CROWDSTRIKE

Checklist per RFP del Next-Gen SIEM

Fai evolvere il tuo security operations center per ottenere risultati di sicurezza superiori, ridurre la complessità e abbattere i costi

La chiave per modernizzare il tuo SOC

Le soluzioni SIEM legacy hanno fallito con il SOC. Sono spesso troppo lente, complesse e costose e molte sono state progettate per un'epoca in cui i volumi di dati, la velocità degli avversari e la sofisticazione degli attacchi erano una frazione minima di quello che sono oggi. Man mano che la tua organizzazione diventa più complessa, proliferano anche le fonti di dati, costringendo il team a dedicare più tempo e risorse alla configurazione, alla manutenzione e al tentativo di estrarre dal SIEM risultati di sicurezza efficaci piuttosto che concentrarsi sulle compromissioni da bloccare.

Se hai deciso di intraprendere il percorso per evolvere il tuo security operations center, hai bisogno di una soluzione che sia immensamente più veloce, più facile da implementare e più conveniente rispetto ai SIEM legacy. Questo nuovo approccio unifica tutte le operazioni di rilevamento, indagine e risposta alle minacce in un'unica piattaforma IA e cloud native per un livello di efficienza e velocità ineguagliabile. Abbattendo i silos e consolidando gli strumenti, potrai ridurre drasticamente la complessità e i costi. In più, potrai superare una delle sfide più difficili dei SIEM legacy, ovvero l'inserimento dati, perché i tuoi dati di sicurezza importanti sono già presenti nella piattaforma. CrowdStrike Falcon® Next-Gen SIEM è stato creato per consentirti di ottenere una visibilità completa e aiutarti a superare le sfide associate ai SIEM legacy. CrowdStrike ha sviluppato Falcon Next-Gen SIEM per mantenere la sua promessa: fermare le compromissioni.

La checklist per le "Request for proposal" (RFP) ti offre la possibilità di sfruttare il punto di vista di CrowdStrike riguardo al Next-Gen SIEM e ti aiuta a identificare il miglior fornitore o partner in grado di risolvere le tue sfide di sicurezza, in linea con i tuoi obiettivi. La checklist è il giusto punto di partenza per avviare il tuo processo di valutazione, comparare i vari fornitori e prendere decisioni informate per evolvere il tuo SOC.

Checklist dei requisiti

Architettura SIEM e deployment

- [ ] Modello di deployment Software-as-a-Service (SaaS) per contenere i costi e semplificare gli aggiornamenti
- [ ] Una vera architettura cloud native, non un processo lift-and-shift, per garantire la scalabilità
- [ ] Opzioni di deployment multi-tenancy per organizzazioni complesse e geograficamente distribuite
- [ ] Controllo granulare degli accessi basato sui ruoli (RBAC), per limitare le autorizzazioni e l'accesso
- [ ] Processo di migrazione fluido con tempistiche ragionevoli, aspettative chiare e opzioni di configurazione personalizzate
- [ ] Opzioni di formazione flessibili per aiutare il tuo team a crescere, acquisire sicurezza e padronanza nell'utilizzo del nuovo deployment SIEM
- [ ] Manutenzione semplificata e aggiornamenti tempestivi per proteggerti dalle minacce emergenti e risolvere qualsiasi tipo di problema
- [ ] Servizi di supporto affidabili con personale qualificato e accordi sui livelli di servizio (SLA)
- [ ] Rilascio di nuove release con cadenza regolare per migliorare efficienza e user experience

Onboarding, elaborazione e gestione dei dati

- [ ] Sviluppato sui dati degli endpoint altamente affidabili ed esteso ai dati di terze parti per una visibilità completa
- [ ] Varietà di connettori dati out-of-the-box disponibili e pronti all'uso tra i domini IT e di sicurezza
- [ ] Data Parser immediatamente disponibili per garantire l'accesso e la leggibilità, per un'analisi più rapida
- [ ] HTTP event collector (HEC) per semplificare l'onboarding di fonti di dati personalizzate e sfruttare i parser per normalizzare la data ingestion
- [ ] Gestione unificata della flotta, per consentire agli agenti di raccolta log di monitorare facilmente l'acquisizione e l'integrità dei dati
- [ ] Solide funzionalità API per condividere i dati con le applicazioni, in modo semplice e sicuro

- [ ] Supporto delle pipeline di dati per spostare i dati in modo efficiente e indirizzarli nel SIEM
- [ ] Data ingestion su scala petabyte per eseguire rapidamente l'onboarding di nuovi dati nel SIEM
- [ ] Data ingestion non indicizzata per velocizzare il recupero dei dati e utilizzare in modo efficiente le risorse disponibili
- [ ] Normalizzazione dei dati per diversi campi di informazioni e formati di dati, per velocizzare le analisi
- [ ] Parser pronti all'uso, per convertire i dati in un formato adatto a strutturare i dati
- [ ] Componenti nativi dell'ecosistema, per ridurre gli attriti durante l'interoperabilità tra strumenti suddivisi in silos, ad esempio:
    - [ ] Extended Detection and Response (XDR)
    - [ ] Endpoint detection and response (EDR)
    - [ ] Threat intelligence
    - [ ] Global Cloud-native Application Protection Platform (CNAPP)
    - [ ] Identity Threat Detection and Response (ITDR)
    - [ ] Next-generation antivirus (NGAV)
    - [ ] Data protection
    - [ ] Exposure Management
- [ ] Latenza inferiore al secondo per elaborare i log, avvisare in caso di minaccia e rendere i dati utilizzabili in tempo reale
- [ ] Libertà di accedere ai tuoi dati quando, dove e in qualsiasi modo tu abbia bisogno
- [ ] Più opzioni di ricerca, dalla ricerca a testo libero alla ricerca RegEx avanzata dei patterns
- [ ] Ricerca fulminea e scalabile tra dataset di grandi dimensioni e volumi dati in continua crescita
- [ ] Unico linguaggio di query multipiattaforma user-friendly, per superare la barriera di ingresso
- [ ] Dashboard delle metriche, per valutare lo stato del sistema, gestire i dati e prevedere l'utilizzo

Analisi

- [ ] Regole di correlazione sensibili e altamente attendibili, disponibili e pronte all'uso, continuamente testate e facili da regolare
- [ ] Ampia gamma di rilevamenti pronti all'uso in vari domini di sicurezza, tra i quali:
  - [ ] Endpoint
  - [ ] Cloud
  - [ ] Identità
  - [ ] Rete
  - [ ] Email
  - [ ] Applicazioni
- [ ] Supporto per la condivisione aperta dei rilevamenti, come le regole Sigma, YARA e Snort
- [ ] Utilizzo dell'intelligenza artificiale generativa (GenAI) per consentire agli analisti di qualsiasi livello di fare di più con meno, rispondendo alle domande in un linguaggio semplice
- [ ] Analisi basata su GenAI, per setacciare grandi volumi di dati e rilevare anomalie
- [ ] Analisi comportamentale che sfrutta l'analisi statistica e il machine learning (ML), come l'analisi comportamentale di utenti ed entità (UEBA)
- [ ] Rilevamento delle anomalie basato sull'IA per identificare gli utenti anomali, creando gruppi di peer dinamici
- [ ] Arricchimento contestuale con TTP dal framework MITRE ATT&CK®
- [ ] Possibilità di applicare tag e di arricchire i dati analizzati con threat intelligence di alta qualità, fornendo indicatori di compromissione (IOC) con classificazione di attendibilità, contesto del malware, informazioni sulla campagna e nomi degli avversari
- [ ] Mappatura della copertura di rilevamento rispetto al framework MITRE ATT&CK, per azioni più rapide
- [ ] Dashboard per visualizzazioni di casi d'uso comuni, pronte all'uso per una visibilità immediata

- [ ] Dashboard personalizzabili e viste preferenziali che possono basarsi su qualsiasi query per analizzare e visualizzare i dati
- [ ] Inclusione di query documentate di threat hunting, regolarmente aggiornate ed estratte dalle informazioni più recenti di threat intelligence, per identificare gli avversari più sofisticati
- [ ] Workflow delle analisi, per rendere operativi i processi di threat hunting e ridurre gli sforzi manuali necessari per creare, convalidare, ottimizzare e rendere operative le indagini sulle minacce
- [ ] Test di terze parti sulle funzionalità di protezione e rilevamento, come valutazioni di MITRE Engenuity ATT&CK e SE Labs, per risultati superiori

Indagine e risposta all'incidente

- [ ] Assegnazione della priorità agli alert in base alla severità e al raggruppamento, per passare al setaccio ogni cosa in modo più rapido
- [ ] Gestione completa degli incidenti per creare incidenti da un rilevamento o da un gruppo di rilevamenti correlati, mantenendo organizzate le informazioni.
- [ ] Funzionalità di orchestrazione, automazione e risposta (SOAR) completamente integrate, incluse come standard
- [ ] Strumento intuitivo e senza codice per la creazione dei workflow, per automatizzare qualsiasi caso d'uso ed espletare tutte le attività
- [ ] Numerosi modelli di workflow pronti all'uso, per i casi d'uso più diffusi e con opzioni personalizzabili
- [ ] Automazione dei workflow attivata in base a eventi o rilevamenti, pianificati o su richiesta
- [ ] Ampio ecosistema di integrazioni tra domini di sicurezza e strumenti IT, come gli strumenti di gestione dei servizi IT (ITSM)
- [ ] Integrazione bidirezionale tra SIEM e SOAR, per garantire la condivisione delle informazioni
- [ ] Capacità di automatizzare le attività investigative di routine, come le correlazioni e la raccolta di dati
- [ ] Integrazione con threat intelligence leader di settore, focalizzata sugli avversari, per generare report sulle minacce, profili delle minacce, report tecnici, sandboxing di malware e report giornalieri sull'indicatore di compromissione (IOC) per le minacce emergenti
- [ ] Threat intelligence che copre oltre 230 avversari distinti, in base all'analisi di trilioni di eventi di endpoint a settimana

- [ ] Visualizzazioni avanzate delle indagini, come visualizzazioni grafiche per comprendere le relazioni tra entità e percorsi degli avversari e visualizzazioni in sequenza temporale per comprendere la progressione di un attacco
- [ ] Collaborazione in tempo reale tra analisti che possono condividere e documentare i risultati
- [ ] Possibilità di inviare notifiche tramite il metodo di comunicazione preferito, come email o Slack
- [ ] Massima flessibilità nell'automatizzare qualsiasi caso d'uso, con molteplici azioni di risposta predefinite
- [ ] Stretta integrazione di agenti di rilevamento e risposta agli endpoint, per eseguire qualsiasi azione sugli endpoint, come isolamento della rete, quarantena, risposta in tempo reale e altro ancora
- [ ] Integrazione con qualsiasi API basata su HTTP, per creare azioni in low-code o full-code
- [ ] Accesso ai dati storici, per abilitare casi d'uso di threat hunting su grandi volumi di dati
- [ ] Possibilità di creare applicazioni personalizzate per implementare più casi d'uso e colmare le lacune dei prodotti
- [ ] Possibilità di personalizzare la piattaforma esistente per le operazioni di sicurezza con una piattaforma applicativa low-code (LCAP) integrata e appositamente progettata
- [ ] Motore di indagine basato su GenAI che consente agli analisti di generare riepiloghi degli incidenti in un linguaggio semplice, con consigli sui passaggi successivi da intraprendere

Conservazione dei dati, privacy e compliance

- [ ] Opzioni flessibili per la conservazione dei dati a lungo termine, per dati sempre accessibili e costantemente ad alta velocità
- [ ] Funzionalità di reportistica on-demand, programmate per verifiche e compliance, con possibilità di mantenere un sistema di sicurezza dei record
- [ ] Funzionalità di mascheramento e offuscamento per soddisfare i requisiti di privacy e protezione

Servizi

- [ ] Copertura MDR da parte di esperti, 24 ore su 24, 7 giorni su 7, sui vettori di attacco più importanti: endpoint, identità e dati di terze parti, come e-mail, rilevamento e risposta della rete (NDR), firewall e altro ancora
- [ ] Team di analisti della sicurezza certificati con conoscenze tecnologiche approfondite
- [ ] Threat intelligence integrata per un contesto di attacco completo e gli indicatori di compromissione (IOC) più recenti
- [ ] Threat hunting condotto da personale per rilevare le più sofisticate attività di spionaggio dell'avversario
- [ ] Risoluzione chirurgica delle minacce in una vera modalità end-to-end, inclusa la pulizia completa fino allo stato originale, senza costose reinstallazioni o tempi di inattività
- [ ] Garanzia di prevenzione delle compromissioni senza inutili ostacoli burocratici, per coprire i costi delle compromissioni in caso si verifichino in ambienti protetti
- [ ] Efficacia della copertura di rilevamento degli attacchi come indicato dalle valutazioni MITRE ATT&CK
- [ ] Riconoscimento da parte di analisti e del settore per la convalida della protezione guidata da esperti ed eseguita tramite servizi
- [ ] Servizi operativi e di implementazione per accelerare la configurazione e l'ottimizzazione
- [ ] Ampio ecosistema di fornitori di servizi per un ulteriore supporto strategico

Prezzi

- [ ] Prezzi trasparenti e di facile comprensione per consentire la prevedibilità nella pianificazione
- [ ] Prezzi flessibili che si adattano ai crescenti volumi di dati senza sforare il budget

Profilo del fornitore

- [ ] Maturità della sicurezza informatica con convalida da parte di clienti e analisti
- [ ] Esperienza nella gestione di vari tipi di clienti che variano per dimensioni, regioni geografiche e settori, con i vantaggi dell'immunità della comunità
- [ ] Portafoglio di prodotti e servizi di sicurezza informatica strettamente integrato che favorisce l'innovazione dei prodotti, approfondisce le competenze e amplia le opzioni di offerta

- [ ] Visione a lungo termine per capitalizzare le tendenze del settore e una roadmap in rapido sviluppo per supportare l'esecuzione
- [ ] Riconoscimenti e certificazioni rilevanti da parte di società di analisi e del settore della sicurezza, inclusa la leadership in ambito threat intelligence, sicurezza degli endpoint, protezione del workload cloud, MDR e gestione delle vulnerabilità basata sul rischio

CrowdStrike sta guidando il futuro delle operazioni di sicurezza con IA nativa, offrendo una piattaforma SOC completa per aiutare i clienti a fermare le compromissioni, ottenere la compliance e risolvere le sfide di sicurezza di qualsiasi entità. Estendendo le funzionalità EDR, la threat intelligence e i servizi degli esperti del settore, Falcon Next-Gen SIEM offre visibilità e protezione complete.

Il tuo team avrà accesso immediato alle informazioni complete dei dati fondamentali di cui hai bisogno, già integrati. Un set di connettori dati, in continua crescita, libera tutta la potenza del tuo intero ecosistema, consentendoti di dedicare più tempo a debellare le minacce e meno tempo all'onboarding dei dati.

Costruito da zero attorno a una moderna esperienza di analisi della sicurezza, Falcon Next-Gen SIEM amplifica la velocità e l'efficienza dell'incident response in modo da poter sconfiggere rapidamente gli avversari e ridurre i costi del SOC.

Richiedi una demo
per osservare Falcon Next-Gen SIEM in azione

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della sicurezza informatica, ha ridefinito la sicurezza moderna con la piattaforma cloud native più avanzata al mondo per la protezione delle aree critiche del rischio aziendale: endpoint e workload cloud, identità e dati.

Con la tecnologia CrowdStrike Security Cloud e l'intelligenza artificiale di prima classe, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, le informazioni sulle minacce, lo spionaggio degli avversari in evoluzione e la telemetria arricchita proveniente da tutta l'azienda per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'élite e osservabilità prioritaria delle vulnerabilità.

Costruita appositamente nel cloud con un'architettura basata su un unico agent leggero, la piattaforma Falcon assicura un deployment rapido e scalabile, protezione e prestazioni superiori, complessità ridotta e un time-to-value immediato.

CrowdStrike: We stop breaches.