

Studio sui risultati della sicurezza

Volume 2

Cinque procedure di sicurezza da
sfruttare al massimo



Sommario






Sono tornati i magnifici cinque	3
Risultati principali	4
Strategie per l'aggiornamento proattivo della tecnologia	6
Tecnologie di sicurezza integrate ed efficienti	13
Sviluppare funzionalità di rilevamento delle minacce e di risposta agli incidenti	19
Disaster recovery tempestivo e resilienza	29
Conclusioni e raccomandazioni	34
Informazioni su Cisco Secure	36
Appendice – Dati demografici del campione del sondaggio.	37

Sono tornati i "magnifici cinque"

Lo [studio Cisco sui risultati della sicurezza del 2021](#) mirava a valutare quantitativamente gli aspetti più importanti nella gestione della cybersecurity. Abbiamo esaminato 25 procedure di sicurezza generali e verificato in che misura fossero correlate agli 11 risultati del programma. Il rapporto tra procedure e risultati può essere verificato in modo interattivo leggendo lo [studio Cisco sui risultati della sicurezza del 2021](#) sul sito Web oppure scaricando il report completo.

Conclusi i test, tra le 25 procedure se ne sono distinte cinque in termini di contributo complessivo alla riuscita del programma di sicurezza in tutti i risultati misurati.

Nelle pagine che seguono, ci concentriamo su questi fattori di successo, i "magnifici cinque", per individuare quali strategie possono renderli più efficaci. Ecco i "magnifici cinque":

	Aggiornamento proattivo della tecnologia	L'azienda ha adottato una strategia di aggiornamento proattivo della tecnologia, che prevede aggiornamenti frequenti alle migliori tecnologie IT e di sicurezza disponibili.
	Tecnologia perfettamente integrata	Le tecnologie di sicurezza sono perfettamente integrate e funzionano in sinergia.
	Risposta tempestiva agli incidenti	Le funzionalità di risposta agli incidenti consentono di effettuare indagini sugli eventi e adottare misure correttive in modo tempestivo ed efficace.
	Rilevamento accurato delle minacce	Le funzionalità di rilevamento delle minacce permettono di conoscere in profondità gli eventi di sicurezza con la massima visibilità.
	Disaster recovery tempestivo	Le misure di ripristino limitano le conseguenze dell'attacco e aumentano la resilienza operativa in caso di un incidente di sicurezza.

L'ampia efficacia di queste procedure ci spinge a chiedercene il motivo. Che cosa le rende così fondamentali? Quali fattori le rendono più o meno efficaci? In che modo le aziende devono implementarle per ottenere i migliori risultati? È proprio per rispondere a queste domande che ripercorriamo insieme lo studio sui risultati della sicurezza.

Nelle pagine che seguono, ci concentriamo su questi fattori di successo, i "magnifici cinque", per individuare quali strategie possono renderli più efficaci. Abbiamo condotto un sondaggio indipendente in doppio cieco su oltre 5.100 professionisti IT e della sicurezza di tutto il mondo. In questa sede ne analizziamo i dati, estrapoliamo i risultati salienti e li condividiamo con l'obiettivo di raggiungere nuovi traguardi nel campo della sicurezza.

Conclusioni principali

Abbiamo chiesto a oltre 5.100 professionisti della sicurezza e dell'IT di 27 paesi quale approccio adottano nella propria azienda per aggiornare e integrare l'architettura di sicurezza, rilevare le minacce, attuare azioni correttive e rimanere resilienti in caso di eventi catastrofici. La mole e la varietà di informazioni, difficoltà, strategie e successi condivisi è stata considerevole. Ogni risposta è stata analizzata sotto diversi aspetti, arrivando alle principali conclusioni riportate di seguito.

Aggiornare e integrare l'architettura

- Un IT moderno e integrato contribuisce al successo complessivo del programma di sicurezza più di qualsiasi altra procedura o controllo.
- Le moderne architetture nel cloud sono molto più facili da aggiornare con regolarità.
- Le aziende che si affidano a un solo fornitore raddoppiano le probabilità di avere un'infrastruttura tecnologica integrata.
- Con tecnologie di sicurezza integrate, la probabilità di raggiungere livelli elevati di automazione dei processi è sette volte più alta.

Rilevare e reagire alle minacce informatiche

- Dove le persone coinvolte sono competenti, i processi e la tecnologia efficaci, i programmi SecOps registrano prestazioni più alte di 3,5 volte rispetto ai programmi basati su risorse più deboli.
- I team di rilevamento e risposta esterni vengono percepiti come più efficienti, ma i team interni mostrano un tempo medio di risposta più breve (6 giorni contro 13 giorni).
- I team che usano molto l'intelligence sulle minacce raddoppiano le probabilità di avere funzionalità di rilevamento e risposta efficaci.
- L'automazione raddoppia le prestazioni dei team alle prime armi e permette ai team esperti di avere prestazioni pressoché perfette (95%).

Rimanere resilienti quando si verificano eventi catastrofici

- Nelle aziende in cui la responsabilità ultima della continuità operativa e del disaster recovery è dei quadri dirigenziali, le probabilità di avere programmi efficaci è maggiore, circa l'11% in più rispetto alla media.
- Le probabilità di resilienza operativa non migliorano finché la continuità operativa e il disaster recovery non riguardano almeno l'80% dei sistemi critici.
- Le aziende che conducono test diversificati per verificare periodicamente la continuità operativa e il disaster recovery hanno una probabilità 2,5 volte maggiore di essere resilienti in caso di incidenti.
- Le aziende che hanno adottato l'ingegneria del caos nelle proprie procedure standard hanno il doppio delle probabilità di registrare livelli elevati di resilienza.

Informazioni sul sondaggio


Campionamento	Partecipanti	Analisi
Cisco ha affidato a YouGov, un'azienda di ricerca, la somministrazione di un sondaggio completamente anonimo verso la metà del 2021, da condursi con una tecnica di campionamento stratificato e casuale.	Sono stati intervistati 5.123 professionisti di IT, sicurezza e privacy ancora in attività in 27 paesi. I dati demografici del campione sono riportati in appendice .	Il Cyentia Institute, per conto di Cisco, ha fornito un'analisi indipendente dei dati del sondaggio e ha generato tutti i risultati presentati in questo studio.

5.123

professionisti di IT,
sicurezza e privacy
ancora in attività in

27

paesi



"Dobbiamo sapere che stiamo facendo tutto il possibile per mantenere sicuri i sistemi. Sappiamo quanto siano sofisticati gli hacker e quanto utilizzino ogni giorno nuove tecniche, sempre più avanzate. Vogliamo proteggere i nostri dispositivi, gli utenti e l'azienda in modo da ridurre la superficie esposta in caso di violazioni della sicurezza."

Eric J. Mandela, Assistant Director,
Technology Infrastructure, Allied Beverage Group

[Leggi di più](#)

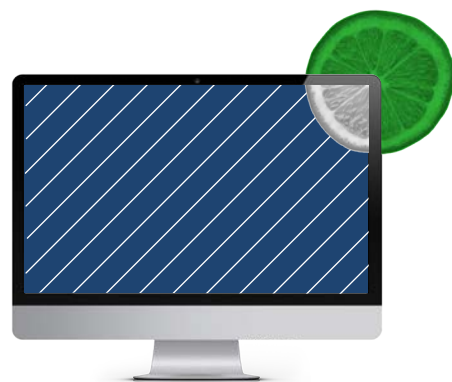
Strategie per l'aggiornamento proattivo della tecnologia

Secondo il precedente studio Cisco, un approccio proattivo all'aggiornamento e alla gestione delle migliori tecnologie IT e di sicurezza ha contribuito alla riuscita dei programmi di cybersecurity più di qualsiasi altra procedura. Non è un dato da sottovalutare, considerato che tutte e 25 le procedure oggetto dei test sono comunque considerate "best practice". Obiettivo di questo studio di follow-up è quindi capire cosa rende questa procedura così efficace.

Prima di entrare nel merito delle strategie di aggiornamento della tecnologia, esaminiamo anzitutto qual è lo stato delle infrastrutture esistenti. Abbiamo chiesto agli intervistati quale percentuale delle tecnologie di sicurezza al momento adottate consideravano obsolete. In media, il 39% delle tecnologie di sicurezza utilizzate è considerato obsoleto. Quasi il 13% degli intervistati afferma che almeno 8 su 10 degli strumenti di sicurezza utilizzati iniziano a mostrare i segni dell'età.

Già questo dato in sé aiuta a spiegare i molteplici vantaggi che derivano da una strategia proattiva di aggiornamento della tecnologia. Apparentemente, le tecnologie più recenti includono funzionalità avanzate in grado di contrastare la moltitudine di minacce informatiche in continua evoluzione. Ma c'è di più, continuiamo quindi ad approfondire questo argomento.

In media, il 39% delle tecnologie di sicurezza utilizzate è considerato obsoleto.



Le caratteristiche dell'infrastruttura influiscono sulle iniziative di aggiornamento?

Nello studio originale, avevamo ipotizzato che più le architetture sono moderne e basate sul cloud, più avrebbero potuto essere efficaci perché più facili da gestire e con misure di sicurezza integrate. Per verificare ulteriormente tale ipotesi, abbiamo chiesto agli intervistati di descrivere in generale la loro infrastruttura tecnologica scegliendo un insieme di descrittori, tra cui:

- Infrastrutture on-premises o nel cloud
- Infrastrutture moderne o obsolete
- Infrastrutture consolidate o distribuite

Questi aspetti dell'architettura contribuiscono all'efficacia delle funzionalità di aggiornamento della tecnologia? Molto, come mostrato nella figura 1. **Le aziende con architetture moderne, integrate e basate su cloud hanno più del doppio delle probabilità di aggiornare le proprie tecnologie in modo efficace rispetto alle aziende che usano tecnologie obsolete, separate e on-premises.** Ma prima di presentare questo grafico alla prossima riunione sulle strategie di migrazione al cloud, considera che le aziende con ambienti prevalentemente on-premises funzionano ancora ben al di sopra della media se hanno un IT moderno.

Certo, il cloud rende più facile implementare strategie di aggiornamento efficaci, ma il problema principale resta l'infrastruttura datata. Quando mantenere aggiornate infrastrutture vecchie diventa troppo complicato, può essere il momento giusto per pensare di adottare una nuova architettura. Naturalmente non è sempre possibile o conveniente con un'infrastruttura esistente o cruciale, ma il principio generale resta valido.

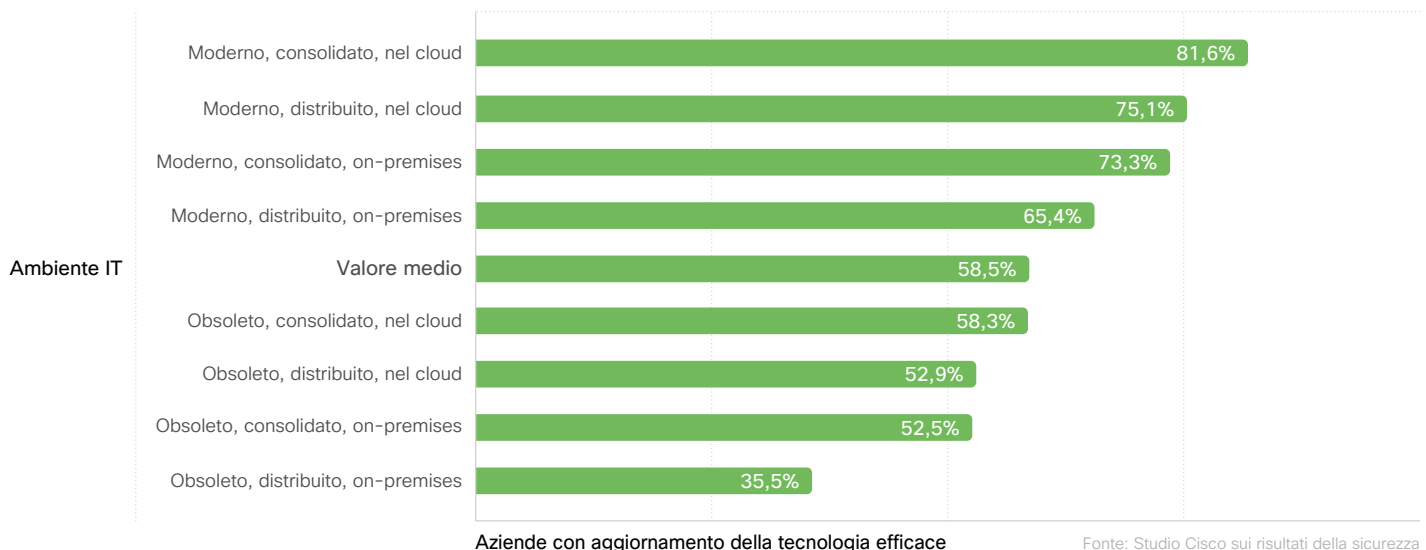


Figura 1 - Effetto delle caratteristiche dell'architettura IT sull'aggiornamento della tecnologia

81,6% delle aziende con architetture moderne, integrate e basate sul cloud vantano funzionalità efficaci di aggiornamento della tecnologia

Gli aggiornamenti frequenti aiutano la sicurezza a stare al passo con il business?

Secondo lo [studio sui risultati della sicurezza del 2021](#), il risultato più strettamente correlato a una strategia di aggiornamento proattivo della tecnologia era proprio avere un programma di sicurezza adeguato alle esigenze e alla crescita dell'azienda. In effetti, questo è stato il legame più stretto tra procedura e risultato emerso in tutto lo studio.

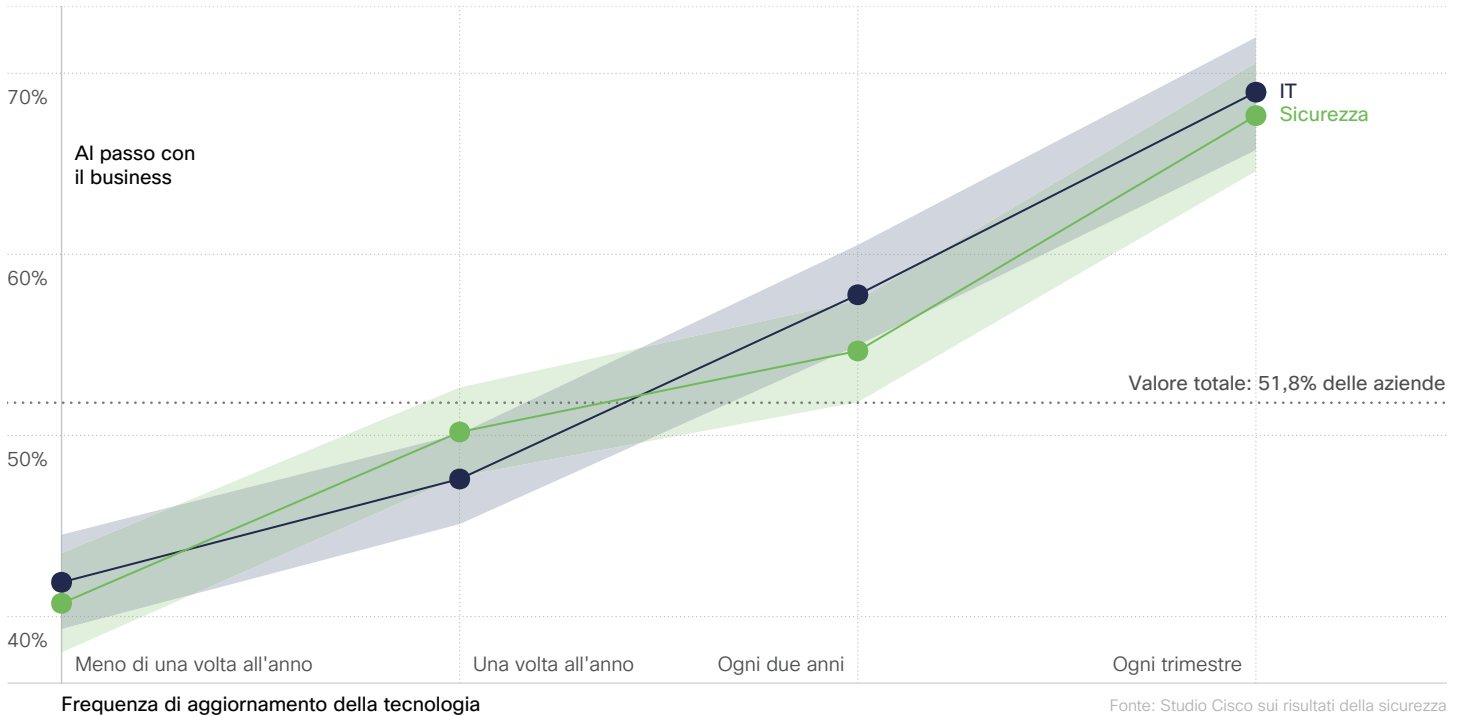


Figura 2 – Effetto della frequenza di aggiornamento della tecnologia sulla capacità del programma di sicurezza di adeguarsi al business¹

Abbiamo chiesto agli intervistati con quale frequenza venissero effettuati gli aggiornamenti dell'IT e della sicurezza nelle proprie aziende e confrontato tali risposte con la capacità dichiarata del programma di sicurezza di adeguarsi al business. Esiste una relazione tra queste due variabili? In

effetti, sì; aumentando la frequenza degli aggiornamenti, questo importante risultato migliora costantemente. **Complessivamente, le aziende che aggiornano le tecnologie IT e di sicurezza ogni trimestre hanno circa il 30% di probabilità in più di**

tenere il passo con il business rispetto alle aziende che eseguono aggiornamenti con una frequenza inferiore. Suona come un valido motto motivazionale per i team IT sotto pressione: tieni i sistemi aggiornati e continua così.

¹ I grafici di tutto il documento riportano l'etichetta "Valore medio" per una pratica o un risultato particolare. Questa percentuale rappresenta il valore medio tra tutte le risposte a quella specifica serie di domande. Viene fornito come riferimento e serve a capire chi si mantiene sopra la media e chi invece registra risultati poco accettabili. In alcuni grafici viene inoltre mostrato il grado di incertezza tramite barre di errore o aree sfumate. Quando queste aree si sovrappongono alla riga "Valore medio", non possiamo dedurre che quell'aspetto del programma di sicurezza che stiamo esaminando abbia un effetto sul risultato o sulla procedura.

Quale reparto, o quali figure professionali, devono promuovere l'aggiornamento della tecnologia?

Abbiamo stabilito che aggiornamenti frequenti favoriscono il business e la sua crescita, ma quale reparto, o quali figure professionali, devono assumersi il compito di guidare questo processo? Abbiamo chiesto agli intervistati di individuare i principali fattori che determinano l'aggiornamento delle tecnologie di sicurezza. Le risposte fornite possono essere raggruppate in tre grandi categorie:

- **Gestito dal fornitore:** la pianificazione è determinata da un provider SaaS o fa parte di un'iniziativa di consolidamento più ampia del fornitore (fattore più comune)
- **Approccio proattivo:** con un programma prestabilito o quando le nuove funzionalità o i nuovi scenari d'uso lo richiedono (il secondo fattore più comune)
- **Approccio reattivo:** in risposta a un incidente, quando la tecnologia si mostra obsoleta o per soddisfare i requisiti di conformità (meno comune)

Di per sé questi fattori sono già interessanti, ma ciò che vogliamo davvero sapere è se siano correlati a procedure più efficaci di aggiornamento della tecnologia. La figura 3 ci fornisce la risposta; le iniziative di aggiornamento della tecnologia che hanno maggiore successo sono quelle gestite dai fornitori (o dove i fornitori sono coinvolti attivamente). **Meno della metà delle aziende con approccio reattivo dichiara di avere funzionalità di aggiornamento efficaci, rispetto a quasi i due terzi delle aziende in cui gli aggiornamenti vengono gestiti dal fornitore.**

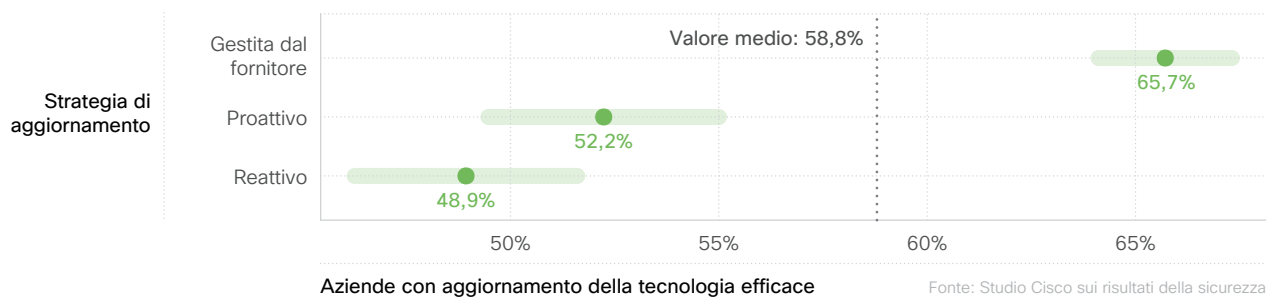


Figura 3 - Effetto dei fattori principali sull'aggiornamento delle tecnologie di sicurezza

Certo, detto da un fornitore di prodotti IT e di sicurezza, tutto ciò sembra sospetto. Eppure, lo ribadiamo, non abbiamo avuto alcuna influenza su questo risultato. Il sondaggio è stato condotto da un'azienda di ricerca indipendente e rinomata, gli intervistati non avevano idea che il sondaggio fosse sponsorizzato da Cisco e i dati, rappresentati nella figura 3, sono stati analizzati dal celebre Cyentia Institute. E, per non sbagliare, useremo ogni cautela possibile nell'interpretare questi risultati.

Sospettiamo infatti che gran parte dei miglioramenti attribuiti all'approccio basato sul fornitore dipenda dal fatto che sia più facile aggiornare periodicamente le architetture cloud o SaaS. E non perché i fornitori siano in qualche modo più bravi, ma perché sono senz'altro in grado di evitare gli ostacoli interni e superare i pantani politici che possono intralciare i piani di aggiornamento.

Per dirla con Rob Base e DJ EZ Rock, "ci vogliono due persone per fare andare bene le cose e due per renderle straordinarie." Chi avrebbe potuto immaginare la loro anima da architetti della sicurezza! Può diventare molto semplice realizzare gli obiettivi di sicurezza sfruttando l'inerzia del fornitore della soluzione tecnologica per averla sempre aggiornata.

65,7% delle aziende che si affidano agli aggiornamenti dei fornitori dichiara solide funzionalità di aggiornamento della tecnologia

Aggiornare per funzionalità o compatibilità?

Nella sezione precedente abbiamo esaminato gli scenari che richiedono alle aziende di aggiornare le tecnologie; ora vedremo i motivi che portano a preferire una soluzione a un'altra. La figura 4 riporta i criteri di scelta preferiti dagli intervistati. Una soluzione integrata nella tecnologia esistente è di gran lunga la preferita, seguita da soluzioni che offrono le funzionalità migliori o soddisfano esigenze particolari. Sorprenderà forse che i costi sono l'ultima preoccupazione.

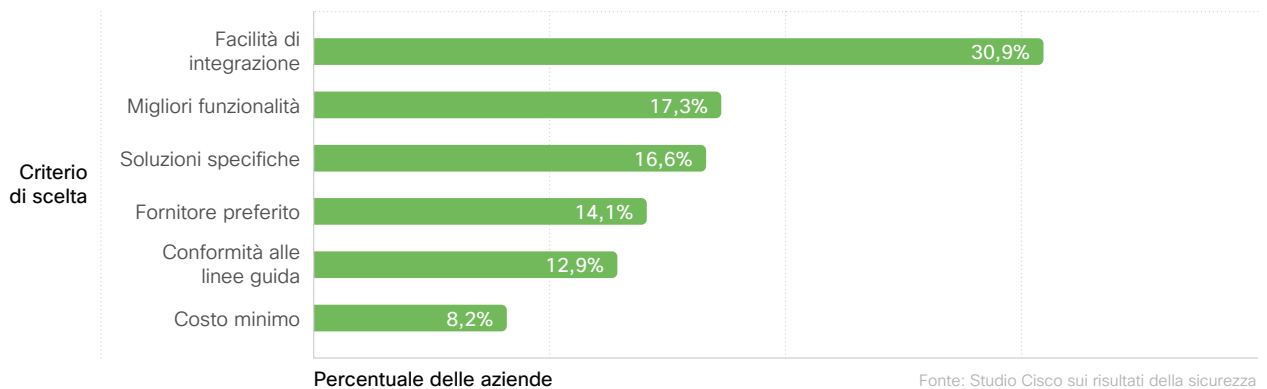
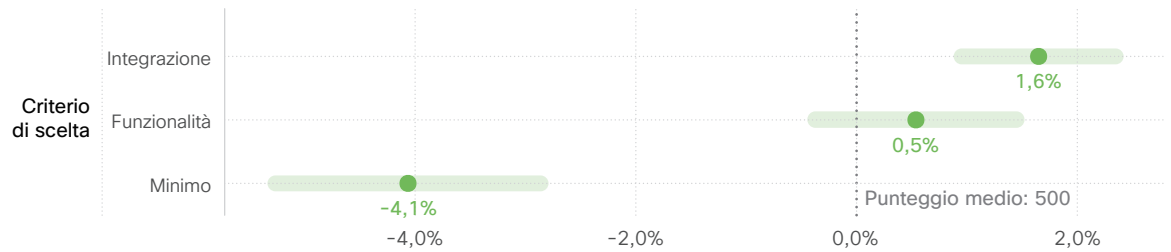


Figura 4 - Principali criteri di selezione per aggiornare i prodotti di sicurezza

Tutto molto giusto, ma qualcuno di questi criteri gioca un ruolo in termini di efficacia di un programma di sicurezza? Per rispondere a questa domanda, abbiamo raggruppato i criteri di scelta della figura 4 in tre categorie:

- **Minimo:** soluzione con il costo minimo; conformità alle linee guida
- **Integrazione facile:** integrazione nella tecnologia esistente; uso dei fornitori preferiti
- **Funzionalità:** migliori; soluzioni specifiche

Abbiamo quindi confrontato queste categorie con un punteggio aggregato creato per ogni azienda in base al raggiungimento degli 11 risultati della sicurezza. Se il valore assoluto del punteggio non dice molto, permette però di mettere a confronto le diverse strategie di aggiornamento. **Come mostrato nella figura 5, preferire l'integrazione e le funzionalità nella scelta dei prodotti offre risultati migliori rispetto ai costi minimi o ai requisiti di conformità. E l'approccio basato sull'integrazione è l'unico che supera in modo significativo la media.**



Differenza in percentuale dal punteggio medio dei risultati della sicurezza Fonte: Studio Cisco sui risultati della sicurezza


Figura 5 - Effetto del criterio di scelta della tecnologia sul punteggio complessivo dei risultati della sicurezza

Le differenze qui sono piuttosto esigue in termini di efficacia complessiva del programma. Ed è probabile che questi dati rappresentino solo un timido accenno a quali debbano essere le priorità e le procedure di un programma di sicurezza in una prospettiva più ampia. Allo stesso tempo, ci suggeriscono anche che vale la pena prendere in considerazione questioni apparentemente più leggere, ad esempio perché scegliamo un prodotto anziché un altro. E se stai valutando le funzionalità ai fini dell'aggiornamento della soluzione di sicurezza, prendi spunto da questo grafico per dare priorità alla compatibilità e alle funzionalità rispetto ai costi.

Cos'è il punteggio dei risultati della sicurezza?

Abbiamo chiesto agli intervistati di valutare la riuscita del proprio programma di sicurezza rispetto a 12 diversi risultati. Nella prima edizione dello [studio sui risultati della sicurezza](#), abbiamo analizzato i risultati in modo approfondito; alcuni dei risultati verranno esaminati singolarmente anche in questo studio. Volevamo inoltre creare un punteggio aggregato in grado di rappresentare complessivamente l'efficacia del programma di sicurezza in base al grado di conseguimento di ciascuno dei 12 risultati. Questo dato aggregato è chiamato "punteggio dei risultati della sicurezza" e lo menzioneremo più volte nel corso del documento.

Per ottenere questo punteggio, abbiamo utilizzato una sofisticata tecnica statistica chiamata "Item Response Theory". Questa tecnica ci consente di valutare le aziende in base al conseguimento di tutti i risultati, assegnando un punteggio che tiene conto anche della difficoltà con cui alcuni dei risultati possono essere raggiunti. Questa tecnica collaudata consente di creare punteggi standardizzati. Se il valore assoluto del punteggio non dice molto, permette però di mettere a confronto i diversi programmi.



"I CISO devono essere al tempo stesso influencer ed educatori. Se vogliamo essere efficaci, dobbiamo essere all'avanguardia nelle decisioni sulle strategie da adottare. Ma mentre cerchiamo di convincere le persone che la sicurezza è importante, che abbiamo bisogno degli investimenti giusti e che dobbiamo essere coinvolti in ogni aspetto del business, è nostro compito anche educare. La maggior parte dei dirigenti non ha una formazione specifica in materia di sicurezza e spetta a noi informarli dei rischi impliciti in ogni fase quando si prende una decisione."

Helen Patton, Advisory CISO, Cisco  [@CisoHelen](https://twitter.com/CisoHelen)

Ascolta Helen parlare di come è cambiato il ruolo dei CISO in [questo interessante episodio](#) del nostro podcast Security Stories

Tecnologie di sicurezza integrate ed efficienti

Secondo il nostro ultimo [studio sui risultati della sicurezza](#), tecnologie di sicurezza integrate ed efficienti in un'infrastruttura IT più grande contribuiscono alla probabilità di conseguire tutti i risultati del programma. Abbiamo posto una serie di domande con l'intenzione di approfondire quali fossero i fattori alla base di questo risultato, a partire dai motivi dell'integrazione.

Secondo gli intervistati, l'obiettivo più comune per cui si desidera integrare le tecnologie di sicurezza è migliorare l'efficienza del monitoraggio e dell'auditing. Un motivo che suona familiare, considerata la difficoltà e la frustrazione di dover controllare numerose console o dashboard per ricostruire in qualche modo ciò che accade sulla rete. Anche una facile collaborazione e l'automazione sono stati individuati come motivi comuni che spingono a preferire l'integrazione delle tecnologie di sicurezza (ne parleremo meglio più avanti). Abbiamo confrontato queste motivazioni con i livelli di integrazione tecnologica e i risultati del programma dichiarati, ma non è emersa una forte correlazione. Forse "cosa" o "come" valgono più di "perché" quando si parla di integrazione delle tecnologie di sicurezza? Approfondiamo questo tema nelle prossime domande.

Secondo gli intervistati, l'obiettivo più comune per cui si desidera integrare le tecnologie di sicurezza è migliorare l'efficienza del monitoraggio e dell'auditing.



Acquistare o realizzare una tecnologia integrata?

Dallo studio precedente sappiamo che integrare le tecnologie di sicurezza genera risultati positivi, ma qual è il modo migliore per ottenere un'infrastruttura tecnologica perfettamente integrata? Acquistare l'integrazione? Realizzarla su misura in base alle esigenze specifiche? O non fare nulla? Proviamo a scoprirlo.

Abbiamo chiesto agli intervistati quale approccio adottassero generalmente per l'integrazione delle tecnologie di sicurezza e riportato le risposte nella figura 6. **Complessivamente, più di tre quarti delle aziende preferisce acquistare soluzioni integrate piuttosto che crearle.** Di queste aziende, quasi il 40% sceglie tecnologie dotate di integrazioni preconfigurate nell'infrastruttura esistente. E quasi il 37% va persino oltre e preferisce affidarsi a un unico fornitore, in modo che le soluzioni siano integrate sin dall'inizio o facciano parte di una piattaforma più ampia. Solo poco più del 20% è disposto a realizzare autonomamente l'integrazione, a condizione che il prodotto soddisfi le esigenze specifiche. La percentuale di chi non prende iniziative in merito rimane bassa.

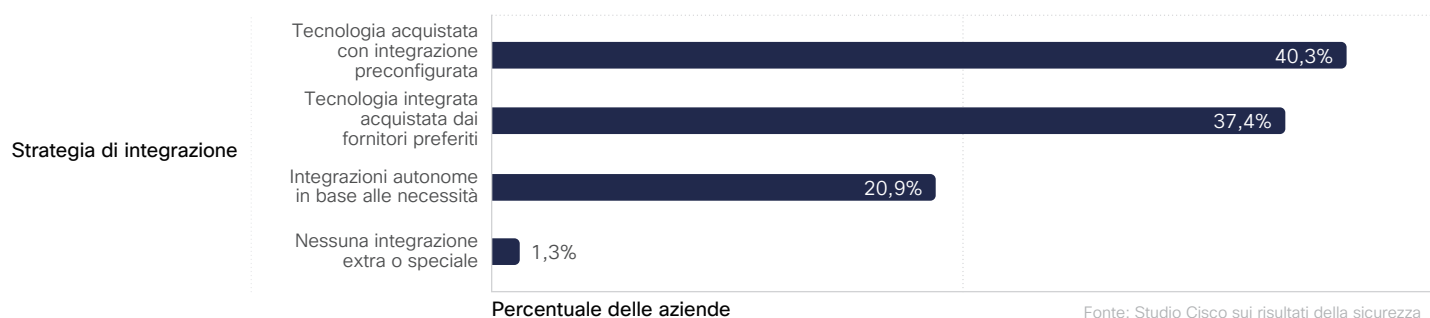


Figura 6 – Approcci comuni all'integrazione delle tecnologie di sicurezza in tutte le aziende

Nel complesso,
più di

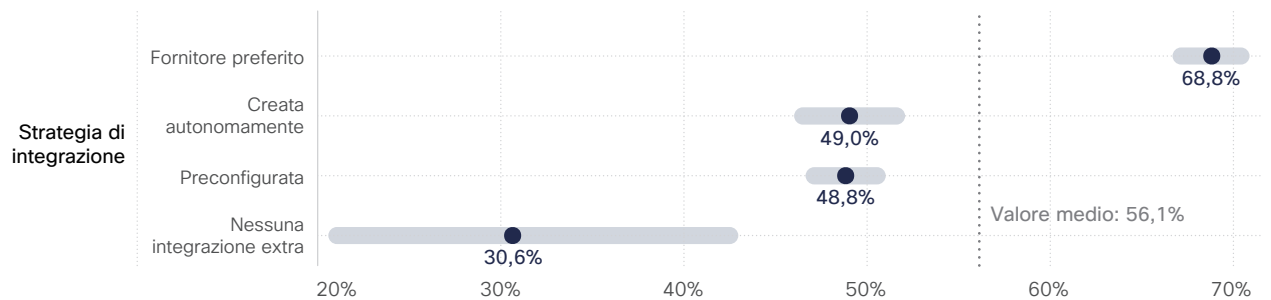
3/4

delle aziende preferisce
acquistare soluzioni
integrate anziché
realizzarle

Nella figura 7 cerchiamo di capire se i diversi approcci all'integrazione fanno una differenza. Qui di nuovo constatiamo i vantaggi di collaborare con i fornitori per mantenere la tecnologia moderna e integrata. **Come si evince dal grafico, preferire un unico fornitore assicura il doppio della probabilità di ottenere tecnologie di sicurezza integrate rispetto a un approccio di "non intervento" (circa il 69% contro circa il 31%).** Inoltre, secondo la nostra ricerca, questo dato rimane coerente nelle aziende di ogni dimensione, anche se i vantaggi di preferire un unico fornitore sono leggermente maggiori nelle piccole e medie imprese.

E sì, siamo consapevoli che questo risultato può sembrare stranamente favorevole a un'azienda come la nostra che offre un'ampia gamma di soluzioni di sicurezza integrate. Né possiamo nascondere che ci faccia piacere, in quanto avalla la strategia di Cisco, ma ricordiamo ancora una volta che lo studio è stato condotto in doppio cieco e i risultati non sono stati manipolati in alcun modo.

Non sorprende invece che le aziende propense al "non intervento" finiscano per incarnare una profezia che si autoavvera. **Ci aspettiamo tuttavia che qualcuno sarà sorpreso dal constatare che non c'è praticamente alcuna differenza tra coloro che acquistano prodotti con integrazioni preconfigurate e quelli che li integrano autonomamente.** Solo meno della metà (intorno al 49%) delle aziende che adottano questi approcci dichiara livelli di integrazione soddisfacenti.



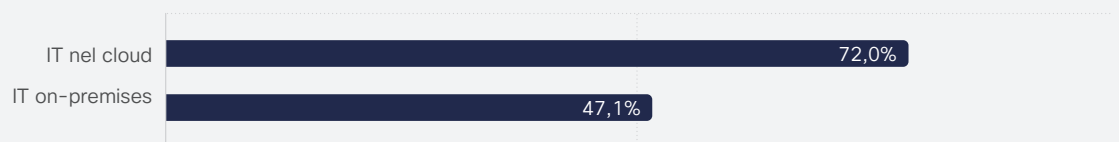
Aziende con integrazione della tecnologia efficace

Fonte: Studio Cisco sui risultati della sicurezza

Figura 7 – Effetto degli approcci di integrazione comuni sul livello di integrazione delle tecnologie di sicurezza

Cloud, con possibilità di integrazione

Abbiamo tutti sentito parlare di aziende ancora indecise se implementare (o espandere) le attività di integrazione delle tecnologie di sicurezza in ambienti cloud o on-premises. Se ti riconosci in questo ritratto, ecco alcune considerazioni utili per la valutazione. La buona notizia è che molti degli intervistati hanno dichiarato buoni risultati sia in ambienti on-premises sia in ambienti cloud. Ciò premesso, sembra che sia molto più facile ottenere un'efficace integrazione tecnologica nel cloud.



Aziende con integrazione della tecnologia efficace

Fonte: Studio Cisco sui risultati della sicurezza

Figura 8 – Effetto degli ambienti cloud o on-premises sul livello di integrazione delle tecnologie di sicurezza

L'integrazione favorisce l'automazione?

Come abbiamo visto all'inizio di questa sezione, l'automazione non è tra i motivi più comuni che spingono verso l'integrazione tecnologica. Ma per il 44% delle aziende rappresenta comunque un incentivo. Motivazioni a parte, ci sono prove che le tecnologie integrate favoriscano realmente una migliore automazione dei processi di sicurezza? Sì, come confermato nella figura 9.

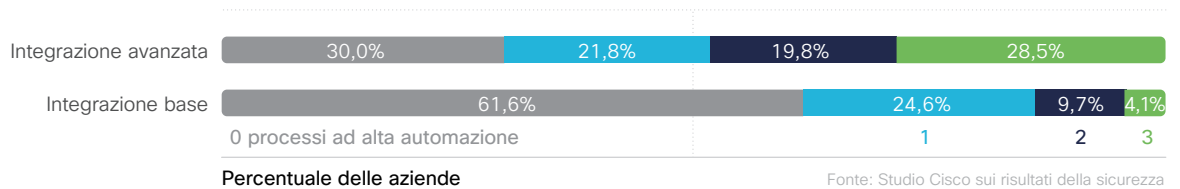


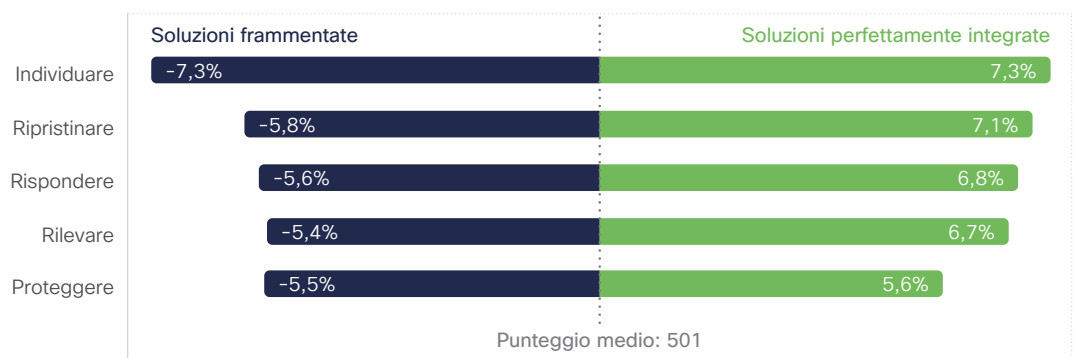
Figura 9 – Effetto dell'integrazione della tecnologia sull'automazione dei processi di sicurezza

Le due barre orizzontali della figura 9 rappresentano le aziende in base al livello di integrazione delle tecnologie di sicurezza (avanzata o base). I segmenti colorati equivalgono al numero di attività di sicurezza principali (monitoraggio degli eventi, analisi e risposta agli incidenti) supportate dall'automazione avanzata. La percentuale di aziende senza processi automatizzati è più del doppio tra le aziende con integrazione base. **Al contrario, le aziende con tecnologie di sicurezza perfettamente integrate hanno una probabilità sette volte maggiore di raggiungere elevati livelli di automazione in tutti e tre i processi (4,1% contro il 28,5%).** Sembra davvero una motivazione convincente.

Quali funzioni devono essere integrate?

Successivamente, abbiamo chiesto agli intervistati di valutare il livello di integrazione delle tecnologie a supporto delle cinque funzioni principali individuate dal NIST Cybersecurity Framework (CSF). Abbiamo sottoposto agli intervistati una scala di valutazione che andava da tecnologie molto frammentate (isolate e non comunicanti) a tecnologie molto integrate (coordinate in unità funzionali). Quindi abbiamo creato un modello che rappresentasse l'effetto del punteggio complessivo dei risultati della sicurezza per ciascuna azienda.

La figura 10 mostra una certa parità per tutte e cinque le funzioni. **Cercare di armonizzare e integrare una qualsiasi delle aree funzionali individuate dal NIST CSF aumenta l'efficacia del programma di sicurezza dall'11% al 15% circa.** La risposta alla domanda posta nel titolo è quindi "tutte quante". Ma se ti stai chiedendo da dove iniziare, sicuramente la funzione "individuare" è quella che comporta i maggiori vantaggi.



Differenza in percentuale dal punteggio medio dei risultati della sicurezza Fonte: Studio Cisco sui risultati della sicurezza

Figura 10 – Effetto dell'integrazione delle funzioni NIST CSF sul punteggio complessivo della sicurezza

Non possiamo fare a meno di vedere una correlazione tra questo risultato e ciò che abbiamo appreso nella sezione precedente sul monitoraggio, l'auditing e la collaborazione come fattori trainanti per integrare la tecnologia. Insieme, questi due risultati sembrano sottolineare quanto sia importante avere una buona visibilità in tutta l'azienda. È logico pensare che un approccio frammentato, per dirla con il CSF, allo sviluppo di un piano di gestione dei rischi di cybersecurity che coinvolga sistemi, persone, risorse, dati e funzionalità non può dare risultati soddisfacenti. Questo tema sarà ulteriormente confermato nella sezione successiva, dove parleremo di rilevamento delle minacce e risposta agli incidenti.

Qualche osservazione su integrazione, individuazione e informazioni

Oltre al grafico che abbiamo appena discusso, tutti i dati di questo studio riportano in modo coerente alla relazione cruciale tra integrazione, individuazione e informazioni. Se non sappiamo individuare una risorsa o una minaccia, non possiamo neanche sapere che è presente e non ci daremo da fare per istituire una difesa puntuale finché non sarà troppo tardi.

La figura 11 illustra bene questo concetto. Per ogni azienda, abbiamo confrontato il livello di integrazione della funzione "Individuare" del NIST CSF con la capacità di rilevare le minacce in modo accurato e tempestivo. **Se i sistemi per individuare le risorse critiche sono molto integrati, le aziende possono vantare funzionalità di rilevamento delle minacce molto più efficaci (+41%).** Quindi, in un certo senso, combattere la frammentazione e combattere gli hacker vanno di pari passo.

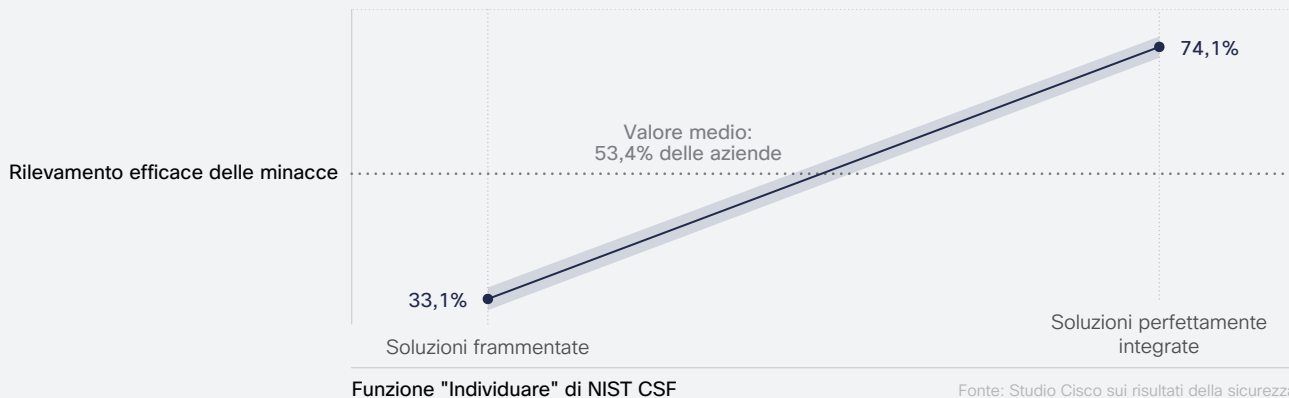



Figura 11 – Effetto dell'integrazione della funzione Individuare (NIST CSF) sul rilevamento delle minacce

Nelle aziende con sistemi molto integrati, le funzionalità di rilevamento delle minacce sono più efficaci di

+41%



"L'automazione consente ai nostri tecnici di reagire tempestivamente alle nuove minacce. Ora possiamo concentrarci sui concetti di sicurezza, anziché dover aggiornare continuamente le regole e monitorare la rete senza sosta. Cisco indaga in profondità ed estrae le informazioni che ci servono per proteggere e gestire la nostra infrastruttura nel modo migliore. Possiamo contare ora su una sinergia perfetta tra intelligenza umana e intelligenza della macchina."

Steve Erzberger, CTO, Frankfurter Bankgesellschaft (Svizzera) AG

[Leggi di più](#)



Sviluppare funzionalità di rilevamento delle minacce e di risposta agli incidenti

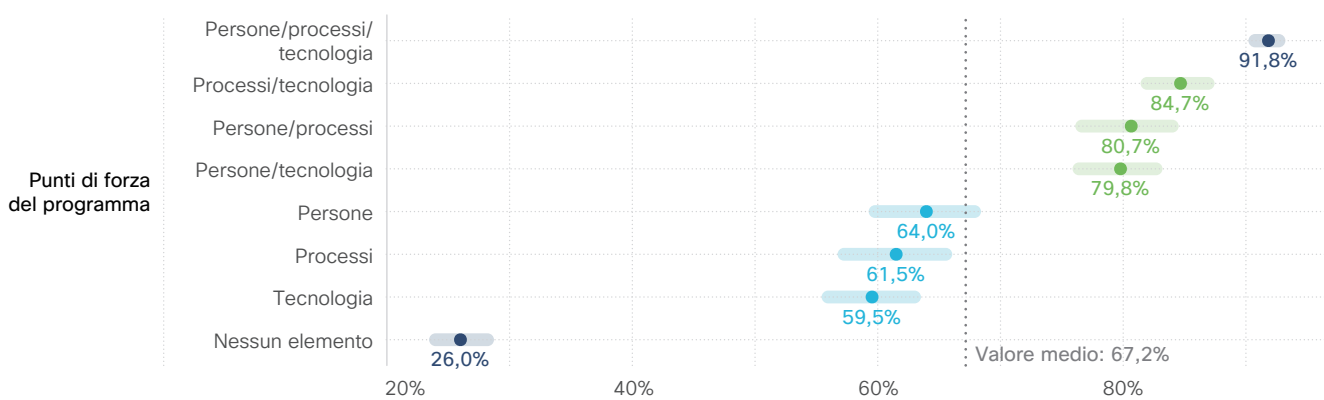
In questa sezione esaminiamo due procedure di sicurezza distinte, entrambe confluite nei "magnifici cinque". Ma dal momento che il rilevamento delle minacce e la risposta agli incidenti (IR) spesso condividono persone, processi e tecnologie sotto il termine più ampio di gestione operativa della sicurezza (SecOps), abbiamo posto una serie di domande comuni, che ha senso analizzare nella stessa sezione di questo studio.

Quasi tutte le aziende (circa il 92%) con persone competenti e processi e tecnologie efficaci possono vantare funzionalità avanzate di rilevamento delle minacce e risposta agli incidenti.

A chi dare priorità tra persone, processi e tecnologia?

Iniziamo il nostro esame proprio parlando di persone, processi e tecnologia, una triade nota anche con l'acronimo PPT. Tutti e tre questi elementi confluiscono spesso nella descrizione delle funzioni di sicurezza, in particolare nel rilevamento delle minacce e nella risposta agli incidenti. Ma in questa triade c'è un fattore predominante? È chiaro a cosa ci riferiamo, passiamo quindi subito all'analisi.

Esaminando la figura 12 dal basso, notiamo che solo un quarto circa delle aziende i cui programmi non possono vantare persone competenti e processi o tecnologia sufficientemente efficaci dichiara di essere soddisfatto delle proprie SecOps. Rafforzare un elemento qualsiasi di questa triade può aumentare la percentuale fino al 60-64%. Le persone competenti sembrano concedere un lieve vantaggio, ma essendoci qualche sovrapposizione, non dobbiamo enfatizzare troppo questo aspetto. È importante invece osservare che tutti e tre gli elementi offrono un buon punto di partenza per migliorare le funzionalità di rilevamento e risposta.



Aziende con funzionalità efficaci di rilevamento e risposta

Fonte: Studio Cisco sui risultati della sicurezza

Figura 12 – Effetto di un rafforzamento di persone, processi e tecnologia sulle funzionalità di rilevamento e risposta

Continuando a esaminare la figura 12, notiamo come il rafforzamento di due aspetti aumenta l'efficacia dei programmi SecOps sopra la media e migliora le funzionalità di circa il 15-20% rispetto ai programmi che hanno puntato su uno solo dei tre elementi. Ancora una volta, non è tanto importante rafforzare un singolo elemento, ma il fatto che ne siano stati rafforzati due. È rassicurante sapere di avere una certa libertà di manovra e di poter personalizzare la roadmap delle SecOps.

Ed eccoci infine ai programmi migliori, rappresentati nella figura 12, in cui l'intera tripletta delle SecOps è rafforzata. **Quasi tutte le aziende (circa il 92%) con persone competenti e processi e tecnologie efficaci possono vantare funzionalità avanzate di rilevamento delle minacce e risposta agli incidenti.** Le prestazioni sono in questo caso maggiori di 3,5 volte rispetto ai programmi di sicurezza che non hanno puntato su nessuno di questi elementi. Quindi, inizia da dove pensi di poter ottenere il massimo, ma non fermarti finché non raggiungi l'apice della triade.

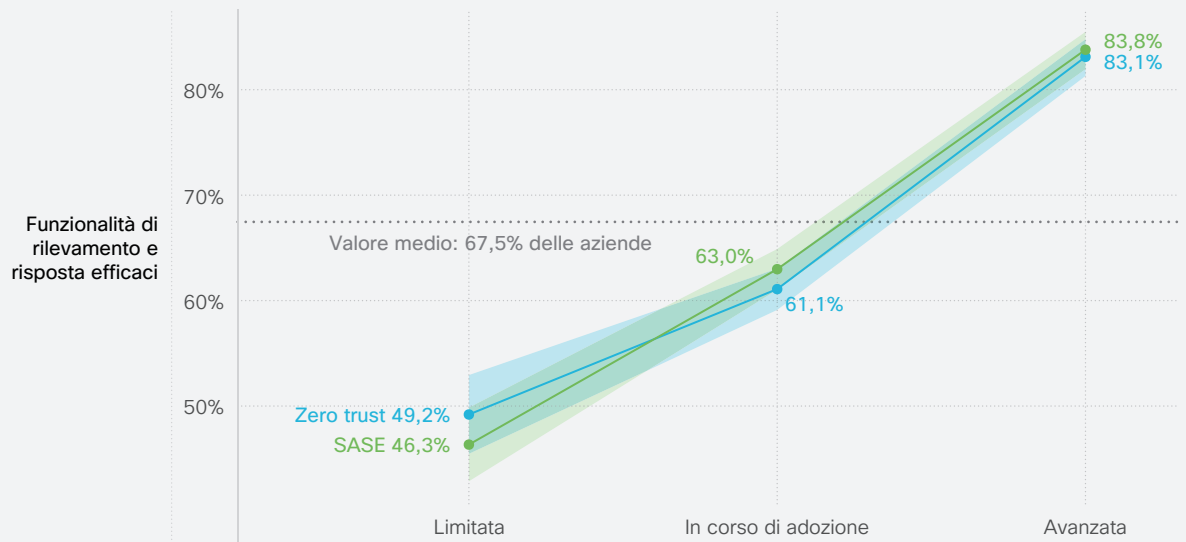
Le aziende con persone competenti e processi e tecnologia efficaci vantano funzionalità di rilevamento e risposta migliori di

3,5X

rispetto a coloro che sono carenti in tutte e tre le aree

Gli approcci Zero Trust e SASE migliorano le SecOps?

Sappiamo che descrittori astratti come "tecnologia efficace" rendono difficile ricavare conclusioni concrete dai risultati esaminati. Ecco perché abbiamo ideato un paio di domande di follow-up su architetture specifiche. Abbiamo chiesto agli intervistati se usano soluzioni Zero Trust e Secure Access Service Edge (SASE) per comprendere meglio se influiscono sul rilevamento delle minacce e la risposta agli incidenti, e quindi sui risultati dei programmi di sicurezza.



Adozione dell'architettura

Fonte: Studio Cisco sui risultati della sicurezza

Figura 13 - Effetto delle architetture Zero Trust e SASE sulle funzionalità di rilevamento e risposta

Le aziende con implementazioni avanzate di soluzioni Zero Trust o SASE hanno circa il 35% di probabilità in più di dichiarare SecOps efficaci rispetto alle aziende che hanno appena iniziato a implementarle. Questi

risultati confermano i risultati che abbiamo condiviso in precedenza sui numerosi vantaggi che le architetture moderne possono offrire ai programmi di cybersecurity.

È vero che team più grandi risolvono più problemi?

Abbiamo imparato come rafforzare il fattore umano sia importante per migliorare le funzionalità di rilevamento delle minacce e risposta agli incidenti. Ma è meglio concentrarsi sull'aspetto quantitativo, ovvero sul numero di persone, o sull'aspetto qualitativo, ossia sulle competenze? È chiaro che sono importanti entrambi gli aspetti, ma la domanda rimane: abbiamo prove che la quantità pesi più della qualità, o viceversa, quando si tratta di sviluppare team di SecOps efficienti?

Per rispondere a questa domanda, abbiamo innanzitutto calcolato la percentuale di persone coinvolte nelle SecOps sul totale dei dipendenti impiegati. Abbiamo quindi confrontato tale valore con l'efficacia dichiarata delle funzionalità di rilevamento e risposta. Nella figura 14 sono riportati i risultati di questi calcoli e, anche se non chiarisce del tutto il dilemma tra quantità e qualità, offre alcuni spunti di riflessione interessanti.

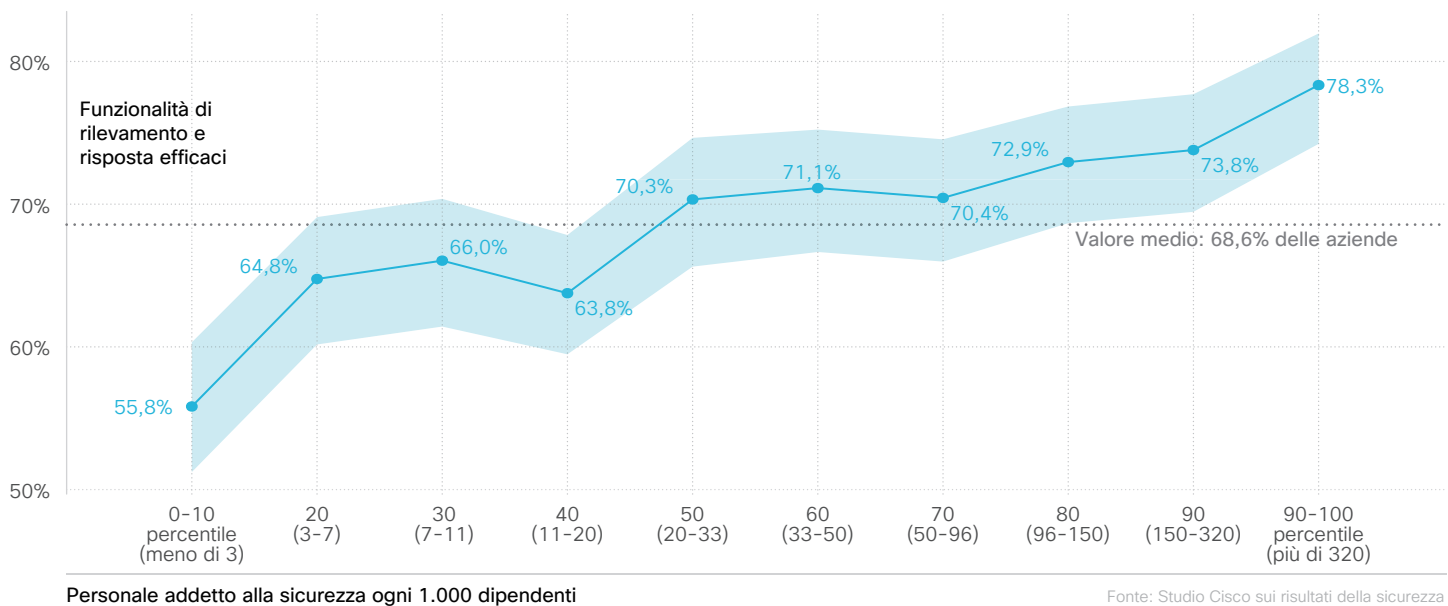


Figura 14 – Effetto della percentuale di personale addetto alla sicurezza sulle funzionalità di rilevamento e risposta

La prima riflessione che possiamo fare è che la percentuale di personale che si dedica alla sicurezza è correlata a migliori funzionalità di rilevamento e risposta. La probabilità di avere funzionalità efficaci è superiore di oltre il 20% nelle aziende con la percentuale di addetti alla sicurezza più alta. Tuttavia, hai notato come la linea tratteggiata che rappresenta il valore medio attraversi la maggior parte dell'area sfumata in azzurro? Ciò significa sostanzialmente che anche le aziende che non sono agli estremi nel grafico, ovvero la maggior parte, hanno la stessa probabilità di avere programmi SecOps efficaci.

Come dobbiamo interpretare questo dato? Possiamo affermare con certezza che le aziende con team di sicurezza grandi hanno più probabilità di avere funzionalità di rilevamento e risposta efficaci rispetto alle aziende con team esigui. Ma il numero di persone di un team non basta da solo ad eliminare tutti i problemi e garantire la riuscita di un programma di sicurezza. Inoltre, la differenza tra team grandi ed esigui non spiega l'aumento di prestazioni associato al fattore umano (persone competenti) di cui abbiamo discusso nella sezione precedente. **Dobbiamo quindi concludere che la qualità ha lo stesso peso, se non superiore, della quantità quando si tratta di creare team efficienti per il rilevamento delle minacce e la risposta agli incidenti.**

Il problema dei team di sicurezza continua a essere la grave penuria di personale.

Con le risorse ridotte e le minacce in aumento, molti professionisti della cybersecurity sono sottoposti a un lavoro intenso e rischiano l'esaurimento nervoso. Quali misure proattive possiamo adottare per favorire il loro benessere? [In questo eBook](#) abbiamo chiesto ai responsabili e professionisti del settore di condividere opinioni ed esperienze sulla gestione del benessere mentale.

Team SecOps: interno, esterno o misto?

Abbiamo visto come l'efficienza di un team SecOps non riguarda meramente il numero di persone, ma anche le loro competenze. Ci chiediamo ora, a parità di condizioni, per i team di rilevamento delle minacce e risposta agli incidenti, è meglio esternalizzare, internalizzare o condividere le responsabilità? Vediamo come i dati rispondono a questa domanda, ma attenzione, le conclusioni potrebbero non essere così nette.

Abbiamo chiesto agli intervistati quale fosse il loro modello di team e abbiamo confrontato le risposte con la loro valutazione delle funzionalità di rilevamento e risposta. **Come mostrato nella figura 15, le aziende con team prevalentemente interni o esterni hanno più probabilità (rispettivamente del 20% e del 30%) di avere programmi SecOps efficaci rispetto alle aziende con un modello misto.** Dato che il modello misto è quello adottato nella maggior parte delle aziende, abbiamo pensato valesse la pena osservare la questione da un'angolazione diversa, prima di condannarle tutte all'insuccesso solo perché l'indagine (sembra) giungere a questa conclusione.

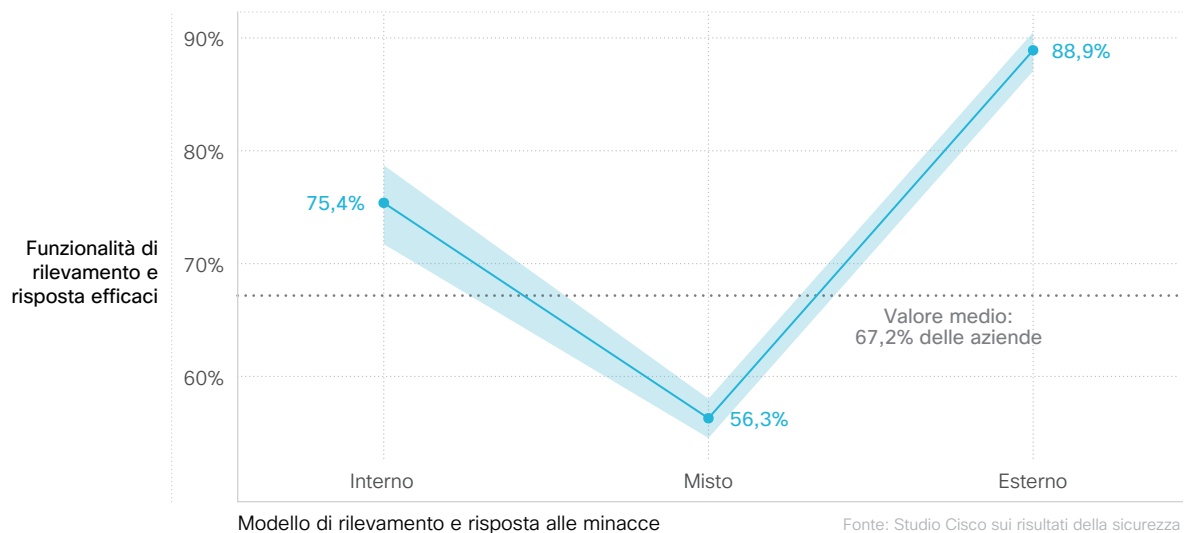


Figura 15 - Effetto dei modelli di team sull'efficacia percepita delle funzionalità di rilevamento e risposta

Le aziende con team prevalentemente interni o esterni hanno il

20 - 30%

in più di probabilità di avere programmi di sicurezza più efficaci di coloro che hanno un modello misto

Oltre a chiedere agli intervistati di valutare l'efficacia percepita delle funzionalità di rilevamento e risposta, abbiamo cercato di ottenere metriche più oggettive per il confronto. Ad esempio, abbiamo calcolato il tempo medio di risposta (MTTR), ovvero il tempo medio necessario per correggere o mitigare gli effetti di un incidente di sicurezza. Nella nostra analisi precedente, queste metriche tendono a concordare con le valutazioni soggettive. Nel nostro caso invece le due prospettive si contraddicono, come chiarisce la figura 16.



Figura 16 – Effetto dei modelli di team sul tempo medio di risposta agli incidenti di sicurezza²

Se osserviamo la figura 16, sembrerebbe che le aziende con team interni di rilevamento e risposta godano di un MTTR inferiore alla metà rispetto alle aziende con team esterni (circa 6 giorni contro 13 giorni). Le aziende con modelli ibridi si posizionano all'incirca a metà (circa 8 giorni), con tempi medi di risposta che non sono così brevi come quelli dei team interni, ma sicuramente più brevi di quelli dei team esterni.

È ovvio che ciò pone qualche interrogativo. Qual è l'approccio corretto, la prospettiva o la metrica? E, ancora più importante, su quale basarsi per prendere decisioni efficaci? Ammettiamo di esitare in questo caso tra "entrambi" e "nessuno dei due", ma la nostra indecisione non fa che rispecchiare i dati, che in questo ambito sono discordanti.

Naturalmente, le azioni correttive sono attività complesse che coinvolgono molti aspetti e non sempre è possibile eseguirle in autonomia. Potrebbe essere necessario ad esempio aspettare che il fornitore rilasci una patch o la correzione di un bug per risolvere completamente una vulnerabilità. La patch poi deve essere testata nell'ambiente in uso prima di essere implementata in produzione. Le parti coinvolte sono molte.

A dire il vero, è difficile qui interpretare i dati con certezza. Forse cercare di raccogliere metriche tramite un sondaggio è fuorviante. Forse i criteri per valutare l'MTTR e le

funzionalità sono abbastanza diversi da poter avere un efficace programma di rilevamento e risposta in termini generali, ma percentuali di intervento e correzione piuttosto basse. Forse i programmi sono più lenti perché svolgono azioni più approfondite. O forse è coordinarsi con il team esterno che fa perdere tempo. Forse ci si sente protetti solo perché si paga un team di esperti. O forse ancora stiamo solo vedendo la versione SecOps dell'effetto Dunning-Kruger. Probabilmente tutto vero e molto di più. Consigliamo quindi di usare questa sezione per avviare discussioni proficue e non per prendere decisioni.

² In questo grafico abbiamo usato la media geometrica, più rappresentativa di un valore "tipico". In genere il MTTR riportato era inferiore a 2-3 settimane, in alcuni rari casi gli intervistati hanno dichiarato di impiegare mesi, se non addirittura anni. L'uso della media geometrica riesce a rappresentare meglio i valori "tipici" senza la distorsione dei valori estremi.

È intelligente usare l'intelligence?

L'effetto Dunning-Kruger, che abbiamo menzionato prima, sembra essere la risposta perfetta a questa domanda. Abbiamo chiesto agli intervistati se usano l'intelligence sulle minacce informatiche nei loro programmi di SecOps. Nella maggior parte delle aziende (85%) l'intelligence viene in qualche modo usata, ma meno di un terzo (31%) delle aziende afferma di usarla in modo intensivo. Le funzionalità di rilevamento e risposta sono più efficienti, più efficaci e più veloci se si usa l'intelligence sulle minacce? Esaminiamo la figura 17.

È curioso notare come la maggior parte delle aziende che non usa affatto l'intelligence sulle minacce pensa di avere funzionalità efficaci. Ecco che torna alla memoria il vecchio adagio "beata ignoranza", anche perché basta immergersi appena nelle benefiche acque dell'intelligence per far dissolvere tale percezione e farne scendere la percentuale dall'84% al 46%. **Le aziende che fanno un uso intensivo dell'intelligence sulle minacce hanno quasi il doppio delle probabilità di avere funzionalità di rilevamento e risposta efficaci rispetto a quelle che la usano meno. E in un esempio in cui le valutazioni e le metriche delle funzionalità concordano, le aziende che usano maggiormente l'intelligence hanno anche tempi medi di risposta che sono circa la metà.**

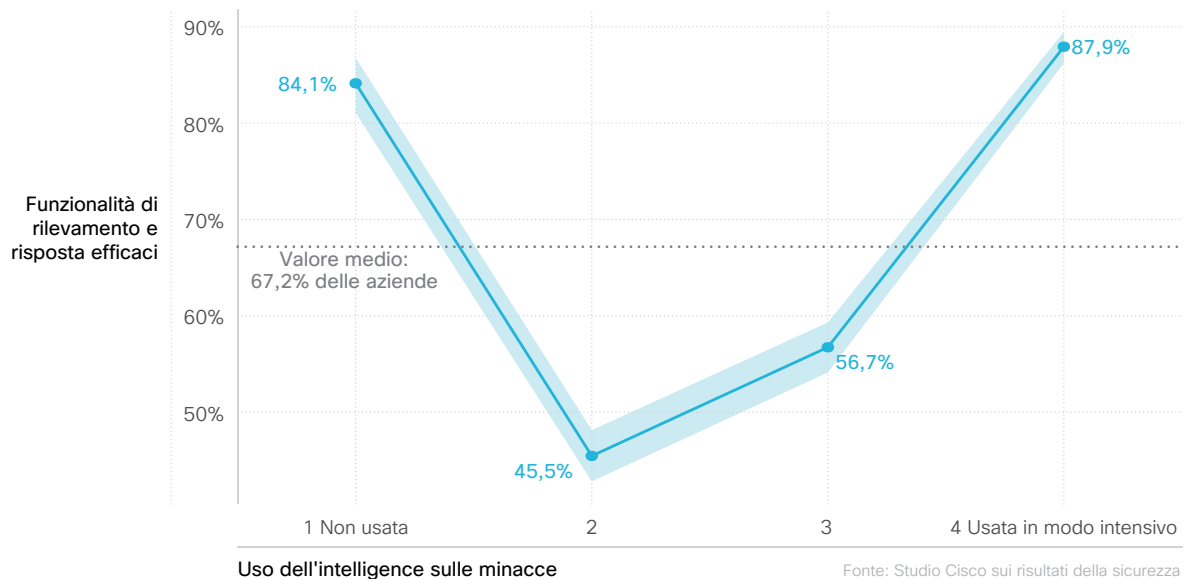


Figura 17 - Effetto dell'uso dell'intelligence sulle funzionalità di rilevamento e risposta

Una volta lo psicologo e autore di best-seller Daniel Kahneman ha detto: "Siamo ciechi rispetto alla nostra cecità. Abbiamo ben poca idea di quanto poco sappiamo." Proprio quello suggerito dalla figura 17, ossia che appena iniziano a conoscere un po' le

minacce informatiche, le aziende si rendono subito conto di quanto poco sappiano. Un uso intensivo dell'intelligence ricostruisce la fiducia nell'efficacia della proprie funzionalità, con l'eccezione che ora non è più una fiducia cieca.

Le aziende che fanno ampio uso dell'intelligence sulle minacce hanno circa

2X

in più di probabilità di avere funzionalità di rilevamento e risposta efficaci

L'automazione può sostituire le persone?

La domanda del titolo potrebbe sembrare una domanda retorica. Ma non arriviamo a conclusioni affrettate. E corriamo il rischio di scatenare l'ira di tutta la community dei responsabili della sicurezza suggerendo che l'automazione può, di fatto, sostituire le persone. Non essere impulsivo. Prima di gettare nel cestino questo documento e aggiungerci alla lista dei contatti bloccati, respira profondamente e continua a leggere.

La figura 18 include elementi già esaminati in altri grafici, team di sicurezza e automazione. Le due linee raffigurano due diversi tipi di programmi di sicurezza. La linea blu scuro rappresenta le aziende che NON hanno risorse umane efficienti e competenti, la linea azzurra rappresenta le aziende che possono vantare questo lusso. In entrambi gli scenari, muovendoci da sinistra verso destra osserviamo l'effetto benefico di un aumento dell'automazione sulle funzionalità di rilevamento e risposta.

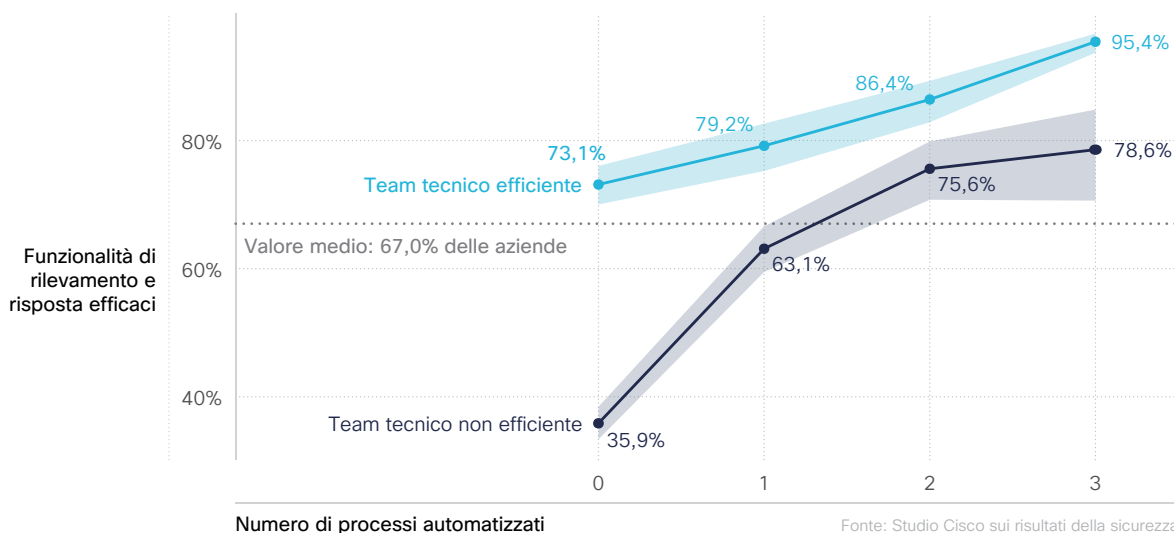


Figura 18 – Effetto dei team di sicurezza e dell'automazione sulle funzionalità di rilevamento e risposta

Cominciamo dalla linea arancione. Solo un terzo circa delle aziende che non hanno validi team della sicurezza e non usano processi automatizzati dichiara di avere funzionalità di rilevamento e risposta efficaci. Il risultato cambia notevolmente quando una delle procedure oggetto dell'indagine (monitoraggio delle minacce, analisi degli eventi e risposta agli incidenti) è automatizzata. Automatizzare due processi aumenta ulteriormente il valore, automatizzarli tutti e tre raddoppia le prestazioni rispetto ai team con personale non esperto. **Oltre i tre quarti dei programmi di sicurezza che non possono contare su personale competente sono ancora in grado di avere funzionalità efficaci se i livelli di automazione sono elevati.**

Immaginiamo ora una linea che congiunge il punto più a destra della linea blu scuro al punto iniziale della linea azzurra. Cosa suggerisce? **Un programma di sicurezza con un team meno esperto ma livelli di automazione avanzati genera risultati simili a un programma con un team efficiente e scarsa automazione.** Oppure, in altre parole, un'automazione efficace può sostituire un team efficiente. Vedi? Non ti mentivamo.

Ma la lezione più importante che si ricava dalla figura 18 non è certo come risolvere il dilemma uomo-macchina. Seguire la linea blu in tutti i livelli successivi di automazione offre un motivo molto convincente per perseguire entrambi gli obiettivi. I programmi di sicurezza che riescono ad avere un team competente e processi automatizzati per il rilevamento delle minacce e la risposta agli incidenti garantiscono l'efficacia della gestione operativa della sicurezza (oltre il 95%). Non si tratta quindi di usare l'automazione per sostituire team competenti e qualificati, ma di usarla per aumentarne il potenziale e permettere loro di dedicarsi alle attività prioritarie per il business.

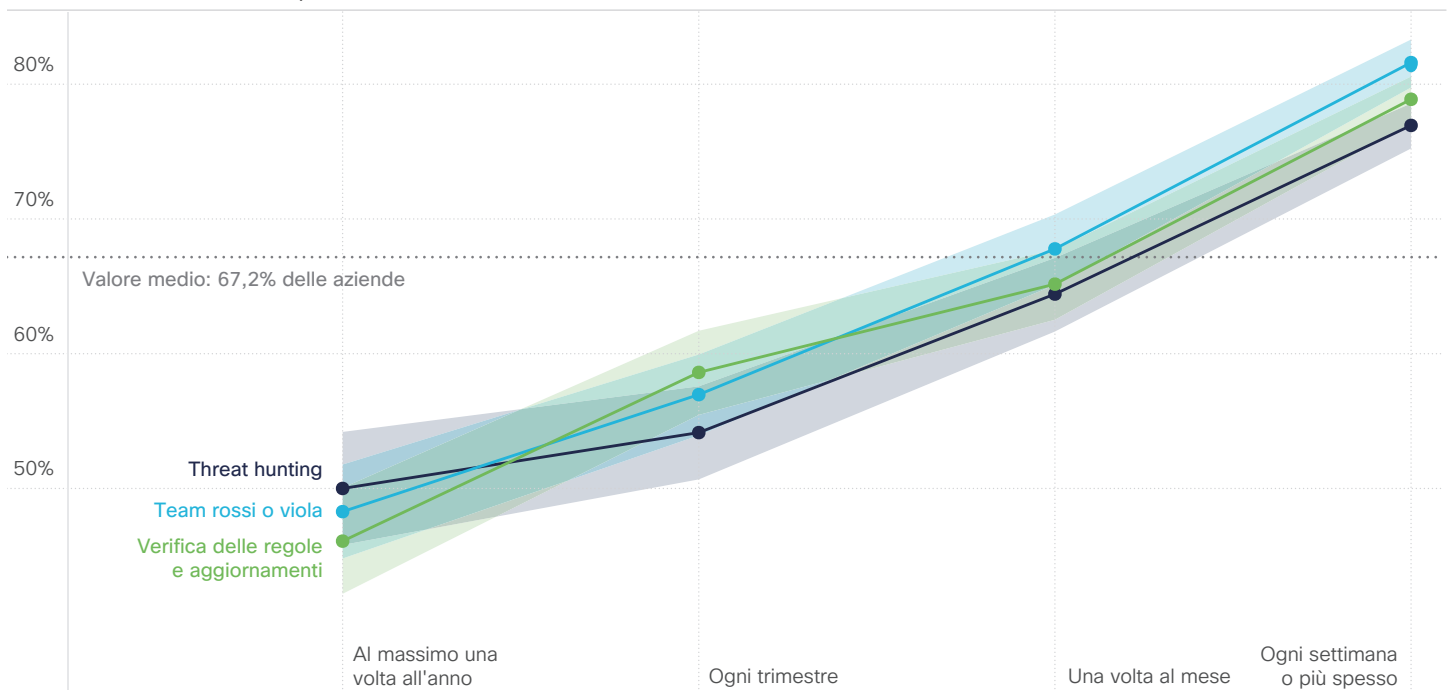
Con quale frequenza dovremmo modificare i programmi o fare threat hunting?

Sono molte le attività che si potrebbero citare e che, svolte con regolarità, migliorerebbero i programmi di rilevamento e risposta. In un sondaggio informale su questo argomento, ne avevamo individuate soprattutto tre:

- Verifica e aggiornamento delle regole di rilevamento e degli scenari d'uso
- Ricerca proattiva dei segnali di attività malevole
- Esercitazioni di gruppo con team rossi e/o viola

Abbiamo chiesto agli intervistati con quale frequenza vengono condotte queste attività e abbiamo confrontato le risposte con l'efficacia percepita delle funzionalità di rilevamento e risposta. I risultati riportati nella figura 19 non potrebbero essere più chiari.

Funzionalità di rilevamento e risposta efficaci



Fonte: Studio Cisco sui risultati della sicurezza


Fonte: Studio Cisco sui risultati della sicurezza

Figura 19 – Effetto della frequenza delle attività sulle funzionalità di rilevamento e risposta

Modifica delle regole, team rossi/viola e threat hunting seguono tutte una medesima traiettoria. Più vengono svolte, più i programmi di sicurezza se ne avvantaggiano. **Le aziende che le conducono almeno una volta alla settimana registrano un aumento delle prestazioni di circa il 30% rispetto a quelle che le eseguono annualmente o con una cadenza ancora maggiore.** Quindi, quanto spesso dovrebbero essere svolte? La risposta è semplice, "più spesso è, meglio è".

Le aziende che conducono queste attività su base settimanale registrano un aumento delle prestazioni del

30%
circa



"La sicurezza cambia continuamente e dobbiamo rimanere informati sulle varie tendenze. [In precedenza], abbiamo perso molto tempo a risolvere i problemi di sicurezza e gli incidenti. Ora che abbiamo semplificato il processo e ridotto i tempi per le indagini, possiamo seguire le nuove tendenze e integrare nuove soluzioni per dotare la nostra rete didattica di un'infrastruttura più sicura."

Bahruz Ibrahimov, Senior Information Security Engineer, AzEduNet

[Leggi di più](#)

Disaster recovery tempestivo e resilienza

È interessante notare come gli aspetti considerati principali nella cybersecurity attraversino una sorta di corsi e ricorsi storici. Dopo alcuni anni passati a occuparsi di violazioni dei dati e spionaggio informatico, i riflettori sono di nuovo puntati su continuità operativa e disaster recovery (BCDR, Business Continuity and Disaster Recovery). E non a torto. Il ransomware dilagante, le interruzioni dei principali provider di servizi hosting e molto altro hanno imposto un ripensamento delle strategie per assicurare la resilienza di fronte a minacce incessanti.

Lo studio sui risultati della sicurezza del 2021 ha classificato il disaster recovery come il quarto fattore più importante che contribuisce a creare programmi di cybersecurity efficaci. Le procedure di disaster recovery hanno mostrato correlazioni significative con tutti gli 11 risultati tranne uno (cultura della sicurezza). Tenendo presente tutto questo, esaminiamo ora le strategie con cui è possibile aumentare l'efficacia di questa procedura e diventare più resilienti.

Il ransomware dilagante, le interruzioni dei principali provider di servizi hosting e molto altro hanno imposto un ripensamento delle strategie per assicurare la resilienza di fronte a minacce incessanti.



Quale responsabilità hanno i ruoli direttivi nella supervisione delle misure di disaster recovery?

Eravamo curiosi di sapere chi avesse l'ultima parola nelle misure di disaster recovery. È emerso che la responsabilità finale riguarda il CIO, il CISO e altre figure direttive che non fanno parte del reparto IT. Circa un quarto delle procedure BCDR è assegnato a questi ruoli. La responsabilità a livello di consiglio direttivo è meno visibile, ma pur sempre presente nel 18% delle aziende intervistate.

Confrontare queste risposte con la valutazione degli intervistati in merito a continuità operativa e disaster recovery ha confermato che la questione della supervisione non era una mera curiosità. **Come si evince dalla figura 20, le aziende in cui i processi BCDR sono supervisionati a livello di consiglio direttivo hanno maggiori probabilità di avere programmi efficaci (11% sopra la media).** Quando le funzioni di continuità operativa e disaster recovery sono assegnate al CIO, si registrano le percentuali più basse, notevolmente al di sotto della media.

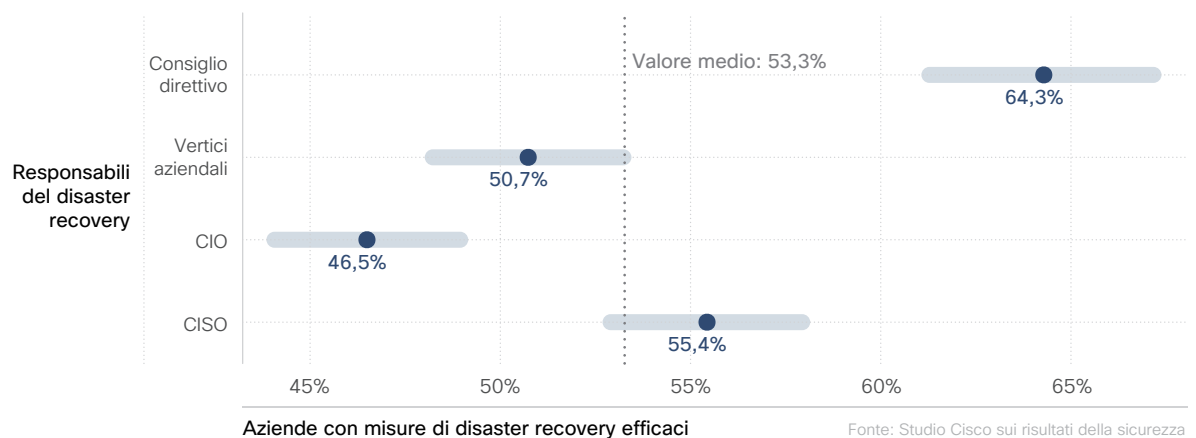


Figura 20 – Effetto della supervisione a livello direttivo sulle misure di disaster recovery

Potremmo spiegare in molti modi ragionevoli i risultati della figura 20. Possiamo supporre ad esempio che le aziende che hanno indicato come supervisore il consiglio direttivo siano in fondo anche quelle che più si preoccupano di rischi operativi e resilienza. Tali preoccupazioni si traducono presumibilmente in una vigilanza

più rigorosa, un supporto più efficace e un maggiore investimento. Quindi, se la tua azienda fatica a migliorare le misure di disaster recovery, potrebbe essere logico ribaltare la prospettiva e andare a verificare chi ne abbia la responsabilità effettiva.

E le attività da svolgere quotidianamente per assicurare il disaster recovery?

Oltre alla supervisione finale, abbiamo anche chiesto a chi è affidato l'incarico di tradurre in pratica gli aspetti più strategici del disaster recovery. **Le operazioni che rientrano nei compiti dei team di cybersecurity o di continuità operativa tendono a registrare le prestazioni migliori.** I programmi gestiti dall'IT in genere hanno prestazioni inferiori. È interessante notare che la visibilità a livello di consiglio direttivo sembra agire come elemento trainante di tutti gli altri. Le percentuali di successo si equivalgono statisticamente a prescindere da dove ricadono le responsabilità quotidiane fintanto che la supervisione finale spetta al consiglio direttivo.

L'ambito del disaster recovery è importante?

Probabilmente non ti stupirà sapere che gli incidenti avvengono quando meno ce li aspettiamo. Gli incidenti di cybersecurity non fanno eccezione, ecco perché anche in questo caso il buon senso suggerisce di essere sempre pronti a ogni evenienza. Più facile a dirsi che a farsi, ovviamente.

A conferma di come non sia facile, meno di tre aziende su dieci afferma che le misure di disaster recovery coprono almeno l'80% dei sistemi critici. La metà delle aziende rientra tra il 50% e il 79% e poco meno del 20% ammette tassi di copertura inferiori. A prima vista non sembra male. Dopotutto, i sistemi critici sono coperti nella maggior parte delle aziende. Purtroppo, questo fatto ignora la fastidiosa tendenza degli incidenti di colpire in aree inaspettate. I nostri dati indicano che ciò avviene più spesso di quanto vorremmo ammettere.

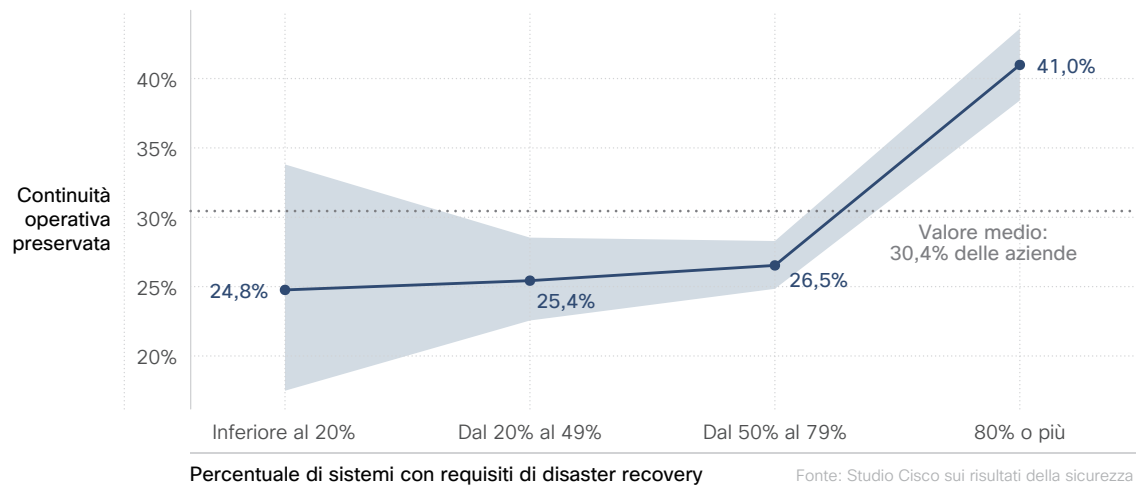


Figura 21 – Effetto della copertura delle risorse critiche sulle misure di disaster recovery

Nella figura 21 viene misurato un nuovo risultato aggiunto per questo studio, ossia la capacità dell'azienda di mantenere la continuità operativa nonostante eventi catastrofici. Questo è anche uno dei tre risultati con cui gli intervistati dichiarano di avere le maggiori difficoltà. È quindi ancora più importante trovare metodi efficaci per aumentare le probabilità di riuscita.

La figura 21 ci offre un'indicazione importante su come gestire la continuità operativa.

Non sono percepibili miglioramenti nella probabilità di ottenere questo risultato finché le funzionalità BCDR non riguardano almeno l'80% dei sistemi critici.

Ciò dipende sicuramente dalla strana propensione delle catastrofi a verificarsi quando meno ce lo aspettiamo. Non possiamo quindi aspettarci che gli investimenti in continuità operativa e disaster recovery si traducano in risultati immediati. Forse non è una buona notizia, ma d'altra parte un evento catastrofico non è mai una buona notizia.

La pratica migliora le misure di disaster recovery?

Rispondiamo a questa domanda andando subito al punto. No, purtroppo no. Certo avere un po' di pratica è meglio che non averla affatto. Ma, quanto meglio? Cerchiamo di capirlo insieme.

Un noto adagio militare dice, "Nessun piano sopravvive al primo contatto con il nemico". E si adatta bene anche al campo di battaglia della cybersecurity. Abbiamo diversi modi per testare le funzionalità BCDR, tra cui esami dettagliati dei piani, simulazioni di situazioni di emergenza, test in tempo reale, test in parallelo e test di produzione completi. Abbiamo chiesto agli intervistati la frequenza con cui le loro aziende si impegnano in tali esercitazioni e abbiamo confrontato le risposte con la probabilità di mantenere la continuità operativa.

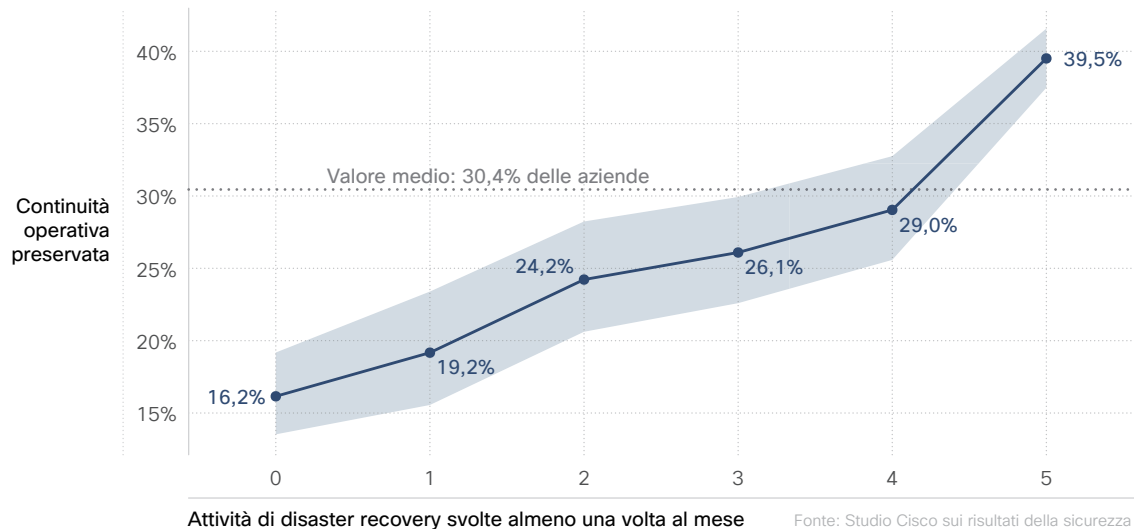


Figura 22 – Effetto delle attività di verifica sulle misure di disaster recovery

Nessuna di queste procedure è risultata superiore alle altre in termini di efficacia, ma possiamo dire che tutte contribuiscono insieme a migliorare la resilienza. **Le aziende che svolgevano regolarmente tutti e cinque i tipi di test sul disaster recovery avevano quasi 2,5 volte in più di probabilità di mantenere la continuità operativa rispetto alle aziende che non svolgevano nessun test.** Quali conclusioni possiamo trarne? Non lasciare la resilienza al caso e mettere alla prova le misure di continuità operativa e disaster recovery in condizioni estreme e da diverse prospettive.

Le aziende che svolgono regolarmente tutti e cinque i tipi di test di disaster recovery hanno

2,5X

in più di probabilità di continuare a lavorare anche in caso di crisi impreviste

Dovremmo scatenare il caos?

Non ci stancheremo mai di sottolineare quanto sia importante mettere alla prova il piano di disaster recovery. Pensiamo proprio all'ingegneria del caos, una tecnica che crea periodicamente e intenzionalmente eventi catastrofici per testare la capacità dei sistemi di resistere a eventi e condizioni impreviste. Potresti inserire meccanismi di ingegneria del caos nei sistemi IT e di sicurezza della tua azienda per aiutarla a essere più resiliente? Sei nel posto giusto per scoprirlo.

Abbiamo chiesto agli intervistati in che misura le loro aziende adottano meccanismi di ingegneria del caos e abbiamo scoperto che tali meccanismi erano più diffusi di quanto ci aspettassimo. Abbiamo notato anche una relazione tra questi meccanismi e l'integrazione delle tecnologie. Come si evince dalla figura 23, oltre due terzi delle aziende per le quali l'ingegneria del caos è una pratica comune dichiara di usare tecnologie altamente integrate per le procedure di ripristino. Non è chiaro se l'integrazione richieda o permetta l'ingegneria del caos. Come per molti aspetti in questo ambito, probabilmente fa entrambe le cose. Monitora questa disciplina emergente, soprattutto se sei responsabile delle funzionalità BCDR in un ambiente IT complesso e perfettamente integrato.

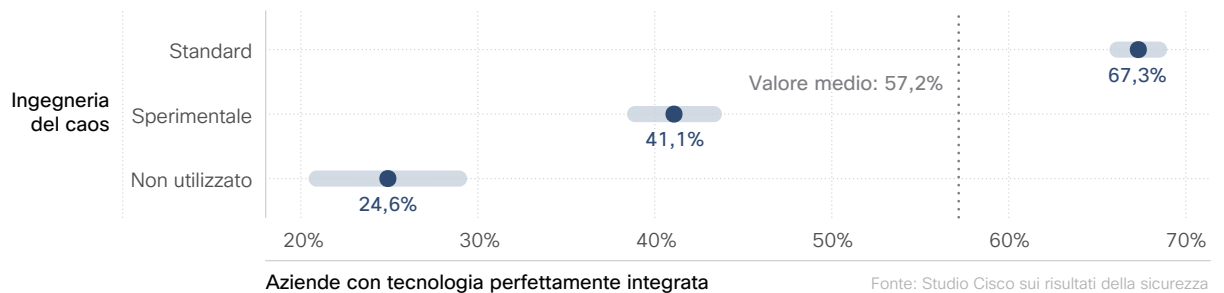


Figura 23 – Rapporto tra ingegneria del caos e livello di integrazione IT

Il confronto tra la portata dell'ingegneria del caos e il risultato della resilienza operativa nella figura 24 offre un valido motivo per mettere alla prova la resilienza della rete. **Le aziende che usano l'ingegneria del caos in procedure standard hanno il doppio delle probabilità di ottenere elevati risultati di resilienza operativa rispetto alle aziende che non la usano.** Se ciò ti sorprende, non sei certo il solo. La buona notizia è che puoi scatenare il caos prima che il caos ti sorprenda, mettendo alla prova la resilienza della rete con verifiche e simulazioni mirate.

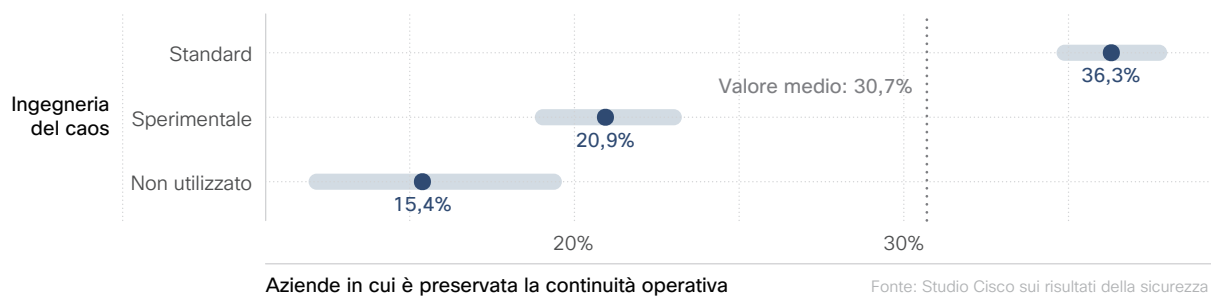


Figura 24 – Effetto dell'ingegneria del caos sulla resilienza operativa

Conclusioni e raccomandazioni

Siamo partiti dalle procedure di sicurezza più efficaci individuate in uno studio precedente, abbiamo quindi cercato di capire cosa rendesse queste procedure così efficaci con un nuovo sondaggio e infine abbiamo condiviso i risultati. È nostro augurio che dopo aver letto questo documento, tu abbia acquisito numerosi consigli pratici su come rendere più efficace il tuo programma di cybersecurity.

È sempre utile riflettere sui risultati di uno studio del genere e confrontarsi nel merito con altre persone. Ecco perché abbiamo chiesto al nostro team di consulenti CISO di valutare ciascuna delle procedure esaminate e incluso di seguito le loro valutazioni. Per ulteriori informazioni e conclusioni, puoi leggere la nostra [serie di blog Security Outcomes Study](#).

Aggiornamento proattivo della tecnologia



"Il tema del "debito di sicurezza" è centrale. Per i CISO la strada da seguire è sviluppare una strategia "Buy, Hold, Sell", ossia acquistare, gestire, vendere. Conoscere le risorse esistenti, definire un'architettura adattabile, ridurre il rischio di dipendenze e implementare un ciclo di revisione per i successivi aggiornamenti."

Richard Archdeacon, Advisory CISO, Cisco

Tecnologia perfettamente integrata



"Sappiamo che un IT moderno e perfettamente integrato contribuisce alla riuscita complessiva del programma di sicurezza. Ecco quindi alcune azioni per migliorare l'ambiente: cercare soluzioni di sicurezza basate su cloud, analizzare le opportunità di automazione, garantire che tra i criteri di acquisto compaia anche l'integrazione della tecnologia."

Helen Patton, Advisory CISO, Cisco [@CisoHelen](#)

Risposta tempestiva agli incidenti



"Un team efficiente offre concreti vantaggi nella risposta agli incidenti. È un buon punto di partenza, ma deve essere accompagnato da altre iniziative. Quando le aziende sanno coordinare persone competenti, processi efficienti e tecnologie efficaci, ottengono funzionalità di rilevamento e risposta avanzate."

Dave Lewis, Advisory CISO, Cisco [@gattaca](#)

Rilevamento accurato delle minacce



"Scegli le persone più qualificate per i tuoi team di SecOps, perché non è solo il numero di addetti che conta. Se non riesci a ottenere il livello di competenze necessario, l'automazione può aiutarti a colmare il divario creato da personale più giovane e a ottenere risultati altrettanto validi di quelli che avresti avuto con un personale più esperto."

Wendy Nather, Advisory CISO, Cisco  [@wendynather](https://twitter.com/wendynather)

Disaster recovery tempestivo



"I risultati di questo report evidenziano il valore della continuità operativa e del disaster recovery, ma queste misure non sono isolate dalle altre. La definizione delle priorità e la classificazione dei rischi delle risorse devono essere condivise con le altre funzioni di gestione del rischio. Analogamente, occorre integrare perfettamente la gestione delle risorse e delle minacce per garantire che tutti i team lavorino in modo coordinato."

Wolfgang Goerlich, Advisory CISO, Cisco  [@jwgoerlich](https://twitter.com/jwgoerlich)

Informazioni su Cisco Secure

Cisco si è affermata da tempo come leader a livello mondiale nella tecnologia alla base di Internet, sviluppando al contempo soluzioni di cybersecurity aperte e integrate. Siamo fermamente convinti che le soluzioni di sicurezza debbano essere armonizzate tra loro. In altre parole devono imparare l'una dall'altra. Devono restare in ascolto e reagire come un'unità coordinata. In questo modo, la sicurezza diventa più sistematica e acquista maggiore efficacia. Per anni i nostri clienti si sono rivolti a noi in qualità di più grande provider al mondo di servizi di networking e infrastrutture IT e più grande azienda di cybersecurity per imprese.

Cisco Secure punta a migliorare la qualità della sicurezza, più che aumentarne la quantità. Offre un approccio alla sicurezza semplice e incentrato sul cliente affinché l'implementazione, la gestione e l'uso siano facili e completamente integrati. Ispirati dalle persone e dalle loro esigenze concrete in tutto ciò che facciamo, sappiamo che i clienti vogliono ridurre ogni complessità e difficoltà e vogliono potersi fidare della soluzione di sicurezza. Ciò che conta sono i risultati. E semplificare senza essere semplicisti. La nostra piattaforma nativa del cloud rappresenta un grande traguardo.

Aiutiamo la community degli esperti di sicurezza con la certezza di essere al sicuro dalle minacce attuali e future con la piattaforma [Cisco SecureX](#). Aiutiamo il 100% delle aziende Fortune 100 a proteggere il lavoro, ovunque si svolga, con la piattaforma più ampia e integrata. Scopri di più su come semplifichiamo le esperienze, acceleriamo il successo e proteggiamo il futuro all'indirizzo cisco.com/go/secure.



Appendice – Dati demografici del campione del sondaggio

In questa appendice sono riportati i dati demografici del campione di intervistati che hanno fornito le 5.123 risposte di questo sondaggio. Ci auguriamo che ciò possa aiutare a capire quanto siano rappresentativi i dati discussi.

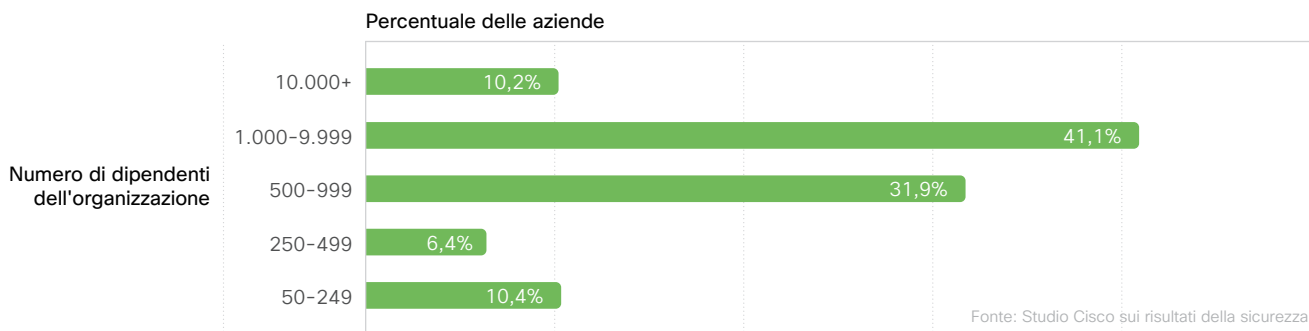


Figura A1 – Numero di dipendenti per le aziende partecipanti

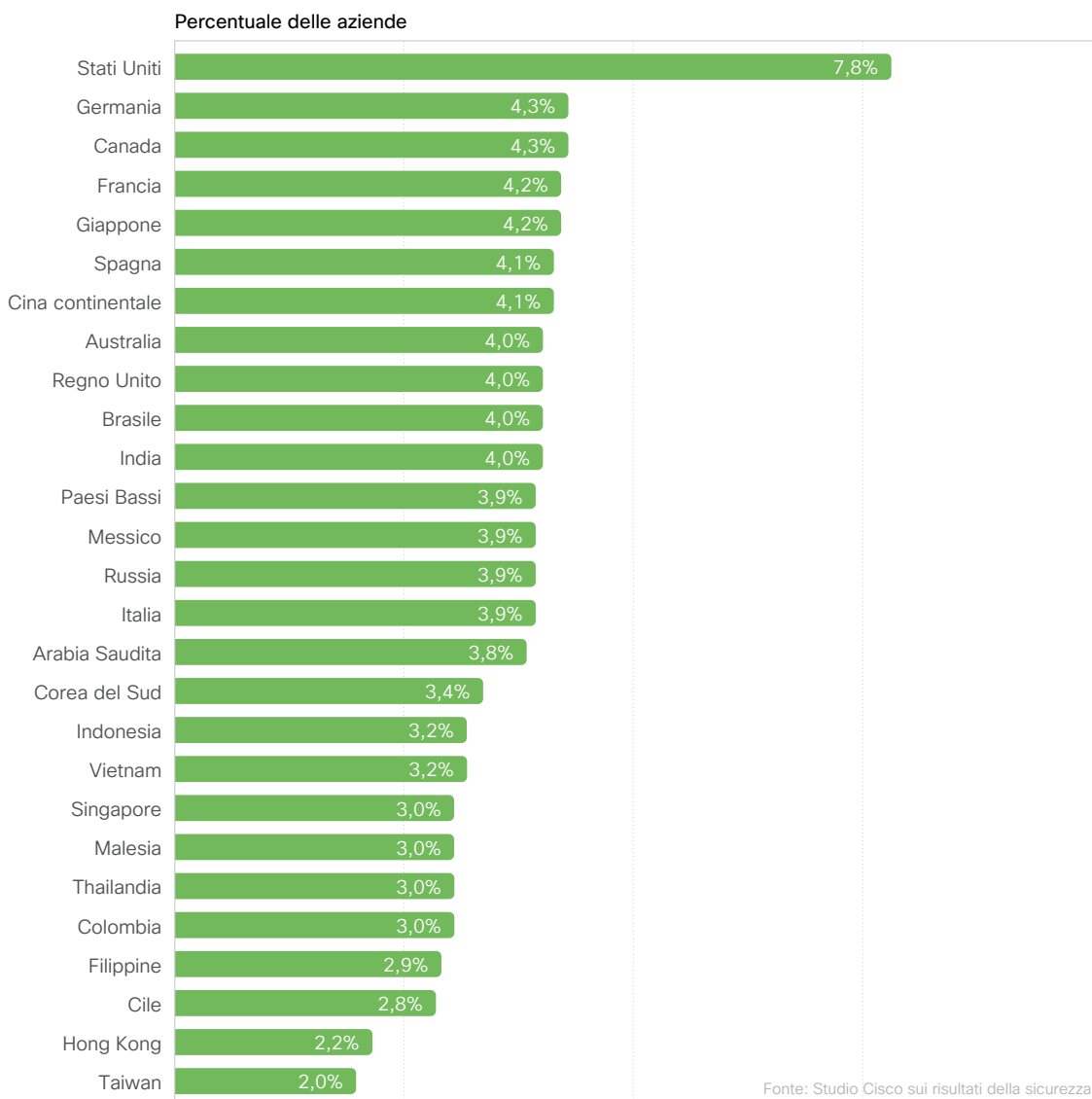


Figura A2 – Paesi in cui le aziende partecipanti hanno la sede centrale

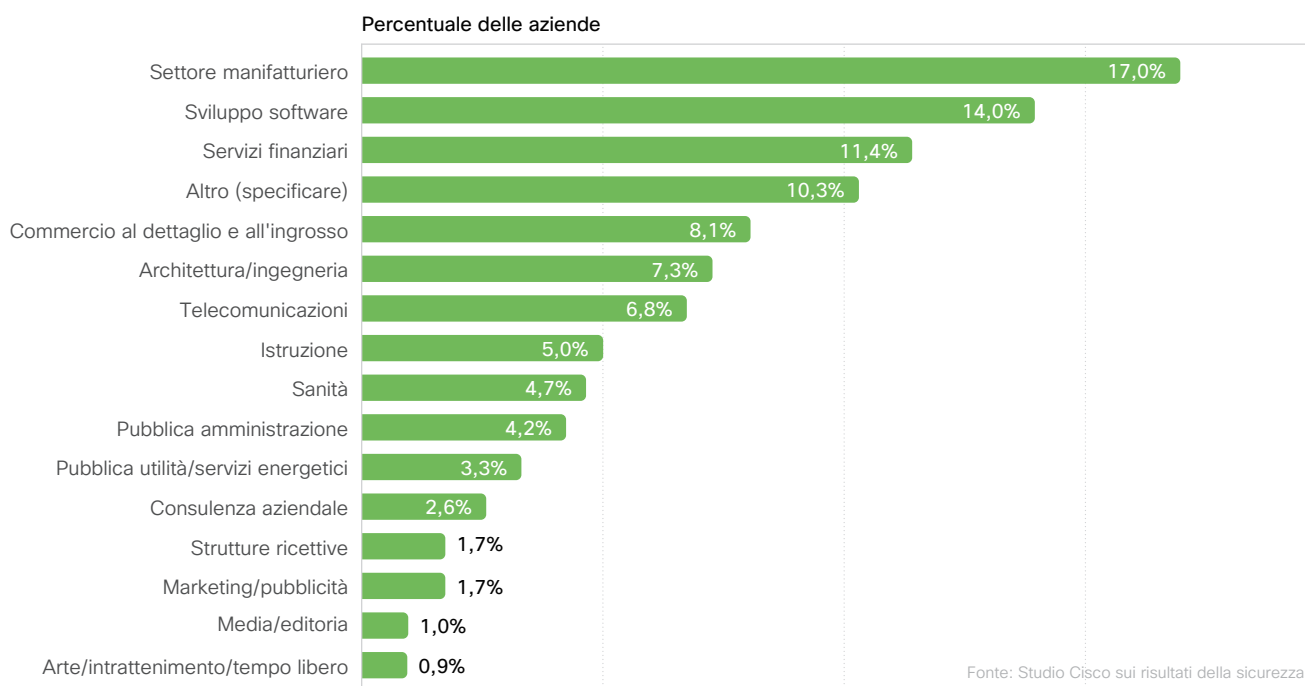


Figura A3 – Settori rappresentati dalle aziende partecipanti

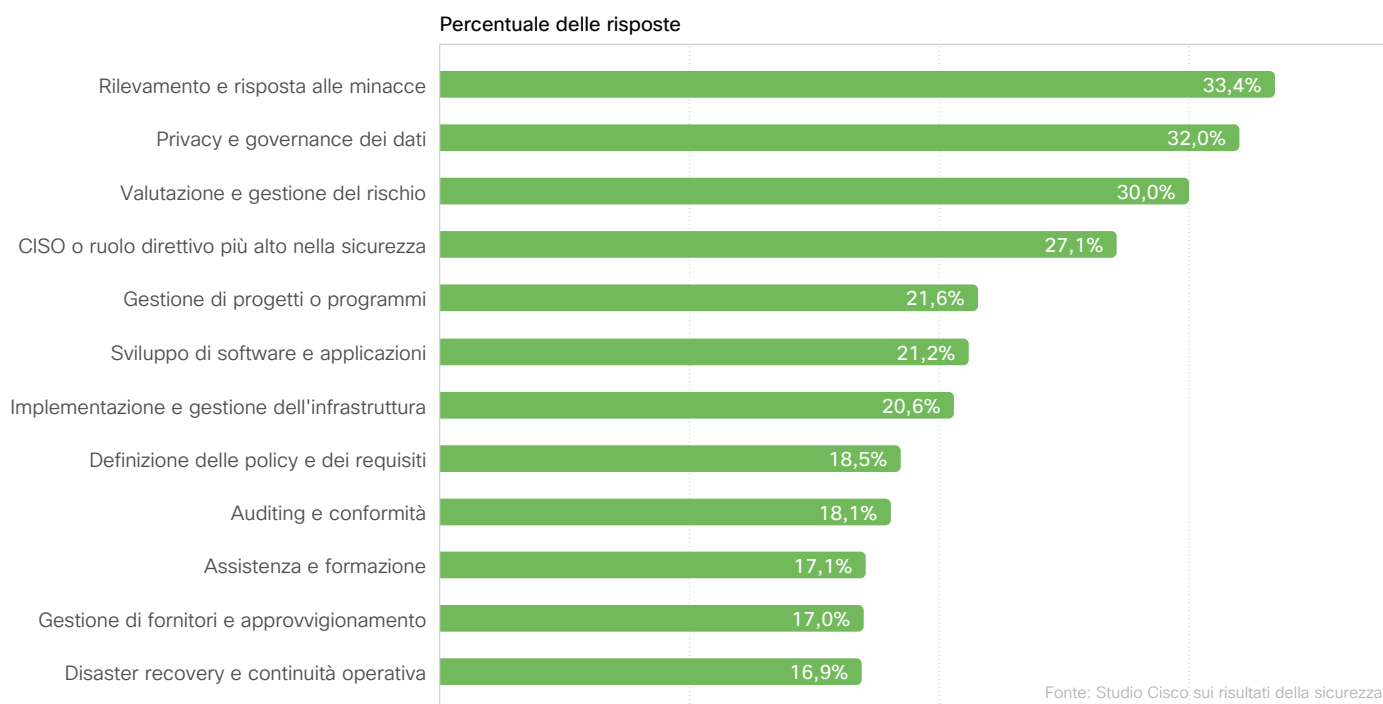


Figura A4 – Principali responsabilità lavorative tra gli intervistati

Sede centrale Americhe

Cisco Systems, Inc.
San Jose, CA

Sede centrale Asia Pacifico

Cisco Systems (USA), Pte. Ltd.
Singapore

Sede centrale Europa

Cisco Systems International BV
Amsterdam, Paesi Bassi

Pubblicato a dicembre 2021

© 2021 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati.

Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Per consultare l'elenco dei marchi Cisco, visitare il sito Web all'indirizzo www.cisco.com/go/trademarks. I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'uso del termine "partner" non implica una relazione di partnership tra Cisco e altre aziende.
779292577 | 12/21