SOLUTION NOTE

SOC INSIGHTS

Applica analisi basate sull'AI per trasformare grandi quantità di dati di intelligence su eventi, reti, ecosistemi e DNS in informazioni fruibili per aumentare l'efficienza delle SecOps

OSTACOLI ALL'EFFICIENZA DELLE SECOPS

Come per altre funzioni delle organizzazioni aziendali o governative, il moderno SOC fatica a fare di più con le risorse disponibili. Secondo il SANS 2023 SOC Survey[1], l'80% dei 10 principali ostacoli che impediscono di sfruttare appieno le funzionalità SOC rientrano in tre aree:

- Comprensione e gestione degli avvisi
- Integrazione o automazione limitata tra gli strumenti
- Esecuzione di compiti chiave con il personale e le competenze disponibili

Ma la statistica più tragica potrebbe essere che tutti questi ostacoli hanno avuto un impatto sui SOC per oltre un decennio. I miglioramenti incrementali derivanti dalla semplice assegnazione automatica di priorità agli incidenti in base alla classificazione del malware e ad altri filtri di base non sono stati in grado di tenere il passo con la crescita degli avvisi e di altri eventi che potrebbero richiedere l'attenzione degli analisti SOC. Quindi, le cose sono solo peggiorate.

SOC INSIGHTS: INFORMAZIONI SOC BASATE SULL'AI

Le moderne minacce persistenti sfruttano infrastrutture flessibili degli aggressori e sistemi C2 dinamici per ospitare e distribuire numerosi strumenti di pen-test, exploit, crittografia e altri strumenti coinvolti anche in un singolo attacco. Ciò li rende estremamente dipendenti dal DNS ed evidenzia una debolezza fondamentale che i difensori possono sfruttare per rilevare e bloccare queste minacce.

Il DNS vede le attività legittime e dannose indipendentemente dal protocollo, dalla piattaforma, dal sistema operativo, dall'applicazione e persino dalla posizione. Grazie a questa visibilità unica, un programma pilota condotto dal direttore della sicurezza informatica dell'NSA ha rivelato che la protezione del DNS può ridurre gli attacchi malware del 92%[2]!

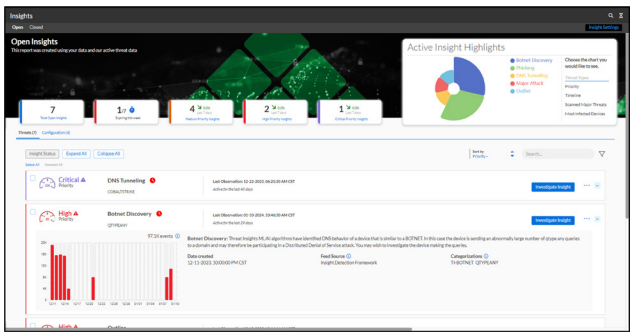

Figura 1: La pagina di riepilogo di SOC Insights consente agli analisti di accedere con un solo clic a ciò che conta di più.

DATI E CIFRE

- Il 60% degli analisti SOC afferma che i loro **carichi di lavoro stanno aumentando**, e il 65% **probabilmente cambierà lavoro** nel prossimo anno[4].
- Il 55% degli intervistati ha affermato che **gli avvisi critici vengono persi** spesso su base settimanale e persino giornaliera[5].
- Il 64% degli analisti afferma che **il lavoro manuale richiede più della metà del loro tempo**[6].
- L'errata configurazione è uno dei **3 principali fattori delle violazioni legate agli errori**[3].
- 8 dei 10 principali **ostacoli che impediscono il pieno utilizzo del SOC** riguardano gli avvisi, l'integrazione degli strumenti e la carenza di competenze[1].
- Il 77% dei CEO è preoccupato per la **disponibilità di competenze chiave**[7].
- **Il 92% delle attività di malware e C2 può essere controllato a livello DNS** con la giusta intelligence e visibilità DNS[2].

SOC Insights collabora con la soluzione DNSDR (DNS Detection and Response) di Infoblox, BloxOne Threat Defense, per offrire analisi basate sull'AI, al fine di rilevare attività di minacce sconosciute che altri strumenti non rilevano, aumentare l'efficienza del SOC e migliorare il ROI complessivo degli investimenti attuali nella sicurezza.

RISOLVERE PIÙ PROBLEMI CON UNA SERIE DI INSIGHTS

Le indagini successive agli incidenti o alle violazioni spesso rivelano che i primi indicatori di attività dannose non sono stati colti a causa di configurazioni errate, problemi di integrazione degli strumenti di sicurezza o per semplice sovraccarico di avvisi. SOC Insights applica l'analisi basata sull'AI su una vasta quantità di dati per contribuire ad affrontare questi rischi.

Security Insights

Il componente aggiuntivo per la sicurezza di SOC Insights è disponibile per BloxOne Threat Defense "Business Cloud" o "Advanced" e utilizza l'AI per distillare grandi quantità di visibilità e intelligence su eventi, rete, ecosistema e DNS in una serie gestibile di informazioni fruibili sulla sicurezza.

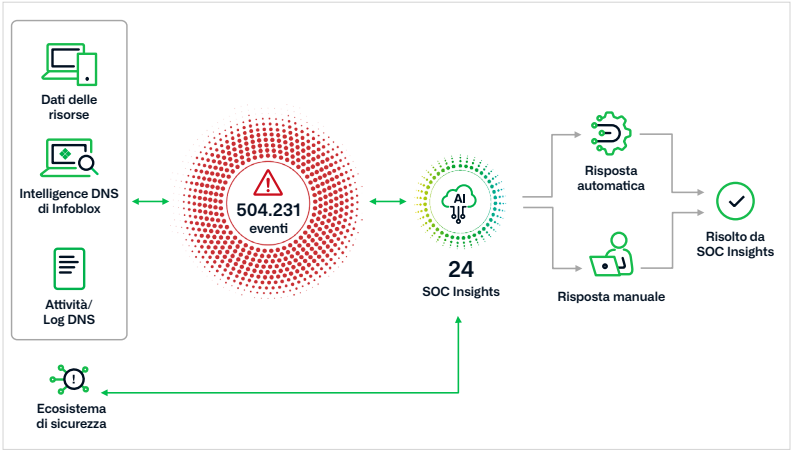

Figura 2: SOC Insights elimina il sovraccarico di avvisi, distillando montagne di eventi in un insieme più gestibile di informazioni significative e fruibili.

- Zero Day DNS™
- Minaccia persistente
- Diffusione attiva delle minacce
- Attacco grave
- Rilevazione botnet
- Comunicazione anomala
- Phishing
- Malware
- Resolver DNS aperto
- Tunneling DNS
- Attività di perdita di dati
- Attacco mirato
- Errori DNS eccessivi
- Dominio lookalike monitorato

Informazioni sulla configurazione

La funzione per la configurazione di SOC Insights è inclusa in BloxOne Threat Defense "Business Cloud" e "Advanced" per aiutare gli utenti ad assicurarsi di sfruttare appieno le best practices attuali ed evitare errori comuni. Segui i video e altre guide per risolvere errori e punti deboli o disattivare gli avvisi non necessari per le eccezioni consentite.

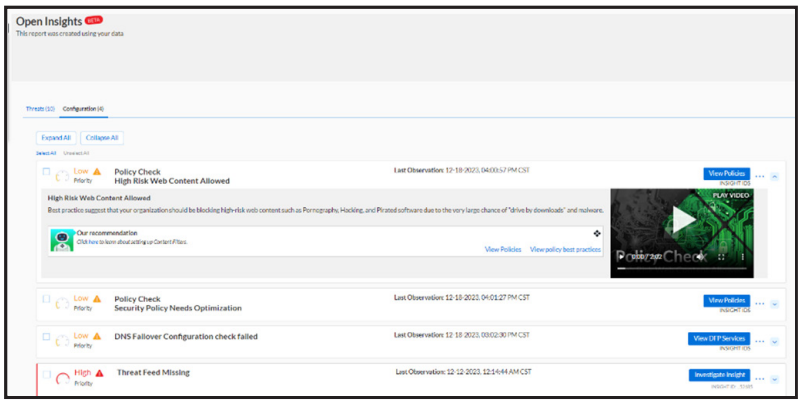

Figura 3: Identificazione proattiva degli errori di configurazione e pericolosi per garantire capacità ottimali di difesa, analisi e risposta.

- Feed delle minacce DNS mancante
- Chiave gratuita di VirusTotal mancante
- Politica di sicurezza che necessita di ottimizzazione
- Errore di verifica del failover DNS
- Mancata corrispondenza dell'azione del feed
- Dettagli delle risorse nascoste dal DFP
- Politica di sicurezza in modalità di logging
- Filtri dei contenuti Web disattivati
- Contenuti Web ad alto rischio consentiti

UN IMPATTO FINANZIARIO, OPERATIVO E AZIENDALE POSITIVO

Mentre la maggior parte degli strumenti di sicurezza può promettere poco più di "semplicità d'uso" e "meno violazioni", SOC Insights può fare molto di più, dalla riduzione dello stress e del turnover degli analisti alla riduzione di molti problemi di sicurezza derivanti da espansioni, fusioni e acquisizioni e altre iniziative aziendali. Per esempio:

- La natura del DNS semplifica l'unificazione di una nuova posizione o di un nuovo partner commerciale in un'infrastruttura DNS comune in pochi minuti anziché in mesi.
- Le informazioni sulla configurazione sono altamente proattive per aiutare a mitigare le violazioni o le perdite di dati dovute a una "errata configurazione", che è uno dei 3 fattori principali riportati nelle violazioni legate agli errori[3].
- L'autocorrelazione di "malware", "phishing", "botnet" e altre attività "gravi" o di "diffusione" consente a chi risponde all'attacco di affrontare molte minacce contemporaneamente, aumentando la propria efficienza.
- Passare a una strategia di sicurezza più proattiva con la possibilità di monitorare categorie di informazioni quali "valori anomali", "tunneling DNS" e "resolver aperto", nonché le esclusive funzionalità di visibilità delle applicazioni e di lookalike di BloxOne Threat Defense.
- L'integrazione dell'intelligence dell'ecosistema di sicurezza migliora il ROI dell'intero stack di sicurezza offrendo "informazioni" fruibili anziché solo log ed eventi non elaborati.
- SOC Insights raccoglie automaticamente i dati rilevanti e consente agli analisti di visualizzare e orientare tali dati per giungere a conclusioni più rapide e con maggiore sicurezza. Ciò contribuisce a ridurre lo stress e a fidelizzare maggiormente i professionisti della sicurezza qualificati ed esperti.

RISULTATI STRAORDINARI

I clienti segnalano vantaggi significativi nell'utilizzo di SOC Insights con BloxOne Threat Defense, tra cui:

- Riduzione degli avvisi EDR e FW del 50%
- Risparmio medio di 500 ore di analisi SOC al mese
- 400.000 dollari di risparmi sulla produttività all'anno

MIGLIORA SIEM, SOAR E ALTRE PARTI DELL'ECOSISTEMA CON LE INFORMAZIONI APPROFONDITE

Le SecOps conoscono il valore e i limiti della condivisione dei dati grezzi nell'ecosistema di sicurezza. Ciò ha reso le competenze su SIEM e SOAR tra le più impegnative per la maggior parte delle organizzazioni. SOC Insights alleggerisce il carico di lavoro di questi altri strumenti e può condividere le informazioni risultanti in tutto lo stack di sicurezza per rendere gli altri strumenti più efficaci, aumentando ulteriormente l'efficienza complessiva delle SecOps.

1 "SANS 2023 SOC Survey", giugno 2023, di Chris Crowley, Barbara Filkins, John Pescatore

2 "NSA launches pilot program to secure defense contractors", 18 giugno 2020, di Lauren C. Williams, NEXTGOV/FCW

3 "Verizon 2023 DBIR Report"

4 Voice of the SOC Analyst

5 The Orca Security 2022 Cloud Security Alert Fatigue Report

6 Voice of the SOC Analyst

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

infoblox.

Infoblox unisce networking e sicurezza per offrire prestazioni e protezione senza pari. Scelti dalle aziende Fortune 100 e dagli innovatori emergenti, forniamo visibilità e controllo in tempo reale su chi e cosa si connette alla tua rete, in modo che la tua organizzazione funzioni più velocemente e blocchi le minacce in modo più rapido.

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versione: 20240411v2