MANDIANT®

SCHEDA TECNICA

Compromise Assessment

Rilevare la presenza di un attacco in corso o compiuto in passato nel vostro ambiente

PERCHÉ LE SOLUZIONI MANDIANT?

Le Soluzioni Mandiant offrono servizi in prima linea nel settore della sicurezza e dell'intelligence informatica dal 2004. I nostri esperti di sicurezza hanno contrastato le violazioni più complesse in ogni angolo del mondo. Conosciamo in dettaglio gli attori esistenti ed emergenti delle minacce, così come la rapida evoluzione delle loro tattiche, tecniche e procedure.

VANTAGGI

- Analisi dettagliata dello specifico ambiente al fine di riscontrare una violazione in corso o compiuta in passato
- Offre una panoramica sui rischi e sulle vulnerabilità del sistema
- Individua le problematiche legate allo stato della sicurezza
- Fornisce consigli per sviluppare ulteriormente la capacità della vostra azienda di rispondere in modo efficace agli incidenti
- Flessibilità per implementare tecnologie in loco o su cloud

Nello stato attuale della sicurezza informatica, le violazioni sono inevitabili.

– Kevin Mandia
Chief Executive Officer, FireEye

Mandiant Compromise Assessment combina la nostra lunga esperienza nella lotta alle intrusioni, le nostre soluzioni avanzate di intelligence informatica e la tecnologia di FireEye per fornire una valutazione che:

- Rileva gli attacchi in corso o compiuti in passato all'interno della vostra società
- Valuta il rischio individuando i punti deboli all'interno dell'architettura di sicurezza, le vulnerabilità, utilizzi impropri o violazioni di policy ed errori di configurazione della sicurezza del sistema
- Migliora la capacità della vostra società di rispondere in modo efficace agli incidenti

La necessità di Compromise Assessments
La violazione dei dati di alto profilo di cui si parla nei media rappresenta soltanto una parte minima delle attività malevole svolte dagli hacker a livello globale. Sapere se la sicurezza della vostra società è stata violata e trovare il modo per ridurre il rischio di attacco è fondamentale per evitare di essere la prossima azienda a finire in prima pagina per una violazione dei dati.

Il nostro approccio
Combiniamo la nostra lunga esperienza nel rispondere alle intrusioni e le nostre soluzioni avanzate di intelligence informatica con una struttura modulare di tecnologie FireEye per fornire una valutazione che soddisfi i requisiti aziendali in termini di velocità, scalabilità ed efficienza. Oltre a riscontrare una violazione in corso o compiuta in passato, la valutazione offre:

Contesto estrapolato da informazioni sulle minacce
Identificazione dell'autore dell'attacco e delle motivazioni per consentire alle società di sapere se vengono prese di mira.

Individuazione dei rischi
Rilevamento dei punti deboli nell'architettura di sicurezza e nella configurazione, compresa l'assenza di patch o software di sicurezza.

Agevolazione delle indagini future
Consulenza strategica per consentire agli esperti di sicurezza della vostra società di rispondere meglio alle intrusioni.

I consulenti di Mandiant si avvalgono delle tecnologie FireEye per cercare endpoint, monitorare il traffico di rete, ispezionare e-mail e analizzare registri di altri dispositivi di sicurezza al fine di rilevare la presenza di un attacco. I consulenti utilizzano inoltre tecniche di analisi dei dati senza firma per individuare le attività di aggressori precedentemente passate inosservate. I clienti scelgono la combinazione di tecnologie che più si addice al loro ambiente.

- Ispezione degli endpoint: gli agenti FireEye Endpoint Security effettuano un rilevamento in tempo reale delle attività malevole, inclusi i malware e altre tattiche, tecniche e procedure e analizzano gli endpoint di Windows, macOS e Linux. Gli esperti Mandiant garantiscono la flessibilità necessaria per le implementazioni in loco e su cloud.
- Ispezione della rete: i sensori di FireEye Network Security vengono implementati in punti di monitoraggio strategici dell'impresa al fine di contrastare attività compromettenti quali comunicazioni di comando e controllo di malware, accessi remoti non autorizzati e furto di dati.
- Ispezione di e-mail: la soluzione FireEye Email Security è condotta in loco o su cloud può essere configurata al fine di effettuare un'ispezione passiva delle e-mail in entrata e in uscita. L'ispezione dinamica degli allegati consente agli esperti di Mandiant di rilevare le intrusioni prima di altri prodotti basati su firma.
- Ispezione dei registri: i consulenti di Mandiant fanno leva su diverse tecnologie in grado di analizzare i registri di applicazioni e le infrastrutture al fine di individuare le attività malevoli.

ISPEZIONE DEGLI ENDPOINT

- Segnalazione in tempo reale delle attività sospette o malevole in corso
- Rilevamento di malware commerciali mediante il motore antivirus integrato dell'agente FireEye
- Supporto multi-piattaforma per il sistema operativo
  - Windows
  - macOS
  - Linux
- Individuazione di anomalie che indicano la presenza di malware sofisticati

ISPEZIONE DELLA RETE

- Acquisizione di pacchetti completi combinata con firme di rilevamento personalizzate
- Rilevamento automatizzato e decodifica del traffico di comando e controllo dell'autore dell'attacco

ISPEZIONE DI E-MAIL

- Rileva gli attacchi mirati di phishing compiuti dagli hacker per riottenere l'accesso all'ambiente dopo un evento di correzione
- Utilizza il motore Multi-Vector Virtual Execution™ (MVX) senza firme per analizzare gli allegati di e-mail e gli indirizzi URL rispetto a un'ampia struttura a matrice multipla di sistemi operativi, applicazioni e browser web
- Supporta l'analisi delle immagini dei sistemi operativi Microsoft Windows e macOS
- Analizza le minacce nascoste nei file, compresi gli allegati crittografati e protetti da password

Per maggiori informazioni sulle Soluzioni Mandiant, visita il sito: **www.FireEye.com/mandiant**

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

Informazioni sulle Soluzioni Mandiant
Le Soluzioni Mandiant offrono esperienza di prima linea e intelligence sulle minacce leader di mercato, con funzionalità continua di security validation in grado di fornire alle organizzazioni gli strumenti necessari per aumentare l'efficacia della sicurezza e ridurre i rischi aziendali.

MANDIANT®