La carrera en ciberseguridad o el efecto de la reina Roja

Javier Huito Pacheco
Enterprise Account Executive
Javier.huito@Sophos.com

SOPHOS

Ayuntamiento de Sevilla
@Ayto_Sevilla

🔴 AVISO IMPORTANTE 📣 El Ayuntamiento se ha visto afectado por un

Diario de Sevilla

REGÍSTRATE | INICIAR SESIÓN

El Ayuntamiento de Sevilla sigue sin gestión on line dos semanas después del ciberataque

SERVICIOS PÚBLICOS

El Ayuntamiento de Sevilla sigue sin gestión on line dos semanas después del ciberataque

- No hay aún fecha definitiva para la recuperación plena de los servicios telemáticos
- La web municipal y la plataforma de atención ciudadana en los distritos continúan sin funcionar
- El Ayuntamiento de Sevilla reanuda los trámites presenciales tras el ciberataque

El Ayuntamiento de Sevilla sigue sufriendo los efectos del ciberataque ocurrido hace dos semanas. / D. S.

DIEGO J. GENIZ
20 Septiembre, 2023 - 06:15h

4:03 PM · Sep 5, 2023 · **139K** Views

SOPHOS

LOCKBIT 3.0

LEAKED DATA

TWITTER › | HOW TO BUY BITCOIN › | CONTACT US ›

PRESS ABOUT US › | AFFILIATE RULES › | MIRRORS ›

UNTIL FILES

16D18H20M43S

PUBLICATION

Deadline: 26 Nov, 2022 11:11:28 UTC

[redacted]

[redacted]

We advise you to pay to remove the data =) Also in the leak will have access to the company itself.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 05 NOV, 2022 15:06 UTC UPDATED: 06 NOV, 2022 21:09 UTC

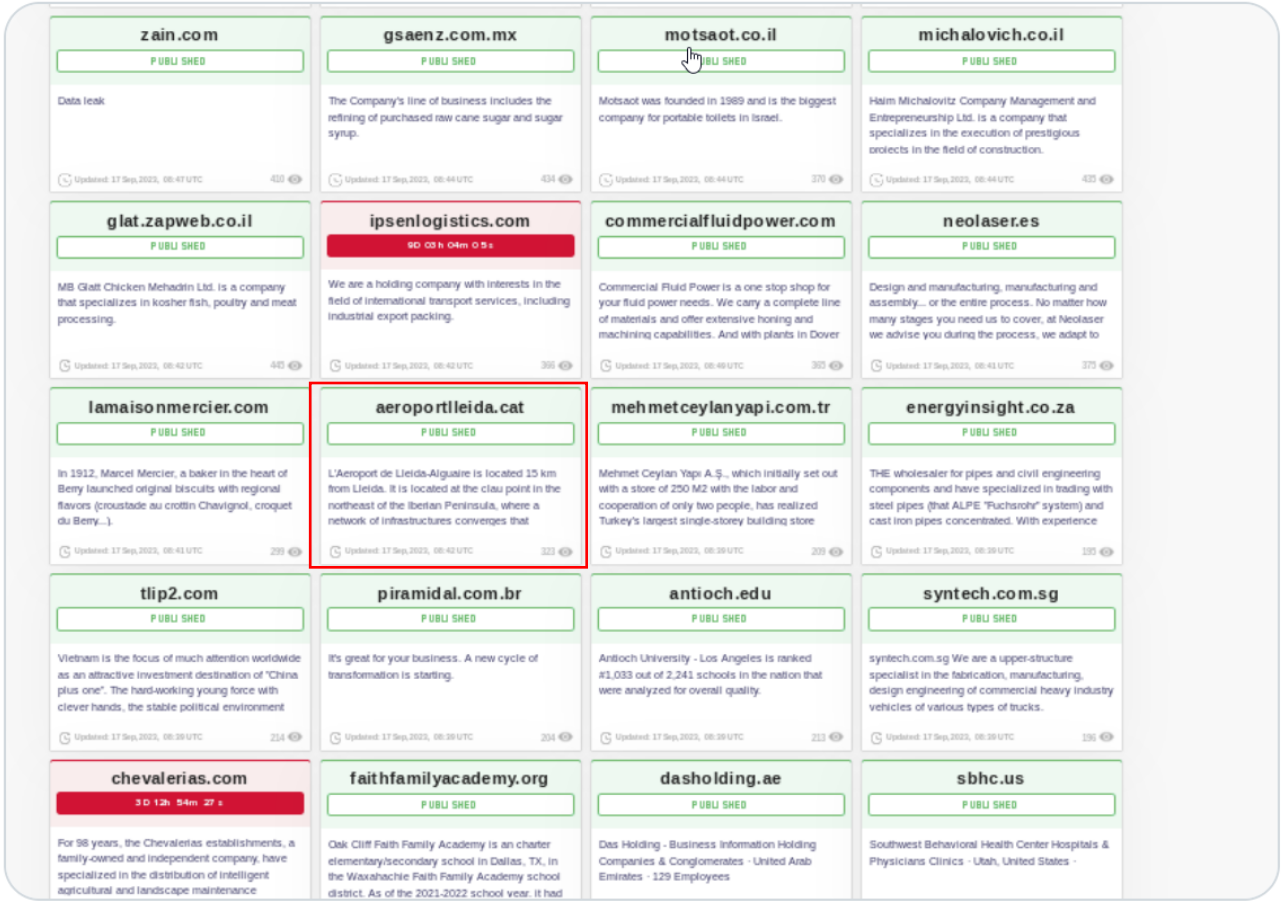
EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 10000	$ 2000000	$ 2000000

SOPHOS

FalconFeedsio
@FalconFeedsio

LockBit #ransomware group has added 23 victims to their #darkweb portal.

#lockbit
#DeepWeb #CyberRisk #ThreatIntelligence #CTI



11:53 AM · Sep 17, 2023 · **22K** Views

SOPHOS

Sophos X-Ops

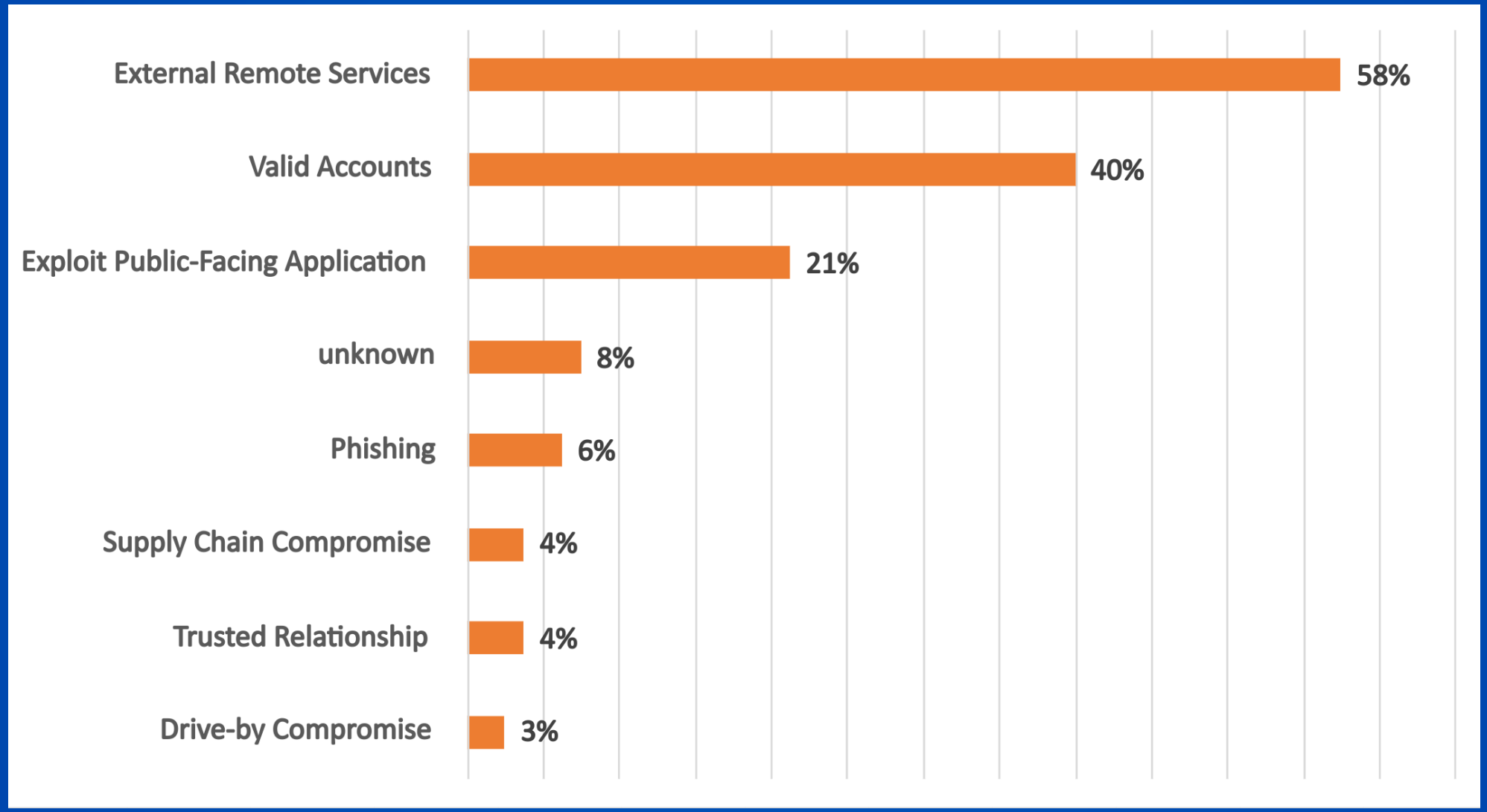
The 2023 Active Adversary Report for Tech Leaders

SOPHOS

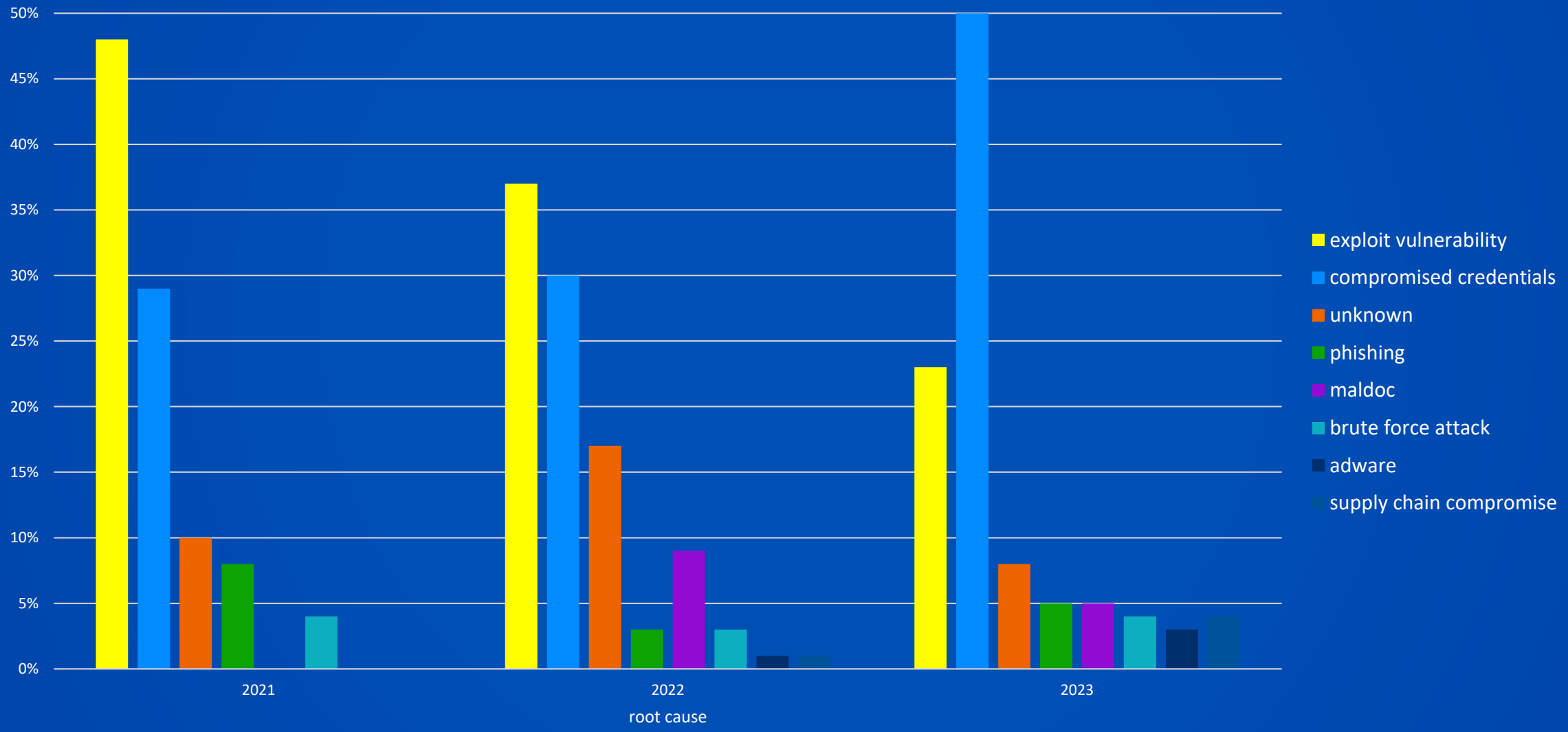
Tipos de ataques

	2022	1H2023
Ransomware	68.42%	68.75%
Network Breach	18.42%	16.25%
Data Extortion	3.29%	8.75%
Data Exfiltration	3.29%	2.50%
Web Shell	2.63%	1.25%
DDoS	—	1.25%
Loader	3.29%	1.25%

Acceso Inicial – IAB

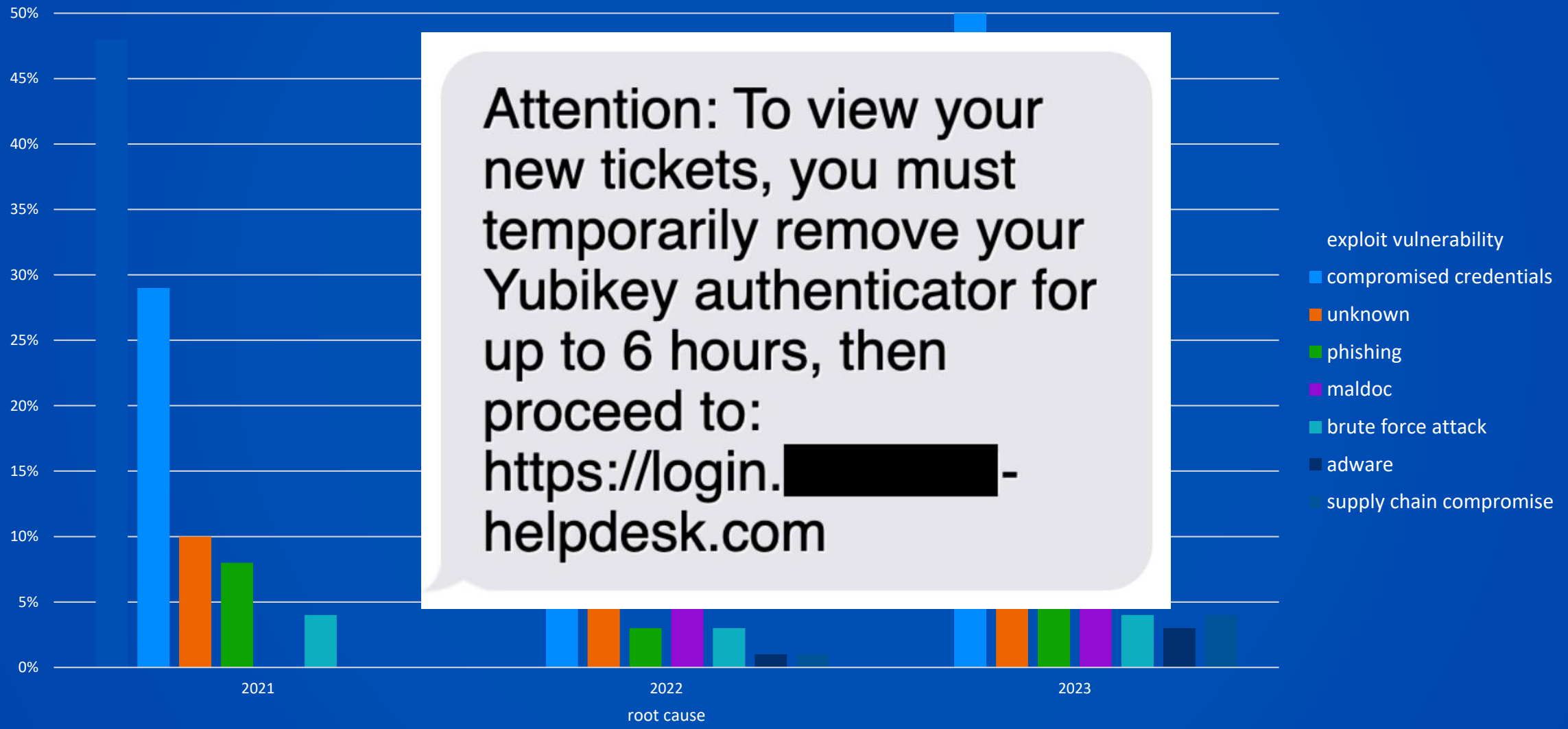


Causa raiz



SOPHOS

Causa raiz



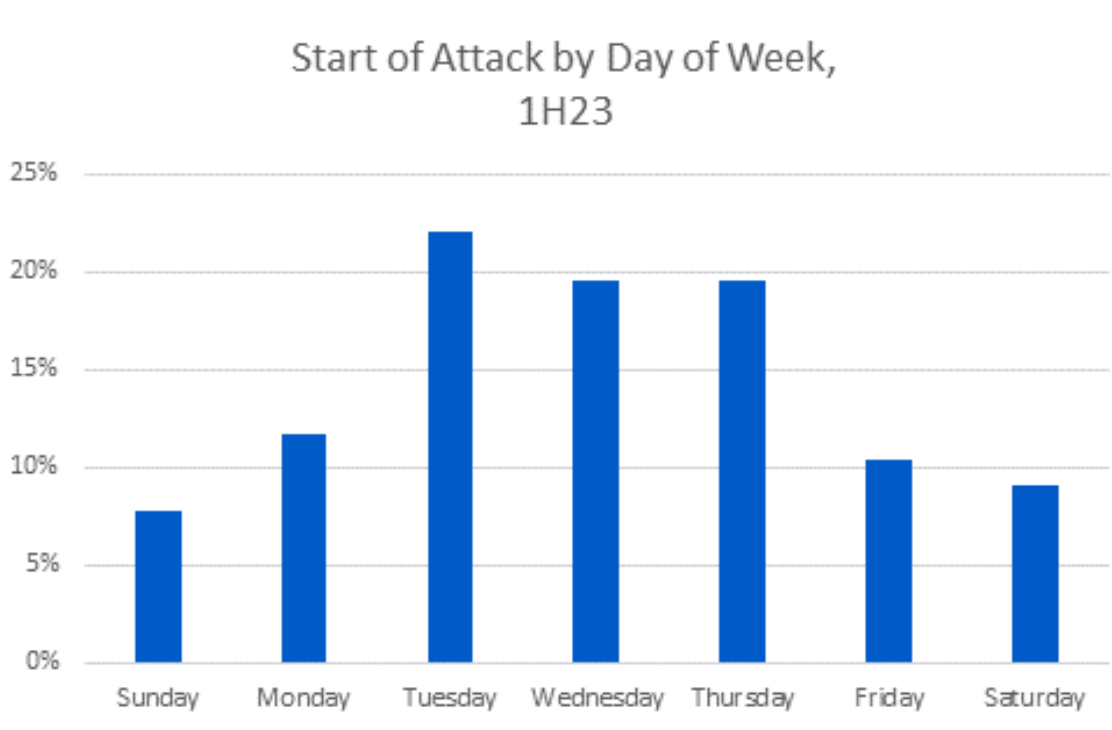
https://sec.okta.com/articles/2023/07/unexpected-endorsement-webauthn

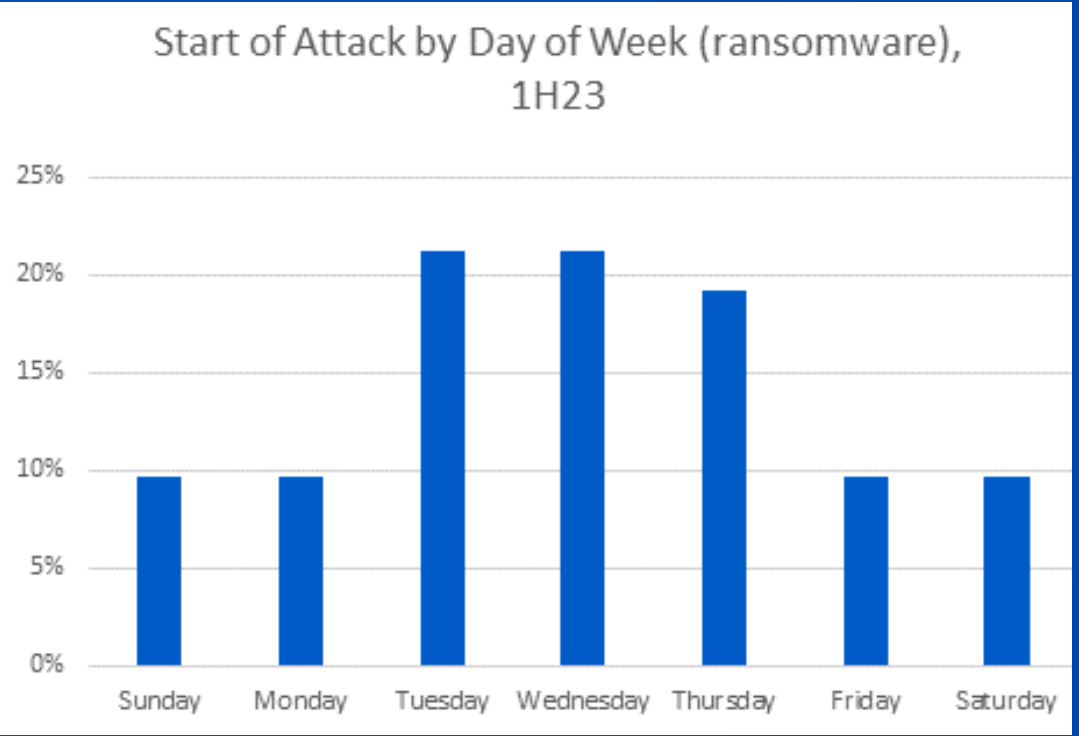
Ransomware dwell time

Ransomware dwell time

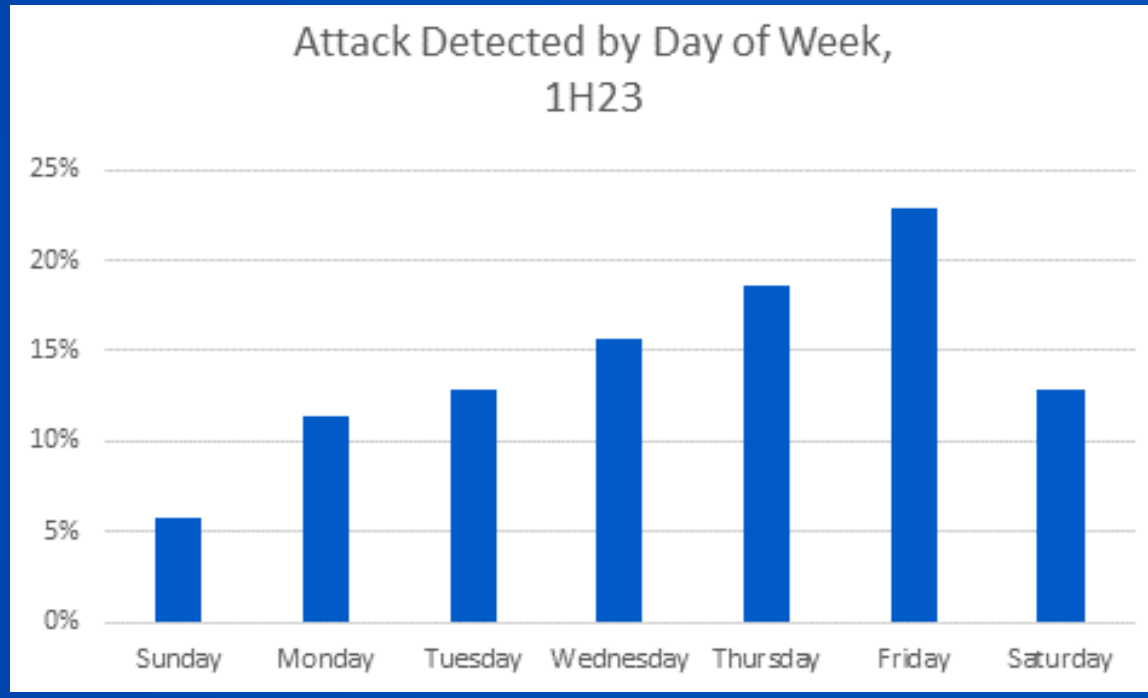
2020	2021	2022	1H23
18 days	11 days	9 days	5 days

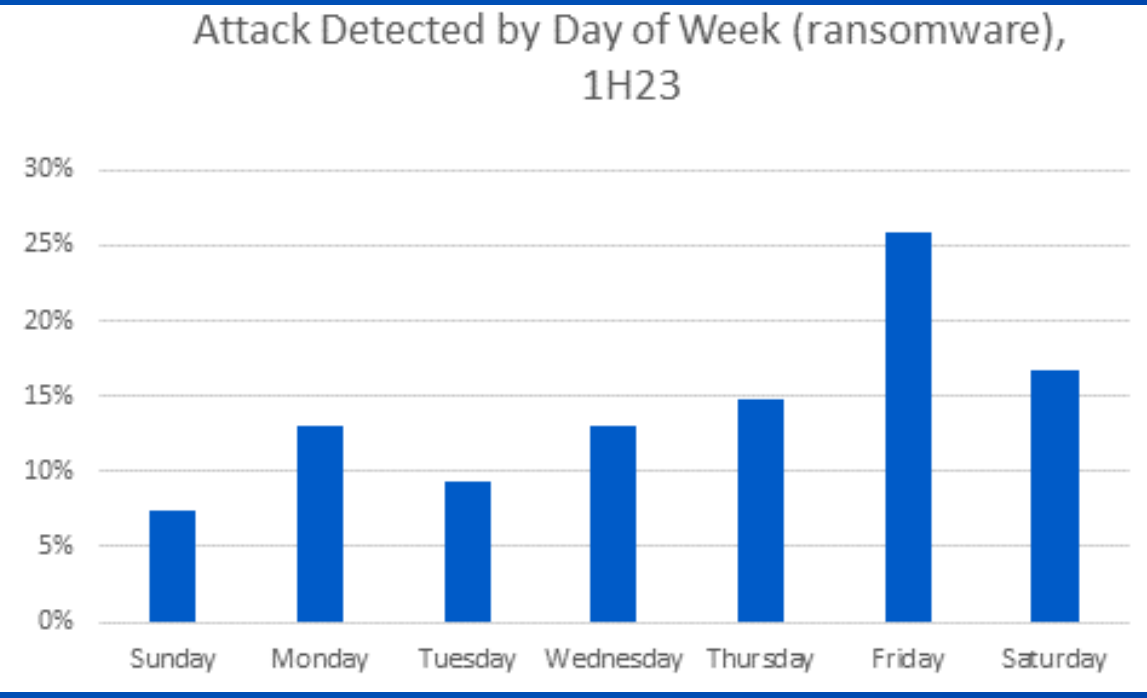
Start of attack – local time





Attack detected – local time





Attribution

	2022	1H2023
LockBit	15.38%	14.55%
AlphaVM/BlackCat	12.50%	12.73%
Royal	3.85%	10.91%
Play	2.88%	7.27%
CryTOX	.96%	7.27%
Black Basta	.96%	7.27%
Akira	(did not chart)	5.45%

La "orquídea de Darwin", *Angraecum sesquipedale*

THE

VARIOUS CONTRIVANCES

BY WHICH

ORCHIDS ARE FERTILISED BY INSECTS.

By CHARLES DARWIN, M.A., F.R.S., &c.

SECOND EDITION, REVISED.

WITH ILLUSTRATIONS.

NEW YORK:
D. APPLETON AND COMPANY,
549 AND 551 BROADWAY.
1877.

La "orquídea de Darwin", *Angraecum sesquipedale*

SOPHOS

Polilla de halcón, *Xanthopan morganii praedicta*

SOPHOS

Lewis Carrol, *Alicia a través del espejo, 1872*

«Alicia miró alrededor suyo con gran sorpresa.

-Pero ¿cómo? ¡Si parece que hemos estado bajo este árbol todo el tiempo! ¡Todo está igual que antes!

-¡Pues claro que sí! -convino la Reina-. Y, ¿cómo si no?

-Bueno, lo que es en mi país -aclaró Alicia, jadeando aún bastante, cuando se corre tan rápido como lo hemos estado haciendo y durante algún tiempo, se suele llegar a alguna otra parte…

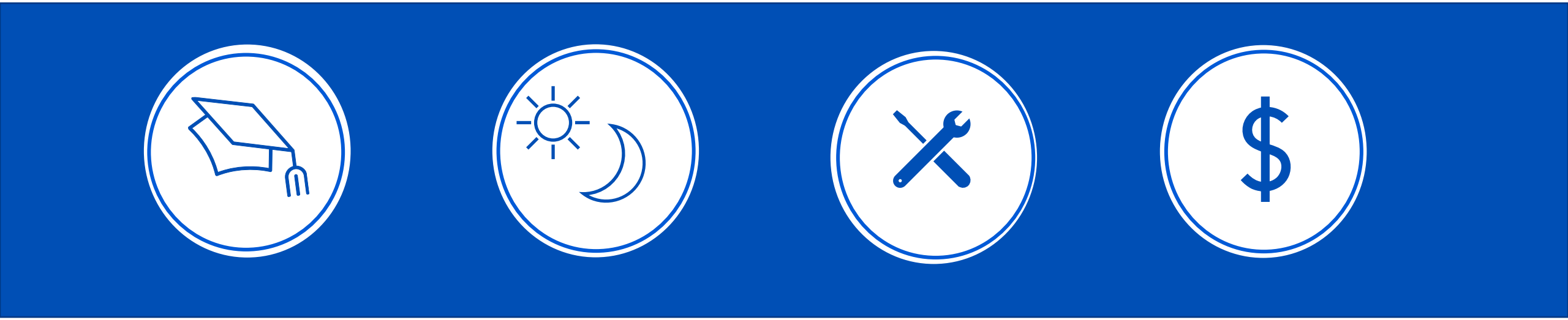
-¡Un país bastante lento! -replicó la Reina-. Lo que es aquí, como ves, hace falta correr todo cuanto una pueda para permanecer en el mismo sitio. Si se quiere llegar a otra parte hay que correr por lo menos dos veces más rápido.»

Lewis Carrol, *Alicia a través del espejo, 1872*

SOPHOS

SOPHOS

La ciberseguridad se ha vuelto compleja para que la mayoría de las organizaciones puedan gestionarla con eficacia.



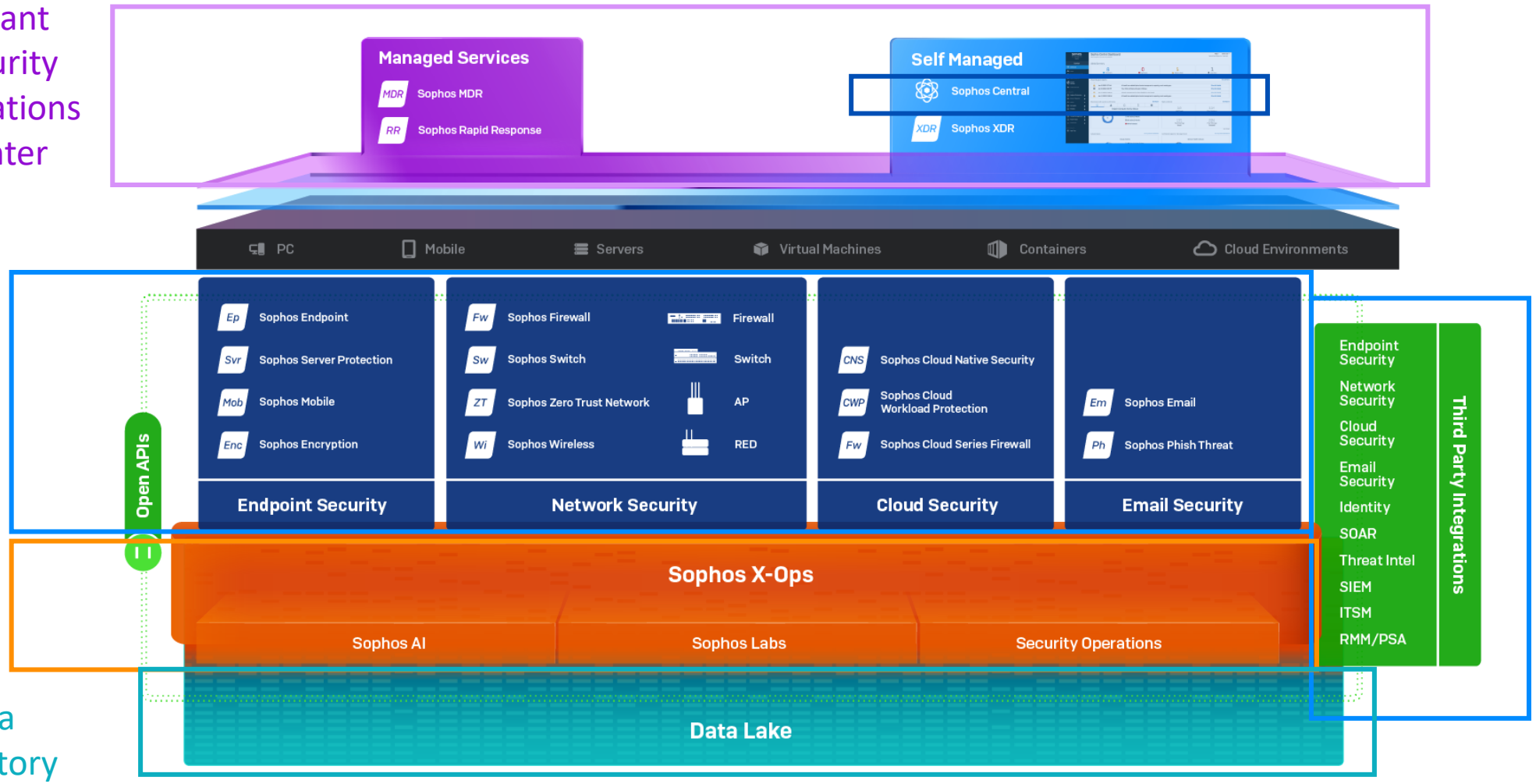
SOPHOS

La ciberseguridad se ha vuelto compleja para que la mayoría de las organizaciones puedan gestionarla con eficacia.

Los servicios de ciberseguridad proporcionan los conocimientos técnicos necesarios las 24 horas del día para adelantarse a los ataques avanzados de hoy en día.

Cloud-based security platform

Instant Security Operations Center



SOPHOS

Sophos MDR: Industry-Leading Openness and Flexibility

Sophos MDR

Compatible con su entorno

Podemos utilizar nuestras herramientas, las de otro proveedor o cualquier combinación de ambas.

Compatible con sus necesidades

Tanto si necesita una respuesta completa a incidentes como ayuda para tomar decisiones más precisas

Compatible con su empresa

Nuestro equipo tiene una amplia experiencia en la caza de amenazas dirigidas a organizaciones de todos los sectores.

Sophos

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

Endpoint

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

Firewall

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

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, Duo, ManageEngine

Network

Darktrace, Thinkst Canary, Skyhigh Security, Vectra

24x7 Coverage from Seven Global SOCs

SOPHOS

Sophos MDR

Threat Hunting

Las búsquedas proactivas de amenazas realizadas por analistas altamente cualificados descubren y eliminan rápidamente más amenazas de las que los productos de seguridad pueden detectar por sí solos.

Threat Detection

Gracias a las funciones de detección y respuesta ampliadas (XDR), que detectan amenazas conocidas y comportamientos potencialmente maliciosos dondequiera que residan sus datos.

Incident Response

Nuestros analistas responden a las amenazas en cuestión de minutos, tanto si necesita una respuesta completa a incidentes como si necesita ayuda para tomar decisiones más precisas.

18,000+ Clientes MDR

99.98% de las amenazas bloqueadas automáticamente*

Tiempos medios de respuesta a amenazas de Sophos MDR

Time to Detect	Less than 1 Minute
Time to Investigate	Less than 25 Minutes
Time to Respond	Less than 12 Minutes

Líderes en servicios de ciberseguridad

El proveedor de MDR más fiable

18,000+

Clientes MDR

Más organizaciones confían en Sophos para MDR que en cualquier otro proveedor

Proveedor MDR mejor valorado

4.8/5

En MDR

Sophos es el servicio MDR mejor valorado y más revisado en Gartner Peer Insights

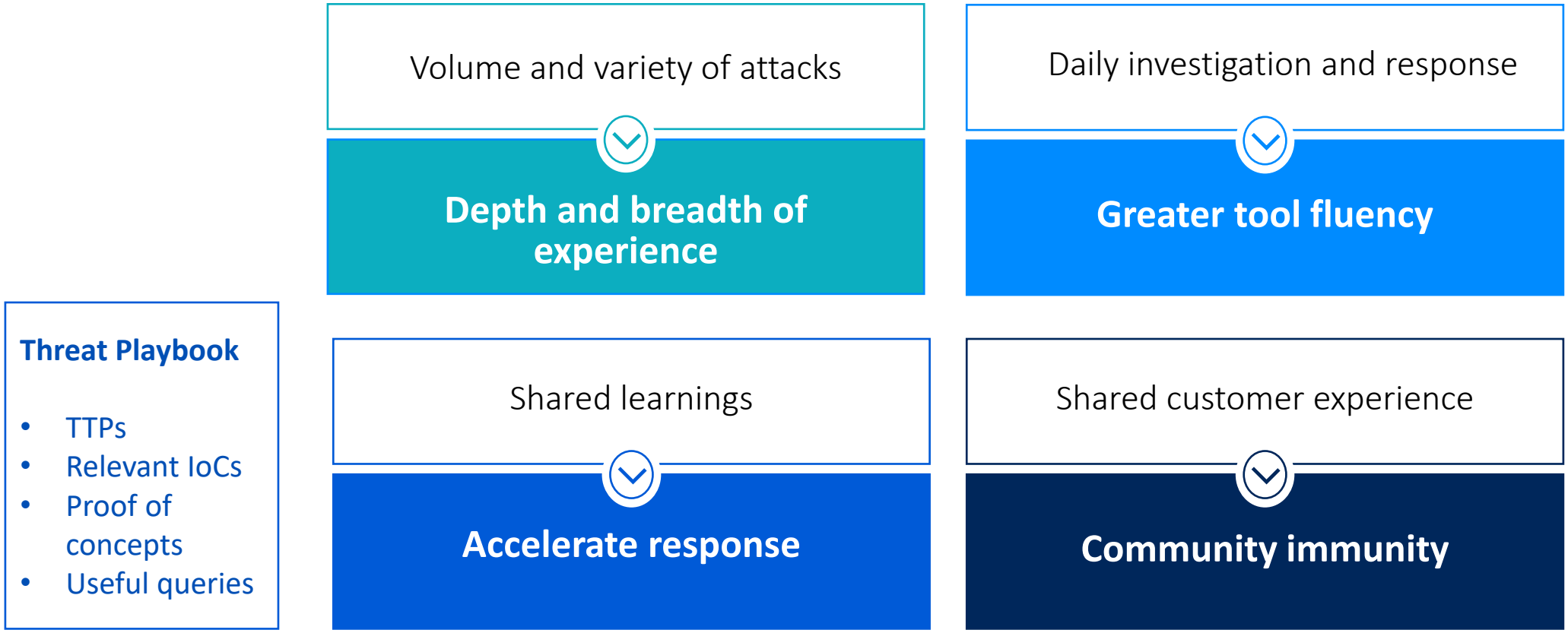
Protección validada por el sector

MITRE

SE Labs

AV-TEST

24/7/365 Ransomware y prevención de brechas



The Sophos Breach Protection Warranty covers up to $1 million in response expenses

We're introducing a breach protection warranty with **Sophos MDR Complete**

The warranty will be included with all **1-, 2- and 3-year license purchases**, new and renew

Customers enjoy **comprehensive coverage**: endpoints, servers, Windows, macOS, no geographic limits

The warranty is **underwritten by Sophos**, demonstrating our confidence in our protection

The Sophos Advantage: MDR and Cybersecurity

More organizations trust Sophos for MDR than any other vendor in the world.

- The **largest provider** of Managed Detection and Response Services (MDR)
- The **highest rated** and **most reviewed** MDR service on Gartner Peer Insights
- The **top-rated** MDR service on G2
- Industry-leading **compatibility** with virtually any environment or tech stack
- **The most expansive** portfolio of world-class products and managed security services

SOPHOS

Cybersecurity delivered.

Javier Huito Pacheco
Enterprise Account Executive
Javier.huito@Sophos.com