SOPHOS

Lo Stato Della Cybersecurity Nel 2023: L'Impatto Sul Business Provocato Dagli Avversari

I risultati di uno studio indipendente condotto tra gennaio e febbraio 2023, a cui hanno partecipato 3.000 IT Manager, dislocati in 14 paesi del mondo.

Whitepaper Sophos. Aprile 2023

Metodologia Di Ricerca

Per esplorare l'impatto commerciale effettivo della cybersecurity nel 2023, Sophos ha affidato a un'azienda esterna l'incarico di condurre un sondaggio indipendente tra 3.000 IT/Cybersecurity Manager in 14 paesi. Tutti gli intervistati provenivano da organizzazioni con un numero di dipendenti compreso tra 100 e 5.000. Il sondaggio è stato svolto da Vanson Bourne nei mesi di gennaio e febbraio 2023.

3000
intervistati

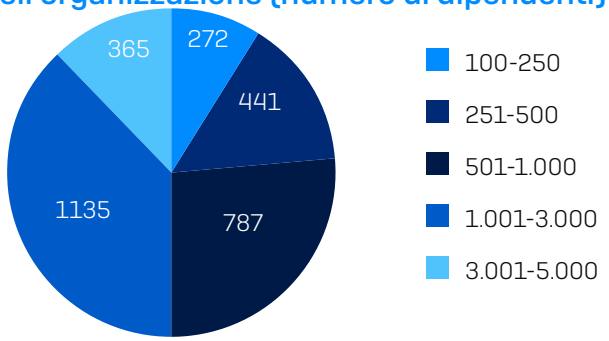
100-5.000
dipendenti

14
paesi

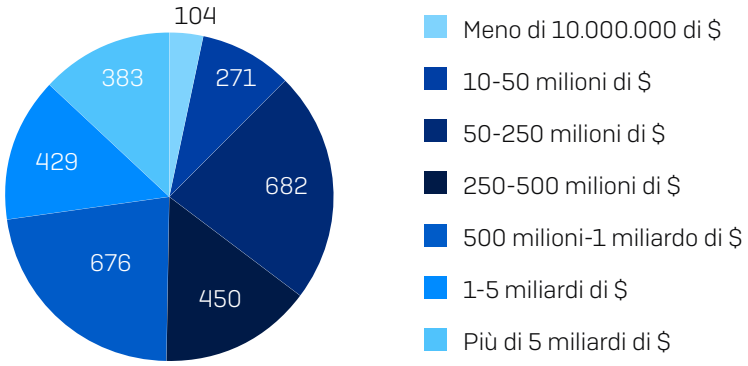
da <10 Mio a >5 Mrd di $
di fatturato annuo

Gen/feb 23
mesi in cui è stata condotta la ricerca

Numero di intervistati in base alle dimensioni dell'organizzazione (numero di dipendenti)



Numero di intervistati in base alle dimensioni dell'organizzazione (fatturato annuo)



Partecipanti per paese

PAESE	NUMERO DI PARTECIPANTI	PAESE	NUMERO DI PARTECIPANTI
Stati Uniti	500	Regno Unito	200
Germania	300	Sud Africa	200
India	300	Francia	150
Giappone	300	Spagna	150
Australia	200	Austria	100
Brasile	200	Singapore	100
Italia	200	Svizzera	100

Riepilogo

Situazione: Gli Avversari Informatici Si Evolvono Sempre Più Rapidamente E I Team Di Cybersecurity Non Riescono A Tenere Il Passo

Dallo studio è emerso che la realtà attuale del panorama della cybersecurity è caratterizzata da un sistema che vede cybercriminali e team di IT security che sviluppano le proprie strategie a velocità diverse. Grazie all'automazione, ai modelli di cybercrimine "as-a-service", a furti di identità sempre più difficili da smascherare e a una straordinaria capacità di adattamento, gli avversari informatici si stanno evolvendo sempre più rapidamente e sono ora in grado di sferrare un'ampia selezione di attacchi estremamente sofisticati su vasta scala. L'anno scorso il 94% delle organizzazioni ha subito un attacco informatico; di conseguenza, qualsiasi azienda, indipendentemente dalle dimensioni, deve partire dal presupposto che verrà presa di mira nel 2023.

Rallentati dalla carenza di competenze tecniche adeguate e da un volume eccessivo di avvisi, e dovendo dedicare una quantità eccessiva di tempo all'incident response, i team di IT security non riescono a tenere il passo con i cybercriminali. "L'operazionalizzazione" del rilevamento e della risposta alle minacce è un processo difficile da implementare per la maggior parte delle organizzazioni, con il 93% degli intervistati che afferma di ritenere complicata l'esecuzione di operazioni di sicurezza essenziali.

L'impossibilità di indagare su tutti gli avvisi di sicurezza è un problema diffuso. In media, poco meno della metà (48%) di tutti gli avvisi viene analizzata per stabilire se si tratti di segnali di attività pericolosa; inoltre, la maggior parte delle organizzazioni fa fatica a identificare (71%) e attribuire la giusta priorità (71%) agli avvisi/eventi su cui indagare. Per gli avvisi che lo dovessero richiedere, il processo completo di rilevamento, indagine e risposta implica un investimento medio di tempo che varia da nove ore, per le organizzazioni con 100-3.000 dipendenti, a 15 ore se il numero di dipendenti è compreso tra 3.001 e 5.000.

Operativamente, i team informatici non nutrono molta fiducia nei propri processi interni: gli errori di configurazione degli strumenti di sicurezza sono stati infatti identificati come il principale rischio alla sicurezza percepito per il 2023. Più della metà (52%) dei professionisti dell'IT sostiene che le cyberminacce sono ora troppo avanzate per essere affrontate in maniera efficace della propria organizzazione senza alcun aiuto esterno. Questa percentuale sale al 64% per le aziende di piccole dimensioni (100-250 dipendenti).

L'Impatto Sul Business:: La Situazione Ha Gravi Conseguenze In Termini Finanziari, Operativi E Di Risorse

Questo sistema a due velocità ha un impatto molto forte sull'intera organizzazione. Le ripercussioni finanziarie dirette di un incidente informatico sono enormi e tristemente ben note, con costi medi necessari per rimediare ai danni causati da un attacco ransomware che possono raggiungere gli 1,4 milioni di $ per le piccole e medie imprese[1]. Questi costi di riparazione in seguito agli incidenti sono, tuttavia, solo parte della storia.

La capacità di realizzazione dei progetti dei team informatici risulta ridotta, con il 55% degli intervistati che sostiene che dover gestire le minacce ha avuto un impatto negativo sulla capacità del proprio team IT di dedicarsi ad altri progetti. La natura urgente e imprevedibile della cybersecurity ostacola anche le iniziative di maggiore impatto commerciale: il 64% degli intervistati preferirebbe infatti che il team IT dedicasse più tempo alle attività di importanza strategica e meno tempo agli interventi di emergenza.

Le ore interminabili investite nel rilevamento, nell'indagine e nella correzione degli avvisi di sicurezza hanno anche ripercussioni finanziarie significative, in termini di costo delle risorse umane.

Inoltre, la situazione rappresenta un peso estremamente gravoso per i dipendenti. Il 57% dei professionisti dell'IT confessa che a volte il pensiero che l'organizzazione possa essere colpita da un attacco informatico gli impedisce di dormire; questa percentuale sale al 65% per gli intervistati che lavorano in organizzazioni con 3.001-5.000 dipendenti. Considerando gli elevati costi implicati dai processi di assunzione, formazione e fidelizzazione del personale in questo ambito, le ripercussioni generano ulteriori problemi e costi per l'azienda.

1 La Vera Storia Del Ransomware 2022, Sophos

Consiglio: Accelerare I Meccanismi Di Difesa Per Superare Gli Avversari Informatici

Per poter permettere ai team di IT security di superare i cybercriminali nella "gara" della cybersecurity del 2023, occorre un approccio completo ma diretto. Prima di tutto, le organizzazioni devono implementare un processo di incident response facilmente scalabile, incentrato sulla riduzione della superficie di attacco e del volume di avvisi, ottimizzando i tempi di risposta grazie all'uso di servizi specializzati.

Successivamente, le organizzazioni devono applicare difese adattive, in grado di adeguarsi automaticamente alla situazione. In questo modo potranno rallentare gli avversari e guadagnare tempo prezioso per i team di sicurezza informatica.

Infine, devono implementare un circolo virtuoso che includa una combinazione ben bilanciata di tecnologie e competenze umane, per mettere il turbo ai sistemi di difesa e incrementarne la velocità, l'efficacia e l'impatto. Insieme, tutti questi fattori accelerano i meccanismi di difesa, permettendo ai team informatici di superare i loro avversari.

Un elemento assolutamente cruciale per la buona riuscita di questa strategia è l'uso di servizi specializzati di terze parti. La buona notizia è che le organizzazioni hanno già adottato un approccio ibrido all'implementazione della cybersecurity, con il 94% delle aziende che collabora con specialisti esterni per incrementare il potenziale dei propri team operativi interni. Con il continuo intensificarsi delle attività dei cybercriminali, la collaborazione con un team dedicato di esperti di sicurezza è sempre più indispensabile.

I risultati più salienti

Il 94% delle organizzazioni ha subito un attacco informatico l'anno scorso

L'esfiltrazione dei dati è il problema di sicurezza che preoccupa di più per il 2023

Il 93% degli intervistati reputa difficile gestire la cybersecurity

Il 48% degli avvisi di sicurezza viene analizzato

15 ore è il tempo medio necessario per rilevare, indagare e rispondere a un avviso nelle organizzazioni con 3.001-5.000 dipendenti

Gli errori di configurazione degli strumenti di sicurezza sono il principale rischio di sicurezza percepito per il 2023

Il 52% degli intervistati sostiene che le cyberminacce sono ora troppo avanzate per essere affrontate dal team tecnico della propria organizzazione senza un aiuto esterno

Il 55% degli intervistati indica che dover gestire le cyberminacce ha limitato la disponibilità del team IT per altri progetti

Il 64% degli intervistati preferirebbe che il team IT dedicasse più tempo ad attività di importanza strategica e meno tempo a interventi di emergenza

Il 57% dei professionisti dell'IT confessa che il pensiero che l'organizzazione possa essere colpita da un attacco informatico impedisce loro di dormire sonni tranquilli

Le Cyberminacce Nel 2023: La Realtà Attuale Di Chi Lavora In Prima Linea

Le Principali Preoccupazioni Di Cybersecurity Per Il 2023

Il 99% dei professionisti dell'IT nutre serie preoccupazioni sulle cyberminacce che potrebbero colpirne l'organizzazione nel 2023. L'esfiltrazione dei dati (il furto di informazioni per mano di un criminale esterno) si trova al primo posto nella classifica delle minacce che causano maggiore preoccupazione ai professionisti dell'IT, seguita a distanza ravvicinata dal phishing (incluso lo spearphishing). Il ransomware completa il podio delle prime tre fonti di preoccupazione segnalate.

È importante ricordare che queste tre minacce sono spesso correlate: di solito un'e-mail di phishing è la prima fase di un attacco che porta poi all'esfiltrazione dei dati e al ransomware.

CYBERMINACCIA	PERCENTUALE DI INTERVISTATI PER CUI QUESTA MINACCIA È LA PREOCCUPAZIONE PRINCIPALE
Esfiltrazione dei dati (furto per mano di un cybercriminale esterno)	41%
Phishing (incluso spearphishing)	40%
Ransomware	35%
Cyber-estorsione	33%
Attacchi Denial of Service (DDoS)	32%
Business Email Compromise	31%
Active adversary (hacker umani che sferrano attacchi hands-on-keyboard)	30%
Malware dei dispositivi mobili	30%
Cryptominer	22%
Wiper	16%
Altro	0%
Non nutro preoccupazioni per alcuna cyberminaccia che potrebbe colpire la mia organizzazione nel 2023	1%
Non lo so	0%

Pensando al 2023, quali sono le cyberminacce che potrebbero colpire la tua organizzazione che ti preoccupano maggiormente? (n=3.000)

Gli Avversari Informatici Eseguono Ora Una Miriade Di Attacchi Su Vasta Scala

Le preoccupazioni dei professionisti dell'IT riflettono molto fedelmente la realtà attuale di quello che accade in prima linea: il 94% delle organizzazioni ha infatti subito almeno un attacco l'anno scorso. Sebbene il ransomware sia stato l'attacco più frequente, i cybercriminali sferrano un'ampia selezione di attacchi su vasta scala. L'estensione e la profondità degli attacchi costituisce un rischio notevole e in costante aumento per i team di cybersecurity.

Dietro a queste statistiche si cela un'economia cybercriminale sempre più professionale, che include la crescita del modello "as-a-service" sotto forma di "access-as-a-service", "phishing-as-a-service" e "scamming-as-a-service". L'evoluzione delle operazioni del cybercrimine ha reso l'intero sistema molto più accessibile per gli aspiranti cybercriminali [per saperne di più, leggi il Sophos 2023 Threat Report].

Una selezione degli attacchi informatici non ransomware subiti, con la percentuale di organizzazioni che li ha segnalati

27%	**27%**	**26%**
E-mail pericolose	Phishing (incluso spearphishing)	Esfiltrazione dei dati (da parte di un cybercriminale)
24%	**24%**	**21%**
Cyber-estorsione	Business Email Compromise	Malware dei dispositivi mobili
18%	**24%**	**14%**
Cryptominer	Denial of Service (DDoS)	Wiper

Gli Attacchi Per Mano Di Active Adversary Sono Ora Comuni

23%
Percentuale di organizzazioni che l'anno scorso hanno subito un attacco in cui erano coinvolti active adversary

30%
Percentuale di intervistati che identificano gli active adversary come la principale preoccupazione di cybersecurity per il 2023

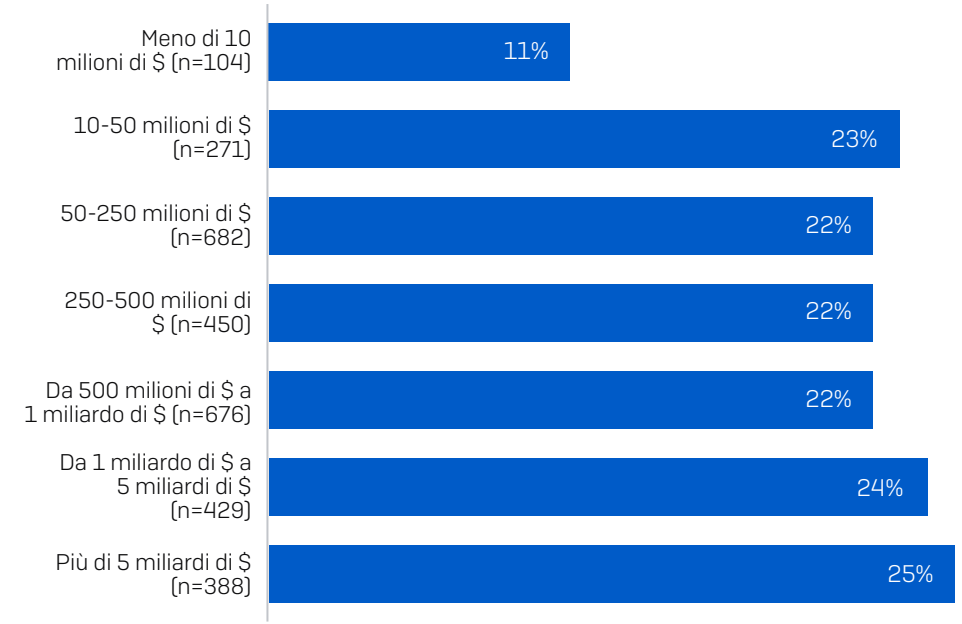
Gli active adversary sono cybercriminali che adattano le proprie tecniche, tattiche e procedure (TTP) sul momento, grazie a operazioni hands-on-keyboard eseguite in tempo reale per rispondere alle attività di difesa dei team di IT security e delle tecnologie di protezione. È inoltre una strategia che permette di eludere il rilevamento. Questi attacchi, che spesso causano incidenti ransomware e violazioni dei dati devastanti, sono tra i più difficili da bloccare.

Il 23% degli intervistati dichiara che l'hanno scorso la propria organizzazione ha subito un attacco in cui erano coinvolti active adversary. La percentuale di attacco è coerente e non cambia in base alle dimensioni dell'organizzazione, con una variazione massima di soli due punti percentuali tra segmenti di mercato che includono organizzazioni di dimensioni diverse.

È interessante osservare che, per le organizzazioni con un fatturato annuo inferiore ai 10 milioni di $, la percentuale di attacchi con active adversary segnalati scende ad appena l'11%, il che potrebbe indicare che i cybercriminali preferiscono volutamente concentrarsi su vittime che hanno risorse finanziarie più estese. L'individuazione degli active adversary richiede elevati livelli di competenze, per cui è probabile che la percentuale effettiva di incidenti sia in realtà più alta.

Rispecchiando il potenziale devastante di questi attacchi, il 30% degli intervistati afferma che gli active adversary sono una delle principali preoccupazioni di cybersecurity per il 2023.

Attacchi Con Active Adversary Subiti, In Base Al Fatturato Della Vittima

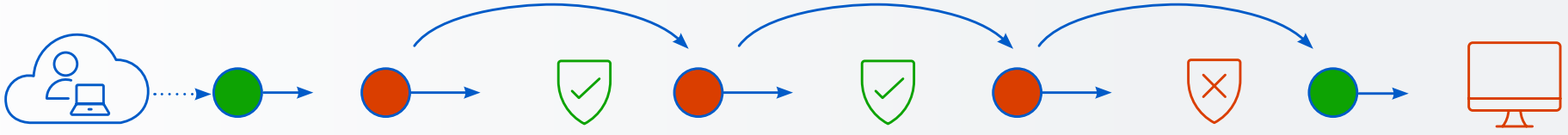


Hai subito uno o più attacchi informatici l'anno scorso? Sì, active adversary (hacker umani che sferrano attacchi hands-on-keyboard)

Capire Gli Active Adversary

Per comprendere pienamente le sfide affrontate dai team di IT security, è fondamentale capire che bloccare gli active adversary non basta per sventarne i piani. Questi avversari informatici sono abili e ostinati e sfruttano un gran numero di tecniche, tattiche e procedure (TTP) per raggiungere i loro obiettivi, con strategie che includono:

- L'exploit delle vulnerabilità di sicurezza per infiltrarsi nei sistemi delle organizzazioni, per poi spostarsi lateralmente una volta all'interno della rete. I criminali sfruttano credenziali rubate, vulnerabilità per le quali non sono state applicate patch, errori di configurazione negli strumenti di sicurezza e altro.
- L'uso improprio di strumenti informatici legittimi, che vengono normalmente utilizzati dai team di IT security per evitare di attivare il rilevamento.
- La modifica della propria strategia di attacco in tempo reale, per rispondere ai controlli di sicurezza. Gli hacker continuano a cambiare tecnica fino a quando non raggiungono gli obiettivi che si sono prefissati.



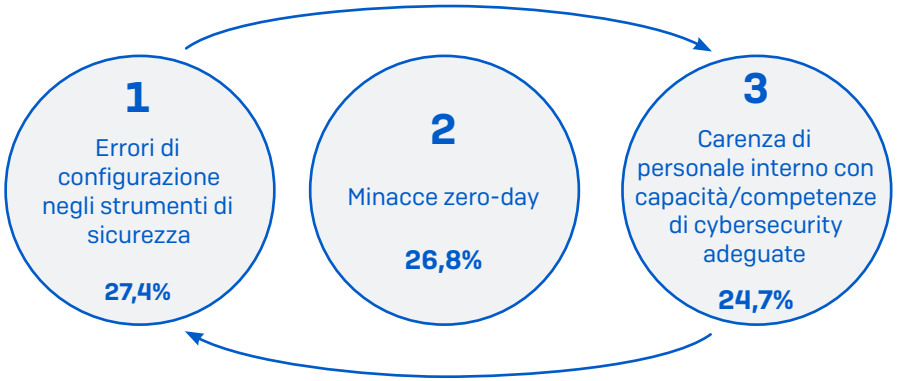
La Cybersecurity Nel 2023: La Prospettiva Dei Team Di IT Security

Le Principali Preoccupazioni Di Cybersecurity

Gli errori di configurazione nei controlli di sicurezza (ad es. in una soluzione endpoint o firewall) sono tra i principali rischi di sicurezza percepiti che sono stati segnalati dagli intervistati: il 27,4% delle risposte li colloca infatti nella top 3 dei rischi informatici. Questa posizione in classifica è la rappresentazione perfetta delle sfide affrontate dai team IT per garantire la corretta configurazione dei controlli di sicurezza e la loro continua implementazione. Inoltre, dimostra il livello di preparazione dei cybercriminali a sfruttare qualsiasi vulnerabilità nelle difese di un'organizzazione.

Gli attacchi zero-day (ovvero gli attacchi che sfruttano una vulnerabilità di sicurezza o un difetto dei software mai osservato prima) si trovano in seconda posizione, citati tra i principali tre rischi informatici dal 26,8% degli intervistati. La carenza di personale interno con capacità/competenze di cybersecurity adeguate si trova al terzo posto nella classifica, in quanto viene considerata tra i principali tre rischi informatici dal 25% dei partecipanti al sondaggio.

Esiste una correlazione diretta tra la carenza di competenze e gli errori di configurazione negli strumenti di sicurezza: senza il tempo, le conoscenze e l'esperienza necessari per configurare correttamente i controlli, è inevitabile che si creino punti deboli nei sistemi di difesa.



RISCHIO DI CYBERSECURITY	PERCENTUALE DI INTERVISTATI CHE INCLUDONO QUESTO RISCHIO NELLE PROPRIE TRE PREOCCUPAZIONI PRINCIPALI
Errore di configurazione nei controlli di sicurezza (ad es. in una soluzione endpoint o firewall)	27%
Minacce zero-day (una minaccia che sfrutta una tecnica di attacco mai osservata prima)	27%
Carenza di personale interno con capacità/competenze di cybersecurity adeguate	25%
Credenziali e dati di accesso rubati	24%
Dispositivi privi di protezione (inclusi dispositivi non noti)	24%
Mancanza di strumenti di cybersecurity	23%
Vulnerabilità a cui non sono state applicate patch	22%
Possibilità di concedere l'accesso agli utenti remoti	20%
Reti wireless non sicure	20%
Utenti interni (incidente non intenzionale)	18%
Partner/supply chain	18%
Strumenti di accesso remoto	18%
Utenti interni (incidente intenzionale)	17%
Dispositivi IoT	17%
Altro	0%
Nessuno di questi è un rischio di cybersecurity per la mia organizzazione	0%
Non lo so	0%

Chi/cosa consideri siano i tre principali tre rischi di cybersecurity per la tua organizzazione? Combinazione di risposte con rischi classificati come primo, secondo e terzo (n=3.000)

Approcci Diversi Alle Indagini Sugli Incidenti

Le organizzazioni indagano sul **48% dei loro avvisi di sicurezza** per identificare eventuali segnali di attività pericolosa

Una delle sfide affrontate dai team di IT security è dover identificare gli avvisi sui quali occorre indagare; questo implica anche la necessità di ottimizzare il modo in cui vengono utilizzate le limitate risorse a loro disposizione.

In media, poco meno della metà (48%) di tutti gli avvisi di sicurezza viene analizzata per stabilire se si tratti di segnali di attività pericolosa; questa statistica raggiunge il 54% per le organizzazioni con 3.001-5.000 dipendenti. Tuttavia, gli approcci adottati variano molto: Il 16% delle organizzazioni indaga su più di tre quarti degli avvisi (incluso un 5% che afferma di analizzare tutti gli avvisi), mentre il 18% svolge indagini su un quarto degli avvisi o meno.

Classificando i risultati in base al settore, gli intervistati che lavorano nel settore del governo centrale/federale svolgono indagini sulla percentuale più bassa di avvisi (39%) (n=89), mentre il settore delle fonti di energia, petrolio/gas e utenze indaga sulla maggior parte di avvisi (55%) (n=69).

Le Implicazioni Dei Processi Di Rilevamento, Indagine E Risposta

Il tempo medio necessario per rilevare, indagare e rispondere a un avviso è pari a nove ore per le organizzazioni con 100-3.000 dipendenti e a 15 ore per le organizzazioni con 3.001-5.000 dipendenti. Con molta probabilità, questa variazione è dovuta alla maggiore complessità degli ambienti operativi di queste ultime.

Dal sondaggio è emersa un'enorme differenza tra i vari settori, con più del doppio di tempo richiesto per le organizzazioni che operano nell'industria manifatturiera e nella produzione (15 ore) e nel settore delle fonti di energia, petrolio/gas e utenze (18 ore), rispetto alle 6,75 ore del settore di IT, tecnologie e telecomunicazioni.

È importante tenere presente che gran parte degli avvisi non raggiunge la fase di risposta. Le tecnologie di sicurezza bloccano proattivamente la maggior parte degli attacchi, mentre un sottoinsieme di avvisi viene selezionato e segnalato per essere sottoposto a indagini. Anche le azioni di risposta sono molto diverse e questo è dovuto alla natura dell'evento che richiede correzione: potrebbe infatti trattarsi semplicemente di rimuovere un'e-mail di phishing dalle caselle di posta degli utenti, ma potrebbe anche essere necessaria la ristrutturazione completa di un'intera server farm.

Tempo medio necessario per rilevare, indagare e rispondere a un avviso

ATTIVITÀ	100-3.000 DIPENDENTI (n=2.460)	3.001-5.000 DIPENDENTI (n=350)	IT, TECNOLOGIE E TELECOMUNICAZIONI (n=98)	INDUSTRIA MANIFATTURIERA E PRODUZIONE (n=331)	FONTI DI ENERGIA, PETROLIO/GAS E UTENZE (n=66)
Rilevamento	3 ore	3 ore	1,5 ore	3 ore	6 ore
Indagine	3 ore	6 ore	2,25 ore	6 ore	6 ore
Risposta	3 ore	6 ore	3 ore	6 ore	6 ore
Totale	**9 ore**	**15 ore**	**6,75 ore**	**15 ore**	**18 ore**

Di quanto tempo ha bisogno la tua organizzazione per rilevare, indagare e, se necessario, correggere un potenziale incidente? (n=2.812 di intervistati che svolgono indagini internamente)

Alle Organizzazioni Mancano Competenze Fondamentali Di SecOps

Come abbiamo già visto, per i professionisti dell'IT la carenza di personale interno con capacità/competenze di cybersecurity adeguate è uno dei principali rischi di sicurezza per il 2023. Approfondendo ulteriormente, il sondaggio rivela che la maggior parte delle organizzazioni fa fatica a svolgere le normali mansioni quotidiane di SecOps, incluse quelle essenziali, con il 93% degli intervistati che riconosce come "problematica" almeno una delle seguenti attività:

- Identificazione dei segnali pertinenti tra tutte le informazioni non rilevanti (problematica per il 71%)
- Attribuzione della giusta priorità ai segnali/agli avvisi su cui indagare (problematica per il 71%)
- Raccolta di una quantità sufficiente di dati per stabilire se un segnale indica un pericolo o è innocuo (problematica per il 71%)
- Correzione tempestiva di avvisi o incidenti pericolosi (problematica per il 71%)
- Identificazione della root cause dell'incidente (problematica per il 75%)
- Compilazione di informazioni accurate sulle indagini (problematica per il 68%)

La sfida più comune sembra essere l'identificazione della root cause dell'incidente, segnalata come problematica dal 75% degli intervistati.

Le organizzazioni con il fatturato annuo più basso (inferiore ai 10 milioni di $) sono quelle con maggiore probabilità di avere difficoltà a svolgere le normali attività di SecOps, seguite da quelle con il fatturato più alto (superiore ai 5 miliardi di $). Entrambi gli estremi implicano ostacoli, sebbene diversi: la complessità organizzativa e dei sistemi svolgerà infatti un ruolo più significativo nelle organizzazioni più grandi.

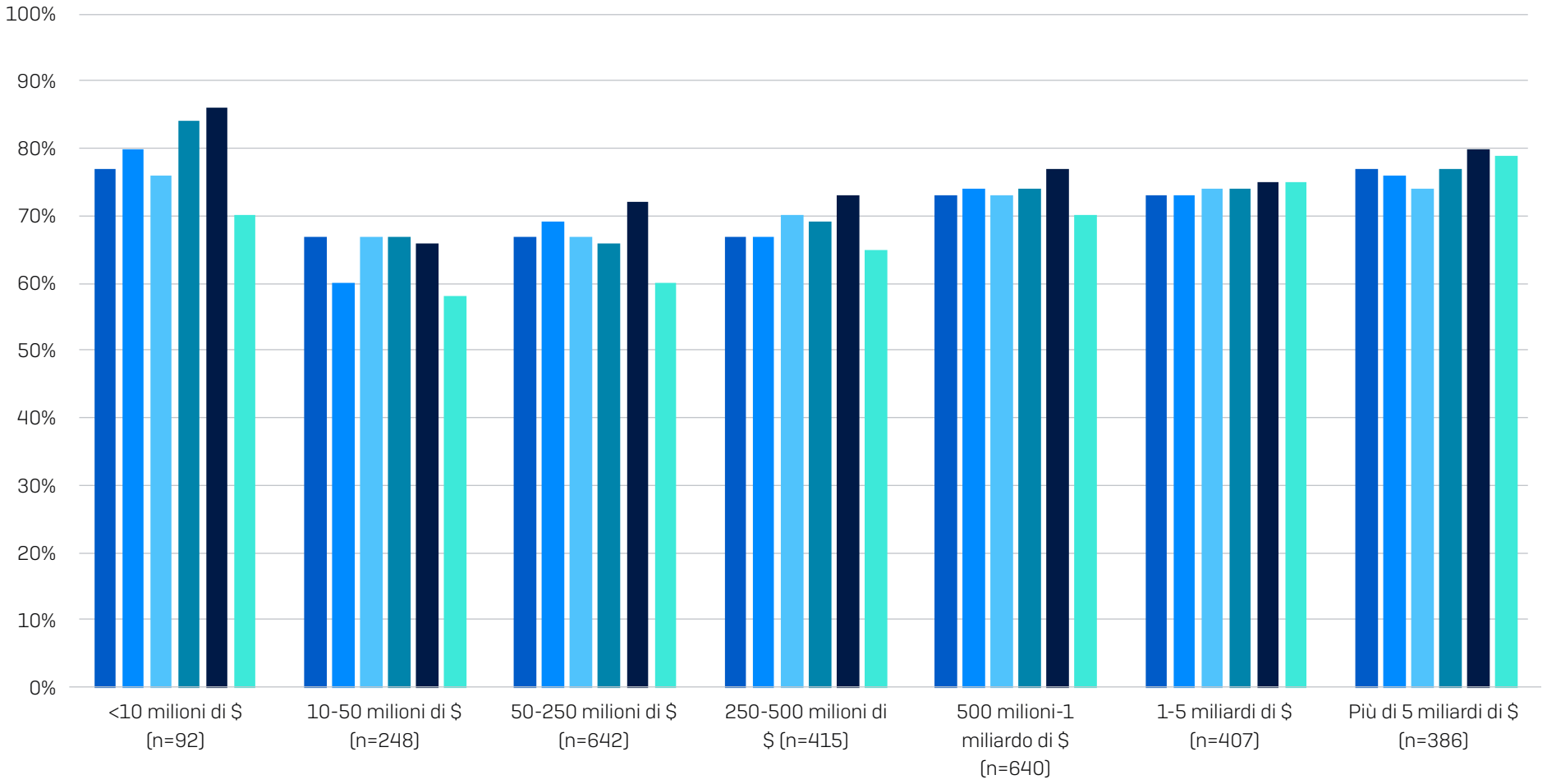
La carenza di personale provoca un effetto domino: indagare sugli avvisi richiede più tempo; questo a sua volta diminuisce la capacità dei team di svolgere attività e in ultima analisi tutto ciò porta a un incremento dell'esposizione ai rischi.

93%
Percentuale di intervistati che ha difficoltà a svolgere attività di SecOps

75%
Percentuale di intervistati che segnala come problematica l'identificazione della root cause dell'incidente

71%
Percentuale di intervistati che fa fatica a identificare gli avvisi sui quali occorre indagare

Organizzazioni che ritengono "problematiche" le attività di SecOps, in base al fatturato



Intervistati la cui organizzazione ritiene "molto problematiche" o "parzialmente problematiche" le attività di SecOps durante le attività di indagine su avvisi sospetti (n=2.812 intervistati che gestiscono internamente le indagini sugli avvisi di sicurezza)

- Identificazione dei segnali pertinenti tra tutte le informazioni non rilevanti, ovvero comprensione di quali segnali/avvisi devono essere analizzati
- Attribuzione della giusta priorità ai segnali/agli avvisi su cui indagare
- Raccolta di una quantità sufficiente di dati per stabilire se un segnale indica un elemento pericoloso o innocuo
- Identificazione della root cause dell'incidente, ovvero il modo in cui l'avversario informatico è riuscito a infiltrarsi nell'organizzazione
- Correzione tempestiva di avvisi o incidenti pericolosi
- Compilazione di informazioni accurate sulle indagini

Gli Avversari Informatici Hanno Superato I Team Informatici

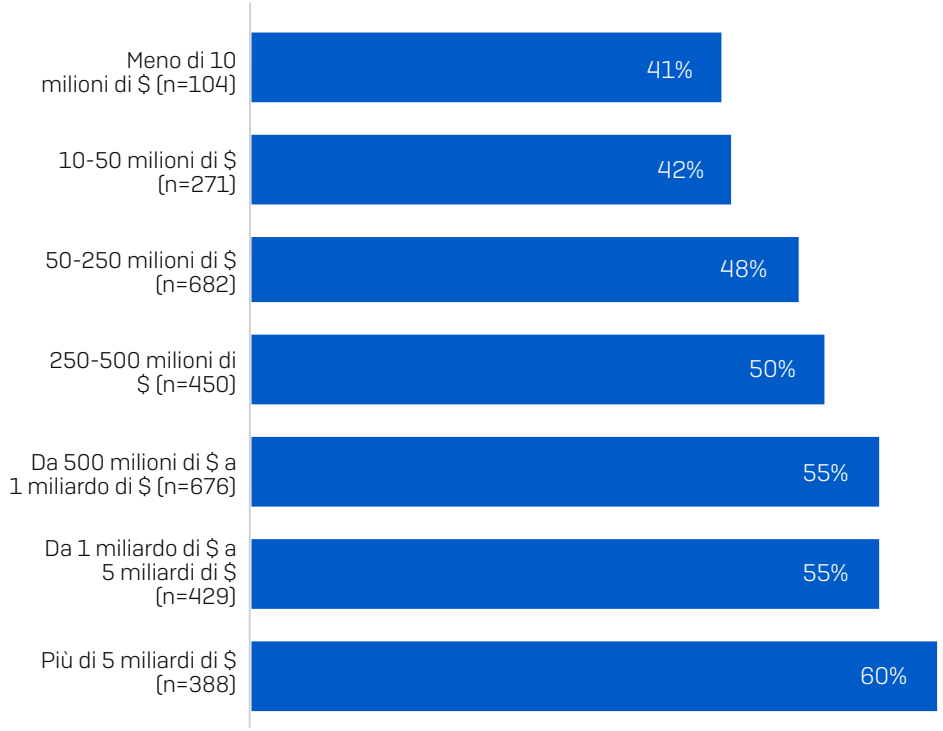
52%

Percentuale di intervistati che sostiene che le cyberminacce sono ora troppo avanzate per essere affrontate dal team tecnico della propria organizzazione senza alcun aiuto esterno

Più della metà (52%) dei professionisti IT sostiene che le cyberminacce sono ora troppo avanzate per essere affrontate dal team tecnico della propria organizzazione senza alcun aiuto esterno. Questa percentuale sale al 64% per le aziende di piccole dimensioni (100-250 dipendenti).

Parallelamente all'aumento del fatturato, cresce anche la probabilità che i team interni di un'organizzazione non riescano a tenere il passo con i malintenzionati. Molto probabilmente, questo è dovuto alla maggiore complessità dell'ambiente di cybersecurity interno nelle organizzazioni con un fatturato più alto, nonché loro alla maggiore propensione ad affidarsi a servizi di sicurezza specializzati. Potrebbe anche essere il motivo alla base di quella che sembra essere una maggiore comprensione dell'ambiente delle minacce e delle sfide implicate dalle attività di difesa contro le minacce più avanzate.

Le cyberminacce sono ora troppo avanzate per essere affrontate dal team tecnico dell'organizzazione, senza alcun aiuto esterno



In quale misura ti trovi d'accordo o in disaccordo con la seguente affermazione: le cyberminacce sono ora troppo avanzate per essere affrontate dal team tecnico della mia organizzazione senza alcun aiuto esterno. Pienamente d'accordo, parzialmente d'accordo (base di partecipanti indicata nel grafico)

L'Impatto Sul Business

L'Impatto Sulla Capacità Di Realizzazione Dei Progetti

64%
Percentuale di intervistati che preferirebbe che il team IT dedicasse più tempo ad attività di importanza strategica e meno tempo a interventi di emergenza

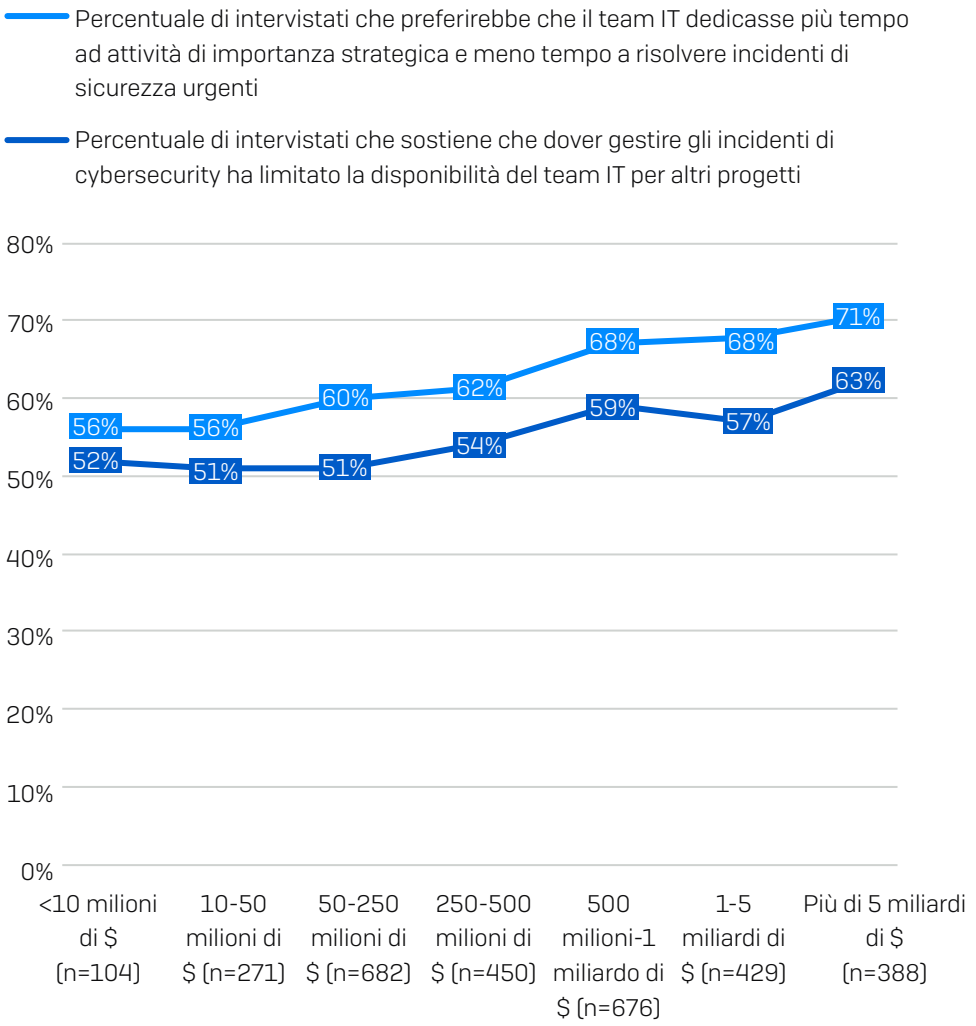
55%
Percentuale di intervistati che sostiene che dover gestire le cyberminacce ha limitato la disponibilità del team IT per altri progetti

Per il 60% delle organizzazioni, la cybersecurity e le operazioni IT sono strettamente correlate: il 52% degli intervistati ha un team IT che include un team dedicato alla cybersecuriry, mentre nell'8% dei casi è il team IT a gestire la cybersecurity. Il rimanente 40% delle organizzazioni prese in esame affida la cybersecurity e le operazioni IT a team diversi. Il tempo e l'impegno richiesti per gestire la cybersecurity implicano conseguenze tangibili su come viene organizzato l'ambiente informatico.

Più della metà (55%) delle organizzazioni sostiene che dover gestire le cyberminacce ha avuto un impatto negativo sulla capacità del proprio team IT di dedicarsi ad altri progetti, e l'impatto è più sentito tra le organizzazioni con un fatturato più alto.

La natura urgente e imprevedibile della cybersecurity ostacola anche le iniziative di maggiore impatto commerciale: in media, il 64% degli intervistati preferirebbe infatti che il team IT dedicasse più tempo ad attività di importanza strategica e meno tempo a interventi di emergenza. Anche in questo caso, a un aumento del fatturato corrisponde un maggiore impatto sulla capacità di realizzazione dei progetti.

L'impatto negativo della cybersecurity sulla capacità di realizzazione dei progetti



In quale misura ti trovi d'accordo o in disaccordo con la seguente affermazione: dover gestire gli incidenti di cybersecurity ha limitato la disponibilità del team IT per altri progetti, preferirei che il team IT dedicasse più tempo ad attività di importanza strategica e meno tempo a risolvere incidenti di sicurezza urgenti (base di partecipanti indicata nel grafico)

L'Impatto Finanziario

Quello della cybersecurity è un ambiente difficile, che implica varie ripercussioni finanziarie per un'organizzazione. I costi più alti per un singolo incidente si presentano quando si verifica un incidente informatico molto grave. Come indicato nel report Sophos La Vera Storia Del Ransomware 2022, il costo medio per rimediare ai danni del ransomware è pari a 1,4 milioni di $.

Tuttavia, l'impatto finanziario di dover gestire gli attacchi informatici non riguarda solo i costi di rimozione del malware. Con uno stipendio annuo medio appena inferiore ai 100.000 $ per un tecnico specializzato di IT security negli Stati Uniti[2], il costo orario (in termini di risorse umane) di ciascun avviso di sicurezza è piuttosto alto. Anche se gli stipendi variano in base alle condizioni locali, l'impatto finanziario del lunghissimo processo di indagine sull'incidente è tutt'altro che irrisorio.

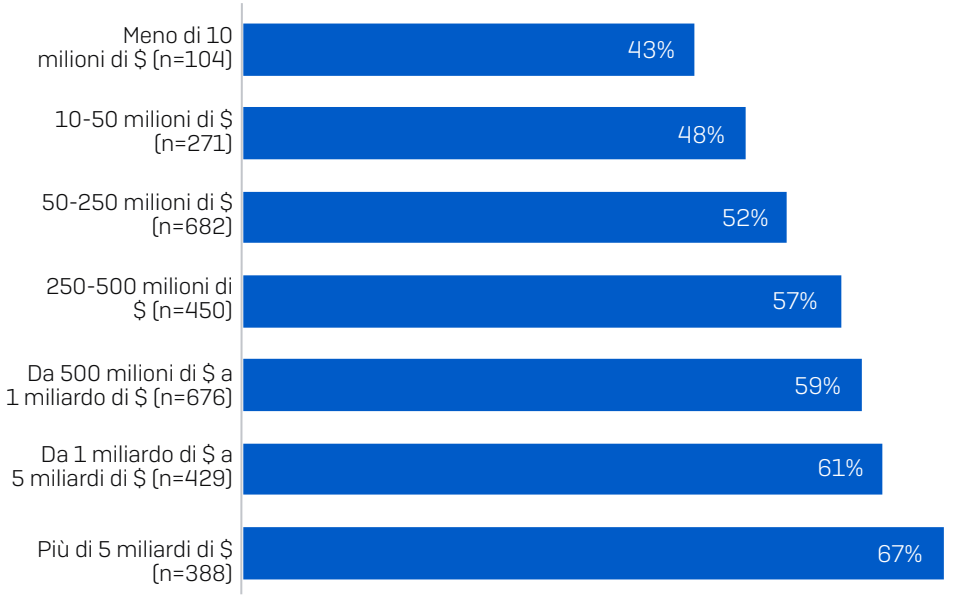
L'Impatto Sulle Risorse

Il 57% degli intervistati confessa che a volte il pensiero che l'organizzazione possa essere colpita da un attacco informatico gli impedisce di dormire. Considerando gli elevatissimi costi implicati dall'assunzione e dalla fidelizzazione di personale in questo campo, ne risulta una grande preoccupazione sia in termini di benessere psico-fisico, sia dal punto di vista finanziario. Inoltre, questo scenario indica che i team di IT security non nutrono piena fiducia nei propri strumenti di sicurezza.

Lo stress è un problema molto grave nell'ambito della cybersecurity. L'eccessiva quantità di avvisi e di lavoro da svolgere esercita una forte pressione sui dipendenti. Se sono oberati di lavoro, i team hanno maggiore probabilità di lasciarsi sfuggire segnali importanti. Questo contribuisce a incrementare ulteriormente la pressione a cui sono esposti questi dipendenti. Gli esseri umani hanno un limite e prima o poi cederanno sotto il peso dello stress.

La tendenza degli intervistati a non riuscire a dormire a causa delle preoccupazioni di cybersecurity aumenta in maniera direttamente proporzionale al fatturato dell'organizzazione in cui lavorano: la percentuale passa infatti dal 43% delle organizzazioni con un fatturato annuo di meno di 10 milioni di $, al 67% delle organizzazioni che hanno più di 5 miliardi di $ di fatturato.

Percentuale di intervistati che confessa che il pensiero che l'organizzazione possa essere colpita da un attacco informatico gli impedisce di dormire



In quale misura ti trovi d'accordo o in disaccordo con la seguente affermazione: a volte il pensiero che l'organizzazione possa essere colpita da un attacco informatico mi impedisce di dormire (base di partecipanti indicata nel grafico)

2 In base allo stipendio medio di un tecnico specializzato di IT security nel mese di marzo 2023, https://www.indeed.com/career/it-security-specialist/salaries

Raccomandazioni

Per affrontare queste sfide serve un approccio diretto e a tre fasi, che includa: 1. l'implementazione di un processo di incident response più scalabile, in grado di accelerare i tempi di risposta; 2. l'uso di sistemi di difesa adattivi per rallentare gli avversari informatici; e 3. la creazione di un circolo virtuoso per incrementare la protezione e ridurre i costi.

Un'analogia utile è la strategia bellica dell'"alzata di scudi". Per bloccare avversari informatici estremamente abili e persistenti, le organizzazioni devono ottimizzare le proprie difese (alzando appunto gli "scudi"), integrando tecnologie sensibili al contesto, in grado di elevare il livello di protezione in base al contesto. E soprattutto, le organizzazioni devono sfruttare il tempo che guadagnano utilizzando queste difese per incorporare nei processi le competenze umane necessarie per eliminare la root cause.

L'Uso Di Tecnologie Potenti È Un Must

La qualità delle tue tecnologie di cybersecurity è fondamentale, e i controlli di sicurezza che adotti devono garantire:

- **Ottimizzazione della prevenzione**, rilevando e bloccando automaticamente quante più minacce possibili nelle prime fasi della catena di attacco. In questo modo, potrai ridurre il rischio a cui è esposta la tua organizzazione, sollevando il personale di cybersecurity da vari oneri e offrendo a questo team la possibilità di concentrarsi su una quantità minore di incidenti.
- **Riduzione dell'esposizione ai rischi**, semplificando i processi volti a verificare che le soluzioni di sicurezza acquistate siano state implementate in maniera corretta e ottimale, prevenendo gli errori di configurazione.
- **Blocco degli avversari informatici**. Le tecnologie che rilevano e bloccano immediatamente l'attività dei cybercriminali sono frustranti per gli hacker e aiutano il team di cybersecurity a guadagnare tempo prezioso per neutralizzare l'incidente.

Ottimizzazione della prevenzione

Blocca tempestivamente gli attacchi, per diminuire l'impatto sui sistemi

Riduzione dell'esposizione ai rischi

Limita le opportunità di cui possono approfittare gli avversari informatici per sfruttare lacune o vulnerabilità dei sistemi di sicurezza

Blocco degli avversari informatici

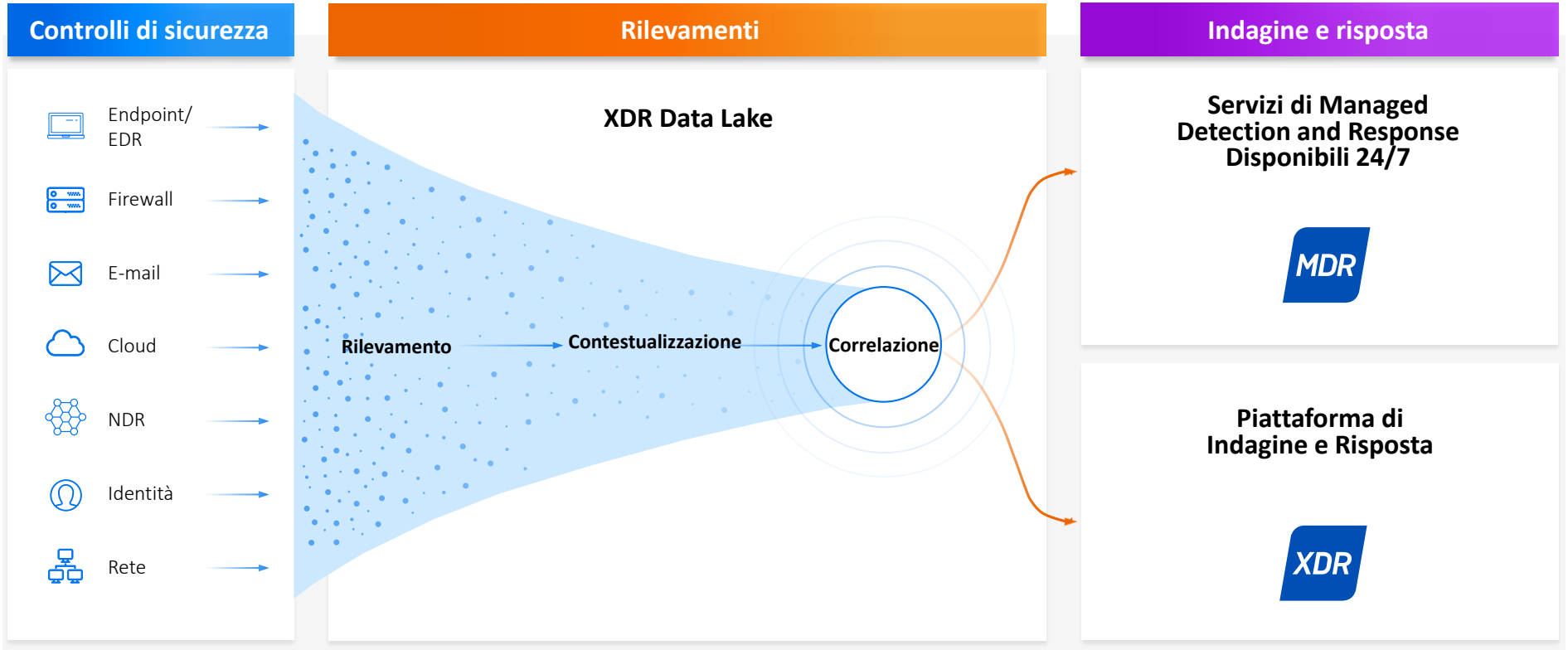
Regala tempo prezioso ai team di IT security, quando affrontano attacchi avanzati e coordinati da una mente umana

Risolvi Il Problema Principale Con Le Giuste Persone E Tecnologie

I sistemi di protezione regalano tempo prezioso ai responsabili di IT security, che possono così svolgere indagini e rispondere agli attacchi. Tuttavia, non garantiscono una prevenzione efficace al 100% ed è per questo motivo che è indispensabile eliminare la root cause in maniera tempestiva, informata e strategicamente corretta.

Come indicano i risultati del nostro studio, gli avversari informatici si muovono in varie direzioni. L'uso della telemetria nell'intero ambiente di sicurezza, sfruttando i controlli di sicurezza già implementati dalle organizzazioni, permette ai team di cybersecurity di intercettare e rispondere alle minacce più rapidamente, incrementando così il ritorno sull'investimento nelle tecnologie attuali.

Spesso, individuare attività dannose tra tutti gli avvisi relativi a eventi innocui può essere paragonabile alla ricerca del proverbiale ago nel pagliaio, se non addirittura alla ricerca di un ago specifico in una montagna di aghi. Elaborare i segnali con una piattaforma di Extended Detection and Response (XDR) in grado di aggiungere informazioni contestuali e di connettere gli avvisi correlati permette ai team di cybersecurity di un'organizzazione di dedicare rapidamente la propria attenzione agli elementi più importanti. L'indagine e la risposta possono essere svolte dal team interno, utilizzando una piattaforma XDR. In alternativa, le organizzazioni possono affidare le attività di rilevamento, indagine e risposta a un servizio esterno, composto da tecnici specializzati in Managed Detection and Response (MDR).



Accelerare I Meccanismi Di Difesa

Quando un meccanismo viene messo in moto e fatto procedere ad alta velocità, è difficile fermarlo. Più viene fatto girare, più il meccanismo va veloce. Le organizzazioni possono accelerare il proprio meccanismo di cybersecurity utilizzando una combinazione ottimale tra tecnologie di sicurezza e competenze umane. L'applicazione di controlli di sicurezza completi riduce la quantità di avvisi che devono essere esaminati dai responsabili di IT security, permettendo così a questo team di concentrarsi sulla neutralizzazione degli attacchi e sul miglioramento del profilo di sicurezza aziendale. Tutto ciò consente a sua volta di incrementare l'efficacia dei controlli di sicurezza, generando così un circolo virtuoso.

La Maggior Parte Delle Organizzazioni Ha Intenzione Di Implementare I Controlli Di Sicurezza e I Servizi Necessari

Dal sondaggio è emerso che la maggior parte delle organizzazioni ha intenzione di aggiungere al proprio stack ulteriori soluzioni di rilevamento e risposta alle minacce nei prossimi 12 mesi. Più di tre quarti (78%) degli intervistati prevedono di aggiungere strumenti di Endpoint Detection and Response (EDR) e/o Extended Detection and Response (XDR) l'anno prossimo.

L'indagine e la risposta a cyberminacce avanzate sono competenze tecniche molto avanzate e per garantire il monitoraggio 24/7 dei sistemi occorrono da cinque a sei persone. Come indica il fatto che nei tre principali rischi di sicurezza percepiti per il 2023 identificati nel sondaggio c'è la carenza di personale interno con capacità/competenze di cybersecurity adeguate, molte organizzazioni scelgono di rivolgersi a esperti esterni per ricevere assistenza: il 44% delle organizzazioni ha infatti intenzione di cominciare a collaborare con un fornitore di servizi di Managed Detection and Response (MDR) nei prossimi 12 mesi.

Percentuale di organizzazioni che hanno intenzione di adottare soluzioni di rilevamento e risposta nei prossimi 12 mesi

78%	**44%**
EDR/XDR	MDR

Sophos Può Aiutarti

Sophos offre servizi e tecnologie che permettono alle organizzazioni di accelerare i meccanismi di difesa e superare gli avversari informatici. Proteggiamo oltre 550.000 organizzazioni contro le minacce più avanzate e Sophos MDR è il servizio MDR più utilizzato in assoluto a livello globale.

Comincia Subito Con I Sistemi Di Difesa Più Potenti

Le nostre soluzioni per endpoint/EDR, firewall, e-mail, rete e cloud rallentano i cybercriminali, regalando ai team di IT security tempo prezioso e fornendo tutte le informazioni di cui hanno bisogno per avviare un'azione di risposta:

- **Ottimizzazione della prevenzione:** Sophos blocca automaticamente il 99,98% delle minacce prima che riescano a infiltrarsi nei sistemi, riducendo il rischio e permettendo ai team di IT security di concentrarsi su un numero ristretto di incidenti che richiedono un intervento umano
- **Riduzione dell'esposizione ai rischi:** fin dal primo giorno vengono implementate impostazioni di protezione ottimali, eliminando qualsiasi lacuna di sicurezza. Gli Account Health Check integrati indicano quando mancano software essenziali e segnalano eventuali problemi di configurazione che possono portare a infezioni prevenibili.
- **Blocco degli avversari informatici.** La protezione adattiva contro gli active adversary attiva automaticamente un sistema di difesa avanzato non appena viene rilevata un'intrusione di tipo "hands-on-keyboard", generando una situazione frustrante per gli hacker e aiutando il team di IT security a guadagnare tempo prezioso per avviare un'azione di risposta.

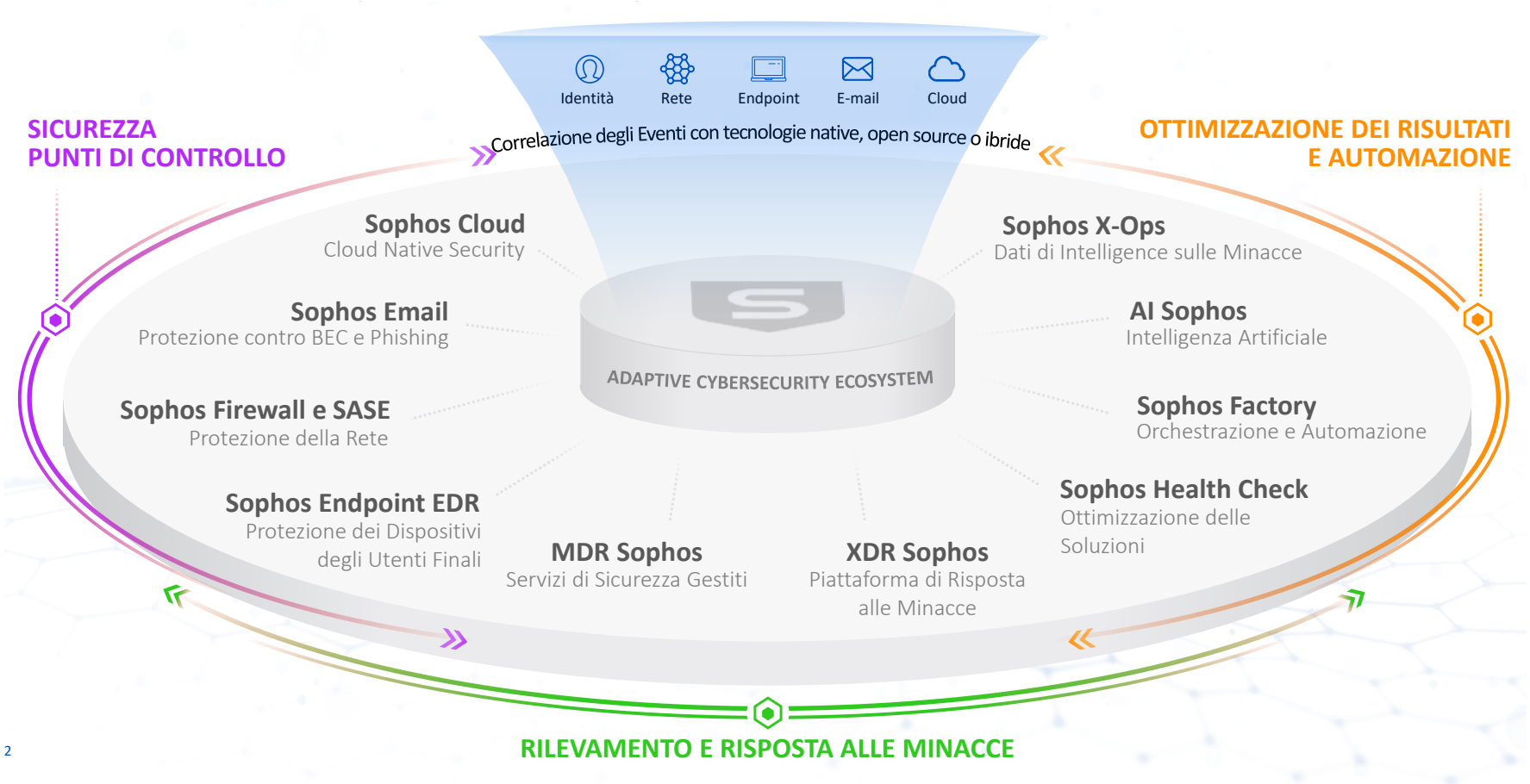
Ottimizza Il Rilevamento, Le Indagini E La Risposta

Quando i team di IT security hanno maggiore visibilità, possono agire in maniera più veloce. Sophos utilizza rilevamenti provenienti dall'intero ecosistema di strumenti di protezione, integrando la telemetria dei controlli di sicurezza Sophos e di terze parti, per accelerare i processi di rilevamento e risposta, ottimizzando così il ritorno sull'investimento nelle soluzioni attualmente utilizzate dai clienti.

Il servizio Sophos MDR mette a tua disposizione le competenze di oltre 500 tecnici specializzati, che individuano proattivamente le minacce, svolgono indagini e rispondono agli active adversary e ad altri attacchi per conto tuo a qualsiasi ora del giorno e della notte. Con un tempo di risposta medio di appena 38 minuti, Sophos MDR è nettamente più rapido dei team interni. Alternativamente, le organizzazioni possono optare per la piattaforma Sophos XDR, che include funzionalità complete di EDR e permette di svolgere indagini e rispondere agli attacchi autonomamente o collaborando con il team Sophos MDR.

Qualsiasi sia la fase di crescita in cui si trova la tua organizzazione e qualunque sia la tua visione per il futuro, Sophos può aiutarti ad accelerare i tuoi meccanismi di difesa e passare in testa, anche in presenza di avversari informatici estremamente abili. Per saperne di più, visita www.sophos.it o parla con uno dei nostri consulenti di sicurezza.

Ottieni Risultati Di Cybersecurity Ottimali Con Sophos



29/03/2023 (WP-NP)

SOPHOS