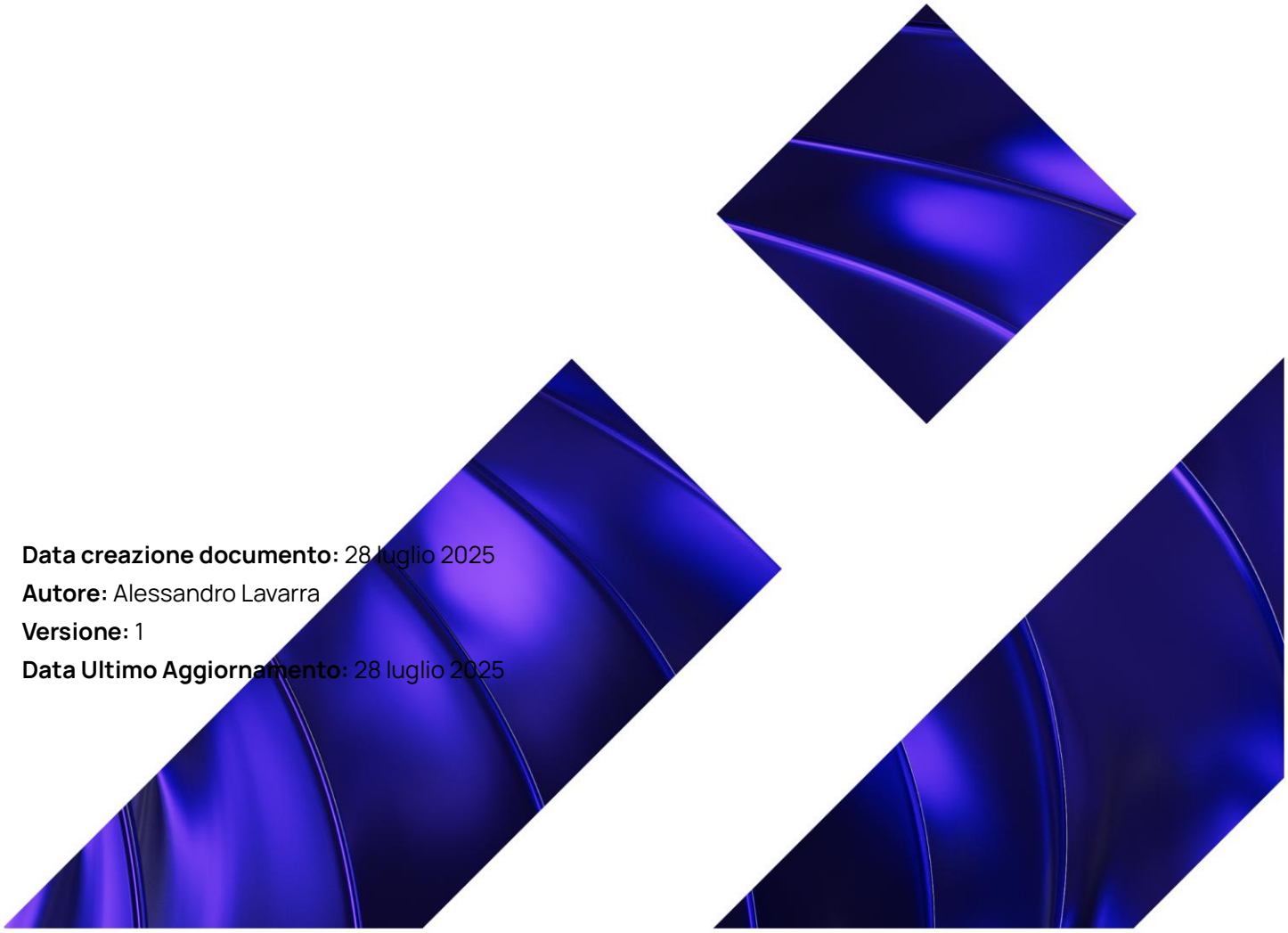
# Platform based security

## Sicurezza informatica: meno tecnici, più piattaforme intelligenti



**Data creazione documento:** 28 luglio 2025
**Autore:** Alessandro Lavarra
**Versione:** 1
**Data Ultimo Aggiornamento:** 28 luglio 2025

Se la tua strategia di cyber security si basa su un team di analisti “accaventiquattro” e su una stratificazione di strumenti puntuali, preparati: stai perdendo la battaglia.

Sì, perché i primi sono introvabili e i secondi generano più punti ciechi che informazioni utili. L'approccio dei SOC più tradizionali “human based” è obsoleto, soprattutto in un'Italia alle prese con la cronica carenza di competenze specialistiche e anche i system integrator nostrani, troppo spesso, non sono particolarmente evoluti in strategia. Il mercato della cyber security in Italia soffre di una certa variabilità nella sua maturità. Molti fino a ieri si occupavano di applicativi, genericamente di infrastrutture o, nel migliore dei casi, di reti con però un'indole più da installatore che da designer o progettista.

La risposta? Ovviamente arriva dalla tecnologia, ed è l'approccio alla cyber security “platform based”.

Questo richiede un cambio di paradigma e un saltino culturale che, come sappiamo, non è mai facile da compiere. La sicurezza by platform è una strategia che automatizza e semplifica le operation di cyber security e le centralizza in una unica o in poche piattaforme, appunto, permettendo anche alle realtà con risorse limitate, statisticamente tutte, di difendersi efficacemente.

**Sgombriamo subito il campo dal primo pregiudizio: il prezzo.**

Dal punto di vista degli investimenti è solo apparentemente più cara, perché ci presenta così, a freddo, dei costi diretti alti ma, contando anche i servizi specialistici che si devono associare, evita costi indiretti molto più consistenti e, soprattutto, alza significativamente la sicurezza e lascia spazio per i percorsi di miglioramento continuo.

In tutti i casi in cui l'abbiamo adottata con decisione, poi, abbiamo registrato nel tempo un tale miglioramento della postura di sicurezza da permettere la dismissione di vari servizi e strumenti di contorno alle attività principali con benefici enormi e cessazione di costi diretti e complessità tecniche e amministrative.

In questo articolo vedremo come la rivoluzione tecnologica delle platform può liberarti dalla frustrazione della ricerca infinita di talenti o dall'illusione di risolvere il problema esternalizzando carichi di lavoro su organizzazioni che soffrono della stessa mancanza di risorse di cui soffri tu.

**Il Problema numero uno: carenza di talenti.**

Alla domanda “quali sono le tre top sfide o minacce per la tua organizzazione IT?”, rivolta da Gartner a un pool di CIO, le risposte sono state: Skill insufficienti, scarsa maturità tecnologica e gestione del debito tecnico.

Questo fenomeno è tipico di tutto il settore IT da molti anni. Le tecnologie evolvono freneticamente e non è possibile tenere il passo. Le aziende fanno fatica ad inserire personale qualificato e le qualifiche invecchiano molto rapidamente.

Oggi una delle più gravi carenze è proprio nel settore della cybersecurity a causa dell'aumento delle minacce, dell'instabilità geopolitica e della scarsa maturità di tutto il settore.

I dipartimenti HR di aziende tradizionali, manifatturiere, GDO, logistica che siano, non sono attrezzati per lavorare efficacemente con il settore del digital, il cui mercato del lavoro ha logiche molto diverse sui compensi e sull'organizzazione del lavoro.

Le persone che si assumono vengono sostanzialmente sottratte all'impresa vicina e il gioco è sempre a somma zero e, in un settore così dinamico, non è certo lungimirante fondare la propria strategia a medio termine su una o due persone, perché alla fine queste sono le dimensioni dei team.

Le difficoltà dei system integrator italiani nell'integrare soluzioni complesse e il mercato della tecnologia che cresce con una curva a cui è impossibile tenere testa, fanno il resto.

Ci sono 3.500 (qualche analista dice 7.000) soluzioni di cyber security censite nel mercato. Soluzioni che risolvono problemi puntuali e specifici, magari in modo brillante e molto efficace, ma questa proliferazione, lungi dal garantire una maggiore sicurezza, spesso crea sovrapposizioni e catene ingestibili.

**La maturità dei fornitori.**

Non si può pensare di agire andando all'inseguimento di ogni singola novità e stratificando sottoscrizioni su sottoscrizioni. Novità nate in paesi e per mercati con una cultura cyber molto più matura della nostra e con organizzazioni con team articolati e formati, oltre che potere di spesa in cyber security maggiore.

Pretendere che i system integrator ancora legati ad un modello di sicurezza perimetrale, ci guidino efficacemente in questa complessità è un'illusione pericolosa. Startup e vendor cercano di metterti in casa prodotti con un ciclo di valutazione strettissimo: presentazione, PoC, offerta irripetibile nel trimestre.

E poi l'orchestrazione con le altre soluzioni? Il fine tuning? La corretta strategia di impiego nel tuo ecosistema chi la implementa? Spesso il partner che ti veicola la soluzione è stato coinvolto dal vendor "by opportunity" o magari ha i requisiti minimi: un commerciale e un tecnico certificati che, alla fine, al massimo fanno il compitino, senza una reale comprensione strategica dell'intero quadro.

Questa è la situazione tipica, e aggrava ulteriormente la frammentazione e la mancanza di una visione unitaria della sicurezza.

Quindi ti trovi con una rete piatta o scarsamente segmentata, magari residui di apparati unmanaged in qualche branch o magazzino appena acquisito o nei punti vendita, un'architettura firewall tradizionale per la sicurezza perimetrale ma con ormai tre quarti delle applicazioni as a service o in cloud e più utenti in mobilità che in ufficio.

Aggiungiamo che oggi fornitori, consulenti e manutentori hanno esteso i confini di che cosa è un tuo utente e cosa un ospite e non puoi più risolvere confinandoli in una guest dietro a un captive portal. Assumiamo che hai superato l'era dell'antivirus e hai un buon EDR per gli asset gestiti e però un po' di punti aperti per quelli non gestiti OT e IoT.

Finalmente, tra notizie di cronaca e normative europee, si sbloccano dei budget per la sicurezza. Che cosa fare? Chi ha già investito in quella direzione e vuole difendere i propri alti margini ti suggerirá che la strada è impegnare un gruzzoletto per un SIEM e un relativo SOC as a service dove squadre di analisti presidieranno e analizzeranno ogni cosa H24.

Ma l'occhio umano, per quanto esperto, ha i suoi tempi di reazione, il patching sui sistemi ha tempi morti informaticamente eterni, la tua organizzazione ha branch produttivi o uffici commerciali che fanno il giro del sole e la tua postura generale ha troppi punti scoperti.

Da un phishing andato a buon fine può partire un path di attacco che dura giorni e fa il giro dei tuoi sistemi raccogliendo dati e aprendo backdoor senza matchare i modelli del SIEM. Ahimè, capita: la superficie di attacco è ampia, i sistemi scollegati, l'intero impianto è sbilanciato in difesa, l'unico giocatore di qualità è il portiere e a forza di dai un goal entra e nel caso di un breach ne basta uno.

Per noi questo scenario tipico significa partire al rovescio e trascurare l'evoluzione delle tecnologie.

**Soluzione: back to basic e sicurezza "Platform Based"**

Le due azioni sinergiche da intraprendere sono una decisa aderenza ai fondamentali della sicurezza, affiancata dall'adozione strategica di soluzioni "Platform Based" che ne amplificano l'efficacia.

Implementare rigorosamente azioni strutturali "scolastiche" e cruciali, come una segmentazione e segregazione della rete ben definite, per limitare la propagazione degli attacchi e una restrizione degli accessi granulare basata su criteri contestuali come la geolocalizzazione e la postura del dispositivo (device posture) per ridurre la superficie d'attacco. Queste misure, sebbene fondamentali, sono spesso trascurate.

È qui entra in gioco la potenza delle piattaforme ad ampio spettro come le soluzioni SASE (Secure Access Service Edge) e le piattaforme UEBA (User and Entity Behavior Analytics). Soluzioni come CATO Networks (SASE) offrono una gestione unificata e sicura della rete, integrando funzionalità di sicurezza perimetrale, controllo degli accessi (ZTNA), CASB e DLP, semplificando radicalmente la gestione in un'unica piattaforma.

A complemento, soprattutto per organizzazioni con dati e risorse di rete molto distribuite e miste, on-premise e in cloud, le piattaforme UEBA come Darktrace forniscono visibilità avanzata su tutti gli eventi di rete e le attività degli utenti, andando oltre la semplice analisi delle firme e rilevando anomalie sottili. Darktrace si distingue inoltre per le sue capacità di "Autonomous Response", agendo in tempo reale per contenere gli attacchi anche in scenari complessi.

L'adozione di queste piattaforme porta benefici di sicurezza immediati, semplifica l'architettura e fornisce una miniera di informazioni preziose che possono guidare e potenziare le azioni di hardening e miglioramento continuo. La visibilità centralizzata e l'analisi comportamentale avanzata offerte da SASE e UEBA permettono di identificare le aree della rete più vulnerabili, i comportamenti anomali e le lacune nelle politiche di accesso, consentendo di implementare le remediation.

**Più efficienza, visibilità e tempo per la prevenzione**

La combinazione di un ritorno ai fondamentali della sicurezza potenziato dalla visibilità e dalle capacità di automazione offerte dalle piattaforme come SASE (CATO Networks) e UEBA con capacità di response (Darktrace) rappresenta la strategia vincente per costruire una cybersecurity che sia più un percorso virtuoso che non un rimedio momentaneo, anche in un contesto di risorse limitate.

Centralizzazione e automazione alzano la trasparenza degli ecosistemi di rete e sicurezza e riducono il carico di lavoro e la dipendenza da personale numeroso. Un buon servizio gestito garantisce la piena adozione degli strumenti e la capacità di valutare gli insight generati da questa visibilità. Il ruolo del partner tecnico qui è molto importante per individuare gli ambiti di miglioramento e prioritizzare le attività, sempre tenendo conto della proporzione tra costi e impatti, in modo da mettere immediatamente in campo tutte le azioni a basso effort e alto beneficio possibili.

**Il ruolo trasformato: l'umano al servizio della strategia non dell'emergenza**:

L'aumento della visibilità permette di identificare, analizzare e rispondere alle minacce più rapidamente e restituisce tempo per il passaggio cruciale dalla reaction alla prevention.

Intelligenza artificiale e machine learning completano il quadro perché, integrati nelle piattaforme, garantiscono analisi di volumi di informazioni impensabili per team umani e reazione in tempo reale, sgravando i team dalle attività più stressanti (i team di cyber security soffrono di burnout a causa dell'alto volume ingestibile di informazioni e correlazioni a cui sono esposti).

Liberando gli analisti dalle attività ripetitive e a basso valore aggiunto, i partner di cyber security possono spostare il focus sulle attività di analisi degli insight, definizione delle policy e miglioramento continuo, potenziare il threat hunting proattivo con strumenti con visibilità più ampia e lasciare al personale interno la possibilità di concentrare le poche risorse su decisioni strategiche di alto livello.

**Come scegliere la piattaforma giusta per il contesto italiano**:

In Italia la statistica ci dice che siamo esposti a minacce informatiche più che altri paesi e che molta strada è da fare. Il mio consiglio è trovare partner non orientati alla vendita di tecnologie ma alla creazione di percorsi di semplificazione, miglioramento continuo e piena adozione di piattaforme abilitanti.

L'approccio "platform based" non è solo una tendenza, ma una soluzione rapida per la cybersecurity italiana: restituisce efficienza, riduce la dipendenza da competenze sempre meno disponibili, lascia spazio per la sicurezza proattiva.

Gli elementi chiave di una piattaforma sono: consolidamento, integrazione nativa e ampia copertura funzionale, visibilità centralizzata, automazione, correlazione e analisi facilitata, gestione unificata delle policy, scalabilità.

Il mio consiglio è: informatevi, dedicate del tempo per valutare e sperimentare piattaforme che garantiscono convergenza (come CATO Networks, la piattaforma SASE per eccellenza che copre esigenze di rete, di accesso, di sicurezza perimetrale, CASB, DLP, XDR) o copertura di ampi use case come la suite di Darktrace che spazia dall'analisi capillare degli eventi di rete alla protezione in chiave "comportamentale" delle e-mail.

È ora di pensare ad un altro modello che non sia SIEM + SOC as a Service implementati on top ad architetture di sicurezza e rete lacunose. La tecnologia e un partner con competenze verticali possono supportare una strategia più efficiente ed elegante.