An integrated Europe
An integrated MDR
…working better together

Benjamin Burgher-Fuller

Global Sales Engineering Lead - ESET HQ

MADE IN EU

ESET®

Digital Security
Progress. Protected.

How is MDR defined?

"Managed Detection and Response (MDR) is a service that provides customers with remotely delivered security operations centre (SOC) functions, enabling rapid detection, analysis, investigation, and response to threats"

Gartner

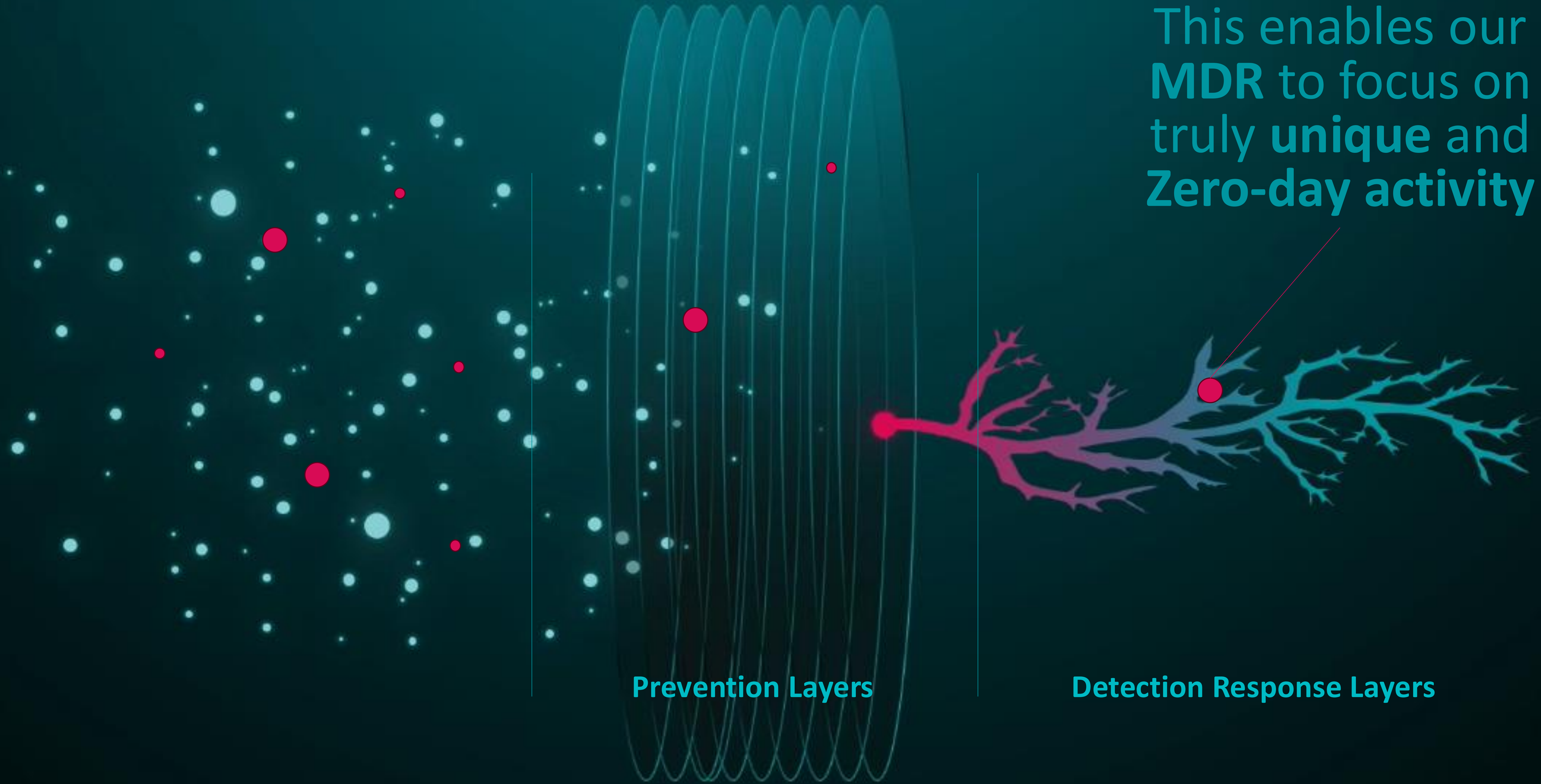
How do we define?

ESET MDR

ESET PROTECT

	ESET PROTECT MDR	ESET PROTECT ELITE	ESET PROTECT ENTERPRISE	ESET PROTECT COMPLETE	ESET PROTECT ADVANCED	ESET PROTECT ENTRY
MDR	✓					
XDR	✓	✓	✓			
MODERN ENDPOINT PROTECTION	✓	✓	✓	✓	✓	✓
MANAGEMENT CONSOLE	✓	✓	✓	✓	✓	✓
MOBILE THREAT DEFENSE	✓	✓	✓	✓	✓	
ADVANCED THREAT DEFENSE	✓	✓	✓	✓	✓	
FULL DISK ENCRYPTION	✓	✓	✓	✓	✓	
EMAIL AND CLOUD OFFICE PROTECTION	✓	✓		✓		
VULNERABILITY & PATCH MANAGEMENT	✓	✓		✓		
MULTI-FACTOR AUTHENTICATION	✓	✓				
PREMIUM SUPPORT	✓					
AI ADVISOR						
CYBERSECURITY AWARENESS TRAINING						
THREAT INTELLIGENCE FEEDS						

This enables our **MDR** to focus on truly **unique** and **Zero-day activity**

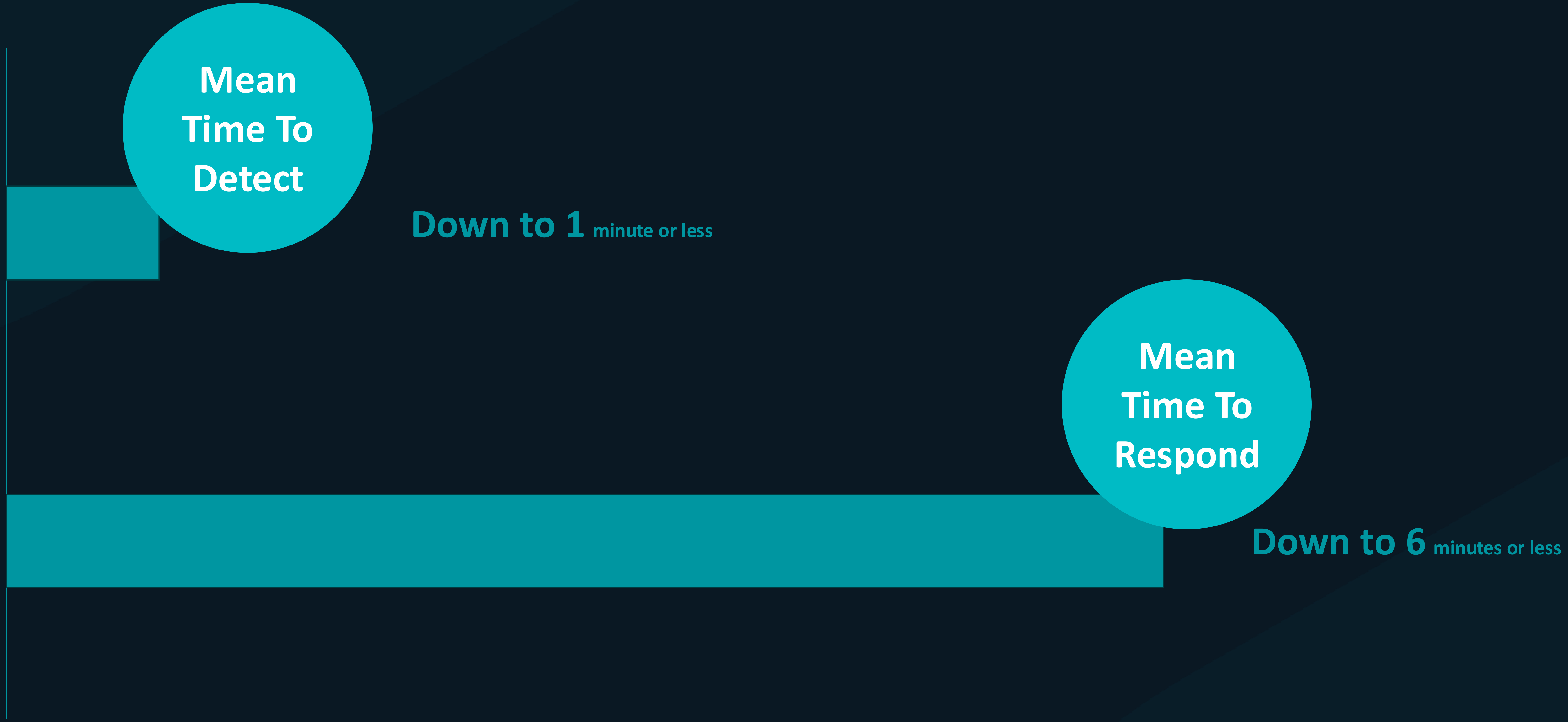


An attacker will spend 204 days In your network unnoticed before they attack

Source: 2023 IBM report

76%+ Of all ransomware infections occur outside working hours. With 49% taking place during the night times on weekdays and 27% over the weekend

Time to detect and respond 2025

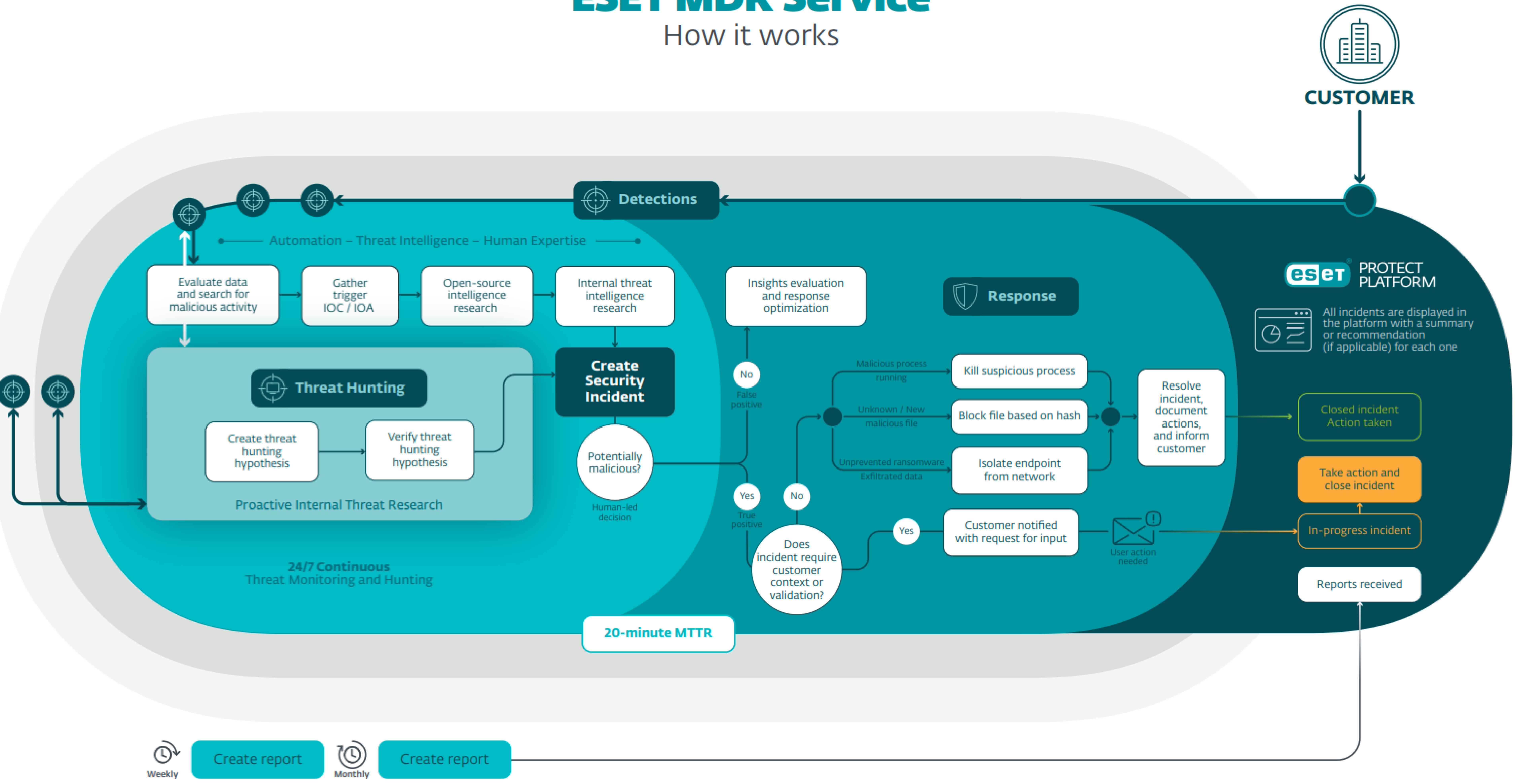


Down to 1 minute or less

Down to 6 minutes or less

ESET MDR Service

How it works



CUSTOMER

Detections

Automation – Threat Intelligence – Human Expertise

Evaluate data and search for malicious activity

Gather trigger IOC / IOA

Open-source intelligence research

Internal threat intelligence research

Create Security Incident

Threat Hunting

Create threat hunting hypothesis

Verify threat hunting hypothesis

Proactive Internal Threat Research

Potentially malicious?

Human-led decision

No

False positive

Yes

True positive

Insights evaluation and response optimization

24/7 Continuous Threat Monitoring and Hunting

20-minute MTTR

Does incident require customer context or validation?

No

Yes

Response

Malicious process running

Kill suspicious process

Unknown / New malicious file

Block file based on hash

Unprevented ransomware Exfiltrated data

Isolate endpoint from network

Resolve incident, document actions, and inform customer

Customer notified with request for input

User action needed

eset PROTECT PLATFORM

All incidents are displayed in the platform with a summary or recommendation (if applicable) for each one

Closed incident Action taken

Take action and close incident

In-progress incident

Reports received

Weekly

Create report

Monthly

Create report

+15%

Reported attacks

5,100

-35%

Payments

$813 million

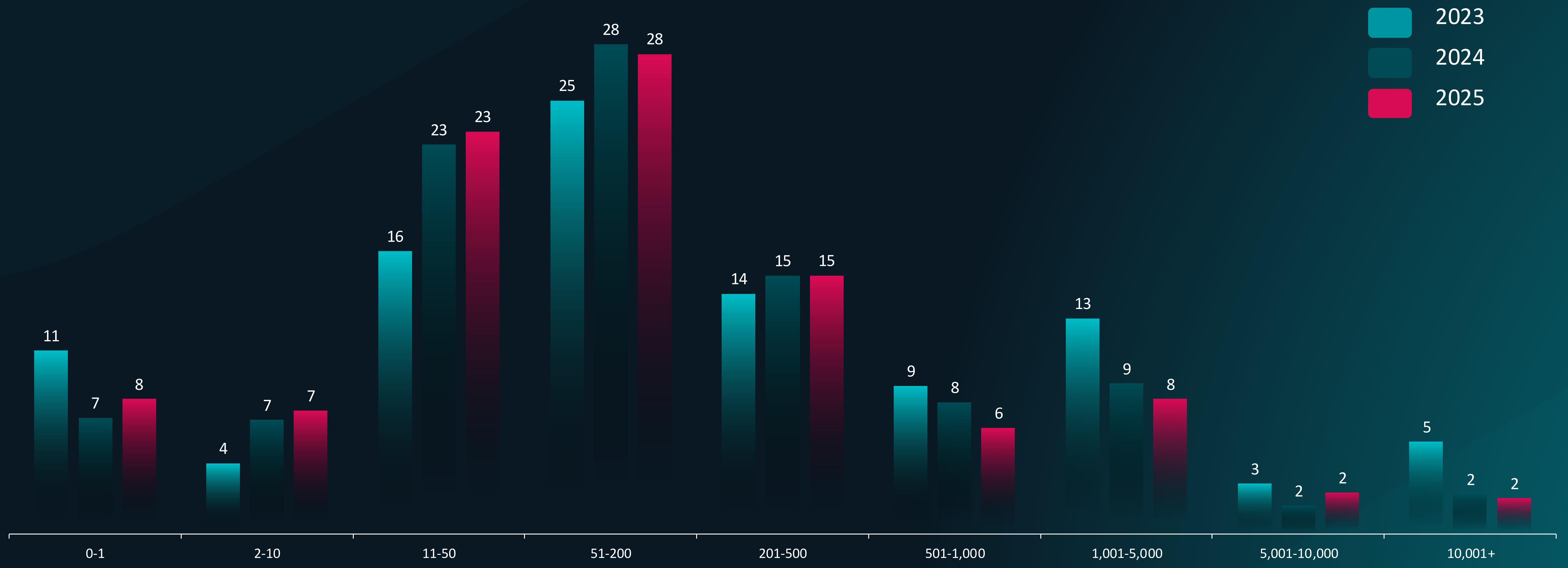
+43%

Gangs

96

Source: Chainalysis, ecrime.ch

Distribution of victims by size



Source: ecrime.ch

EDR killers

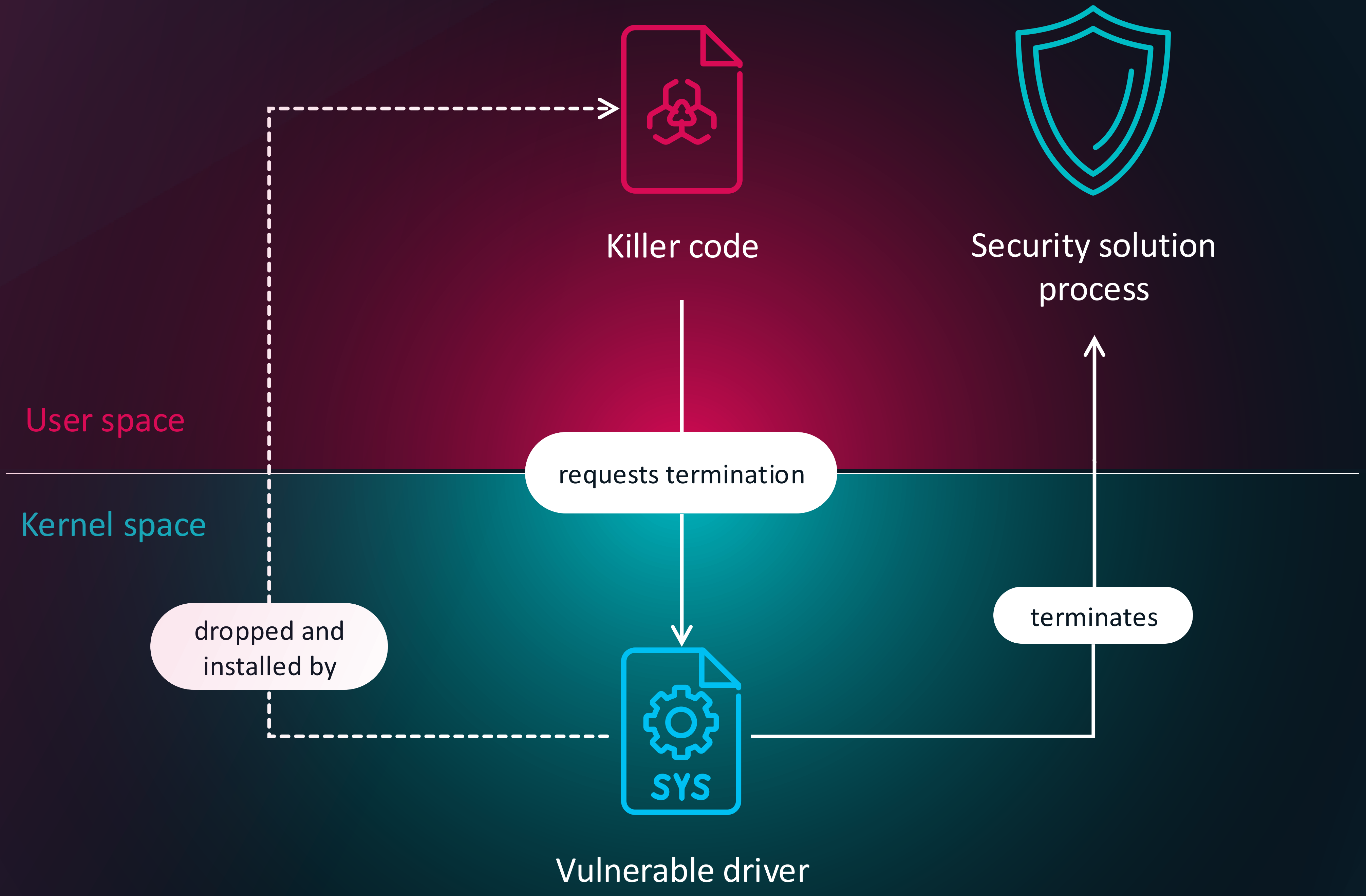
Growing variety

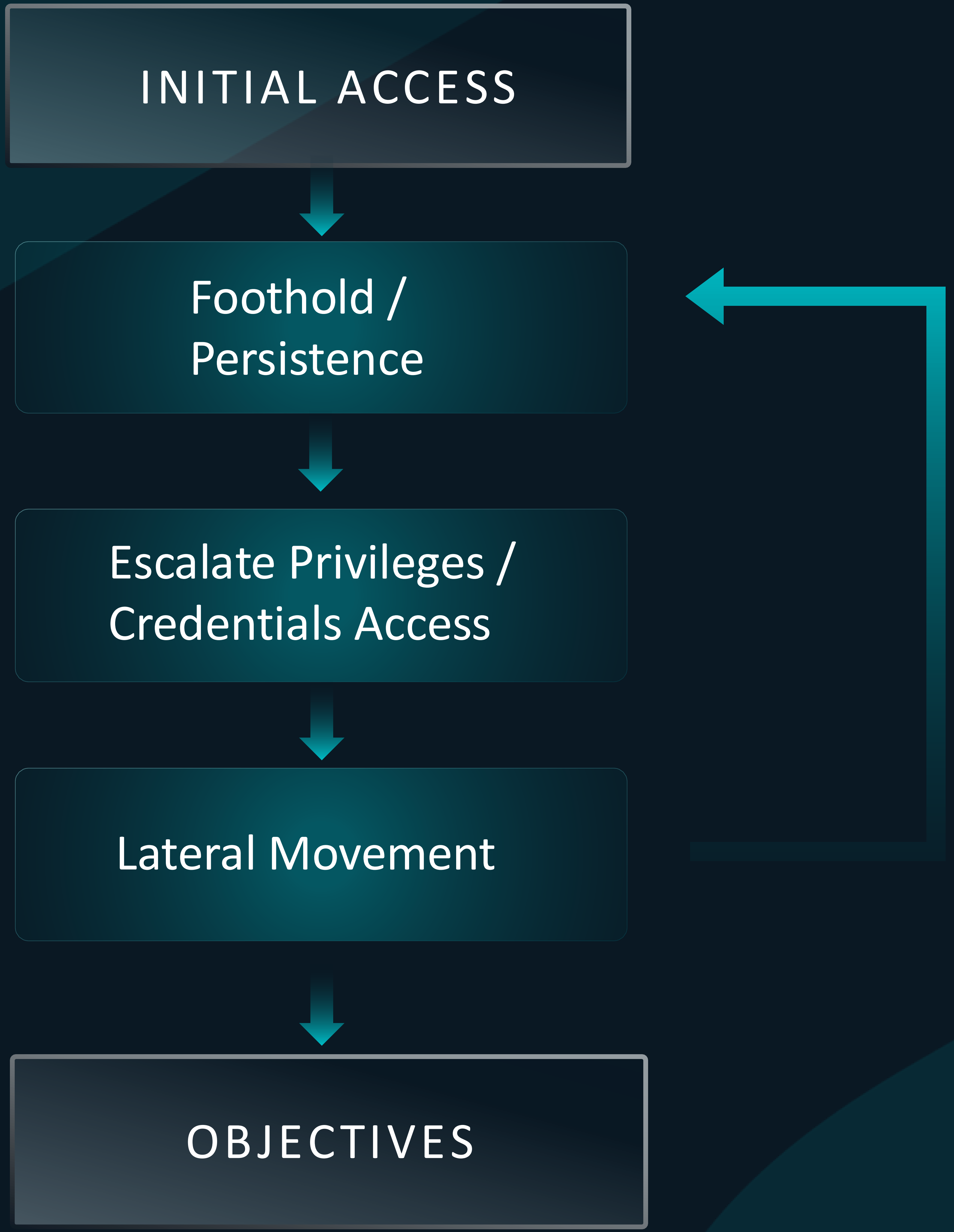
RMM tools

Legitimate but abused

Data stealing

No encryption


Killer code
Security solution process
User space
requests termination
Kernel space
dropped and installed by
terminates
SYS
Vulnerable driver



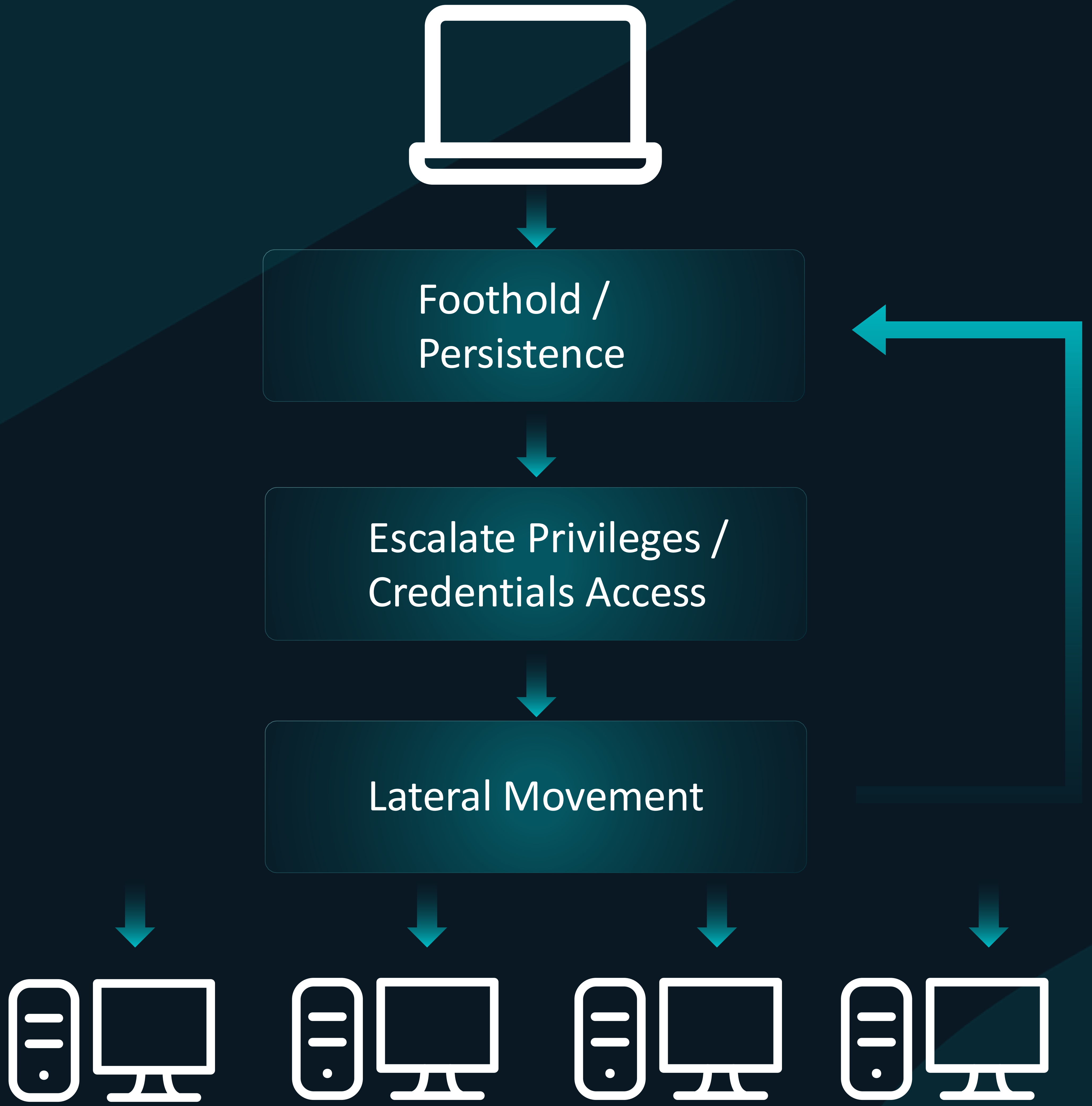
INITIAL ACCESS

Foothold / Persistence

Escalate Privileges / Credentials Access

Lateral Movement

OBJECTIVES

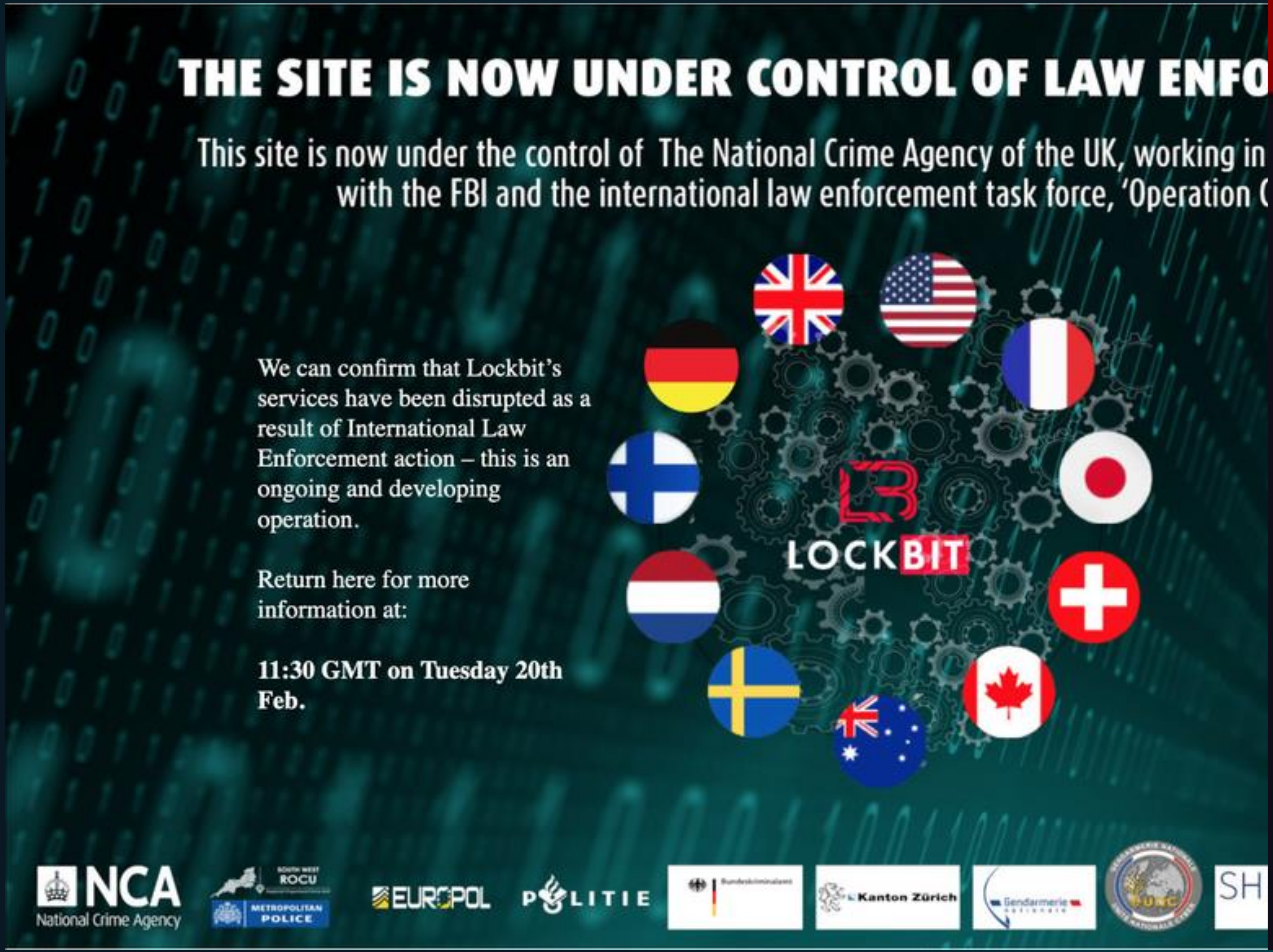


Foothold / Persistence

Escalate Privileges / Credentials Access

Lateral Movement

Ransomware takedowns



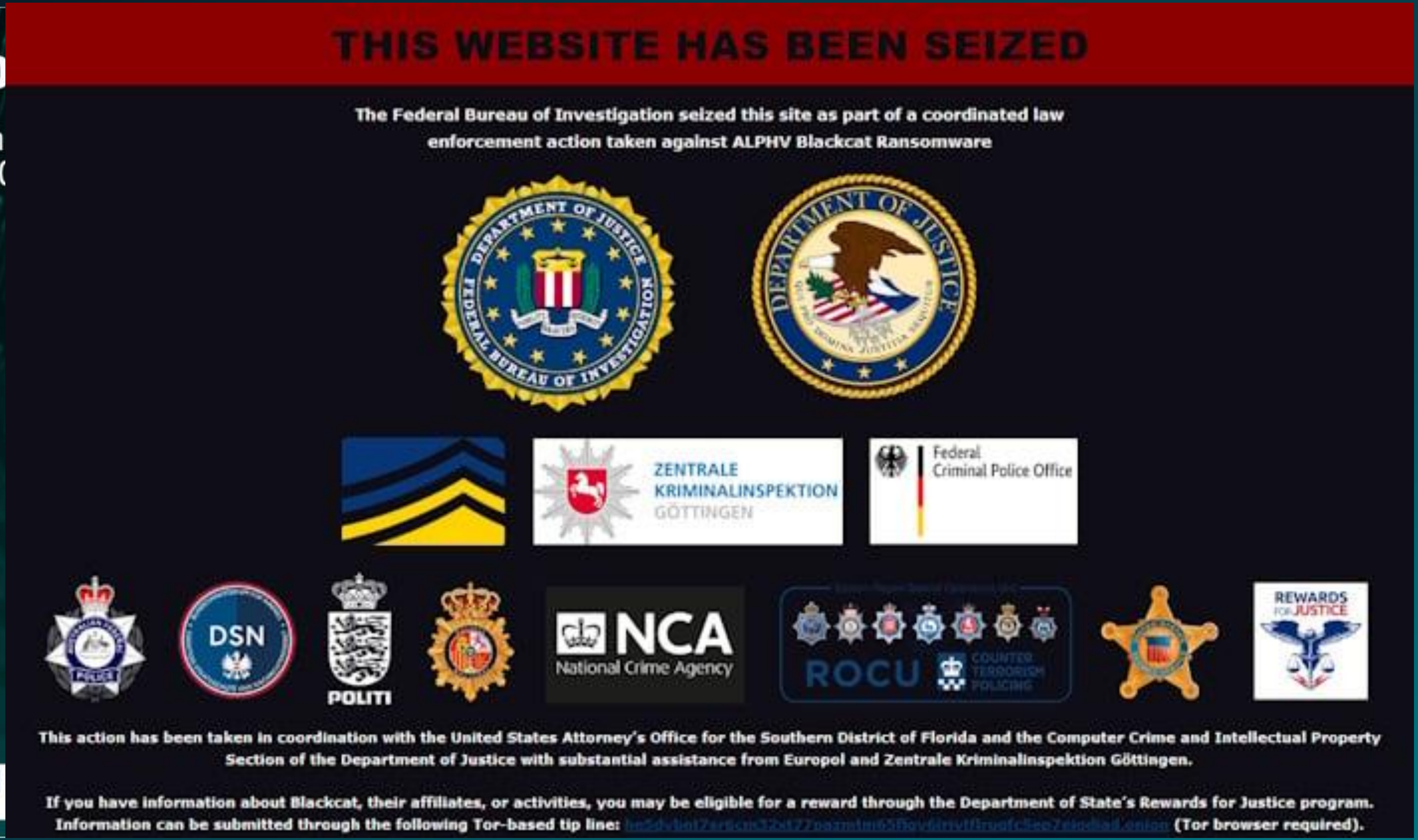
THE SITE IS NOW UNDER CONTROL OF LAW ENFO

This site is now under the control of The National Crime Agency of the UK, working in
with the FBI and the international law enforcement task force, 'Operation C

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.



THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

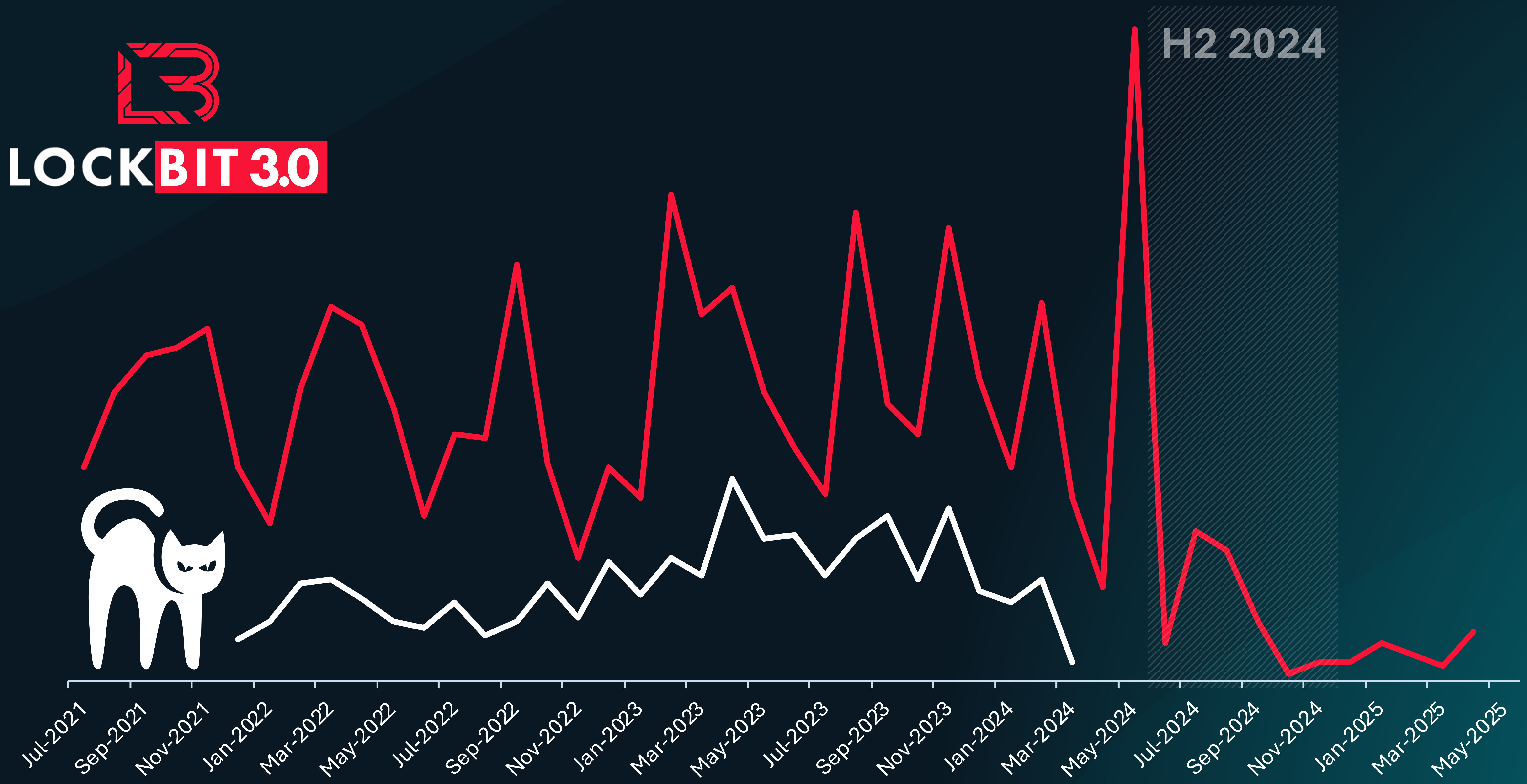
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
ZENTRALE KRIMINALINSPEKTION GÖTTINGEN
Federal Criminal Police Office
DSN
POLITI
NCA
National Crime Agency
ROCU
COUNTER TERRORISM POLICING
REWARDS FOR JUSTICE

This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line: [illegible] (Tor browser required).

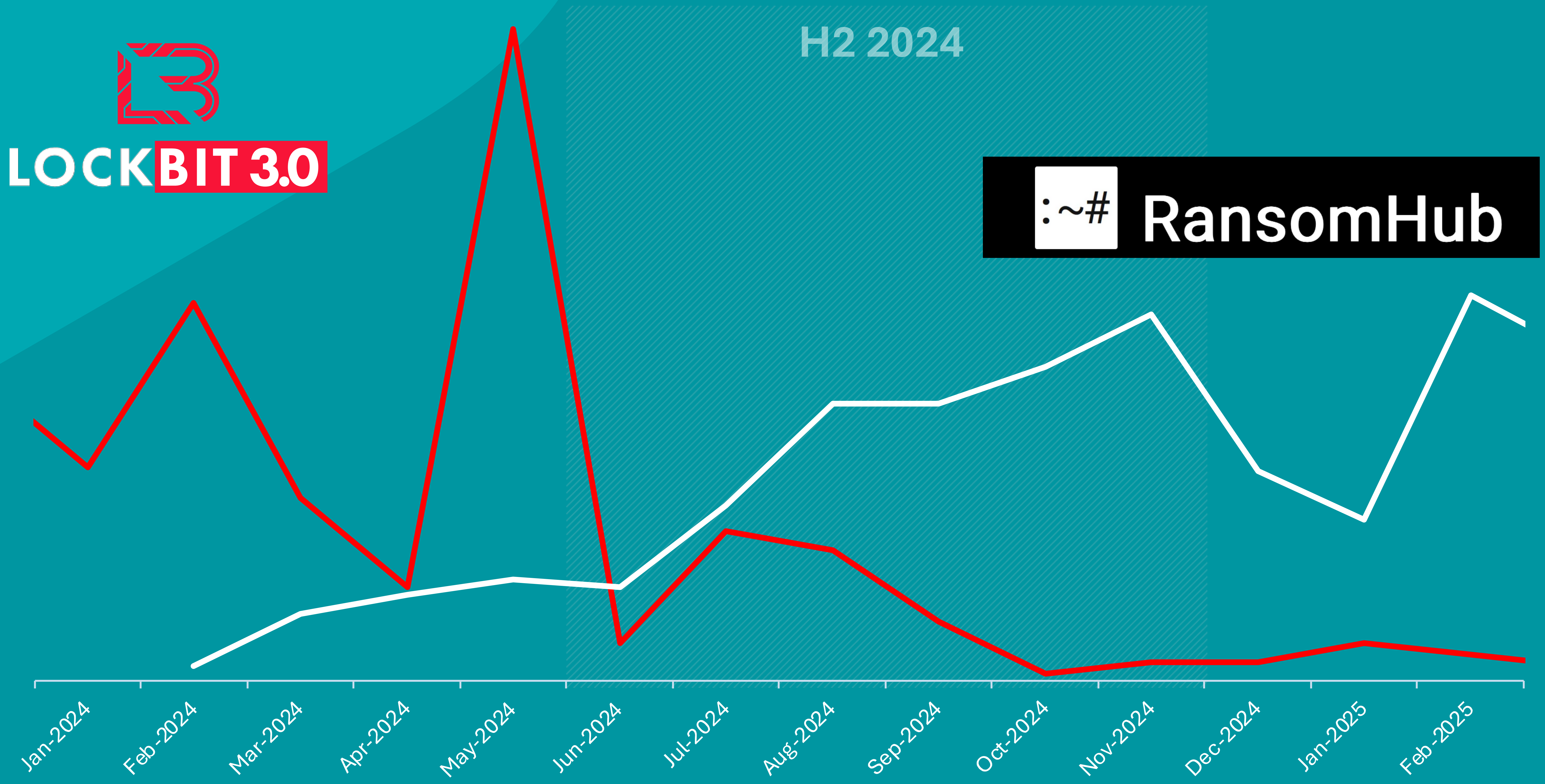
INTERNAL

Victims according to data leak sites

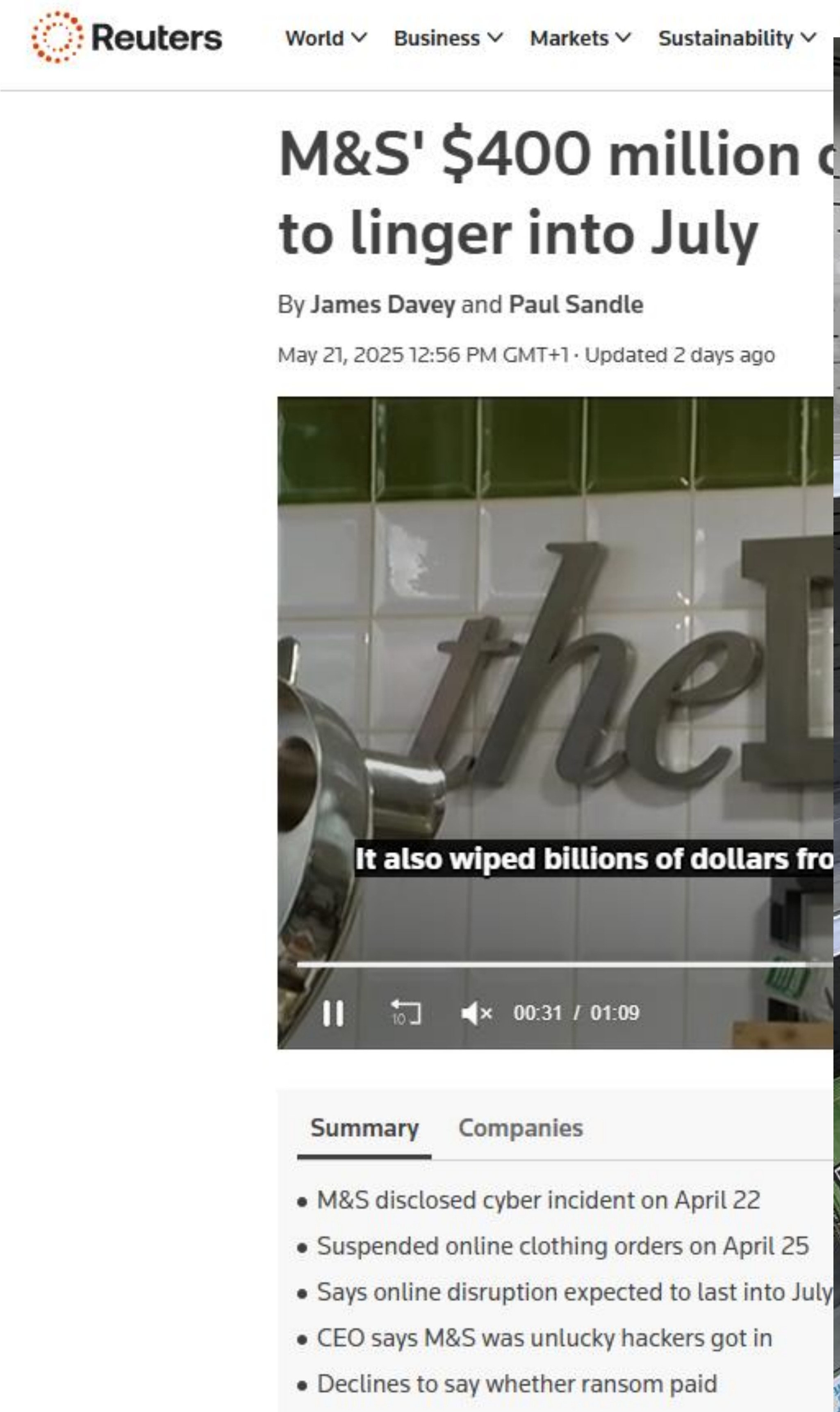


:~# RansomHub

Victims according to data leak sites



DragonForce



Reuters

World Business Markets Sustainability

M&S' $400 million c… to linger into July

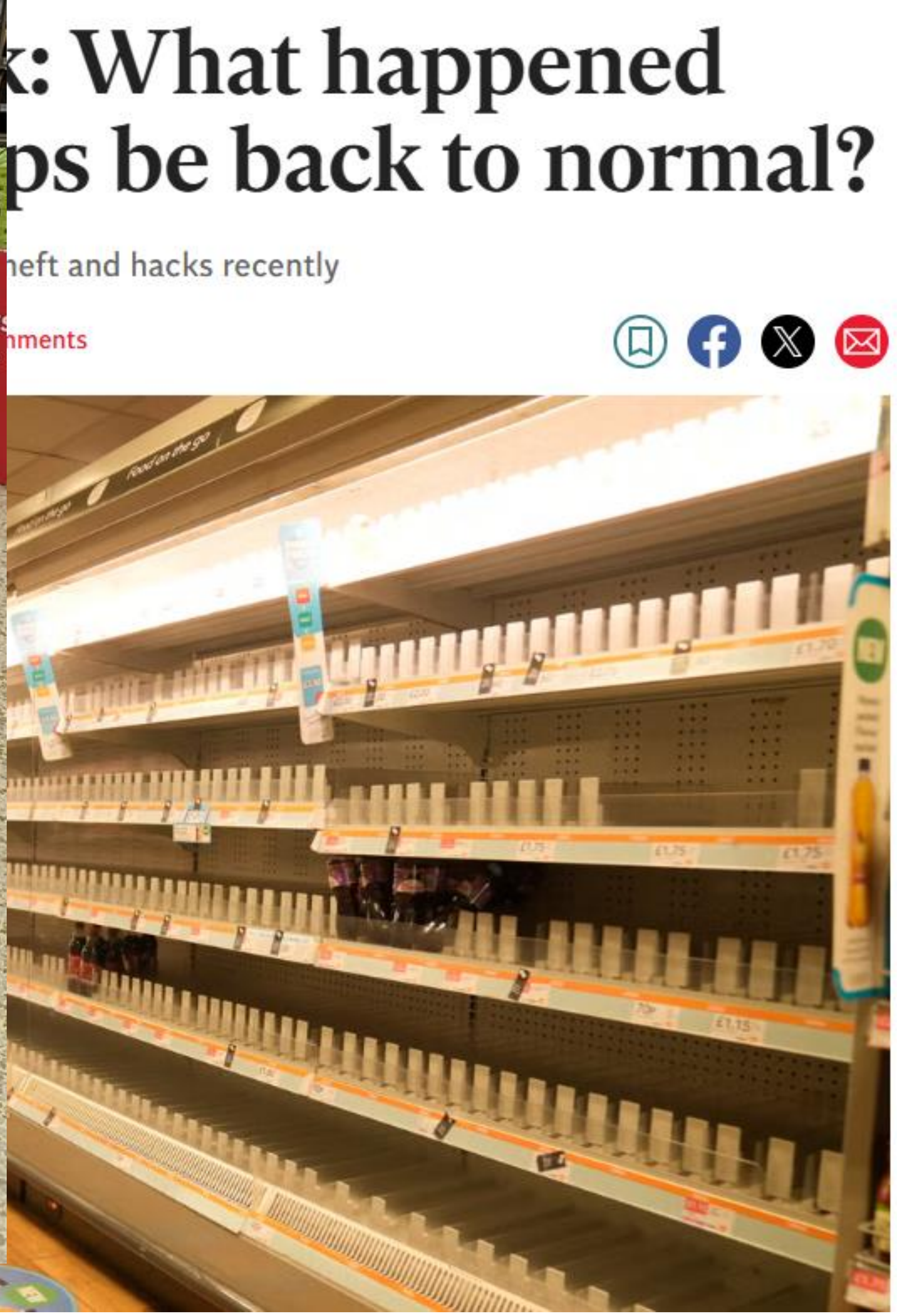
By James Davey and Paul Sandle

May 21, 2025 12:56 PM GMT+1 · Updated 2 days ago

Summary Companies

- M&S disclosed cyber incident on April 22
- Suspended online clothing orders on April 25
- Says online disruption expected to last into July
- CEO says M&S was unlucky hackers got in
- Declines to say whether ransom paid

CUSTOMER INFORMATION
Please bear with us while we fix some technical issues affecting product availability.
£8
PRICES you'll love
DEEP PAN THE VEGGIE ONE

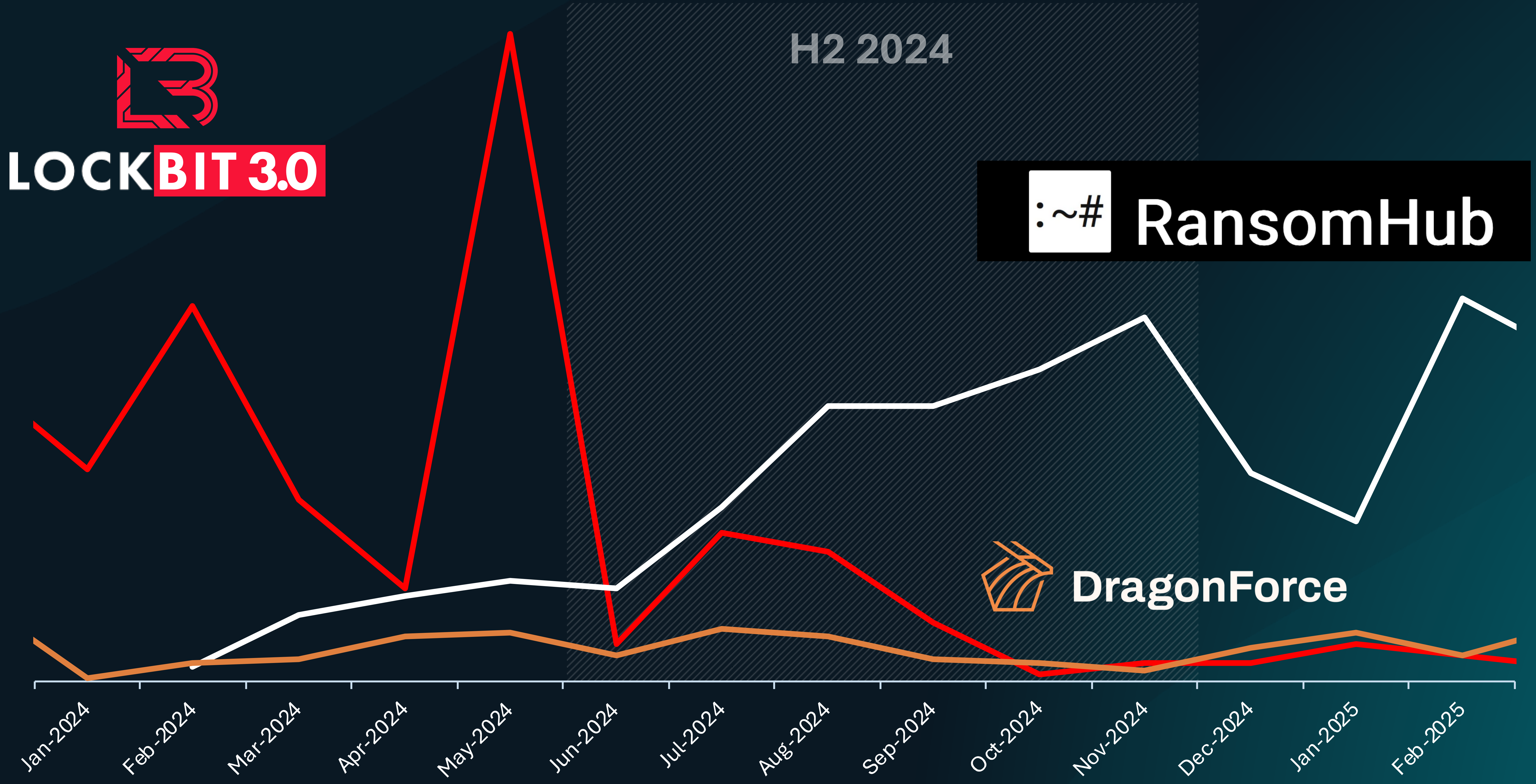


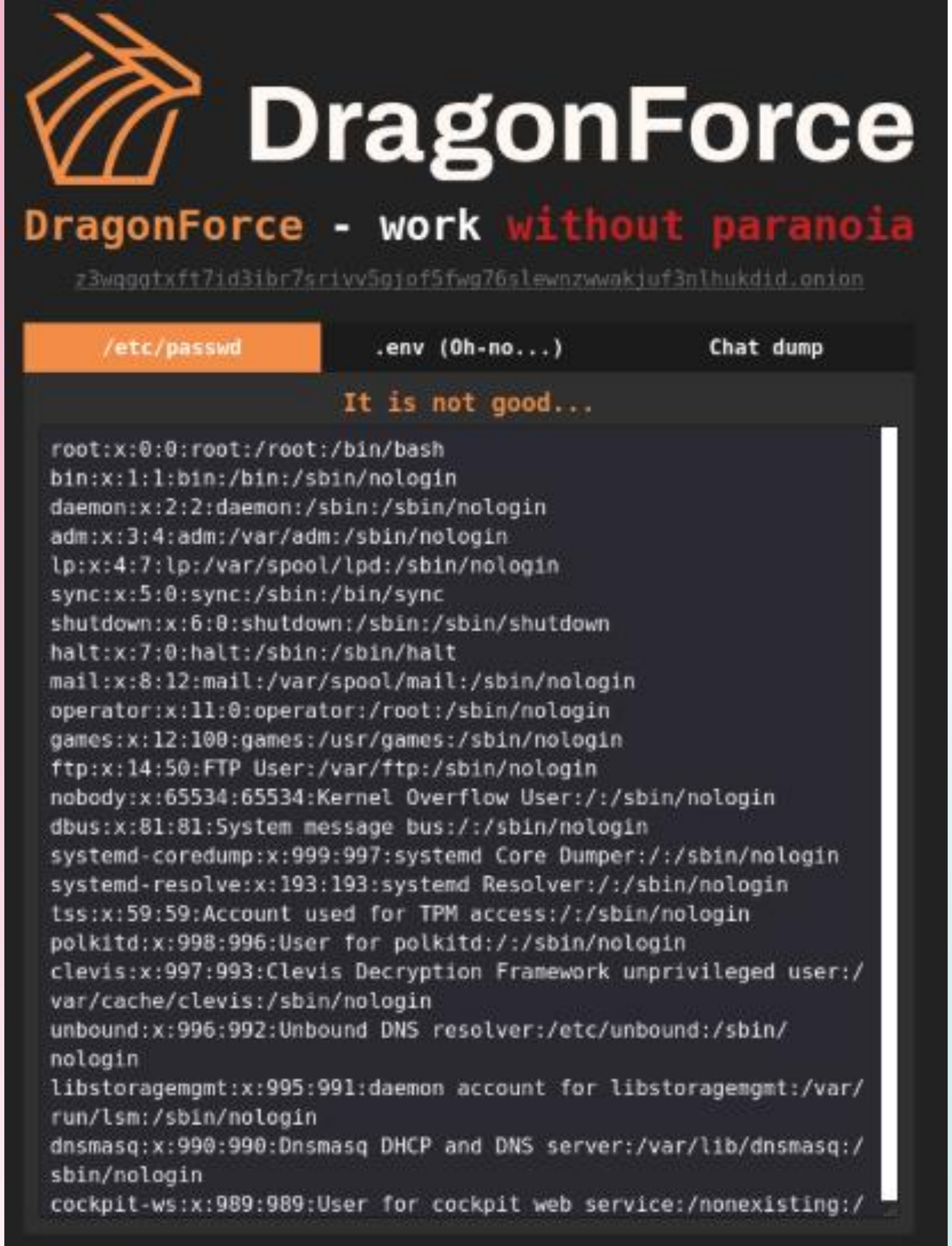
…k: What happened …ps be back to normal?

…heft and hacks recently

…nments

Victims according to data leak sites



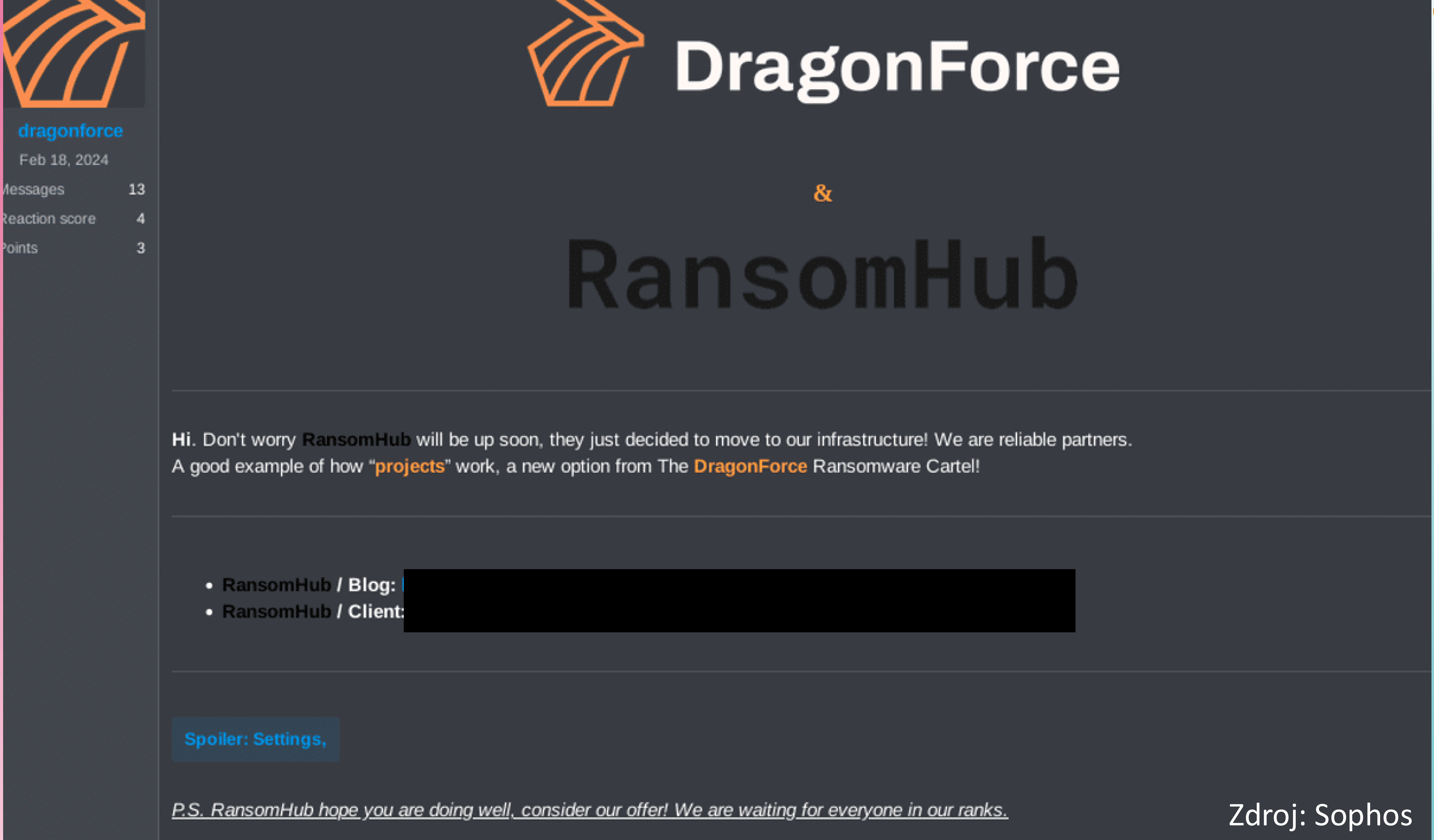


DragonForce - work without paranoia

z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

It is not good...

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
clevis:x:997:993:Clevis Decryption Framework unprivileged user:/
var/cache/clevis:/sbin/nologin
unbound:x:996:992:Unbound DNS resolver:/etc/unbound:/sbin/
nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/
run/lsm:/sbin/nologin
dnsmasq:x:990:990:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/
sbin/nologin
cockpit-ws:x:989:989:User for cockpit web service:/nonexisting:/
```



Hi. Don't worry **RansomHub** will be up soon, they just decided to move to our infrastructure! We are reliable partners.
A good example of how "**projects**" work, a new option from The **DragonForce** Ransomware Cartel!

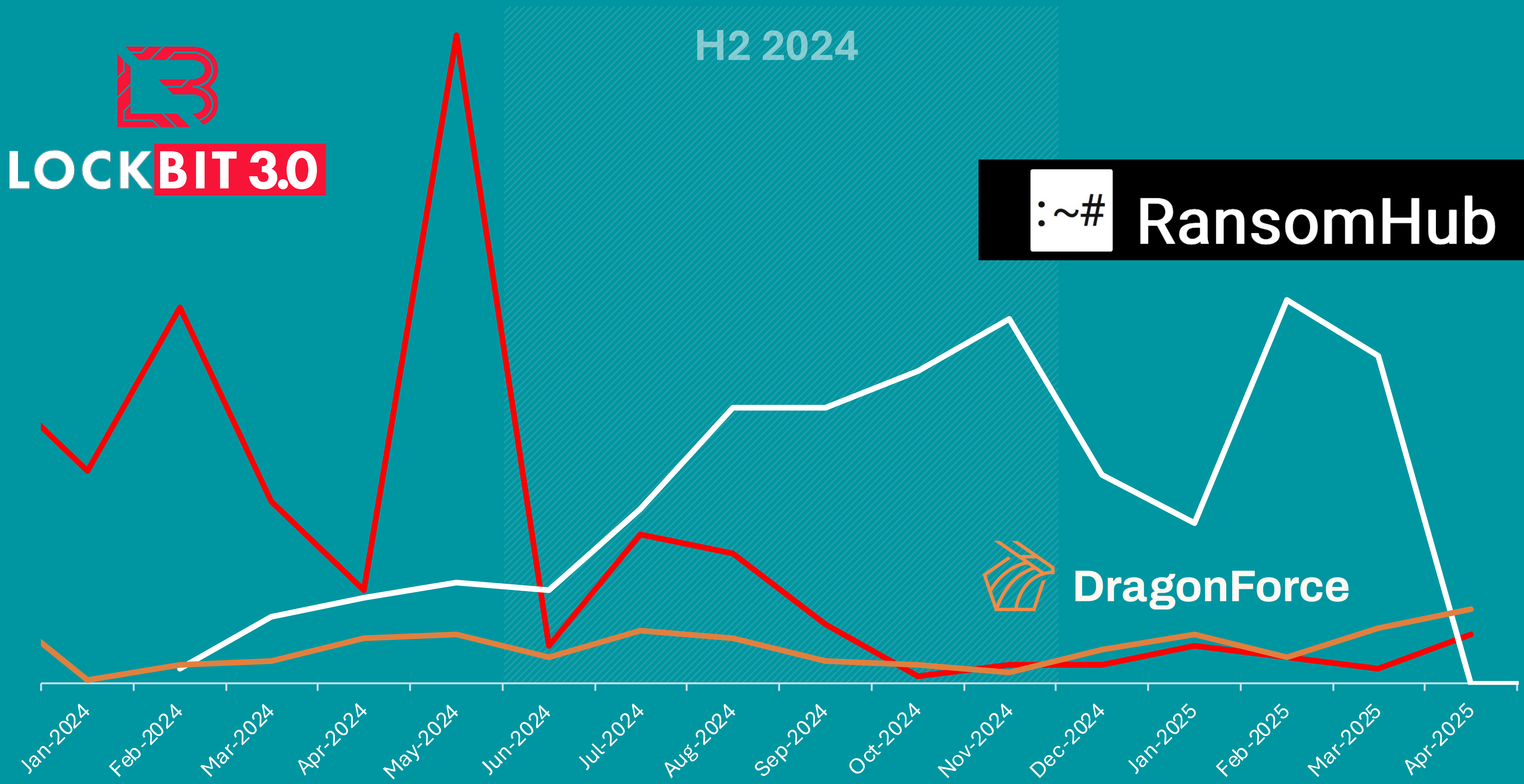
- **RansomHub / Blog:** [redacted]
- **RansomHub / Client:**

Spoiler: Settings,

P.S. RansomHub hope you are doing well, consider our offer! We are waiting for everyone in our ranks.

Zdroj: Sophos

Victims according to data leak sites



What would be the cost of a breach for you?

Who makes the decisions?

- Incident Response
- Data Recovery
- Downtime
- System Restoration
- Legal & Regulatory Compliance
- Notification & Communication
- Assessment of losses
- **Cyber Security Enhancements**

European
Commission

NIS 2

- Governance & Leadership
- Risk Management & Security Measures
- Supply Chain Security
- Incident Reporting & Response
- Legal & Regulatory Compliance
- Training & Awareness
- Continuous Improvement
- Technical Standards & Certifications
- Reporting & Communication
- Management Accountability

Finland
Norway
Sweden
Estonia
Latvia
Denmark
Lithuania
Ireland
United Kingdom
Belarus
Poland
Netherlands
Germany
Belgium
Luxembourg
Czechia
Ukraine
Slovakia
France
Liechtenstein
Switzerland
Austria
Hungary
Moldova
Slovenia
Croatia
Romania
Bosnia and Herzegovina
Serbia
Monaco
San Marino
Andorra
Italy
Kosovo*
Montenegro
Bulgaria
Vatican City
North Macedonia
Albania
Spain
Portugal
Greece
Turkey
Malta

Digital Security
Progress. Protected.

Thank you!