

SCHEMA TECNICA

Digital Threat Monitoring

Notifiche istantanee di minaccia per la tua presenza digitale



CARATTERISTICHE PRINCIPALI

- Monitoraggio in tempo reale delle minacce digitali per le tue risorse
- Notifiche istantanee qualora la tua azienda o i tuoi dati vengano menzionati o presi di mira
- Avvisi quando la tua azienda o i tuoi dati vengono esposti o compromessi
- Supportato dal contesto di intelligence da parte degli esperti di sicurezza leader del settore
- Funzioni di ricognizione su misura per la tua azienda
- Assistenza degli analisti di intelligence personalizzabile

Le difese informatiche tradizionali sono pensate per proteggere le risorse presenti nella tua rete (nell'edge, all'interno del server o sull'endpoint).

In un mondo estremamente connesso come quello attuale, però, è necessario salvaguardare anche le risorse esterne al perimetro. Stiamo parlando, ad esempio, del brand della tua azienda, del personale e della tua comunità di partner integrati. La visibilità delle minacce che mirano a queste risorse può essere altrettanto importante quanto la visibilità delle minacce volte a colpire direttamente le risorse interne.

FireEye Digital Threat Monitoring™ riduce questo rischio evidenziando tempestivamente le minacce cui si trovano a far fronte le tue risorse esterne esposte. Il servizio viene erogato mediante un'esclusiva combinazione di tecnologia avanzata e intelligence sulle minacce leader a livello mondiale. Il servizio consente di contrastare in modo proattivo rischi quali perdita di credenziali, esposizione pubblica, minacce alle risorse e altri potenziali danni a livello monetario o di credibilità. Ottieni visibilità su aspetti del Web altrimenti inaccessibili, attraverso l'analisi mirata da parte di esperti di minacce informatiche di FireEye, che possono avvalersi del supporto dell'intera organizzazione FireEye Threat Intelligence.

La visibilità e le informazioni di cui hai bisogno

Digital Threat Monitoring si basa sulla tecnologia di riconoscimento Web automatico di proprietà, che raccoglie e analizza i contenuti dell'Open Web e del Dark Web. Ha come obiettivo principale siti impiegati per le comunicazioni da soggetti malintenzionati. Utilizzando query basate su parole chiave specificate dall'utente (ad es. brand, VIP e aziende partner), il servizio esegue un'analisi e genera avvisi di minacce in caso di corrispondenze potenzialmente sospette.

Questi avvisi di minacce sono accessibili attraverso l'apposito dashboard sul portale FireEye Intelligence Portal. Ciascun avviso contiene attributi quali stato, fonte e gravità, oltre a preziose informazioni per aiutare a gestire le risorse monitorate. Il dashboard degli avvisi ti consente inoltre di adottare specifiche misure su uno o più avvisi di minacce, ad esempio contattare un analista di FireEye.

PAROLE CHIAVE

Query basate su parole chiave definite dal cliente, che possono comprendere marchi, VIP e aziende partner.



TECNOLOGIA DI RICONOSCIMENTO WEB DI PROPRIETÀ

La tecnologia di riconoscimento Web automatico di proprietà raccoglie e analizza i contenuti dell'Open Web e del Dark Web.



INDAGINI E ANALISI

Con un livello di servizi Digital Threat Monitoring più elevato puoi applicare un flag a un avviso di minaccia specifico e richiedere un'indagine.



AVVISI E DASHBOARD

Digital Threat Monitoring conduce analisi e genera avvisi di minacce in caso di corrispondenze potenzialmente rilevanti.



Figura 1. Come funziona FireEye Digital Threat Monitoring.

Con un livello di servizi Digital Threat Monitoring più elevato puoi applicare un flag a un avviso e richiedere un'indagine. Un analista di intelligence FireEye condurrà una valutazione approfondita, fornendoti ulteriore contesto per aiutarti a comprendere la minaccia. Se necessario, ti farà inoltre avere tutte le informazioni in suo possesso, così come eventuali informazioni sulle minacce di FireEye correlate.

Tabella 1. Descrizioni del servizio FireEye Digital Threat Monitoring.

L'ambito delle prestazioni scelte per il servizio di Digital Threat Monitoring dipende dal programma di monitoraggio e dal livello di supporto degli analisti di cui hai bisogno.

Servizio	Descrizione
Digital Threat Assessment	Una valutazione occasionale eseguita nell'arco di 30 giorni utilizzando le parole chiave selezionate dal cliente. Gli analisti di intelligence di FireEye consegnano un unico rapporto che valuta le minacce identificate e include informazioni dettagliate.
Digital Threat Monitoring Standard (abbonamento)	Monitoraggio costante delle query basate su parole chiave selezionate dal cliente nell'Open Web, Deep Web e Dark Web. Le corrispondenze rilevanti generano avvisi accessibili all'interno del portale FireEye Intelligence.
Digital Threat Monitoring Advanced (abbonamento)	Abbonamento Standard e in più fino a 40 indagini svolte dagli analisti d'intelligence FireEye.
Digital Threat Monitoring Enterprise (abbonamento)	Abbonamento Standard e in più fino a 80 indagini svolte dagli analisti d'intelligence FireEye.

La seguente tabella evidenzia le principali differenze tra i vari livelli dell'offerta di Digital Threat Monitoring.

Tabella 2. Confronto delle funzionalità del servizio Digital Threat Monitoring.

Prestazioni	Digital Threat Assessment	Digital Threat Monitoring Standard	Digital Threat Monitoring Advanced	Digital Threat Monitoring Enterprise
Integrazione	Sì	Sì	Sì	Sì
Parole chiave illimitate	Sì	Sì	Sì	Sì
Utenti illimitati	-	Sì	Sì	Sì
Avvisi di minacce	-	Sì	Sì	Sì
Categorie di parole chiave	Tutte	Tutte	Tutte	Tutte
Indagini	-	tramite Expertise On Demand	40 all'anno/ 10 per trimestre	80 all'anno/20 per trimestre
Accesso al portale FireEye Intelligence	-	Sì	Sì	Sì
Riepiloghi degli avvisi di minacce digitali	-	Sì	Sì	Sì
Gestione autonoma delle parole chiave	-	Sì	Sì	Sì

Notifiche istantanee in un panorama in evoluzione

FireEye Digital Threat Monitoring fornisce notifiche istantanee qualora marchio, dati e VIP vengono menzionati, presi di mira o esposti. Questa soluzione aiuta a identificare le violazioni, le esposizioni e le minacce digitali nell'Open Web, nel Deep Web e nel Dark Web, e offre informazioni sull'esposizione della tua organizzazione nel panorama in continua evoluzione delle minacce, fornendo i seguenti vantaggi al tuo programma di sicurezza e alla tua situazione:

- **Rilevanza:** Funzioni di ricognizione su misura per la tua azienda.
- **Visibilità:** Avvisi quando la tua azienda o i tuoi dati vengono esposti o compromessi.
- **Preparazione alle emergenze:** Notifiche istantanee qualora la tua azienda o i tuoi dati vengano menzionati o presi di mira.
- **Competenze:** Contesto di intelligence e analisi da parte degli esperti di sicurezza leader del settore.
- **Minacce specifiche:** Raccolta dei dati e avvisi in tempo reale per il monitoraggio del profilo della minaccia digitale della tua azienda.

Per maggiori informazioni su come FireEye Digital Threat Monitoring può aiutare a ridurre i rischi mettendo tempestivamente in evidenza le minacce al di fuori del tuo perimetro, visita <https://www.fireeye.com/solutions/cyber-threat-intelligence/digital-threat-monitoring.html>.

FireEye Italia Srl

Piazza IV Novembre, 7, 20124 Milano, Italy.
+39 0294 750 535
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.

