FIREEYE AS A SERVICE

ESTENDI LE OPERAZIONI DEL TUO PROGRAMMA DI SICUREZZA CON ESPERIENZA, INFORMAZIONI SULLE MINACCE E TECNOLOGIA LEADER DI SETTORE

PANORAMICA

Le attuali minacce alla sicurezza sono sempre più sofisticate per il modo in cui puntano l'obiettivo, attaccano e si infiltrano nelle aziende per sottrarne le risorse più importanti. La tecnologia di per sé non è in grado di sconfiggere un aggressore ed è tanto difficile quanto oneroso assumere, formare e trattenere esperti in materia di sicurezza. Ti serve un partner affidabile che monitori rete e sistemi 24 ore su 24 usando una piattaforma tecnologica avanzata e le più aggiornate informazioni sulle minacce a livello globale. Hai bisogno di FireEye as a Service.

FireEye as a Service

FireEye as a Service è un servizio gestito di rilevamento, indagine e risposta che riduce al minimo il potenziale impatto sull'attività dei sempre più sofisticati e mirati attacchi informatici.

FireEye as a Service fornisce sicurezza di livello Fortune 50 ad una frazione del costo, accelerando la difesa tramite un'indagine approfondita delle minacce, la valutazione del compromesso e consigli pratici di correzione, nonché la visibilità nelle campagne di attacco emergenti.

Come funziona

FireEye as a Service integra le persone, la tecnologia e le informazioni per individuare e investigare gli autori degli attacchi alle reti aziendali.

FireEye as a Service sfrutta gli investimenti esistenti in tecnologia sia di FireEye che di terze parti per fornire visibilità in tempo reale in tutta l'azienda, incluse le sedi più remote.

Gli esperti analisti delle minacce di FireEye vanno oltre il tradizionale monitoraggio della sicurezza, utilizzando tecniche di proprietà alimentate da informazioni sulle minacce basate su avversario, vittima e macchina per individuare, indagare e scovare in modo proattivo le minacce non rilevate in precedenza.

CARATTERISTICHE

- **Consapevolezza della situazione senza precedenti:** visibilità in tempo reale nella valutazione in corso e la risposta alle minacce emergenti tramite la nostra dashboard di protezione della community.
- **Risposte, non solo avvisi:** rapporti di compromissione approfonditi che valutano l'attività dell'aggressore e mostrano prove in termini di catena di attacco e comprendono un ampio contesto e consigli di risposta in modo da poter valutare rapidamente i rischi e prendere provvedimenti.
- **Team di esperti:** migliaia di analisti delle minacce, esperti di malware, addetti alla risposta alle minacce, curatori di soluzioni di intelligence ed esperti forensi.
- **Tecniche di ricerca avanzate:** gli analisti per la valutazione delle minacce FireEye forniscono approfondimenti dettagliati sui comportamenti che non possono essere replicati.
- **Avanzati centri di risposta alle minacce in tutto il mondo:** (ATRCs) negli Stati Uniti (Virginia e California), Irlanda, Germania, Singapore, Sydney e Giappone forniscono una copertura 24x7.
- **Informazioni sulle minacce applicate:** gli analisti della sicurezza applicano le ultime informazioni su macchina, vittima e avversario per individuare e definire più velocemente le minacce nel tuo ambiente.
- **Capacità di sfruttare gli investimenti esistenti:** integrazione con qualsiasi operazione di sicurezza in loco, nel cloud o in un ambiente ibrido
- **Engagement Managers:** sostegno supplementare come analisi di campioni di malware, analisi forensi approfondite o risposta agli incidenti in loco.

FireEye®

Una volta convalidato un segnale di compromissione, sarai immediatamente informato e riceverai un report completo con l'indicazione del contesto della minaccia (chi, cosa, quando e come) per consentire una risposta efficace. In alcuni casi, forniremo raccomandazioni per mettere immediatamente in quarantena i sistemi e impedire agli autori degli attacchi di avanzare in azienda. Se richiesto, gli addetti alla risposta agli eventi FireEye con competenze forensi sono in grado di aiutarti a risolvere gli eventi tempestivamente e a valutare in modo immediato e puntuale l'impatto della divulgazione di informazioni.

Un nuovo tipo di sicurezza gestita con FireEye as a Service

Amplifica il tuo team: esperti analisti delle minacce

Esperti analisti delle minacce di FireEye monitorano la tua rete e i vostri endpoint 24 ore su 24, 7 giorni su 7, utilizzando le informazioni e le metodologie di proprietà più aggiornate per cercare segnali di compromissione ed eseguire una valutazione accurata e indagini proattive. Questi esperti determinano la portata dell'attacco visualizzata attraverso la catena di attacco dell'aggressore per rivelare cosa, quando e come si sono verificati gli attacchi e chi potrebbe esserci dietro. Applicano le loro conoscenze dei gruppi di attacco e del loro funzionamento per fornire raccomandazioni attuabili, con l'aggiunta del contesto dell'aggressore.

Visibilità nelle campagne emergenti: Community Protection

Community Protection fornisce ai clienti una visibilità in tempo reale e la consapevolezza della situazione delle minacce emergenti. Quando FireEye rileva una minaccia emergente, viene avviata un'indagine interdisciplinare che sfrutta le informazioni sull'avversario del nostro team FireEye iSIGHT, il nostro punto di vista in tutti i mercati verticali e geopolitici, la visibilità in prima linea dei nostri consulenti Mandiant e la telemetria dei nostri prodotti distribuiti in tutto il mondo. I clienti possono visualizzare la risposta in corso ad ogni evento attraverso un ciclo di vita di quattro fasi: valutazione, mobilitazione, sostentamento e risoluzione. Inoltre, Community Protection espone le tecniche FireEye as a Service che rilevano l'evento, le funzionalità di rilevamento degli eventi dei nostri prodotti e i dettagli e il contesto che FireEye iSIGHT Intelligence fornisce.

Sicurezza di livello Fortune 50 a una frazione del costo

FireEye as a Service ti aiuta a migliorare la postura di sicurezza ed estendere le funzionalità SOC al 15-25% di quanto ti costerebbe farlo da solo. Sarai in grado di dare la priorità alle minacce importanti per aumentare l'efficacia delle tue risposte. Questo rende più efficace il personale esistente e lo aiuterà a concentrarsi sulle attività, come la ricerca proattiva, che hanno bisogno di più supervisione umana. Rilevare e contenere minacce note ed emergenti prima che

Funzionalità

Servizio completamente gestito

Con FireEye as a Service, potrai contare su un partner affidabile capace di fornirti tecnologie potenti, informazioni fruibili e una competenza specializzata nell'ambito di un servizio completamente gestito mirato alla prevenzione delle minacce avanzate.

Monitoraggio professionale

Il team di esperti analisti di minacce FireEye monitora il tuo ambiente 24 ore su 24, 7 giorni su 7, applicando le informazioni e le metodologie di proprietà più aggiornate alla ricerca di segnali di compromissione.

Indagine

Quando viene attivato un avviso, i nostri analisti delle minacce indagano per determinare la portata dell'attacco, ispezionando a fondo il traffico di rete o l'endpoint per determinare l'entità della compromissione. Utilizzando le informazioni FireEye, questi analisti sono in grado di identificare la linea temporale in tutta la catena di attacco per rivelare quando e come si è verificato un attacco, chi c'era dietro e qual era l'obiettivo.

Intelligence applicata alle minacce

Nuove soluzioni di intelligence vengono generate e applicate attraverso l'analisi da parte di persone esperte e la condivisione automatica delle informazioni, fornendo una visibilità globale delle minacce emergenti.

Risposte, non avvisi

Gli analisti di minacce leader del settore e gli esperti di risposta agli eventi utilizzano le conoscenze forensi in materia di reti e sistemi per investigare, classificare e analizzare il rischio in tempo reale, fornendo immediatamente report dettagliati che illustrano esattamente ciò che è avvenuto, con l'indicazione di consigli su come contenere la minaccia.

Potente difesa

Nel tuo ambiente saranno installate tecnologie FireEye, che effettuano più di 50 miliardi di analisi con virtual machine ed elaborano 400.000 campioni di malware diversi ogni giorno. Milioni di sensori che raccolgono nuove informazioni in tutto il mondo vengono sovrapposti a informazioni dettagliate, contestualizzate e aggiornate nel tuo ecosistema FireEye ogni 60 minuti, offrendoti una potente difesa per il rilevamento e la prevenzione delle minacce.

Una copertura all'altezza delle vostre esigenze

FireEye as a Service offre due livelli di servizio per garantirti la flessibilità necessaria per adattarsi alle tue mutevoli esigenze:

causino danni aiuterà anche a eliminare i costosi e laboriosi processi di correzione

Continuous Guidance è un servizio di rilevamento gestito che sfrutta le informazioni di sicurezza di FireEye e di terze parti per aiutare i clienti a identificare, convalidare e definire la priorità di minacce note ed emergenti.

Dopo aver rilevato una potenziale minaccia, i nostri analisti convalidano e valutano l'incidente, assegnando un livello di gravità sulla base delle informazioni sulle minacce accumulate, l'esperienza e la conoscenza del modus operandi degli aggressori. I nostri Incident Advisories forniscono informazioni complete, tra cui le prove scoperte e le informazioni sulle minacce rilevanti per aiutarti a capire l'attacco.

Se è necessaria un'ulteriore indagine, Continuous Guidance consiglia i passi da seguire per determinare la portata dell'attacco. Per le minacce note, forniamo consigli di correzione per accelerare la risposta.

Continuous Vigilance si affianca a Continuous Guidance con un'approfondita indagine di minacce note ed emergenti.

Abbiniamo la nostra vasta conoscenza del comportamento di gruppo delle minacce a metodi di indagine di proprietà, per scoprire eventuali segni di intrusione, apprendere il modus operandi degli aggressori e valutare la portata delle loro capacità. Usiamo anche tecniche di rilevamento guidate dall'analista per una ricerca proattiva degli indicatori dissimulati di un tentativo di compromissione che elude le difese tecnologiche tradizionali.

Le nostre Compromise Assessments offrono un contesto definitivo orientato all'azione, necessario per comprendere appieno le minacce, valutarne il rischio e agire di conseguenza.

FUNZIONALITÀ	CONTINUOUS GUIDANCE	CONTINUOUS VIGILANCE
Fornisce protezione della comunità	Sì	Sì
Ingloba gli avvisi FireEye	Sì	Sì
Risolve duplicati, falsi positivi e avvisi benigni	Sì	Sì
Convalida e definisce la priorità degli incidenti	Sì	Sì
Informazioni sulle minacce	Arricchisce solo l'incidente	Accesso al portale FireEye Intelligence
Indaga avvisi sospetti e confermati	Il cliente ha accesso a Guided Investigations tramite TAP	FireEye conduce indagini
Conduce rilevamento guidato dall'analista (ricerca proattiva)	No	Sì
Fornisce rapporti critici	Incident Advisory (con consigli di indagine)	Compromise Report (con consigli di correzione)
Fornisce Engagement Managers	Pool	Specializzato

Per maggiori informazioni su FireEye, visitare 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

DS.FAAS.IT-IT.032017

FireEye