splunk>

SCHEDA DEL PRODOTTO

App Splunk® Enterprise Security

Sicurezza basata su dati analitici e sul monitoraggio continuo contro le minacce alla sicurezza odierne

Come muoversi in uno scenario caratterizzato dalla dinamicità delle minacce

L'azienda moderna richiede tecnologie per la sicurezza che siano in grado di adattarsi alle minacce dinamiche odierne, alle tattiche degli avversari in continua evoluzione, alle minacce avanzate e alle mutevoli esigenze del business. Per sapersi muovere in questo nuovo scenario, gli analisti della sicurezza devono agire in fretta per poter ridurre i tempi di risposta alle minacce e prendere decisioni importanti per il business. Per superare tutte queste nuove sfide, i team della sicurezza devono disporre di funzionalità analitiche e di risposta contestuale alle violazioni, oltre ad essere in grado di implementare rapidamente le tecniche di rilevamento delle nuove minacce.

Una componente fondamentale di questo scenario dinamico è il fatto che gli aggressori hanno il tempo, le competenze e le risorse per creare scenari di attacco non rilevabili dai prodotti di sicurezza mirati e dai sistemi per la gestione delle informazioni e degli eventi di sicurezza (SIEM) a valle. Le loro azioni si nascondono in terabyte di dati generati dalle normali attività degli utenti. Gli autori di questi tipi di attacchi persistenti si sono resi conto che molti team addetti alla sicurezza non riescono a rilevare tali attacchi a causa di silos di dati presenti nell'organizzazione, di problemi di raccolta dei dati, di sfide a livello di scalabilità o per mancanza di funzionalità di analisi. I team addetti alla sicurezza possono fermare questi aggressori applicando l'analisi del contesto di rischio ai dati rilevanti ai fini della sicurezza in modo da analizzare l'attività delle minacce. Quando all'analisi si applicano i feed sull'intelligence delle minacce, gli analisti possono identificare minacce in precedenza sconosciute e abilitare la riduzione proattiva delle minacce. È possibile aggiungere ulteriore contesto da altre fonti di dati aziendali (ad es., i sistemi di gestione del tempo, i database HR, i database di asset) per rilevare e comprendere le minacce interne, incluse frodi e furti di proprietà intellettuale. La dinamicità delle minacce richiede che i team addetti alla sicurezza adottino le funzionalità di sicurezza basata su dati analitici in modo da allineare il piano di sicurezza al rischio aziendale.

Per rilevare le minacce avanzate e scoraggiare gli aggressori interni è necessario un approccio alla sicurezza basato sul rischio che può essere implementato solo tramite una piattaforma per l'intelligence di sicurezza che operi sui big data. Tale piattaforma deve saper raccogliere tutti i dati macchina e i dati di intelligence sulle diverse minacce esistenti ed essere poi in grado di correlare questi dati con qualsiasi dato macchina scelto dagli analisti. Queste funzionalità stimolano la creatività degli analisti della sicurezza, consentendo loro di sfruttare le visualizzazioni e utilizzare le analisi statistiche per individuare minacce sconosciute.

Definizione di sicurezza basata su dati analitici:

Il processo di rilevamento di relazioni tra tutti i dati significativi per la sicurezza, inclusi dati originati da infrastrutture IT, prodotti di sicurezza mirati e tutti i dati generati dalla macchine per adattarsi rapidamente a uno scenario di minacce in continua evoluzione.

L'app Splunk Enterprise Security

Che sia stata implementata per il monitoraggio continuo, per la risposta alle violazioni, per un SOC (security operations center) o per i dirigenti che hanno bisogno di avere un quadro del rischio di business, l'app Splunk Enterprise Security (ES) ti offre la flessibilità per personalizzare le viste in modo da adattarle alle specifiche esigenze. L'app Splunk Enterprise Security include funzioni quali l'acquisizione di dati della rete di tipo "point and click", un framework intelligence delle minacce facile da usare e correlazioni e soglie automodificanti. Queste funzionalità insieme ti consentono di monitorare le minacce note e sconosciute. I principali contenuti pronti all'uso includono:

Revisione e classificazione delle violazioni: inclusa nell'ambito di una funzionalità di revisione delle violazioni completa, la classificazione consente la riassegnazione in blocco di eventi e le modifiche allo stato e alla classificazione delle criticità. Inoltre tutte le attività degli analisti sono disponibili a scopi di audit

Report e metriche di sicurezza: sfrutta decine di report, dashboard e metriche pronti all'uso; qualsiasi risultato di ricerca può essere rappresentato sotto forma di grafici, dashboard o tabelle in modo da trasformare i dati grezzi non strutturati in dati analitici; esporta i dati grezzi in formato PDF o CSV

Analisi basata sul rischio: allinea il piano di sicurezza al tuo business individuando le relazioni e applicando un punteggio di rischio a qualsiasi dato, rivelando i fattori che hanno contribuito a tale punteggio; assegna in modo facile e rapido qualsiasi indicatore chiave di sicurezza o delle prestazioni a un evento per generare un punteggio di rischio tramite il Framework di rischio

Framework sull'intelligence delle minacce: integra, rimuovi i duplicati e assegna pesi ai feed sull'intelligence delle minacce (che siano essi aperti, proprietari o locali). Il processo di intelligence risulterà quindi semplificato e potrà diventare una componente chiave del tuo workflow delle operazioni di sicurezza

Editor di ricerca unificato: un'esperienza intuitiva e uniforme di creazione delle ricerche (incluse le ricerche guidate); per le ricerche di correlazione degli indicatori chiave di sicurezza o degli indicatori chiave delle prestazioni e per le visualizzazioni di indagini sull' identità e gli asset (vedere Figura 1)

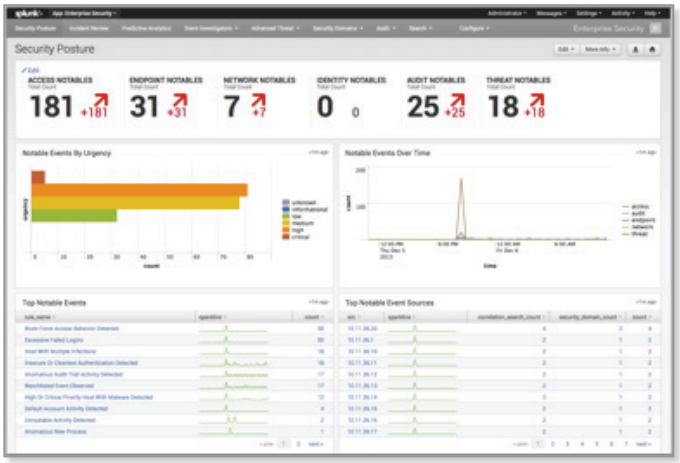

Figura 1. Enterprise Security 3.2 - Dashboard del piano di sicurezza

Analisi statistica: le dashboard preconfigurate consentono di individuare le anomalie nei dati relativi a eventi e protocolli mediante le soglie e le baseline in grado di autoconfigurarsi

Dashboard flessibili: crea il tuo portale di sicurezza personale in base al tuo ruolo relativamente a ciò che è importante per la tua organizzazione (vedere Figura 2); organizza e correla visivamente diverse fonti di dati in un'unica interfaccia utente per trovare le relazioni e comprendere meglio il contesto

Grazie alla raccolta indicizzata in base al tempo di qualsiasi dato, non è necessaria alcuna normalizzazione anticipata ed è possibile applicare uno schema di dati al momento della ricerca. Inoltre sono rimossi gli ostacoli che impediscono l'acquisizione e la visualizzazione dei dati dell'applicazione e dei dati operativi ai fini del contesto degli eventi di sicurezza. La piattaforma Splunk è in grado di acquisire dati strutturati e non strutturati da sistemi IT, sistemi di sicurezza, sistemi di produzione o da qualsiasi fonte di dati macchina e di visualizzare questi dati nel contesto della gestione delle modifiche e dell'accesso fisico per facilitare le operazioni di sicurezza. Splunk Enterprise e l'app Splunk Enterprise Security offrono una soluzione per l'intelligence di sicurezza unica, flessibile e scalabile che supera i limiti delle tecnologie SIEM tradizionali.

Panoramica dell'app Splunk Enterprise Security

Piano di sicurezza

Ottieni una libreria di widget relativi al piano di sicurezza in modo da inserirvi qualsiasi dashboard o creare facilmente le tue dashboard personali. Osserva gli eventi di sicurezza in base alla posizione, all'host, al source type, ai raggruppamenti di asset e all'area geografica. Gli indicatori chiave delle prestazioni offrono funzionalità di creazione di trend e monitoraggio in tempo reale del tuo piano di sicurezza.

Revisione e indagine sulle violazioni

L'app Splunk Enterprise Security supporta il drilldown dagli elementi grafici alle acquisizioni di dati grezzi e dati della rete, in modo da comprendere tutte le comunicazioni di rete. Le azioni di workflow uniche nel loro genere aumentano il processo di indagine per la sicurezza e consentono all'utente di incentrarsi su una singola informazione comune o su qualsiasi altro dato per sviluppare rapidamente il contesto della minaccia.

Protezione degli accessi

Semplifica il monitoraggio del controllo degli accessi, l'analisi delle eccezioni e i processi di audit per le applicazioni, i sistemi operativi e i sistemi di gestione dell'identità in tutta l'azienda. Soddisfa i requisiti di conformità e di computer forensic per tenere traccia degli utenti con privilegi elevati e dei tentativi di accesso a qualsiasi applicazione business critical.

Protezione degli endpoint

Aumenta l'efficacia dei prodotti di sicurezza degli endpoint quali Symantec™ Endpoint Protection, IBM® Proventia Desktop o McAfee® Endpoint Protection. Suddividi le minacce in base alle priorità e osserva i trend a lungo termine. La protezione degli endpoint include ricerche, report e una libreria di allarmi per malware, attività poco frequenti, utilizzo delle risorse e disponibilità.

Protezione della rete

Monitora e rileva gli eventi dai dispositivi di rete e di sicurezza in tutta l'organizzazione. Scopri le anomalie nei dati dei protocolli, firewall, router, DHCP, access point wireless, bilanciatori di carico, sensori per il rilevamento delle intrusioni e dispositivi per impedire la perdita di dati. Sfrutta le correlazioni, le ricerche, i report e le dashboard per monitorare e inviare allarmi sull'attività nella rete.

Centro asset/Centro identità

Capire dove risiedono gli asset, chi li controlla, il loro livello di criticità e chi dovrebbe accedere alle informazioni critiche sui sistemi consente di dividere per priorità gli eventi e le indagini di sicurezza. L'app sfrutta la capacità di Splunk di eseguire in tempo reale 'lookup' dei dati archiviati in un database di asset, in una active directory, in fogli di lavoro o in file CSV e utilizza le informazioni come contesto per gli eventi di sicurezza nei report e nelle dashboard.

Analisi del rischio

Identifica le origini e l'entità del rischio nel tuo ambiente e scopri i fattori che contribuiscono al comportamento di rischio. Utilizza i punteggi di rischio per scoprire attività insolite.

Audit della revisione delle violazioni

Per scopi di governance, audit e protezione dalle manomissioni, l'app Splunk Enterprise Security fornisce report su tutte le attività di sistema e degli utenti in modo da avere un audit trail completo. La piattaforma Splunk utilizza la firma dei dati per mantenere la catena di custodia e rilevare eventuali alterazioni ai dati originali di log e di eventi.

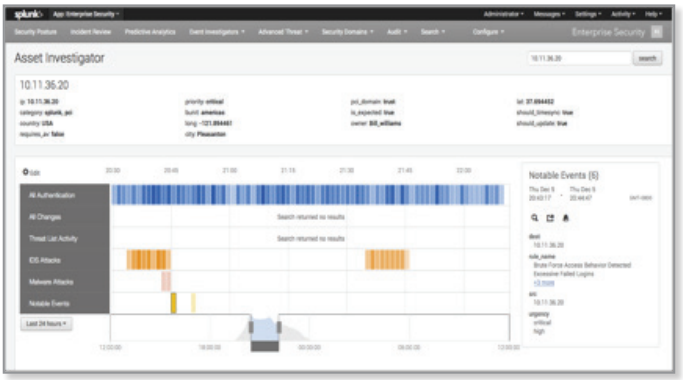

Figura 2. Security 3.2 - Investigatore di asset

Download gratuito

Scarica Splunk gratuitamente. Otterrai una licenza Splunk Enterprise 6 valida per 60 giorni e potrai indicizzare fino a 500 MB di dati al giorno. Entro 60 giorni avrai l'opzione di passare a una licenza gratuita perpetua o di acquistare una versione Enterprise contattando sales@splunk.com.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 apps.splunk.com

Art. n. FS-SPLUNK-AppEntSec-117-A4