



Digital Security
Progress. Protected.

Your Cybersecurity Partner of choice

Andrea Russi

Presales Engineer

Iniziamo con un quiz!

[ESET QUIZ \(sli.do\)](https://sli.do/ESET-QUIZ)

About ESET

2000 EMPLOYEES

23 OFFICES

13 R&D CENTERS



30+ years in the market



Private company, no debt



Always focused on technology



Biggest European Union vendor



Growing YoY since its inception



Owned by original founders



Strong values



Progress. Protected.



Digital Security
Progress. Protected.

2200+ EMPLOYEES | 23 OFFICES | 12 R&D CENTERS

REGIONAL CENTERS

- BRATISLAVA
- SAN DIEGO
- BUENOS AIRES
- SINGAPORE

OFFICES

- PRAGUE
- JABLONEC NAD NISOU
- SAO PAULO
- JENA
- KRAKOW
- SYDNEY
- TAUNTON
- BOURNEMOUTH
- TORONTO
- MONTREAL
- IAȘI
- MEXICO CITY
- ZILINA
- BRNO
- TOKYO
- MILAN

RESEARCH AND DEVELOPMENT CENTERS

- BRATISLAVA
- BUENOS AIRES
- SINGAPORE
- PRAGUE
- KOSICE
- KRAKOW
- MONTREAL
- ZILINA
- IAȘI
- BRNO
- TAUNTON



Digital Security
Progress. Protected.

1bn+

internet users protected

400K+

Business Customers

150M

Users

4,000+

Enterprise Customers

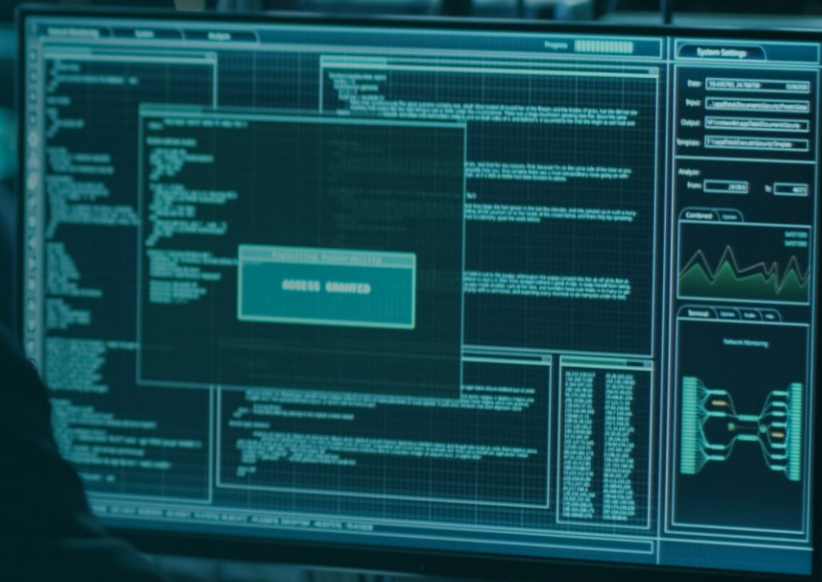
100,000

Partners

50

ISP&Telco Partners

Nowadays Era of Advanced Cyberattacks



ES 2022 – the “anyone can
make an electric car” edition

ncy scams: What
how to protect

igned kernel drivers –
unguarded gateway to
indows' core

ell vulnerability:
ve know so far

the alarms go off:
y steps to take after
a breach

welive security

BY



welivesecurity™ BY ESET

Breaking the habit: Top 10 bad cybersecurity habits to shed in 2022

Be alert, be proactive and break these 10 bad habits to improve your cyber-hygiene in 2022

Phil Muncaster
3 Jan 2022 - 11:30AM

welivesecurity™ BY ESET

Prime targets: Governments shouldn't go it alone on cybersecurity

A year into the pandemic, ESET reveals new research into activities of the LuckyMouse APT group and considers how governments can rise to the cybersecurity challenges of the accelerated shift to digital

Phil Muncaster

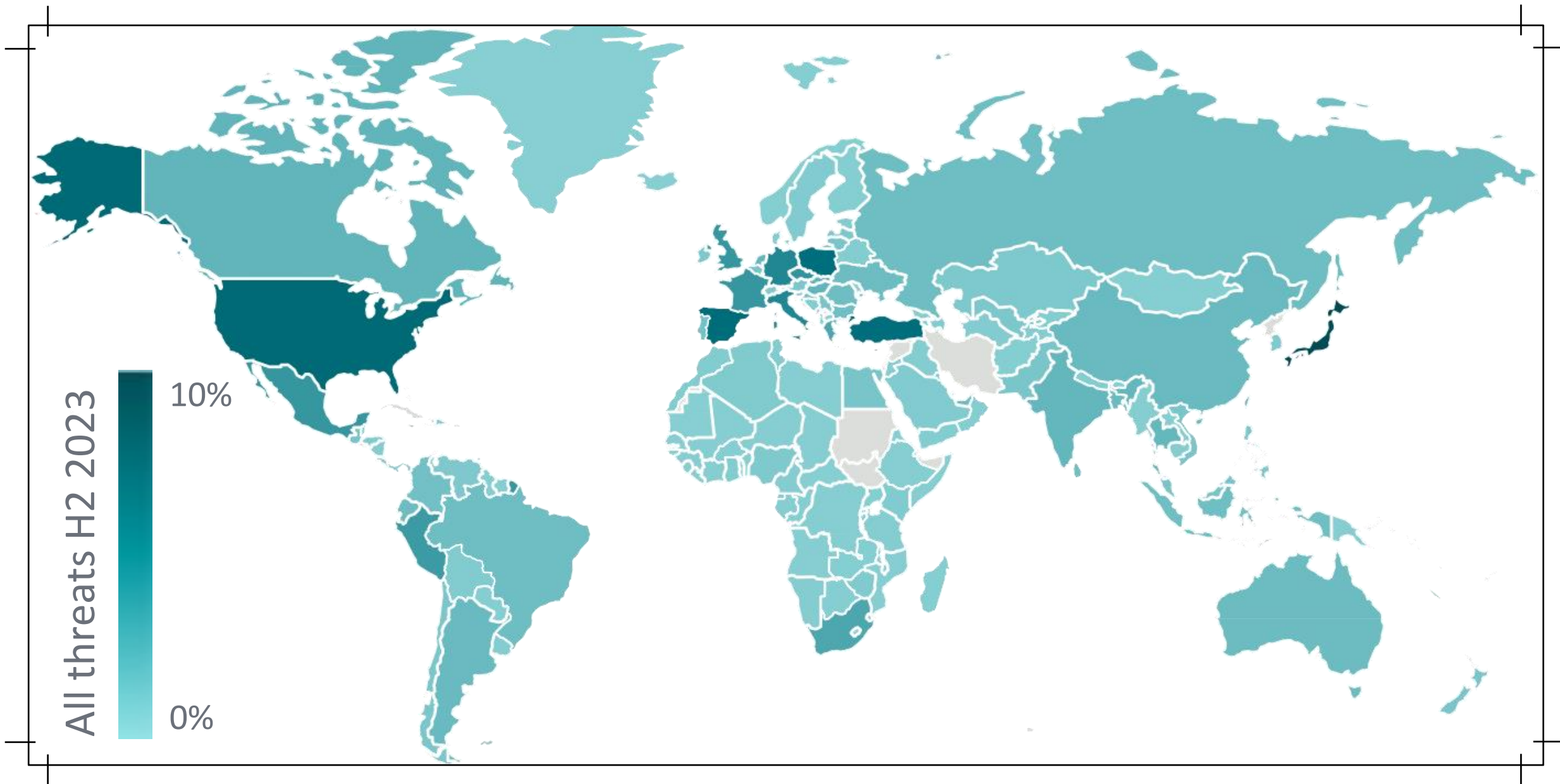
welivesecurity™ BY ESET

What are buffer over attacks and how are

welivesecurity™ BY ESET

What is a cyberattack surface and how can you reduce it?

Discover the best ways to mitigate your organization's attack surface, in order to maximize cybersecurity.



All threats H2 2023

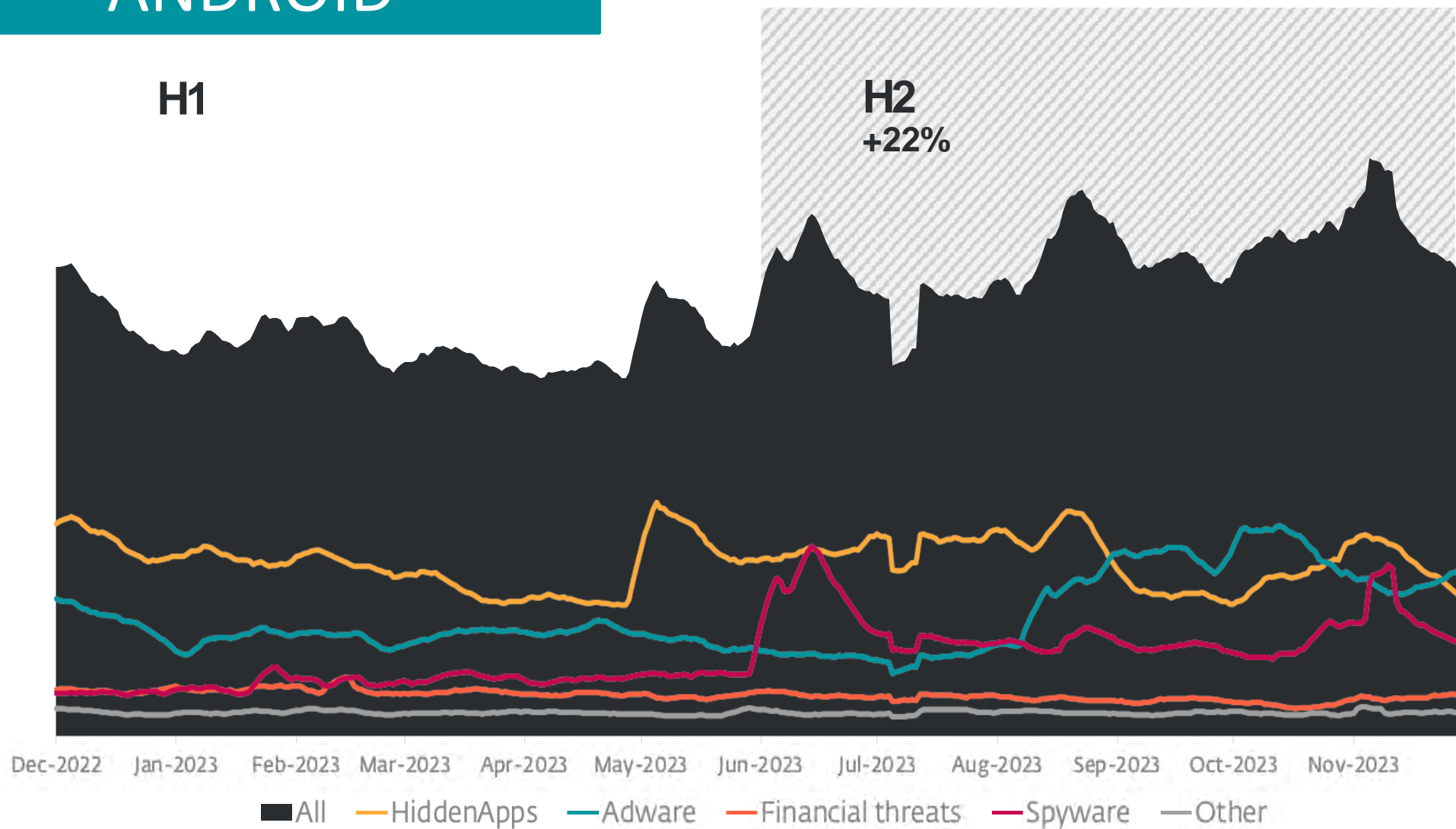
10%

0%

ANDROID

H1

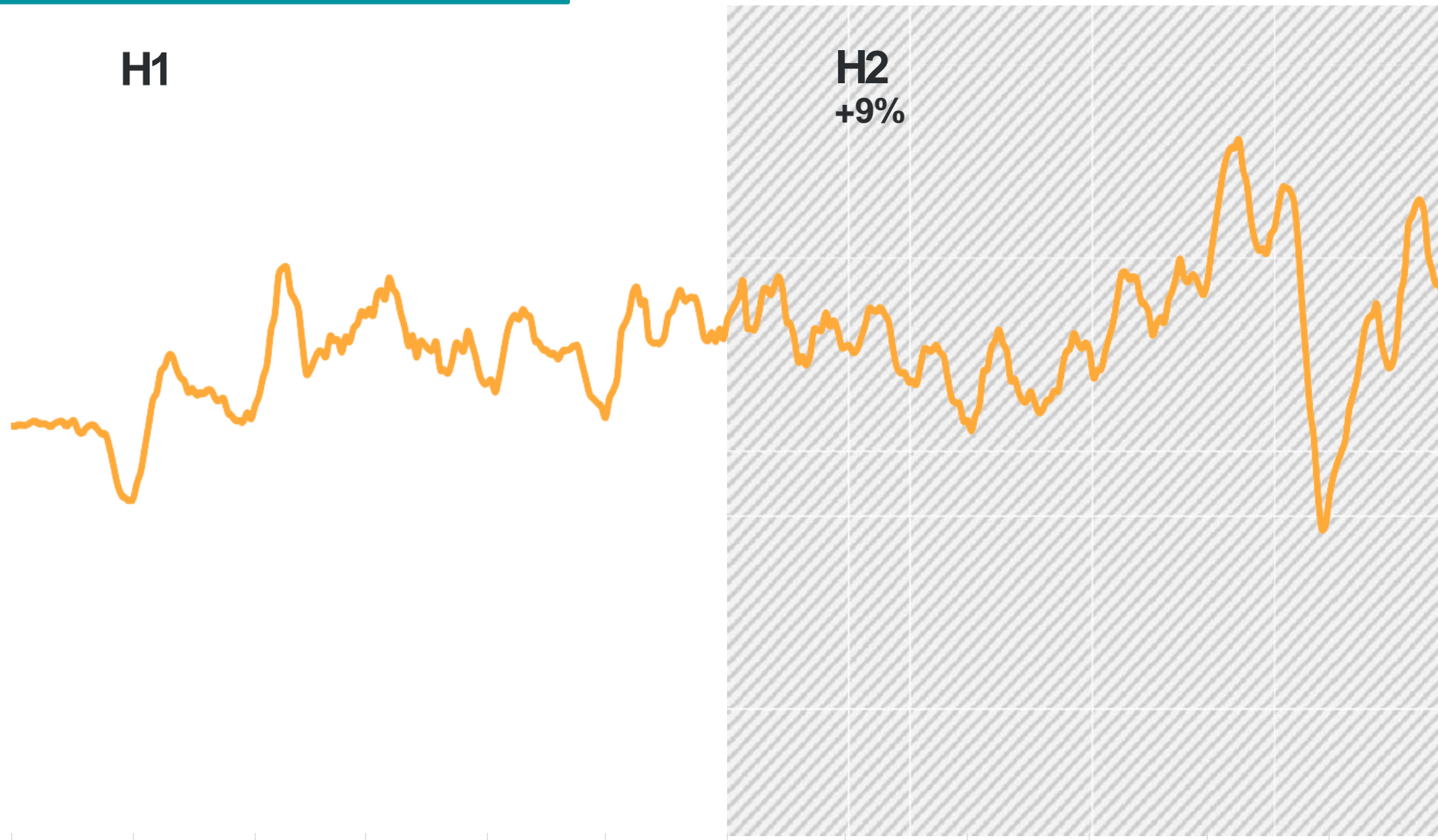
H2
+22%



EXPLOITS

H1

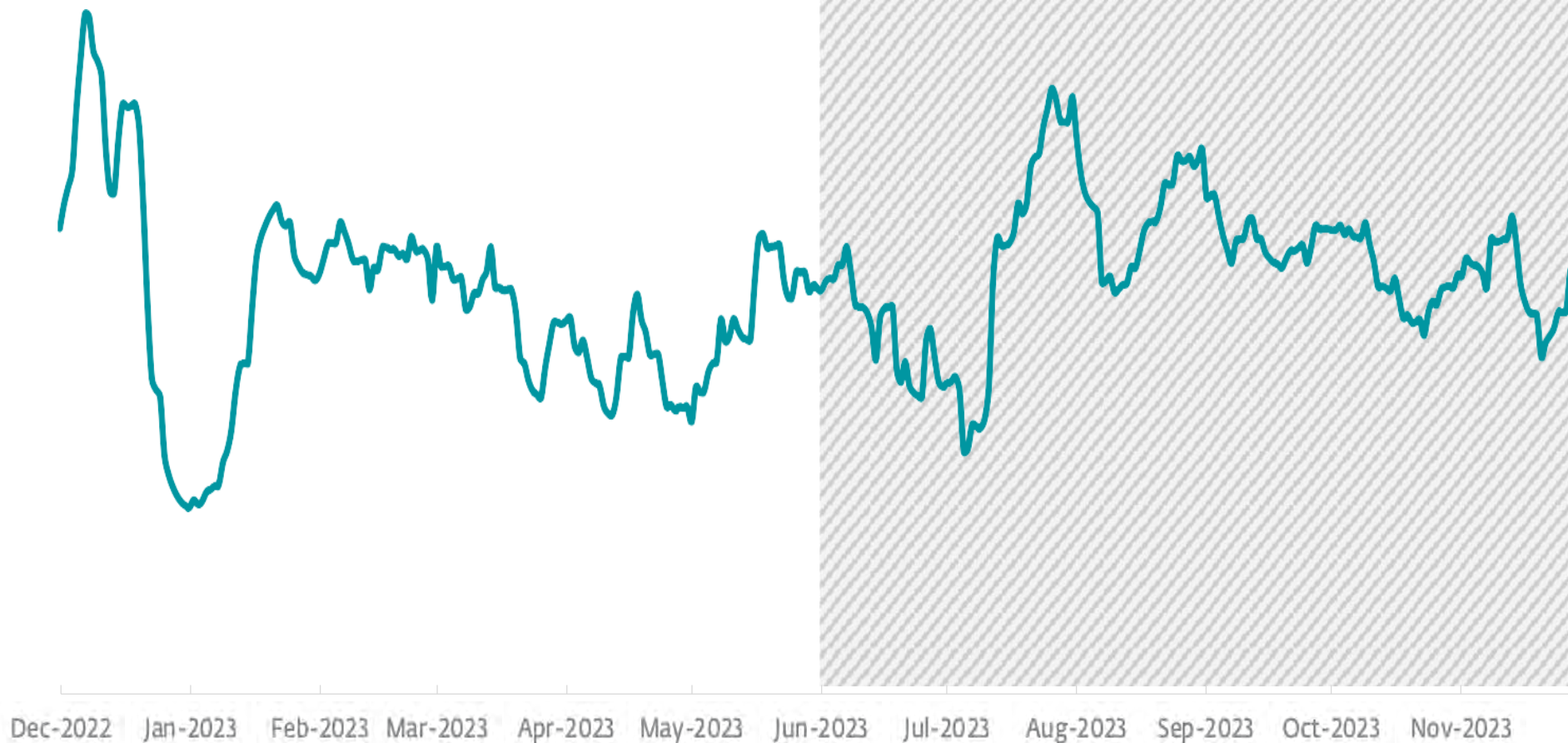
H2
+9%



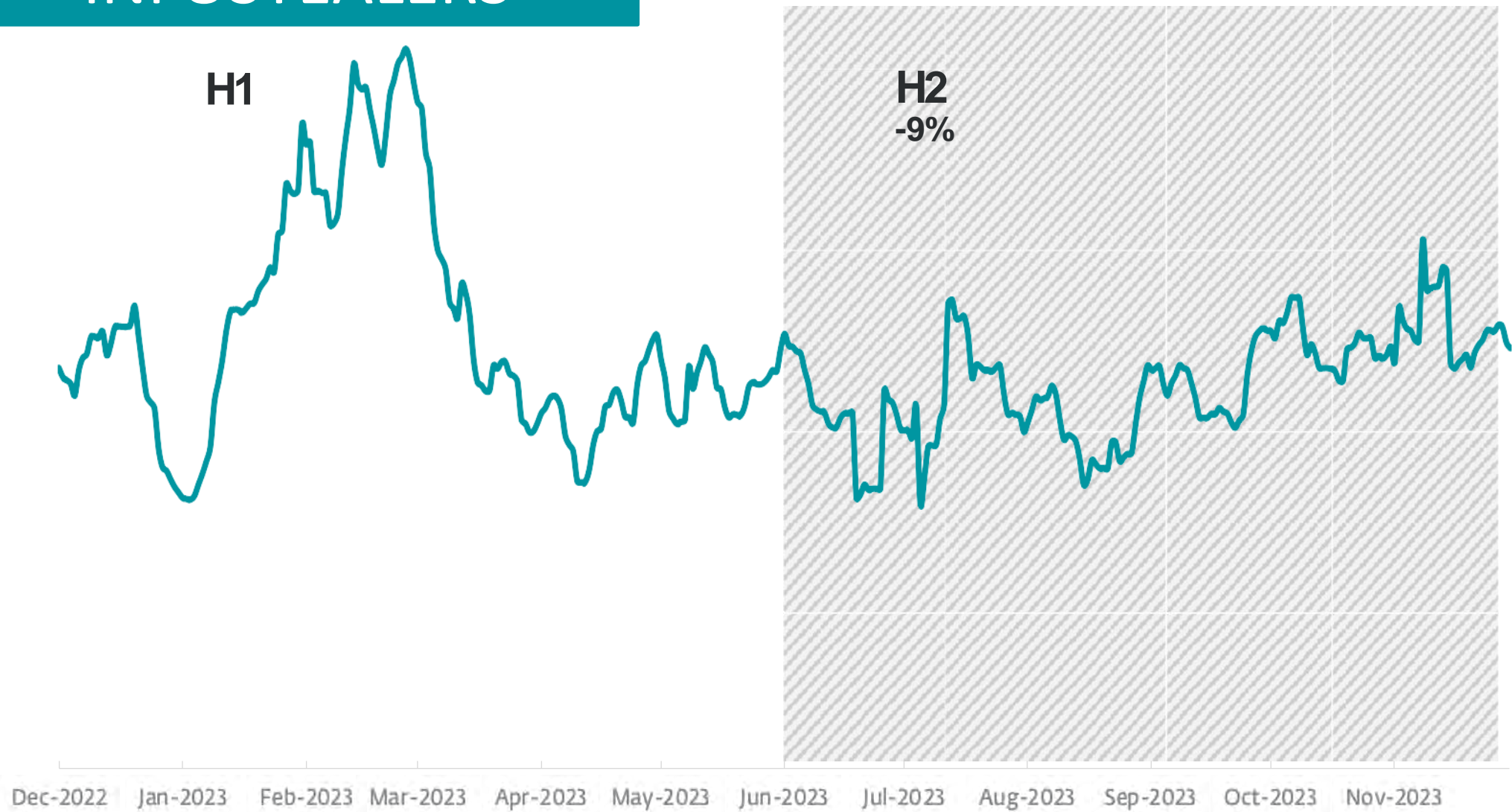
DOWLOADERS

H1

H2
+10%

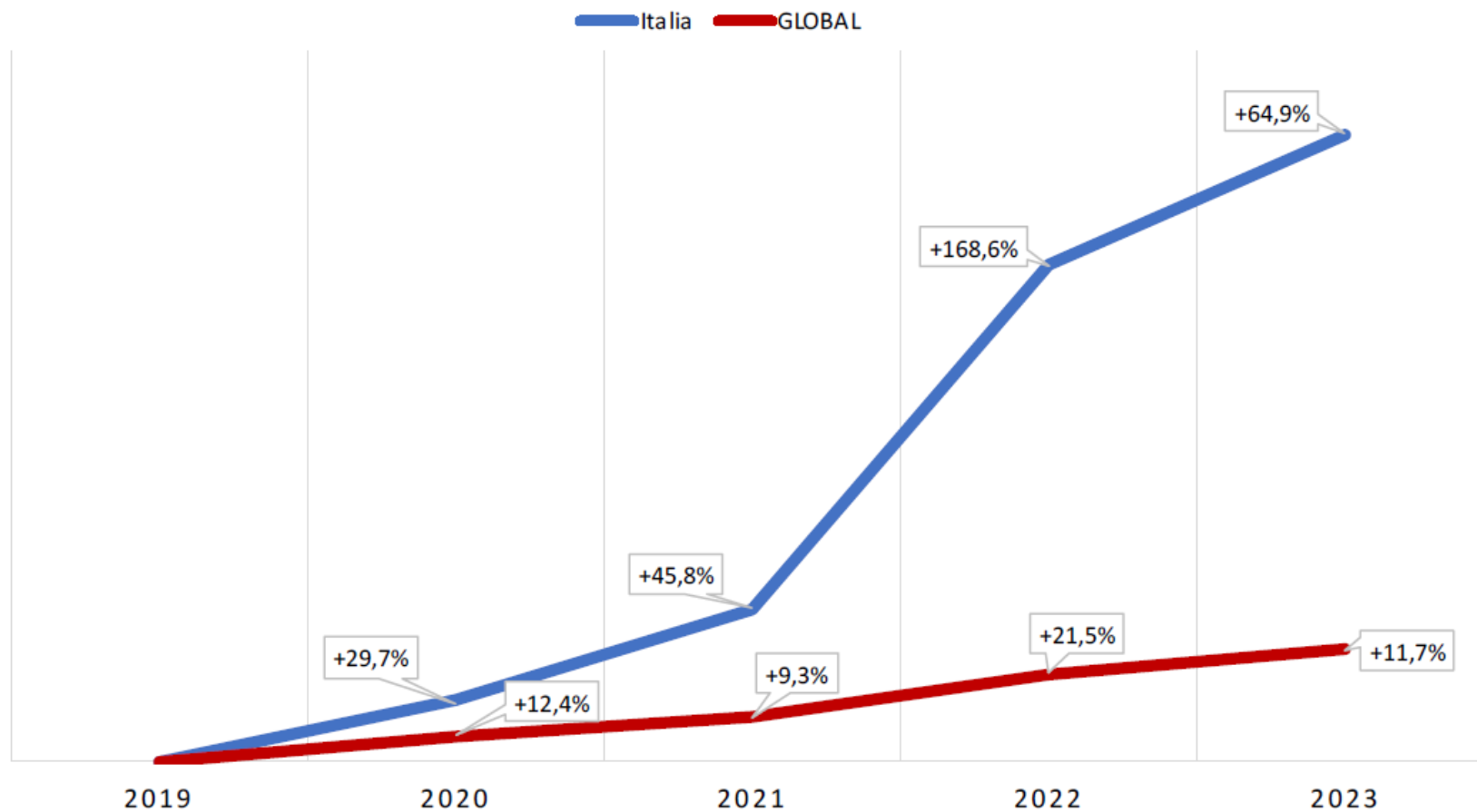


INFOSTEALERS



E il Clusit?

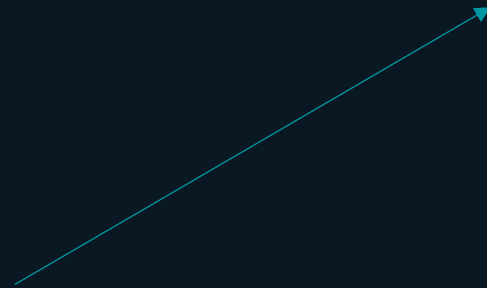
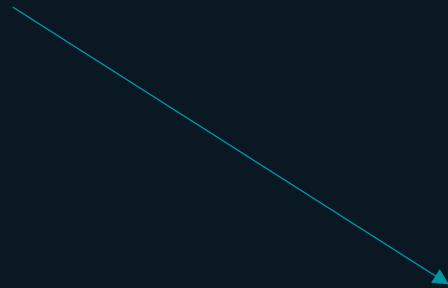
Cyber attacchi in Italia dal 2019 al 2023



Bassa Cultura

Bassi Investimenti

Bassa percezione del rischio



+ New chat

Search prompts...

No data.

- Settings
- Log in
- About us

Can you provide a Python script to exploit a buffer overflow vulnerability in a given application?

Sure, here's a basic Python script that demonstrates how to exploit a buffer overflow vulnerability:

```
python
import socket

# Create an array of buffers, from 1 to 5000, with increments of 200.
buffer=["A"]
counter=100
while len(buffer) <= 30:
    buffer.append("A"*counter)
    counter=counter+200

for string in buffer:
    try:
        print "Fuzzing with %s bytes" % len(string)
        s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(('IP', PORT)) # Replace IP and PORT with the target IP and port
        s.send(('COMMAND '+string+'\r\n'))
        s.close()
    except:
        print "Error connecting to server"
        sys.exit()
```

This script creates an array of buffers and sends them to the target application. The `socket` module is used to create a TCP socket and connect to the target. The `send` method is then used to send the buffer to the target. If the connection fails, the script will print an error message and exit.

Remember to replace 'IP' and 'PORT' with the actual IP address and port of the target application. Also, you'll need to modify the `send` method to send the buffer in the format expected by the target application.

Regenerate response

HackerGPT GPT-4

Plugin Store

Perform a DNS information scan on hackerone.com.

```
json
{ "command": "nuclei -target hackerone.com -tags dns" }
```

Starting the scan. It might take a minute.

Still working on it, please hold on...

Scan done! Now processing the results...

Nuclei Scan Results

Target: "hackerone.com"

Scan Date and Time: 1/3/2024, 10:14:33 AM GMT

Results:

```
[mx-service-detector:Google Apps] [dns]
[mx-fingerprint] [dns] [info] hackerone.com
[dmarc-detect] [dns] [info] _dmarc.hackerone.com
[caa-fingerprint] [dns]
[nameserver-fingerprint]
[dssec-detection] [dns] [info] hackerone.com
```

Regenerate response

Home

+ New Chat

Search chats...

New Folder

Today

- Explain how to identify and exploit XSS vulnerabilities

Yesterday

- test

Explain how to identify and exploit XSS vulnerabilities

Mr. Robot

Explain how to identify and exploit XSS vulnerabilities

HackerGPT

Cross-Site Scripting (XSS) vulnerabilities occur when a web application allows user input to be displayed in a web page without proper sanitization or encoding. This enables an attacker to inject malicious scripts into the web page, which can then be executed by other users visiting the affected page. Here's a step-by-step guide on how to identify and exploit XSS vulnerabilities, assuming you have permission to perform these tests:

- Identify potential entry points:** Look for any user-controlled input fields or areas in the application where data can be submitted, such as form fields, URL parameters, and HTTP headers. Common entry points include search bars, comment sections, and user profiles.
- Analyze the application's behavior:** Submit various types of input data into the identified entry points. Observe the application's response and behavior. Pay attention to any unusual error messages, redirection, or changes in the returned content.
- Test for reflected (non-persistent) XSS:** Inject simple payloads like `<script>alert('XSS')`.

Ask anything. Type "/" for prompts and "#" for files.

Type a message ...

Resilience

Firewall

**Vulnerability
Assesment**

Sandbox

Encryption

MDR

Antivirus

XDR

**Intrusion
Detection**

SIEM

**Antispam
and
antiphishing**

DLP

Patching

2FA

**Penetration
test**

Cyber Security today

H24

What are the prominent threats in cybersecurity today?



**Active
Components**



**Fileless
Attacks**



**Lateral
Movement**



**Data
Affected**



**Techniques
Used**



**Root
Cause**

What is happening?

How did it start?

Where did it start?

When did it start?

Is it contained?

How do we prevent it in future?

We think it's a cyber-attack

We're not sure

We're not sure

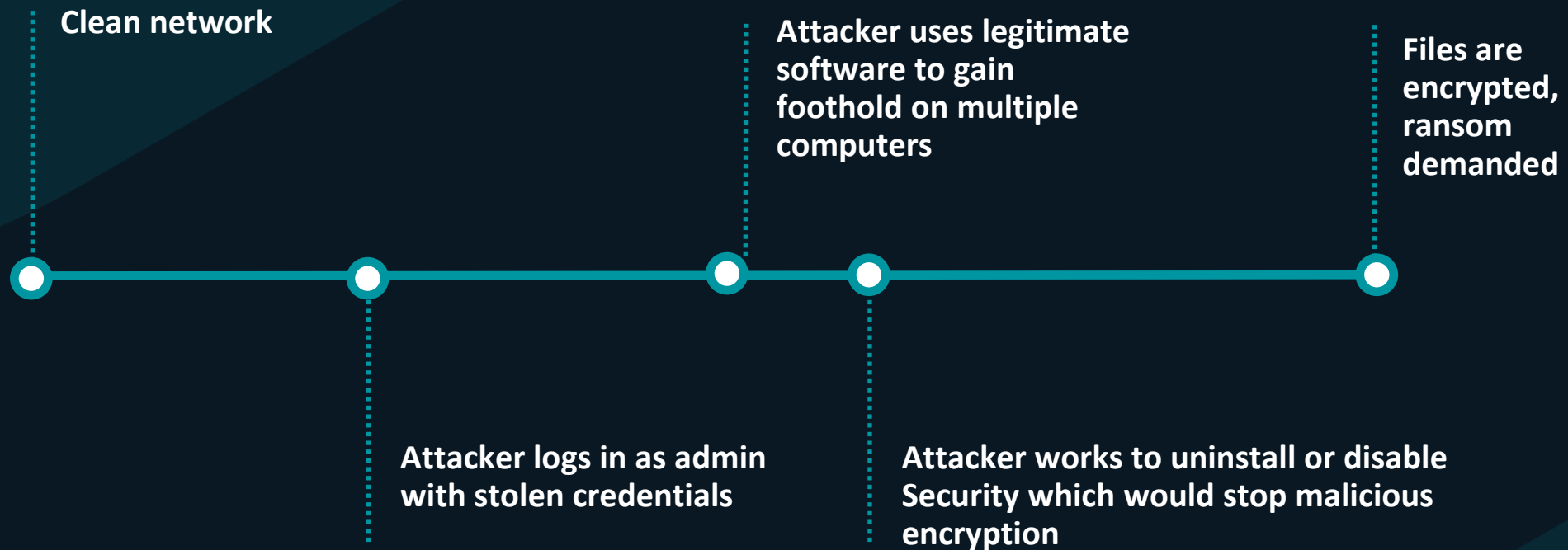
We're not sure

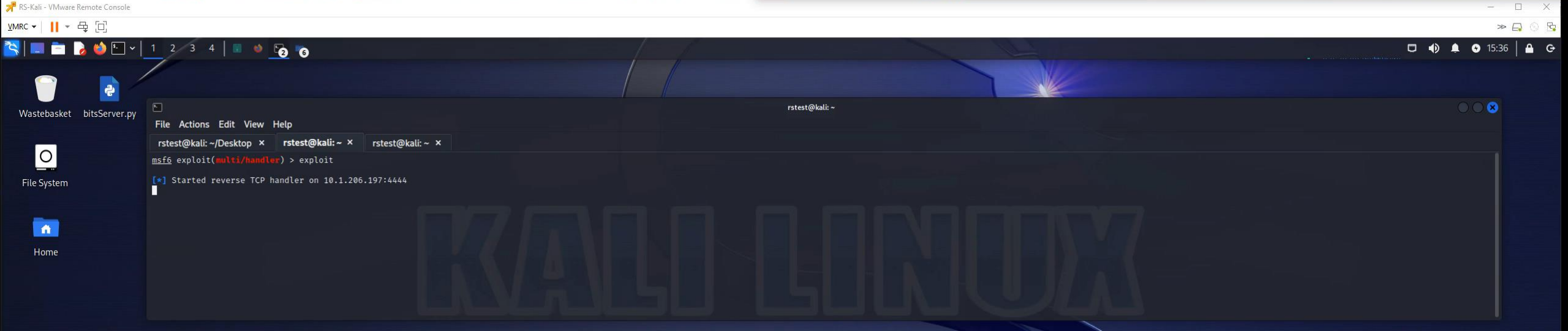
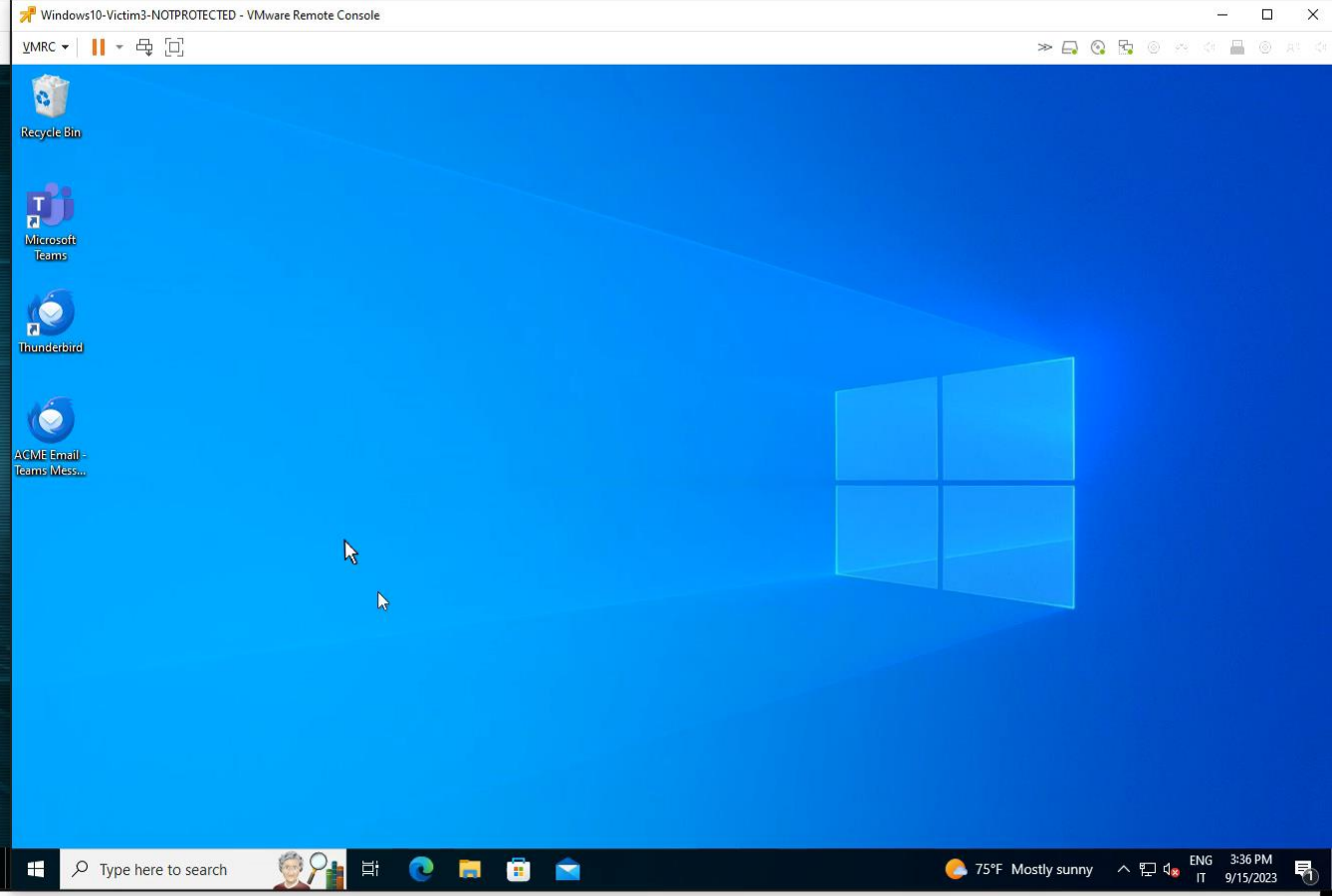
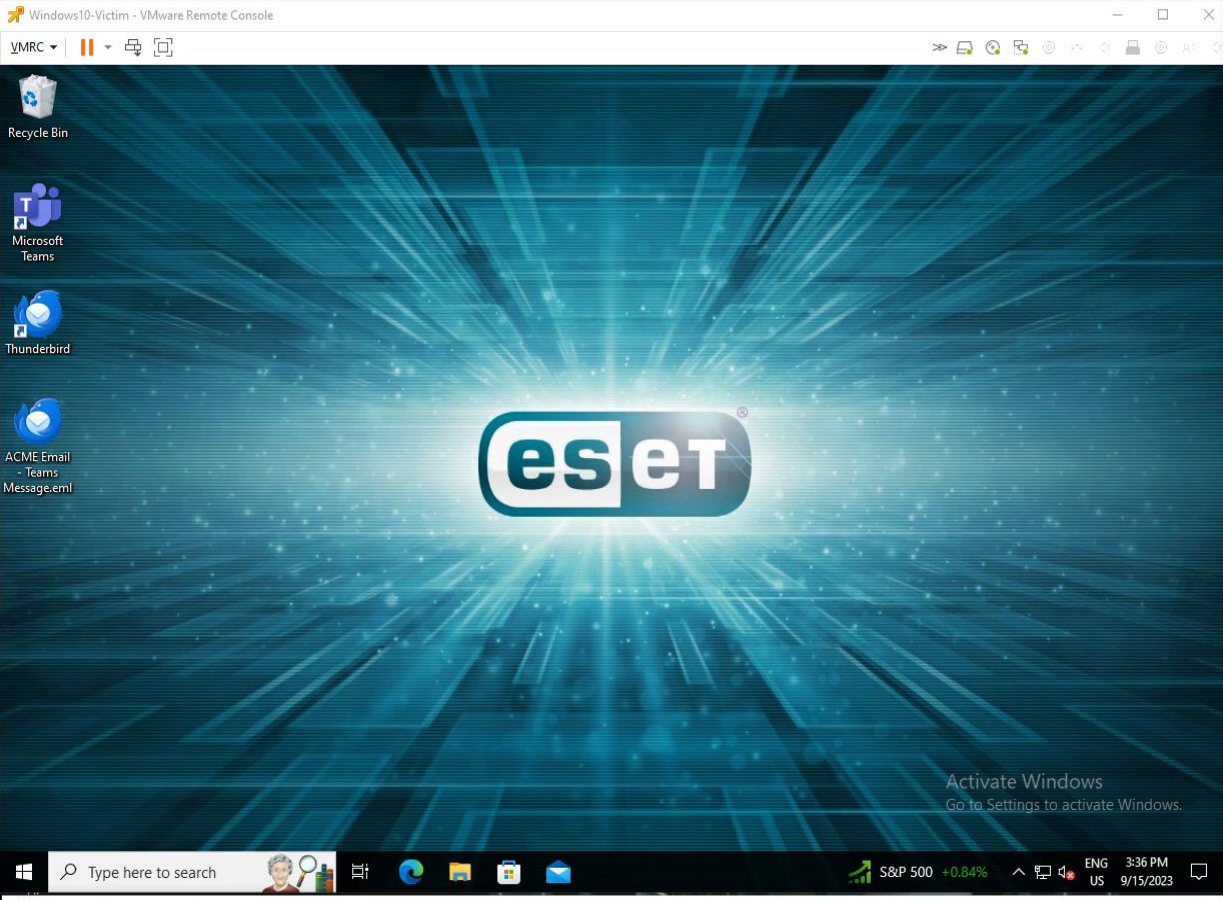
We're not sure

We're not sure

**XDR allows you to answer
those questions**

What does a ransomware attack look like?





Do companies really need H24?

Vulnerabilities are often exploited **within hours** of their discovery

Patches get reverse-engineered and exploits are live **in days** as part of exploit toolkits

Time from initial breach to malware execution is getting shorter and shorter

WHY MDR?

Gartner says: **MDR services** enable these leaders' organizations to benefit from a modern, turnkey and 24/7 approach to cybersecurity and suggests that **organizations lacking internal 24/7 cybersecurity operations embrace an MDR service** that employs containment for incident response. .

50%

of organizations will be using MDR services for threat monitoring by 2025

Global MDR market size growth

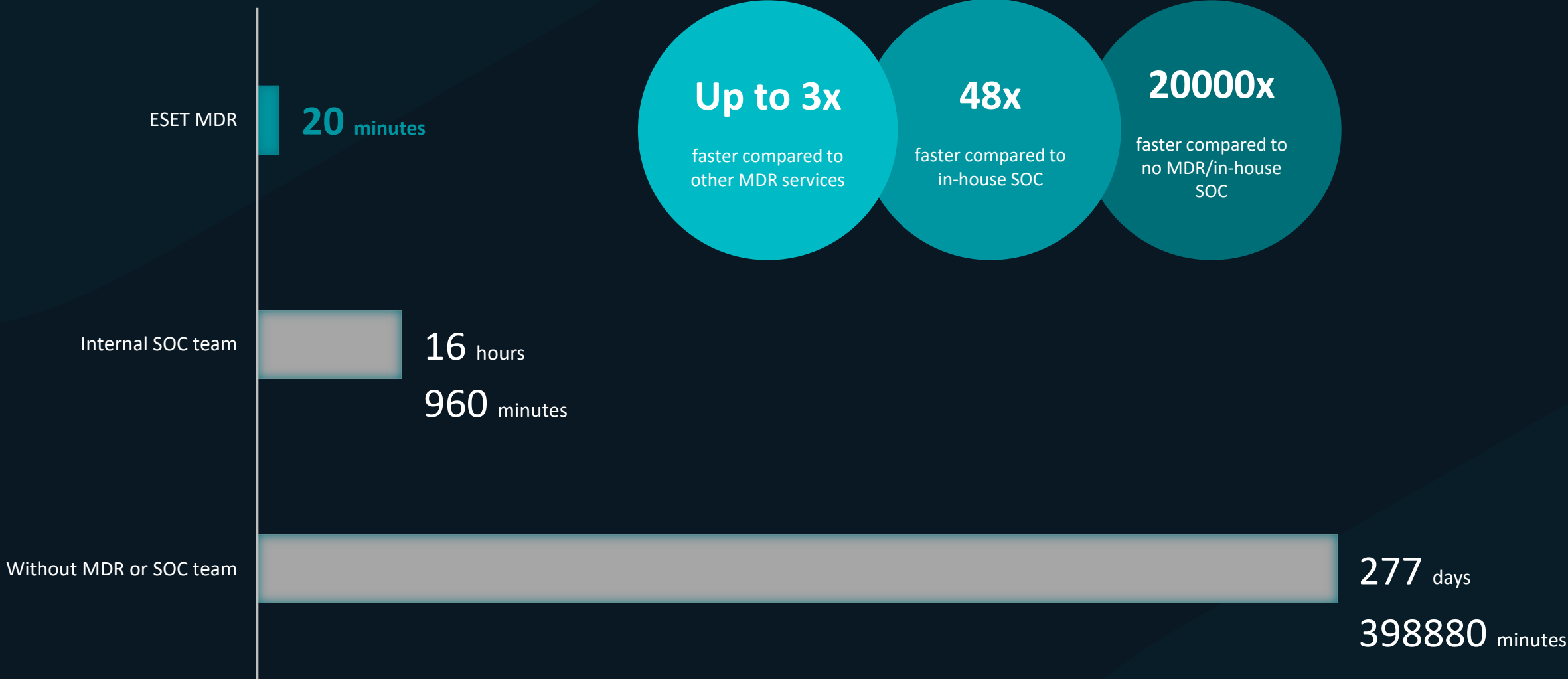
\$ 2.6 billion in 2022 —→ **\$ 5.6 billion by 2027**

82% of ransomware attacks target SMBs

The average impact of a data breach on SMB organizations is **\$3.3 million**

Time to detect and respond is crucial

Time to detect and respond



ESET MDR key benefits



**Best security experts on
the planet – working
for you**



Instant response

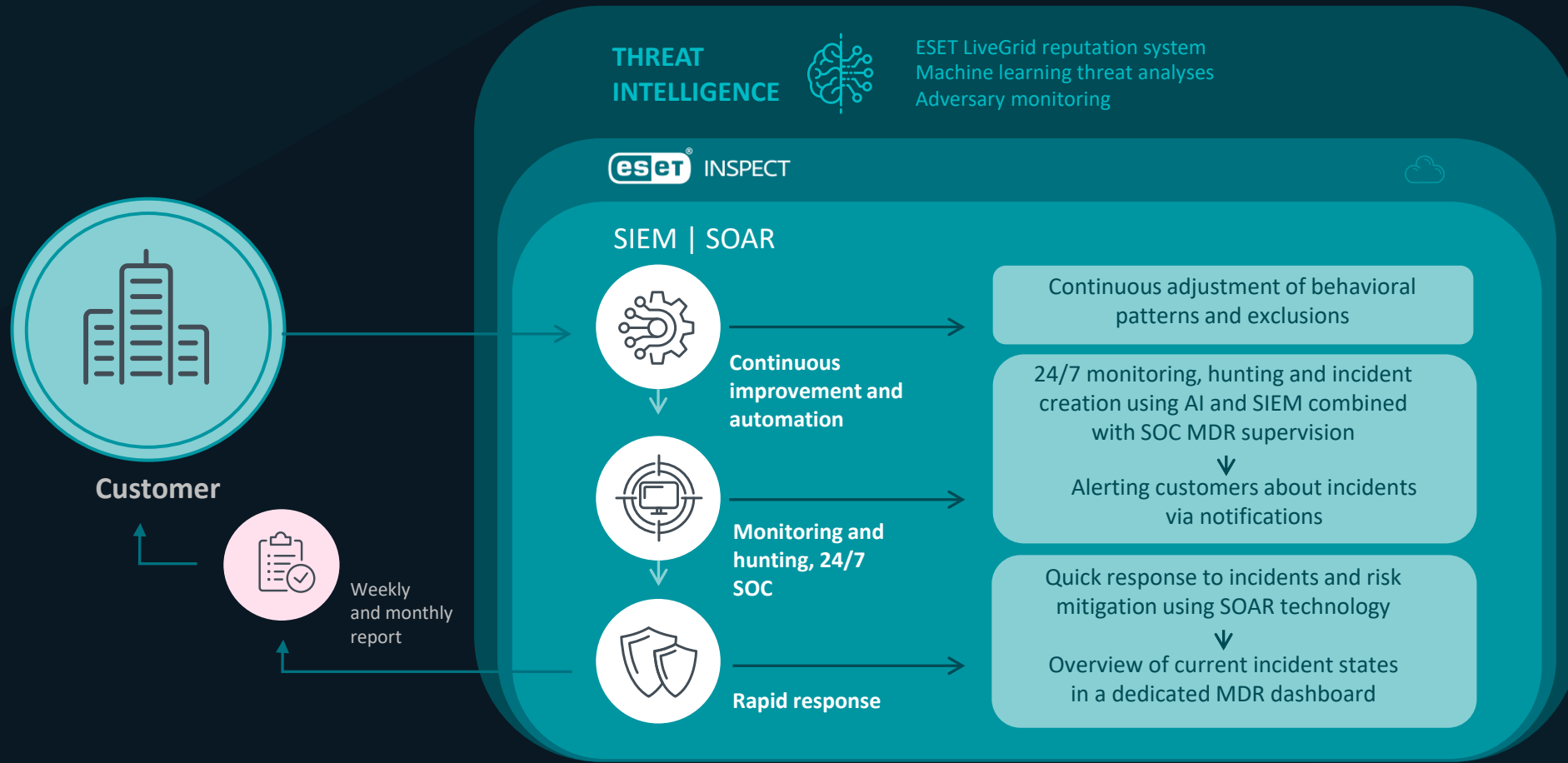


Always on



Compliance

How ESET MDR works



Ready to see it in action?



Digital Security

I computer sono
incredibilmente veloci,
accurati e stupidi.
Gli uomini sono
incredibilmente lenti,
inaccurati e intelligenti.

L'insieme dei due
costituisce una forza
incalcolabile.

- *Albert Einstein* -





Andrea Russi

Presales Engineer ESET Italia

marketingitaly@eset.com