> cybersecurity summit 2026_

IL TEMPO È L'ARMA.

Attacchi a velocità di macchina, team al limite, scadenze che si avvicinano. Cosa ci hanno detto gli IT manager al Cybersecurity Summit 2026.

E come trasformare la pressione del tempo in un vantaggio.

FIRENZE · 25.09.2026
HISOLUTION.IT

// PERCHÉ QUESTO REPORT

Oggi parliamo di tempo. Il tuo e il suo.

Durante un attacco informatico il tempo si comprime: ogni secondo pesa quanto un'ora, e in quello spazio minuscolo si decide se l'attacco vince o viene fermato.

Per chi attacca, il tempo è l'arma più preziosa. Per chi difende, se sa leggerlo e anticiparlo, può diventare un alleato. È il filo che ha tenuto insieme il Cybersecurity Summit 2026, il 25 settembre a Firenze.

A fine giornata abbiamo chiesto ai partecipanti, IT manager, CIO e responsabili della sicurezza, di rispondere a poche domande secche. In queste pagine le loro risposte si incrociano con i dati di **Clusit** e **Sophos**, con le storie raccontate sul palco e con una lista di cose da fare subito.

Il team HiSolution

INDICE

01 **Il tempo di chi attacca**
Più attacchi, più veloci, di notte

02 **Il tempo di chi difende**
Team piccoli, perimetri che crescono

03 **La voce della sala**
Cosa ci hanno detto gli IT manager

04 **Il paradosso**
Scadenze vicine, urgenza tiepida

05 **Cosa preoccupa**
Incidenti e timori dichiarati

06 **Dove investire**
Le priorità dei partecipanti

07 **Dal palco**
Tre aziende raccontano

08 **HiSolution Console**
Un accesso, non dieci

09 **La scadenza**
Per chi è in perimetro NIS2

10 **10 mosse**
Per riprendersi il tempo

// 01 · IL TEMPO DI CHI ATTACCA

Più attacchi. Più veloci. Mentre dormi.

Il 2025 ha segnato il record di attacchi gravi. E chi attacca sceglie il momento in cui nessuno guarda: la notte, il weekend, i festivi.

// QUANTI · RAPPORTO CLUSIT 2026

5.265
attacchi gravi nel mondo nel 2025, **+49%**: il numero più alto mai registrato

9,6%
degli incidenti mondiali colpisce l'Italia, ben oltre il suo peso economico

+42%
gli attacchi gravi in Italia rispetto al 2024

// QUANDO E COME · SOPHOS ACTIVE ADVERSARY REPORT 2026

88%
dei payload ransomware è distribuito fuori orario, di notte o nei festivi

3,4 ore
il tempo mediano per arrivare ad Active Directory dall'intrusione

67%
degli incidenti parte da un'identità compromessa

> LETTURA

Anche il furto dei dati segue lo stesso orario: il 79% delle esfiltrazioni avviene fuori dall'ufficio. Se la difesa lavora 8 ore al giorno, l'attaccante ha le altre 16.

Fonti: Clusit, "Dati dal Rapporto Clusit 2026", 11 marzo 2026. Sophos, Active Adversary Report 2026 (661 casi IR e MDR, novembre 2024 – ottobre 2025).

// 02 · IL TEMPO DI CHI DIFENDE

Dall'altra parte c'è un team che non basta mai.

È il volto di chi gestisce la sicurezza ogni giorno: poche persone, un perimetro che si allarga e la responsabilità di tenere tutto acceso, sempre.

Team sottodimensionato	Per un'infrastruttura che cresce ogni anno.
Competenze difficili da trovare	Personale ICT qualificato e specializzato è raro.
Sempre reperibili	Essere la business continuity dell'azienda, anche in ferie.
Multisede	Conoscere il perimetro tecnologico di tutte le sedi.
Troppi tool, troppe dashboard	Manca la visione d'insieme.

Il punto non è lavorare di più. È smettere di spendere il tempo dei tecnici a guardare log e rincorrere allarmi, per restituirlo a quello che fa crescere l'azienda.

// 03 · LA VOCE DELLA SALA

Poche domande. Risposte senza filtri.

A fine giornata abbiamo chiesto ai partecipanti del Summit di compilare un questionario breve, in forma anonima.

52%

ha avuto un incidente recente: attacchi, downtime o perdita di dati

56%

ha una scadenza di audit o normativa in arrivo

56%

sta valutando altri fornitori in questo momento

40%

dichiara un budget IT annuale oltre i 100.000 euro

> LETTURA

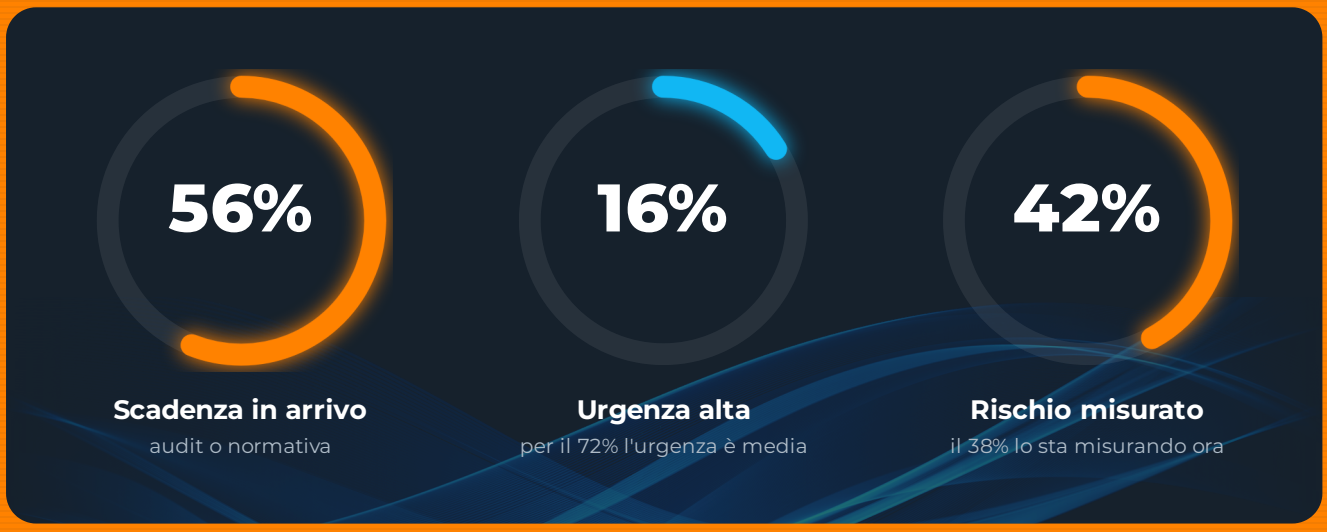
Un pubblico che è già stato colpito, ha scadenze in agenda e sta guardando il mercato. Il momento per decidere è adesso.

Percentuali sui questionari validi raccolti al Cybersecurity Summit 2026, Firenze, 25 settembre 2026. Campione non statistico: partecipanti all'evento.

// 04 · IL PARADOSSO

Le scadenze sono vicine. L'urgenza no.

Più di metà dei partecipanti ha un audit o una scadenza normativa in arrivo, ma solo il 16% sente un'urgenza alta di cambiare. E meno della metà ha già misurato il proprio rischio cyber.



> **È esattamente in questo spazio, tra "lo so" e "lo sto facendo", che un incidente trova un'azienda impreparata.**

// 05 · COSA TIENE SVEGLI LA NOTTE

Non è teoria. È già successo.

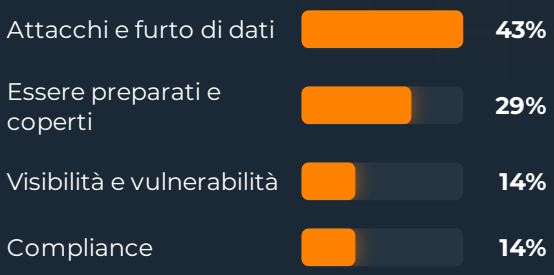
Incidenti recenti dichiarati

% dei rispondenti



La preoccupazione principale

% delle risposte aperte, raggruppate per tema



// NELLE LORO PAROLE

> *Non poter rispondere.*

> *Vulnerabilità non considerate.*

> *Furto di credenziali, accesso ai backup.*

La paura più citata resta l'attacco con perdita o furto di dati. Subito dopo arriva un timore meno tecnico e più onesto: non essere pronti, non essere coperti, non riuscire a rispondere quando serve. Ed è proprio qui che il tempo fa la differenza.

Risposte anonime dal questionario del Cybersecurity Summit 2026. Raggruppamento per tema a cura di HiSolution.

// 06 · DOVE INVESTIRE

Essere in regola. Verificare. Poter ripartire.

Abbiamo chiesto quali servizi potrebbero migliorare la sicurezza nei prossimi mesi. Le prime tre scelte disegnano un percorso preciso.



01 · REGOLE

Quasi uno su due chiede supporto sulla compliance: servono metodo ed evidenze, non solo tecnologia.

02 · VERIFICA

Il Penetration Test è al secondo posto: prima di dichiararsi sicuri, si vuole sapere dove si è esposti.

03 · RIPARTENZA

Backup e disaster recovery chiudono il podio: la domanda non è più "se", ma "quanto velocemente".

// 07 · DAL PALCO · TAVOLA ROTONDA

Tre aziende.
Tre modi di riprendersi il tempo.

Etruria Retail

Fabio Ravaglia · Responsabile Sistemi Informativi

Cooperativa nata a Siena nel 1961, circa 290 punti vendita nell'Italia centrale.

"Con una rete così vasta non potevamo più permetterci zone d'ombra. Tradurre il rischio in un numero ha fatto capire al board che la sicurezza protegge il valore dell'azienda."

CONSIGLIO > **Non aspettate un incidente per misurare il rischio.**

Sistemi ICT

Fabio Lazzaro · CTO

MSP toscano che da vent'anni porta in cloud i gestionali di professionisti e PMI.

"Lo strumento c'era, ma mancava il tempo per gestirlo. Sapere che l'infrastruttura è presidiata anche a Ferragosto e a Natale ha restituito tempo all'innovazione."

CONSIGLIO > **Il tempo dei vostri tecnici è la risorsa più preziosa: non sprecatela a guardare log.**

DPV

Fabrizio Gramaglia · CTO & CISO

30 anni nel Trade Marketing, 220 persone su cinque sedi operative.

"Avevamo molti fornitori, ognuno conosceva un solo pezzo. Oggi il valore è la serenità operativa: un unico interlocutore che conosce ogni dettaglio."

CONSIGLIO > **Scegliete un partner che risolva i problemi, non uno che si limiti a segnalarli.**

Tavola rotonda moderata da HiSolution con Francesco Vigiani, Key Area Manager HiSolution. Risposte in sintesi.

// TRENTA MINUTI IN QUATTRO PAROLE

01 **CHIAREZZA**

02 **TEMPO**

03 **FIDUCIA**

04 **ASCOLTO**

> *Partiamo sempre da quello che vi tiene svegli la notte. Il resto viene da sé.*
>
> FRANCESCO VIGIANI · KEY AREA MANAGER HISOLUTION

Tre aziende, tre esigenze diverse, la stessa scelta di fondo: smettere di rincorrere le emergenze e iniziare a governare il rischio prima che diventi un problema.

// 08 · LA NOVITÀ

NEW · HISOLUTION CONSOLE

Un accesso.
Non dieci.

Troppi tool e troppe dashboard tolgono la visione d'insieme. HiSolution Console riunisce i servizi in un unico punto: la sicurezza passa da costo tecnico a decisione strategica.



01

Un accesso, non dieci

Niente più mille password e dashboard diverse.

02

Tutto a colpo d'occhio

Se succede qualcosa, lo vedi subito.

03

Un unico interlocutore

Per gestire tutta la tua infrastruttura.

INTEGRAZIONI

HiDetect · HiLog · HiMFA · HiBackup

COMING SOON

Ticketing in console con Halo PSA: apri, segui e chiudi i ticket senza uscire. Connettori per piattaforme di terze parti.

Illustrazione indicativa, non rappresenta l'interfaccia reale del prodotto.

// 09 · LA SCADENZA

E se sei in perimetro NIS2, il tempo ha una data.

Non tutte le aziende rientrano nella NIS2. Ma chi è in elenco dal 2025 deve avere le misure di base operative e documentate entro il 31 ottobre 2026. E chi lavora per un soggetto NIS2 riceverà dai propri clienti richieste di evidenze di sicurezza.

16.10.2024 — **Il D.Lgs. 138/2024 entra in vigore**
Recepisce in Italia la direttiva NIS2.

GEN 2026 — **Notifica degli incidenti operativa**
Per chi è in elenco dal 2025.

31.10.2026 — **Misure di sicurezza di base operative**
18 mesi dalla comunicazione ACN di inserimento.

DA NOV 2026 — **ACN passa alla vigilanza**
Dall'accompagnamento alle verifiche.

NOTIFICA INCIDENTI
24h · 72h · 1 mese
Pre-notifica, notifica con prima valutazione, relazione finale.

QUANTE MISURE
37 / 43
Misure di base per soggetti importanti ed essenziali.

SANZIONI MASSIME
2% · 1,4%
Del fatturato mondiale, o 10 e 7 milioni di euro.

Il termine esatto decorre dalla comunicazione ACN ricevuta e va ricalcolato per ogni organizzazione. Chi è entrato in elenco nel 2026 ha tempo fino al 31 luglio 2027.

Fonti: D.Lgs. 138/2024; Determinazioni ACN 379907/2025 e 127434/2026; ICT Security Magazine, agg. 22 settembre 2026. Il contenuto non costituisce consulenza legale.

// 10 · CHECKLIST

10 mosse per riprenderti il tempo.

01 **Misura il rischio con un numero**
Sai dove sei esposto e puoi spiegarlo al vertice in una riga.
HiCompliance

02 **Copri la notte e i festivi**
Monitoraggio e risposta 24/7: l'88% del ransomware arriva fuori orario.
HiDetect

03 **Blinda le identità**
Autenticazione a più fattori: due incidenti su tre partono da un'identità compromessa.
HiMFA

04 **Conserva i log abbastanza a lungo**
Sette giorni non bastano per ricostruire un attacco.
HiLog

05 **Chiudi le vulnerabilità**
Patch regolari e test per sapere dove si entra.
HiPatch · Pen Test

06 **Compra tempo con i backup**
Backup frequenti, isolati e ripristino provato: ogni ora di frequenza è un'ora di lavoro salvata.
HiBackup

07 **Allena le persone**
Il phishing è sempre più credibile: simulazioni e formazione continua.
HiPhish Threat · Formazione

08 **Doppia verifica sui pagamenti**
Una telefonata di conferma sopra soglia ferma le frodi via email.
Processo interno

09 **Una sola vista d'insieme**
Meno dashboard, meno password, più controllo.
HiSolution Console

10 **Se sei NIS2, documenta tutto**
Ricalcola il tuo termine e per ogni misura: responsabile, scadenza, prova.
Compliance NIS2

Per ogni mossa è indicato il servizio HiSolution che può accompagnarti. I dati citati vengono dal Sophos Active Adversary Report 2026.

// METODOLOGIA E FONTI

Come abbiamo costruito questo report.

Il questionario

Compilato dai partecipanti al Cybersecurity Summit 2026 di HiSolution, Firenze, 25 settembre 2026. Domande su preoccupazione principale, incidenti recenti, misurazione del rischio, scadenze ICT, valutazione di altri fornitori, budget IT, urgenza del cambiamento e servizi di interesse.

Base: 25 questionari validi. Le percentuali sono arrotondate all'unità; per la misurazione del rischio la base è di 24 risposte, per la preoccupazione principale di 21 risposte aperte, raggruppate per tema da HiSolution. Il campione non è statistico: rappresenta i partecipanti all'evento, in prevalenza responsabili IT e figure tecniche.

La tavola rotonda

Interventi di Etruria Retail, Sistemi ICT e DPV, riportati in sintesi.

Le fonti esterne

Clusit, comunicato "Dati dal Rapporto Clusit 2026", 11 marzo 2026: attacchi noti, andati a segno e di particolare gravità.

Sophos, Active Adversary Report 2026: 661 casi di Incident Response e MDR gestiti tra novembre 2024 e ottobre 2025 in 70 Paesi.

D.Lgs. 4 settembre 2024, n. 138 e **Determinazioni ACN** 379907/2025, 127434/2026, 127437/2026, 155238/2026.

ICT Security Magazine, "NIS2: la mappa completa degli adempimenti da qui a ottobre 2026", aggiornamento del 22 settembre 2026.

I riferimenti normativi sono aggiornati a settembre 2026. Il report ha scopo informativo e non costituisce consulenza legale.

> la domanda giusta_

La domanda non è se sarai attaccato.
È quanto tempo ti servirà per accorgertene.

Misura il tuo rischio

Un assessment per sapere dove sei esposto, cosa manca e in che ordine intervenire.

Prova HiSolution Console

Una demo con un nostro specialista, anche online.

hisolution.it

hi solution
better ICT for every business

HISOLUTION SRL · VECCHIANO (PI)
MANAGED SERVICE PROVIDER