Il Panorama della Cybersecurity nel 2023

Giovanni Giovannelli
Senior Sales Engineer @SOPHOS

24 Maggio 2023

SOPHOS
Cybersecurity delivered.

Sophos in due parole

- Leader mondiale nei servizi di cyber-sicurezza e nella sicurezza degli endpoint, delle reti e del cloud
- 4.100 dipendenti
- Oltre 1.1 miliardi di dollari di fatturato
- Oltre 554.000 Clienti che si affidano alle nostre soluzioni
- Oltre 100 milioni di Utenti protetti
- Uno dei provider di servizi di cyber-sicurezza con più crescita al mondo, con oltre 15.000 Clienti
- Suddivisione del mercato: 51% EMEA, 37% America, 12% APJ

Trend Principali

Sophos Threat Report 2023

Il Report studia gli sviluppi criminali e le principali minacce rilevate a livello mondiale nell'anno precedente.

Si parla di Ransomware, crime-as-a-service, metodi per il furto di credenziali, dispositivi mobili e molto altro…

Ciò di cui si parla in questo report impatterà sulle pratiche di sicurezza che verranno intraprese nel 2023

Trend Principali

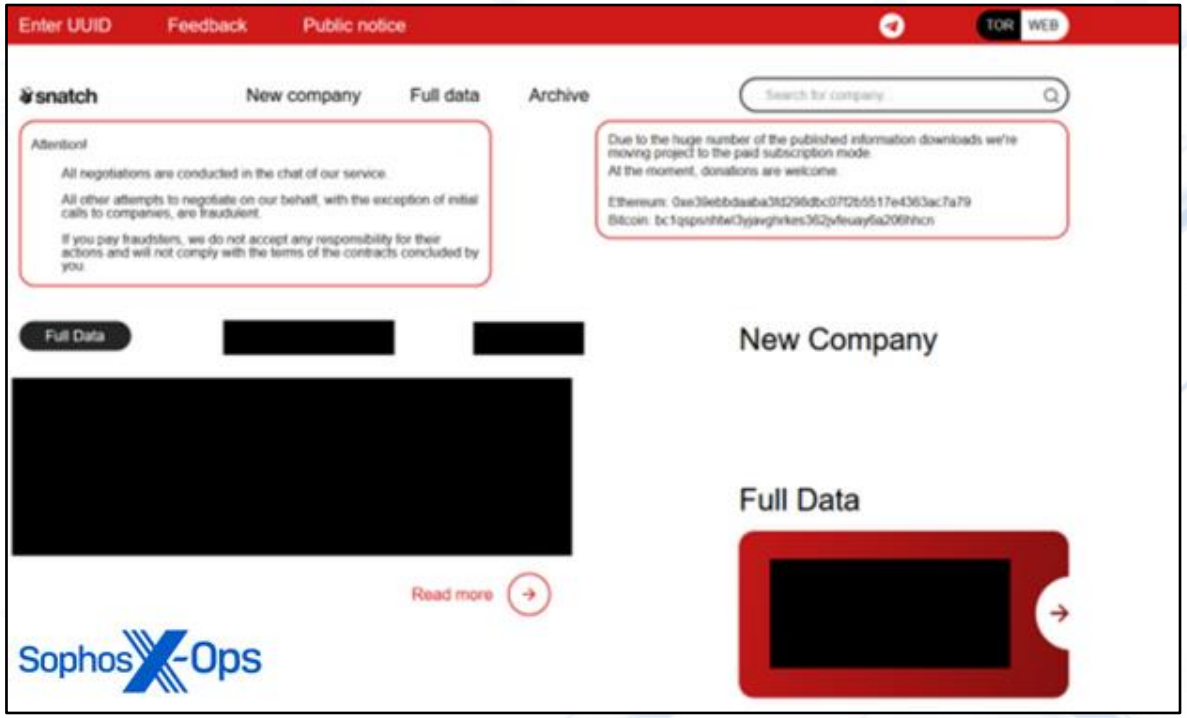
1. I Ransomware continuano ad essere una delle minacce più pericolose, con tecniche di attacco “innovative”
2. Il concetto di “cybercrime-as-a-service“ ha preso definitivamente piede, consentendo a chiunque di diventare un cyber criminale
3. Il furto di informazioni e di credenziali è in crescita
4. I Cyber criminali utilizzano sempre di più strumenti già presenti sui sistemi per lanciare attacchi, rendendo meno efficaci le difese tecnologiche
5. I dispositivi mobili sono al centro di nuovi tipi di attacco e sia i sistemi Android che Apple sono vulnerabili

I Ransomware continuano ad essere una delle minacce più pericolose

SOPHOS

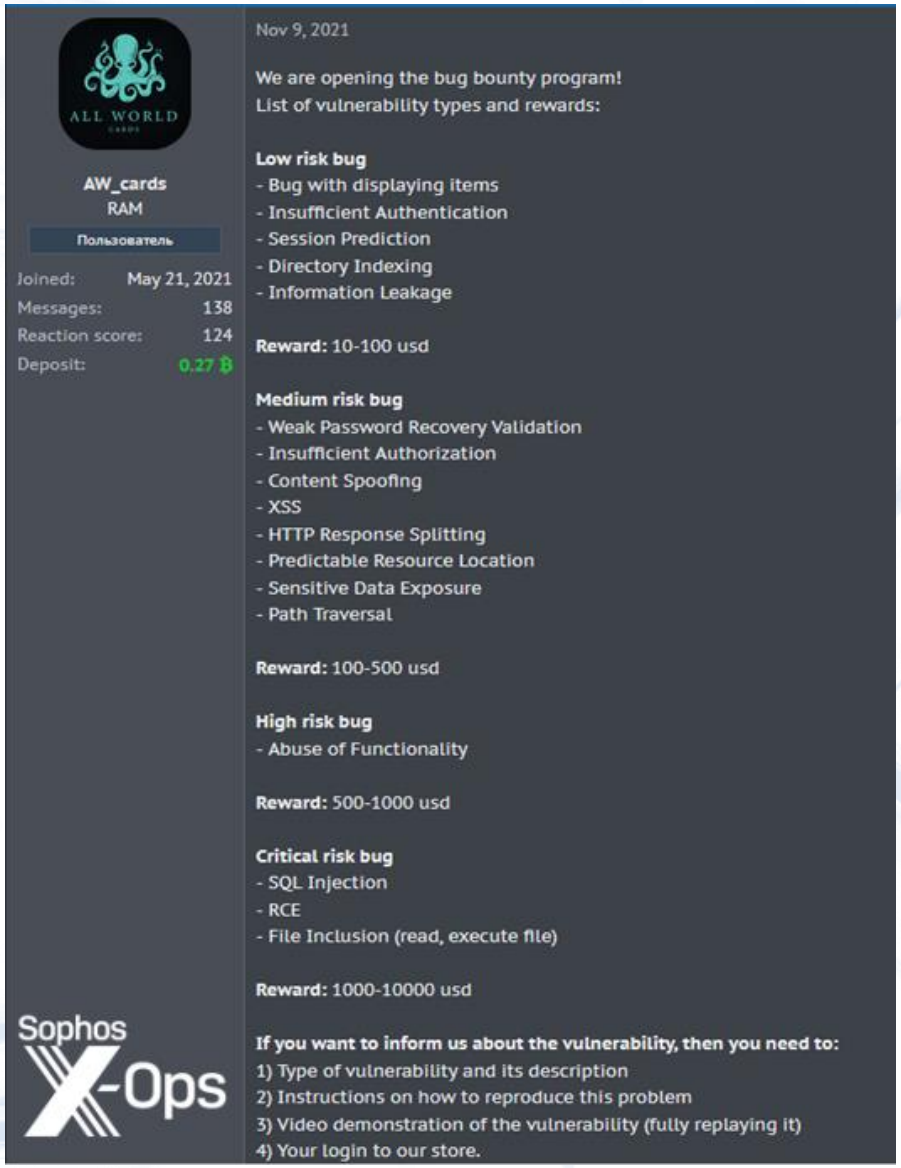
Quando si tratta di diffondere il loro malware, gli attaccanti Ransomware continuano ad evolversi

- Utilizzo di applicazioni legittime
- Nuovi metodi per estorcere denaro
  - Vendita dei dati con un modello a sottoscrizione
  - Vendita dei dati al miglior offerente
  - Offrire alle vittime la possibilità di nascondere il fatto di essere stati compromessi
- Gli obiettivi non sono solo i sistemi Windows, ma anche Linux



Quando si tratta di “Innovazione”, LockBit vince

- LockBit offre ricompense comprese tra 1.000 ed 1 Milione di dollari per attività che vanno dalla segnalazione di nuovi bug nei software di attacco fino alla proposizione di nuove idee di attacco
- LockBit inoltre offre alle sue vittime la possibilità di ricomprare o distruggere i propri dati, oppure di estendere la scadenza per la loro diffusione

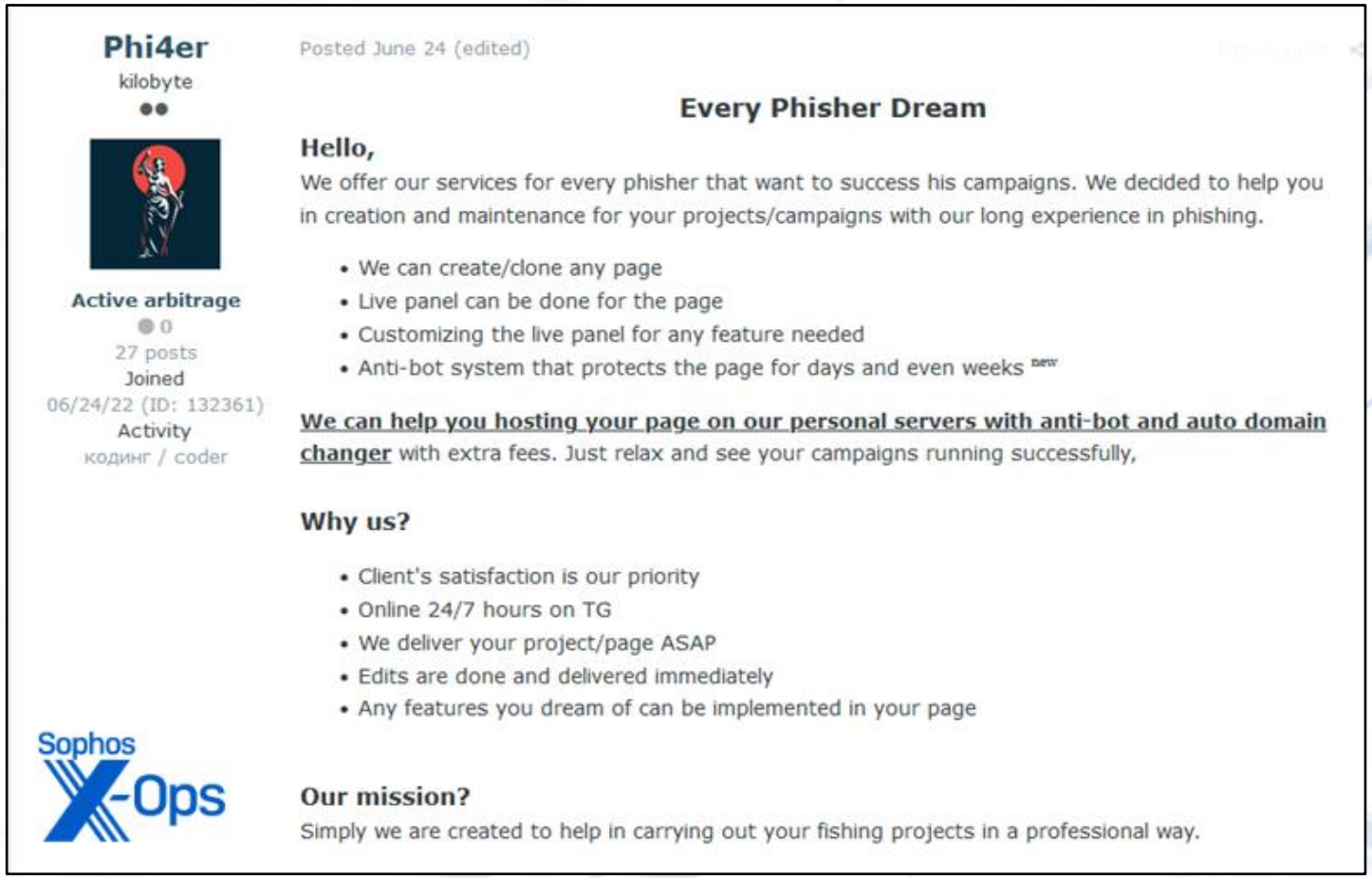


I cyber criminali hanno raggiunto un nuovo livello di strategia Go-to-Market

SOPHOS

I Cyber criminali operano come le normali aziende

- Sempre più gruppi di cyber criminali stanno seguendo il modello “as-a-service” per proporre i loro servizi
- Non solo kit per lanciare email di phishing o virus
- Anche servizi per scoprire le vulnerabilità che presenta un’azienda



Phi4er
kilobyte
●●

Active arbitrage
0
27 posts
Joined
06/24/22 (ID: 132361)
Activity
кодинг / coder

Posted June 24 (edited)

Every Phisher Dream

Hello,

We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks new

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Sophos X-Ops

Our mission?

Simply we are created to help in carrying out your fishing projects in a professional way.

Esiste un mercato del lavoro parallelo

dripper
HDD-drive
Пользователь
Joined: May 19, 2022
Messages: 44
Reaction score: 6

Jun 23, 2022

Sophos X-Ops

I am looking for pentesting job.

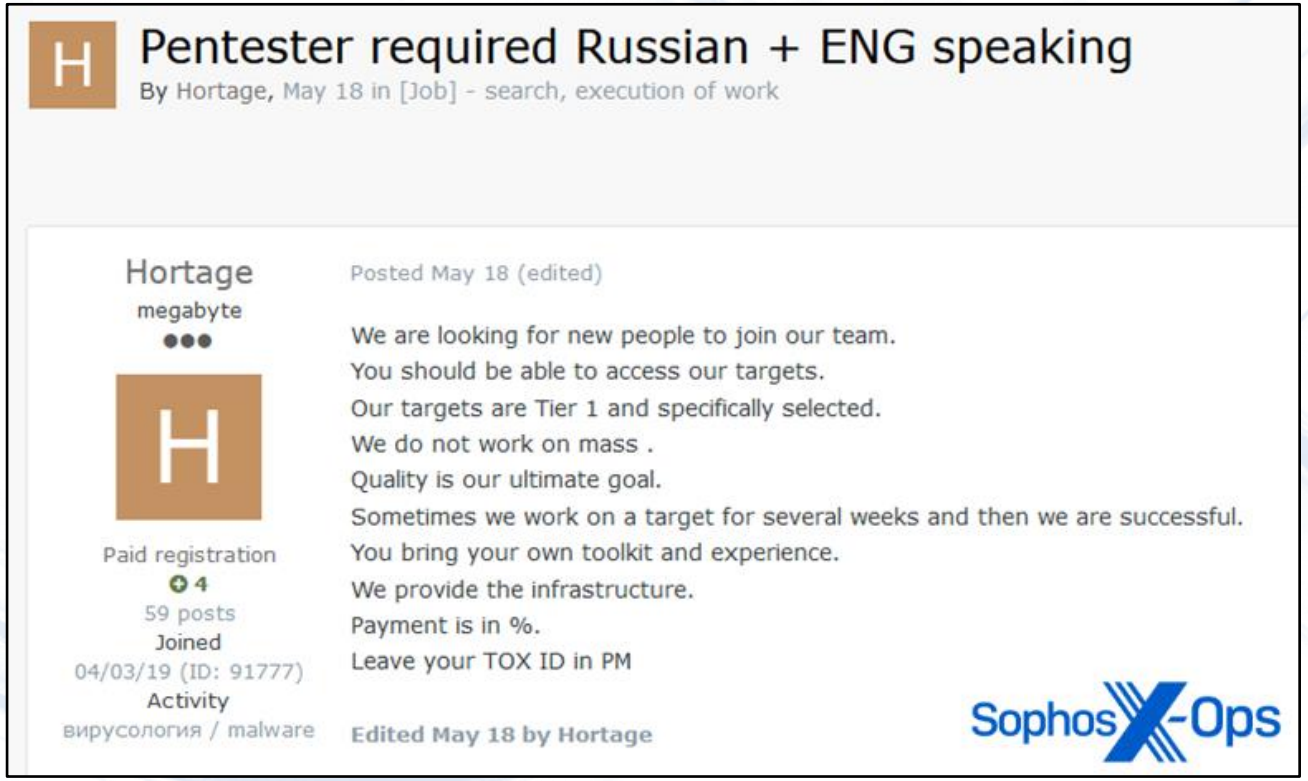
I have experience in AV Bypass on your docx/xlsx and bins
I can do lateral movement for you
I can code for you in C/Cpp python NIM
I have experience make crypts and loaders

More details in PM.

Make damage memorable.

Vengono utilizzate tecniche di Marketing

- Molti marketplace usano grafica accattivante per proporre o richiedere specifiche figure professionali
- I criminali pagano per pubblicizzare i propri servizi



Furti di credenziali in crescita

Grazie alla diffusione dei servizi Internet, la richiesta di credenziali è in crescita

- Credenziali rubate offrono la possibilità di infiltrarsi nelle reti delle aziende (p.es. credenziali Google o Microsoft)

- Alcune credenziali, come le sessioni “cookie”, possono essere usate per bypassare i codici temporanei di accesso

Gli attaccanti sfruttano programmi legittimi e già presenti nei sistemi

Uso di programmi legittimi per lanciare attacchi

- Vengono sfruttati gli stessi programmi che servono per trovare vulnerabilità o punti deboli nelle reti, usati normalmente dai team di sicurezza
- Vengono usati anche programmi già presenti nei computer/server e normalmente utilizzati dagli amministratori di Sistema
- Il vantaggio è averli già a disposizione senza dover installare nulla

I dispositivi mobili sono al centro di nuove tipologie di attacco

Cyber-truffe

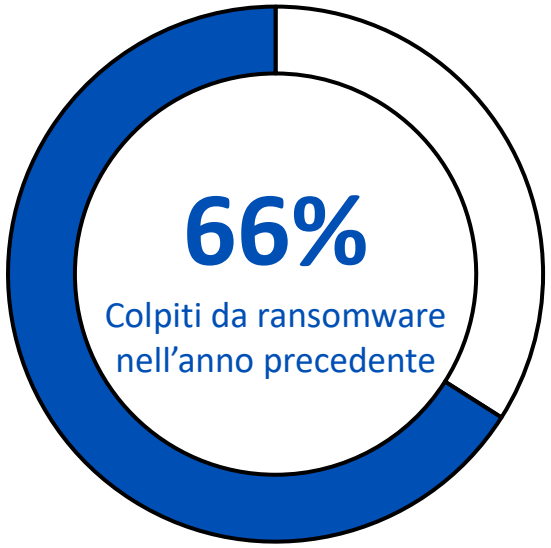
- Applicazioni e siti web fraudolenti, profili social finti
- App malevole a disposizione di utenti Android
- Dispositivi Apple non più immuni: siti malevoli all'interno delle app

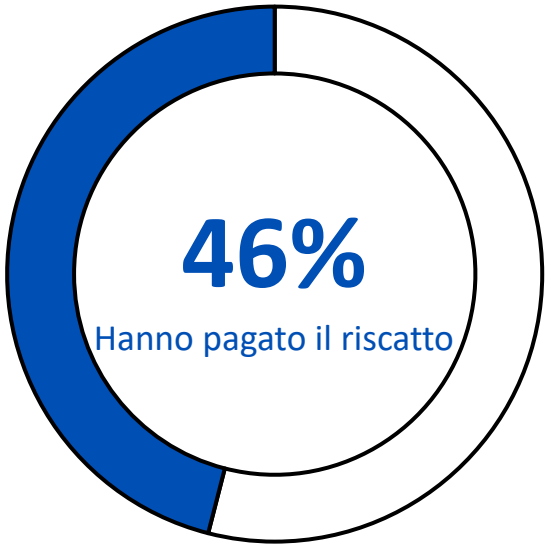
I Ransomware continuano ad essere una delle minacce più pericolose

SOPHOS

Gli attacchi Ransomware sono in costante aumento

Sondaggio su 5.600 IT Manager in 31 paesi





VansonBourne

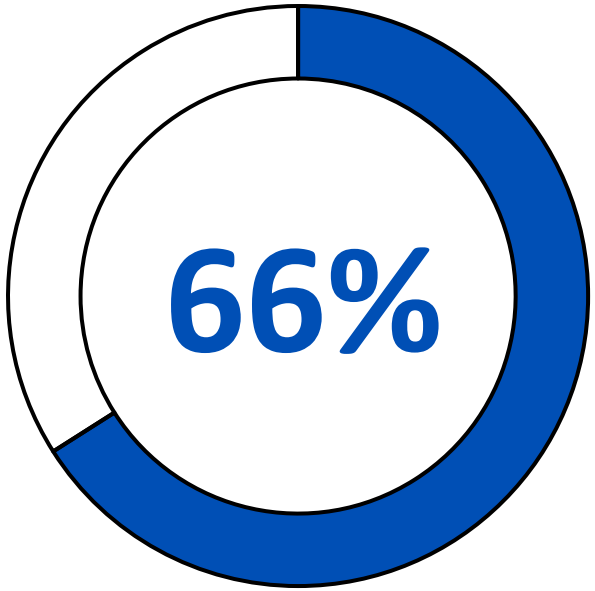
$1.4M

Costo medio per ripristinare un attacco Ransomware

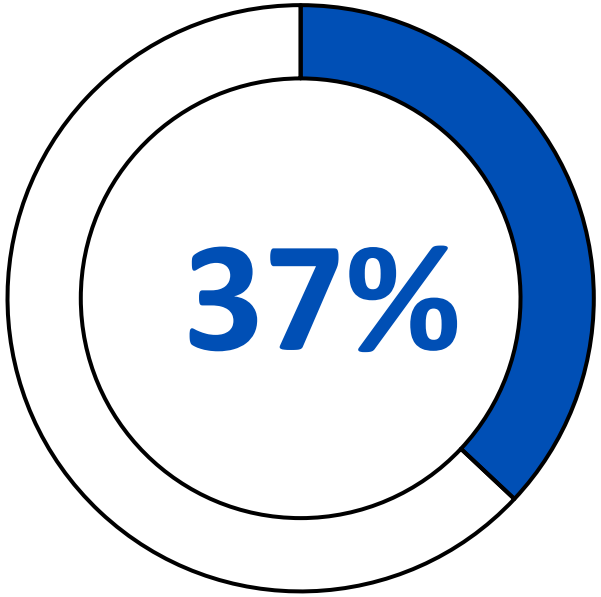
SOPHOS

Gli attacchi Ransomware sono in costante aumento

Colpiti da Ransomware nell’anno precedente



2021

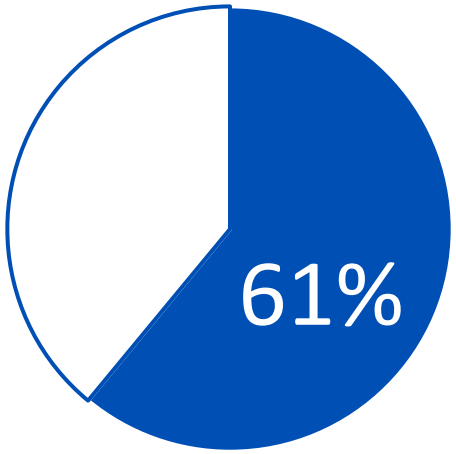


2020

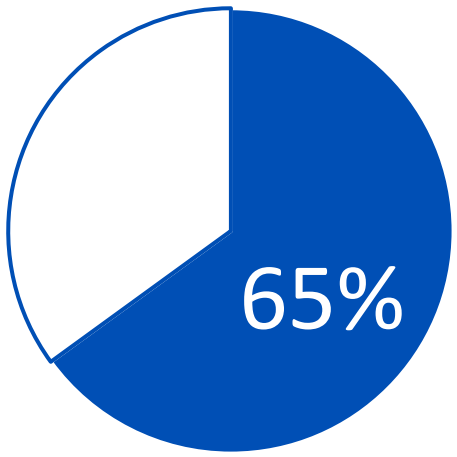
Nell’ultimo anno, la tua azienda è stata colpita da ransomware? Risposta: Sì

Meno aziende recuperano i dati dopo il pagamento del riscatto

Percentuale di aziende in cui alcuni dati sono stati recuperati dopo il pagamento del riscatto

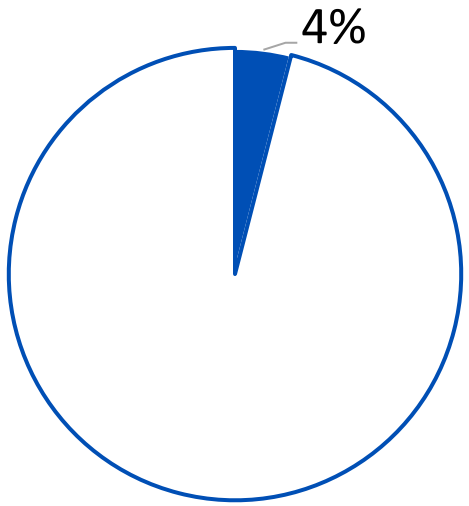


2021

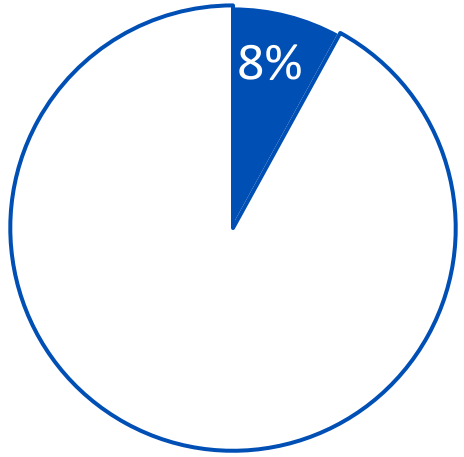


2020

Percentuale di aziende in cui TUTTI i dati sono stati recuperati dopo il pagamento del riscatto



2021



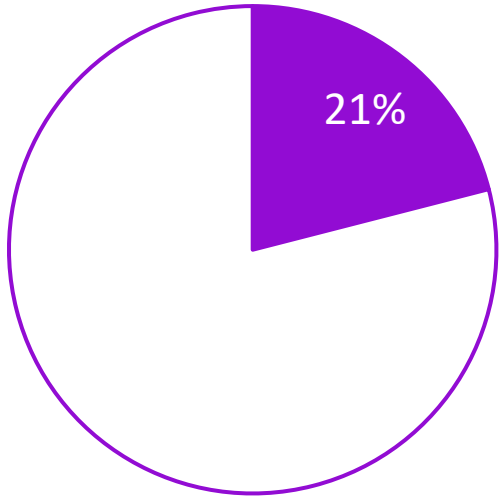
2020

Le somme pagate di riscatto sono aumentate in tutti i settori

965 hanno deciso di rivelare la somma pagata di riscatto

3X

Percentuale di riscatti pagati ammontanti a $1M o più



Percentuale di riscatti pagati ammontanti a meno di $10.000

$812.360

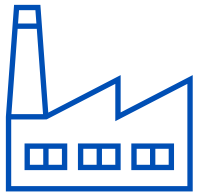
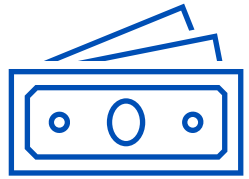
Riscatto medio pagato

Qual è la somma pagata come riscatto dalla tua azienda nell'attacco Ransomware più significativo? US$. (n=965 aziende che hanno pagato il riscatto ed hanno deciso di rivelarne l'entità)

Ripristinare un attacco Ransomware è complicato

1 MESE

Tempo medio di ripristino

PIU' LENTI	PIU' VELOCI
 Scuola e Università	 PA Locale e Centrale
 Manifatturiero	 Servizi Finanziari

Costo medio per il ripristino da un attacco Ransomware

Country	2021	2020	YoY Change
Average (3,702)	$1.40	$1.85	-24%
Australia (200)	$1.01	$1.84	-45%
Austria (84)	$0.81	$7.75	-90%
Belgium (75)	$3.71	$4.75	-22%
Brazil (110)	$0.69	$0.82	-16%
Canada (117)	$0.65	$1.92	-66%
Chile (129)	$1.58	$0.73	116%
Colombia (126)	$0.50	$1.26	-60%
Czech Republic (77)	$2.58	$0.37	589%
France (146)	$2.03	$1.11	83%
Germany (266)	$1.73	$1.17	48%
Hungary (76)	$1.51	n/a	n/a
India (233)	$2.81	$3.38	-17%
Israel (66)	$1.41	$0.57	148%
Italy (121)	$1.65	$0.68	141%
Japan (182)	$0.96	$1.61	-40%

Country	2021	2020	YoY Change
Malaysia (118)	$1.22	$0.77	58%
Mexico (148)	$0.88	$2.03	-57%
Netherlands (104)	$0.98	$2.71	-64%
Nigeria (71)	$3.43	$0.46	644%
Philippines (103)	$1.34	$0.82	63%
Poland (77)	$1.78	n/a	n/a
Saudi Arabia (56)	$0.65	$0.45	46%
Singapore (98)	$1.91	$3.46	-45%
South Africa (101)	$0.71	n/a	n/a
Spain (106)	$0.75	$0.60	25%
Sweden (69)	$0.75	$1.40	-46%
Switzerland (60)	$1.64	$1.43	15%
Turkey (60)	$0.37	$0.58	-36%
UAE (59)	$1.26	$0.52	144%
[illegible]	$1.08	$1.96	-45%
US (292)	$1.08	$2.09	-49%

Qual è stato il costo approssimativo affrontato dalla tua azienda per ripristinare i danni del più recente attacco Ransomware (considerando il tempo di down, il tempo speso dalle persone, il costo dei dispositivi, il costo della rete, le opportunità perse, l'eventuale pagamento del riscatto, ecc.)? US$ Milione

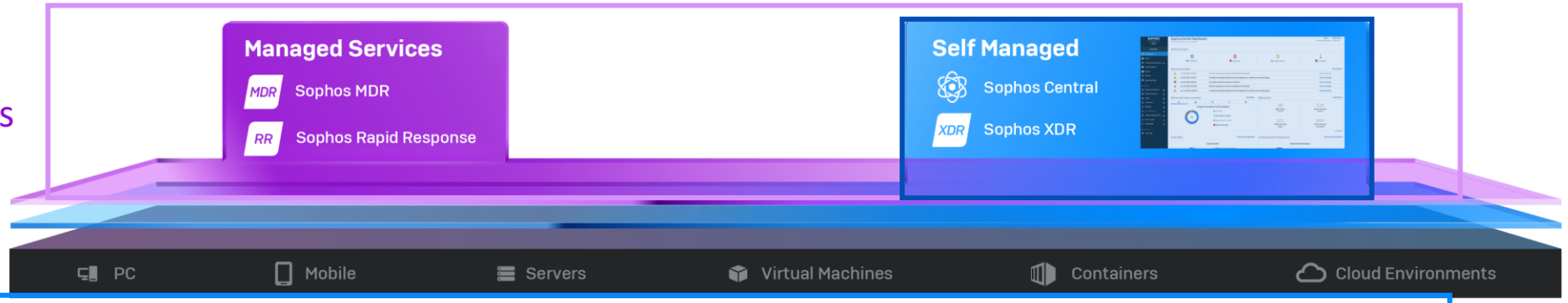
SOPHOS

Come ci possiamo difendere

Adaptive Cybersecurity Ecosystem

Cloud-based security platform

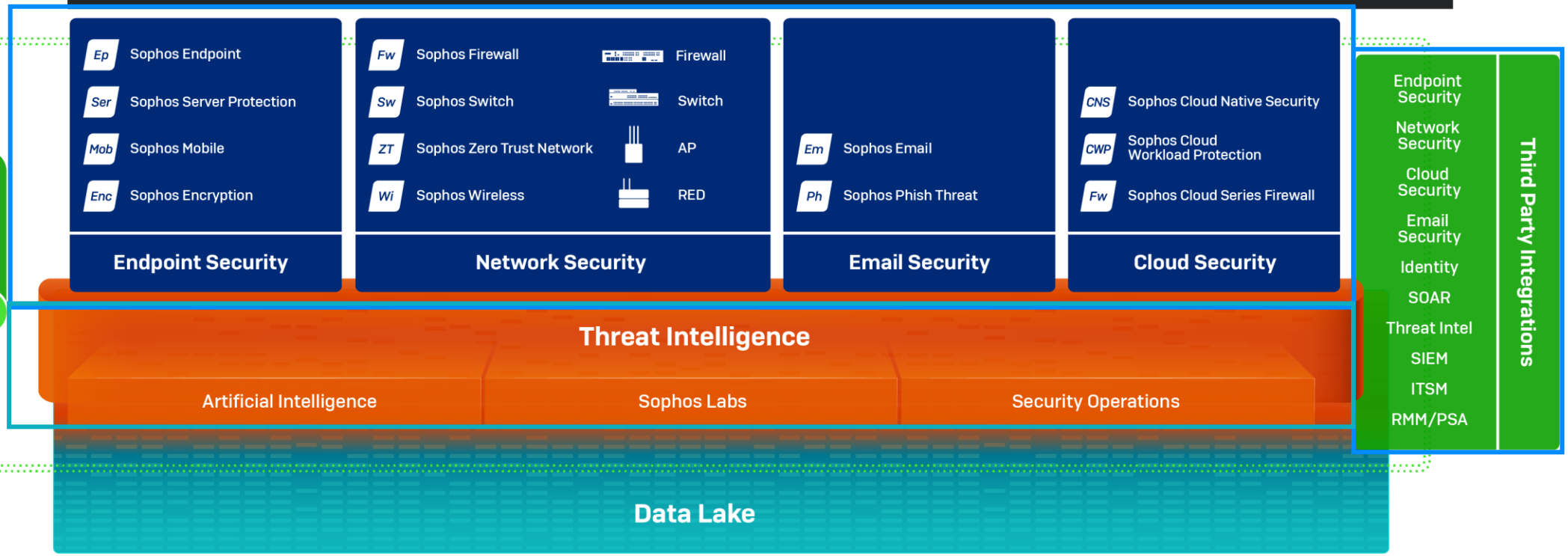
Instant Security Operations Center



Integrated cyber defenses

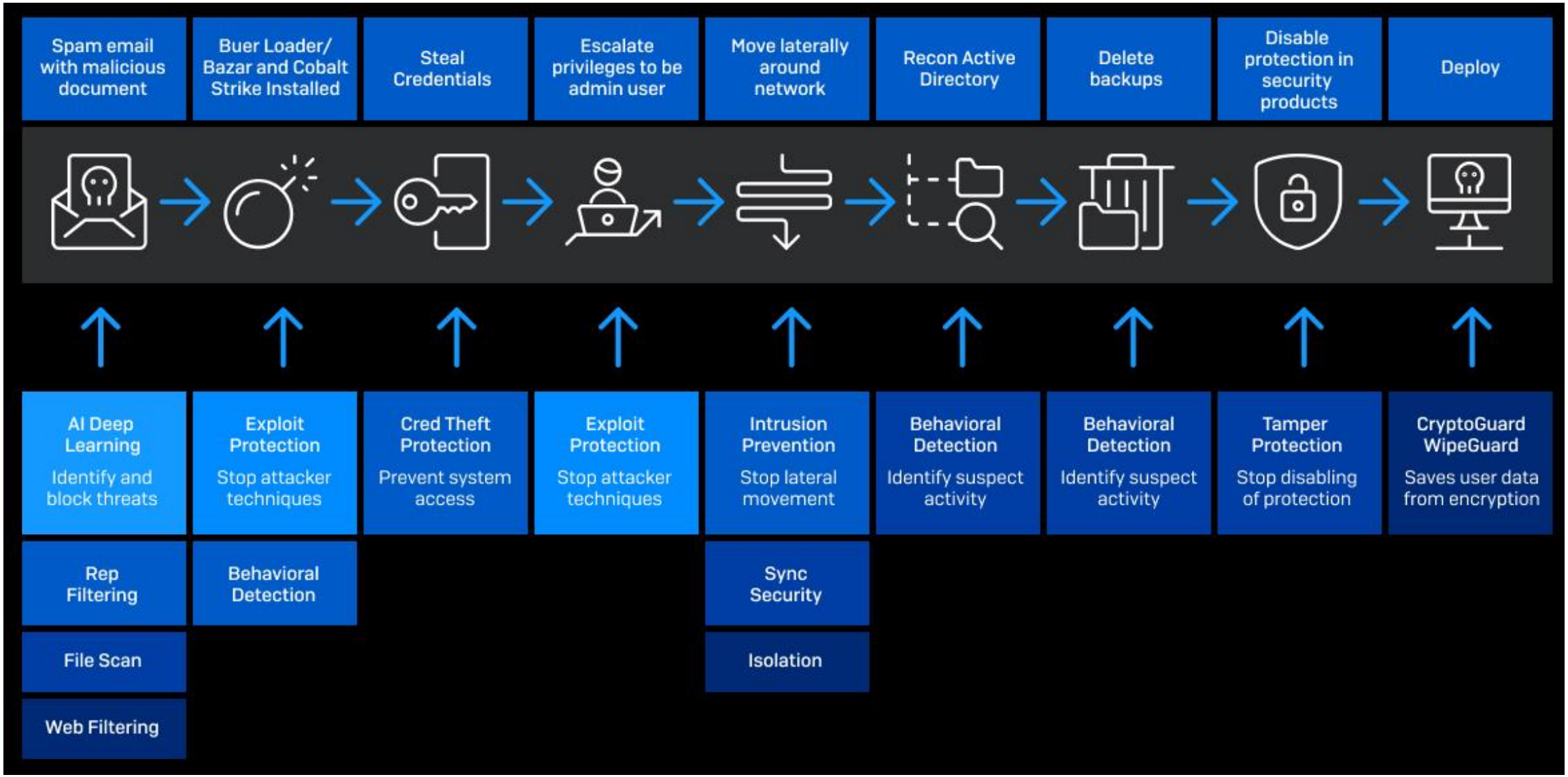
Open APIs

Expert team



SOPHOS

Ottimizzare la Prevenzione



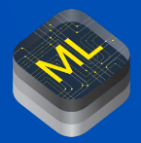
Sophos Firewall

- Protezione del traffico di rete
- Blocco dei Centri di Controllo
- Controllo del traffico Internet (anche HTTPS)
- Sandbox

Protezione della posta elettronica

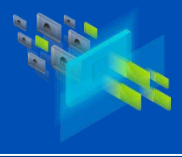
Sophos Email

- Semplicità nella configurazione e nella gestione
- Protezione dei dati sensibili dallo spam, attacchi phishing e virus, inclusi i ransomware
- Sandbox



Sicurezza predittiva della posta elettronica con AI

Protezione dei dati sensibili



Protezione dallo spam e dal phishing

Le soluzioni tecnologiche sono sufficienti a fermare gli attacchi?

Ancora due considerazioni…

Formazione degli utenti

Sophos Phish Threat – *Simulazione di un attacco Phishing in 3 semplici passi*

1

Scegli un attacco

- Centinaia di template di attacchi (in diverse lingue), continuamente aggiornati da Sophos

2

Scegli un mini corso di formazione

- Oltre 30 corsi interattivi che coprono argomenti inerenti la sicurezza informatica

3

Monitora i risultati e misura i miglioramenti

- Report sulle campagne di attacco
- Dati sul comportamento degli utenti

Dobbiamo trovare metodi più efficaci per rispondere agli attacchi

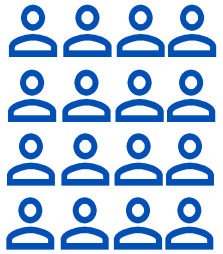
Gartner®

Entro il 2025, il 50% delle organizzazioni utilizzerà i servizi Managed Detection and Response che offrono capacità di contenimento e mitigazione delle minacce per le funzioni di monitoraggio, rilevamento e risposta alle minacce

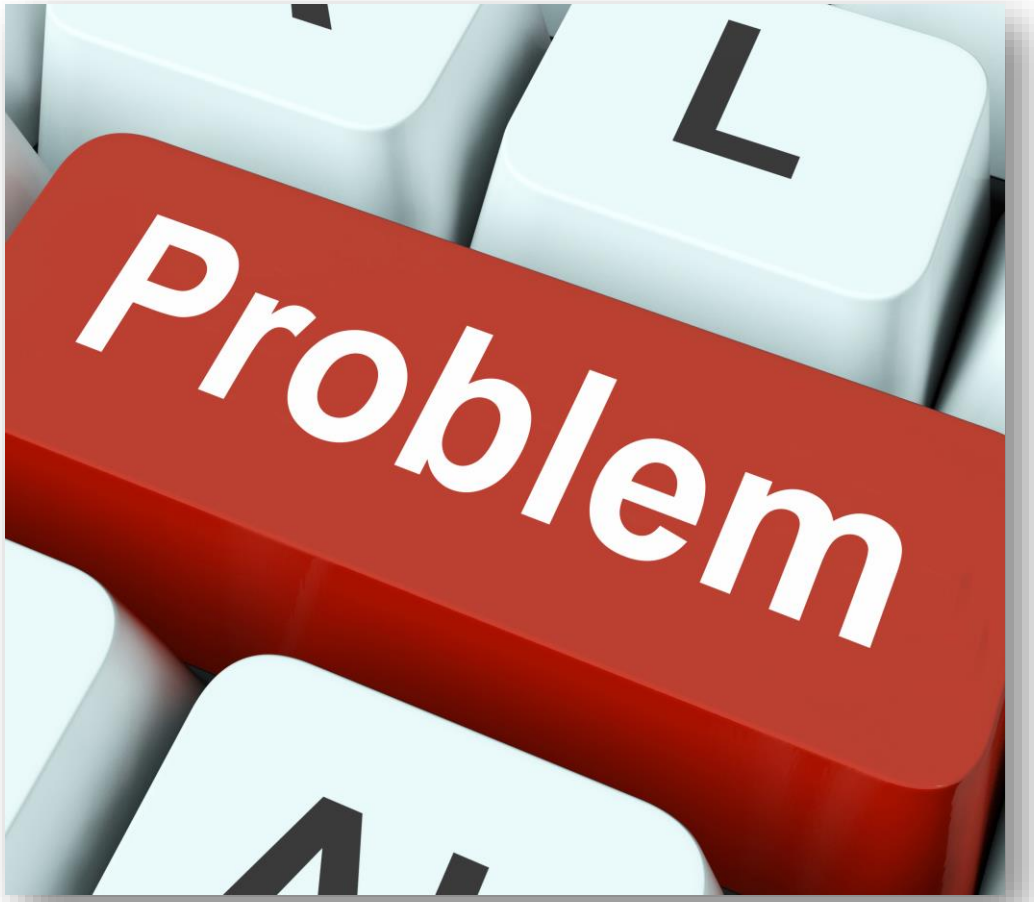
Perchè c’è bisogno di servizi di MDR?

Non si hanno le risorse necessarie per adattarsi nella difesa dalle **minacce che evolvono velocemente**.

Sono pochissime le aziende che vogliono/possono investire e dotarsi di infrastrutture di cybersecurity in casa



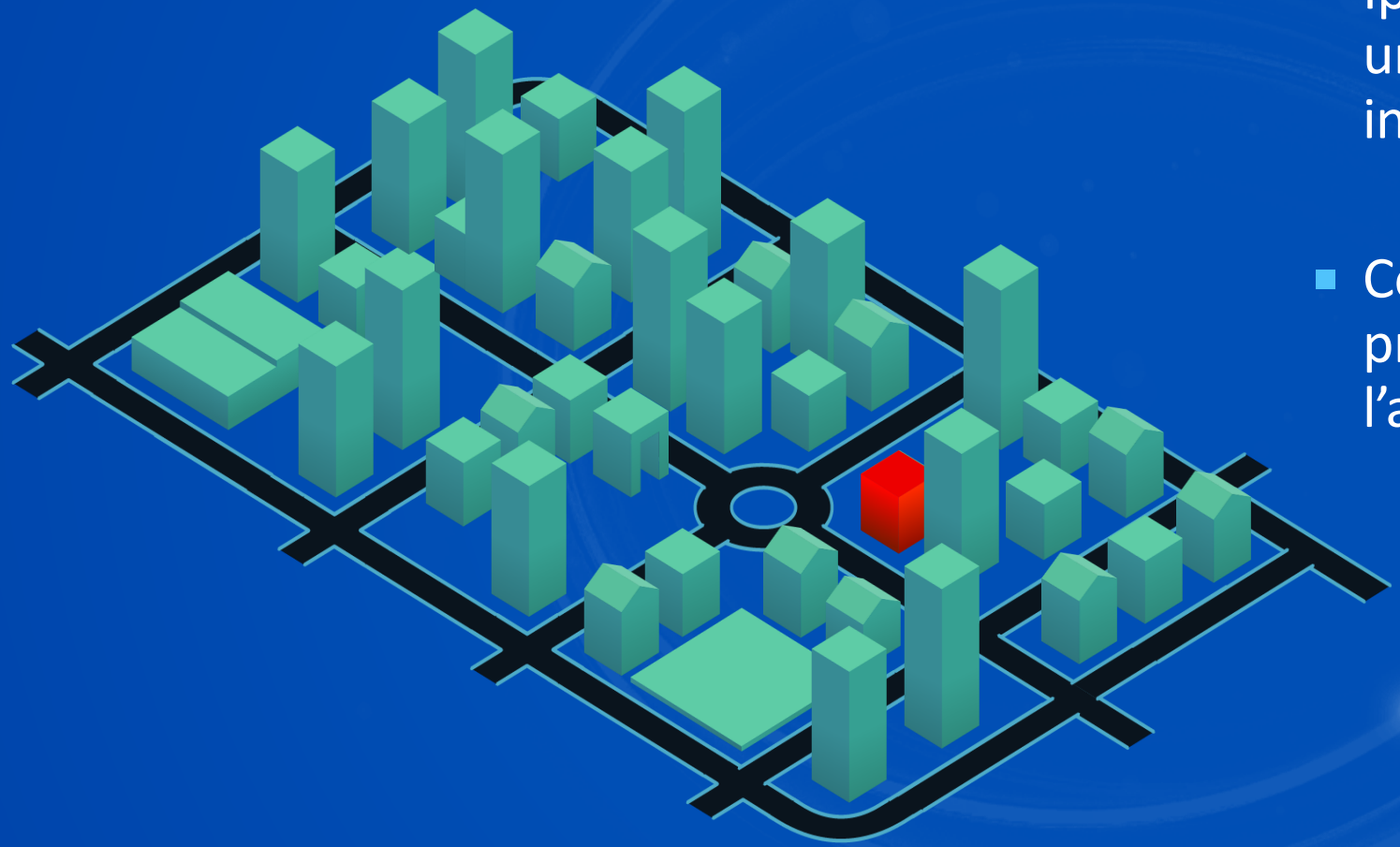
Le aziende di tutto il mondo **non vogliono diventare esperte di Cybersecurity.** Vogliono stare al sicuro per continuare ad occuparsi delle vere esigenze **del loro business!**



Proteggiamo la nostra città

- Pensiamo alla nostra azienda come ad una città
- Ogni palazzo rappresenta uno o più host (computer, server, smartphone, tablet, stampante, telecamera, ecc…)
- Le strade sono la rete

Reagiamo solo quando c’è un problema

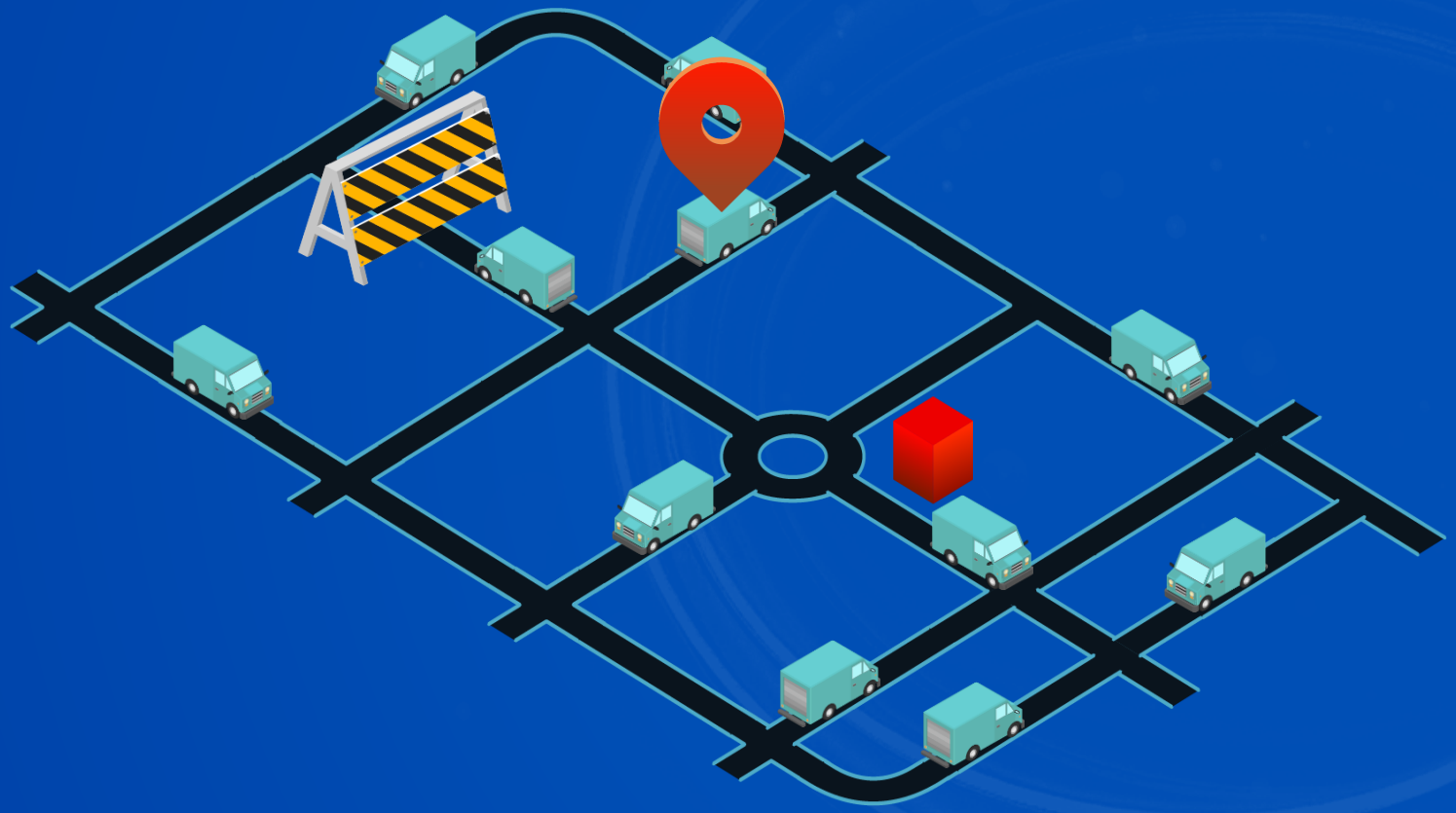


- Ipotizziamo che questo edificio sia una sistema con dati preziosi al suo interno.
- Cosa accadrebbe se provassimo a proteggerci solo quando scatta l’allarme rosso?

Reagiamo solo quando c’è un problema

- L’allarme ha funzionato… ma se tutto quello che è successo prima dell’allarme ci fosse sfuggito?
- **Rischieremmo una corsa contro il tempo!**

Il momento del furto è solo l'apice del problema



- I sistemi di sicurezza che reagiscono solo quando c'è un problema possono bloccare le azioni più evidenti
- Ma se il ladro utilizzasse i nostri stessi mezzi per rubare e fuggire?
- Potremmo provare a bloccare alcune strade…
- **Ma il ladro solitamente conosce strade secondarie, scorciatoie e metodi per confondersi!**

Sophos Managed Detection and Response (MDR)

Un servizio completamente gestito, 24 ore su 24, 7 giorni su 7, fornito da esperti specializzati nel rilevamento e nella risposta agli attacchi informatici che le sole soluzioni tecnologiche non possono prevenire

Sophos MDR

Caccia alle minacce

Attività condotta da analisti esperti nella caccia alle minacce. Lo scopo è di scovare e di eliminare le minacce più rapidamente di quanto possano fare i soli prodotti di sicurezza

Rilevamento Minacce

Eseguito grazie all'integrazione dei dati prelevati da diverse fonti di Sicurezza, allo scopo di intercettare comportamenti potenzialmente malevoli

Risposta agli incidenti

Neutralizzazione degli attacchi eseguita in pochi minuti, in modalità completamente gestita o collaborativa con il team interno

Adatto a tutte le aziende, sia per dimensione che per settore

Quanto deve essere veloce un servizio MDR?

16.000+ Clienti MDR

1.000+ Clienti ogni mese

99.98% delle minacce bloccate automaticamente*

Tempi medi di risposta del servizio Sophos MDR

Tempo di rilevamento	Meno di 1 minuto
Tempo d'investigazione	Meno di 25 minuti
Tempo di risposta	Meno di 12 minuti

300+ Clienti MDR in Italia

SOPHOS

Sophos MDR

Adesso la nostra città è decisamente più protetta

24 ore su 24
7 giorni su 7

SOPHOS

SOPHOS