RAPPORTO

Rapporto 2023 sullo stato della tecnologia operativa e della sicurezza informatica

FORTINET

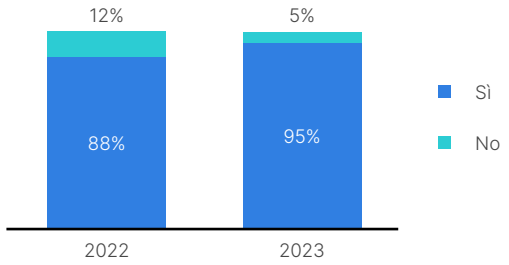
Sommario

Principali risultati

Persone

In quasi tutte le organizzazioni intervistate, i CISO sono o saranno presto responsabili della sicurezza informatica OT. Inoltre, è da notare che un numero maggiore di professionisti della sicurezza informatica OT proviene da posizioni di leadership nella sicurezza IT anziché dal team operativo.

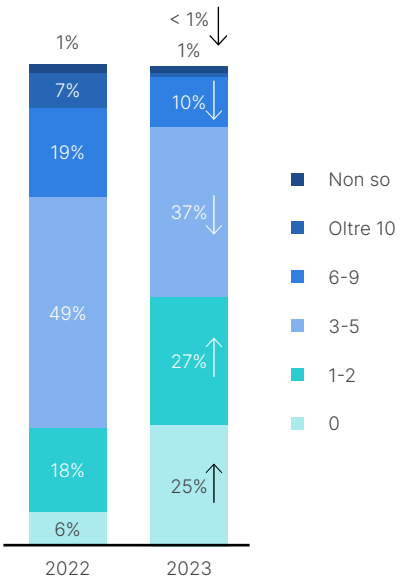
Sicurezza informatica sotto il controllo del CISO nei prossimi 12 mesi



Incidenti di sicurezza informatica

Sebbene il numero di organizzazioni che non hanno subito un'intrusione di sicurezza informatica sia aumentato notevolmente su base annua (dal 6% nel 2022 al **25% nel 2023**), c'è ancora un significativo margine di miglioramento. Infatti, tre quarti delle organizzazioni OT hanno segnalato almeno un'intrusione nell'ultimo anno e quasi un terzo degli intervistati ha dichiarato di essere stata vittima di un attacco ransomware (**32%**, un dato immutato rispetto al 2022). Le intrusioni causate da malware e phishing sono aumentate, rispettivamente, del **12%** e del **9%**.

Numero di intrusioni nell'ultimo anno

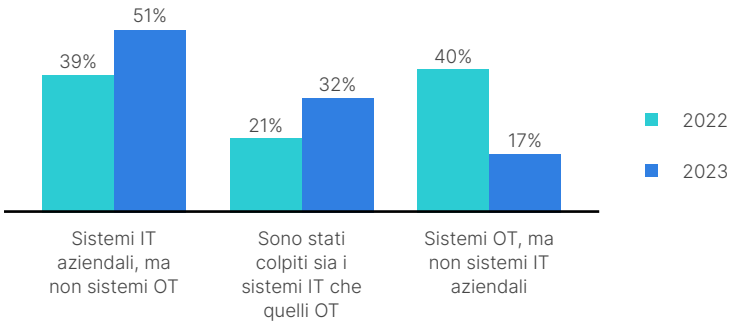


N. in base alla maturità della sicurezza informatica	Livello 0–2	Livello 3	Livello 4
Non so	1%	0%	0%
Oltre 10	1%	2%	0%
6-9	11%	11%	6%
3-5	38%	35%	40%
1-2	36%[B]	21%	25%
0	14%	31%[A]	29%[A]

L'impatto delle intrusioni

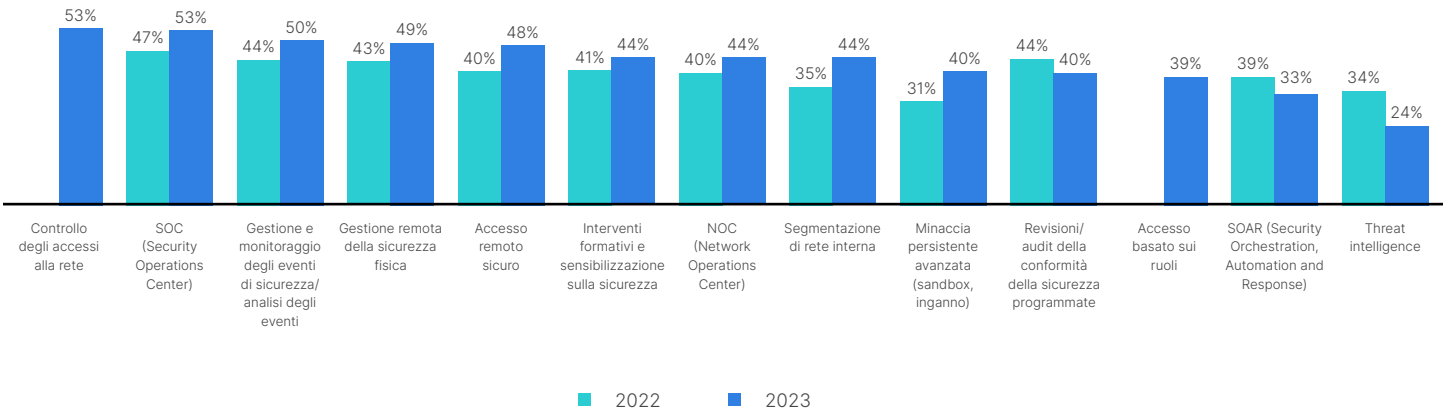
Quando si è verificato un attacco informatico all'inizio di quest'anno, quasi un terzo **(32%)** degli intervistati ha indicato che sono stati colpiti sia i sistemi IT che quelli OT, rispetto al 21% dello scorso anno. Per combattere le intrusioni, i professionisti OT stanno aumentando le soluzioni di sicurezza informatica nelle loro reti industriali.

Ambienti colpiti



Le minacce persistenti avanzate, la segmentazione della rete interna e l'accesso remoto sicuro hanno registrato il maggior incremento, mentre la threat intelligence è diminuita come soluzione.

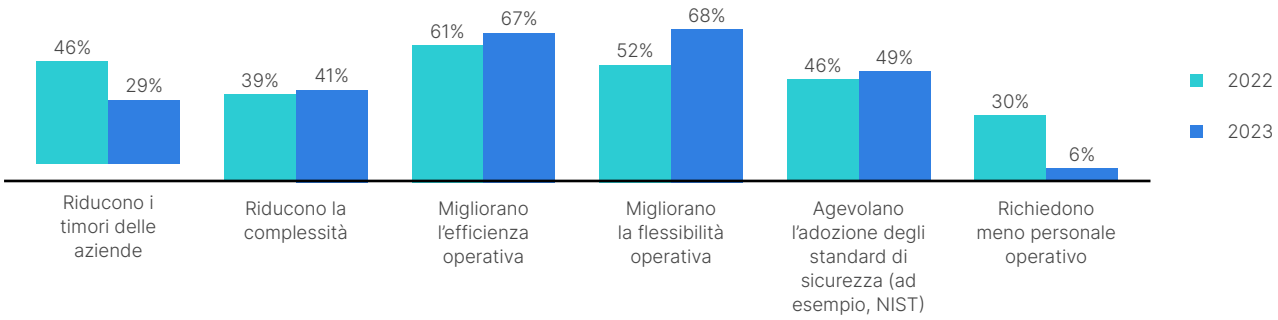
Funzionalità di sicurezza e sicurezza informatica implementate



In che modo la sicurezza informatica è di supporto

Sebbene i risultati del sondaggio rivelino che le soluzioni di sicurezza informatica continuano a contribuire al successo della maggior parte dei professionisti OT **(76%)**, in particolare migliorando l'efficienza **(67%)** e la flessibilità **(68%)**, i dati mostrano anche che la dispersione delle soluzioni rende più difficile proteggere in modo coerente il panorama IT/OT convergente.

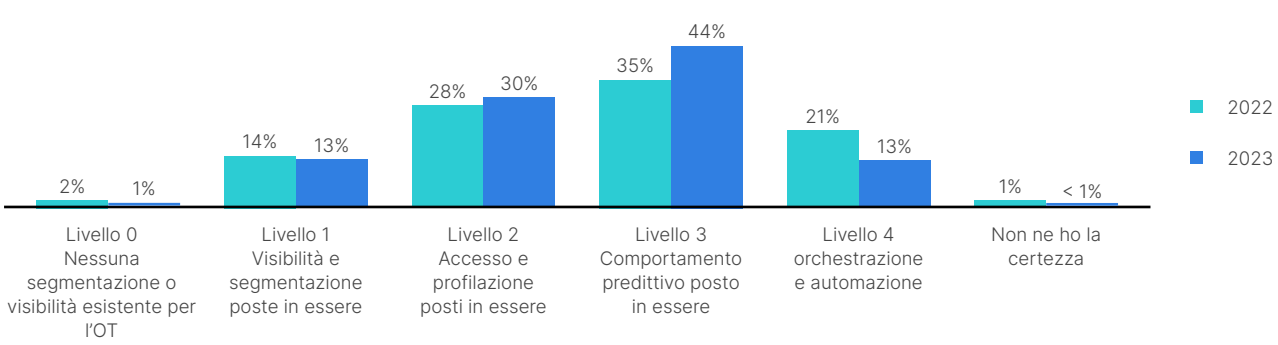
In che modo le soluzioni di sicurezza informatica contribuiscono al successo (nella top 3)



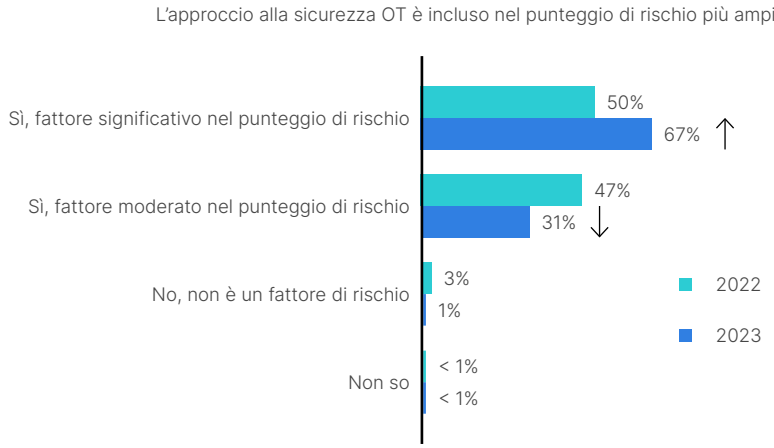
Approccio alla sicurezza informatica

Sebbene quest'anno il numero di individui che definiscono l'approccio alla sicurezza informatica OT della propria azienda come di livello 4 ("estremamente maturo") sia inferiore rispetto al 2022, ovvero sia sceso al **13% dal 21%**, il **44%** di tutte le organizzazioni si colloca ora al livello 3, rispetto al 35% dell'anno scorso, il che potrebbe riflettere una maturazione dell'approccio alla valutazione delle capacità, che si traduce in una visione più realistica dello stato del proprio approccio.

Maturità dell'approccio alla sicurezza OT



Quasi tutte le organizzazioni (98%) include ora l'approccio alla sicurezza informatica OT nel più ampio punteggio di rischio condiviso con l'alta dirigenza e i consigli di amministrazione.

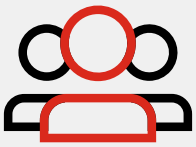


Executive Summary

Il "Fortinet 2023 State of Operational Technology and Cybersecurity Report" è il nostro quinto studio annuale basato sui dati di un'approfondita indagine mondiale condotta da una rispettata società di ricerca indipendente su 570 professionisti dell'OT.

La protezione dei sistemi OT è oggi più che mai criticapoiché sempre più organizzazioni connettono i loro ambienti OT a Internet. Sebbene la convergenza IT/OT offra molti vantaggi, è ostacolata e compromessa da minacce informatiche avanzate e distruttive. La ricaduta di questi attacchi è sempre più mirata agli ambienti OT. Per questi motivi, i dati del sondaggio di quest'anno indicano che la sicurezza informatica OT è oggi più che mai centrale e cruciale nel portfolio di rischi di un'organizzazione.

Un'analisi dei dati del 2023 rivela attualmente la presenza di quattro tendenze globali di rilievo:



Il rapporto 2023 rileva che il 95% delle organizzazioni ha nominato i propri CISO responsabili della sicurezza informatica OT.

- Il calo complessivo delle intrusioni è dovuto a un minor numero di violazioni da parte di insider, anche se il ransomware e il phishing rappresentano comunque minacce importanti. Tuttavia, più che a una diminuzione del rischio informatico, questo potrebbe essere dovuto all'adozione di un approccio più mirato da parte dei cybercriminali.
- Quasi tutte le organizzazioni hanno affidato la responsabilità della sicurezza informatica OT ad un CISO (Chief Information Security Officer) anziché ad un dirigente o ad un team operativo.
- Le organizzazioni e i professionisti del settore OT si affidano a un'ampia gamma di soluzioni di sicurezza informatica per combattere le intrusioni. Vi sono indicazioni che i prodotti monofunzionali e la dispersione delle soluzioni possano rendere più complessa l'applicazione delle policy e il loro rispetto in modo coerente nel panorama IT/OT convergente. Le organizzazioni e i professionisti dell'OT si affidano a una vasta gamma di soluzioni di sicurezza informatica per contrastare le intrusioni. Ci sono indicazioni che l'utilizzo di prodotti specifici e la diffusione di varie soluzioni possono rendere più complesso l'attuazione delle politiche e l'enforcement coerente delle stesse nell'ambito della convergenza IT/OT.
- Il numero di intervistati che considerano la maturità della sicurezza informatica della propria organizzazione al livello 4 è sceso dal 21% di un anno fa al 13% di oggi, mentre coloro che considerano la propria sicurezza informatica al livello 3 sono aumentati dal 35% al 44%. Questa oscillazione dei dati sembra indicare che i professionisti OT abbiano applicato un modello di autovalutazione più realistico delle capacità di sicurezza informatica OT della propria organizzazione.

Dopo cinque anni di sondaggi condotti tra i professionisti OT, la notizia più incoraggiante è che la sicurezza informatica sembra essere finalmente uscita dall'ombra. La sicurezza informatica OT attualmente al centro dell'attenzione della classe dirigenziale delle aziende. Tuttavia, la maggior parte di esse ha ancora molto lavoro da fare poiché non si può mai permettere di adagiarsi sulla situazione quando si parla di sicurezza informatica.

Per aiutare la tua organizzazione a migliorare il proprio approccio alla sicurezza OT, il Report sullo stato della tecnologia operativa e della sicurezza informatica di quest'anno si conclude con un elenco di best practice comuni che le organizzazioni di alto livello utilizzano per garantire la sicurezza dei propri sistemi OT.

Introduzione

Oggi nessuno può mettere in dubbio l'importanza di proteggere i sistemi OT. La tecnologia operativa controlla le infrastrutture critiche su cui tutti facciamo affidamento, dalla gestione della rete elettrica al funzionamento dei sistemi idrici e fognari, dalla gestione delle reti di trasporto alla produzione di beni essenziali e all'attivazione delle supply chain globali. E, per non dimenticare, l'OT è anche una componente chiave degli sforzi di accelerazione digitale di molte organizzazioni industriali.

Le attuali condizioni di mercato hanno reso l'adozione delle metodologie e delle tecnologie dell'Industria 4.0 un'"era di connettività, analisi avanzata, automazione e tecnologia di produzione avanzata"[1] essenziale per le aziende manifatturiere e altri settori per rimanere competitivi.

Minacce di sicurezza informatica per l'OT

La convergenza delle reti IT e OT non ha mancato di attirare l'attenzione dei cybercriminali e degli Stati-nazione aggressivi. I recenti rapporti FortiGuard Labs Global Threat Landscape sottolineano l'aumento del rilevamento di malware e di attività dannose nei sistemi OT.[2]

Diversi attacchi alla sicurezza informatica di alto profilo evidenziano questa problematica e fungono da campanello d'allarme per tutti coloro che sono responsabili della protezione dei sistemi OT. Un esempio lampante sono le costanti aggressioni della Russia nei confronti delle infrastrutture critiche dell'Ucraina[3], che è degenerata in una "guerra calda" fisica più di un anno fa.[4] Ma questi attacchi non si limitano all'aggressione aperta tra Stati-nazione. I sistemi tecnologici operativi in tutto il mondo continuano ad essere il bersaglio dei cybercriminali, in particolare l'industria manifatturiera, che continua ad essere vittima di numerosi attacchi ransomware mirati contro i propri sistemi OT.[5]

Purtroppo, la percentuale di organizzazioni nel sondaggio di quest'anno che hanno subito un'intrusione ransomware (32%) è rimasta immutata rispetto al gruppo dell'anno scorso. È necessario compiere progressi nella difesa da questo tipo di attacchi. Data l'evoluzione e la crescente sofisticazione delle operazioni ransomware, non sorprende che l'84% delle organizzazioni rappresentate nel sondaggio Fortinet 2023 Global Ransomware Report di quest'anno rimanga "molto" o "estremamente" preoccupata di fronte a questo tipo di minacce.[6]

Sebbene le violazioni intenzionali e non intenzionali da parte di insider siano diminuite considerevolmente quest'anno, secondo gli intervistati, le intrusioni da malware e phishing sono aumentate in modo significativo, rispettivamente del 12% e del 9%. Questi risultati del sondaggio sono supportati dall'ultimo FortiGuard Labs Global Threat Report, in cui si afferma: "Il malware è in grado di dominare le prime pagine dei giornali e di tenere le aziende con il fiato sospeso".[7]

No Longer Air-Gapped

Ora che le infrastrutture IT e OT sono state quasi universalmente integrate, l'isolamento che in precedenza manteneva i sistemi OT quasi invulnerabili agli attacchi informatici è scomparso. Di conseguenza, le superfici di attacco delle organizzazioni industriali si sono notevolmente ampliate. Se a questo si aggiunge la più massiccia distribuzione dei dispositivi Industrial-Internet-of-Things (IIoT), la nuova suscettibilità dell'OT al panorama delle minacce IT e l'elevato valore degli ambienti di produzione che aumentano la motivazione di un'organizzazione a pagare un riscatto, è chiaro perché la protezione dell'OT sia diventata di vitale importanza.

La sicurezza informatica OT sotto i riflettori

Nel Report sullo stato della tecnologia operativa e della sicurezza informatica[8] dello scorso anno si affermava che l'aumento dell'attenzione e degli investimenti nella sicurezza informatica OT è uno sviluppo eccellente. Tuttavia, come emerge dal sondaggio di quest'anno, molte organizzazioni hanno ancora molta strada da percorrere per proteggere adeguatamente i propri sistemi OT.

Analizziamo in modo più approfondito i dati del sondaggio di quest'anno e scopriamo quali lezioni possiamo trarre dallo stato attuale della sicurezza informatica OT. Ci auguriamo che uno dei titoli del nostro rapporto dell'anno prossimo riguardi i progressi significativi compiuti per proteggere i sistemi OT.

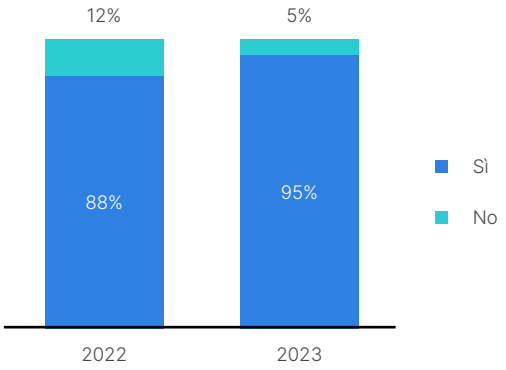
Approfondimenti critici

Approfondimento critico n. 1: la responsabilità della sicurezza informatica OT si sta spostando dal personale OT agli esperti di sicurezza informatica

Il personale che si occupa di OT è presente in quasi tutti i principali settori industriali: manifatturiero, trasporti, logistica, sanitario, farmaceutico, petrolifero, gas, energetico, servizi pubblici, chimico, idrico, acque reflue e così via. E tradizionalmente, questi professionisti OT sono anche profondamente coinvolti nelle decisioni di acquisto in termini di sicurezza informatica per i loro ambienti OT.

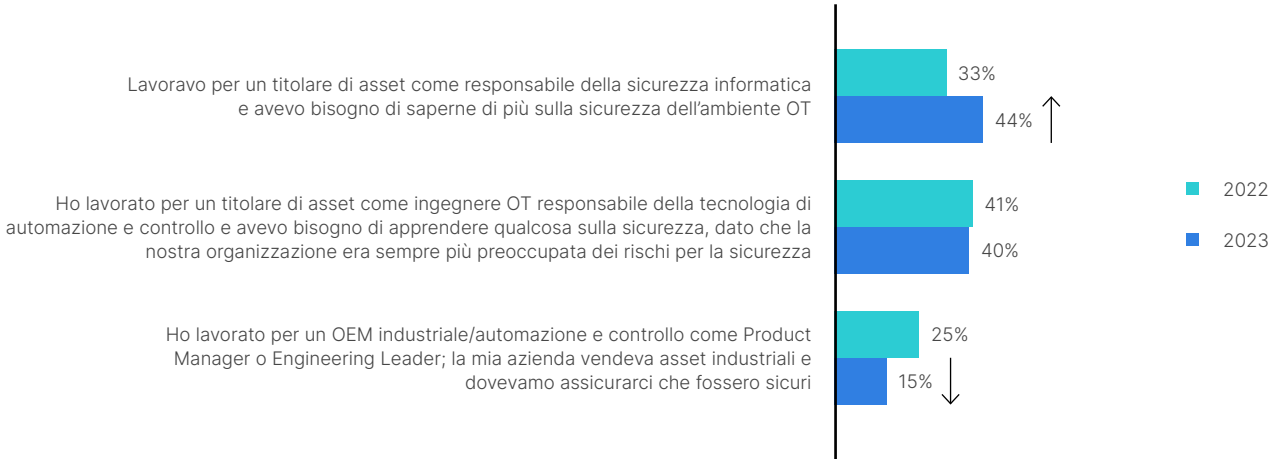
Tuttavia, sembra che la continua vulnerabilità delle reti OT agli attacchi informatici abbia portato a spostare le decisioni sulla sicurezza informatica OT sotto la responsabilità del CISO. I dati mostrano anche che i professionisti della sicurezza OT provengono principalmente dal team IT piuttosto che da quelli con esperienza nel product management. Di conseguenza, come indicano i dati dell'indagine, i leader dell'alta direzione e i responsabili della sicurezza tradizionali, in particolare il CISO/CSO, stanno diventando sempre più coinvolti e impegnati nella presa di decisioni sulla sicurezza informatica.

D: La tua organizzazione prevede di affidare la sicurezza informatica OT al CISO nei prossimi 12 mesi?



Sicurezza informatica sotto il controllo del CISO nei prossimi 12 mesi

D: Quale percorso professionale ti ha spinto a lavorare nell'ambito della sicurezza OT?

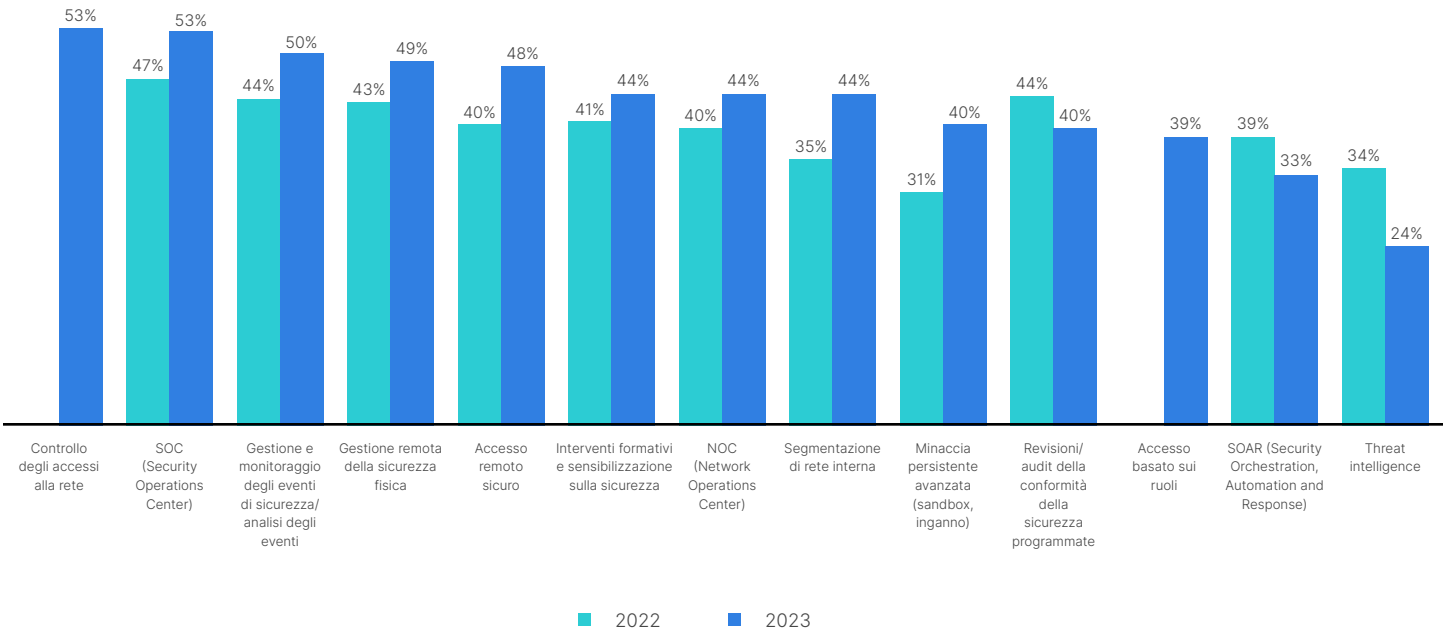


Percorso professionale che ha spinto a lavorare nell'ambito della sicurezza OT

Approfondimento critico n. 2: i professionisti OT si affidano a una serie di soluzioni

I professionisti OT intervistati quest'anno sono alla ricerca di soluzioni di sicurezza informatica che, in primo luogo, rilevino le vulnerabilità note. Una delle principali problematiche che i team OT devono affrontare è che i downtime sono spesso molto più critici rispetto agli ambienti IT. Di conseguenza, il successo di una rete OT si misura meno con la garanzia della riservatezza e dell'integrità dei dati e più con la disponibilità dei sistemi critici. Quindi, sono particolarmente apprezzati i tempi di risposta agli attacchi, come illustrato dall'aumento generalizzato dell'implementazione di soluzioni di rete OT e di sicurezza informatica.

Tuttavia, come nel caso delle reti IT, la semplice presenza di soluzioni non è sufficiente a prevenire tutti gli attacchi alle reti OT. Parte della problematica può essere legata alla dispersione di soluzioni e fornitori, che rende più difficile rilevare una minaccia e impedire una risposta coordinata.



Funzionalità di sicurezza e sicurezza informatica implementate

Approfondimento critico n. 3: il numero di intrusioni è ancora problematico

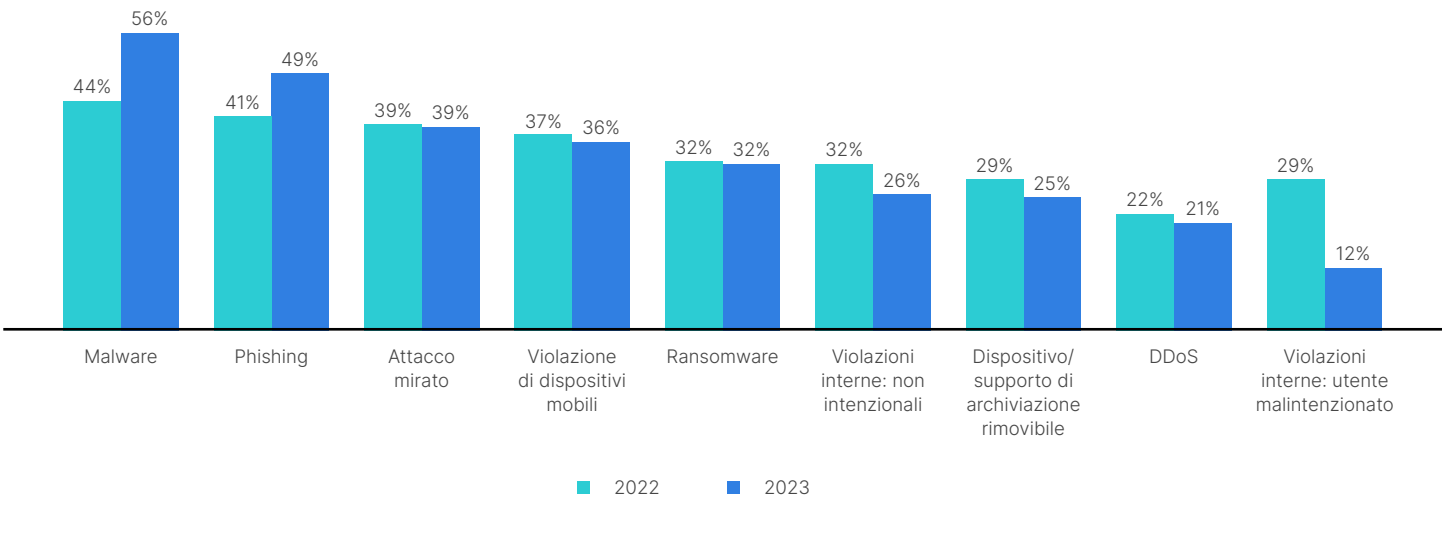
Il numero di intrusioni subite è in calo, tuttavia il 75% delle organizzazioni intervistate ha dichiarato di aver subito almeno un'intrusione negli ultimi 12 mesi. Il calo complessivo è attribuito ad un minor numero di violazioni da parte di insider, non ad un minor numero di attacchi da parte di cybercriminali.

Tuttavia, gli incidenti di malware e phishing sono ancora le minacce più comuni e sono aumentati rispetto all'anno scorso, ma il ransomware rimane la preoccupazione maggiore e gli incidenti continuano a crescere. Gli impatti sono stati ampi e hanno interessato sempre più spesso i sistemi IT e OT, ma tendenzialmente sono stati risolti entro poche ore (sempre più spesso in pochi minuti).

Una parte della diminuzione delle intrusioni potrebbe essere dovuta a un cambiamento nelle tattiche dei cybercriminali. Tuttavia, gli approcci degli aggressori sono ancora efficaci se consideriamo l'aumento del malware e del phishing. In ogni caso, dato l'elevato valore dei sistemi OT, possiamo prevedere un passaggio ad attacchi più mirati.

È importante notare che l'eccessiva sicurezza di essere pronti danneggia le organizzazioni tanto quanto la presenza di una tecnologia sbagliata, che, secondo il nostro ultimo rapporto sul ransomware[9] è un altro problema che la maggior parte delle organizzazioni è costretta ad affrontare. Sebbene la difesa contro il ransomware, ad esempio, sia una priorità assoluta per la maggior parte delle organizzazioni, molte soluzioni che queste identificano come fondamentali per la loro strategia di sicurezza informatica forniscono una scarsa protezione contro gli attacchi ransomware.

D: Quali tipi di intrusioni sono state subite? (sono possibili più opzioni)



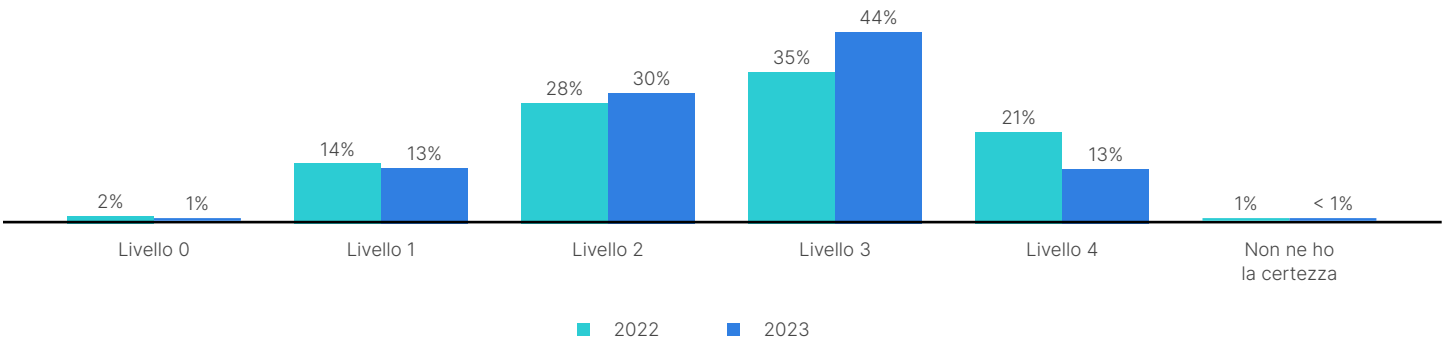
Intrusioni subite

Approfondimento critico n. 4: il livello medio di maturità della sicurezza informatica sta migliorando

Un'autovalutazione accurata delle proprie capacità di sicurezza informatica e della maturità dell'approccio adottato è un primo passo fondamentale per migliorare le difese informatiche e proteggere adeguatamente gli ambienti OT. A livello globale, quest'anno sono diminuite le aziende che definiscono il proprio approccio alla sicurezza informatica OT come estremamente maturo, passando dal 21% del 2022 al 13% di quest'anno. Allo stesso tempo, il 44% delle organizzazioni definisce la maturità del proprio approccio alla sicurezza informatica OT di livello 3, rispetto al 35% di un anno fa. Questi dati indicano che gli intervistati di quest'anno potrebbero aver adottato un modello di autovalutazione più realistico delle proprie capacità di sicurezza informatica OT.

Scala di maturità	
Livello 0	Nessuna segmentazione o visibilità esistente per l'OT
Livello 1	Visibilità e segmentazione poste in essere
Livello 2	Accesso e profilazione posti in essere
Livello 3	Comportamento predittivo posto in essere
Livello 4	Sfruttamento di orchestrazione e automazione

D: Come definiresti la maturità del tuo approccio alla sicurezza OT?

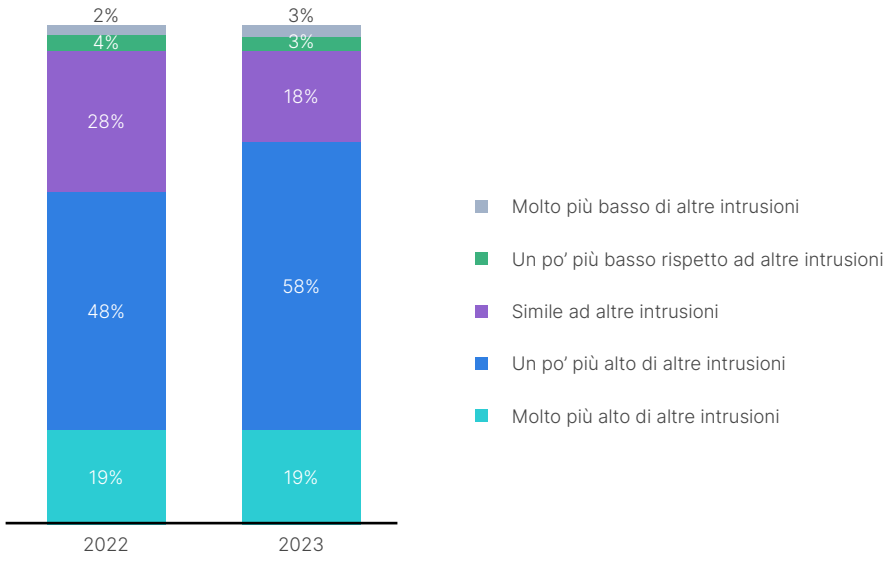


Maturità dell'approccio alla sicurezza OT

Un’analisi più approfondita dell’indagine 2023

D: Rispetto ad altre intrusioni, quanto ti preoccupa l’impatto del ransomware sul tuo ambiente OT?

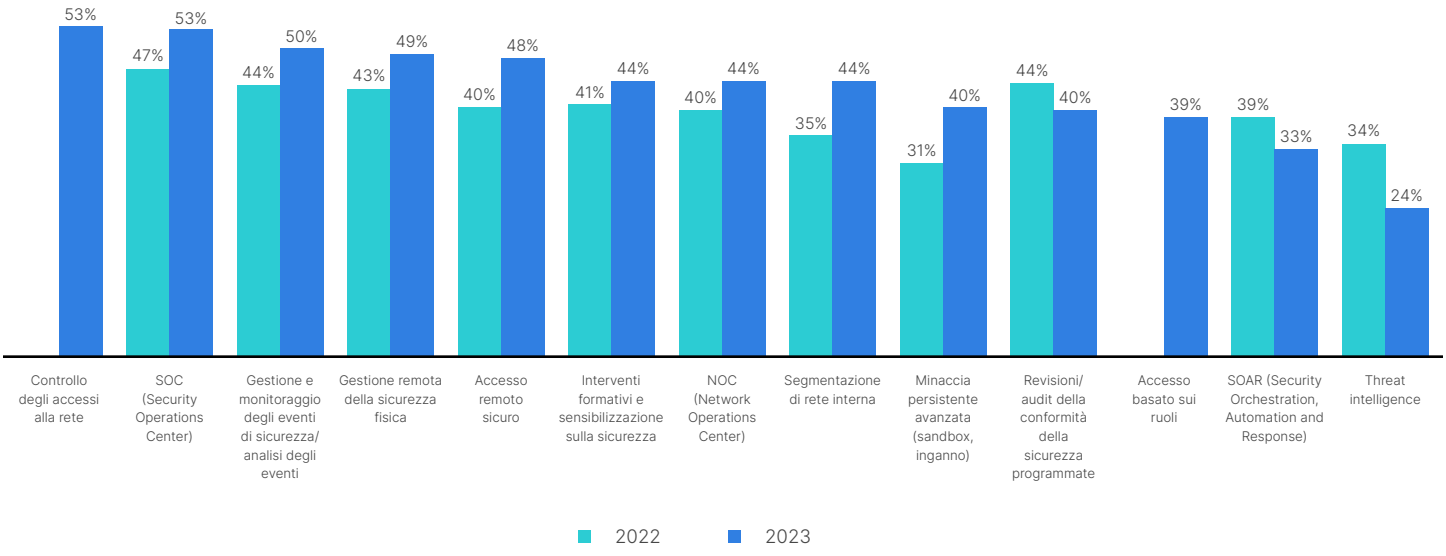
Gli incidenti di ransomware che si verificano nella rete aziendale o IT possono avere un impatto diretto o indiretto sulla produzione. Le organizzazioni sono sempre più preoccupate rispetto ad altre intrusioni (nonostante il phishing e il malware siano più comuni). Pertanto, il ransomware rimane una delle principali preoccupazioni a causa delle implicazioni produttive e finanziarie.



Timori riguardo all’impatto del ransomware

D: Quali sono le funzionalità di sicurezza e sicurezza informatica su cui puoi contare attualmente?

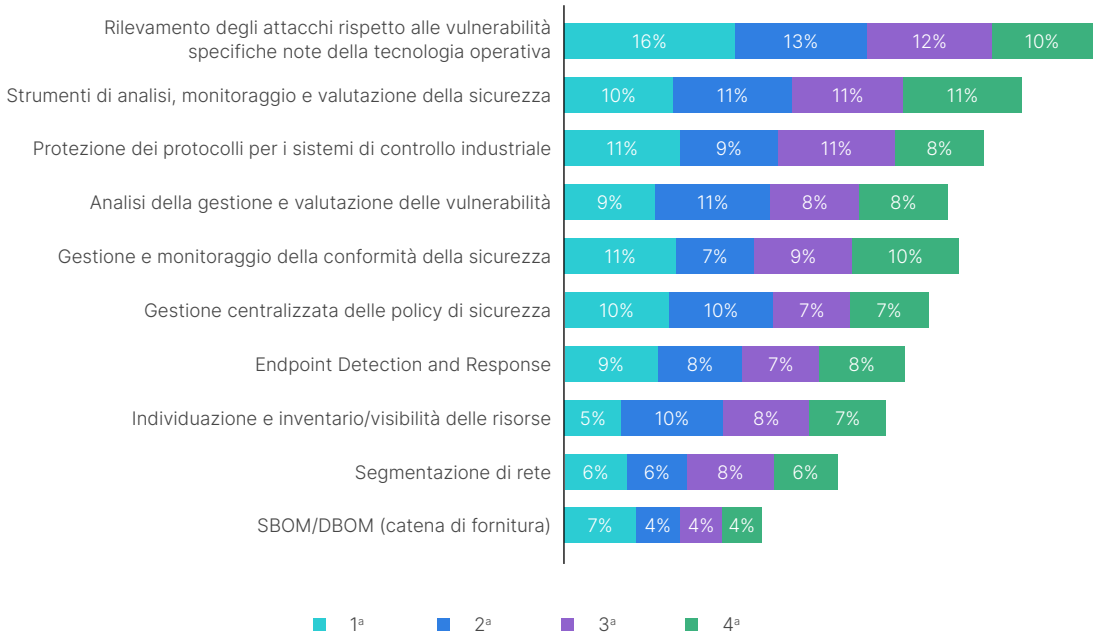
Per combattere le intrusioni, i professionisti del settore OT stanno rafforzando le numerose funzionalità di sicurezza informatica e di difesa attualmente implementate. Con l’aumento delle funzionalità, sospettiamo che gli audit di sicurezza siano in declino a causa della proliferazione di queste funzionalità aggiuntive e delle soluzioni più avanzate, come SOAR e threat intelligence. Una volta che queste nuove funzionalità saranno stabilmente operative, è probabile che gli audit ritorneranno ai livelli preesistenti.



Funzionalità di sicurezza e sicurezza informatica implementate

D: Quali sono le funzionalità più importanti nelle soluzioni di sicurezza informatica OT? (classificane un massimo di quattro)

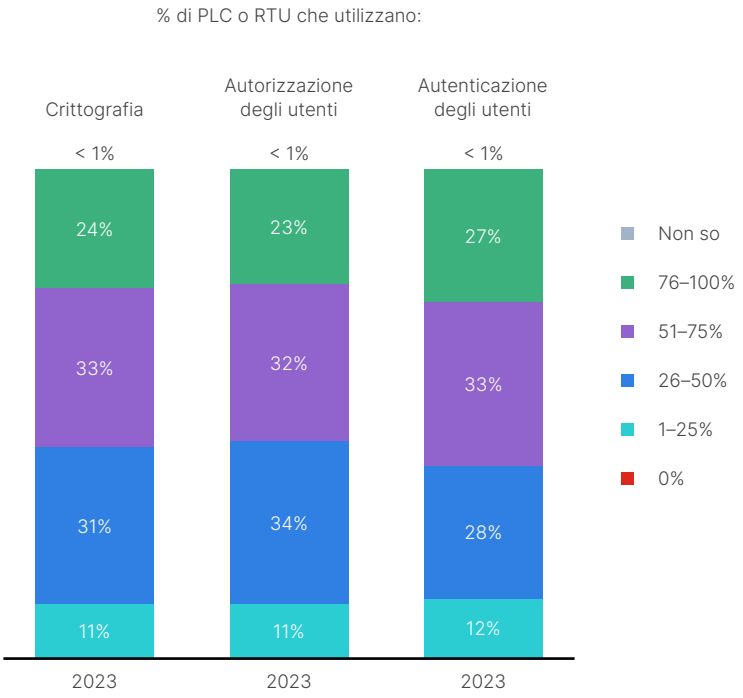
Il rilevamento degli attacchi contro le vulnerabilità note è attualmente la funzionalità più essenziale delle soluzioni di sicurezza informatica, con un'importanza crescente nell'ultimo anno. Un'altra indicazione della crescente maturità nella sicurezza OT è la minore priorità nel rilevamento e nella segmentazione degli asset. Un dato che abbiamo notato nel settore è la sua coerenza con la CIS Critical Security Controls ICS Companion Guide,[10] ovvero la maggior parte dei clienti ha compiuto queste procedure di base e sta passando a soluzioni di base e organizzative più avanzate.



Funzionalità delle soluzioni di sicurezza più importanti (classifica)

D: Quale percentuale dei tuoi PLC o RTU utilizza ciascuna delle seguenti funzionalità di sicurezza?

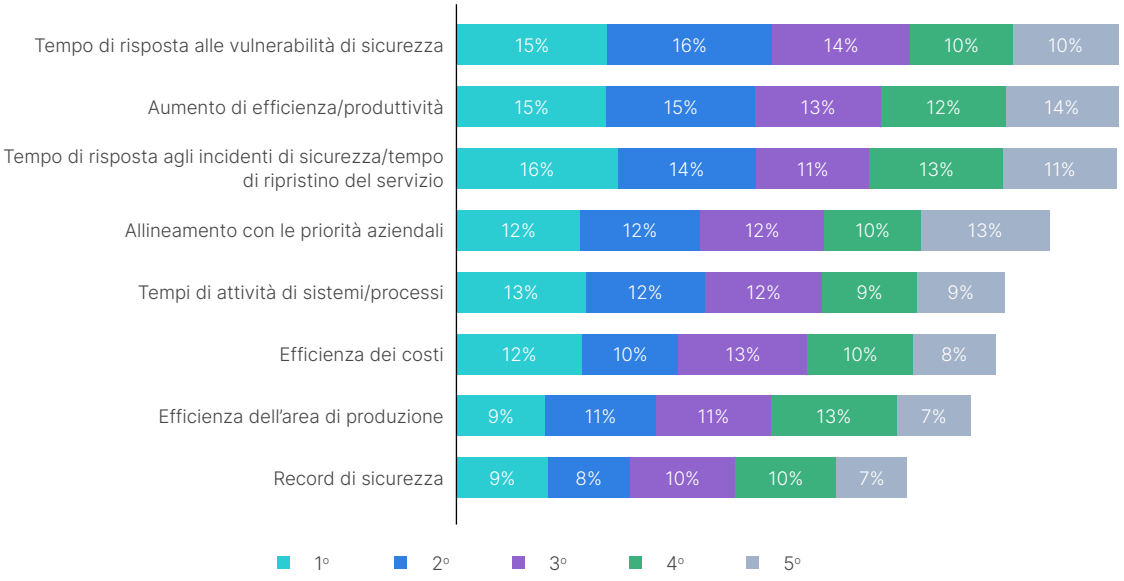
La crittografia, l'autorizzazione e l'autenticazione degli utenti tendono a essere utilizzate in oltre il 50% dei PLC o delle RTU.



Impatto globale

D: Come viene misurato il tuo successo? (classificane un massimo di cinque)

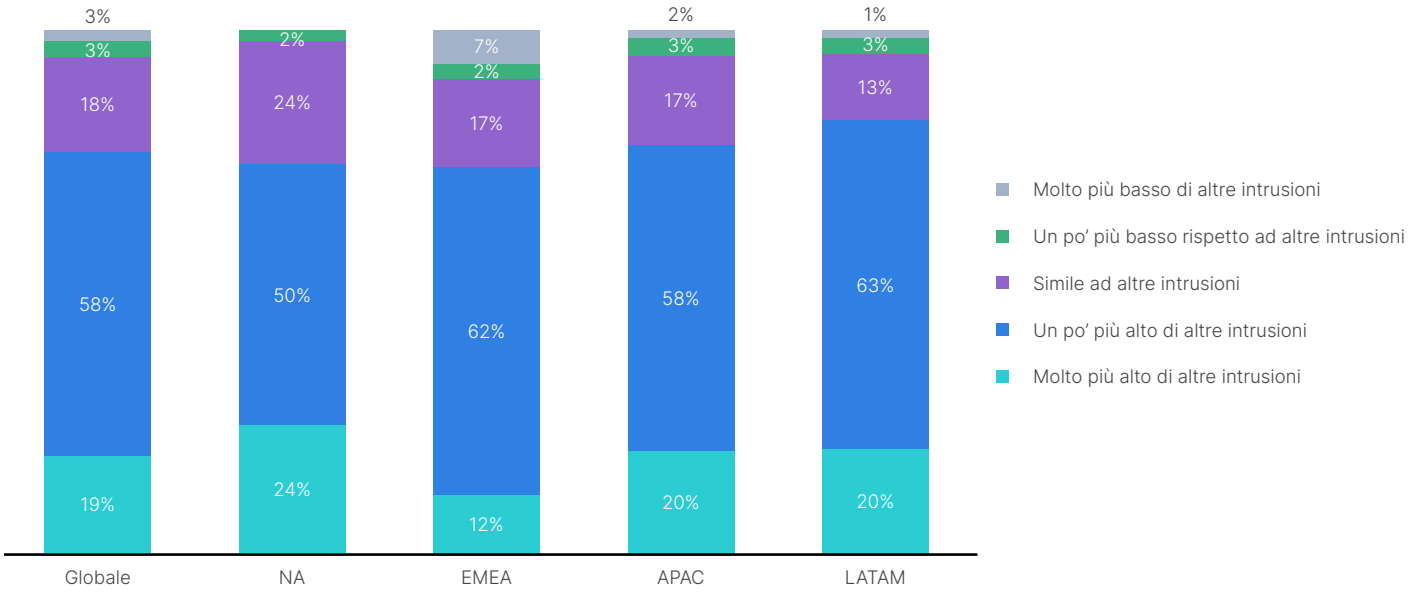
È interessante notare che non esiste un'unica definizione di successo dell'OT, il che indica l'immaturità dello spazio di sicurezza OT. Tuttavia, come ci si aspetta per gli ambienti OT, i guadagni in termini di tempi di risposta e produttività sono saliti in cima alla classifica.



Come viene misurato il successo (classifica)

D: Rispetto ad altre intrusioni, quanto ti preoccupa l'impatto del ransomware sul tuo ambiente OT?

Sebbene gli attacchi ransomware non siano le intrusioni più comuni, sono la principale preoccupazione della maggior parte delle organizzazioni a livello globale (più di qualsiasi altra minaccia), probabilmente a causa della loro notorietà e dell'elevato costo di ripristino dei sistemi colpiti.



Timori riguardo all'impatto del ransomware

Best practice

Il 75% delle organizzazioni che hanno partecipato al sondaggio di quest'anno ha segnalato almeno un'intrusione negli ultimi 12 mesi. Che tu ci creda o meno, si tratta di un miglioramento rispetto al 2022, quando oltre il 90% aveva segnalato almeno un'intrusione. E quest'anno solo l'11% degli intervistati ha segnalato sei o più intrusioni, mentre l'anno scorso il 27% aveva segnalato sei o più intrusioni.

Sebbene le soluzioni di sicurezza informatica continuino a contribuire al successo della maggior parte dei professionisti OT (76%), in particolare migliorando l'efficienza (67%) e la flessibilità (68%), i dati del rapporto indicano anche che la dispersione delle soluzioni rende ancora difficile integrare, utilizzare e applicare in modo coerente le policy in un panorama IT/OT sempre più convergente. Il problema è aggravato dall'obsolescenza dei sistemi, con la maggior parte delle organizzazioni (74%) che riferisce che l'età media dei sistemi ICS distribuiti nella propria organizzazione è compresa tra i sei e i dieci anni. Non c'è dubbio che siano stati compiuti dei progressi nella sicurezza informatica OT globale, ma le organizzazioni devono continuare a migliorare nel tempo.

Di seguito sono riportate alcune delle best practice che abbiamo ipotizzato essere alla base del piccolo ma significativo miglioramento riscontrato nei risultati del sondaggio di quest'anno.

Sviluppa una strategia di piattaforma di sicurezza informatica per fornitori e OT.

Il consolidamento riduce la complessità e accelera i risultati. Il primo passo è iniziare a realizzare una piattaforma nel tempo, collaborando con fornitori che progettano i loro prodotti tendendo conto di aspetti quali integrazione e automazione. Il fornitore giusto consentirà alle organizzazioni di integrare e applicare in modo coerente le policy in un panorama IT/OT sempre più convergente. Inoltre, cerca di affidarti a fornitori con un ampio portfolio di soluzioni in grado di fornire soluzioni di base per l'inventario e la segmentazione degli asset e soluzioni più avanzate, come un SOC OT o la capacità di supportare un SOC IT/OT congiunto.

Distribuisci la tecnologia di controllo degli accessi alla rete (NAC, Network Access Control).

Per risolvere le problematiche associate alla protezione dei sistemi ICS (Industrial Control System), SCADA (Supervisory Control And Data Acquisition), IoT (Internet of Things), dei dispositivi BYOD (Bring Your Own Device) e di altri endpoint, è necessario che la tecnologia NAC avanzata faccia parte di un'architettura di sicurezza completa. Una soluzione NAC efficace contribuisce anche a mantenere il controllo completo della rete di un'organizzazione, gestendo i nuovi dispositivi che desiderano connettersi o comunicare con altre parti dell'infrastruttura dell'organizzazione.

Adotta un approccio zero-trust.

Implementa i passaggi di base dell'inventario e della segmentazione degli asset. L'accesso zero-trust prevede la verifica continua di tutti gli utenti, le applicazioni e i dispositivi che desiderano accedere agli asset critici, indipendentemente da dove risiedono.

Integra formazione e corsi miratialla sensibilizzazione sulla sicurezza informatica.

La formazione sulla sicurezza informatica rimane fondamentale perché la battaglia contro i cybercriminali richiederà sempre più la responsabilizzazione collettiva di tutti i dipendenti, che dovranno avere le conoscenze e la consapevolezza necessarie per collaborare alla protezione di se stessi e dei dati dell'organizzazione. Le organizzazioni devono prendere in considerazione la possibilità di includere una formazione non tecnica rivolta a tutti coloro che utilizzano un computer o un dispositivo mobile, dai telelavoratori alle loro famiglie.

Suggerimenti principali

1. Continua ad implementare passaggi di base dell'inventario e della segmentazione degli asset, quindi utilizza soluzioni di microsegmentazione e di applicazione di patch virtuali più avanzate per proteggere i dispositivi dalle vulnerabilità note, in modo da avere il tempo sufficiente per applicare correttamente le patch ai dispositivi.
2. Collabora con i team IT, OT e di produzione per valutare adeguatamente i rischi informatici e di produzione, in particolare gli incidenti ransomware. Informa il CISO per assicurare la sensibilizzazione, la definizione delle priorità, il budget e l'allocazione del personale.
3. Sviluppa una strategia per la piattaforma di sicurezza informatica dei fornitori e dell'OT. Vengono introdotte molte nuove soluzioni di sicurezza, ma il gap di personale aumenta. Inoltre, man mano che il tuo approccio alla sicurezza matura, cerca di affidarti a fornitori con un ampio portfolio di soluzioni in grado di fornire soluzioni di base per l'inventario e la segmentazione degli asset e soluzioni più avanzate come un SOC OT o la capacità di supportare un SOC IT/OT congiunto.

Metodologia di studio

La maggior parte degli intervistati ha una funzione lavorativa di "operazioni di stabilimento" o "operazioni di produzione", e quasi un terzo è costituito da vicepresidenti o direttori delle operazioni di stabilimento. La maggior parte degli intervistati, indipendentemente dal ruolo ricoperto, è profondamente coinvolta nelle decisioni di acquisto in fatto di sicurezza informatica. E questi individui hanno sempre più l'ultima parola nelle decisioni di acquisto dell'OT. L'indagine di quest'anno ha rilevato che il 91% degli intervistati è regolarmente coinvolto nelle decisioni di acquisto delle soluzioni di sicurezza informatica della propria organizzazione.

Tutti coloro che hanno partecipato al sondaggio di quest'anno operavano in uno dei seguenti settori:

- Produzione
- Trasporti, logistica
- Sanitario, farmaceutico
- Petrolio, gas, raffinazione
- Energia, utenze
- Chimico, petrolchimico
- Idrico, acque reflue

Obiettivi dello studio

Fortinet si è rivolta a InMoment, un'azienda di terzi con competenze di ricerca, con l'obiettivo di sviluppare i tratti distintivi di un professionista OT.

Il sondaggio in essere ha lo scopo di comprendere più approfonditamente quanto segue:

- Come si inserisce il professionista OT nelle organizzazioni
- Come vengono utilizzate le funzionalità di sicurezza
- Come vengono monitorate e segnalate le informazioni
- Influenze e fattori di successo

Approccio

È stato utilizzato un campione per ottenere 570 risposte complete con i seguenti tipi di intervistati da un'azienda in:

- Produzione
- Trasporti, logistica
- Sanitario, farmaceutico
- Petrolio, gas, raffinazione
- Energia, utenze
- Chimico, petrolchimico
- Idrico, acque reflue
  - con oltre 1.000 dipendenti, con alcune eccezioni
- La tecnologia operativa è di competenza funzionale
- Ha responsabilità di segnalazione per le operazioni di produzione o di stabilimento

- È coinvolta nelle decisioni di acquisto in materia di sicurezza informatica
- Espansione a livello mondiale nel 2022 e 2023:
  - i partecipanti al sondaggio provenivano da diverse località del mondo, tra cui: Australia, Nuova Zelanda, Brasile, Canada, Egitto, Francia, Germania, India, Giappone, Messico, Sudafrica, Regno Unito e Stati Uniti.

Conclusioni

Il Rapporto 2023 sullo stato della tecnologia operativa e della sicurezza informatica rileva che le organizzazioni stanno rendendo prioritaria la sicurezza informatica per gli ambienti OT. Si tratta di una tendenza importante e necessaria, perché il 75% delle organizzazioni intervistate ha dovuto affrontare almeno un attacco informatico negli ultimi 12 mesi. I dati del sondaggio suggeriscono che la sicurezza informatica OT sta migliorando o maturando e gli incidenti sembrano diminuire. Allo stesso modo, i rischi associati agli incidenti OT stanno diventando più evidenti a causa degli eventi mondiali. Inoltre, le aziende hanno iniziato ad adottare un approccio alla sicurezza OT più aggressivo e i team IT sono sempre più coinvolti nelle reti industriali.

I dati del nostro sondaggio dimostrano un aumento generalizzato di varie soluzioni di sicurezza informatica OT. La sicurezza informatica della tecnologia operativa, l'ownership, il rischio e l'implementazione di soluzioni di sicurezza maturano ed impattano. Tuttavia, la maggior parte delle organizzazioni deve ancora percorrere molta strada per proteggersi adeguatamente dal malware più comune, come il ransomware.

[1] "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?", McKinsey and Company, 17 agosto 2022.

[2] 2022 Global Threat Landscape Report, FortiGuard Labs, 22 febbraio 2023.

[3] "Cyber-Attack Against Ukrainian Critical Infrastructure", CISA, 20 luglio 2021.

[4] "Ukraine: Russian attacks on critical energy infrastructure amount to war crimes", Amnesty International, 22 ottobre 2022.

[5] Jonathan Reed, Pipedream Malware Can Disrupt or Destroy Industrial Systems, Security Intelligence, 19 aprile 2023.

[6] The 2023 Global Ransomware Report, Fortinet, 24 aprile 2023.

[7] 2022 Global Threat Landscape Report, FortiGuard Labs, 22 febbraio 2023.

[8] Rapporto sullo stato della tecnologia operativa e della sicurezza informatica 2022, Fortinet, 21 giugno 2022.

[9] The 2023 Global Ransomware Report, Fortinet, 24 aprile 2023.

[10] CIS Critical Security Controls ICS Companion Guide, Center for Internet Security, Version 7.

giugno 20, 2023 10:44 AM

2101968-0-0-IT