RAPPORTO

Rapporto 2022 sullo stato dell'Operational Technology e della Cybersecurity

SOMMARIO

Infografica: risultati in evidenza

Persone

Il **33%** delle organizzazioni affida la sicurezza OT al vicepresidente/direttore del reparto addetto alla gestione tecnica e operativa della rete

Il **67%** dei responsabili della sicurezza OT proviene da una formazione tecnica OT

Il **43%** degli intervistati considera il tempo di risposta agli incidenti di sicurezza come una delle tre principali misure di successo

Strategia di sicurezza

Il **56%** delle organizzazioni dichiara di aver raggiunto un livello di maturità 3 o 4 nel campo della sicurezza OT

Il **50%** afferma che la strategia è un fattore significativo per il punteggio di rischio globale nel campo della sicurezza OT

Il **13%** delle organizzazioni ha una visibilità centralizzata di tutte le attività OT

Prassi di sicurezza

Il **48%** segnala le compromissioni della sicurezza alla direzione esecutiva

Il **32%** ha distribuito il controllo degli accessi alla rete basato sui ruoli

Il **52%** afferma che tutte le attività OT sono monitorate e seguite dal SOC

Risultati in termini di sicurezza

Il **93%** delle organizzazioni ha subito più di un'intrusione nell'ultimo anno; il **78%** ne subite più di 3

Il **61%** delle intrusioni ha colpito i sistemi OT

Nel **90%** delle intrusioni sono state necessarie ore, se non di più, per ripristinare il servizio

Best practice

È più probabile che le organizzazioni top-tier

- Abbiano una visibilità centralizzata
- Si misurino in base al tempo di risposta alle vulnerabilità
- Distribuiscano un controllo degli accessi alla rete
- Segnalino le compromissioni della sicurezza
- Si avvalgano di un unico fornitore di dispositivi OT

Sintesi preliminare

Il Rapporto 2022 sullo statodell'Operational Technology e della Cybersecurity, giunto alla sua quarta edizione annuale, rileva che le organizzazioni si stanno muovendo ancora troppo lentamente verso una protezione completa delle loro risorse di tecnologia operativa (OT, Operational Technology). Questo avviene in un momento in cui i sistemi OT stanno diventando sempre più importanti per il benessere di molte organizzazioni, gli eventi geopolitici rendono più probabili gli attacchi, un numero sempre maggiore di sistemi OT è connesso a Internet e le minacce basate su IP stanno diventando più avanzate e provocano più danni. Questa combinazione di fattori rende sempre più necessaria la presenza di soluzioni di sicurezza OT nel portfolio di rischi di molte organizzazioni.

Sulla base di un'indagine globale condotta su oltre 500 professionisti della sicurezza OT, il rapporto di quest'anno rileva che, sebbene la sicurezza OT sia al centro dell'attenzione dei leader delle organizzazioni, continua ad essere appannaggio di professionisti di livello relativamente basso. Le speculazioni sul fatto che la sicurezza OT passerà sotto la responsabilità del CISO si sono susseguite a ritmo serrato per anni, ma non c'è alcun segno che le cose si stiano muovendo in questa direzione. Inoltre, sebbene la sicurezza faccia parte delle misurazioni delle prestazioni per la maggior parte degli intervistati, molti sono incentrati più sui fattori di efficienza che potrebbero indurre a tagliare i ponti con la sicurezza.

Sulla base di un'indagine globale condotta su oltre 500 professionisti della sicurezza OT, il rapporto di quest'anno rileva che, sebbene la sicurezza OT sia al centro dell'attenzione dei leader delle organizzazioni, continua ad essere appannaggio di professionisti di livello relativamente basso.

Le organizzazioni registrano modesti passi in avanti nella maturità complessiva del loro approccio alla sicurezza OT, con un numero leggermente superiore di organizzazioni che hanno raggiunto il livello 3. Ma l'analisi di specifiche best practice mette in risalto qualche sfumatura. Solo il 13% degli intervistati ha ottenuto una visibilità centralizzata di tutte le attività OT e solo il 52% è in grado di monitorare tutte le attività OT dal centro operativo di sicurezza (SOC, Security Operations Center). Solo circa la metà degli intervistati dichiara di monitorare e segnalare varie metriche di sicurezza di base e meno della metà degli intervistati utilizza una qualsiasi delle decine di tecnologie e prassi di sicurezza specifiche. Quest'ultimo dato indica una diversità nel modo in cui le organizzazioni affrontano la sicurezza OT e riflette un mercato ancora in evoluzione.

Un aspetto che è migliorato pochissimo nell'ultimo anno è quello dei risultati delle organizzazioni in termini di sicurezza. Il 93% delle organizzazioni ha subito un'intrusione negli ultimi 12 mesi e il 78% ne ha subite più di tre. Gli impatti sono stati: tempi di inattività, perdite finanziarie o di dati, discredito del marchio e persino riduzione della sicurezza fisica. È chiaro che la maggior parte delle organizzazioni ha ancora del lavoro da svolgere. Fortunatamente, una piccola percentuale di intervistati è riuscita a evitare le intrusioni nell'ultimo anno e questo rapporto identifica alcune delle best practice che è più probabile vengano applicate.

Introduzione

Sebbene l'OT sia meno visibile dell'IT nella maggior parte delle organizzazioni e certamente nella coscienza pubblica, non è meno importante per l'economia e per la vita quotidiana delle persone. Dopotutto, i sistemi OT controllano le infrastrutture critiche da cui tutti dipendono: la rete elettrica, i sistemi idrici e fognari, le condutture di carburante, le centrali elettriche e le reti di trasporto. Ed è essenziale per la produzione di tutti i tipi di beni.

L'OT è una componente importante della trasformazione digitale nelle organizzazioni industriali. Le condizioni di mercato in rapida evoluzione hanno reso l'adozione di metodologie e tecnologie "Industria 4.0" praticamente indispensabile già prima del COVID-19. La pandemia ha solo accelerato queste tendenze, lasciando che i "non addetti ai lavori" della tecnologia si affannassero ad aggiornare e semplificare le loro operazioni.[1]

Minacce alla sicurezza in crescita

Questa tendenza non è sfuggita agli autori di minacce. Lo scorso anno, il Global Threat Landscape Report di FortiGuard Labs ha rilevato un aumento significativo dei rilevamenti di sistemi di prevenzione delle intrusioni (IPS, Intrusion Prevention System) nei sistemi OT.[2] Questa osservazione ha coinciso con diversi eventi di sicurezza di alto profilo che hanno interessato i sistemi OT, tra cui gli attacchi ransomware a Colonial Pipeline e JBS che hanno interrotto le forniture di carburante e carne in Nord America lo scorso maggio e giugno.[3]

Uno dei motivi per cui gli attacchi informatici sono aumentati con i sistemi OT nell'ultimo decennio è che sono diventati più vulnerabili agli attacchi provenienti dall'esterno. Mentre i sistemi OT erano tradizionalmente separati dai sistemi IT, oggi queste due infrastrutture sono quasi universalmente integrate. Ciò significa che i sistemi OT sono ora connessi a Internet e teoricamente accessibili da qualsiasi luogo. Questo rappresenta di per sé un aumento significativo della superficie di attacco per le organizzazioni industriali e la crescente ubiquità dei dispositivi Industrial-Internet-of-Things (IIoT) estende ulteriormente tale superficie di attacco. Allo stesso tempo, i sistemi OT connessi sono vulnerabili a un panorama di minacce IT sempre più avanzato.

L'invasione dell'Ucraina da parte della Russia e gli eventi correlati hanno acceso un altro riflettore sulla sicurezza OT. Nell'aprile 2022, la Cybersecurity and Infrastructure Security Agency (CISA) statunitense, insieme alle sue controparti in Australia, Canada, Nuova Zelanda e Regno Unito, ha avvertito che gli aggressori russi sponsorizzati dallo Stato hanno intensificato i loro sforzi in risposta alle dannose sanzioni imposte dall'Occidente. Le agenzie esortano i responsabili delle reti di infrastrutture critiche "a prepararsi e ad attenuare le potenziali minacce informatiche, tra cui malware distruttivo, ransomware, attacchi DDoS e spionaggio informatico, rafforzando le proprie difese informatiche e applicando principi di due diligence nell'identificazione degli indicatori di attività dannose".[4]

In effetti, si è verificato un aumento degli attacchi attribuiti alla Russia e le organizzazioni ucraine ne hanno fatto le spese.[5] Ma le organizzazioni del resto del mondo sono tutt'altro che immuni, con sette fornitori di infrastrutture critiche nazionali (CNI, Critical National Infrastructure) su 10 nel Regno Unito che hanno segnalato un aumento degli attacchi informatici dall'inizio del conflitto.[6]

Un'attenzione crescente alla sicurezza OT

Il risultato è che le aziende di molti settori si stanno dando da fare per garantire la sicurezza di sistemi OT sempre più vulnerabili. Una ricerca condotta per Fortinet da Westlands Advisory[7] rileva che gli investimenti in tecnologie di sicurezza IT/OT e OT specifiche ammontano a 6,9 miliardi di dollari per tutto il 2022. E questi investimenti stanno aumentando più rapidamente rispetto alla spesa per la sicurezza informatica correlata esclusivamente all'IT, con un tasso di crescita annuale composto (CAGR, Compound Annual Growth Rate) previsto del 21% per la sicurezza OT e del 16% per la sicurezza informatica OT/IT da qui al 2027.

Sebbene l'aumento degli investimenti sia un segnale molto positivo, questo rapporto rileva che, nel complesso, le organizzazioni rappresentate nell'indagine di quest'anno hanno ancora una notevole strada da percorrere per proteggere adeguatamente i propri sistemi OT. Tuttavia, un piccolo sottoinsieme di intervistati ha superato gli ultimi 12 mesi senza subire intrusioni e questo rapporto cerca di evidenziare alcuni degli aspetti positivi di queste organizzazioni.

Metodologia di studio

Il Rapporto sullo stato della tecnologia operativa e sulla sicurezza informatica di quest'anno si basa su un'indagine condotta tra il 14 e il 18 marzo 2022 su oltre 500 professionisti del settore OT. Le domande dell'indagine rispecchiano in gran parte quelle poste in indagini analoghe del 2019, 2020 e 2021, riportate nelle versioni precedenti di questo rapporto. Gli intervistati hanno risposto a 40 domande sullo stato della loro infrastruttura di sicurezza OT e OT, sulle best practice di sicurezza e sul processo di selezione dei fornitori.

Diverse aree geografiche, ruoli lavorativi, settori e dispositivi

Una differenza nella coorte dell'indagine di quest'anno rispetto agli anni precedenti è che questo studio è di natura globale piuttosto che focalizzato sul Nord America (Figura 1). Complessivamente, gli intervistati provengono da 28 paesi, di cui 150 in Nord America (NA), 70 in America Latina (LATAM), 130 in Europa, Medio Oriente e Africa (EMEA) e 170 in Asia-Pacifico (APAC).

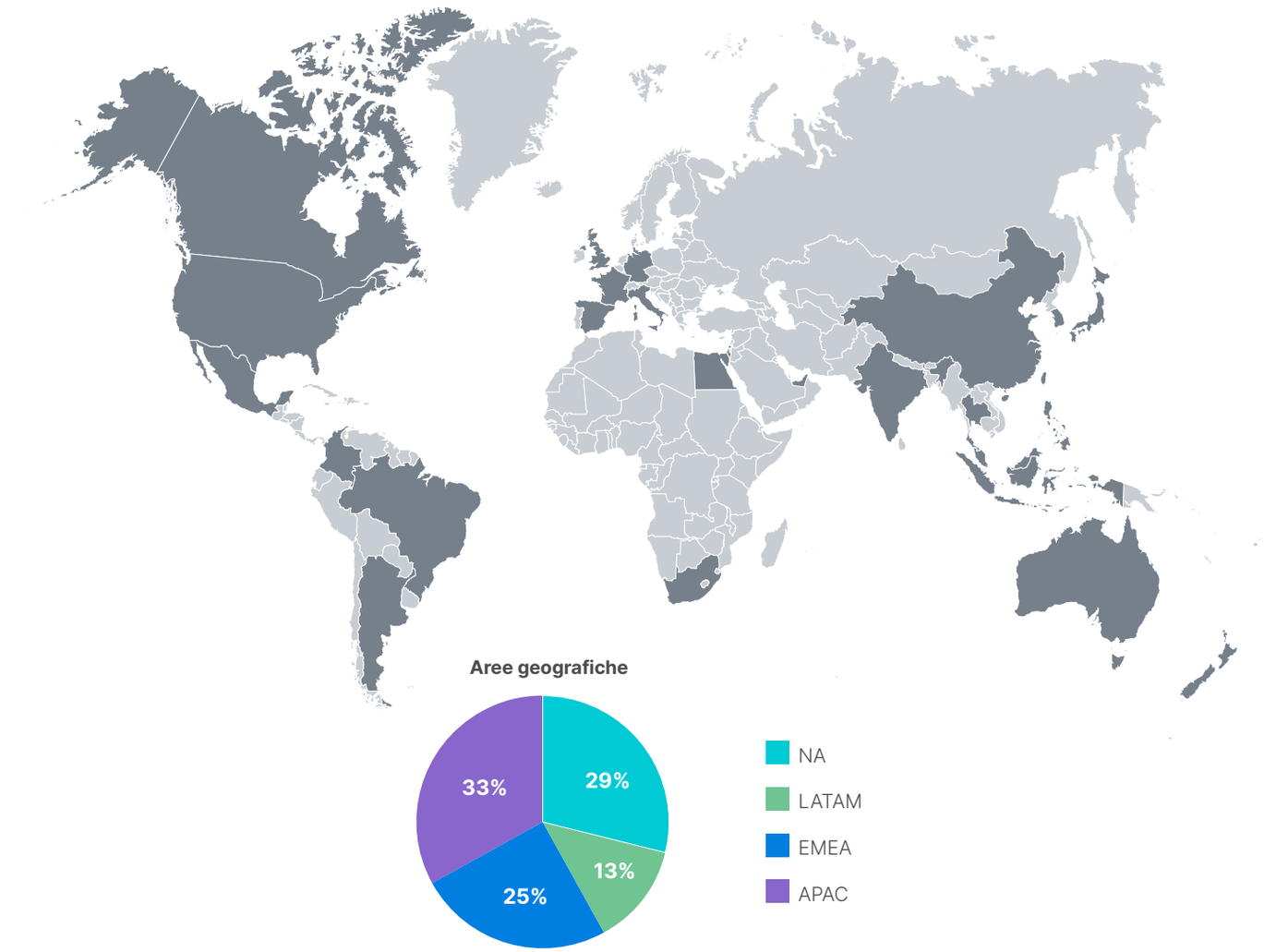


Figura 1: paesi e aree geografiche rappresentati nell'indagine.

L'indagine si è rivolta a persone che ricoprono posizioni di leadership responsabili della sicurezza OT e OT, dai responsabili agli alti dirigenti (Figura 2). Rappresentano una serie di settori industriali che fanno largo uso di OT, tra cui industria manifatturiera, trasporti e logistica e sanità. Sei intervistati su 10 sono i responsabili finali delle decisioni di acquisto di sistemi OT e l'85% dichiara di essere regolarmente consultato sugli acquisti in fatto di sicurezza informatica (Figura 3).

Gli intervistati utilizzano sistemi di controllo industriale (ICS, Industrial Control System) e dispositivi di controllo di supervisione e acquisizione dati (SCADA, Supervisory Control and Data Acquisition) di 15 diversi fornitori (Figura 4). Come negli anni precedenti, Honeywell e Siemens rimangono i marchi più utilizzati dagli intervistati, con un numero maggiore di utenti Honeywell e Schneider rispetto agli anni precedenti. L'uso di Siemens e Yokogawa è diminuito significativamente nello stesso periodo. Alcuni di questi cambiamenti riflettono la più ampia rappresentazione geografica dell'indagine di quest'anno.

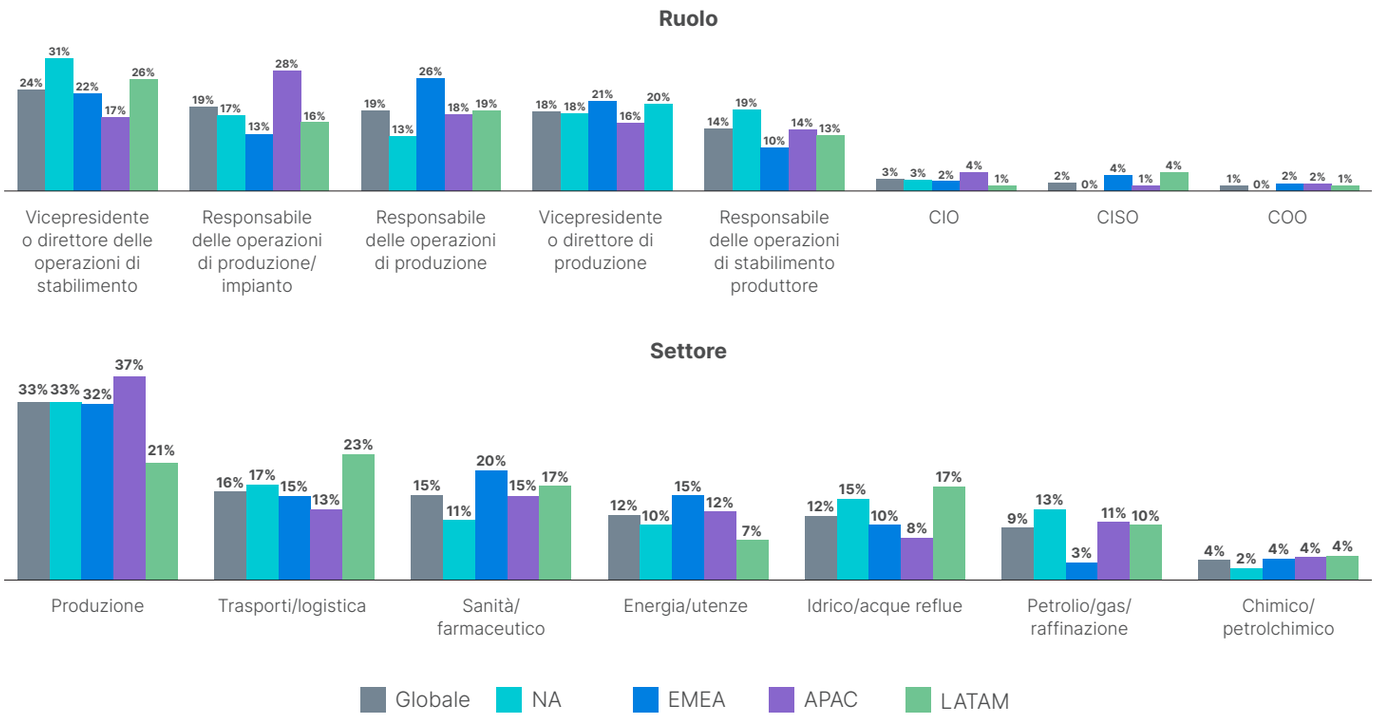


Figura 2: ruoli lavorativi e settori per area geografica.

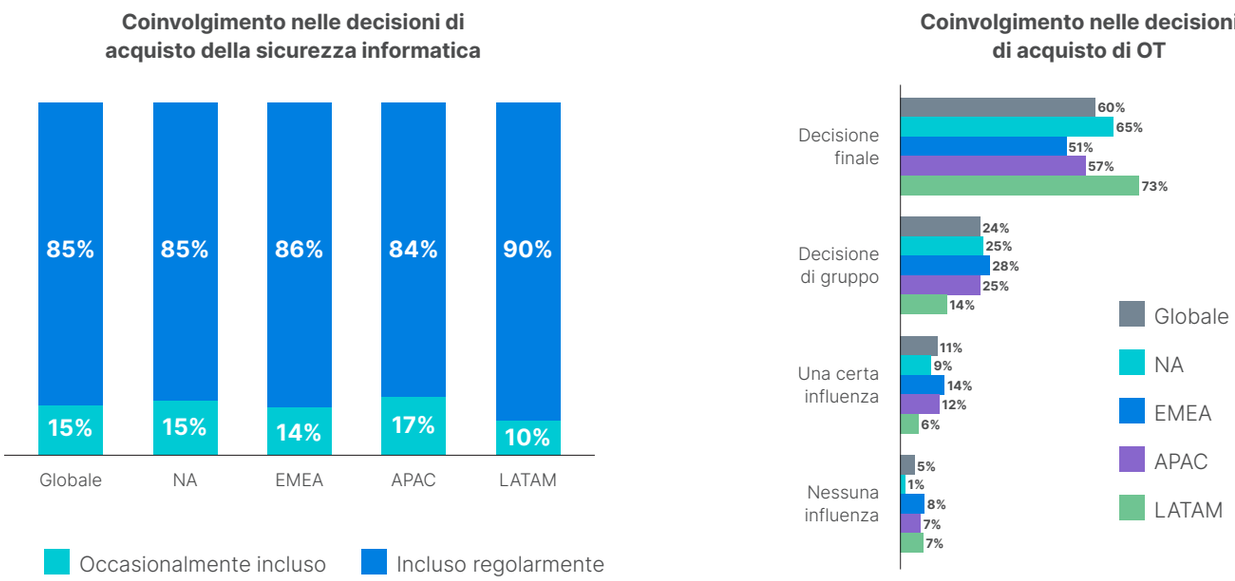


Figura 3: ruolo degli intervistati negli acquisti di sicurezza informatica e OT.

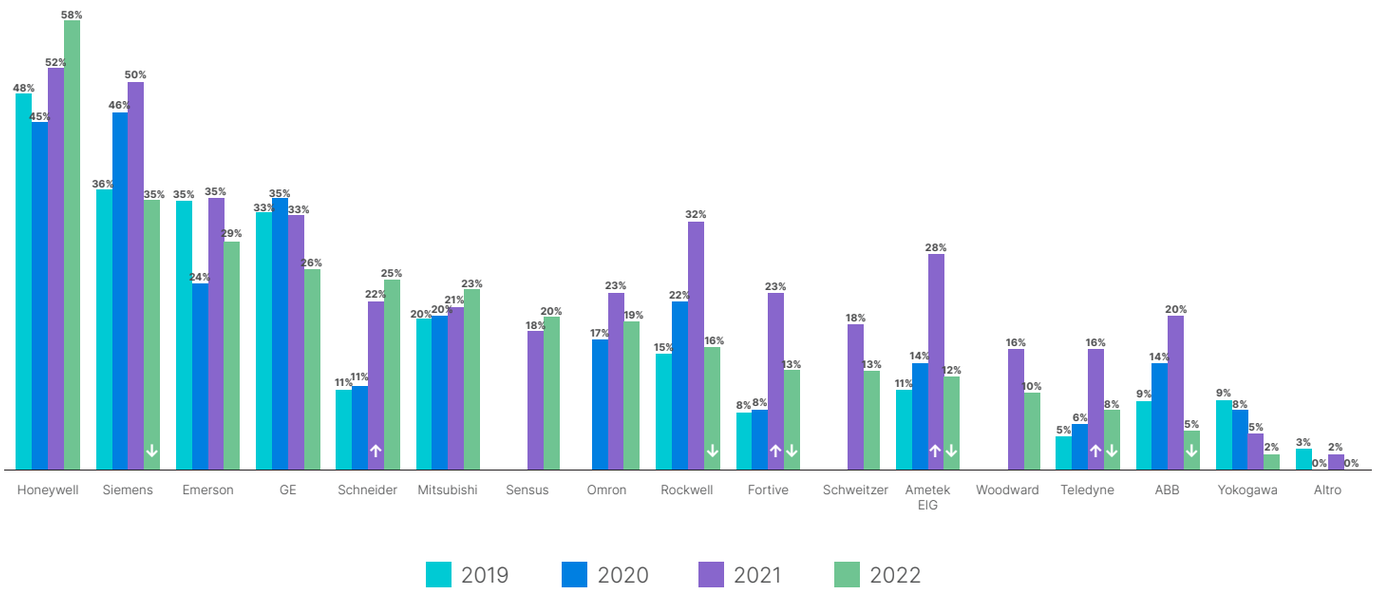


Figura 4: fornitori dei dispositivi OT in uso.

Identificazione degli insight e delle best practice

Questo rapporto analizza i dati per l'intera coorte e in base all'area geografica e al settore. Vengono inoltre confrontati i risultati nordamericani dell'indagine di quest'anno con indagini simili condotte in Nord America nel 2019, 2020 e 2021. Da questa analisi, sono stati individuati cinque punti chiave sullo stato della sicurezza informatica OT oggi.

Nella sezione finale del rapporto, vengono analizzate le risposte all'indagine in base ai risultati effettivi degli intervistati in materia di sicurezza, confrontando le organizzazioni che non sono state soggette a intrusioni nell'ultimo anno con quelle che ne hanno subito più di 10. Da questo confronto emergono diverse best practice alle quali le organizzazioni "top-tier" hanno maggiori probabilità di aderire.

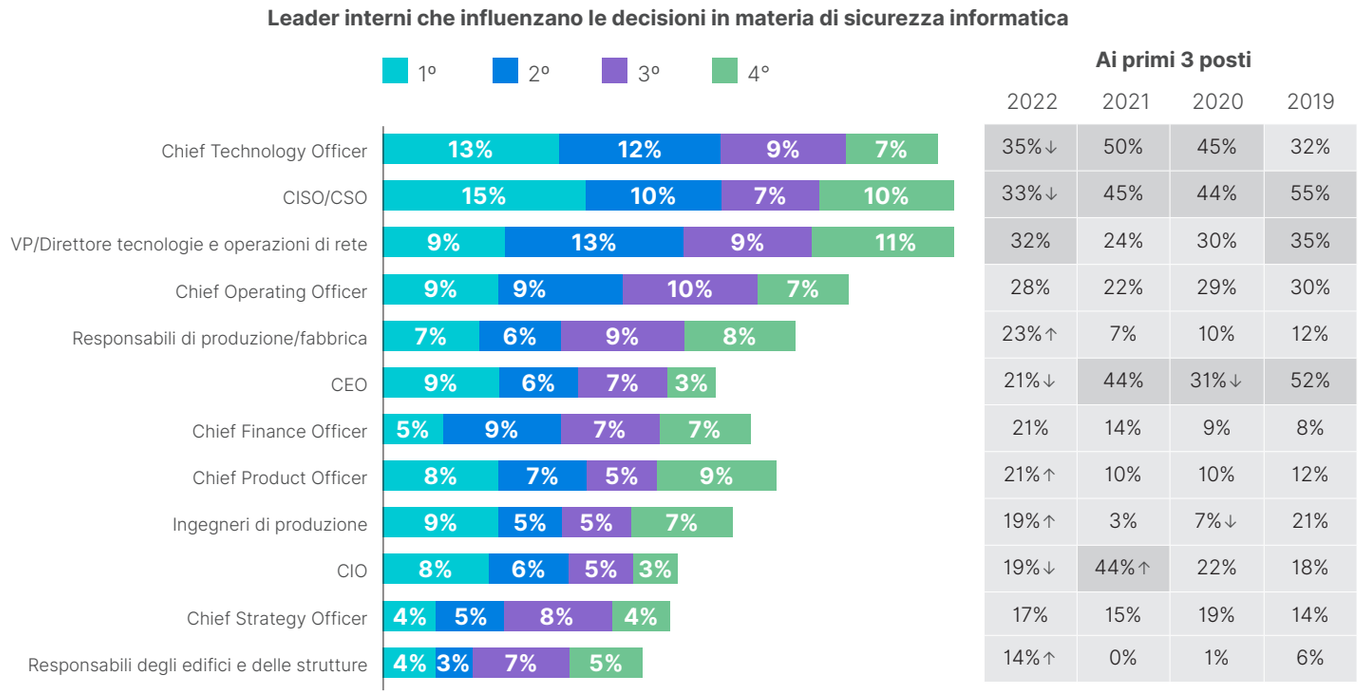
"Le recenti operazioni informatiche sponsorizzate dallo Stato russo hanno incluso attacchi DDoS (Distributed Denial-of-Service), mentre le operazioni precedenti hanno incluso la distribuzione di malware distruttivo contro il governo ucraino e le organizzazioni di infrastrutture critiche".[8]

Considerazioni sulla sicurezza OT

I risultati dell'indagine rivelano che le organizzazioni sono sempre più preoccupate per la sicurezza della loro infrastruttura OT, ma che la loro preparazione a tali minacce è ancora frammentaria e incompleta. Dalla ricerca di quest'anno abbiamo individuato cinque punti chiave:

Insight 1: la sicurezza OT è una preoccupazione a livello aziendale e diversi gruppi si assumono la responsabilità

Non sorprende che la sicurezza dei sistemi OT sia al centro dell'attenzione dei dirigenti di molte organizzazioni, con CTO e CISO/CSO più comunemente citati tra i primi tre leader che influenzano le decisioni in materia di sicurezza informatica. Tuttavia, le risposte all'indagine indicano che questi leader hanno perso influenza nell'ultimo anno (Figura 5). L'anno scorso, il 50% delle organizzazioni ha inserito il CTO tra le prime tre figure che influenzano la sicurezza e il 45% ha fatto lo stesso per il CISO/CSO. Questi numeri sono scesi rispettivamente al 35% e al 33% nel 2022. La natura globale dell'indagine non è stata un fattore di cambiamento, poiché i numeri erano identici per gli intervistati nordamericani e per la coorte complessiva.



	Ai primi 3 posti			
	2022	2021	2020	2019
Chief Technology Officer	35%↓	50%	45%	32%
CISO/CSO	33%↓	45%	44%	55%
VP/Direttore tecnologie e operazioni di rete	32%	24%	30%	35%
Chief Operating Officer	28%	22%	29%	30%
Responsabili di produzione/fabbrica	23%↑	7%	10%	12%
CEO	21%↓	44%	31%↓	52%
Chief Finance Officer	21%	14%	9%	8%
Chief Product Officer	21%↑	10%	10%	12%
Ingegneri di produzione	19%↑	3%	7%↓	21%
CIO	19%↓	44%↑	22%	18%
Chief Strategy Officer	17%	15%	19%	14%
Responsabili degli edifici e delle strutture	14%↑	0%	1%	6%

Figura 5: leader interni che influenzano le decisioni in materia di sicurezza.

Chi è a capo della sicurezza OT, e chi lo sarà?

Tuttavia, alla domanda su chi abbia la responsabilità finale della sicurezza OT nelle loro organizzazioni, una pluralità di intervistati, pari a un terzo, ha nominato il vicepresidente o il direttore dell'ingegneria o delle operazioni di rete (Figura 6). Si tratta di un forte aumento rispetto alla percentuale dello scorso anno e della più alta nei quattro anni in cui è stata condotta l'indagine. Ciò riflette il fatto che la responsabilità della sicurezza OT potrebbe essersi spostata un po' più in alto nell'organigramma rispetto agli anni passati, quando una persona di livello dirigenziale o manageriale era responsabile della sicurezza OT in una pluralità di organizzazioni.

Gli intervistati ipotizzano che questo spostamento verso l'alto dell'organigramma sia una tendenza destinata a crescere. Solo il 15% degli intervistati afferma che oggi il CISO è responsabile della sicurezza OT, ma il 79% prevede che la funzione passerà sotto il CISO nei prossimi 12 mesi (Figura 7). Tuttavia, siamo scettici su questa affermazione, in quanto una grande maggioranza degli intervistati ha fatto questa previsione ogni anno in cui è stata condotta l'indagine, e la percentuale di organizzazioni in cui il CISO è attualmente responsabile della sicurezza OT è in realtà leggermente diminuita nel 2022 rispetto al 2021. Il calo dell'influenza del CISO sulle decisioni in materia di sicurezza, di cui si è già parlato in precedenza, aggiunge peso a questo scetticismo.

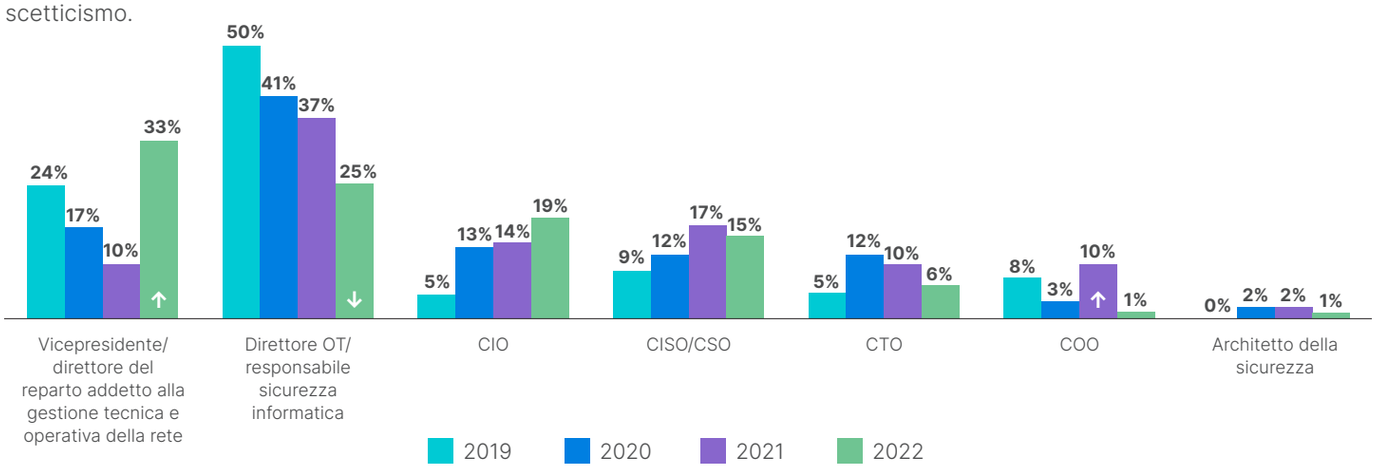


Figura 6: leader attualmente responsabile della sicurezza informatica OT.

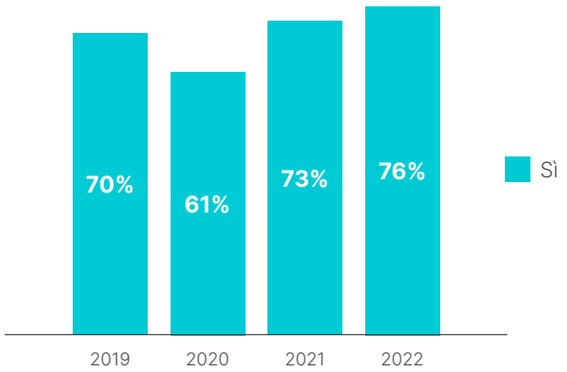


Figura 7: intervistati che prevedono che la sicurezza OT sarà affidata al CISO nei prossimi 12 mesi.

Percorsi lavorativi nella sicurezza OT

Per partecipare all'indagine, gli intervistati dovevano avere una responsabilità significativa in materia di OT. In effetti, l'85% di loro passa più della metà del proprio tempo a gestire questa funzione, che per il 28% richiede più di tre quarti delle ore di lavoro (Figura 8). Due terzi degli intervistati a livello globale svolgono un ruolo nel settore OT, presso organizzazioni industriali o fornitori di soluzioni OT (Figura 9). Il restante terzo proviene da un background di sicurezza informatica, tra cui più della metà degli intervistati dell'America Latina.

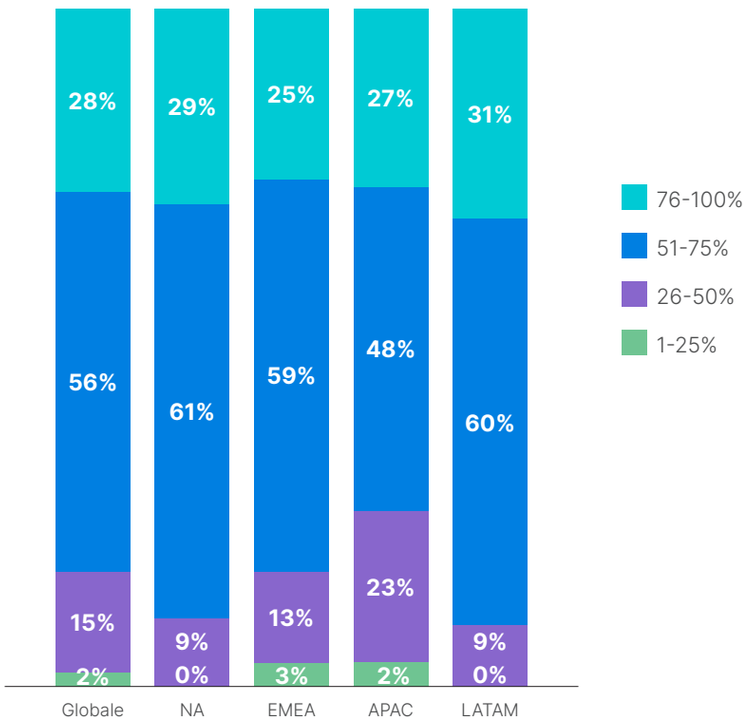


Figura 8: percentuale di tempo dedicato al supporto/gestione della sicurezza OT.

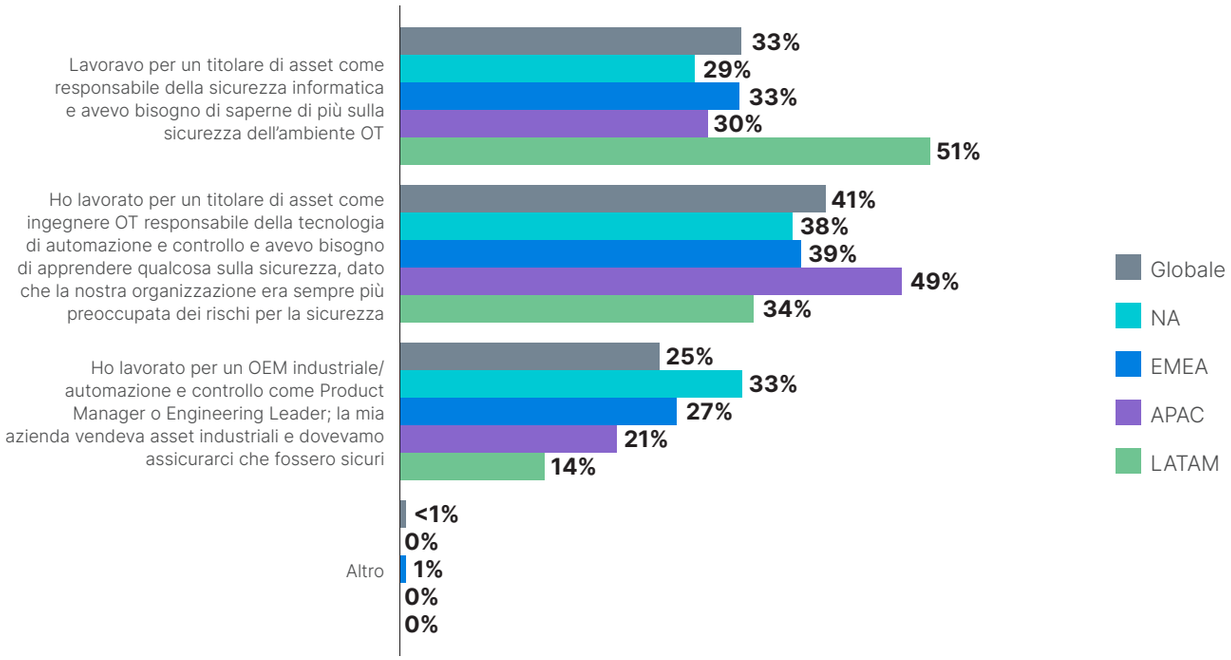
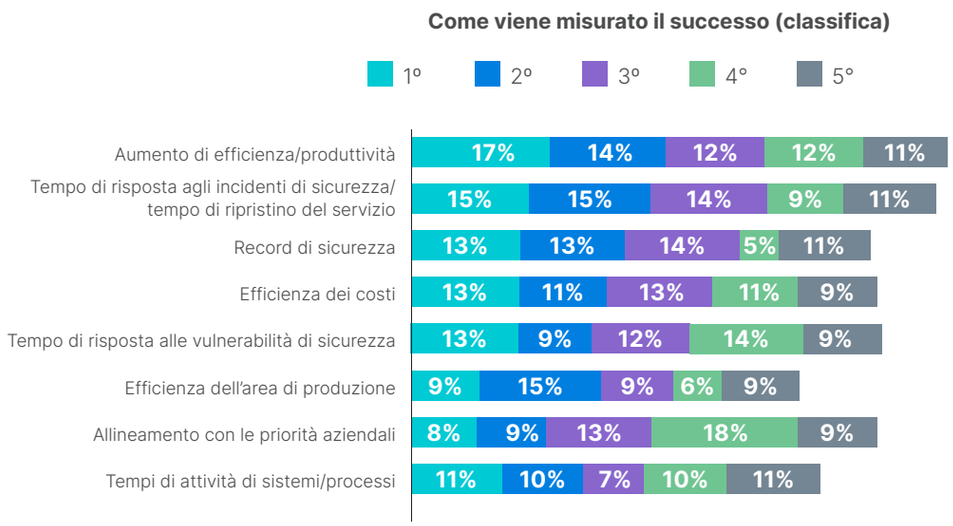


Figura 9: ruolo lavorativo che ha portato alla sicurezza OT.

Insight 2: alcune organizzazioni tendono ancora a privilegiare l'efficienza rispetto alla sicurezza OT

Sebbene ogni organizzazione dichiari di essere preoccupata per la sicurezza OT, un modo per discernere l'importanza della sicurezza è osservare come vengono misurati i leader OT. Nell'indagine di quest'anno, i guadagni di efficienza e produttività sono ancora i più comunemente citati come principale misura di successo, e sono tra le prime tre metriche nel 43% delle organizzazioni (Figura 10). Questa misura è stata la più citata tra le prime tre misure di successo in tutti gli anni in cui è stata condotta l'indagine, ma la sua prevalenza è diminuita del 14% dal 2021 al 2022.

Il CISO è la principale figura che influenza le decisioni in materia di sicurezza OT solo nel 33% delle organizzazioni, in calo rispetto al 45% del 2021.



	Ai primi 3 posti			
	2022	2021	2020	2019
Aumento di efficienza/produttività	43↓	57%	46%	55%
Tempo di risposta agli incidenti di sicurezza/ tempo di ripristino del servizio	43%	N/A	N/A	N/A
Record di sicurezza	40%	34%	44%	41%
Efficienza dei costi	37%	41%	40%	53%
Tempo di risposta alle vulnerabilità di sicurezza	34%↓	47%↑	32%	44%
Efficienza dell'area di produzione	32%	42%	41%↓	42%
Allineamento con le priorità aziendali	29%	33%	24%	29%
Tempi di attività di sistemi/processi	29%↓	41%	40%	35%

Figura 10: classifica delle metriche di successo.

Allo stesso tempo, il 43% degli intervistati ha citato una metrica di sicurezza (il tempo di risposta agli incidenti o di ripristino del servizio) tra le prime tre misure, il che è certamente un buon segno. Anche i tempi di risposta alle vulnerabilità di sicurezza e i tempi di attività di sistemi/processi sono diminuiti in modo significativo, ma il fatto che la metrica di risposta agli incidenti sia nuova per l'indagine del 2022 può essere una delle ragioni per cui le altre scelte relative alla sicurezza sono in calo.

Preoccupazione specifica per il ransomware

Il ransomware ha dominato i titoli dei media nello spazio della sicurezza informatica per diversi anni e le organizzazioni riferiscono di essere molto preoccupate per questa tattica, nonostante sia meno comune di altri tipi di attacchi. Più di due terzi degli intervistati a livello globale (e tre quarti in Nord America) dichiarano di essere più preoccupati del ransomware rispetto ad altre intrusioni (Figura 11). Il ransomware ha causato danni e costi economici significativi nel corso degli anni, e un buon risultato della sua elevata visibilità è che le organizzazioni sono debitamente preoccupate. Tuttavia, altri tipi di attacchi dannosi potrebbero non ricevere l'attenzione che meritano a causa della loro minore visibilità.

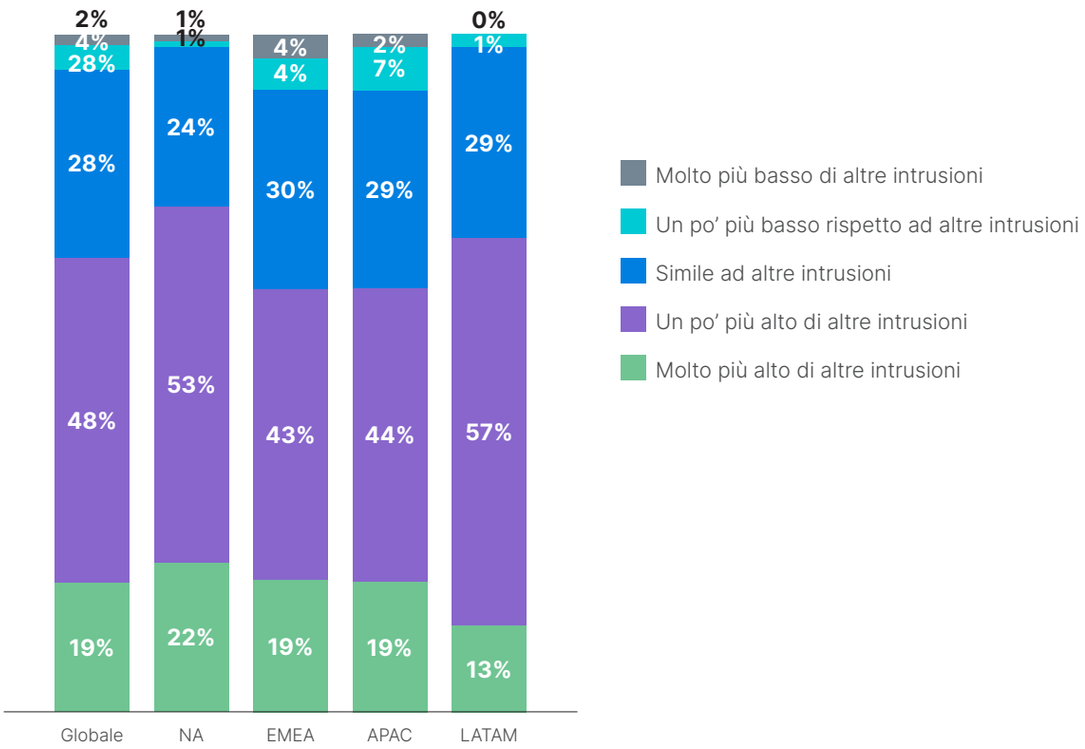


Figura 11: livello di preoccupazione per il ransomware.

Classificazione dell'importanza degli strumenti di sicurezza informatica

Gli intervistati non hanno saputo indicare le caratteristiche delle soluzioni di sicurezza informatica più importanti per le loro organizzazioni. Gli strumenti di analisi, monitoraggio e valutazione della sicurezza sono stati citati come i più importanti, ma solo da una pluralità del 17% (Figura 12). In generale, le soluzioni di gestione e monitoraggio della conformità sono state le più citate tra le prime tre, mentre le funzionalità di protezione dei protocolli specifici dell'OT si sono classificate al secondo posto.

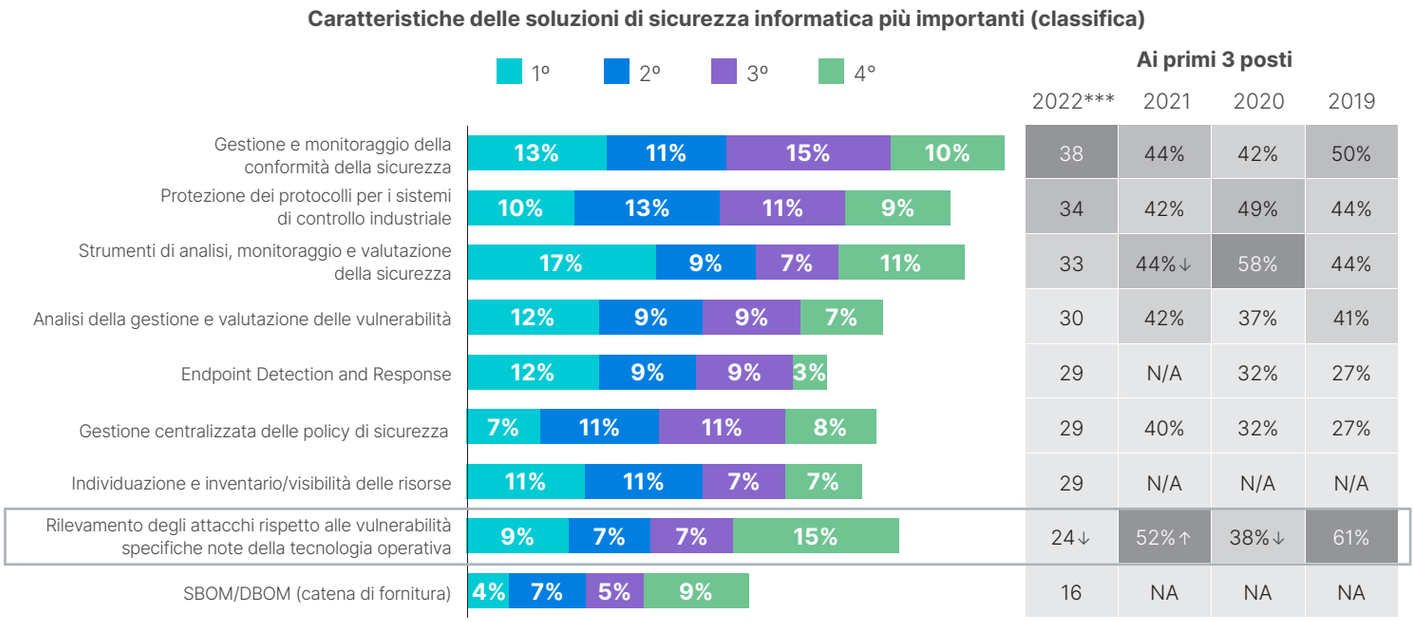


Figura 12: classificazione delle più importanti funzionalità delle soluzioni di sicurezza.

Insight 3: le organizzazioni segnalano un graduale miglioramento della sicurezza OT, ma sono necessari ulteriori miglioramenti

Come negli anni passati, nella nostra indagine abbiamo chiesto agli intervistati di autodichiarare il livello di maturità della sicurezza OT raggiunto dalle loro organizzazioni, con una breve descrizione per ciascuno dei cinque livelli di maturità. Tra tutti gli intervistati, l'84% ha raggiunto almeno il livello 2, avendo stabilito l'accesso e la profilazione (Figura 13). La metà degli intervistati ha raggiunto almeno il livello 3 stabilendo un comportamento predittivo e il 21% ha raggiunto il livello 4 con l'orchestrazione e l'automazione.

Questo dato rappresenta un miglioramento marginale rispetto al 2021, soprattutto grazie al passaggio delle organizzazioni dal livello 2 al livello 3. La percentuale di organizzazioni che raggiungono almeno il livello 3 è aumentata dal 44% al 50% rispetto all'anno precedente.

Il tempo di risposta agli incidenti di sicurezza/ripristino del servizio è una delle prime tre metriche di successo OT per il 43% delle organizzazioni.

Analizzando i risultati per area geografica, una percentuale maggiore di intervistati di America Latina e APAC ha raggiunto il livello 4. In Nord America, invece, un numero maggiore di organizzazioni ha superato il livello 1, ma un numero minore ha raggiunto il livello 4, lasciando più del 70% delle organizzazioni nei livelli intermedi.

Purtroppo, solo la metà degli intervistati afferma che l'approccio alla sicurezza OT della propria organizzazione è un fattore significativo nel punteggio di rischio complessivo (Figura 14), sebbene quasi tutte le altre organizzazioni lo includano come fattore moderato.

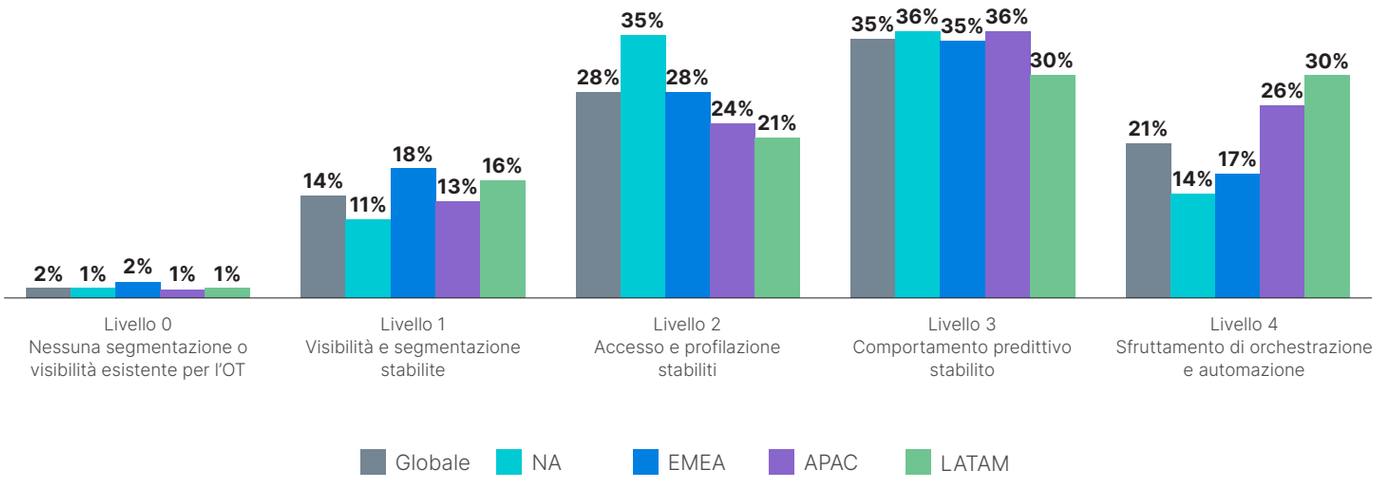


Figura 13: livello di maturità dell'approccio alla sicurezza informatica OT.

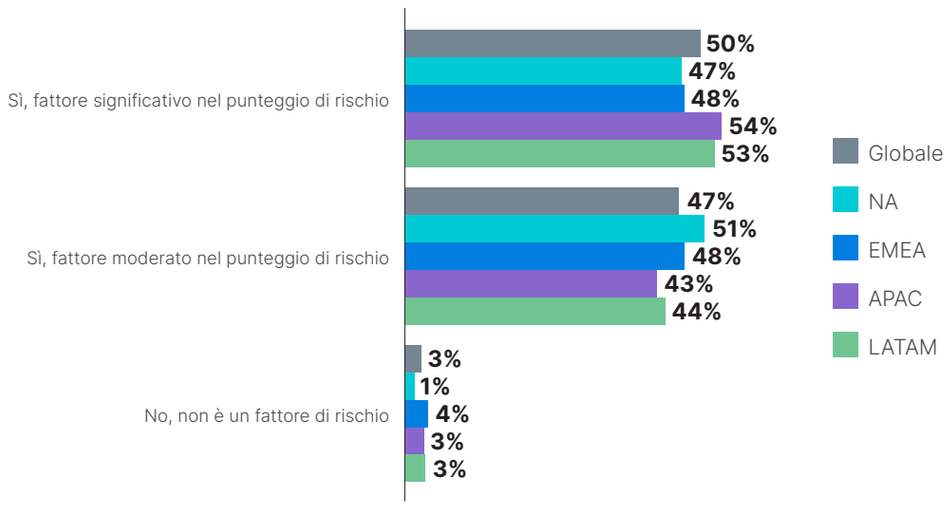


Figura 14: importanza della strategia di sicurezza OT nel punteggio di rischio complessivo.

Maturità complessiva della sicurezza informatica

Agli intervistati è stato anche chiesto di valutare la maturità del loro programma complessivo di sicurezza informatica, che comprende IT e OT. In questo caso, è più probabile che gli intervistati abbiano raggiunto il livello 3 (59%), ma meno probabile che abbiano raggiunto il livello 4 (16%, Figura 15). Anche in questo caso, le aziende di America Latina e APAC mostrano una maturità più elevata, mentre quelle del Nord America occupano complessivamente una posizione più bassa in questo senso. Le organizzazioni più grandi e quelle del settore manifatturiero hanno maggiori probabilità di avere livelli di maturità più elevati, così come le organizzazioni in cui i top leader della tecnologia e della sicurezza hanno influenza sulle decisioni in fatto di sicurezza informatica (Figura 16).

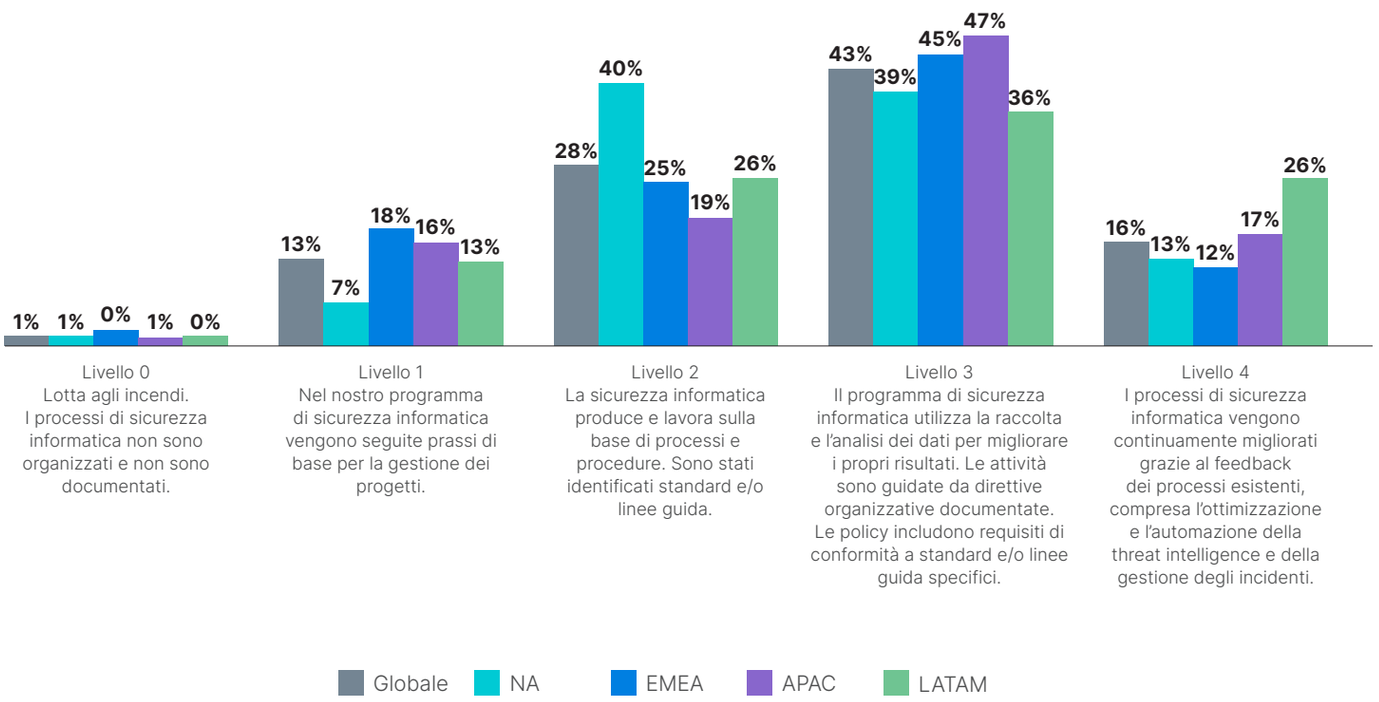
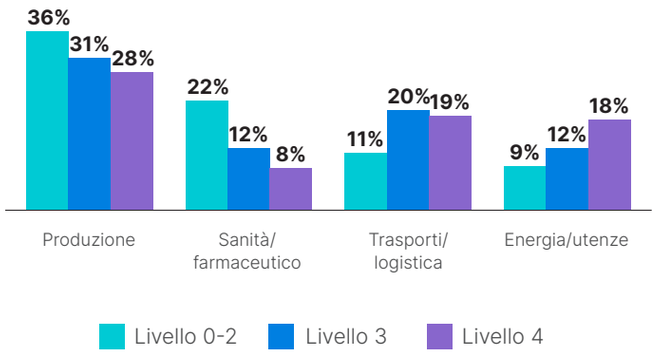
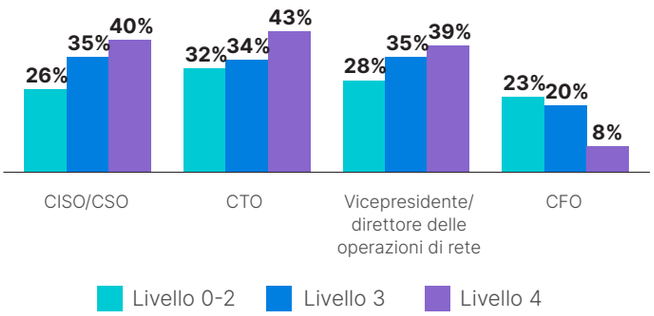


Figura 15: livello di maturità del programma complessivo di sicurezza informatica.





% superiore a 5.000 dipendenti		
21%	28%	41%

% con cui la sicurezza informatica aiuta/impedisce il mio successo		
65%/4%	82%/6%	83%/11%
% con cui aiuta agevolando gli standard di sicurezza		
40%	46%	58%

Figura 16: dati demografici selezionati degli intervistati per livello di maturità del programma di sicurezza informatica.

Visibilità centralizzata

La definizione della visibilità dei processi OT è inclusa nel livello 1 della nostra matrice di maturità della sicurezza OT, ma la granularità di tale visibilità può fare la differenza. Mentre il 98% degli intervistati dichiara di aver raggiunto almeno il livello 1 di maturità della sicurezza OT, solo il 74% afferma che più di tre quarti delle attività OT sono visibili dal team operativo di sicurezza (Figura 17). Questa percentuale è del 77% in Nord America, un miglioramento rispetto ai risultati dell'indagine nordamericana degli anni passati (Figura 18). Tuttavia, la percentuale di intervistati nordamericani che hanno una visibilità del 100% sembra essere in calo: dal 23% nel 2020 al 13% nel 2022.

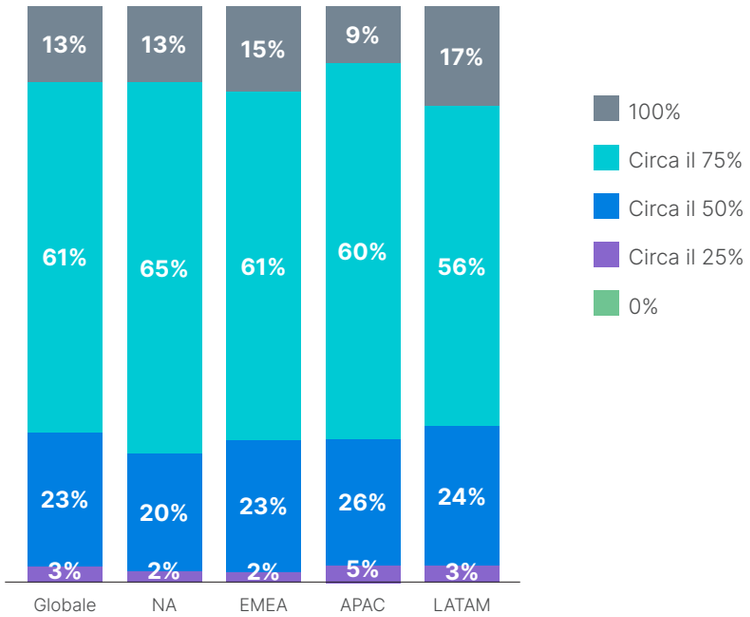


Figura 17: visibilità delle attività OT da parte delle operazioni di sicurezza.

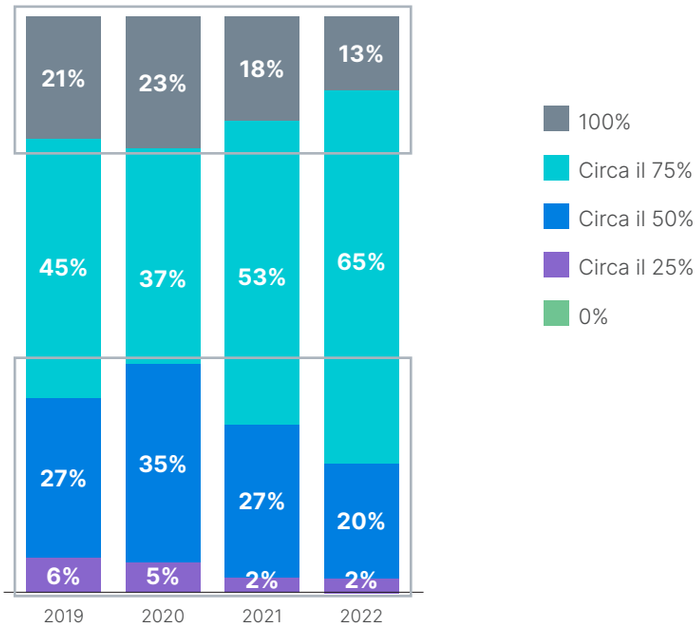


Figura 18: visibilità delle attività OT da parte delle operazioni di sicurezza, Nord America.

Insight 4: le organizzazioni hanno modi diversi di affrontare la sicurezza OT e molte presentano lacune nella sicurezza

Poiché negli anni passati i sistemi OT erano spesso isolati da Internet, la necessità di proteggerli dalle minacce informatiche è relativamente nuova e la nostra indagine ha rilevato che le prassi di sicurezza non sono ancora state standardizzate.

Come è stato già detto, un approccio consiste nell'affidare la gestione della sicurezza OT al SOC, che da anni svolge questo ruolo per i sistemi IT. Quasi tutti gli intervistati hanno adottato questo approccio per almeno alcune attività OT, ma solo il 52% delle organizzazioni è riuscito ad attivare il monitoraggio e la tracciabilità di *tutte* le attività OT da parte del team SOC (Figura 19). Questo dato è rimasto sostanzialmente invariato nei quattro anni in cui abbiamo condotto questa indagine. Le aziende dell'area APAC registrano risultati leggermente migliori in questo senso, con il 59% che monitora tutte le attività del SOC.

Il 50% delle organizzazioni ha raggiunto il livello 3 di maturità della sicurezza OT, rispetto al 44% del 2021.

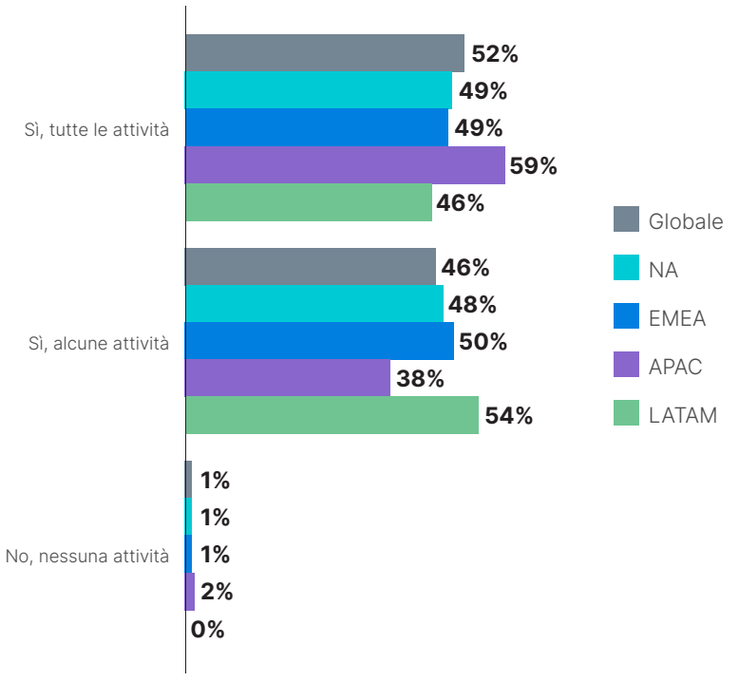


Figura 19: attività OT monitorate e tracciate dal SOC.

Metriche monitorate e segnalate

Per quanto riguarda il monitoraggio e la segnalazione delle metriche di sicurezza, i risultati sono contrastanti. Quando è stato presentato un elenco di misure di base per la sicurezza informatica che dovrebbero essere monitorate in ogni organizzazione, non più del 52% degli intervistati ha dichiarato di monitorarne qualcuna (Figura 20).

Confrontando i risultati nordamericani con gli anni passati, la percentuale che monitora e segnala diverse metriche è diminuita significativamente rispetto al 2021 (Figura 21), comprese le vulnerabilità individuate e bloccate e le intrusioni rilevate e risolte.

Percentuali simili di intervistati riferiscono regolarmente alla direzione esecutiva informazioni di base sulla sicurezza OT. Di fronte a un elenco che comprende informazioni critiche come i rapporti di conformità, le valutazioni di sicurezza e le compromissioni della sicurezza, non più del 53% ha riferito un singolo elemento alla direzione esecutiva (Figura 22).

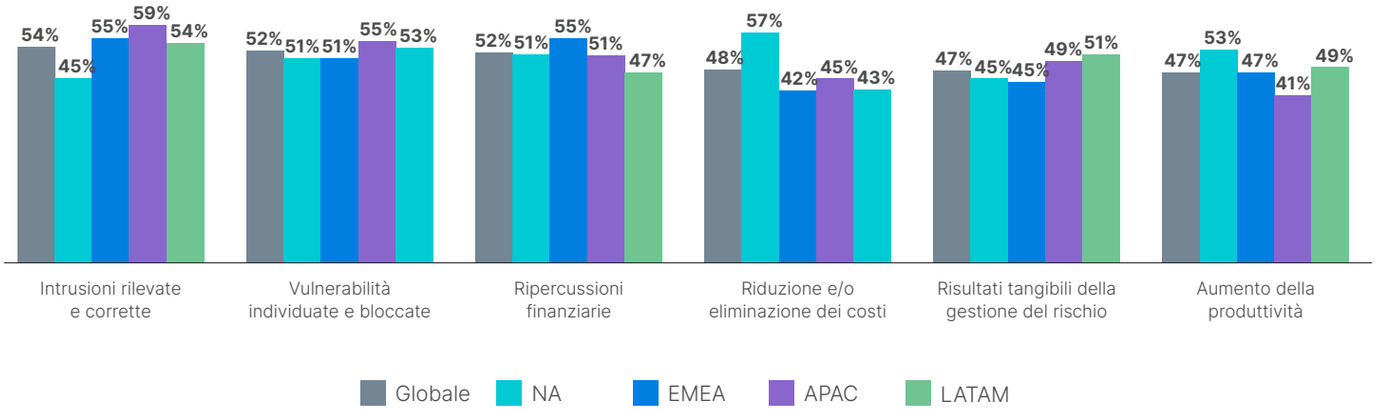


Figura 20: parametri di sicurezza informatica monitorati e documentati.

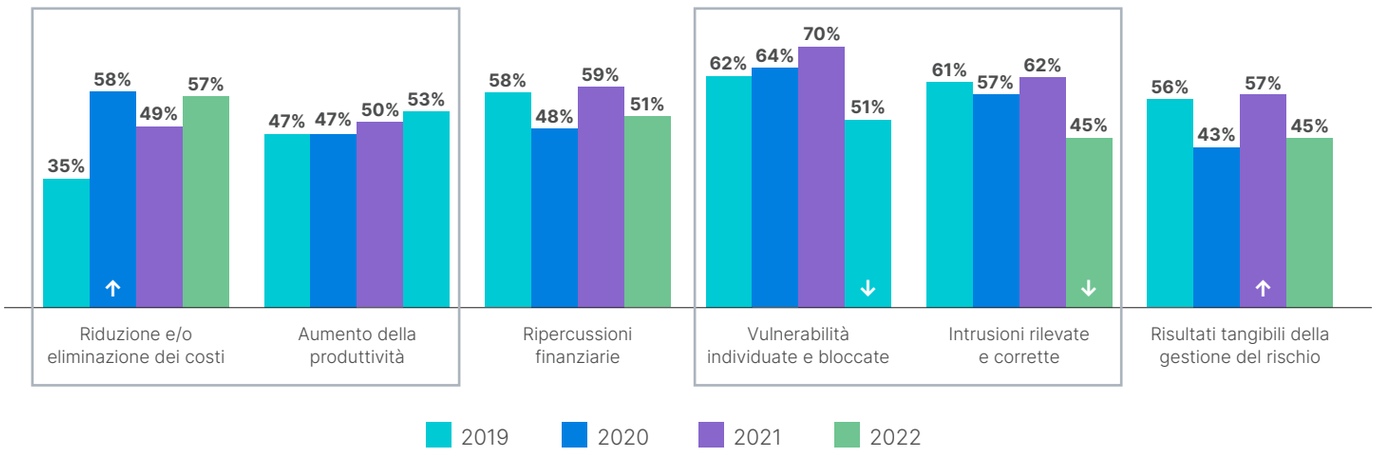


Figura 21: parametri di sicurezza informatica monitorati e documentati, Nord America.

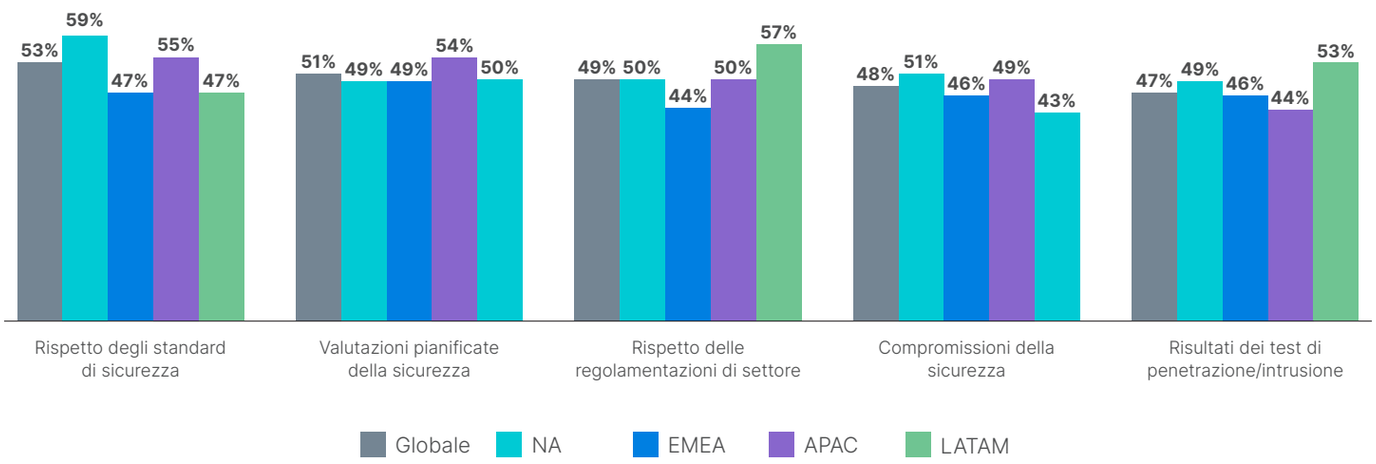


Figura 22: problemi di sicurezza informatica OT segnalati alla direzione esecutiva.

Funzionalità di sicurezza utilizzate

Gli intervistati hanno fornito risposte diverse in merito agli strumenti e alle funzioni di sicurezza che utilizzano per proteggere i loro sistemi OT. A fronte di un elenco piuttosto completo di strumenti e processi, nessuna singola funzionalità è utilizzata da più del 47% degli intervistati (Figura 23). Le soluzioni incluse per la prima volta quest'anno comprendono l'accesso remoto sicuro (41%), l'orchestrazione, l'automazione e la risposta alla sicurezza (SOAR, Security Orchestration, Automation, and Response; 37%) e l'uso di threat intelligence (36%).

Questo approccio basato su "un po' di tutto" riflette un aspetto della sicurezza che per molti versi è ancora agli inizi, con diverse organizzazioni che provano approcci diversi. Una prassi che sta chiaramente perdendo di popolarità è l'uso del centro operativo di rete (NOC, Network Operations Center) per la gestione della sicurezza OT (Figura 24). È interessante notare che gli intervistati nordamericani tendono a utilizzare un numero inferiore delle prassi e funzionalità elencate.

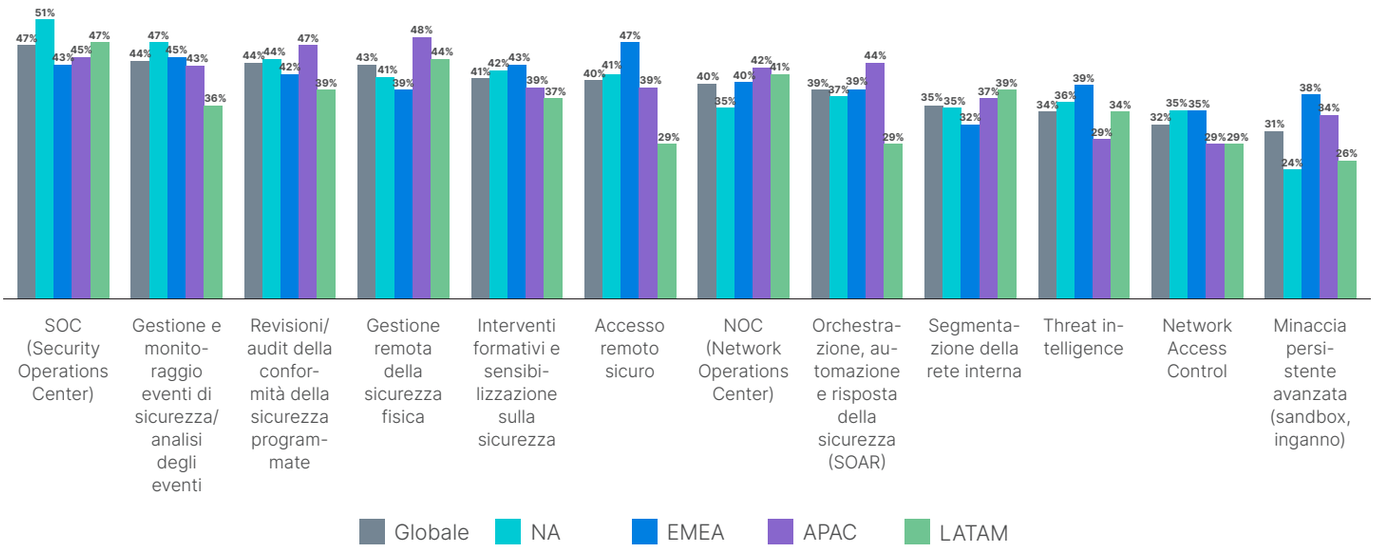


Figura 23: sicurezza informatica e funzionalità di sicurezza in atto.

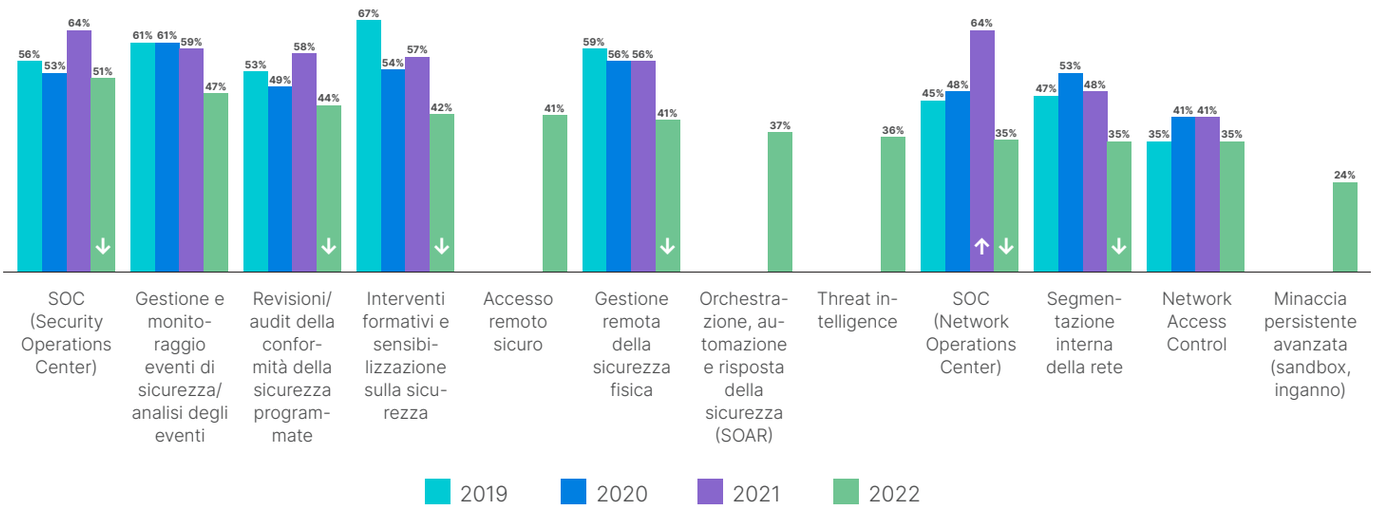


Figura 24: sicurezza informatica e funzionalità di sicurezza in atto, Nord America.

Non più del 47% delle organizzazioni utilizza un singolo strumento o approccio di sicurezza OT.

Complessità dei sistemi di sicurezza e percezione della loro efficacia

La complessità è un problema che può ostacolare la sicurezza OT. La stragrande maggioranza delle organizzazioni utilizza da due a otto fornitori diversi per i propri dispositivi OT e ha tra i 100 e i 10.000 dispositivi in funzione (Figura 25). Solo il 7% delle organizzazioni è riuscito a ridurre il numero di fornitori a uno.

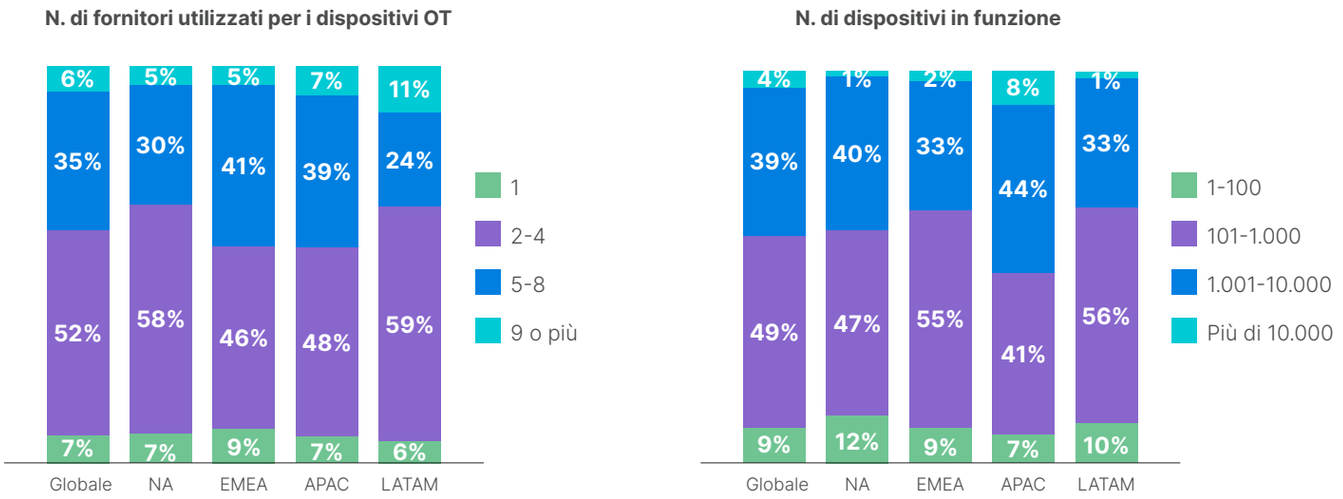


Figura 25: fornitori OT e dispositivi OT utilizzati.

Insight 5: la maggior parte delle organizzazioni subisce ancora più intrusioni all'anno

Ogni anno poniamo agli intervistati una semplice domanda sui loro risultati in termini di sicurezza: quante intrusioni hanno subito negli ultimi 12 mesi? Nel 2022, tre quarti degli intervistati hanno ammesso di aver subito almeno tre intrusioni, il 19% più di sei e il 7% più di dieci (Figura 26). Solo il 6% degli intervistati ha dichiarato di non aver subito intrusioni negli ultimi 12 mesi.

Osservando i risultati nordamericani di questa domanda nell'arco di quattro anni, le cose non stanno migliorando nel complesso, con circa la stessa percentuale che ha subito tre o più intrusioni dal 2020 (Figura 27). Una piccola consolazione è che la percentuale di intervistati nordamericani che hanno subito 10 o più intrusioni è diminuita dal 12% al 5% rispetto all'anno precedente.

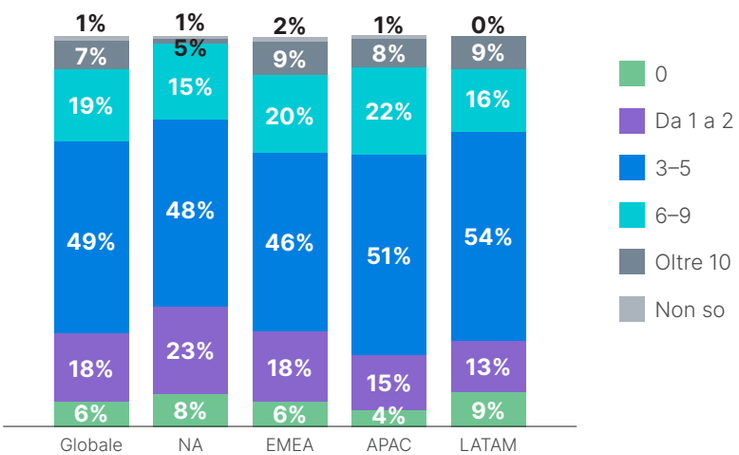


Figura 26: numero di intrusioni nell'ultimo anno.

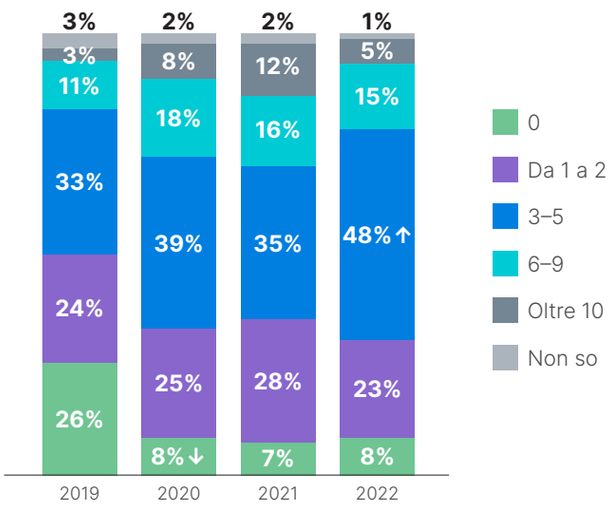


Figura 27: numero di intrusioni nell'ultimo anno, Nord America.

Tipi di attacchi

Gli intervistati hanno subito un'ampia gamma di tipi di attacchi, il che non sorprende visto il numero di intrusioni. In totale, otto tipi di attacchi hanno colpito almeno un quarto degli intervistati, con malware e phishing in cima alla lista, colpendo più del 40% delle organizzazioni (Figura 28). Il ransomware ha colpito meno di un terzo delle organizzazioni in generale, ma con una percentuale del 44% nel caso delle aziende latinoamericane. Inoltre, il numero di intervistati latinoamericani che hanno subito attacchi di phishing è inferiore a quello delle altre aree geografiche. Se si considerano i risultati nordamericani nell'arco di quattro anni, quest'anno le violazioni da malware e da insider malintenzionati sono diminuite (Figura 29).

Il numero complessivo di intrusioni è notevolmente simile indipendentemente dal livello di maturità della sicurezza dichiarato, probabilmente perché le organizzazioni più mature sono in grado di rilevare una percentuale maggiore di intrusioni che si verificano. Ma se si considera il dato in base al tipo di attacco, risulta chiaro che le organizzazioni più mature hanno meno problemi con le minacce interne, mentre rilevano più attacchi dall'esterno (Figura 30).

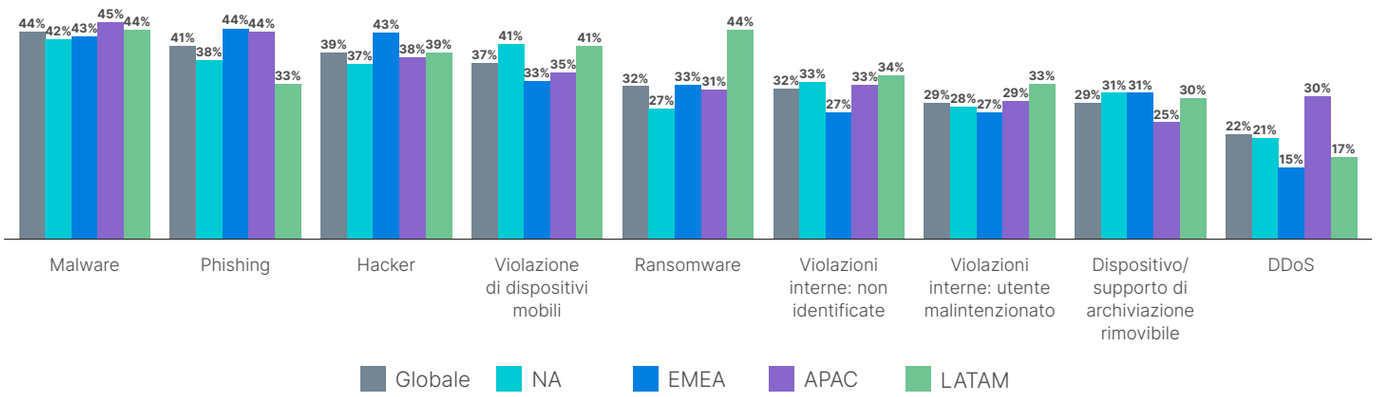


Figura 28: tipi di intrusioni subite.

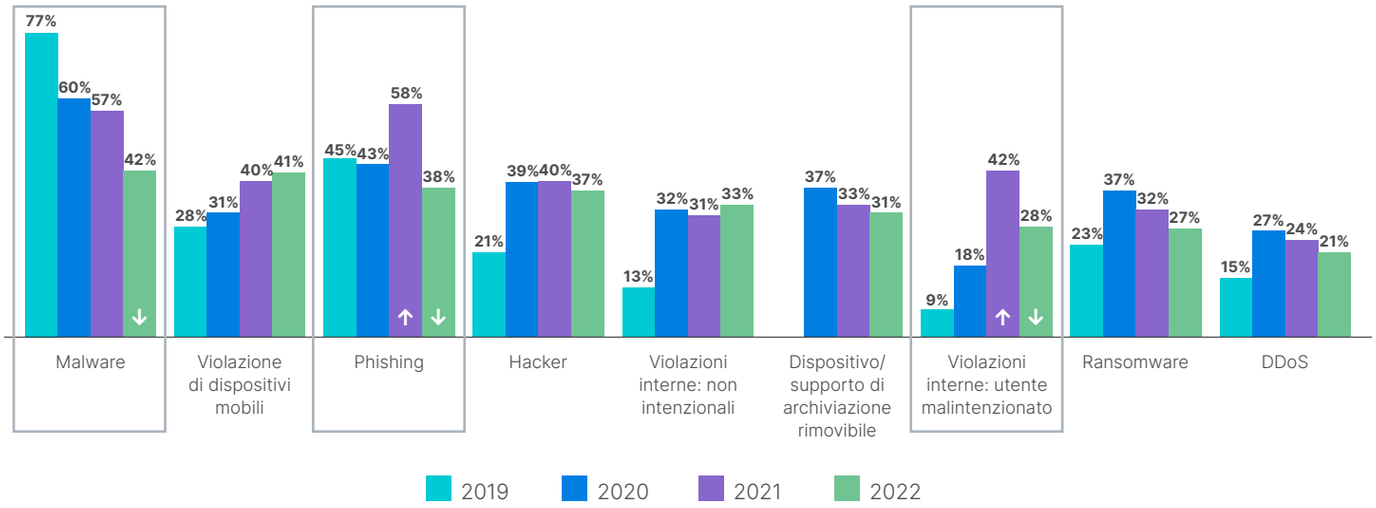


Figura 29: tipi di intrusioni subite, Nord America.

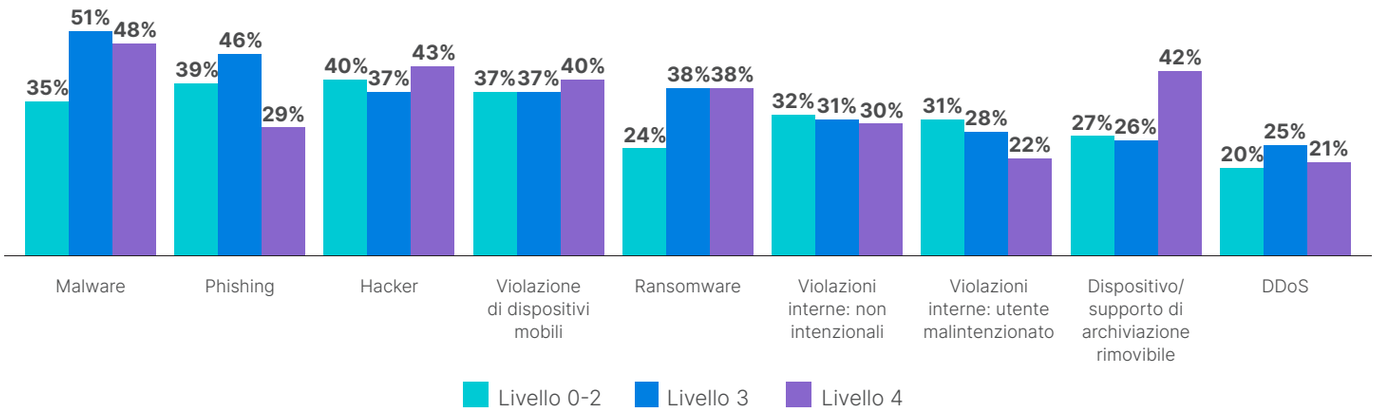


Figura 30: tipi di intrusioni subite per livello di maturità della sicurezza dichiarato.

Impatto degli attacchi

È interessante notare che una percentuale leggermente superiore di attacchi ha colpito i sistemi OT rispetto a quelli IT (Figura 31), con il 61% delle intrusioni che hanno avuto un impatto sui sistemi OT e il 60% su quelli IT. L'impatto commercial delle intrusioni non è stato affatto banale. Quasi la metà degli intervistati ha subito un'interruzione operativa che ha influito sulla produttività, mentre più di un terzo ha subito ripercussioni sui ricavi, sulla perdita di dati, sulla conformità e sul valore del marchio, e persino minacce alla sicurezza fisica (Figura 32). Il 90% degli intervistati ammette che il ripristino del servizio è stato un processo che ha richiesto diverse ore o più (Figura 33).

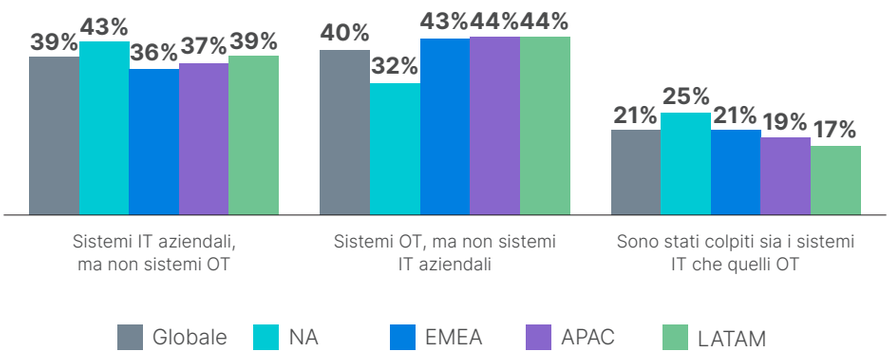


Figura 31: ambienti colpiti da intrusioni.

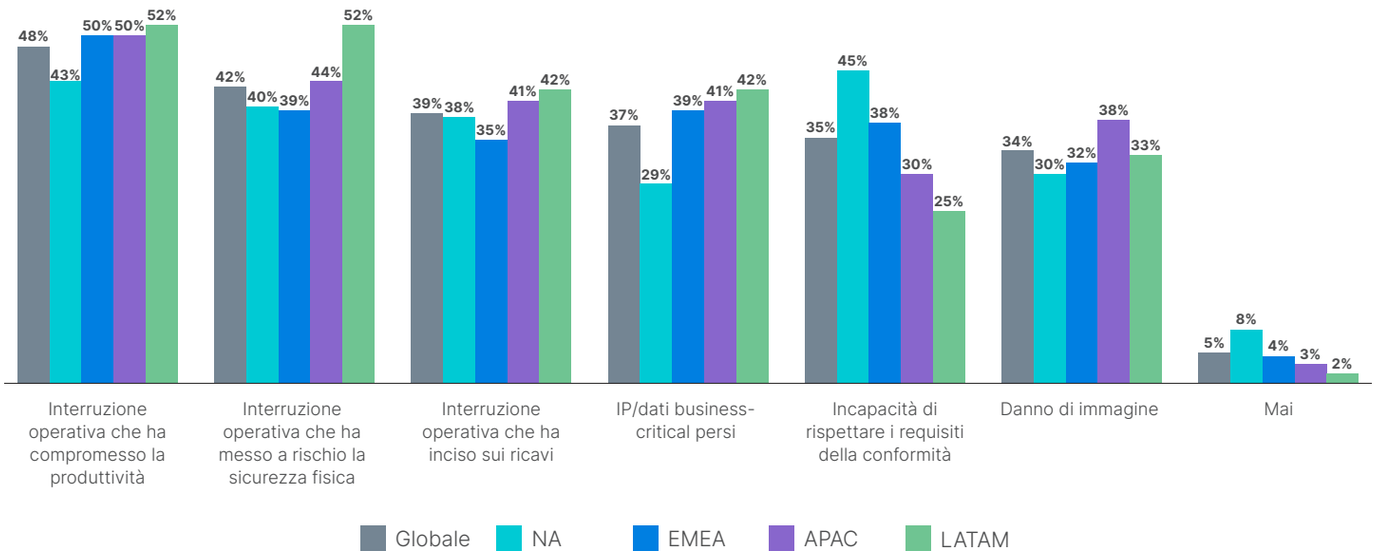


Figura 32: impatti organizzativi delle intrusioni.

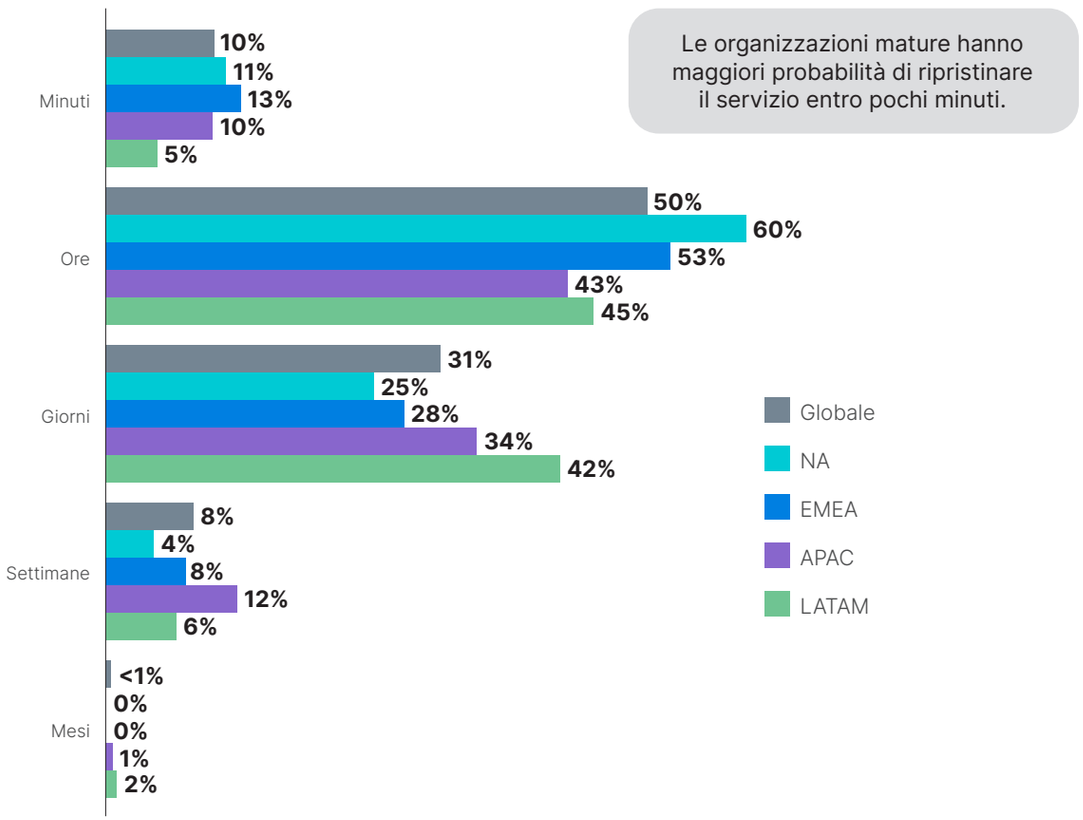


Figura 33: il più lungo ripristino del servizio dopo un'intrusione.

Best practice delle organizzazioni top-tier

Solo il 6% delle organizzazioni rappresentate nell'indagine di quest'anno dichiara di non aver subito intrusioni negli ultimi 12 mesi, mentre il 5% ha segnalato *più di 10 intrusioni.* Abbiamo confrontato le prassi.

Solo il 6% degli intervistati ha dichiarato di aver subito zero intrusioni nell'ultimo anno.

1. Le organizzazioni top-tier hanno il 17% di probabilità in più di avere tutte le attività OT visibili a livello centrale alle operazioni di sicurezza informatica.

La visibilità centralizzata ed end-to-end di tutte le attività OT è fondamentale per garantirne la sicurezza, e nella maggior parte delle organizzazioni si tratta sicuramente di un work in progress. Le organizzazioni top-tier hanno una probabilità più che tripla di aver raggiunto tale visibilità rispetto alle loro controparti di basso livello.

2. Le organizzazioni top-tier hanno il 177% di probabilità in più di avere il tempo di risposta alle vulnerabilità di sicurezza come una delle tre principali metriche di successo.

Come si suol dire, "ciò che viene misurato viene migliorato", rispondere rapidamente alle vulnerabilità della sicurezza OT è fondamentale per proteggere questi sistemi. Le organizzazioni che hanno ottenuto i risultati migliori hanno quasi il triplo delle probabilità di avere questa misurazione come parte importante della loro valutazione delle prestazioni.

3. Le organizzazioni top-tier hanno il 37% di probabilità in più di disporre di una tecnologia di controllo degli accessi alla rete.

Garantire che solo le persone autorizzate possano accedere a sistemi specifici è fondamentale per proteggere qualsiasi asset tecnologico. Quando si tratta di OT, le persone che devono accedere a tali sistemi hanno una gamma relativamente ristretta di ruoli lavorativi. Le organizzazioni che l'anno scorso hanno evitato le intrusioni hanno maggiori probabilità di disporre di tali controlli.

4. Le organizzazioni top-tier hanno il 48% di probabilità in più di segnalare le compromissioni della sicurezza agli alti dirigenti.

Le questioni che vengono incluse nelle relazioni periodiche ai dirigenti tendono a rimanere in primo piano per tutto l'anno. Le organizzazioni che tengono informati gli alti dirigenti delle compromissioni della sicurezza tendono ad averne di meno. Le organizzazioni top-tier tendono a essere più trasparenti nei confronti della direzione esecutiva.

5. Le organizzazioni top-tier hanno il 32% di probabilità in più di avere un SOC che monitora e tiene traccia della sicurezza OT.

I centri operativi di sicurezza (SOC) esistono da decenni e hanno sviluppato best practice dettagliate per la gestione della sicurezza IT. I leader OT che hanno evitato le intrusioni hanno maggiori probabilità di affidare la sicurezza OT allo stesso gruppo.

6. Le organizzazioni top-tier hanno il 44% di probabilità in più che monitorino e documentino le intrusioni rilevate e risolte.

La comprensione degli attacchi passati affina le capacità di un'organizzazione di sventare quelli futuri. Le organizzazioni che hanno evitato le intrusioni sono più propense a segnalarle di routine quando si verificano.

7. Le organizzazioni top-tier sono infinitamente più propense a utilizzare un solo fornitore per i loro dispositivi OT predisposti per il protocollo IP.

Evitare la complessità della rete e dei sistemi è un buon modo per ridurre la superficie di attacco e migliorare la sicurezza. Nessuna delle organizzazioni che hanno subito 10 o più intrusioni utilizzava un solo fornitore per i propri dispositivi OT predisposti per il protocollo IP, mentre quasi un terzo delle organizzazioni top-tier aveva raggiunto questo obiettivo.

Conclusioni

Il Rapporto 2022 sullo stato della tecnologia operativa e sulla sicurezza informatica rileva che gli sforzi per la sicurezza OT delle organizzazioni di tutto il mondo stanno facendo progressi inadeguati verso la protezione completa dei sistemi ICS e SCADA nel mondo relativamente nuovo dell'OT connesso. I progressi incrementali compiuti in termini di maturità della sicurezza dall'anno scorso hanno fatto poco per spostare l'ago della bilancia sui risultati effettivi della sicurezza. Il risultato è che la stragrande maggioranza delle organizzazioni continua a subire intrusioni, nella maggior parte dei casi più volte all'anno.

Dato il clima geopolitico, i governi di tutto il mondo avvertono che è probabile un aumento degli attacchi informatici alle infrastrutture critiche e alle risorse economiche chiave. Le organizzazioni industriali di un ampio spettro di settori faranno bene a far progredire rapidamente la maturità delle loro iniziative di sicurezza OT, sfruttando le tecnologie di comportamento predittivo, orchestrazione e automazione per stabilire un vero accesso zero-trust e difendersi dalle minacce provenienti da insider malintenzionati e benintenzionati, cybercriminali esterni e aggressori sponsorizzati da Stati.

Riferimenti

[1] Mayank Agrawal, et. al, "Industry 4.0: Reimagining Manufacturing Operations After COVID-19", McKinsey, 29 luglio 2020.

[2] "Global Threat Landscape Report, 1H 2021", Fortinet, agosto 2021.

[3] Clare Duffy, "Colonial Pipeline Attack: A 'Wake Up Call' about the Threat of Ransomware", CNN, 16 maggio 2021; Liam Tung, "Ransomware: Meat Firm JBS Says It Paid Out $11m After Attack", ZDnet, 10 giugno 2021.

[4] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure", CISA, 20 aprile 2022.

[5] Catherine Stupp, "Russian Cyberattacks Increase on Ukraine's Critical Infrastructure: Report", Wall Street Journal, 5 aprile 2022.

[6] Phil Muncaster, "Critical Infrastructure Firms See Cyber-Attacks Surge", InfoSecurity, 10 maggio 2022.

[7] Steven Webb, "IT/OT & OT Total Available Market Analysis", Westlands Advisory Research for Fortinet, marzo 2022.

[8] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure", CISA, 20 aprile 2022.

settembre 14, 2022 3:00 PM

1578659-0-0-IT