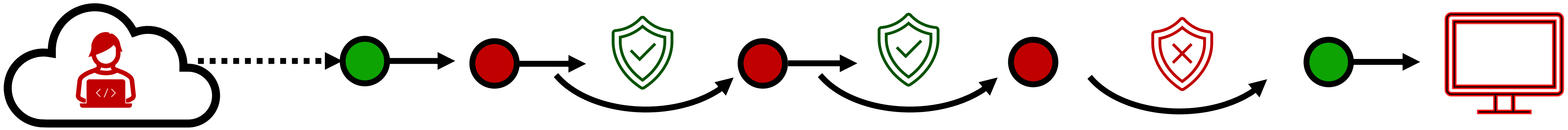
Active Adversary Report 2023

Combatiendo el Cibercrimen como servicio con CiberSeguridad como servicio

Guiu Ocón
Account Executive Sophos Iberia

SOPHOS

Understanding Active Adversaries



Adversary

Gains remote access

Attempt #1

Attack successfully blocked

Attempt #2

Attack successfully blocked

Attempt #3

Attack not blocked

Ransomware deployed

Cybercrime-as-a-service: The Naughty Nine

Access-as-a-service

Gaining access to compromised accounts and systems in bulk through RDP and VPN credentials, web shells, and exploitable vulnerabilities

Malware-as-a-service

Facilitating the distribution of malware within specific regions or sectors with watering-hole attacks, crossover with access-as-a-service listings, and other vulnerabilities

Phishing-as-a-service

How threat actors are offering end-to-end services for cloned sites, hosting, emails to bypass spam filters, and other phishing campaigns

OPSEC-as-a-service

Bundled services provided by threat actors designed to hide Cobalt Strike infections to minimize the risk of detection

Crypting-as-a-service

Common on many forums, crypting as a service involves the use of encrypted malware to bypass detection for a one-time purchase or subscription

Scamming-as-a-service

Designed as classified ads, scamming kits and services help threat actors pose as support specialists for cryptocurrency scams

Vishing-as-a-service

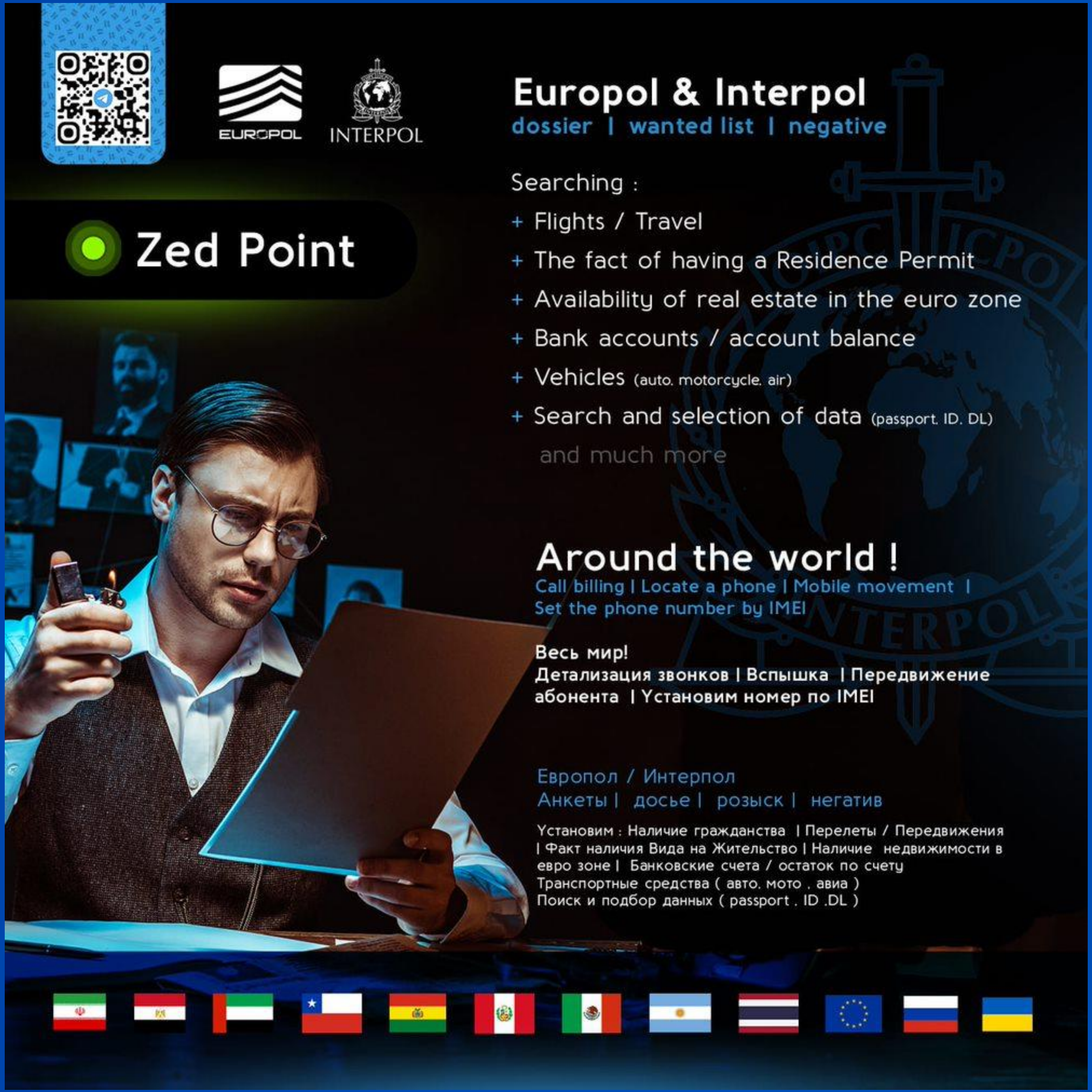
How threat actors offer to rent voice systems to receive calls where victims opt out and speak to a bot, rather than a human

Spamming-as-a-service

Infrastructure designed to build or manage bulk spamming services through a variety of mechanisms, including SMS and email

Scanning-as-a-service

Offering access at discount prices for legitimate commercial tools such as Metasploit and Burp Suite to find and exploit vulnerabilities



Europol & Interpol

dossier | wanted list | negative

Searching :

- Flights / Travel
- The fact of having a Residence Permit
- Availability of real estate in the euro zone
- Bank accounts / account balance
- Vehicles (auto, motorcycle, air)
- Search and selection of data (passport, ID, DL)

and much more

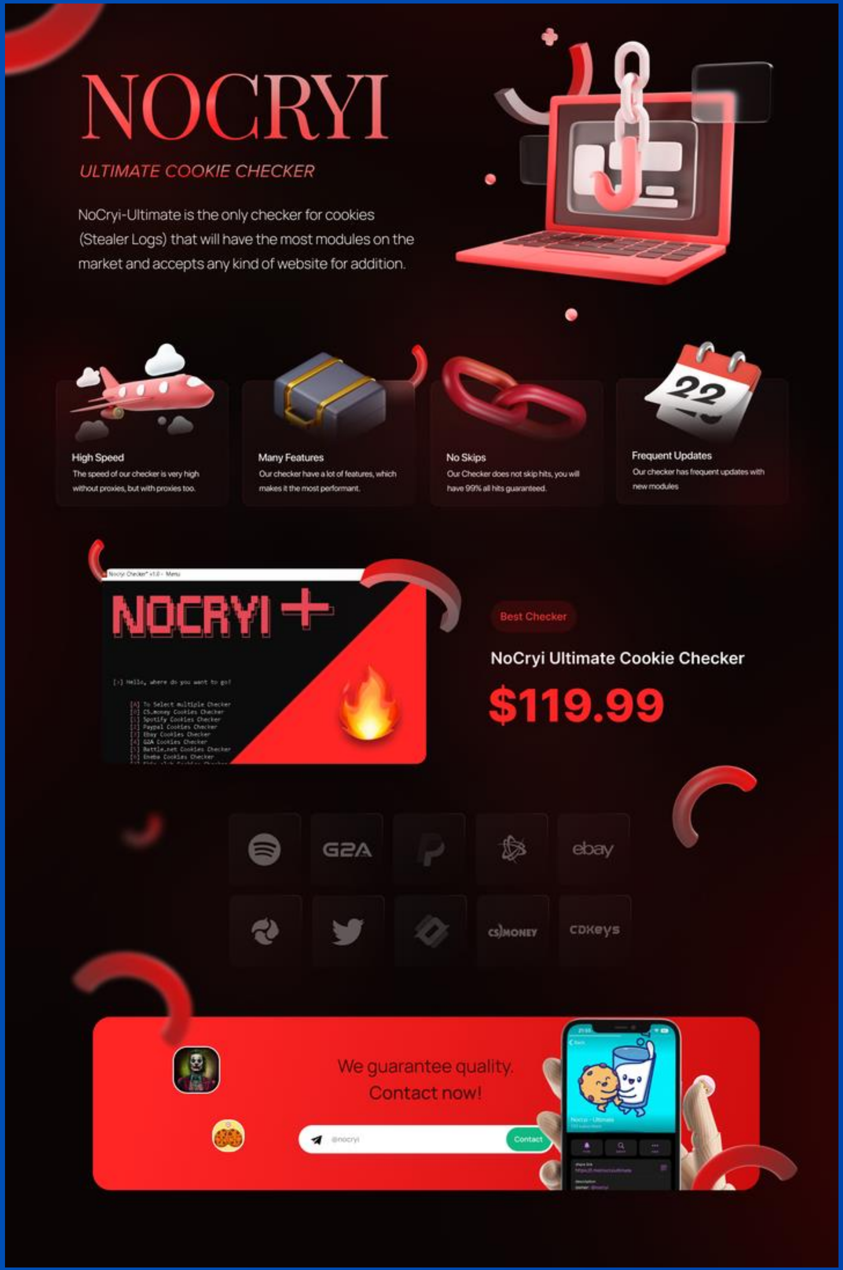
Around the world !

Call billing | Locate a phone | Mobile movement |
Set the phone number by IMEI

Весь мир!
Детализация звонков | Вспышка | Передвижение абонента | Установим номер по IMEI

Европол / Интерпол
Анкеты | досье | розыск | негатив

Установим : Наличие гражданства | Перелеты / Передвижения | Факт наличия Вида на Жительство | Наличие недвижимости в евро зоне | Банковские счета / остаток по счету
Транспортные средства (авто, мото , авиа)
Поиск и подбор данных (passport , ID ,DL)



NOCRYI

ULTIMATE COOKIE CHECKER

NoCryi-Ultimate is the only checker for cookies (Stealer Logs) that will have the most modules on the market and accepts any kind of website for addition.

High Speed
The speed of our checker is very high without proxies, but with proxies too.

Many Features
Our checker have a lot of features, which makes it the most performant.

No Skips
Our Checker does not skip hits, you will have 99% all hits guaranteed.

Frequent Updates
Our checker has frequent updates with new modules

```
Nocryi Checker* v1.0 - Menu
NOCRYI +

[-] Hello, where do you want to go!

    [A] To Select multiple Checker
    [0] CS.money Cookies Checker
    [1] Spotify Cookies Checker
    [2] Paypal Cookies Checker
    [3] Ebay Cookies Checker
    [4] G2A Cookies Checker
    [5] Battle.net Cookies Checker
    [6] Eneba Cookies Checker
```

Best Checker

NoCryi Ultimate Cookie Checker

$119.99

We guarantee quality.
Contact now!

Active Adversary Report 2023

SOPHOS

Who Is the Sophos X-Ops Incident Response Team?

Who

Core Team

50 Digital Forensic Specialists
35 Deployment Engineers

Backed by:

150+ MDR SOC Analysts
400 Malware Analysts in SophosLabs

What

Immediate Response

Quickly triage, contain, and neutralize active threats

Threat Removal

Eject adversaries from your estate to prevent further damage

Analysis of 232 Incident Response Cases

2022 – 1H 2023

2022

152 incident response cases

81% from sub-1000 organizations

22 sectors represented

35 nations represented

1H 2023

80 incident response cases

88% from sub-1000 organizations

25 sectors represented

34 nations represented

Evolving Attack Vectors

Exploited Vulnerabilities

2022

37%

36%
State of Ransomware Survey

2023 H1

23%

Compromised Credentials

2022

30%

29%
State of Ransomware Survey

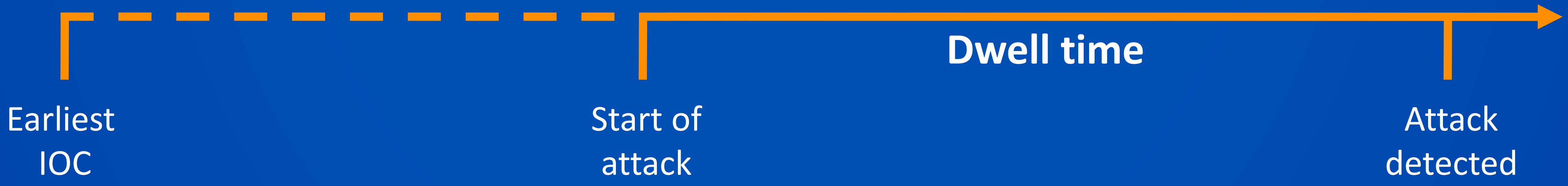
2023 H1

50%

Source: The State of Ransomware 2023, Sophos (n=1,974 organizations hit by ransomware in the last year); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Ransomware dwell time

2020	2021	2022	1H23
18 days	11 days	9 days	5 days



Dwell time

Earliest IOC

Start of attack

Attack detected

La falta de MFA deja la puerta abierta a los adversarios.

39%

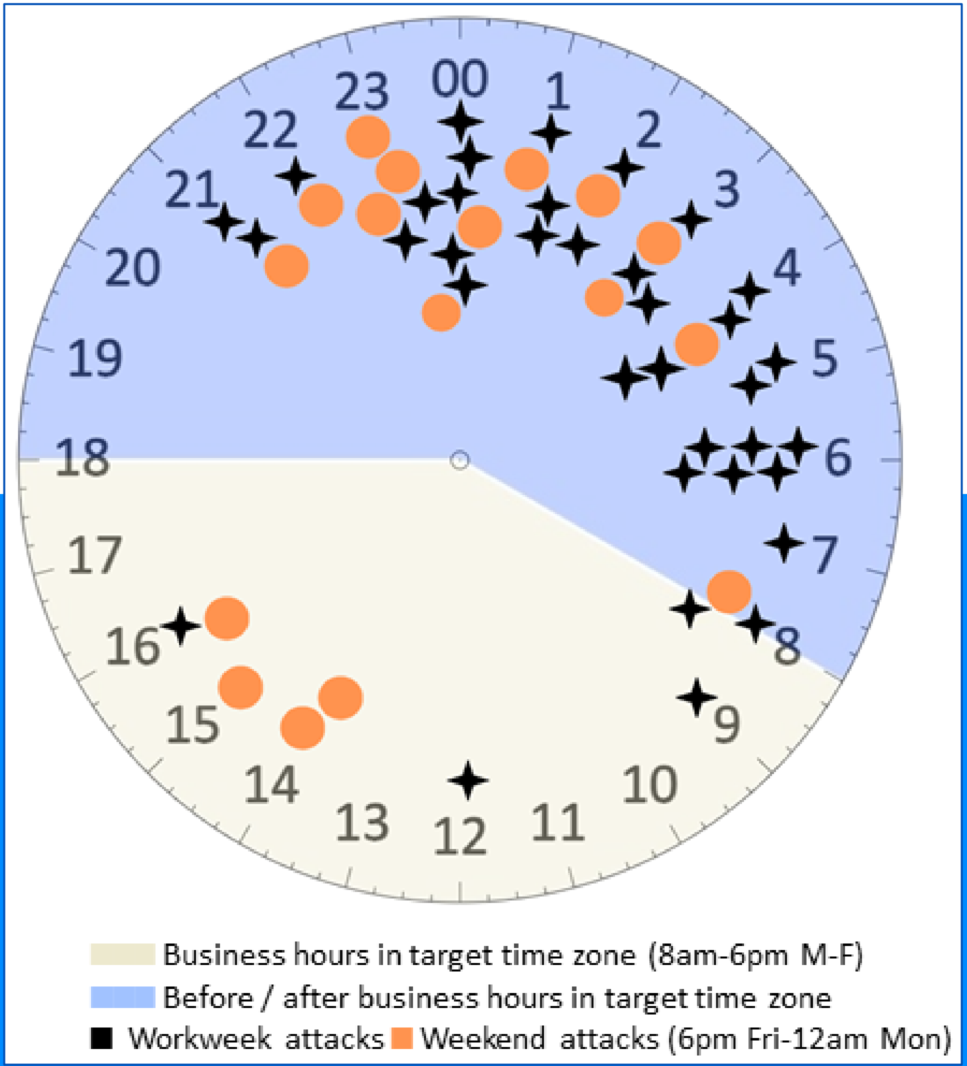
De los incidentes que remediamos en la primera mitad de 2023 no tenían configurada la autenticación multifactor (MFA).

Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Attackers Target Off-Hours

91% de los ataques ransomware comienzan fuera del horario laboral

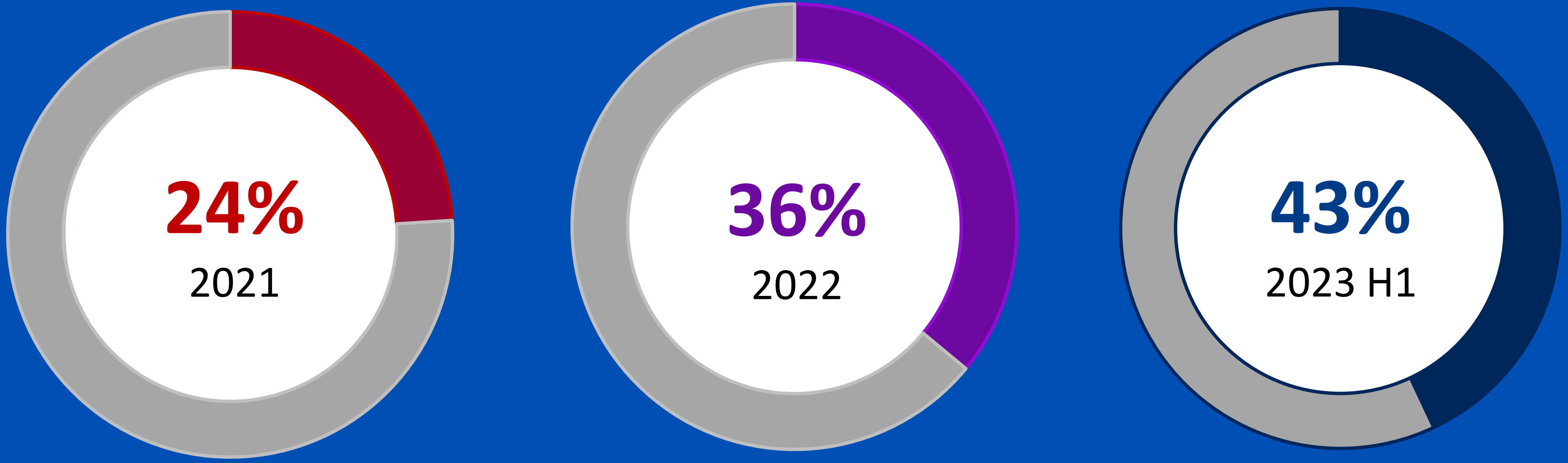
9 ide cada 10 ataques ocurren fuera de entre las 8am to 6pm entre semana.



Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=52)

Disabling Protection Is Now Commonplace

Percentage of Active Directory compromises where adversaries disable protection



Source: Active Adversary Playbook 2022, Sophos (n=144); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Summary Recommendations

Changing the Story: A Two-Prong Approach

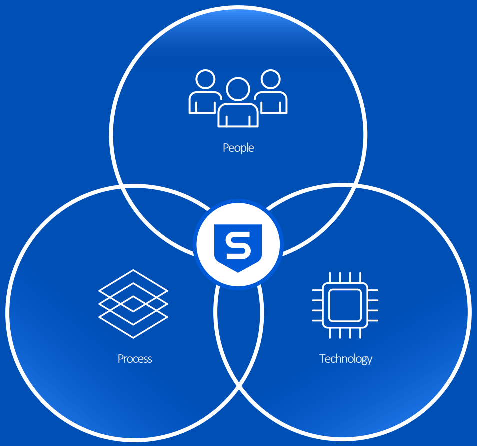
Slow Adversaries

Accelerate Defenders

Managed Detection and Response: Cybersecurity as a Service

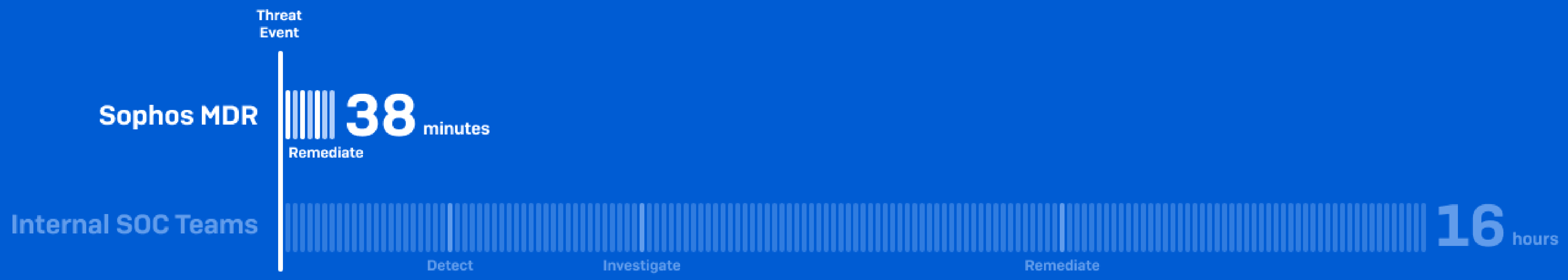
MANAGED DETECTION AND RESPONSE

Superior security outcomes delivered as a service



- ✓ Instant Security Operations Center (SOC)
- ✓ 24/7 Threat Detection and Response
- ✓ Expert-Led Threat Hunting
- ✓ Full-Scale Incident Response Capabilities
- ✓ Superior Cybersecurity Outcomes

Sophos MDR responds to threats 96% faster than internal security teams



*AV-Test 2021 average score; Sophos Managed Threat Response current performance metrics

Sophos MDR Telemetry Sources

Microsoft Security Event Sources

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- O365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity
- **Non-Microsoft Telemetry Sources**

Sophos

XDR Sophos XDR · Fw Sophos Firewall · Cld Sophos Cloud · NDR Sophos NDR · Em Sophos Email · Ep Sophos Endpoint

Endpoint

Symantec (A Division of Broadcom), CrowdStrike, SentinelOne, Trend Micro, BlackBerry Cylance

Firewall

paloalto networks, Fortinet, Check Point, Cisco, SonicWall, WatchGuard

Network

Darktrace, Thinkst Canary, Vectra

Email

mimecast, proofpoint

Identity

okta, Duo, ManageEngine

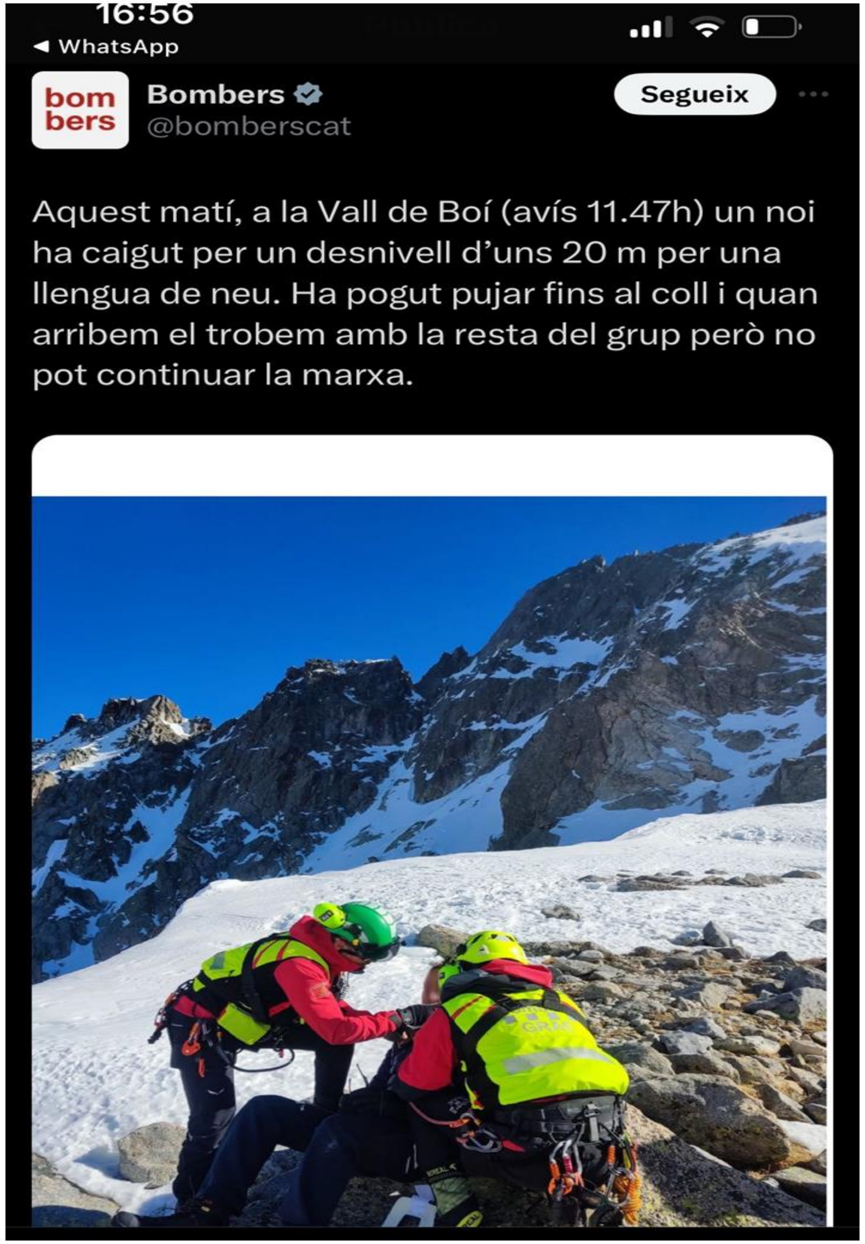
Public Cloud

aws, orca security

Productivity

Google Workspace

Sophos, Microsoft, Endpoint, and Productivity Integrations are included at no additional cost.
Other integration packs are chargeable add-ons.



Bombers
@bomberscat

Aquest matí, a la Vall de Boí (avís 11.47h) un noi ha caigut per un desnivell d'uns 20 m per una llengua de neu. Ha pogut pujar fins al coll i quan arribem el trobem amb la resta del grup però no pot continuar la marxa.

SOPHOS