paloalto NETWORKS | CORTEX XSIAM®

Guida all'acquisto di XSIAM:

come trasformare il SOC per l'era dell'IA

SOMMARIO

Colmare le lacune: prevenzione proattiva nei SOC moderni 3

Trasformare le operazioni di sicurezza 6

Valutare Cortex XSIAM per la tua organizzazione 9

Preparare le operazioni di sicurezza ad affrontare il futuro 12

Migliorare le metriche più importanti del SOC 14

Cortex XSIAM è la soluzione giusta per te? 16

COLMARE LE LACUNE:
PREVENZIONE PROATTIVA NEI SOC MODERNI

Con la sua rapida evoluzione, lo scenario della sicurezza informatica pone le organizzazioni davanti a sfide senza precedenti. Oggi gli autori di minacce presentano un grado di sofisticatezza maggiore, grazie all'impiego di tecniche avanzate e dell'IA per eludere le misure di sicurezza tradizionali. In quanto professionista della sicurezza, probabilmente starai già riscontrando in prima persona il profondo cambiamento nelle necessità del centro operativo di sicurezza (SOC). I vecchi metodi di rilevamento e risposta alle minacce non sono più sufficienti in un momento storico in cui le violazioni possono avvenire nel giro di qualche ora, rispetto alle 24 ore di solo un anno fa[1], e i requisiti normativi si fanno sempre più rigorosi.

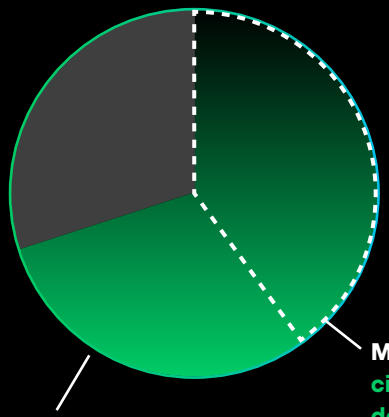
In molti casi i team addetti alla sicurezza riescono a ricostruire l'accaduto soltanto una volta che la violazione si è verificata, individuando la modalità di compromissione del sistema, i sistemi interessati e i dati esfiltrati. Sorge quindi spontanea una domanda: se disponi delle informazioni per comprendere un incidente dopo la violazione, perché non riesci a prevenirla o bloccarla prima che avvenga? Questa lacuna tra analisi post-incidente e prevenzione proattiva è il fulcro dell'evoluzione delle esigenze dei SOC moderni.

Le soluzioni tradizionali di gestione delle informazioni e degli eventi di sicurezza (SIEM), che in passato erano alla base di molte operazioni di sicurezza, faticano a tenere il passo, a causa di configurazioni complesse, integrazioni dispendiose in termini di tempo, ingenti investimenti in tecniche di rilevamento e una quantità spropositata di avvisi.

Le tattiche di multiestorsione continuano ad aumentare

Il panorama degli attacchi ransomware ha subito un'evoluzione significativa negli ultimi anni, con una prevalenza sempre maggiore di tattiche di multiestorsione.

Furto di dati nei casi di ransomware:[2]



Metà del 2021:
circa solo il 40% dei casi

Fine del 2022:
circa il 70% dei casi

75% di aumento

dei furti di dati avvenuti durante attacchi ransomware in un periodo di 18 mesi.

1. *Report globale di Unit 42 sulla risposta agli incidenti 2025*, Palo Alto Networks, 25 febbraio 2025.
2. *Report di Unit 42 su ransomware ed estorsioni 2023*, Unit 42 di Palo Alto Networks, 28 settembre 2025.

Queste sfide possono far sentire sopraffatto il tuo team e rendere vulnerabile la tua organizzazione. La natura isolata di molti strumenti di sicurezza comporta flussi di lavoro inefficienti, un aumento del carico cognitivo per gli analisti e potenziali sviste sulle minacce critiche. Inoltre, la mancanza di integrazione tra le funzioni di sicurezza proattiva (come la gestione delle vulnerabilità) e gli strumenti reattivi ostacola il rilevamento delle minacce in tempo reale e ritarda la risposta agli incidenti, mettendo a rischio l'organizzazione.

Per di più, il prevalente ricorso a regole di correlazione statiche e tecniche di rilevamento estese, aggravato dall'enorme volume di dati, rende difficile l'identificazione di rapporti rilevanti tra gli eventi di sicurezza in tutto l'ambiente e dà quindi origine a una difesa insufficiente dalle minacce. In molti casi questo comporta una visualizzazione degli avvisi come punti dati scollegati e il team SOC si trova costretto ad affrontare attività di correlazione manuali, che comportano un'elevata percentuale di falsi positivi. Questo processo non integrato intacca l'efficacia dell'infrastruttura di sicurezza e mette in luce la necessità di metodologie di rilevamento delle minacce più avanzate e adattive.

Impatto quantificato: il ROI reale della trasformazione del SOC

Da uno studio Total Economic Impact™ di Forrester® Consulting commissionato da Palo Alto Networks sulle distribuzioni di Cortex XSIAM® è emerso che un'organizzazione composita ha ottenuto risultati business-critical misurabili:[3]

257% | $ 5,6 milioni | <6 mesi

ROI a tre anni | Valore attuale netto | Periodo di ammortamento

85% | 70% | $ 3,1 milioni

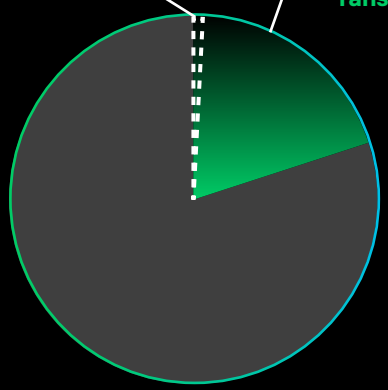
Riduzione nel MTTR | Meno incidenti che richiedono indagini sul SOC | Risparmio ottenuto con il consolidamento degli strumenti

Le tattiche di multiestorsione continuano ad aumentare (continua)

Uso della persecuzione come tattica di estorsione:[4]

Metà del 2021: presente in meno dell'1% dei casi

Fine del 2022: presente in circa il 20% dei casi di ransomware



1.900% di aumento

nell'uso di tattiche persecutorie da parte di gruppi ransomware nello stesso periodo.

Queste statistiche evidenziano un importante cambio di passo nelle strategie ransomware: gli autori di minacce utilizzano sempre più spesso punti di pressione multipli per le estorsioni ai danni delle loro vittime. Il drastico aumento dei furti di dati e delle tattiche persecutorie sottolinea la sempre maggiore complessità e gravità delle minacce di ransomware cui le organizzazioni devono far fronte.

Le vittime pagano per riottenere l'accesso	Gli hacker minacciano di divulgare i dati rubati	Gli attacchi DDoS impediscono l'accesso ai siti Web pubblici	Vengono contattati clienti, partner aziendali e organi di stampa
Crittografia	**Furto di dati**	**DDoS**	**Persecuzione**

3. *Il Total Economic Impact™ di Cortex XSIAM di Palo Alto Networks*, Forrester Consulting, 13 ottobre 2025.
4. Unit 42 Palo Alto Networks, *2023 Report di Unit 42 su ransomware ed estorsioni.*

TRASFORMARE LE OPERAZIONI DI SICUREZZA

La trasformazione del SOC ha inizio con Cortex® Extended Data Lake (XDL), una base pronta per l'IA e destinata alle SecOps piattaformizzate. Agendo come un'unica fonte di verità per il tuo SOC, Cortex XDL integra, normalizza e arricchisce tutti i tuoi dati di sicurezza.

Partendo da queste basi, Cortex XSIAM consolida le funzioni di sicurezza critiche in un'unica piattaforma trasformativa, che include:

- Gestione delle informazioni e degli eventi di sicurezza (SIEM)
- Rilevamento e risposta degli endpoint (EDR)
- Rilevamento e risposta estesi (XDR)
- Orchestrazione, automazione e risposta alla sicurezza (SOAR)
- Gestione della superficie di attacco (ASM)
- Analisi del comportamento di utenti ed entità (UEBA)
- Rilevamento e risposta alle minacce all'identità (ITDR)
- Rilevamento e risposta cloud (CDR)
- Gestione della threat intelligence (TIM)
- Piattaforma di threat intelligence (TIP)

> XSIAM ci offre una maggiore visibilità e indagini più rapide. L'onboarding ottimale dei dati e la configurazione automatizzata sono funzioni rivoluzionarie.
>
> - Mike Dembek
> Architetto di rete, Boyne Resorts

Figura 1. XSIAM Command Center

Cortex XSIAM trasforma le operazioni di sicurezza centralizzando i dati, la difesa basata sull'IA e l'automazione in un'unica piattaforma. Lo XSIAM Command Center mostra una serie di origini di dati, che vanno dagli endpoint e dalla rete all'identità, al cloud, alla telemetria delle applicazioni e molto altro ancora, fornendo al contempo informazioni sullo stato e sul volume dell'acquisizione dei dati.

Grazie a questo consolidamento non è più necessario passare da uno strumento all'altro e ciò consente di ridurre la complessità e migliorare l'efficienza del team. Invece di doverti destreggiare tra varie console e affrontare problemi di integrazione, puoi gestire tutte le operazioni di sicurezza da un'unica piattaforma coerente progettata appositamente per le esigenze del SOC moderno.

Le organizzazioni che distribuiscono Cortex XSIAM hanno ottenuto risultati misurabili. Secondo lo studio sul Total Economic Impact™ di Forrester, un'organizzazione composita ha ottenuto, **entro il terzo anno, una riduzione dell'85% del volume di avvisi che richiedono un'attenzione di livello 1 da parte del SOC**, risparmiando oltre **$ 930.000** in valutazione e operazioni di livello 1. Inoltre, le organizzazioni hanno **ottenuto una riduzione del 70% dei casi che richiedono un'indagine SecOps**, con una **diminuzione dell'85% del tempo medio di risoluzione (MTTR) entro il terzo anno**, per un valore superiore a **$ 1,2 milioni di dollari**.[5]

Le funzionalità di automazione e IA agentica semplificati di XSIAM cambiano radicalmente la modalità di gestione degli incidenti di sicurezza. La piattaforma automatizza l'integrazione, l'analisi e la valutazione dei dati, riducendo notevolmente le attività manuali necessarie agli analisti. Questa automazione consente al team di concentrarsi su ciò che conta davvero, ovvero affrontare incidenti ad alta priorità che richiedono competenze umane.

I modelli di intelligenza artificiale pronti all'uso di XSIAM superano i metodi tradizionali, collegando gli eventi tra le varie origini di dati e offrendo una panoramica completa degli incidenti e dei rischi in un'unica posizione. Grazie al raggruppamento degli avvisi e alla classificazione degli incidenti basata sull'intelligenza artificiale, XSIAM connette senza interruzioni gli eventi a bassa affidabilità, convertendoli in incidenti ad alta affidabilità. La definizione delle priorità si basa sul rischio complessivo, consentendo al team di sicurezza di ottimizzare le proprie attività.

La piattaforma XSIAM garantisce anche la raccolta continua, l'aggregazione e la normalizzazione dei dati non elaborati, non limitandosi ai soli avvisi. Ciò consente al team SOC di condurre facilmente indagini avanzate, per identificare e risolvere le minacce in modo più rapido ed efficace.

Con Cortex XSIAM, noterai un netto miglioramento dell'esperienza e della produttività degli analisti. L'approccio basato sull'IA della piattaforma consente di limitare le informazioni inutili, con la riduzione dell'alert fatigue e la possibilità per il team di concentrarsi sulle minacce critiche. In questo modo gli analisti dedicano meno tempo al triage degli avvisi di routine e più tempo alla propria crescita professionale, con lo svolgimento di indagini approfondite e la ricerca proattiva delle minacce.

Inoltre, l'approccio basato sull'automazione di XSIAM accelera la risoluzione degli incidenti. Con centinaia di pacchetti di contenuti collaudati e testati in Cortex Marketplace, oltre al supporto nativo per server e client MCP, puoi connetterti facilmente all'intero ecosistema di sicurezza per integrare le informazioni e coordinare la risposta. Automatizzando le attività che in precedenza venivano svolte manualmente, l'automazione integrata riduce il tempo e l'impegno necessari per la risposta agli incidenti o la gestione dei rischi, come le esposizioni della superficie di attacco.

Inoltre, puoi aggiungere, personalizzare o modificare le automazioni in base alle tue esigenze specifiche. I playbook possono essere pianificati, eseguiti on-demand o attivati automaticamente dagli avvisi per assicurare una risposta e riduzione dei rischi tempestive.

Quando è il momento di indagare sulle minacce, Cortex Agentic Assistant mette a tua disposizione una forza lavoro di agenti di IA per affrontare qualsiasi sfida di sicurezza. Integrato in XSIAM, si avvale degli agenti di Cortex AgentiX™ per pianificare ed eseguire flussi di lavoro avanzati, convertendo le attività manuali ripetitive in azioni immediate e qualificate. Il tuo team ottiene indicazioni dettagliate e contestualizzate con controlli integrati, che consentono loro di agire più rapidamente, rispondere con decisione e proteggere la tua azienda.

Cortex AgentiX fornisce agenti di IA basati su utenti tipo e fondati su competenze reali per moltiplicare la forza di ogni componente del tuo team. Facendo leva su un'esperienza di leadership ultradecennale nell'automazione della sicurezza, arricchiti da informazioni globali sulle minacce e alimentati da 1,2 miliardi di playbook eseguiti, questi agenti svolgono una funzione di esperti di sicurezza sempre attivi. Gli analisti utilizzano semplicemente prompt in linguaggio naturale e gli agenti pianificano ed eseguono all'istante compiti complessi e in più fasi con rapidità e precisione.

5. Forrester Consulting, *Il Total Economic Impact™*.

VALUTARE CORTEX XSIAM PER LA TUA ORGANIZZAZIONE

Quando valuti Cortex XSIAM per la tua organizzazione, è fondamentale prendere in considerazione diversi fattori chiave. Innanzitutto, valuta i tuoi strumenti di sicurezza attuali e la loro complessità. Se sei in difficoltà con la proliferazione degli strumenti e i flussi di lavoro non integrati tra funzionalità di sicurezza proattive e reattive, l'approccio consolidato di XSIAM potrebbe offrire vantaggi importanti. Considera il tempo che il tuo team dedica al passaggio da uno strumento all'altro e alla correlazione manuale delle informazioni. La piattaforma unificata di XSIAM riduce drasticamente questo carico e migliora l'efficienza del team.

Considera quindi il volume e la varietà dei dati che la tua organizzazione gestisce. XSIAM offre risultati eccellenti in termini di elaborazione e analisi di grandi quantità di dati diversificati, il che lo rende la soluzione ideale per le organizzazioni con ambienti complessi e ricchi di dati. Se ti trovi a gestire un mix di dati on-premise e cloud, faticando a ottenere una visione olistica del tuo livello di sicurezza, la capacità di XSIAM di acquisire e analizzare i dati da varie origini potrebbe essere una vera e propria rivoluzione.

Se svolgi le tue attività in ambienti cloud o ibridi, l'architettura cloud-native e la visibilità completa di XSIAM sulle risorse cloud e on-premise potrebbero migliorare in modo significativo le operazioni di sicurezza. Molte organizzazioni sostengono che gli strumenti di sicurezza tradizionali fanno fatica a fornire una visibilità e una protezione adeguate negli ambienti cloud. XSIAM estende il SOC al cloud, garantendo operazioni di sicurezza e visibilità unificate nell'intera infrastruttura.

Infine, riesamina i requisiti di conformità, un altro fattore di fondamentale importanza. Le solide funzionalità di reporting e l'analisi completa dei dati di XSIAM possono aiutarti a soddisfare in modo più puntuale vari standard normativi. Considera il tempo che attualmente il tuo team dedica al reporting della conformità e come XSIAM potrebbe semplificare questo processo.

Rispetto alla SIEM tradizionale e ad altre piattaforme di sicurezza, XSIAM offre funzionalità migliorate di rilevamento delle minacce con il suo approccio basato sull'intelligenza artificiale. È probabile che tu riscontri una riduzione della complessità operativa e potenziali risparmi significativi grazie agli strumenti consolidati e al miglioramento dell'efficienza. Nella valutazione del ROI, non considerare soltanto i costi diretti, ma anche il valore del tempo in più a disposizione degli analisti e del miglioramento del livello di sicurezza. Pensa quanto tempo in meno impiegherebbe il tuo team per rilevare e rispondere alle minacce con le funzionalità automatizzate di triage e risposta di XSIAM.

Lo studio Total Economic Impact™ di Forrester Consulting ha documentato risultati finanziari reali. Dalla ricerca è emerso che le organizzazioni hanno ottenuto un **ROI del 257% in tre anni** con un **periodo di ammortamento inferiore a sei mesi**. Come riportato nello studio da un vicepresidente della sicurezza globale: "Il tempo medio necessario per rilevare e risolvere i problemi è diminuito di oltre l'80%. Ciò che prima richiedeva quattro ore per essere rilevato e due ore per essere risolto, ora richiede in totale 40-50 minuti."[6]

> “Cortex XSIAM ha trasformato le nostre operazioni di sicurezza in un modo che la nostra SIEM precedente non era in grado di fare. XSIAM ha introdotto automazione e orchestrazione nei flussi di rilevamento, indagine e risposta e per LOLC è stato un enorme miglioramento in termini di produttività e profilo di sicurezza.
>
> - Prasanna Siriwardena
> Direttore informatico, LOLC Holdings PLC

6. Forrester Consulting, *Il Total Economic Impact™*.

Scopri gli ulteriori miglioramenti offerti da XSIAM rispetto alle soluzioni solo SIEM

Risparmio di tempo: SIEM tradizionale e XSIAM a confronto

SIEM XSIAM

Sviluppo del rilevamento delle minacce

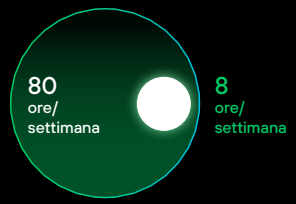
Processi continui per creare avvisi che si adattino a un panorama delle minacce in continua evoluzione.

100
ore/settimana risparmiate

La maggior parte delle attività di sviluppo per il rilevamento delle minacce è stata affidata in outsourcing al team di ricerca XSIAM.

Ottimizzazione degli avvisi

Processi continui per migliorare gli avvisi sulla base della fedeltà in passato.

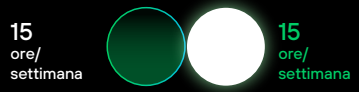


72
ore/settimana risparmiate

L'ottimizzazione degli avvisi degli endpoint è stata esternalizzata al team di ricerca XSIAM.

Manutenzione di sistema

Analisi dei registri, applicazione di patch al server ecc.



Nessuna variazione

Analisi

Creazione di avvisi avanzati che prendono in considerazione statistiche complesse e l'apprendimento automatico.

SIEM

[Lacune nelle funzionalità] Richiede un pacchetto add-on e un modello BYOML. La normalizzazione è difficile.

XSIAM

[Nuova funzionalità] XIAM ha automatizzato la creazione di una base e gli avvisi anonimi attraverso le statistiche e l'apprendimento automatico.

Risultati che fanno risparmiare tempo:

4,5 FTE

Riduzione impegno totale

Figura 2. risparmio di tempo tra SIEM tradizionale e XSIAM

Prima di adottare XSIAM, valuta la preparazione della tua organizzazione alle operazioni di sicurezza basate sull'IA. Considera le competenze del tuo team e i processi attualmente in uso e preparati a un cambio di approccio alle operazioni di sicurezza.

XSIAM può migliorare in modo significativo le operazioni di sicurezza, ma potrebbe richiedere delle modifiche del metodo di lavoro del team. Considera gli aspetti riguardanti la formazione e la gestione dei cambiamenti in caso di adozione di una nuova piattaforma basata sull'IA.

PREPARARE LE OPERAZIONI DI SICUREZZA AD AFFRONTARE IL FUTURO

Cortex XSIAM ha un ruolo cruciale nell'evoluzione dei paradigmi di sicurezza come Zero Trust, Secure Access Service Edge (SASE) e Security Service Edge (SSE). La sua visibilità completa e le funzionalità di analisi avanzate sono perfettamente allineate a questi approcci moderni alla sicurezza, consentendoti di ottenere operazioni di sicurezza a prova di futuro. Nella fase di transizione a un'architettura Zero Trust, XSIAM fornisce informazioni approfondite sul comportamento di utenti ed entità e può aiutarti a implementare e mantenere un modello Zero Trust affidabile.

La piattaforma unifica la risposta reattiva agli incidenti con la gestione proattiva del livello di sicurezza. Per risolvere i problemi legati alle due principali aree di rischio per le aziende, la soluzione fornisce:

- **Cortex Exposure Management:** riduce i falsi allarmi delle vulnerabilità fino al 99% utilizzando la definizione delle priorità basata sull'IA e la correzione automatizzata sia nell'azienda che nel cloud. Questo approccio dirompente si concentra sulle vulnerabilità con exploit attivi utilizzati come armi e nessun controllo compensativo, consentendoti di dare priorità allo 0,01% delle minacce più pericolose.
- **Cortex Email Analytics:** blocca i tentativi di phishing e gli attacchi tramite e-mail avanzati ricorrendo alla combinazione di analisi basati su LLM e funzioni di rilevamento e risposta leader del settore. Poiché le e-mail rimangono il principale strumento di comunicazione (si prevede di raggiungere i 5 miliardi di utenti entro il 2030[7]) e l'obiettivo primario degli attacchi informatici, questo sistema rimuove automaticamente le e-mail dannose, disabilita gli account compromessi e isola gli endpoint colpiti in tempo reale.

Man mano che la tua organizzazione cresce e le minacce evolvono, la scalabilità di XSIAM consente di gestire volumi sempre maggiori di dati e adattarsi alle nuove tipologie di minacce. I rilevatori e i modelli di intelligenza artificiale della piattaforma vengono aggiornati continuamente, fornendoti le più recenti funzionalità di threat intelligence e rilevamento delle minacce, senza che il team debba effettuare aggiornamenti manuali. Questo garantisce una protezione costante dalle minacce più recenti, senza dover ricorrere di continuo all'ottimizzazione e all'aggiornamento manuale degli strumenti di sicurezza.

XSIAM apprende dalle azioni manuali degli analisti e fornisce suggerimenti per le future automazioni, incrementandone la capacità di risolvere automaticamente gli incidenti e migliorando l'efficienza e l'accuratezza nel tempo, al fine di potenziare ogni giorno il livello di sicurezza tuo e della tua organizzazione.

XSIAM sfrutta modelli di dati di apprendimento automatico maturi e specifici per la sicurezza, che standardizzano e raggruppano automaticamente elevate quantità di dati provenienti da varie origini per rilevare le minacce alla sicurezza. Questi modelli sono costruiti sulla base del comportamento appreso da decine di migliaia di ambienti, agevolando la distinzione tra comportamenti anomali e comportamenti dannosi. Ciò riduce notevolmente i falsi positivi e migliora le capacità di rilevamento e prevenzione, bloccando gli attacchi prima che si trasformino in incidenti di sicurezza.

Inoltre, con la funzionalità BYOML (Bring Your Own ML) di XSIAM puoi integrare i tuoi strumenti di apprendimento automatico nella piattaforma, in modo da sfruttarli per eseguire la ricerca delle minacce utilizzando dati centralizzati e standardizzati in XSIAM, migliorando ulteriormente la capacità di rilevamento e risposta alle minacce sofisticate.

Impatto finanziario del consolidamento

Secondo il *Total Economic Impact™ condotto da Forrester Consulting su Cortex XSIAM di Palo Alto Networks*:[8]

$ 3,1 milioni
risparmiati eliminando oltre 20 strumenti legacy (su un periodo totale di 3 anni)

$ 2,2 milioni
di valore da un livello di sicurezza migliorato del 60%

$ 5,6 milioni
di valore attuale netto su 3 anni

Con l'adozione di XSIAM, risolvi le sfide di sicurezza di oggi e prepari la tua organizzazione a soddisfare le esigenze di sicurezza informatica di domani. Questo approccio lungimirante può offrirti fiducia nelle tue capacità di proteggere l'organizzazione in un panorama di minacce in continua evoluzione. Man mano che emergono nuove tipologie di minacce e l'infrastruttura IT della tua organizzazione deve evolversi per gestirle, l'approccio flessibile e basato sull'IA di XSIAM assicura che le tue operazioni di sicurezza possano adattarsi e rispondere in modo efficace.

XSIAM consente un miglioramento quotidiano dei team SOC e del livello di sicurezza dell'organizzazione.

L'aspetto forse più importante è che XSIAM offre un miglioramento continuo grazie all'IA e all'apprendimento automatico. La piattaforma ottimizza con regolarità le funzionalità di rilevamento e risposta sulla base dei nuovi dati e delle tecniche di attacco emergenti. Aumenta così l'efficacia delle operazioni di sicurezza nel tempo, con l'adattamento alle nuove minacce e ai nuovi schemi senza dover ricorrere a un'ottimizzazione manuale costante.

7. *Email Statistics Report 2025-2030*, cloudHQ, 24 aprile, 2025.
8. Forrester Consulting, *Il Total Economic Impact™*.

MIGLIORARE LE METRICHE PIÙ IMPORTANTI DEL SOC

Cortex XSIAM offre un approccio rivoluzionario per ridurre il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR), migliorando notevolmente le operazioni di sicurezza. Grazie agli strumenti avanzati di apprendimento automatico e intelligenza artificiale, XSIAM automatizza le attività monotone di integrazione e analisi dei dati, per consentire al team di identificare le minacce quasi in tempo reale. In questo modo puoi individuare le potenziali violazioni in tempi mai visti prima, spesso sorprendendo i malintenzionati prima ancora che possano causare danni importanti all'organizzazione.

Ma il rilevamento è solo metà dell'opera. L'approccio fondato sull'automazione di XSIAM accelera la risposta agli incidenti, trasformando le ore di indagini manuali in pochi minuti di attività automatizzate. Immagina un team SOC non più sommerso di attività di triage manuale o che non perde più tempo prezioso nella correlazione di dati provenienti da varie origini. Il raggruppamento intelligente degli avvisi e la classificazione degli incidenti basati su IA di XSIAM consentono agli analisti di concentrarsi su ciò che iù conta.

Il nostro approccio unificato alla sicurezza reattiva e proattiva ti consente non solo di accelerare la risposta agli incidenti, ma anche di evitare che molti di essi si verifichino. Grazie all'integrazione di Exposure Management e Email Analytics direttamente nella piattaforma SOC, XSIAM affronta due dei vettori di attacco più comuni basandosi sugli stessi dati unificati, sull'IA e sull'automazione.

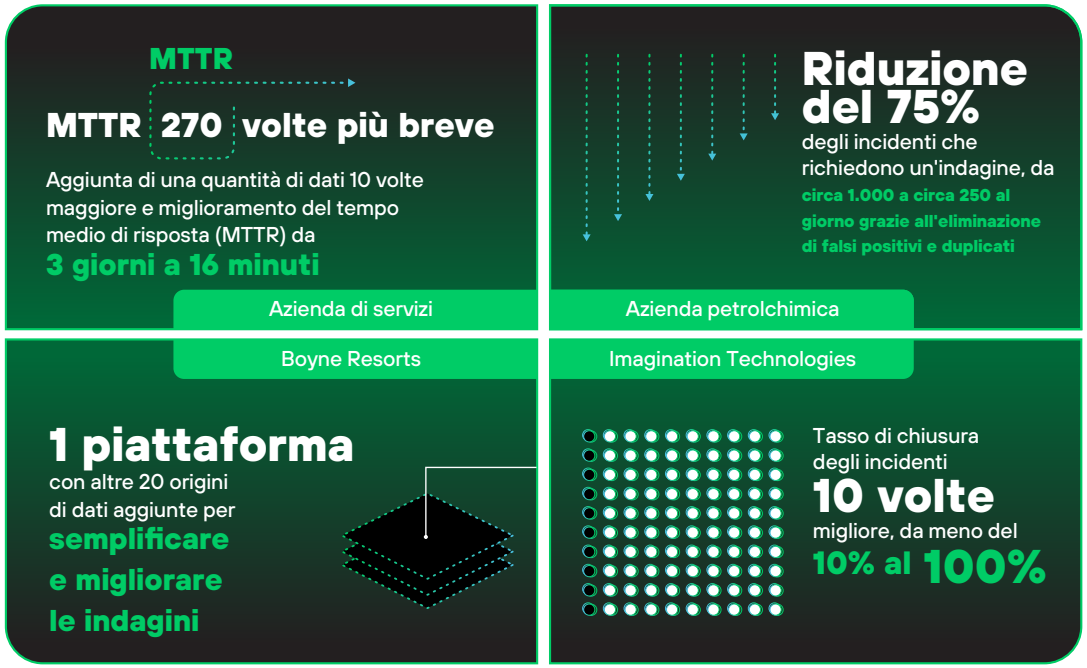


Figura 3. Esempi dei notevoli miglioramenti ottenuti dai clienti che utilizzano XSIAM

L'uso da parte del tuo team di playbook avanzati e agenti Cortex AgentiX che consentono interventi tempestivi e decisivi contro le minacce ti offrirà una drastica riduzione dell'MTTR. Soprattutto, XSIAM apprende e si adatta continuamente al tuo ambiente, migliorando progressivamente il tuo livello di sicurezza. Man mano che affronti minacce nuove ed emergenti, i modelli di IA all'avanguardia di XSIAM si evolvono, tenendoti sempre un passo avanti rispetto ai potenziali avversari.

In questo modo migliori l'MTTD e l'MTTR di oggi e al tempo stesso prepari le operazioni di sicurezza alle sfide di domani. Con Cortex XSIAM puoi affrontare con fiducia il panorama complesso della sicurezza informatica, con la certezza di un'ottimizzazione continua delle metriche più importanti del SOC per proteggere le risorse più preziose della tua organizzazione.

Questi miglioramenti emergono in modo evidente dalle ricerche. Secondo il direttore delle SecOps di un rivenditore specializzato, gli avvisi sono diminuiti da **25.000 a 4.500 a trimestre**. Lo studio ha attestato che, per l'organizzazione composita basata sui clienti intervistati, la distribuzione ha richiesto **tre FTE in due mesi**, con solo **0,5 FTE per la manutenzione annuale continua**.[9]

> “XSIAM integra diverse funzioni in una sola piattaforma unificata e rappresenta per noi la prossima frontiera nel passaggio a un SOC di nuova generazione. Con XSIAM, possiamo aspettarci un aumento dell'automazione e una maggiore responsabilizzazione del nostro team addetto alle operazioni informatiche.
>
> – Rob Jillson
> Responsabile della sicurezza informatica, Resolution Life Australasia

9. Forrester Consulting, *Il Total Economic Impact™*.

CORTEX XSIAM È LA SOLUZIONE GIUSTA PER TE?

1. **Attuali sfide del SOC**
   - ☐ Sei in difficoltà con le configurazioni complesse della SIEM attuale?
   - ☐ Sei alle prese con integrazioni tra gli strumenti di sicurezza che ti rubano molto tempo?
   - ☐ Il tuo team è sommerso da un volume elevato di avvisi?
   - ☐ Hai flussi di lavoro inefficienti a causa degli strumenti di sicurezza separati?
   - ☐ Il collegamento tra le funzioni di sicurezza proattive e la risposta reattiva agli incidenti è discontinuo?

2. **Rilevamento e risposta alle minacce**
   - ☐ Fai eccessivo affidamento su regole di correlazione statiche?
   - ☐ Hai bisogno di migliorare il rilevamento delle minacce in tempo reale?
   - ☐ Il processo di risposta agli incidenti subisce ritardi causati dalla mancanza di integrazione?
   - ☐ L'elevata percentuale di falsi positivi è difficile da gestire?

3. **Gestione dei dati**
   - ☐ Gestisci grandi volumi di dati di sicurezza diversificati?
   - ☐ Ti trovi a gestire un mix di dati on-premise e cloud?
   - ☐ Hai bisogno di funzionalità migliori per la normalizzazione e la correlazione dei dati?

4. **Esigenze in termini di IA e automazione**
   - ☐ Vuoi utilizzare l'IA per migliorare il rilevamento delle minacce?
   - ☐ Vuoi automatizzare le attività di sicurezza di routine?
   - ☐ La riduzione delle attività manuali nella valutazione degli incidenti è una priorità per te?
   - ☐ Devi definire la priorità delle vulnerabilità basate sull'IA per limitare le informazioni inutili?

5. **Requisiti rispetto a una piattaforma unificata**
   - ☐ Hai bisogno di consolidare più funzioni di sicurezza, come SIEM, EDR, XDR, SOAR, gestione delle vulnerabilità e protezione della posta elettronica?
   - ☐ Vuoi gestire le operazioni di sicurezza da un'unica piattaforma?
   - ☐ Vuoi colmare il divario tra la sicurezza proattiva e reattiva?

6. **Ambiente cloud e ibrido**
   - ☐ Stai operando in ambienti cloud o ibridi?
   - ☐ Hai bisogno di una migliore visibilità sulle risorse on-premise e cloud?

7. **Conformità e reporting**
   - ☐ Hai bisogno di semplificare i processi di generazione dei report di conformità?
   - ☐ Sei alla ricerca di analisi dei dati più complete per gli standard normativi?

8. **Scalabilità**
   - ☐ La tua organizzazione è in crescita e richiede, pertanto, la gestione di volumi sempre maggiori di dati?
   - ☐ Hai bisogno di una soluzione in grado di adattarsi alle minacce in evoluzione?

9. **Analisi avanzata**
   - ☐ Ti interessano il raggruppamento degli avvisi e la classificazione degli incidenti basati su IA?
   - ☐ Hai bisogno di una migliore correlazione degli eventi tra le varie origini di dati?
   - ☐ Vuoi utilizzare l'IA per dare priorità alle vulnerabilità più critiche?

10. **Preparazione del team**
    - ☐ Il tuo team è pronto ad adattarsi alle operazioni di sicurezza basate su IA?
    - ☐ Sei disponibile a investire nella formazione su una nuova piattaforma avanzata?

11. **Preparazione al futuro**
    - ☐ Stai passando a modelli di sicurezza Zero Trust, SASE o SSE?
    - ☐ Hai bisogno di una soluzione che migliori costantemente grazie all'intelligenza artificiale e all'apprendimento automatico?

12. **Integrazione personalizzata dell'apprendimento automatico**
    - ☐ Vuoi integrare i tuoi strumenti di apprendimento automatico?

13. **Gestione delle e-mail e delle vulnerabilità**
    - ☐ Hai bisogno di una protezione migliore contro le minacce e-mail avanzate?
    - ☐ Hai difficoltà a gestire i backlog e la definizione delle priorità delle vulnerabilità?
    - ☐ La correzione automatizzata delle vulnerabilità critiche sarebbe vantaggiosa per te?

Se hai risposto "**sì**" alla maggior parte di queste domande, in particolare per quanto riguarda le sfide e gli obiettivi di sicurezza specifici della tua organizzazione, Cortex XSIAM è la soluzione adatta al tuo SOC.

Inizia subito

Scopri come Cortex XSIAM può aiutare te e la tua organizzazione a semplificare le operazioni, bloccare le minacce su vasta scala e accelerare la risoluzione degli incidenti oggi e in futuro.

CONTATTACI →

Informazioni su Cortex XSIAM

Cortex XSIAM è la piattaforma delle operazioni di sicurezza basata sull'intelligenza artificiale per il SOC moderno, che sfrutta la potenza dell'IA per semplificare le operazioni di sicurezza, bloccare le minacce su larga scala e velocizzare la correzione degli incidenti. Riduci i rischi e la complessità delle operazioni centralizzando più prodotti in un'unica e coerente piattaforma, creata appositamente per le operazioni di sicurezza.

Cortex XSIAM unifica le migliori funzioni per le operazioni di sicurezza, tra cui EDR, XDR, SOAR, ASM, UEBA, TIP e SIEM. Inoltre, centralizza tutti i dati sulla sicurezza e utilizza modelli di dati di apprendimento automatico appositamente progettati. Grazie a XSIAM, puoi automatizzare l'integrazione dei dati, l'analisi e le misure di risposta, consentendo agli analisti di concentrarsi sugli incidenti di maggior rilievo. Per maggiori informazioni su Cortex, visita la pagina www.paloaltonetworks.com/cortex/cortex-xsiam.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054 (Stati Uniti)

Telefono	+1.408.753.4000
Vendite	+1.866.320.4788
Assistenza	+1.866.898.9087

cortex_ebook_cortex-xsiam-buyers-guide_102125