MINACCE, STRATEGIE E SOLUZIONI PER LA SICUREZZA DIGITALE

I DATI EMERSI DAL CYBERSECURITY SUMMIT 2026

Un Whitepaper pensato per i decision maker che vogliono trasformare la sicurezza informatica in un vantaggio competitivo.

www.hisolution.it

EXECUTIVE SUMMARY

Il panorama della **cybersecurity** non è mai stato così complesso e così **urgente**. Gli attacchi informatici sono diventati più sofisticati, più frequenti e più devastanti, colpendo organizzazioni di ogni dimensione e settore.

Ransomware, phishing evoluto, compromissione delle identità digitali e vulnerabilità della supply chain sono la realtà quotidiana con cui le aziende italiane devono confrontarsi.

L'obiettivo di questo documento è offrire una lettura chiara del contesto attuale e presentare soluzioni operative per costruire una postura di sicurezza davvero resiliente.

1. IL PANORAMA ATTUALE: UN'ESCALATION SENZA PRECEDENTI

La velocità con cui il panorama delle minacce evolve non ha precedenti. Come emerso durante il **Cybersecurity Summit 2026**, la sicurezza informatica ha smesso di essere una questione puramente tecnica per diventare una **priorità strategica trasversale** a tutta l'organizzazione.

Le minacce che stanno ridefinendo la cybersecurity

Ransomware di nuova generazione

Non più semplici attacchi di cifratura, ma operazioni strutturate con **doppia estorsione** (dati cifrati e minaccia di pubblicazione), **tempi di permanenza prolungati** nelle reti e **targeting selettivo** delle organizzazioni più vulnerabili.

Compromissione delle identità digitali

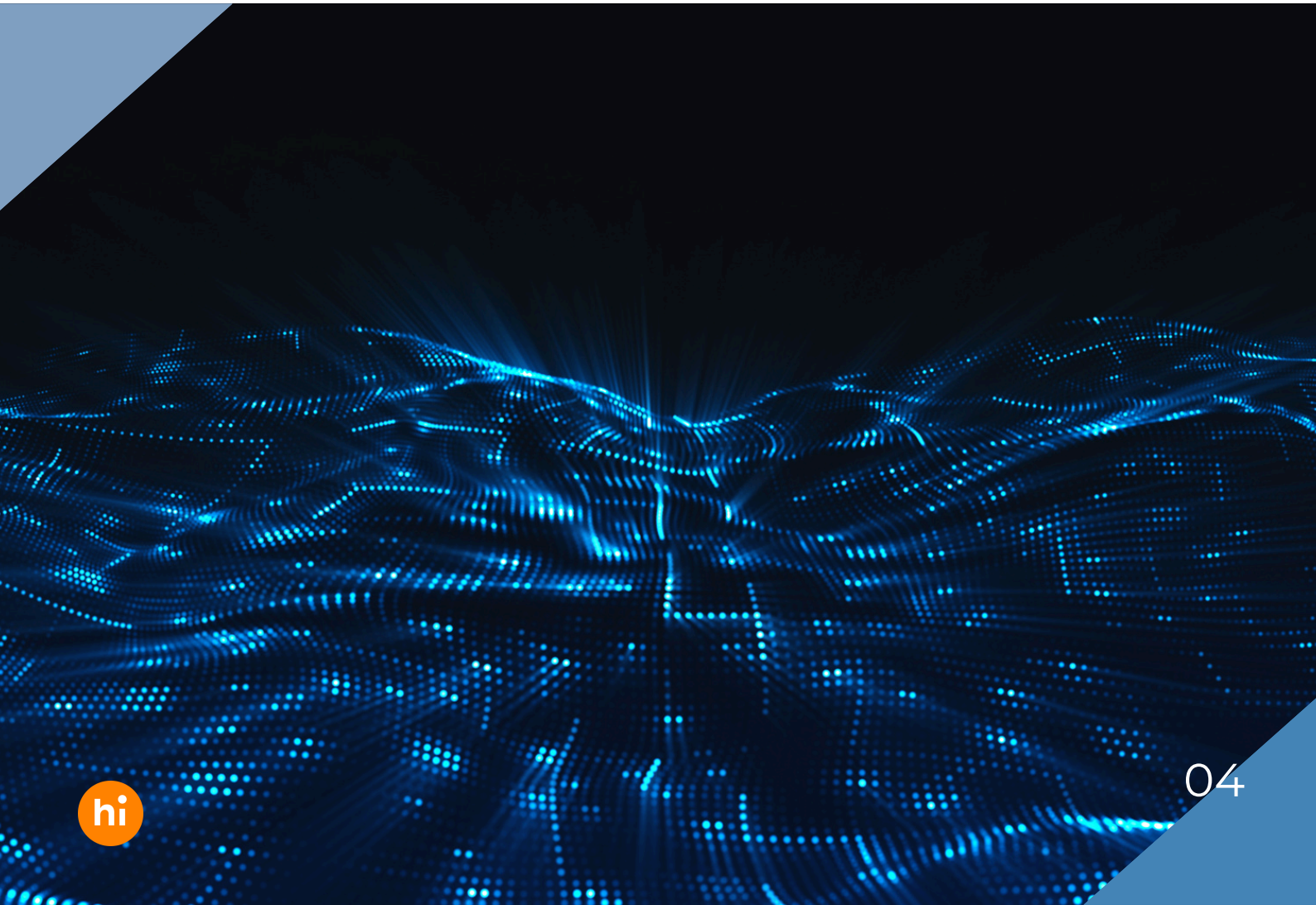
Con ambienti di lavoro sempre più distribuiti e un numero crescente di accessi da remoto, le **credenziali compromesse** rappresentano oggi il vettore d'attacco più sfruttato. Un'identità violata può aprire le porte all'**intera infrastruttura** aziendale.

Vulnerabilità della supply chain

Gli attaccanti non colpiscono sempre la vittima finale direttamente: sempre più spesso entrano attraverso **fornitori**, **partner** o **software di terze parti**, sfruttando la catena di fiducia come punto di accesso privilegiato.

Phishing evoluto e spear phishing

Le campagne di phishing sono diventate altamente personalizzate, sfruttando l'**intelligenza artificiale** per generare messaggi credibili, contestuali e **difficili da distinguere dalle comunicazioni legittime**. L'avvento dell'Intelligenza Artificiale generativa permette oggi ai cybercriminali di creare **messaggi di phishing personalizzati**, contestuali e scritti in un italiano perfetto, eliminando i classici refusi che un tempo ne facilitavano il riconoscimento



IL FATTORE UMANO: IL PERIMETRO PIÙ DIFFICILE DA DIFENDERE

Uno dei messaggi più forti emersi riguarda il **fattore umano**. La tecnologia da sola non basta: molti degli attacchi più gravi continuano a sfruttare errori umani, **comportamenti inconsapevoli o processi non adeguatamente strutturati.**

La **formazione del personale** deve evolversi di pari passo con l'**evoluzione delle minacce guidate dall'IA**, addestrando i collaboratori a riconoscere non solo email sospette, ma anche **tentativi di social engineering più sofisticati** (come il clone vocale o il deepfake).



Costruire una **cultura della sicurezza** diffusa all'interno dell'organizzazione non è più un'opzione: è un requisito fondamentale per migliorare la resilienza aziendale. Questo significa coinvolgere non solo il reparto IT, ma **tutte le funzioni aziendali**: dalla direzione alle risorse umane, dall'amministrazione alle operations.

IL NUOVO PERIMETRO: LE IDENTITÀ DIGITALI

Come sottolineato nel corso degli interventi, il concetto tradizionale di "perimetro di sicurezza" è ormai obsoleto.
In un mondo di cloud, smart working e accessi distribuiti, **il nuovo perimetro è l'identità digitale**.



Il principio guida che si afferma con forza è quello del **"never trust, always verify"**: nessun utente, dispositivo o applicazione dovrebbe essere considerato automaticamente affidabile, indipendentemente dalla sua posizione nella rete.
Ogni accesso deve essere verificato, ogni privilegio deve essere giustificato, ogni anomalia deve essere rilevata.

Strumenti fondamentali in questo scenario

Autenticazione multifattore (MFA)

Sistema di sicurezza che richiede all'utente di verificare la propria identità utilizzando due o più metodi di sblocco diversi.

Controllo degli accessi privilegiati (PAM)

Strategia di cybersecurity progettata per proteggere, monitorare e gestire gli account con diritti di amministratore.

Monitoraggio continuo e rilevamento delle anomalie

Uso di strumenti automatizzati e Intelligenza Artificiale per osservare dati o sistemi 24/7



IL PESO DELLA COMPLIANCE: NIS2 E DORA

Il contesto normativo sta cambiando rapidamente e in modo significativo. La Direttiva **NIS2** e il regolamento **DORA** stanno ridefinendo gli standard di protezione richiesti alle organizzazioni europee, introducendo nuovi obblighi in materia.

- **Governance della sicurezza** ➡️ responsabilità diretta del management
- **Gestione del rischio** ➡️ approccio strutturato e documentato
- **Continuità operativa** ➡️ piani di risposta agli incidenti testati e aggiornati
- **Segnalazione degli incidenti** ➡️ obblighi di notifica stringenti e tempestivi

Per le aziende, la compliance non è più un adempimento burocratico: è una leva per costruire una **postura di sicurezza più matura e strutturata**. Le organizzazioni che non si adeguano rischiano non solo sanzioni, ma soprattutto una **maggiore esposizione agli attacchi**.

CYBERSECURITY E BUSINESS CONTINUITY: UN LEGAME INSCINDIBILE

Un attacco cyber oggi non rappresenta soltanto un problema tecnico. È un rischio concreto per **operatività**, **reputazione** e **competitività**. I **tempi di fermo**, la **perdita di dati sensibili**, il **danno reputazionale** e le **conseguenze legali** possono compromettere la sopravvivenza stessa di un'organizzazione.



Per questo motivo, investire in cybersecurity significa investire nella **continuità del business** e deve essere percepito e comunicato come tale a livello di board e direzione aziendale.

2. LE SOLUZIONI: DALLA CONSAPEVOLEZZA ALL'AZIONE

Conoscere le minacce è il primo passo. Il secondo, quello decisivo, è dotarsi degli **strumenti** giusti per affrontarle. *HiSolution* propone un **approccio integrato** che combina **tecnologia avanzata**, **visibilità centralizzata** e **competenza specialistica**.

HiSolution Console: Visibilità Totale, Controllo Centralizzato

HiSolution Console è la risposta concreta alla crescente complessità degli ambienti IT aziendali. In un contesto in cui le minacce si moltiplicano e gli asset da proteggere si distribuiscono su cloud, endpoint, reti e identità, avere una **visione unificata e centralizzata della propria postura di sicurezza** non è un lusso: è una necessità operativa.

HiSolution Console sfrutta **algoritmi di machine learning** per **correlare i dati in tempo reale**, distinguendo i falsi positivi dalle minacce reali. Questo, unito alla tecnologia di **deep learning di Sophos Intercept X**, permette di **bloccare malware sconosciuti** basandosi sul loro comportamento, prima ancora che vengano catalogati.

COSA OFFRE HISOLUTION CONSOLE

01

Dashboard centralizzata

Un'unica interfaccia per monitorare lo **stato di sicurezza** dell'intera infrastruttura, con **visibilità in tempo reale** su eventi, alert e vulnerabilità.

02

Correlazione degli eventi

Capacità di correlare **segnali provenienti da fonti diverse** per identificare **pattern di attacco complessi** che singoli strumenti isolati non riuscirebbero a rilevare.

03

Gestione degli alert

Prioritizzazione intelligente degli alert per ridurre il rumore e permettere ai team di sicurezza di concentrarsi sulle minacce reali e urgenti.

04

Reportistica e compliance

Generazione di **report strutturati** per supportare i processi di **audit**, la **governance della sicurezza** e gli **adempimenti normativi** (NIS2, DORA, GDPR).

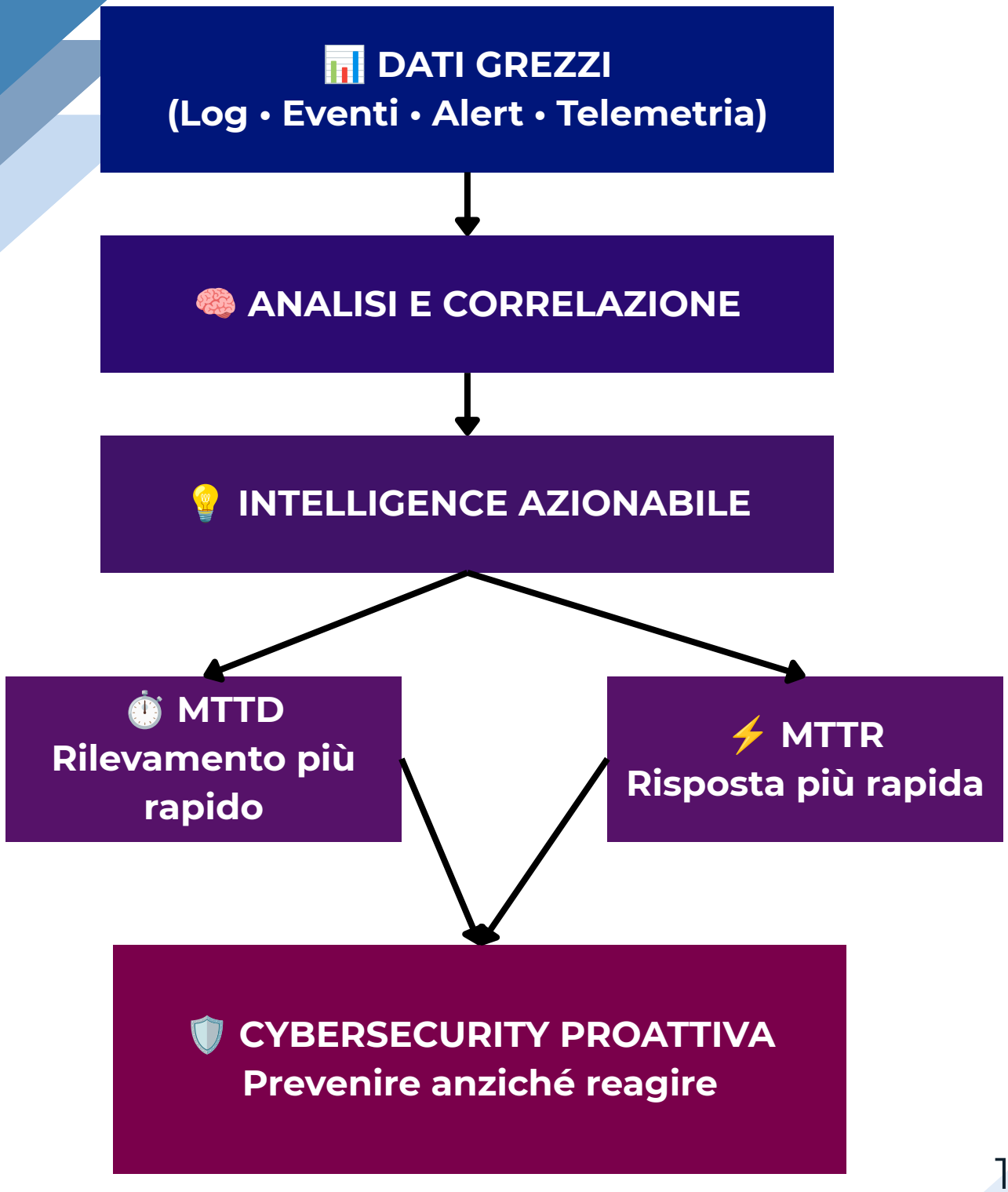
05

Integrazione con l'ecosistema esistente

La Console si integra con le principali soluzioni di sicurezza già presenti nell'ambiente del cliente, **valorizzando gli investimenti già effettuati**.

Il valore per il business

HiSolution Console trasforma dati grezzi in **intelligence azionabile**, riducendo i tempi di rilevamento e risposta agli incidenti (MTTD e MTTR) e permettendo alle organizzazioni di passare **da una postura reattiva a una proattiva**.



SOPHOS: PROTEZIONE AVANZATA CON INTELLIGENCE INTEGRATA

La partnership con Sophos porta nelle organizzazioni clienti di HiSolution **una delle piattaforme di cybersecurity più avanzate e riconosciute a livello globale**, con un approccio che integra **intelligenza artificiale, threat intelligence e risposta automatizzata**.

Le soluzioni Sophos nell'ecosistema HiSolution:

Sophos Firewall — Next-Generation Firewall

Protezione perimetrale avanzata con deep packet inspection, controllo delle applicazioni, prevenzione delle intrusioni e integrazione nativa con gli endpoint Sophos per una risposta coordinata alle minacce.

Sophos Central — Gestione Unificata

Una piattaforma cloud-native che permette di gestire tutti i prodotti Sophos da un'unica console, con visibilità completa su endpoint, rete, server, email e identità.

Sophos Intercept X — Endpoint Protection di Nuova Generazione

Protezione avanzata degli endpoint basata su deep learning e analisi comportamentale. Rileva e blocca ransomware, exploit e malware sconosciuti prima che possano causare danni, grazie a tecnologie anti-ransomware specifiche come CryptoGuard.

Sophos MDR (Managed Detection & Response)

Un servizio di rilevamento e risposta gestito da un team di esperti attivo 24/7. Sophos MDR monitora continuamente l'ambiente del cliente, indaga le minacce e interviene direttamente per neutralizzarle — liberando i team IT interni dal peso della gestione continua degli alert.

Il valore aggiunto della partnership HiSolution & Sophos:

L'integrazione tra la HiSolution Console e le soluzioni Sophos crea un **ecosistema di sicurezza sinergico**, in cui la **visibilità centralizzata** di HiSolution si combina con la **capacità di rilevamento e risposta** di Sophos per offrire una **protezione completa, scalabile e gestita da professionisti certificati**.

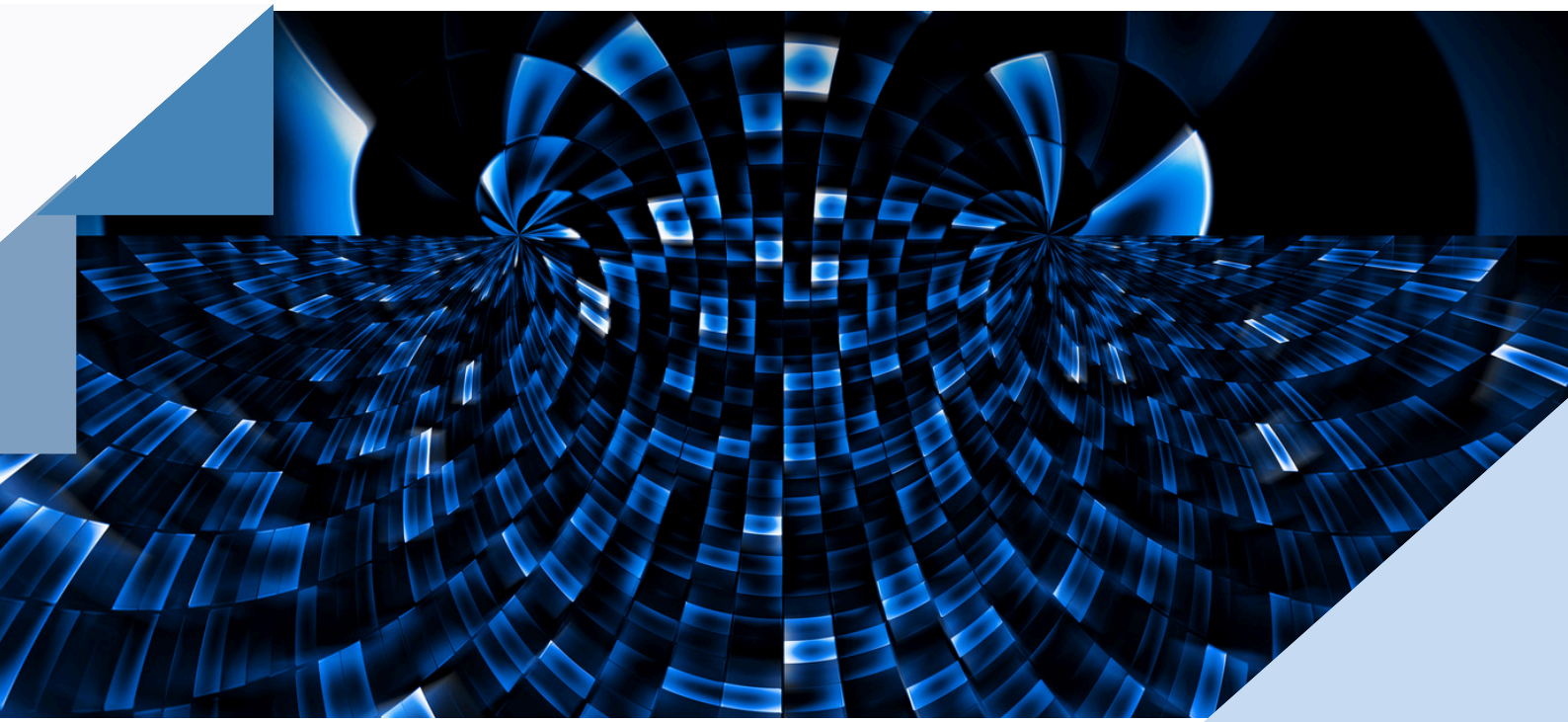
3. CONCLUSIONI: LA SICUREZZA COME SCELTA STRATEGICA

Il Cybersecurity Summit 2026 ha confermato una verità che i professionisti del settore conoscono bene ma che spesso fatica a trovare spazio nelle agende aziendali: **la cybersecurity non è un costo, è un investimento strategico**.

Le organizzazioni che scelgono di affrontare la sicurezza informatica con un approccio strutturato, integrato e proattivo ottengono molteplici vantaggi concreti.

- **Riduzione del rischio di incidenti gravi** e delle relative conseguenze operative, economiche e reputazionali
- **Conformità normativa garantita** e sostenibile nel tempo, senza affanno
- **Continuità operativa anche in scenari di attacco**, grazie a piani di risposta testati e strumenti di ripristino rapido
- **Fiducia da parte di clienti, partner e stakeholder**, che percepiscono la sicurezza come un segnale di maturità e affidabilità aziendale
- **Vantaggio competitivo** in un mercato in cui la reputazione digitale è sempre più un fattore differenziante

Il futuro della **cybersecurity** sarà sempre più orientato verso **modelli proattivi e predittivi**, basati su **automazione e intelligence**. Ma al centro continueranno a esserci le **persone**: le competenze, la consapevolezza e la capacità decisionale dei team che ogni giorno proteggono le infrastrutture digitali delle nostre organizzazioni.



La domanda non è più se un'organizzazione sarà presa di mira, ma quando, e quanto sarà pronta a rispondere.

4. PROSSIMI PASSI: COSTRUISCI LA TUA STRATEGIA DI SICUREZZA CON HISOLUTION

Sei prontə a valutare la tua postura di sicurezza e identificare le aree di miglioramento prioritarie?

HiSolution è al tuo fianco con un **team di esperti certificati**, **soluzioni tecnologiche d'eccellenza** e un **approccio consulenziale** che parte dalla realtà della tua organizzazione.

Richiedi una Demo della HiSolution Console

CONTATTACI

Scopri in modo concreto qual è il livello di esposizione della tua organizzazione e quali azioni prioritarie puoi introdurre subito.

➡️ **Contattaci per fissare un incontro con i nostri esperti!**

📧 **marketing@hisolution.it**
🌐 **www.hisolution.it**

Questo whitepaper è stato redatto da HiSolution sulla base dei contenuti condivisi durante il Cybersecurity Summit 2026. Per ulteriori informazioni sulle soluzioni e i servizi descritti, contattare il nostro team marketing.