interception.

RATE OF VULN. EXPLOITS MORE THAN DOUBLED

Attacks leveraging CVEs as the initial intrusion vector reached 31% in Q3, up from 15% in H1, pressuring defenders to re-evaluate their vulnerability patching programs.

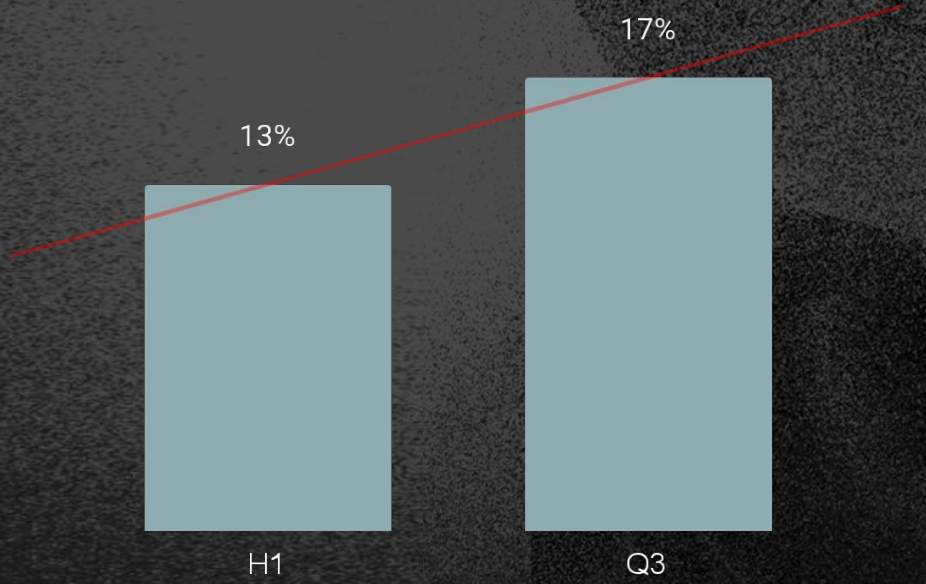
INSIDER THREAT CASES TRIPLED

Incidents involving North North Korean remote worker schemes and disgruntled employees absconding proprietary data rose to 7% in Q3, up from only 2% in H1.

cybereason

LOLBINs USAGE INCREASED TO 17% IN Q3, UP FROM 13% IN H1

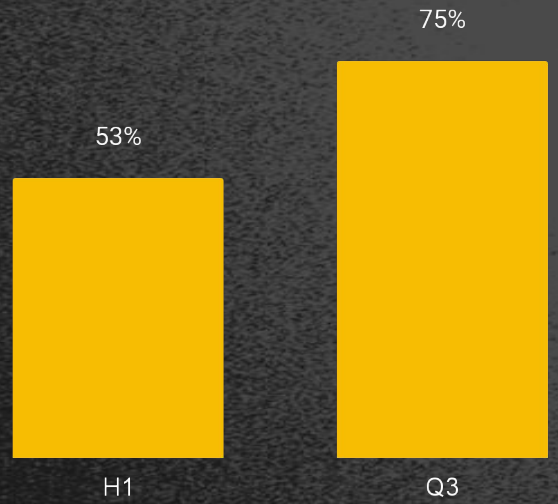
Trusted, built-in system tools let attackers blend in with legitimate activity, evade detection, and carry out attacks without deploying malware.



cybereason

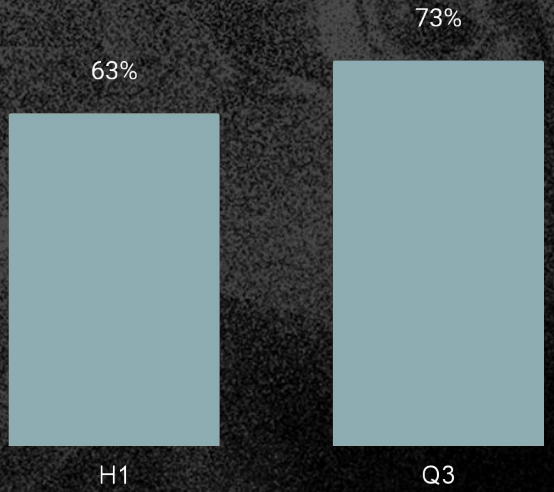
MFA IMPLEMENTATION CONTINUES TO RISE, BUT SO DO BYPASS TECHNIQUES

MFA IMPLEMENTATION



Between H1 and Q3, we saw organizations more regularly implementing MFA, accounting for a 20+ basis points increase.

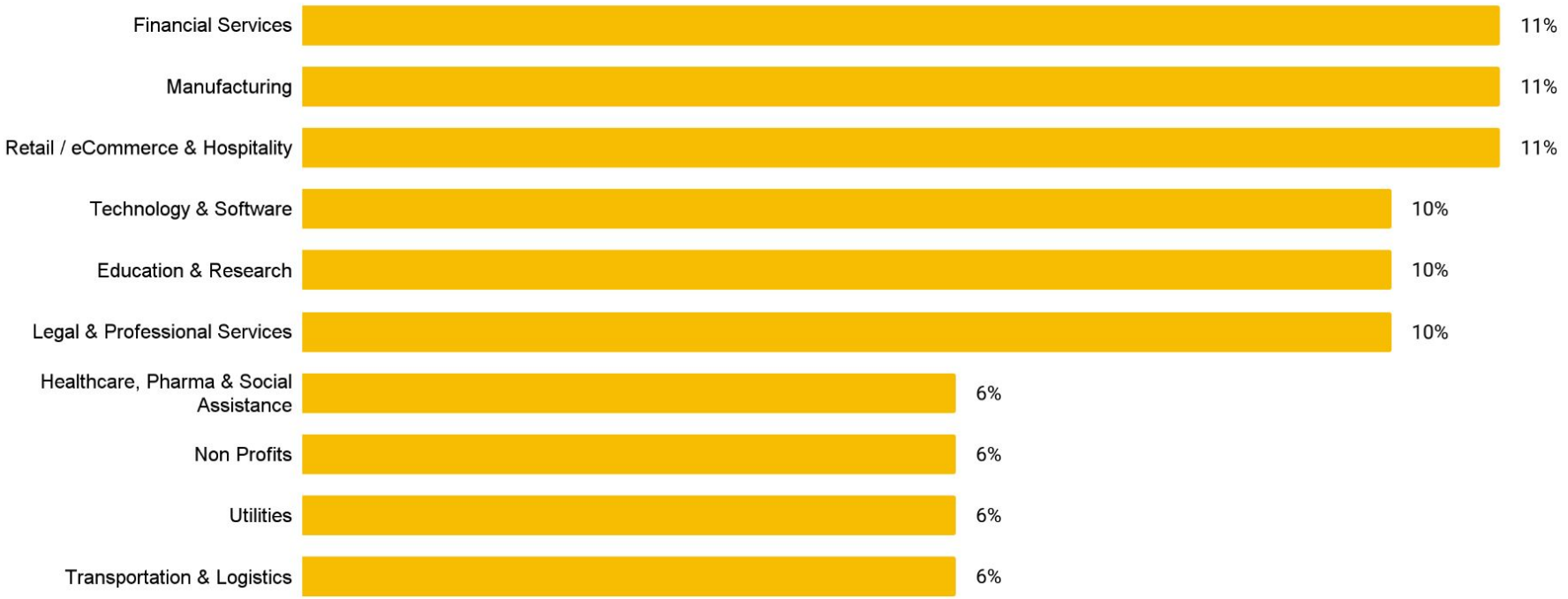
MFA BYPASS



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

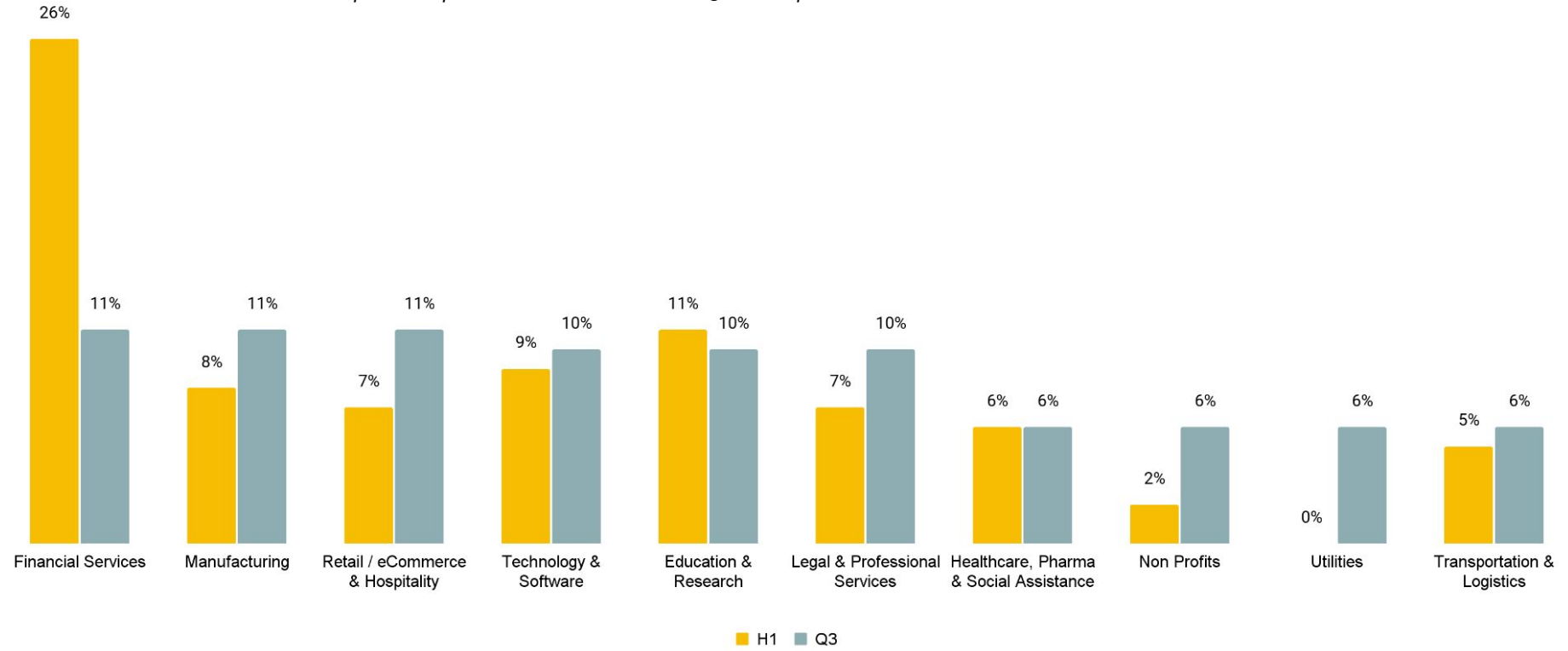
Top 10 Impacted Industries - Q3



cybereason

Impacted Industries Over Time

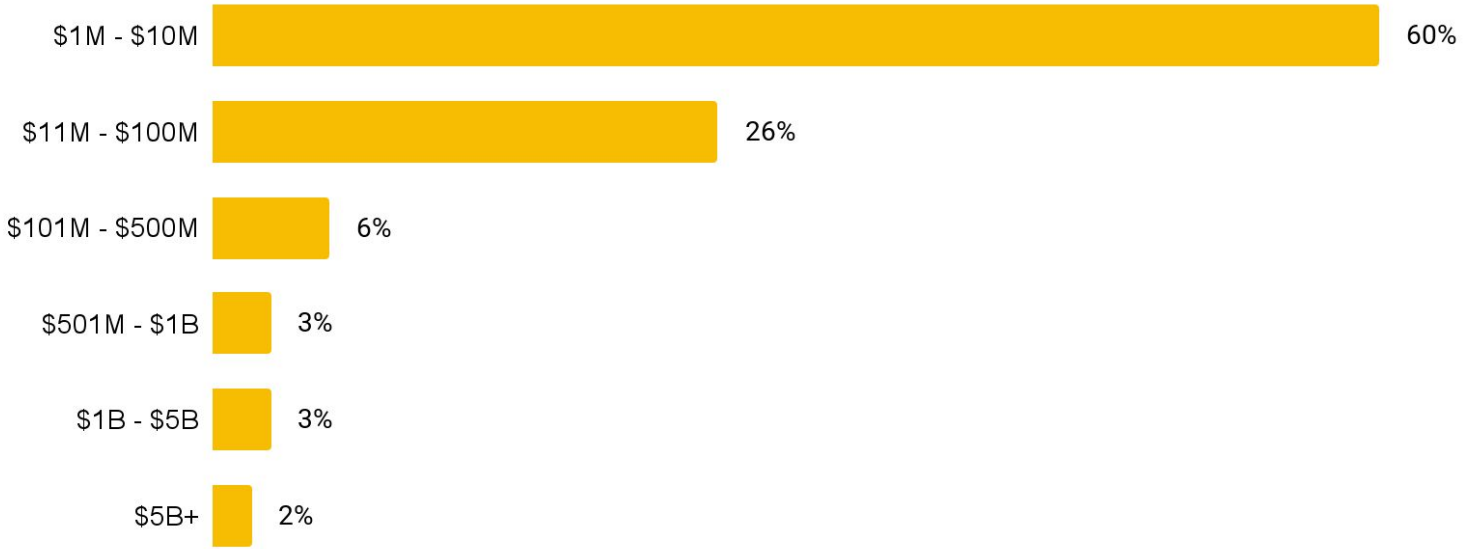
Top 10 impacted industries in Q3 compared to same industries in H1 2025



cybereason

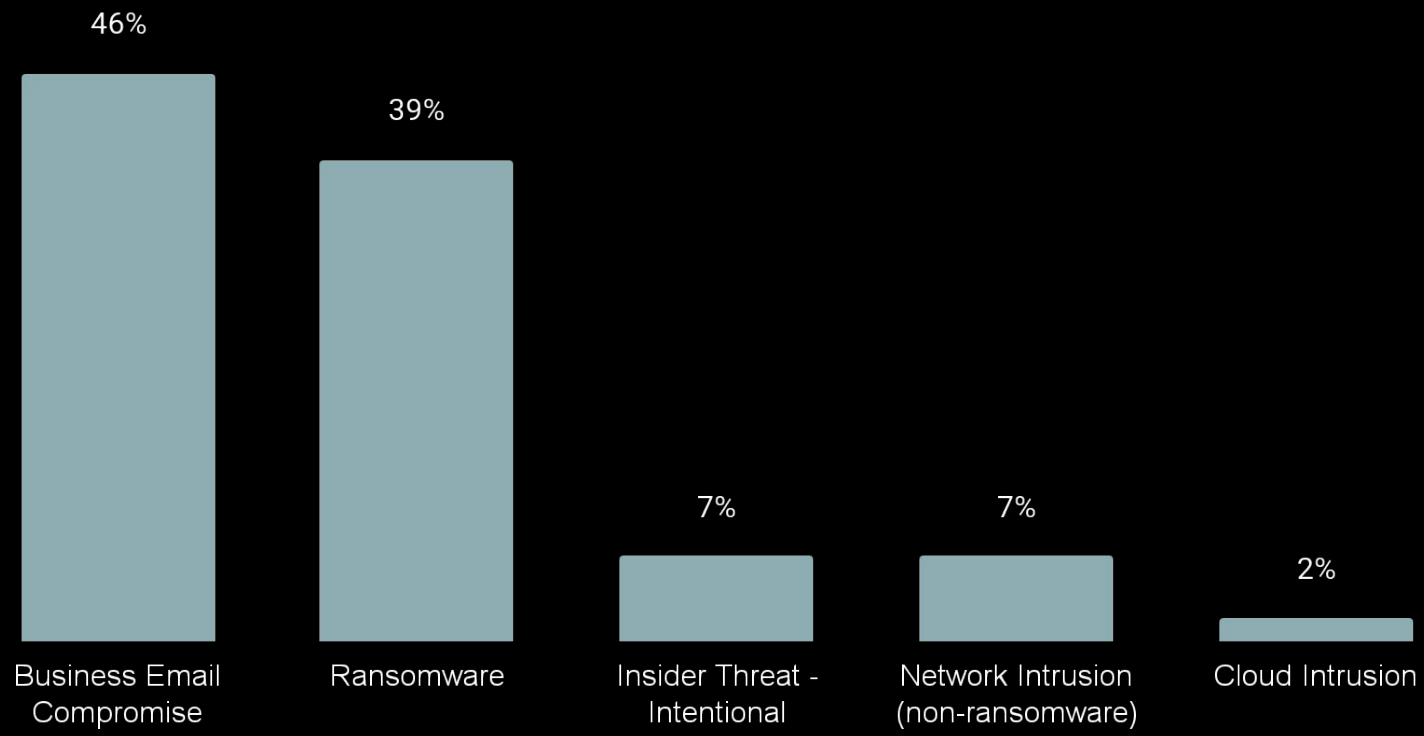
Company Size - Q3

Based on revenue



cybereason

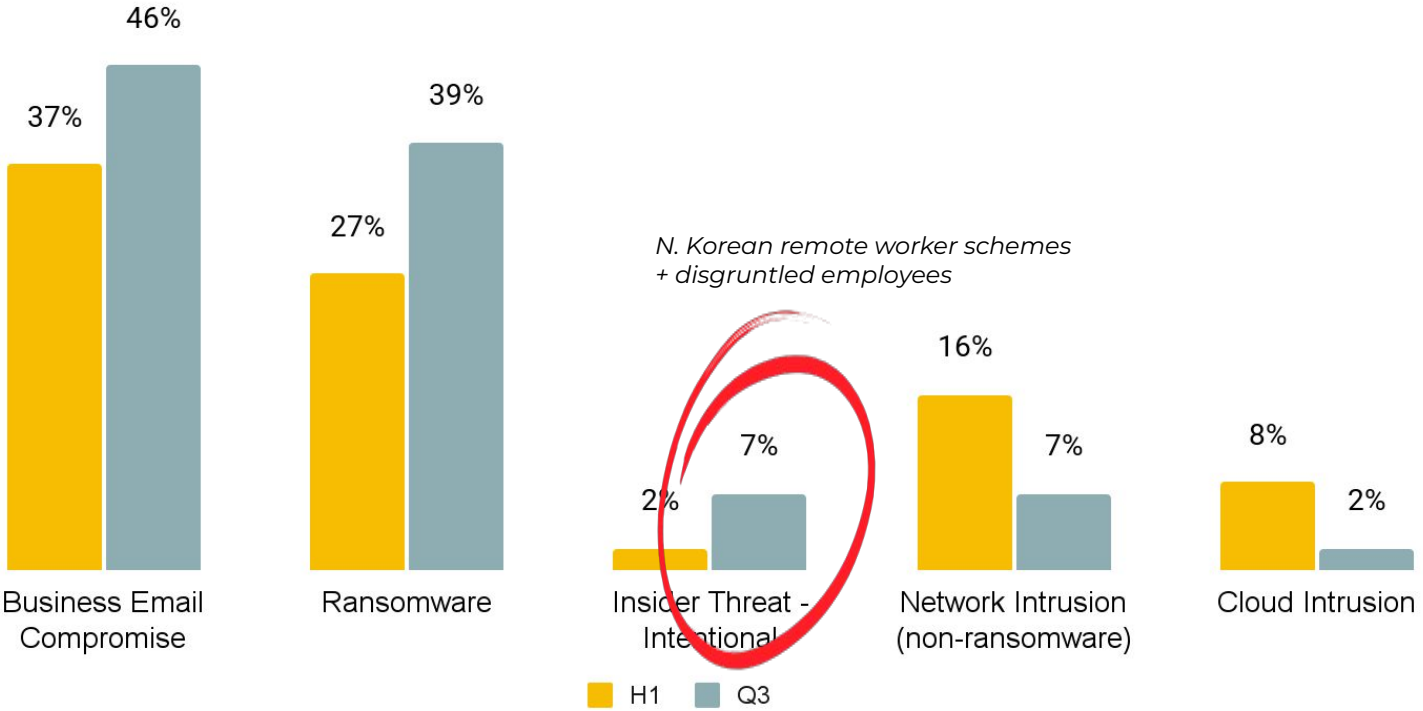
Most Common Incident Types - Q3



cybereason

Common Incident Types Over Time

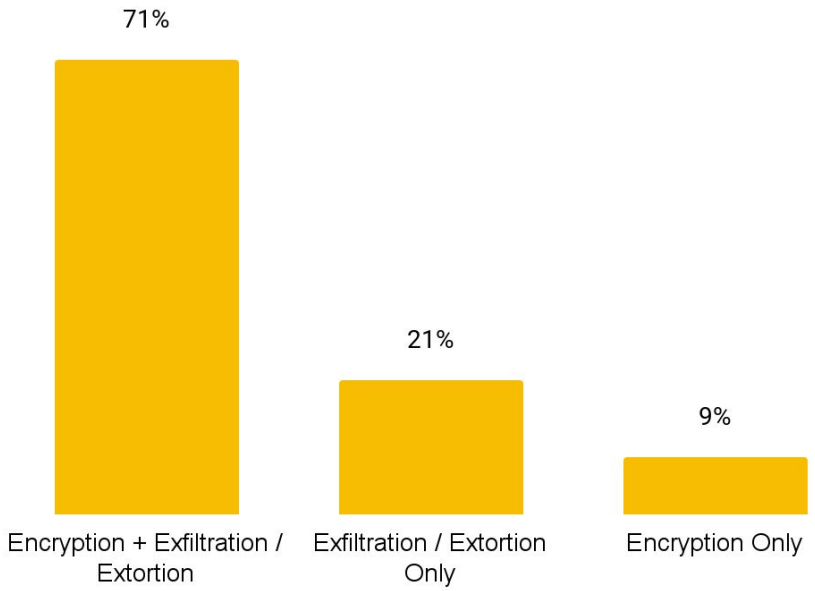
Most common incident types in Q3 compared to same incident types in H1 2025



cybereason

Ransomware Q3

Attack Type Distribution

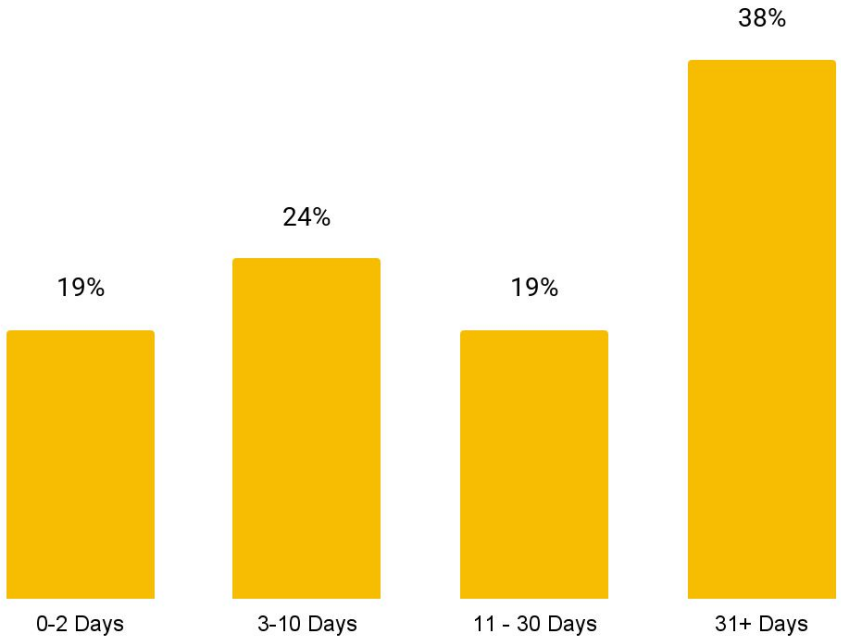


Top Observed Variants

High Activity:	Others:
Akira	Play
Qilin	Ransomhub
Inc	Angels Angels
Medusa	Babuk / Kavva
	Rhysida
	Warlock
	Zlyuk

Dwell Time Q3
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*

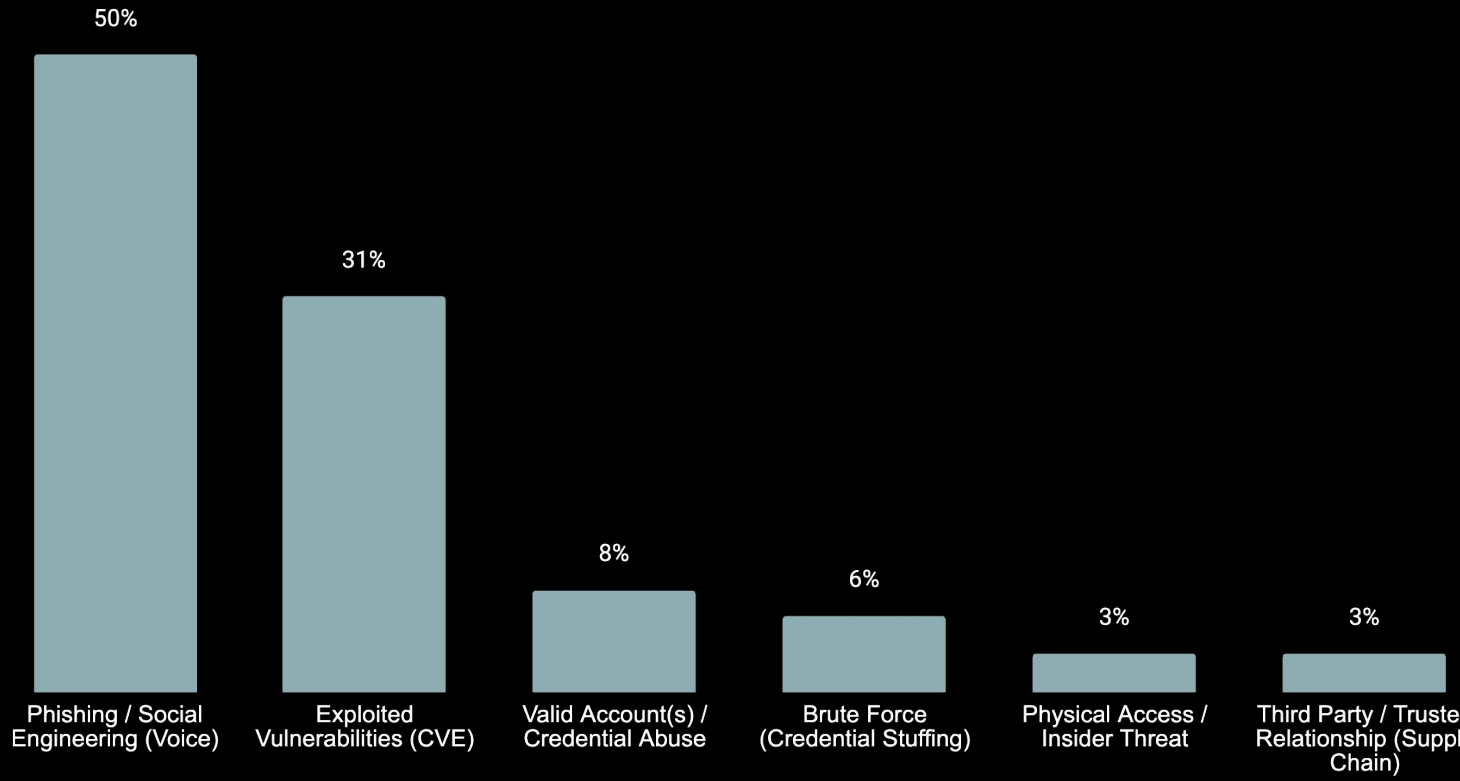
cybereason

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

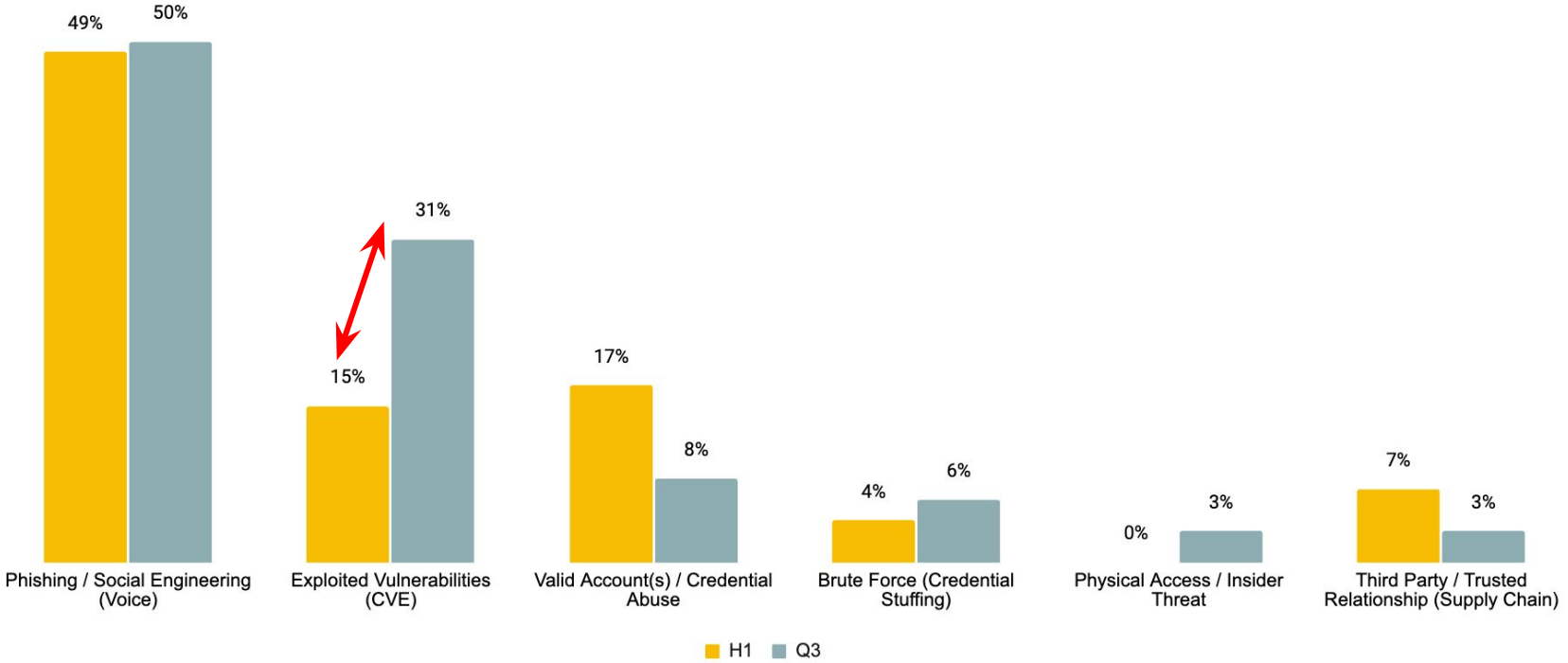
1 - Initial Intrusion Vector - Q3



cybereason

Initial Intrusion Vectors Over Time

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



cybereason

Most Commonly Observed CVEs - Q3

CVE	Impacted Product
CVE-2025-53770	On-Premises Microsoft SharePoint Server
CVE-2025-30406	Gladinet CentreStack
CVE-2025-24477	Fortinet FortiOS
CVE-2024-53704	SonicWall SonicOS SSL-VPN
CVE-2024-40766	SonicWall SonicOS
CVE-2024-23113	Fortinet FortiOS

CVE	Impacted Product
CVE-2024-21762	Fortinet FortiOS
CVE-2023-5970	SonicWall SMA100 SSL-VPN
CVE-2023-44221	SonicWall SonicOS SSL-VPN
CVE-2023-27997	Fortinet FortiOS
CVE-2022-2915	SonicWall SMA100
CVE-2022-1703	SonicWall SMA100 SSL-VPN

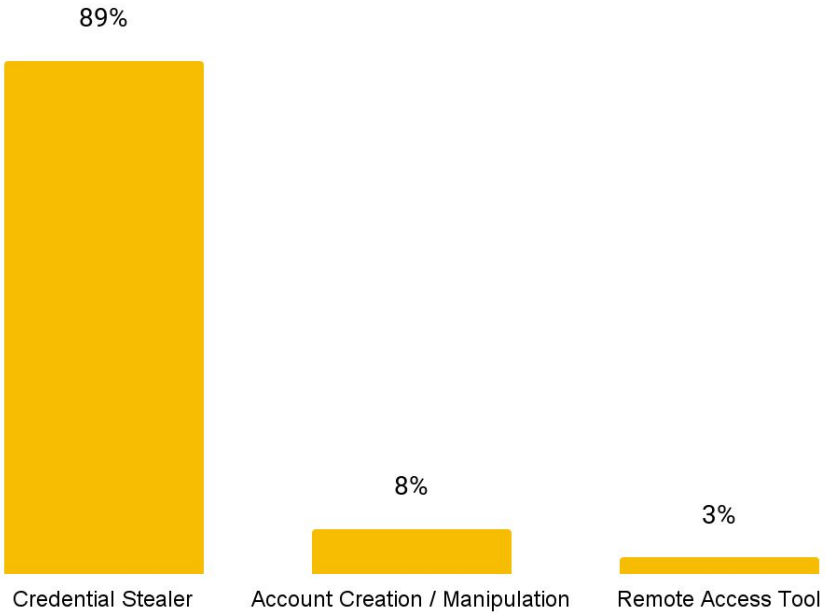
2 - Persistence - Q3

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

Name	Description
AnyDesk	Remote access (desktop) software
Netscan	Network discovery tool
AteraAgent	Remote management and monitoring (RMM) software
LogMeIn	Remote access (desktop) software
SplashTop Remote	Remote management and monitoring (RMM) software
Webshell	Remote access and command script
Pinggy	Remote access tool
OpenSSH	Program that stores private keys for SSH authentication
Metasploit	Penetration testing and exploitation framework
Impacket	Network protocol testing and exploitation framework
Advanced Port Scanner	Network protocol testing and exploitation framework

3 - Escalation - Q3

In cases where Escalation was observed:

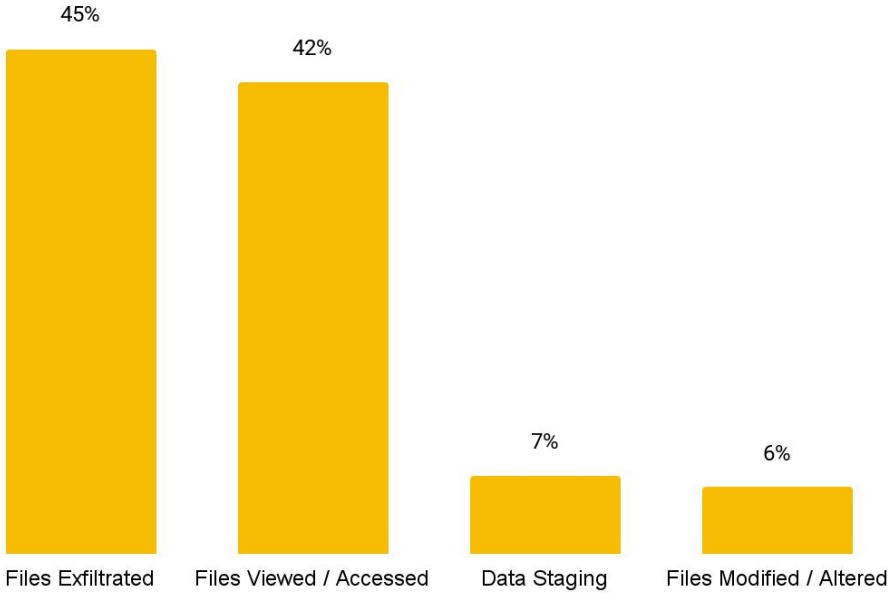


Observed Tools/Techniques used for Escalation:

Name	Description
Mimikatz	Credential stealer
Powershell	Command line
SharpHound	Active directory exploration and exploitation framework
DCSync	Credential stealer

4 - Data at Risk - Q3

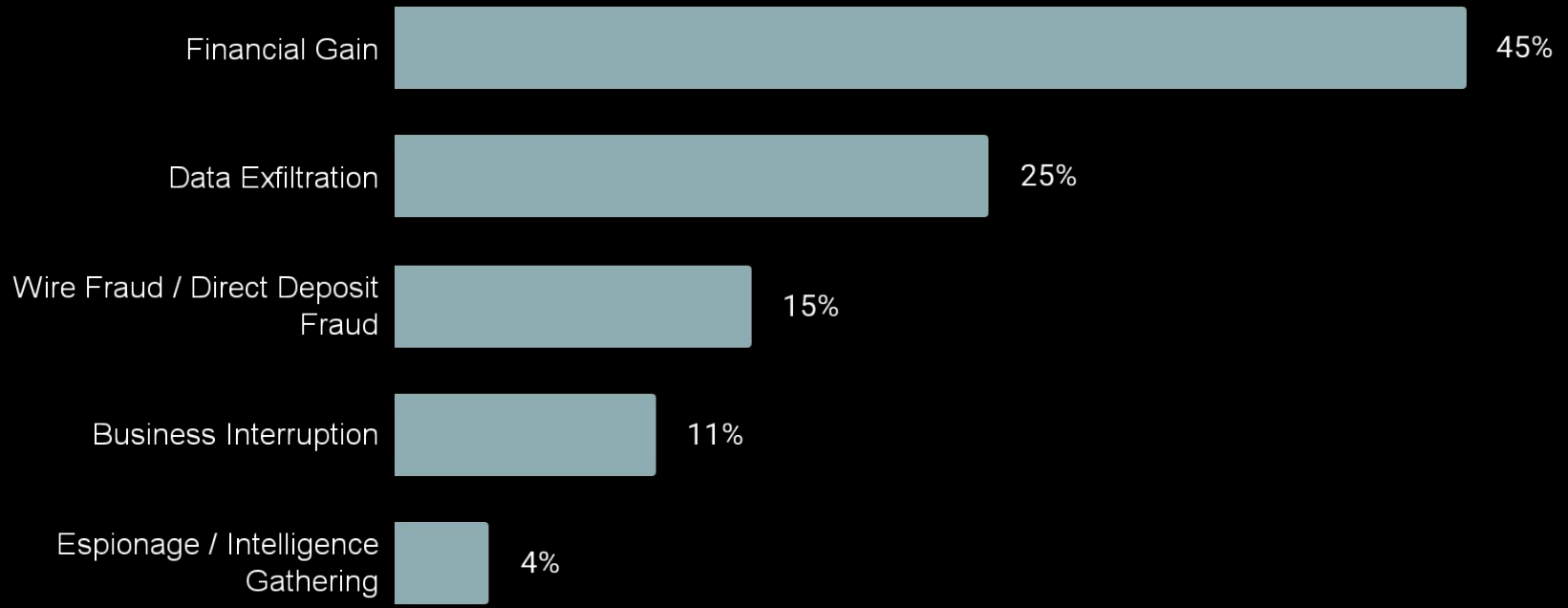
In cases where Data at Risk was observed:



Observed Tools/Techniques for Data at Risk:

Name	Description
WinRar	Software for compressing and archiving files
WinSCP	Open-source SFTP client
Anydesk	Remote access (desktop) software
Rclone	Command-line program for file management
ezupload[.]io	File transfer service

5 - Threat Actor End Goal - Q3



cybereason

About Cybereason

cybereason

TRUSTED INCIDENT RESPONSE TEAM

FRONTLINE EXPERTISE TO ELEVATE YOUR CYBER PREPAREDNESS AND RESILIENCE

BATTLE-TESTED EXPERTISE

7000+
Incident response investigations

200K+
Hours of offensive security engagements

~500
Tabletop exercises orchestrated

Relationships with 100s of law firms and insurance carriers

HOLISTIC EXPOSURE MANAGEMENT

300+
experts versed in infrastructure, applications, systems, and endpoints including OT/IoT and emerging tech

60+ elite DFIR investigators
with eDiscovery, managed review, breach notification and expert witness expertise

ELITE THREAT INTEL & SECURITY RESEARCH

30K+ vulnerabilities
discovered annually

6M+ endpoints
under management

MXDR platform
able to ingest 100s of cloud, SaaS, EDR telemetry

cybereason

PREPAREDNESS & RESILIENCE SOLUTIONS

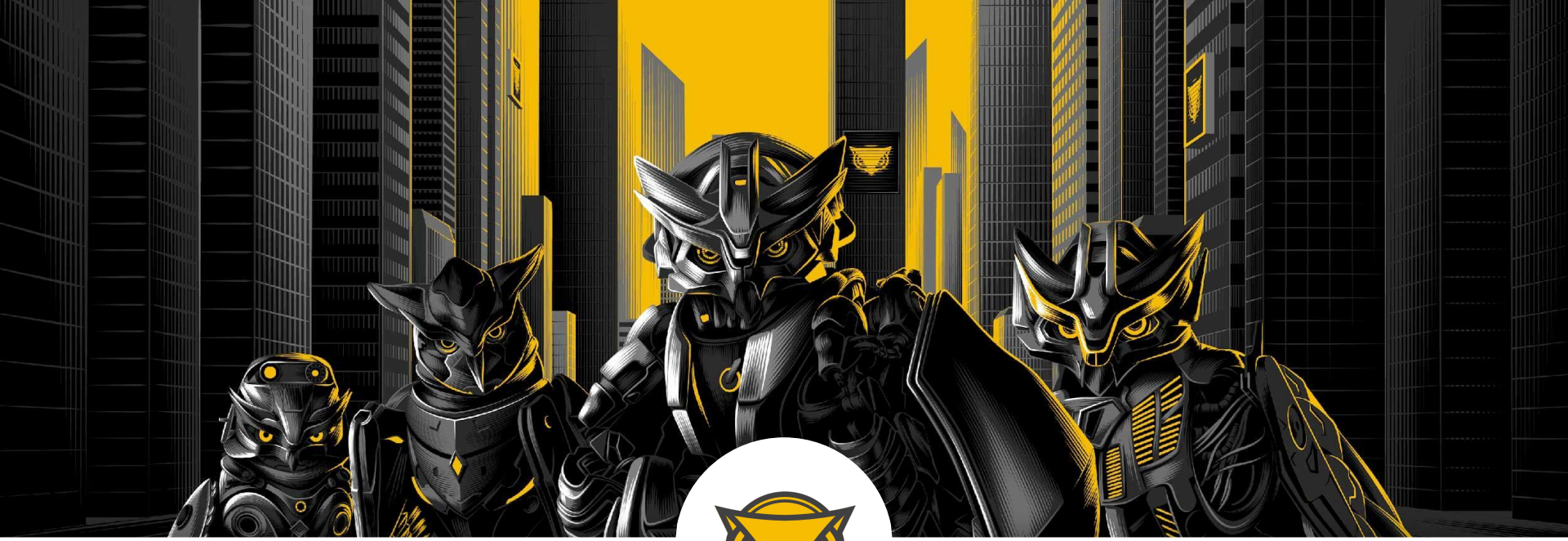
50+ SERVICES TO HANDLE THE ENTIRE LIFECYCLE OF A CYBER INCIDENT

- Offensive Security
- Assessments & Advisory
- Governance, Risk & Compliance
- Cyber Due Diligence
- Managed XDR

- Incident Response
- Tabletop Exercises
- eDiscovery
- Expert Witness
- Breach Notification

- Post-incident Remediation
- Data recovery
- System Re-imaging
- Business Continuity
- Technology Implementation

RESILIENCE RETAINER



cybereason

24x7 expert assistance via response@cybereason.com