SCHEDA TECNICA

FireEye Detection On Demand

Analizza il contenuto alla ricerca di minacce in tutti i punti del flusso di lavoro

CARATTERISTICHE PRINCIPALI

- Rilevamento e prevenzione del malware conosciuto e sconosciuto ovunque
- Implementazione di plug-in supportati da FireEye per browser e cloud storage
- Analisi contestuale del malware rilevato in formato JSON

Introduzione
Le minacce possono arrivare da ogni parte e ogni azienda affronta la sicurezza in modo diverso in base alle proprie esigenze, al settore e all'ambiente. Tuttavia, l'unica cosa che tutte le aziende hanno in comune è la necessità di disporre di una funzionalità di rilevamento delle minacce convalidata e supportata dall'intelligence, con un'analisi contestuale sufficiente per agire.

Con FireEye Detection On Demand, disponibile per i clienti FireEye attraverso un'API (Advanced Threat Intelligence), le organizzazioni possono inviare file in modo protetto per garantire la protezione dalle minacce odierne, sia che sfruttino i sistemi operativi Microsoft Windows o Apple OS X, sia che sfruttino le vulnerabilità delle applicazioni.

FireEye Detection On Demand sfrutta il motore di rilevamento esistente FireEye Multi-Vector Virtual Execution™ (MVX) e l'intelligence Driven Analysis (IDA) per raggiungere rapidamente un verdetto sui file inviati. MVX è un motore di analisi dinamico senza firma che controlla il traffico di rete sospetto per identificare attacchi che eludono i sistemi di difesa tradizionali basati su criteri e firme. IDA è una raccolta di motori contestuali con regole dinamiche, che rilevano e bloccano le attività dannose in tempo reale e retroattivamente grazie alle ultime informazioni basate su macchina, aggressore e vittima.

Rilevamento delle minacce avanzato in tutte le architetture di sicurezza
FireEye Detection On Demand è un servizio di rilevamento delle minacce proprio del cloud che analizza rapidamente i contenuti inviati per identificare il malware residente. A differenza delle soluzioni di sicurezza dei file basate su algoritmi di integrità dei file, controlli delle policy sulle minacce interne o meccanismi di controllo statici, i contenuti inviati vengono elaborati utilizzando le stesse tecnologie che supportano molte offerte consolidate di FireEye.

L'accesso a FireEye Detection On Demand è facilmente configurabile attraverso un'API. Può essere integrato nel flusso di lavoro del centro operativo di sicurezza (*Security Operations Center*, SOC), nell'analisi SIEM (*Security Information and Event Management* [Informazioni di sicurezza e la gestione degli eventi)], nei repository di dati, nelle applicazioni web dei clienti e così via. Offre capacità flessibili di analisi di file e contenuti per identificare comportamenti dannosi ovunque l'azienda ne abbia bisogno.

Oltre a ricevere un verdetto per ogni file e contenuto inviato tramite Detection On Demand, si ricevono dettagli contestuali di supporto, quali file, registro, modifiche di processo e di rete, nonché i risultati rilevanti derivanti dall'aggiornamento continuo di FireEye Dynamic Threat Intelligence.

Come funziona Detection On Demand

FireEye Detection On Demand confronta il contenuto inviato con le più recenti tattiche conosciute e le firme degli attori di minaccia utilizzando l'analisi statica, l'intelligenza artificiale e l'apprendimento automatico. Inoltre, FireEye determina la possibilità di effetti secondari o combinatori in più fasi del ciclo di vita dell'attacco per scoprire exploit e malware finora sconosciuti.

Figura 1. Come funziona Detection On Demand.

FireEye Developer Hub

È possibile dare un'occhiata al FireEye Developer Hub all'indirizzo https://fireeye.dev per scoprire i plug-in e il codice di esempio e collaborare con la comunità di sviluppo di FireEye a Detection On Demand.

Informazioni sull'acquisto

Detection On Demand è disponibile attraverso i normali canali FireEye o direttamente attraverso l'AWS (Amazon Web Services) Marketplace (per i contenuti a basso volume).

Durante l'acquisto del servizio bisogna specificare la propria esigenza in base al numero di invii che si prevede di effettuare nel corso di un solo anno. Gli acquisti su AWS Marketplace prevedono una quota mensile di invio, fatturata annualmente. La velocità di invio dei file è limitata a 100 al minuto. La velocità di invio degli hash è limitata a 200 al minuto.

È possibile che ai file e ad altro materiale inviato a Detection On Demand venga assegnato un valore di invio superiore a un invio; FireEye ti comunicherà i valori standard di invio.

Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye Italia Srl
Piazza IV Novembre, 7. 20124 Milano Italia
+39 0294750535
italy@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.