SCHEDA TECNICA

Abbonamenti a Threat Intelligence

Informa la tua azienda e non solo la tua appliance

CARATTERISTICHE PRINCIPALI

- Fornisce informazioni sulle minacce esaurienti e possibili prendendo in considerazione un ampio ventaglio di soggetti
- Offre una visibilità che va oltre il tipico ciclo di vita dell'attacco, aggiungendo contesto e priorità alle minacce globali
- Migliora la protezione delle risorse e fornisce informazioni più efficaci sulle decisioni relative ai rischi aziendali
- Allinea i programmi e le risorse di sicurezza contro le minacce e gli attori più probabili
- Indirizza i casi d'uso tattici, operativi e strategici
- Migliora la definizione delle priorità, la correzione degli avvisi di sicurezza e la risoluzione delle vulnerabilità di sicurezza

Spesso gli aggressori informatici sono più esperti, finanziati e qualificati di molte organizzazioni di sicurezza. Gli attacchi informatici sono sempre più complessi e i danni che ne conseguono sempre più gravi. Trovare e fidelizzare un professionista della sicurezza qualificato risulta già abbastanza difficile. Trovare le cifre necessarie per affrontare al meglio queste sfide sarebbe proibitivo dal punto di vista dei costi.

Le organizzazioni di sicurezza sono alla ricerca di modi per aumentare le proprie competenze e la propria efficacia in materia di sicurezza. Devono migliorare le loro capacità di risposta e garantire che le loro difese siano allineate contro le minacce più probabili. Tutto ciò senza prosciugare le proprie finanze.

Con gli abbonamenti a FireEye Threat Intelligence è possibile affrontare queste sfide, a costi contenuti, con un'ampia gamma di informazioni di sicurezza efficaci e fruibili a livello strategico, operativo e tattico.

Tabella 1. I vantaggi di FireEye Threat Intelligence.

Le informazioni identificano...	Vantaggio
Quali sono le minacce e gli attori che bisogna affrontare a causa della propria attività, del settore o della regione	Consente di investire e di adottare le misure di sicurezza adeguate per affrontarli
Quali avvisi devono essere analizzati per primi con le relative informazioni contestuali	Riduce il tempo di rilevamento e la gestione degli avvisi, e aumenta la conoscenza del personale
Quali sono le vulnerabilità da risolvere per prime sulla base di quelle sfruttate contro aziende simili	Dà priorità agli sforzi di risoluzione e riduce le probabilità della buona riuscita degli attacchi

Gli abbonamenti a FireEye Threat Intelligence sono personalizzati in base alle esigenze dell'azienda. Tipi di abbonamento, tra cui:

- **Fusion:** approfondimenti completi sulle attività minacciose attuali, passate e future. Include Operational, Cyber Crime, Cyber Espionage, la maggior parte dei contenuti di Cyber Physical e una versione allegata di FireEye Digital Threat Monitoring.
- **Operational:** analisi tecnica del malware e delle relative tattiche, tecniche e procedure (TTP) di noti malintenzionati, compreso l'accesso a una libreria di profili di malware, panoramiche degli attori e indicatori di compromissione (*indicators of compromise*, IOC) leggibili al computer per un quadro contestuale migliorato sulle minacce.
- **Cyber Physical:** approfondimenti fruibili sulle minacce e sui rischi informatici che incombono sugli ambienti industriali e sulla tecnologia operativa (*operational technology*, OT). Comprende tutte le informazioni basate sulla OT di FireEye e sui sistemi di controllo industriale (*industrial control systems*, ICS).
- **Cyber Crime:** valutazioni approfondite e monitoraggio degli attori di minaccia che si concentrano sulla criminalità finanziaria: cosa vogliono, a chi si rivolgono e come operano.
- **Cyber Espionage:** informazioni su gruppi di minacce avanzate persistenti (*advanced persistent threat*, APT) nominati associati a specifici Stati, compresi i loro obiettivi e le TTP che utilizzano, per aiutare i team di sicurezza a comprendere e affrontare le minacce imminenti e in corso.
- **Strategic:** valutazioni delle minacce in importanti settori e regioni, tra cui la geopolitica, gli sviluppi che influenzano il panorama delle minacce informatiche e le previsioni sull'evoluzione dei problemi di minacce informatiche nel breve e nel lungo termine.
- **Vulnerabilità:** valutazioni di informazioni sulle vulnerabilità software identificate in molte tecnologie, insieme a valutazioni di proprietà sulla probabilità di sfruttamento e raccomandazioni di mitigazione.

Generalmente le informazioni vengono presentate sotto forma di report. Le informazioni leggibili al computer e gli IOC sono disponibili, ove applicabile, per integrarsi con i prodotti di sicurezza esistenti, come i SIEM e i gestori di vulnerabilità. Inoltre, gli abbonamenti a FireEye Threat Intelligence includono numerose risorse:

- **Portale FireEye Intelligence:** accesso online ai report di informazioni e alla libreria completa della cronologia di FireEye Threat Intelligence relativa allo specifico abbonamento. Gli IOC associati a specifici tipi di informazioni possono essere scaricati ed è possibile eseguire ricerche per trovare informazioni su attori, malware, attività e altre aree tematiche.
- **Consultazione con gli analisti:** consultazione con gli analisti di FireEye Threat e Technical Intelligence per una comprensione più chiara e approfondita di attori, attacchi e rischi, così da ottenere una migliore visione di come certe informazioni o eventi sono strettamente rapportati ai propri interessi.
- **Opzioni di consegna:** è possibile determinare il modo in cui vengono trasmesse le proprie informazioni e con quale frequenza, compresi gli avvisi via e-mail e i digest.
- **Analisi giornaliera delle novità:** e-mail giornaliera che monitora le attuali storie sulla sicurezza trattate dai media per fornire una visione dettagliata del panorama della sicurezza. Include la copertura mediatica della storia, la valutazione di FireEye sulla sua accuratezza e le relative informazioni di FireEye per aumentare la comprensione e le capacità di risposta.
- **API delle informazioni:** questo punto di integrazione macchina-macchina consente di utilizzare le informazioni di FireEye e i nostri IOC ad alta efficacia all'interno delle operazioni di sicurezza e di rete, della gestione delle vulnerabilità e dei sistemi di risposta agli incidenti.
- **Plug-in del browser:** questo plug-in estende l'integrazione tecnica di FireEye Threat Intelligence a qualsiasi pagina web a cui si accede. Esegue automaticamente la scansione della pagina web per ricercare indicatori tecnici (come indirizzi IP, domini, hash), esegue query sull'API delle informazioni al fine di cercare informazioni rilevanti per FireEye e infine crea, su questa informazione, un collegamento ipertestuale.
- **Strumenti di analisi:** i clienti utilizzano queste utilità online collegate alle informazioni per informarsi su nomi di dominio specifici, indirizzi IP e minacce, e caricare file sospetti per l'analisi.

Anche il miglior personale di sicurezza non può essere a conoscenza di tutte le aree tematiche (compresi gli attori, le minacce, le vulnerabilità, i rimedi efficaci, la caccia alle minacce). Con gli abbonamenti a FireEye Threat Intelligence è possibile avere la conoscenza, l'esperienza, la visibilità e la capacità analitica di FireEye, azienda leader a livello mondiale per l'intelligence sulle minacce. Adesso chiunque all'interno dell'azienda può avere accesso al tipo di informazioni a cui i migliori professionisti della sicurezza dedicano anni di apprendimento.

Il vantaggio offerto da FireEye

FireEye conosce le minacce informatiche e i responsabili meglio di chiunque altro. La ragione di ciò è il nostro incomparabile accesso alle attività informatiche e alle nostre estese operazioni di intelligence sulle minacce. FireEye combina le informazioni sugli avversari, sulle vittime e sulle campagne con i dati telemetrici dei prodotti per generare informazioni sulle minacce fruibili che nessun concorrente è in grado di eguagliare. Le nostre informazioni si basano su:

- Ricercatori sul campo in 22 Paesi di tutto il mondo che parlano oltre 30 lingue e che sfruttano il deep web e il dark web per fornire informazioni sui metodi, motivazioni e infrastrutture degli avversari
- Oltre 15.000 sensori di rete in modalità bidirezionale presso le sedi dei clienti che forniscono dati su quali minacce stanno colpendo i nostri clienti in tutto il mondo
- FireEye Mandiant, l'azienda leader a livello mondiale che fornisce risposta agli incidenti e informazioni provenienti dalle indagini sulle violazioni delle TTP utilizzate dagli attori avanzati per attacchi efficaci
- Il più grande database storico del settore delle attività legate alle minacce, creato a partire dai dati raccolti attraverso gli eventi e gli incidenti gestiti da tutti i nostri esperti e dalla tecnologia
- FireEye è stato nominato unico leader in The Forrester New Wave™: External Threat Intelligence Services, Q3 2018

SUPPORTO CLIENTI DEDICATO

Tre livelli di abilitazione e supporto delle informazioni tra cui scegliere:

LIVELLO 1

Baseline: materiali e processi di base necessari per utilizzare il portale FireEye Intelligence e configurare le API delle informazioni nella propria azienda.

LIVELLO 2

Intelligence Coordination: Baseline + un Intelligence Enablement Manager designato, accesso alle richieste degli analisti di intelligence di FireEye, informative trimestrali sulle minacce e revisioni formali semestrali.

LIVELLO 3

Intelligence Optimization: Intelligence Coordination + un analista designato di Intelligence Optimization, ulteriori richieste di analisti, report personalizzati sulle minacce, workshop strategici e briefing sulle minacce.

Per ulteriori informazioni, visitare: **https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.html** e leggere il **report Forrester**.

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

Informazioni su FireEye, Inc.

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.

FIREEYE™