HiSolution srl via della Canapiglia, 5 Vecchiano (Pisa)
sales@hisolution.it
marketing@hisolution.it
www.hisolution.it



(CYBER) SECURITY BUDGET: COME PRIORITIZZARE GLI INVESTIMENTI IN 5 STEP

Dalla mappatura dei rischi a un piano d'azione personalizzato.

Tempo di lettura

[⏳ 5 minuti]

Introduzione



Il paradosso della sicurezza

Negli ultimi anni, gli investimenti in cyber security sono costantemente cresciuti. Eppure, le violazioni aumentano, i danni sono sempre più gravi e la superficie d'attacco si estende di giorno in giorno. Il problema non è quanto spendi, ma dove e come investi.

Il paradosso della sicurezza

Negli ultimi anni, gli investimenti in cyber security sono costantemente cresciuti. Eppure, le violazioni aumentano, i danni sono sempre più gravi e la superficie d'attacco si estende di giorno in giorno.
Il problema non è quanto spendi, ma dove e come investi.

Le aziende si rafforzano...

+15%

Cresce il budget globale per la cyber security: secondo Gartner, è previsto un aumento da 183,9 a 212 miliardi di dollari.

+96%

Nel 2024, l'investimento globale in tecnologie avanzate di protezione (AI Cybersecurity) è quasi raddoppiato.

+170

Gli atti normativi sulla protezione dei dati che sono stati elaborati o entrati in vigore negli ultimi 2 anni (MIT).

ma gli incidenti aumentano...

+27,4%

La crescita degli incidenti cyber globali rilevati nel 2024 rispetto all'anno precedente (Clusit).

80%

La stragrande maggioranza degli incidenti a livello globale è classificata come critica o grave. Nel 2020, lo era il 50% (Clusit)

4,9 milioni USD

Il costo medio di un data breach nel 2024 a livello mondiale. Gli analisti (IBM) segnalano un aumento del 10% sul 2023.

TI SERVE UN APPROCCIO GUIDATO, OGGETTIVO E PERSONALIZZATO.

Il paradosso della sicurezza

Le aziende si rafforzano...

60%

La percentuale di aziende italiane che ha deciso di incrementare i budget cyber nel 2025 (Osservatorio PoliMI)

+58%

La percentuale di grandi imprese operanti in Italia ad aver nominato un CISO (Osservatorio PoliMI).

+11,5%

Il tasso di crescita annuo (CAGR) del mercato globale dei servizi gestiti di sicurezza dal 2023 al 2028 (Markets and Markets).

ma gli incidenti aumentano!

750 milioni

La quantità di minacce rilevate ogni giorno da Amazon nella propria infrastruttura (alcuni mesi fa, erano 100 milioni) (WSJ)

218

I giorni che le aziende impiegano (in media, a livello globale) per identificare e contenere gli incidenti (IBM, via ESG360)

100 mila USD

La perdita economica subita da un terzo (32%) delle aziende a causa di downtime non programmati (The State of Resilience 2025)

TI SERVE UN APPROCCIO GUIDATO, OGGETTIVO E PERSONALIZZATO.

Security budget: i 5 costi di cui devi tenere conto!

Un piano solido parte da una valutazione precisa delle voci di costo che incidono sulla tua capacità di protezione.

1. COSTO DEL LAVORO

Il personale specializzato è difficile da reperire e trattenere. Considera di quanto hai bisogno per garantire presidio continuo, incident response e governance, anche in contesti distribuiti. In alternativa, valuta il costo dei **servizi di sicurezza gestiti** da partner dedicati (MSSP).

2. COSTO DELLA TECNOLOGIA

Il momento di chiudere le falle esistenti, sanare vulnerabilità e consolidare le difese di base è arrivato. Per aziende più mature, ha senso iniziare a **investire in strumenti evoluti** (es. AI-based detection o XDR) che aumentano **capacità predittiva e automazione**.

3. COSTO DELL'INCIDENT RESPONSE

Detection senza response serve a poco. **Inserisci a budget processi operativi, strumenti di orchestrazione (SOAR**), ma anche test periodici del piano di incident response. La reazione tempestiva riduce drasticamente l'impatto economico di un attacco.

4. COSTI DI AWARENESS

Il fattore umano resta il punto dolente. Oltre alla formazione continua del team IT/security, ti conviene prevedere percorsi continui per tutta l'organizzazione: simulazioni, test, aggiornamenti sulle minacce.
Un consiglio: investi il giusto, ma in modo costante. Un corso di sei mesi seguito da un anno di stop non crea nessuna **cultura della sicurezza**.

5. COSTI DI GOVERNACE

Servono risorse per mantenere aggiornati policy, audit, compliance, reporting e gestione dei fornitori. La governance è il tessuto connettivo della tua **strategia di sicurezza** e ha un costo diretto e ricorrente.

Come definire le priorità di investimento in 5 step

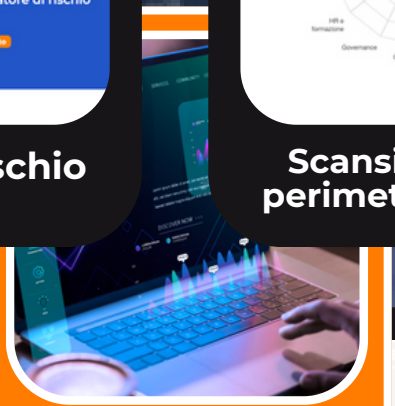
Tra minacce in aumento, compliance sempre più stringenti e un perimetro IT in evoluzione, **capire dove e come allocare risorse non è banale**. La tua azienda non è come le altre: ha un'esposizione specifica verso l'esterno, un suo livello di maturità cyber, è soggetta a differenti obblighi normativi.



Misura il rischio reale



Scansiona il tuo perimetro digitale



Mantieni il controllo, ogni settimana



Esplora il lato oscuro: il Dark Web



Passa all'azione con un Remediation Plan

TI SERVE UN APPROCCIO GUIDATO, OGGETTIVO E PERSONALIZZATO.

1. Misura il rischio reale, non quello percepito



Parti da un'analisi oggettiva.
Il rischio non si improvvisa né si indovina: esistono metodologie strutturate, processi riconosciuti e strumenti tecnici per misurare l'esposizione reale della tua azienda anche in relazione a specifiche normative (es., NIS 2).

Non ti fidare delle impressioni, di casi isolati o delle esperienze di altri.

Cosa devi evitare

- Basarti solo su **minacce viste altrove**;
- **Lasciare fuori intere aree** (es. procedure, autenticazione, supply chain);
- **Presumere che nessuno ti attaccherà**. Questo è l'errore più grave di tutti.

I nostri consigli

- Coinvolgi sia IT sia business per evitare bias di percezione;
- Aggiornati su minacce emergenti, vulnerabilità zero-day e nuovi vettori d'attacco;
- Non ragionare in ottica di azzeramento del rischio, ma di controllo.

In questo modo, avrai un quadro chiaro del rischio che corri realmente ed eviterai azioni a basso impatto solo perché percepite come urgenti.

2. Scansiona il tuo perimetro digitale

Il perimetro IT non è più quello di una volta: app esposte, VPN mal configurate, servizi dimenticati... sono tutte potenziali vie d'ingresso per gli attaccanti.

Una scansione ben fatta ti permette di identificare cosa è visibile dall'esterno e quindi attaccabile.



Cosa devi evitare

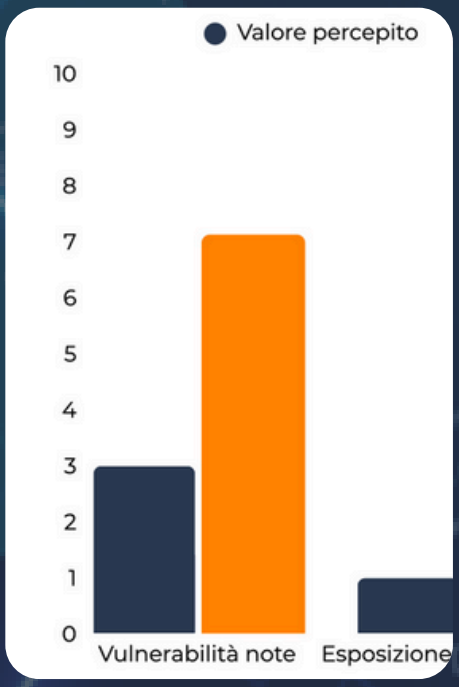
- Pensare che basti un firewall e sei salvo;
- Non sapere quali servizi sono effettivamente esposti su Internet;
- Dimenticare ambienti di test o cloud che nessuno monitora più.

I nostri consigli

- Usa tool di vulnerability scan per vedere la tua rete con gli occhi di chi la attaccherà;
- Ragiona in ottica di gestione continua delle vulnerabilità. Non le azzererai mai, ma le puoi gestire;
- Per stabilire le priorità e arrivare alla remediation (vedi sotto), devi sviluppare una matrice di rischio che combina impatto e probabilità di exploit.

Così facendo, potrai conoscere in ogni momento quanto sei realmente esposto e quanto lavoro dovrai fare per mettere in piedi le giuste contromisure. Senza dover improvvisare nulla in caso di incidente.

3. Esplora il lato oscuro: il dark web



Il furto potrebbe già essere avvenuto, ma tu non lo sai ancora. Credenziali, e-mail aziendali, numeri di carta o documenti interni possono essere in vendita nei marketplace del dark web.

Verificarlo è fondamentale per rispondere nel modo giusto.

Cosa devi evitare

- Pensare che se non hai ricevuto un attacco diretto, allora sei “intatto”;
- Sottovalutare i data breach passati o quelli indiretti (fornitori);
- Ignorare segnali di attività anomale legate a identità digitali aziendali.

I nostri consigli

- Usa servizi di monitoraggio del dark e deep web per scovare dati compromessi;
- Mappa la tua superficie d'attacco estesa. Controlla se i dati dei tuoi partner sono finiti nel dark web;
- Analizza ciò che trovi. Quando i tuoi dati sono nel dark web, non limitarti a cambiarli: studia in quali forum appaiono, da quanto tempo, a che prezzo vengono venduti e con quali altri dati sono associati.

In questo modo, puoi scoprire violazioni che ancora non conosci, anticipare attacchi mirati e agire prima che i dati compromessi vengano sfruttati.

4. Passa all’azione con un remediation plan

Ora serve un piano.
Il remediation plan è la sintesi operativa che ti dice cosa fare, in che ordine, con quale urgenza di fronte alle vulnerabilità.
Deve essere guidato dai dati, non dalle percezioni, e strutturato per rendere chiaro dove e quanto investire.



Cosa devi evitare

- Tentare di risolvere tutte le vulnerabilità, senza una gerarchia chiara;
- Confondere remediation e mitigation: non sempre serve eliminare le vulnerabilità, a volte è più efficace limitarne l’impatto in modo sostenibile;
- Delegare senza ownership chiara: non assegnare compiti generici per la gestione delle vulnerabilità.

I nostri consigli

- Stabilisci per ogni azione tempi, responsabilità e metriche di successo;
- Crea una roadmap progressiva. Ad azioni immediate che riducono il rischio fai seguire interventi strutturali più complessi;
- Documenta ogni decisione e risultato: registra non solo cosa hai fatto, ma perché l'hai fatto, quali alternative hai scartato e che risultati hai ottenuto.

In questo modo, potrai passare dalla consapevolezza all’azione, con un piano su misura che massimizza il ROI di ogni euro investito in sicurezza.

5. Tieni tutto sotto controllo, ogni settimana



Il tuo perimetro digitale cambia continuamente: nuove sedi, nuove persone, nuove app, nuove modalità di lavoro e vulnerabilità. Monitorare l'esposizione in modo continuo è l'unico modo per non vanificare il lavoro fatto e mantenere la protezione sempre aggiornata.

Cosa devi evitare

- Trattare la sicurezza come un'attività una tantum;
- Non aggiornare le analisi dopo modifiche infrastrutturali o organizzative;
- Pensare che siano sufficienti i tool giusti. **Spoiler**: sono necessari anche i processi.

I nostri consigli

- Imposta un monitoraggio ricorrente con report automatici e alert su nuove esposizioni (o ingaggia un partner competente per farlo);
- Confronta i risultati settimana dopo settimana per vedere l'evoluzione del rischio;
- Definisci trigger di riallineamento, eventi che richiedono una rivalutazione completa: acquisizioni, nuove sedi, cambio di fornitori cloud...

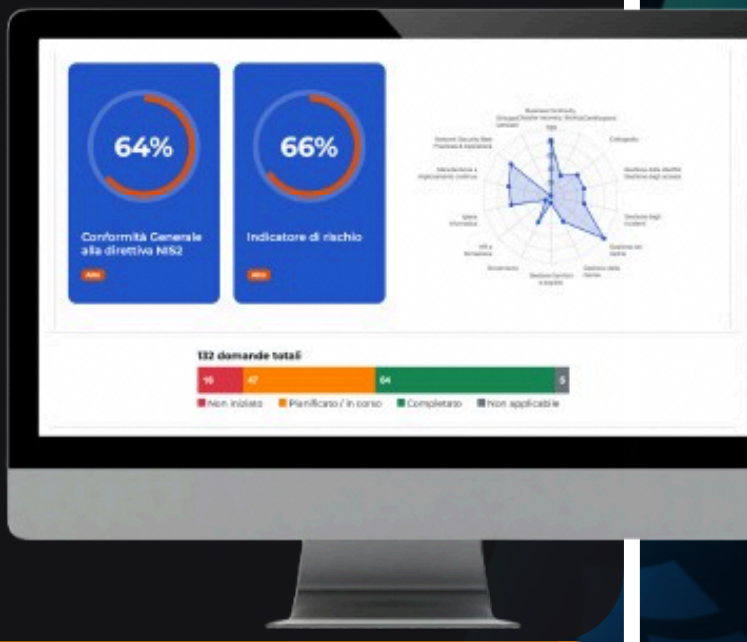
Così facendo, manterrai alta la reattività del sistema di difesa, ti adatterai in tempo reale ai cambiamenti e otterrai continuità nella protezione, che oggi è l'unica soluzione davvero efficace.

Metti ordine nelle priorità: ecco come ti aiutiamo ad allocare il budget in modo efficace

Il paradosso della sicurezza

HiCompliance è la soluzione progettata per ottimizzare il **budget di cybersecurity**, aiutandoti a prioritizzare gli investimenti in base ai rischi reali. Con un approccio strutturato e basato su metodologie riconosciute a livello internazionale, prima di definire una strategia personalizzata, analizziamo in modo oggettivo il rischio cyber a cui è esposta la tua azienda per renderti consapevole di quanto effettivamente l'organizzazione sia **vulnerabile alle minacce**.

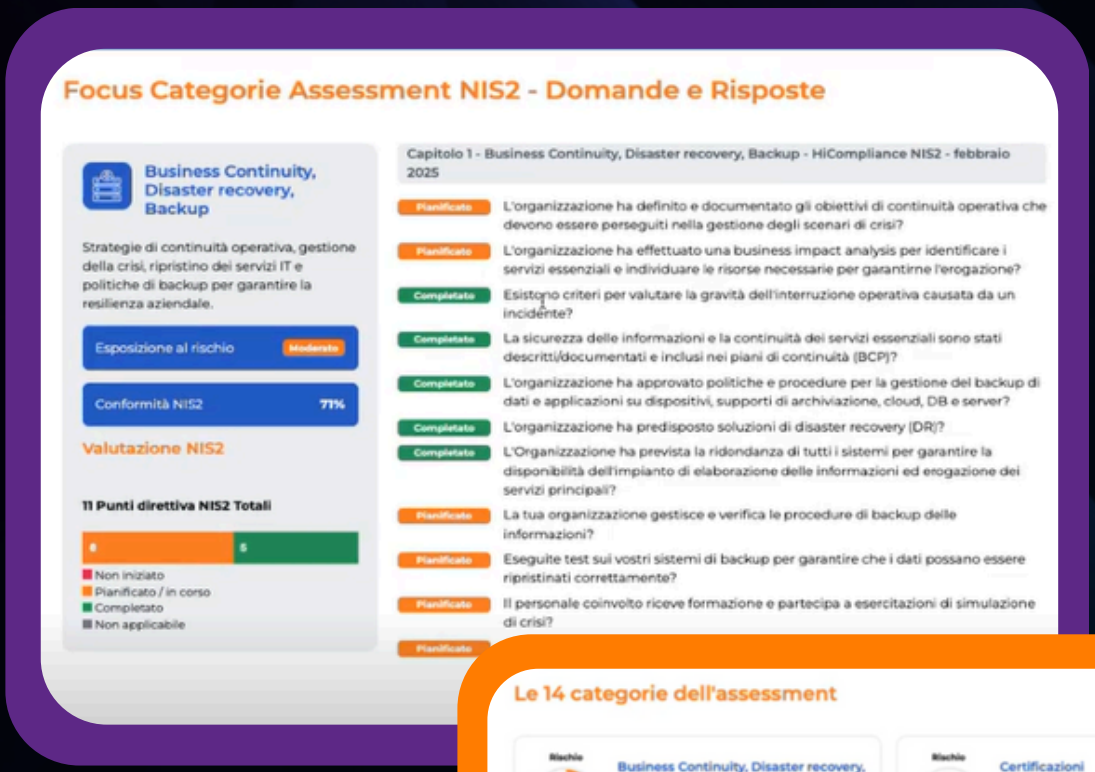
Successivamente, disegniamo insieme un percorso che permette di misurare e monitorare costantemente **il rischio cyber**, fornendo un piano d'azione personalizzato per allocare risorse in modo mirato e rispondere alle esigenze specifiche della tua azienda.

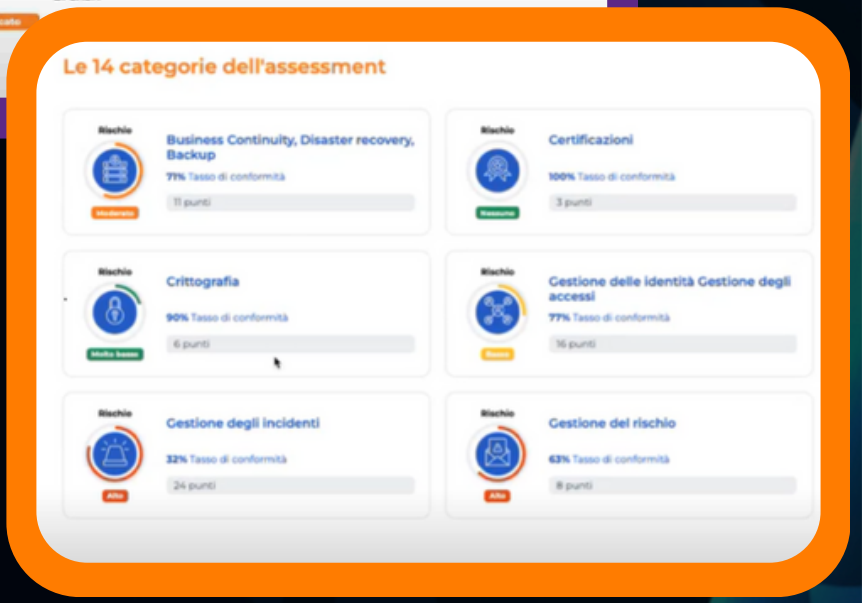


SCOPRI HICOMPLIANCE!

Assessment

Nella fase di assessment valutiamo la **gestione del rischio**, degli incidenti, delle reti e degli endpoint, ma anche i processi, le policy e la conformità alle **best practice**.

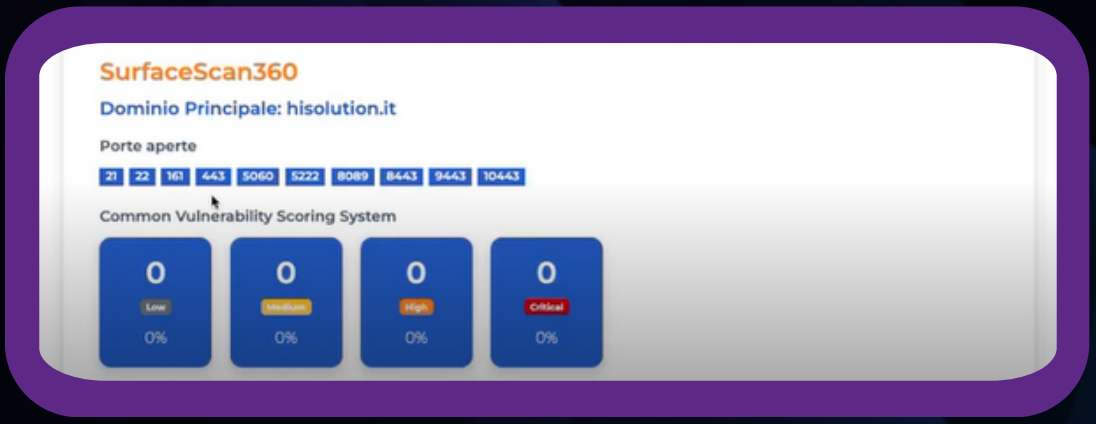




SCOPRI HICOMPLIANCE!

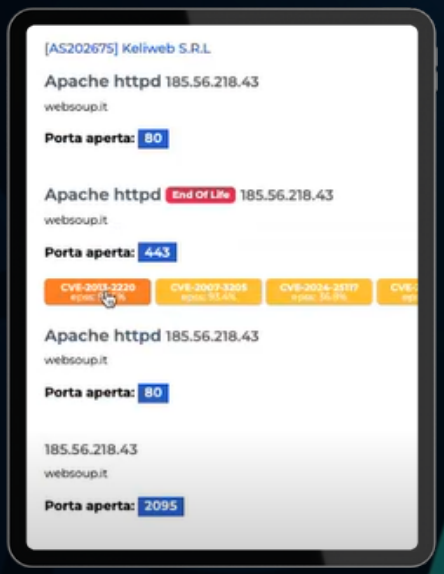
SurfaceScan360

All’assessment segue l’**analisi avanzata della superficie d’attacco** alla ricerca di vulnerabilità, con visibilità continua sugli asset accessibili dall'esterno.



DarkRisk360

All’assessment segue l’**analisi avanzata della superficie d’attacco** alla ricerca di vulnerabilità, con visibilità continua sugli asset accessibili dall'esterno.



SCOPRI HICOMPLIANCE!

Radart Chart

A seguito della correlazione e dell'analisi dei dati, che si avvale anche di tool di AI, sviluppiamo una **radar chart** che evidenzia "a colpo d'occhio" le necessità emerse e le **priorità di investimento,** a beneficio di tutta l'azienda.



Remediation Plan

Sviluppiamo insieme un **piano su misura** per la mitigazione delle vulnerabilità e la conformità con il dettato normativo in essere.

Definiamo chiaramente attività, scadenze e responsabilità, nonché le priorità d'intervento in funzione del livello di rischio.



SCOPRI HICOMPLIANCE!

hi solution
better ICT for every business

HiSolution srl via della Canapiglia, 5 Vecchiano (Pisa)
sales@hisolution.it
marketing@hisolution.it
www.hisolution.it



Il tuo perimetro digitale è già cambiato da quando hai iniziato a leggere questo documento.

INQUADRA IL **QR CODE** PER SCOPRIRE L'OFFERTA CHE TI ABBIAMO RISERVATO!

Non aspettare il prossimo attacco per scoprire cosa ti sei perso!