Proofpoint Managed SIEM

Rafforza la sicurezza del tuo ambiente Splunk

Vantaggi principali

- Miglior rilevamento per una visibilità approfondita - Gli indicatori di violazione provenienti dalla nostra threat intelligence sulle minacce emergenti ti permettono di identificare le minacce nascoste.
- Ricerca intelligente delle minacce per una risposta proattiva - Studiamo i comportamenti dei criminali informatici e cerchiamo prove della loro presenza nel tuo ambiente. Raccogliamo informazioni dettagliate sui fattori contestuali quali la portata dell'obiettivo, la cronologia e altri aspetti, per consentire una risposta e una correzione proattive.
- Monitoraggio e rilevamento 24 ore su 24, 7 giorni su 7 - Ottimizziamo rapidamente il tuo ambiente. Il nostro team di tracciamento delle minacce supporterà il tuo programma SIEM con monitoraggio costante e un rapido tempo medio per l'attività di remediation.
- Progettazione della sicurezza esperta - Il nostro team di progettazione è tra i migliori al mondo e garantisce l'efficienza del tuo ambiente Splunk.

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a mitigare le quattro principali categorie di rischi legati agli utenti.

Proofpoint Managed SIEM ti fornisce l'accesso a un team di esperti dedicati al rilevamento, analisi e neutralizzazione delle minacce. Questo servizio fornisce protezione avanzata contro le minacce agli ambienti Splunk. Ti permette di spostare parte del carico di lavoro associato alla gestione delle informazioni e degli eventi di sicurezza (SIEM) e acquisire capacità avanzate di tracciamento delle minacce.

Proofpoint Managed SIEM aiuta a semplificare le sfide quotidiane che i tuoi team IT e della sicurezza delle informazioni affrontano quando cercano di gestire grandi volumi di avvisi e risolverli rapidamente. Senza il nostro servizio, questi compiti possono risultare insormontabili. Il problema non fa che peggiorare con l'arrivo di nuove tecnologie di rilevamento e l'aumento del numero di avvisi che esse comportano. Questa situazione può portare a un calo di concentrazione a fronte di un elevato numero di allarmi, anche se i tuoi team seguono le best practice e i runbook e utilizzano gli strumenti e le analisi più recenti.

Semplifica le operazioni di sicurezza

I clienti di Splunk che utilizzano Proofpoint Managed SIEM godono di molteplici vantaggi, tra cui:

- **Rilevamento migliorato.** A differenza di altri servizi che si limitano a sfruttare gli avvisi forniti da altre soluzioni SIEM, Proofpoint Managed SIEM migliora il rilevamento grazie alla threat intelligence e agli indicatori di minaccia. Questo ci permette di identificare le minacce che altri servizi non rilevano.
- **Monitoraggio delle minacce e correlazione.** La nostra gamma di soluzioni di sicurezza si basa su numerosi vettori di rilevamento, un potente grafico delle minacce di oltre 1 bilione di nodi basato su machine learning e IA nonché un team di oltre 100 ricercatori delle minacce. L'ampiezza della nostra copertura ci permette non solo di rilevare le minacce, ma anche di correlare gli eventi che potrebbero sembrare scollegati.
- **Protezione contro le minacce 24 ore su 24 e 7 giorni su 7.** Il servizio Proofpoint Managed SIEM è reso disponibile da un team globale di professionisti della sicurezza e rilevamento delle minacce. I nostri esperti sono dislocati nei centri di operazioni della sicurezza dislocati in tutto il mondo. Identificano, assegnano le priorità e indagano sulle minacce per i nostri clienti 24 ore su 24.

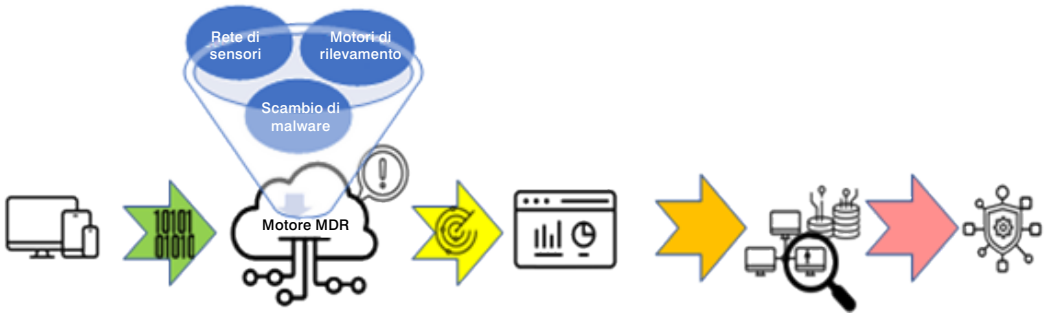

Figura 1. Le fonti inoltrano i log al motore MDR (Managed Detection and Response), che utilizza la threat intelligence di Proofpoint per creare avvisi ottimizzati. Il nostro team smista, analizza e assegna le priorità agli avvisi, effettua analisi correlazionali e traccia le minacce proattivamente per contenerle e neutralizzarle.

Arricchisci i log di Splunk grazie alla threat intelligence di Proofpoint

La threat intelligence di Proofpoint arricchisce i log della tua rete per identificare le minacce che potrebbero non essere state rilevate e creare nuovi avvisi Proofpoint. Una volta rilasciati gli avvisi, assegniamo le priorità e conduciamo ulteriori indagini. I dettagli delle minacce (utenti chiave, obiettivi ad alto valore e schemi d'attacco, ecc.) vengono identificati per facilitare la prioritizzazione e la neutralizzazione degli attacchi. Valutiamo le minacce per procedere al tracciamento delle minacce avanzate, quando necessario.

Il team Proofpoint utilizza un flusso di lavoro di approvazione semplificato per neutralizzare rapidamente le minacce attive. Questo flusso di lavoro contribuisce anche a liberare le risorse di sicurezza della tua azienda che possono così dedicarsi a progetti di sicurezza più importanti o strategici.

Ottimizzare il rilevamento delle minacce nella tua azienda

Proofpoint rafforza le funzionalità SIEM tradizionali grazie a un rilevamento avanzato basato su tecnologie e servizi all'avanguardia offrendo i seguenti vantaggi:

- **Esperienza ineguagliata e competenze proattive.** La threat intelligence di Proofpoint ci consente di offrirti una protezione proattiva. La nostra rete mondiale di sensori e il nostro team di analisti e ricercatori specializzati nelle minacce tracciano e correlano le minacce su diverse piattaforme. I nostri esperti sono anche lungimiranti e creano difese su misura per le tue esigenze, basate sulle best practice del settore e sugli aggiornamenti più recenti delle soluzioni Proofpoint.
- **Operazioni di sicurezza convenienti e costanti.** Assumere, formare e fidelizzare il personale di sicurezza è una sfida. È ancora più vero quando si tratta di conoscenze specialistiche come l'identificazione e la risposta agli incidenti. I nostri servizi gestiti ti danno accesso al nostro team di esperti, sempre a tua disposizione. In questo modo puoi ridurre al minimo il tempo, il denaro e le risorse da dedicare alle sfide legate al personale a livello locale.
- **Report regolari e informazioni di alto livello per la dirigenza.** Grazie ai nostri indicatori, hai a disposizione preziose informazioni sulle tendenze della sicurezza e puoi identificare le nuove direzioni della sicurezza nonché prendere decisioni informate.

Proofpoint Managed SIEM integra tutte queste funzionalità per fornire una difesa efficace. Il nostro team ti aiuta a garantire l'efficacia del tuo ambiente. Ottimizziamo inoltre la configurazione delle regole in Splunk per rilevare le minacce in modo preciso, per esempio implementando gli aggiornamenti, le patch e gli adeguamenti dei sistemi in base alle necessità. Combiniamo rilevamento avanzato, prioritizzazione, neutralizzazione delle minacce ad alta priorità e misure di correzione rapide. In breve, il nostro team offre i migliori servizi in termini di ingegneria della sicurezza. Lascia che ti aiutiamo a colmare le tue lacune di sicurezza e ridurre la tua superficie di attacco complessiva.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **proofpoint.com/it**.