SECURITY ORCHESTRATOR DI FIREEYE

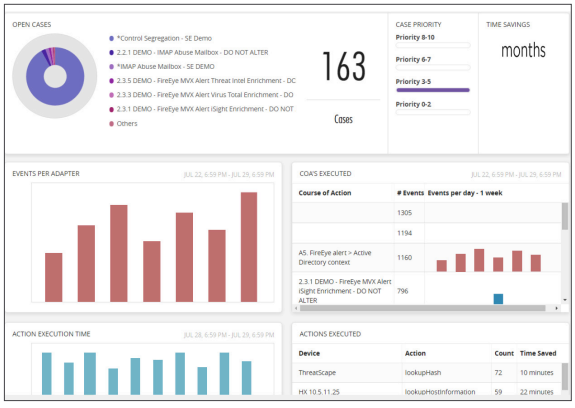
INTEGRATE E AUTOMATIZZATE TECNOLOGIE E PROCESSI DI GESTIONE DEGLI INCIDENTI NELLA VOSTRA INFRASTRUTTURA IT

PANORAMICA

Il volume degli attacchi informatici non è mai stato così elevato e se le vostre difese non sono al passo, il rischio di una violazione aumenta sensibilmente. Gli aggressori dispongono delle risorse intellettuali, della potenza di calcolo e della dorsale delle reti di trasmissione digitale più rapide. Possono replicare le vostre difese a proprio piacimento, modificare la firma degli attacchi, passare tramite morphing a nuovi metodi di fornitura, alterando di continuo la modalità di approccio all'infiltrazione nella vostra rete. Possono farlo tutto il giorno, tutti i giorni. Quando si considera il volume di avvisi con cui la maggior parte dei SOC ha a che fare ogni giorno e il fatto che non sia possibile trovare le risorse per presidiare tali SOC, un programma tradizionale basato sull'intervento e il contenimento manuale deve affrontare una lotta asimmetrica.

Security Orchestrator di FireEye accelera e semplifica il rilevamento delle minacce e il processo di risposta combinando tecnologie e processi di gestione degli incidenti diversi in una singola console che offre risposte guidate in tempo reale migliorando i tempi di reazione, riducendo l'esposizione ai rischi e garantendo l'uniformità dei processi all'interno di un programma di sicurezza. Gli anni di esperienza di FireEye nel contrasto alle violazioni più significative del mondo hanno contribuito a perfezionare i processi di rilevamento, indagine e reazione alle minacce. Security Orchestrator di FireEye vi consente di utilizzare queste procedure ottimali sui dati provenienti dalla distribuzione FireEye e da tecnologie di livello enterprise SIEM e di altra natura.

Security Orchestrator di FireEye è in grado di affrontare modifiche a livello di rete, host e applicazione, oltre che nei sistemi fisici di controllo dell'accesso. La capacità di reagire in pochi secondi blocca in modo efficace gli accessi non autorizzati individuandone la



VANTAGGI

- Migliorate la capacità del team di sicurezza con la distribuzione, la progettazione e playbook pre-costruiti da un team che vanta un'esperienza decennale nelle indagini contro gli attacchi informatici
- Eliminate gli errori mediante un processo standardizzato e l'automazione riducendo il carico sui team SOC
- Consentite ai team SOC di ridurre i rischi grazie a tempi di risposta più rapidi e permettendo loro di concentrarsi su attività prioritarie che possono migliorare ulteriormente la vostra posizione rispetto ai rischi, come la ricerca
- Dashboard e gestione dei casi centralizzati per stabilizzare i processi operativi di sicurezza

FireEye

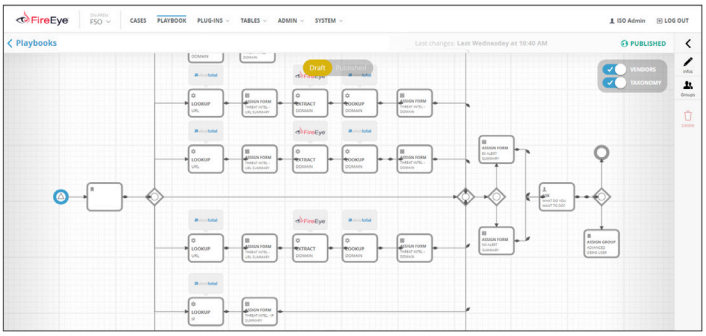
traccia e chiude le porte, limitando i danni e i rischi per l'organizzazione. Con Security Orchestrator di FireEye, potrete risparmiare tempo e risorse unificando i dati relativi all'incidente e le tecnologie di sicurezza in una singola piattaforma operativa.

I nostri clienti riducono in modo significativo i tempi di risposta ed eliminano gli errori dei processi, riducendo in ultima analisi l'esposizione ai rischi generali.

CARATTERISTICHE CHIAVE

Playbook di risposta agli incidenti

Nei playbook di risposta agli incidenti, anche noti come linee di azione (*Courses of Action*, CoA), le operazioni di sicurezza sono codificate in flussi di lavoro a guida umana e attività automatizzate. Con processi dei centri SOC documentati, automatizzati e migliorati grazie all'esperienza di FireEye nel contrasto ai tipi di attacchi più avanzati, i vostri tempi di risposta si ridurranno, mentre l'uniformità dei processi viene garantita da un programma di sicurezza.



Il nuovo programma CoA Builder consente di creare flussi di lavoro intelligenti e ramificati, integrati nella politica di sicurezza della vostra organizzazione e che sostengono le operazioni dell'infrastruttura. Viene fornito con un portafoglio completo di plug-in e flussi di lavoro pre-costruiti per gli strumenti impiegati nelle operazioni di sicurezza, come SIEM, firewall, Threat Intelligence, IPS e sistemi di gestione dei ticket. Consente quindi la creazione di flussi di lavoro adattati alle politiche di sicurezza e all'infrastruttura di supporto della vostra organizzazione. Grazie ai playbook, potete organizzare i flussi di lavoro degli analisti della sicurezza in una sequenza parzialmente o completamente automatizzata di attività, con la possibilità di richiedere agli analisti dei feedback, che verranno utilizzati per dirigere un determinato flusso di lavoro. Il risultato finale sarà un ambiente totalmente operativo con flussi di lavoro di sicurezza sviluppati e approvati dall'organizzazione. Queste modifiche verranno trasformate in flussi di lavoro di automazione che possono essere avviati automaticamente, attivati da eventi all'interno dell'infrastruttura o eseguiti secondo necessità dal personale del SOC.

Accesso basato su ruoli

Create gruppi basati su ruoli e assegnate autorizzazioni granulari a singoli playbook o fasi specifiche all'interno dei playbook. In questo modo ogni team disporrà dell'accesso e dei privilegi necessari a consultare i risultati solo sui flussi di lavoro necessari. Potete utilizzare utenti e gruppi locali o integrare l'elenco Active Directory o Open LDAP e assegnare ruoli in Orchestrator.

Plug-in

Integrate, unificate e controllate l'architettura IT da un singolo pannello di controllo tramite la struttura di plug-in. I plug-in rappresentano il tessuto connettivo che unisce dispositivi, applicazioni, servizi e dati in Security Orchestrator di FireEye. Sono creati per supportare alcune delle nostre tecnologie di sicurezza e infrastruttura più popolari.

Questa architettura integrabile permette alle organizzazioni di escludere o aggiungere tecnologie con tempi minimi di formazione sulla risposta e l'integrazione. I plug-in sono dotati di capacità di comando e controllo bidirezionali per ricevere dati e consentire azioni.

Dashboard centralizzate e ricerca avanzata

Security Orchestrator di FireEye fornisce una dashboard per la ricerca degli strumenti di sicurezza e la facilitazione della caccia agli autori di minacce alla vostra organizzazione. Potete anche gestire casi e passare agevolmente dai playbook a contesti aggiuntivi all'interno dell'infrastruttura di sicurezza esistente.

Inoltre, i vostri analisti possono visualizzare una dashboard centralizzata e mappe delle minacce a livello mondiale per creare una vista completa dei dati e degli attacchi rilevati dalle apparecchiature di FireEye all'interno dell'organizzazione. Tale vista può fornirvi analisi in tempo reale e cronologiche che vi permetteranno un rilevamento e una risposta

rapidi. Avrete anche la possibilità di condurre indagini approfondite tramite ricerche ultrarapide, su livelli e altamente flessibili nei dati di notifica degli avvisi di FireEye. In questo modo, potrete passare rapidamente dall'avviso al contesto più ampio che sottende all'attacco. Tutte le dashboard di ricerca possono essere salvate e inviate tramite e-mail.

Report

Potete creare report occasionali e ricorrenti in cui gli avvisi collegati sono dettagliati, posti in correlazione e visualizzati. I team addetti alla sicurezza possono determinare con rapidità le fonti, la metodologia e gli obiettivi di un attacco e impedirne il futuro ripetersi. I report possono essere personalizzati con:

- Migliaia di parametri degli avvisi
- Filtri chirurgici
- Vari formati di file
- Skin per i grafici specifici dell'organizzazione
- Servizi professionali: Orchestrazione

Servizi di distribuzione personalizzati sono disponibili per la progettazione e la distribuzione di Security Orchestrator di FireEye in un programma e un'architettura di sicurezza. Tali servizi sfruttano l'esperienza di FireEye per la progettazione dei playbook appropriati sulla base delle soluzioni tecnologiche del vostro ambiente e le minacce che l'organizzazione affronta ogni giorno.

Per maggiori informazioni su FireEye, visitate il sito:
www.FireEye.com

A PROPOSITO DI FIREEYE, INC.

FireEye è leader nella sicurezza come servizio basato sulle informazioni. Fungendo da estensione semplice e scalabile delle operazioni di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e i servizi di consulenza Mandiant®, rinomati in tutto il mondo. Con questo approccio, FireEye elimina la complessità e il peso della cybersicurezza per le aziende che hanno difficoltà a prepararsi, prevenire e rispondere agli attacchi informatici. FireEye ha oltre 5.000 clienti in 67 Paesi, tra cui più di 940 dei Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye