

La carrera en ciberseguridad o el efecto de la reina Roja

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

SOPHOS

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



UNTIL FILES

16D18H20M43S

PUBLICATION

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



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

\$ 10000

DESTROY ALL INFORMATION

\$ 2000000

DOWNLOAD DATA AT ANY MOMENT

\$ 2000000

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

#lockbit
#DeepWeb #CyberRisk #ThreatIntelligence #CTI

<p>zain.com PUBLISHED</p> <p>Data leak</p> <p>Updated: 17 Sep, 2023, 08:47 UTC 433</p>	<p>gsaenz.com.mx PUBLISHED</p> <p>The Company's line of business includes the refining of purchased raw cane sugar and sugar syrup.</p> <p>Updated: 17 Sep, 2023, 08:44 UTC 434</p>	<p>motsaot.co.il PUBLISHED</p> <p>Motsaot was founded in 1989 and is the biggest company for portable toilets in Israel.</p> <p>Updated: 17 Sep, 2023, 08:44 UTC 370</p>	<p>michalovich.co.il PUBLISHED</p> <p>Haim Michalovitz Company Management and Entrepreneurship Ltd. is a company that specializes in the execution of prestigious projects in the field of construction.</p> <p>Updated: 17 Sep, 2023, 08:44 UTC 423</p>
<p>glat.zapweb.co.il PUBLISHED</p> <p>MB Glat Chicken Mehadim Ltd. is a company that specializes in kosher fish, poultry and meat processing.</p> <p>Updated: 17 Sep, 2023, 08:42 UTC 443</p>	<p>ipsenlogistics.com 3D 03h 04m 09s</p> <p>We are a holding company with interests in the field of international transport services, including industrial export packing.</p> <p>Updated: 17 Sep, 2023, 08:42 UTC 356</p>	<p>commercialfluidpower.com PUBLISHED</p> <p>Commercial Fluid Power is a one stop shop for your fluid power needs. We carry a complete line of materials and offer extensive honing and machining capabilities. And with plants in Dover</p> <p>Updated: 17 Sep, 2023, 08:40 UTC 303</p>	<p>neolaser.es PUBLISHED</p> <p>Design and manufacturing, manufacturing and assembly... or the entire process. No matter how many stages you need us to cover, at Neolaser we advise you during the process, we adapt to</p> <p>Updated: 17 Sep, 2023, 08:41 UTC 373</p>
<p>lamaisonmercier.com PUBLISHED</p> <p>In 1912, Marcel Mercier, a baker in the heart of Berry launched original biscuits with regional flavors (croustade au crottin Chavignol, croquet du Berry...)</p> <p>Updated: 17 Sep, 2023, 08:41 UTC 289</p>	<p>aeroportlleida.cat PUBLISHED</p> <p>L'Aeroport de Lleida-Alguaire is located 15 km from Lleida. It is located at the clau point in the northeast of the Iberian Peninsula, where a network of infrastructures converges that</p> <p>Updated: 17 Sep, 2023, 08:42 UTC 323</p>	<p>mehmetceylanapi.com.tr PUBLISHED</p> <p>Mehmet Ceylan Yapi A.Ş., which initially set out with a store of 250 M2 with the labor and cooperation of only two people, has realized Turkey's largest single-storey building store</p> <p>Updated: 17 Sep, 2023, 08:39 UTC 209</p>	<p>energyinsight.co.za PUBLISHED</p> <p>THE wholesaler for pipes and civil engineering components and have specialized in trading with steel pipes (that ALPE "Fuchsrohr" system) and cast iron pipes concentrated. With experience</p> <p>Updated: 17 Sep, 2023, 08:39 UTC 133</p>
<p>tlip2.com PUBLISHED</p> <p>Vietnam is the focus of much attention worldwide as an attractive investment destination of "China plus one". The hard-working young force with clever hands, the stable political environment</p> <p>Updated: 17 Sep, 2023, 08:39 UTC 214</p>	<p>piramidal.com.br PUBLISHED</p> <p>It's great for your business. A new cycle of transformation is starting.</p> <p>Updated: 17 Sep, 2023, 08:39 UTC 204</p>	<p>antioch.edu PUBLISHED</p> <p>Antioch University - Los Angeles is ranked #1,033 out of 2,241 schools in the nation that were analyzed for overall quality.</p> <p>Updated: 17 Sep, 2023, 08:39 UTC 213</p>	<p>syntech.com.sg PUBLISHED</p> <p>syntech.com.sg We are an upper-structure specialist in the fabrication, manufacturing, design engineering of commercial heavy industry vehicles of various types of trucks.</p> <p>Updated: 17 Sep, 2023, 08:39 UTC 136</p>
<p>chevalerias.com 3D 12h 54m 27s</p> <p>For 98 years, the Chevalerias establishments, a family-owned and independent company, have specialized in the distribution of intelligent agricultural and landscape maintenance</p>	<p>faithfamilyacademy.org PUBLISHED</p> <p>Oak Cliff Faith Family Academy is an charter elementary/secondary school in Dallas, TX, in the Waxahachie Faith Family Academy school district. As of the 2021-2022 school year, it had</p>	<p>dasholding.ae PUBLISHED</p> <p>Das Holding - Business Information Holding Companies & Conglomerates - United Arab Emirates - 129 Employees</p>	<p>sbhc.us PUBLISHED</p> <p>Southwest Behavioral Health Center Hospitals & Physicians Clinics - Utah, United States</p>



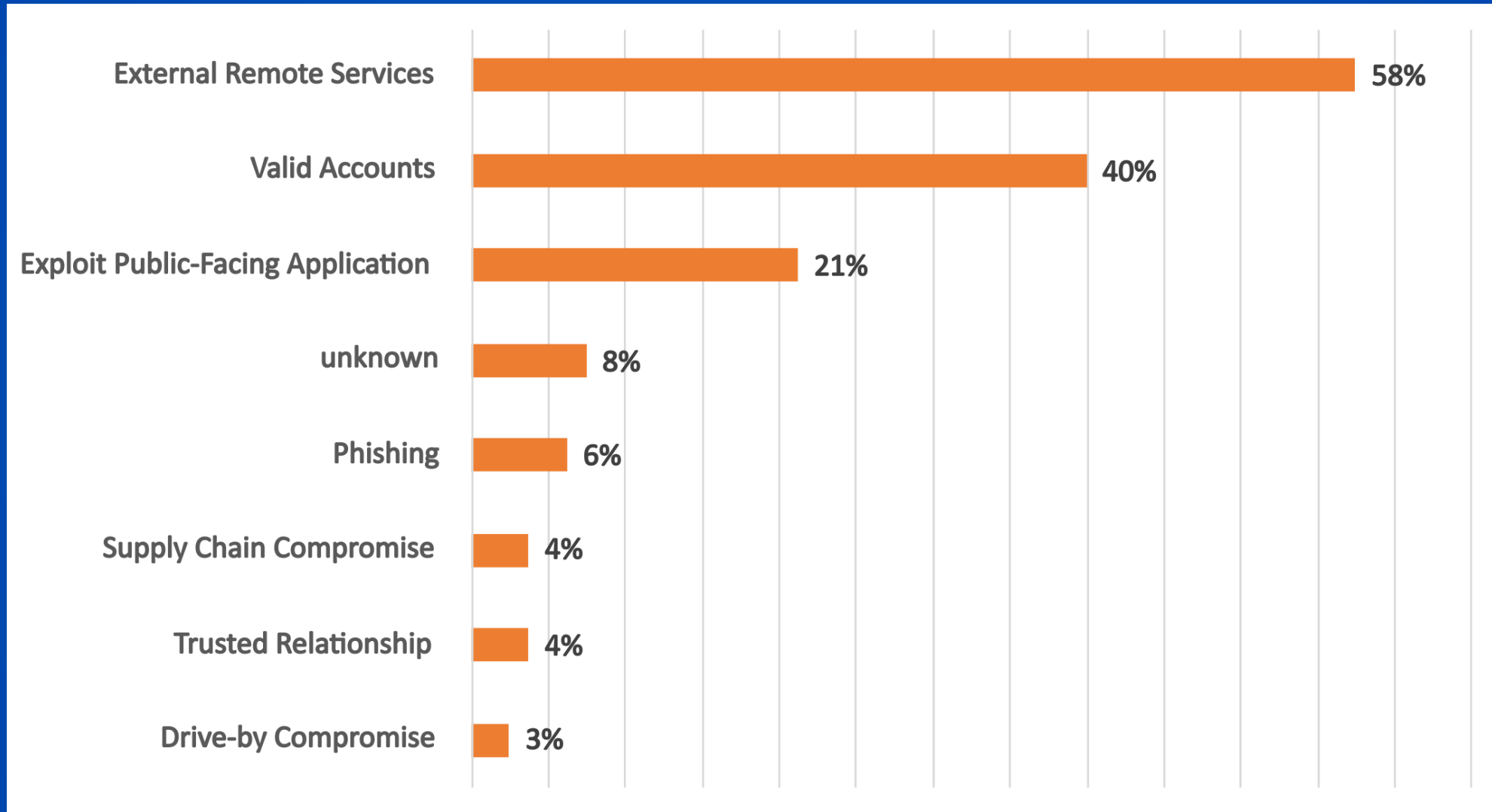
The 2023 Active Adversary Report for Tech Leaders



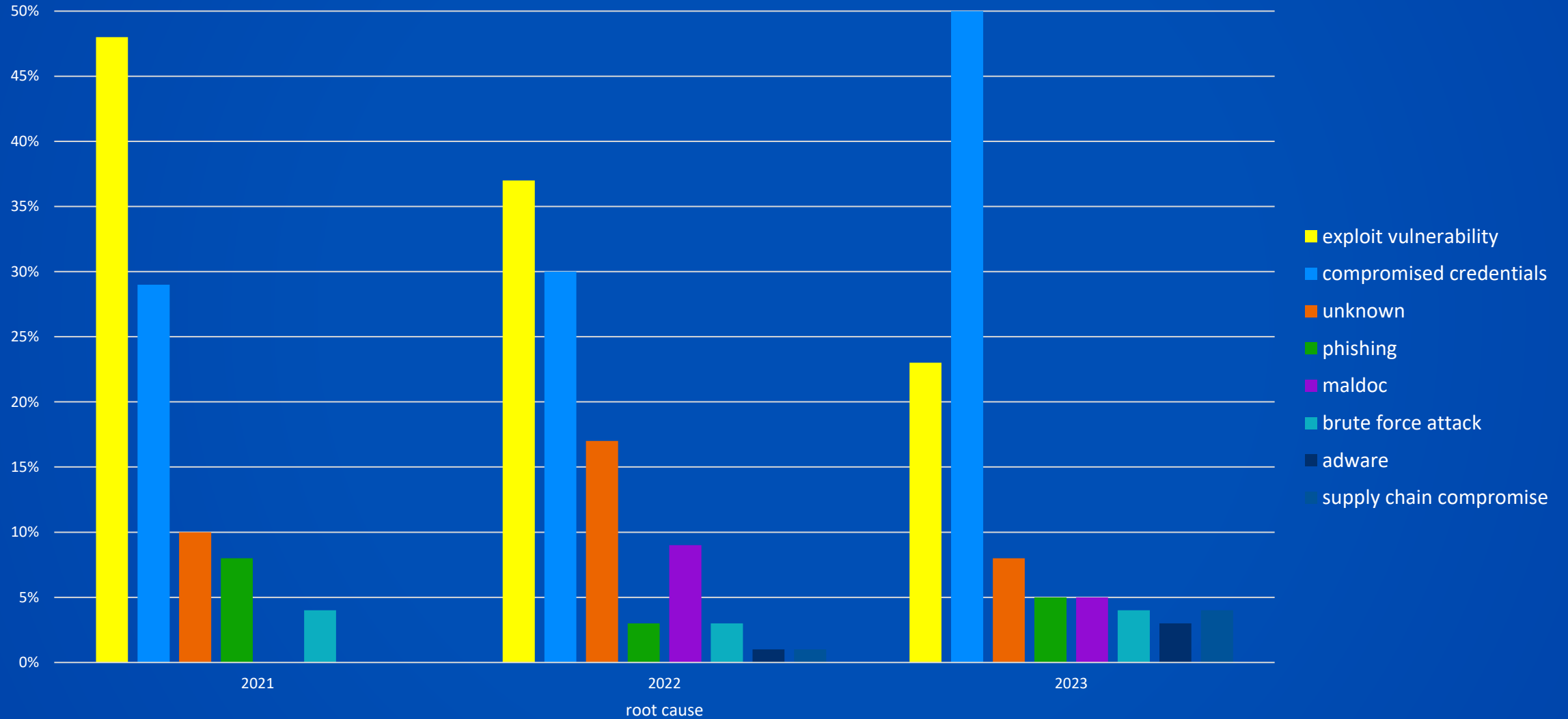
Tipos de ataques

	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%

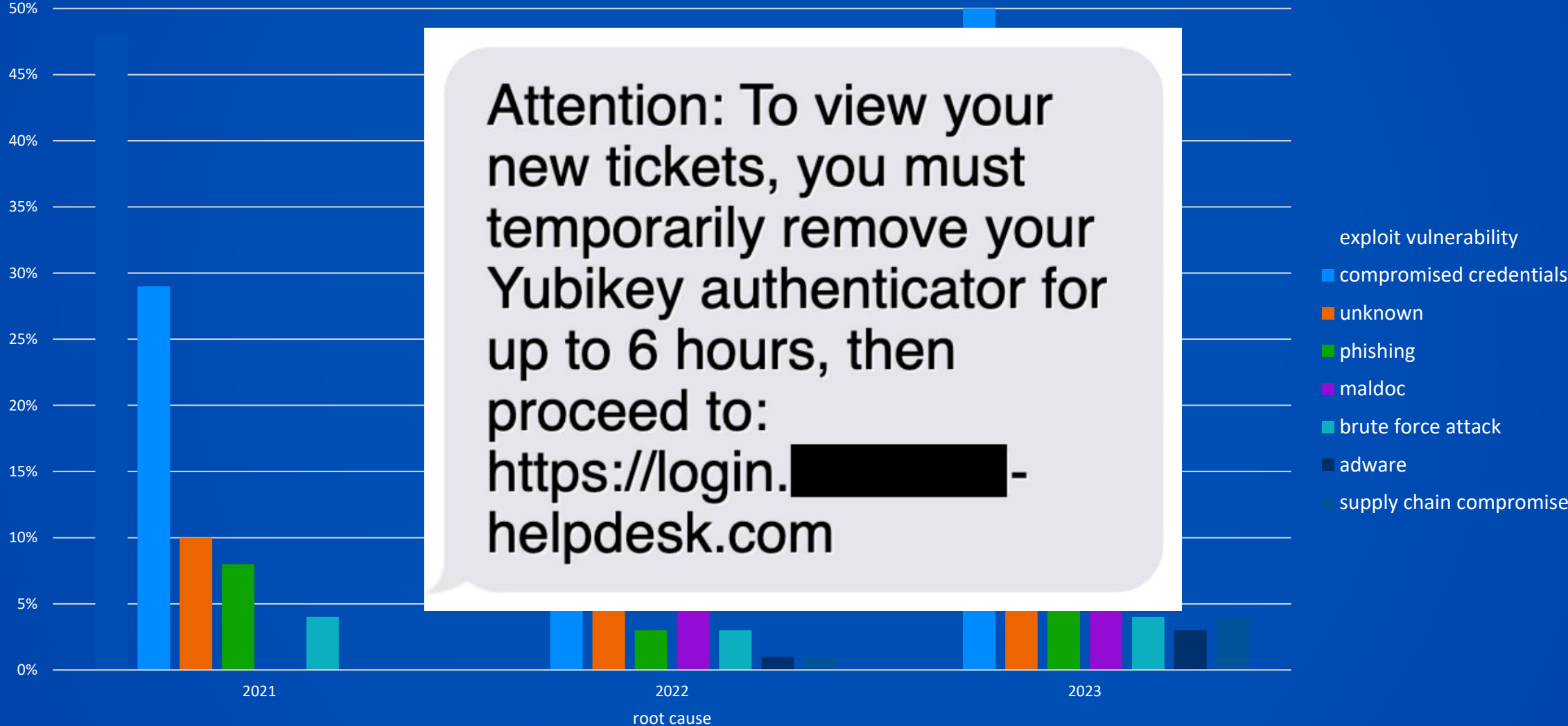
Acceso Inicial – IAB



Causa raiz



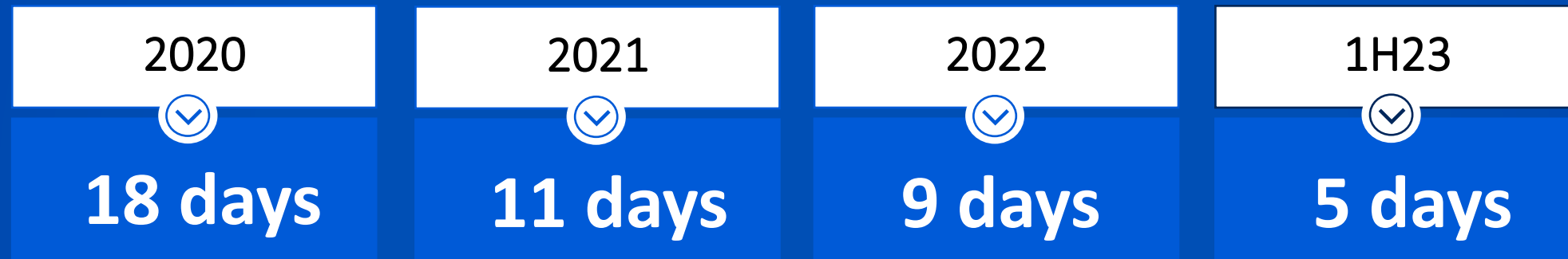
Causa raiz



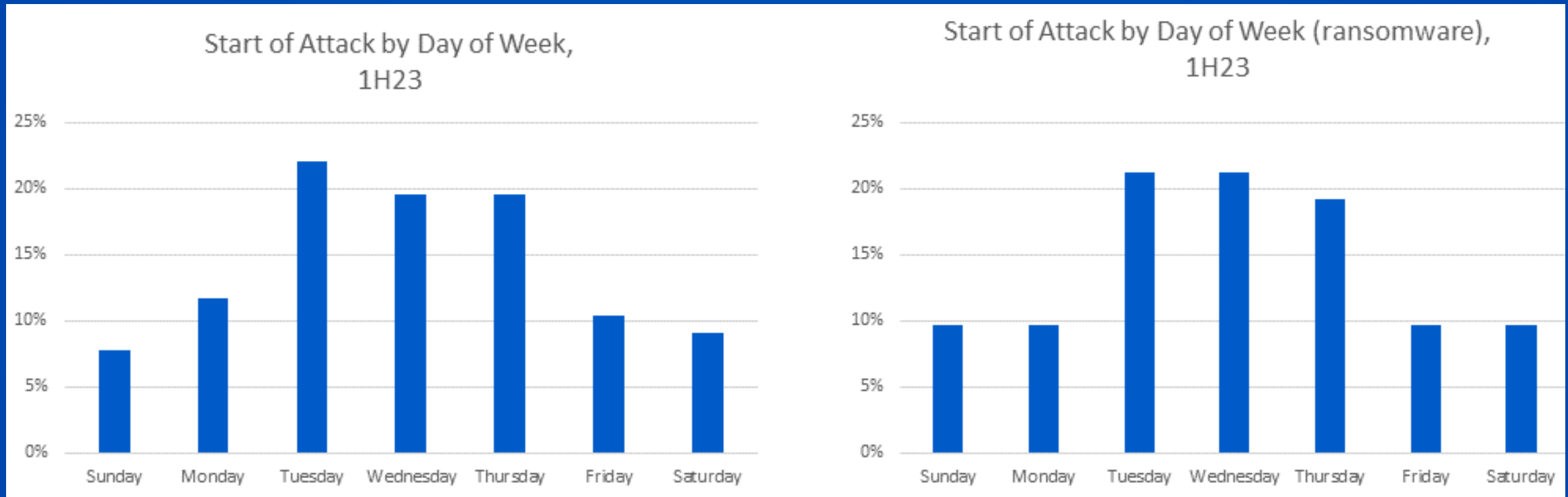
Ransomware dwell time



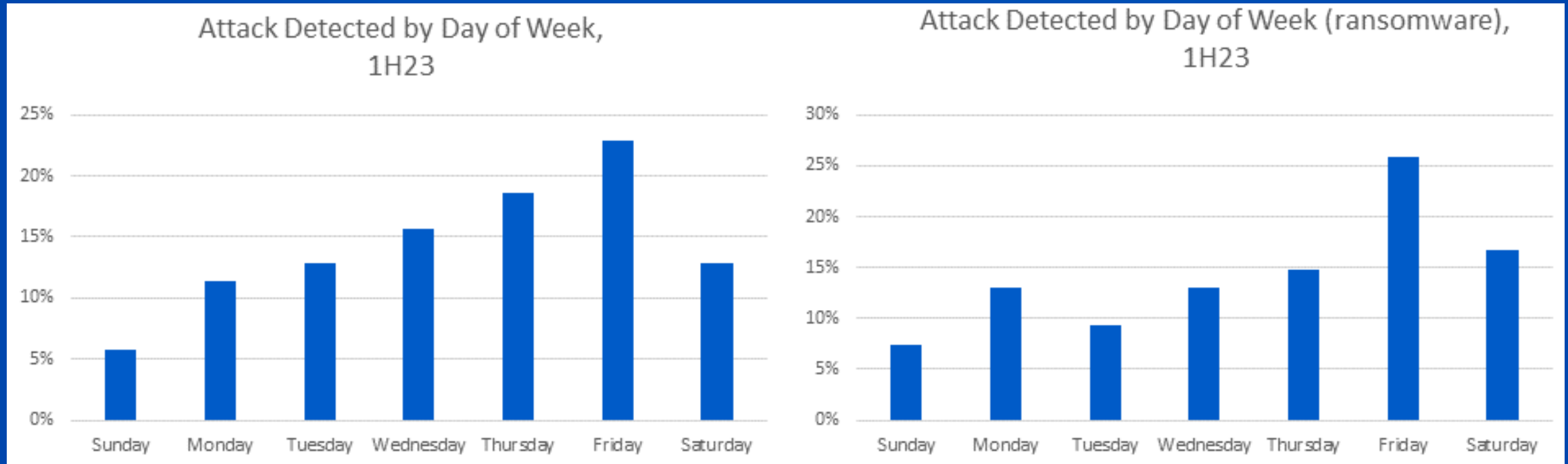
Ransomware dwell time



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*



Polilla de halcón, *Xanthopan morgani praedicta*





Lewis Carroll, *Through the Looking Glass, and what Alice found there*, Macmillan & Co., 1872 © Macmillan & Co Ltd. © Thanks to Macmillan Children's Books

«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.»





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

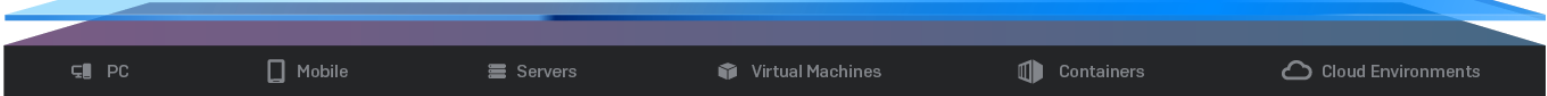


La ciberseguridad se ha vuelto compleja para que la mayoría de las organizaciones puedan gestionarla con eficacia.

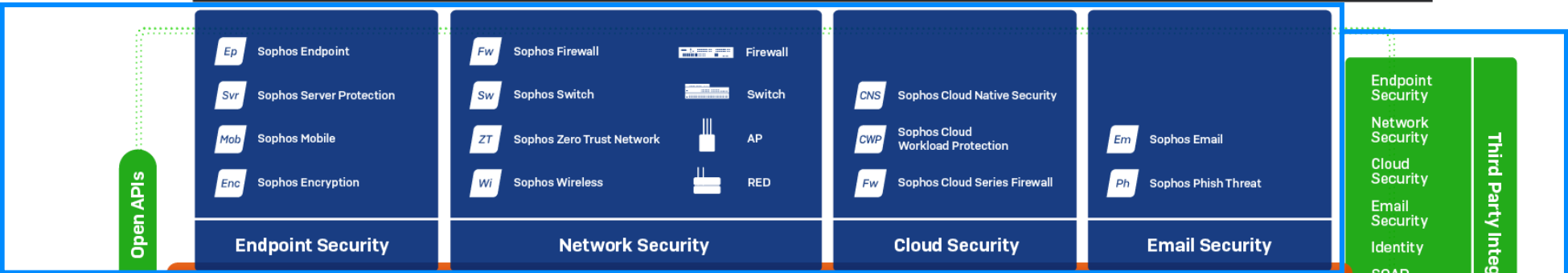
Los servicios de ciberseguridad proporcionan los conocimientos técnicos necesarios las 24 horas del día para adelantarse a los ataques avanzados de hoy en día.

Cloud-based security platform

Instant Security Operations Center



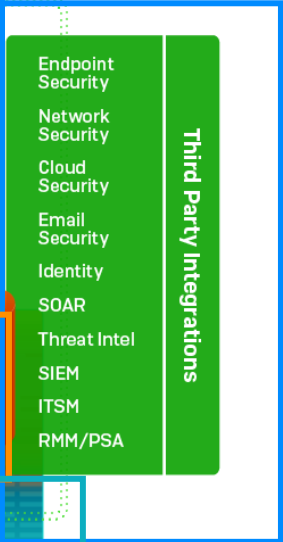
Integrated cyber defenses



Expert team



Data repository



Sophos MDR: Industry-Leading Openness and Flexibility

Sophos

XDR Sophos XDR Fw Sophos Firewall ClD Sophos Cloud NDR Sophos NDR Em Sophos Email Ep Sophos Endpoint



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.

Endpoint

Firewall

Cloud SaaS

Email

Identity

Network

24x7 Coverage from Seven Global SOCs





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

AVTEST

24/7/365 Ransomware y prevención de brechas

Volume and variety of attacks



Depth and breadth of experience

Daily investigation and response



Greater tool fluency

Shared learnings



Accelerate response

Shared customer experience



Community immunity

Threat Playbook

- TTPs
- Relevant IoCs
- Proof of concepts
- Useful queries

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



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