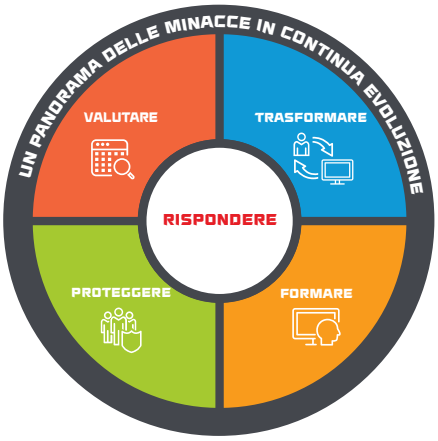
SCHEDA TECNICA

Servizi di consulenza Mandiant e MDR

Interveniamo contro le violazioni gravi e consentiamo alle aziende di proteggere le proprie risorse.

Quadro di riferimento per le esigenze di sicurezza



"Mandiant è all'avanguardia nell'aiutare le organizzazioni a ripensare il modo di prepararsi alle violazioni della sicurezza".

Michael Chertoff
Ex Segretario della Sicurezza Nazionale

Mandiant: la differenza
FireEye Mandiant è in prima linea nello sviluppo di soluzioni per la sicurezza e l'intelligence sule minacce informatiche dal 2004. I nostri esperti di sicurezza hanno dovuto contrastare le violazioni più complesse del mondo. Conosciamo in dettaglio sia le minacce esistenti che quelle emergenti, così come la rapida evoluzione delle tattiche, delle tecniche e delle procedure utilizzate dagli hacker.

Siamo leader nel settore della risposta agli incidenti informatici e dei servizi di sicurezza guidati dalle informazioni e basati sul rischio e aiutiamo le aziende a contrastare gli aggressori prima, durante e dopo un incidente.

Forte della profonda comprensione del comportamento degli aggressori, dell'impareggiabile intelligence sulle minacce e della tecnologia sviluppata ad hoc, i servizi Mandiant di valutazione della sicurezza, trasformazione, formazione e di rilevamento e risposta gestiti (MDR) aiutano a costruire la resilienza funzionale e a chiudere le falle di sicurezza al fine di ridurre il rischio aziendale.

Competenze: da oltre 15 anni in prima linea nello sviluppo di metodologie per contrastare le violazioni più gravi. Noi siamo in grado di vedere quello che gli hacker hanno fatto, come lo hanno fatto, gli strumenti e le tecniche che hanno utilizzato e quello che stavano cercando. Questo ci permette di avere un quadro generale, di comprendere come evolve il comportamento e le motivazioni degli hacker in un modo che altri non conoscono.

Intelligence: l'approccio ai servizi di Mandiant si basa su importanti informazioni di intelligence informatica fornite da centinaia di esperti di informazioni sulle minacce, da migliaia di indagini condotte da Mandiant, da prodotti FireEye e dai nostri servizi di protezione gestiti per una visibilità globale sul panorama delle minacce in rapida evoluzione.

Tecnologia: Gli esperti di Mandiant si avvalgono di tecnologie per endpoint, sensori di rete e piattaforme analitiche di FireEye che possono funzionare sia sul cloud che in loco, a seconda delle esigenze del cliente, e se viene utilizzato Windows, Linux o macOS. Grazie alle nostre tecnologie possiamo rispondere rapidamente su larga scala, riducendo al minimo le spese.

Riepilogo dei servizi speciali di Mandiant.

Funzione di sicurezza	Esigenze di sicurezza	Servizi	Panoramica	Vantaggio
Rispondere	**Risposta alla violazione**	**Servizi di risposta agli eventi**	Indagare, contenere e risolvere gli eventi critici per la sicurezza in modo veloce, scalabile ed efficiente.	Risoluzione degli incidenti gravi legati alla sicurezza e messa in pratica di soluzioni a lungo termine.
		Assistente in sito per la risposta agli incidenti	Stabilire i termini e le condizioni per i servizi di risposta agli incidenti.	Ridurre significativamente i tempi di risposta agli incidenti, riducendo l'impatto complessivo di una violazione.
Valutare	**Controllare la presenza di un autore di attacco**	**Compromise Assessment**	Verificare se la sicurezza del vostro ambiente è o è stata oggetto di violazioni, valutare il rischio futuro di compromissione in base allo stato della sicurezza e migliorare la vostra capacità di reazione.	Saprete se la vostra azienda è stata o meno compromessa, attualmente o in precedenza.
	Prepararsi a rispondere	**Valutazioni di Red Team, Purple Team**	Mettere alla prova la condizione di sicurezza contro le più recenti tecniche, tattiche e procedure (TTP) degli aggressori che incontriamo sulle prime linee della risposta agli incidenti.	Individuare i punti deboli non rilevati prima che lo faccia un hacker.
		Valutazione del programma di sicurezza	Valutazione indipendente della maturità del tuo monitoraggio di sicurezza e delle capacità di risposta, basata sulla nostra esperienza in prima linea.	Valutazione dell'efficienza del programma di sicurezza informatica al fine di migliorare il livello di sicurezza e ridurre i rischi commerciali.
		Esercizio di simulazione	Mettere alla prova il piano di risposta agli incidenti informatici dell'azienda con uno scenario simulato.	Identificare in modo rapido ed efficace le discrepanze tra il processo documentato e la risposta effettiva.
	Valutare i controlli di sicurezza e il livello di sicurezza	**Security Program Assessment**	Valutazione approfondita dei programmi di sicurezza informatica della vostra azienda in dieci ambiti fondamentali per la sicurezza, ognuno dei quali viene confrontato con i requisiti di conformità, sicurezza e settore.	Valutazione dell'efficienza del programma di sicurezza informatica al fine di migliorare la posizione di sicurezza e ridurre i rischi commerciali.
		Verifica dell'integrità dei sistemi di controllo industriale (Industrial Control Systems, ICS)	Valutare in maniera minimamente invasiva la posizione di sicurezza informatica complessiva di un impianto industriale, creando un ponte tra sicurezza IT e OT.	Scoprire le vulnerabilità esposte del sistema di controllo industriale e creare un piano per ridurre i rischi per la sicurezza informatica del sistema.
		Valutazione della sicurezza della Active Directory	Minimizzare il rischio di errori di configurazione, i punti di debolezza nei processi e i metodi di sfruttamento dell'Active Directory.	Ridurre il rischio e l'impatto di un incidente di sicurezza rafforzando una superficie di attacco comune.
		Valutazioni dell'infrastruttura cloud	Migliorare le difese informatiche attraverso architettura e configurazioni del cloud migliori.	Minimizzare il rischio riducendo la superficie di attacco cloud dalle tecniche di sfruttamento più diffuse.
Trasformare	**Livello di sicurezza maturo**	**Sviluppo del Centro di Difesa Informatica (Cyber Defense Center)**	Progettare e mettere a punto un programma di operazioni di sicurezza per la difesa contro gli autori di minacce avanzate.	Migliorare il livello di difesa per ridurre l'impatto degli incidenti di sicurezza; raggiungere un consenso sui miglioramenti per la sicurezza e sulla priorità delle risorse.
Formare	**Formare il mio team**	**Formazione su prodotti, intelligence e competenze**	Permettere agli esperti di sicurezza di aggiornare e migliorare le competenze e le conoscenze necessarie per contrastare in modo efficace le sempre nuove minacce a cui devono far fronte.	Offrire al personale la possibilità di partecipare ad attività didattiche ed esercitazioni pratiche basate su indagini realistiche, e non su scenari ipotetici.
Proteggere	**Rilevamento e risposta gestiti**	**Managed Defense**	Un servizio 24 ore su 24, 7 giorni su 7 gestito da esperti che combina l'esperienza in prima linea con tecnologia e intelligence leader del settore.	Identificare tempestivamente le minacce per ridurre al minimo l'impatto di una violazione.
		Managed Defense per Endpoint	Un servizio 24 ore su 24, 7 giorni su 7 gestito da esperti che utilizza Fireeye Endpoint Security per rilevare, investigare e arginare tempestivamente le minacce all'endpoint.	Migliorare la visibilità attraverso la rete e accelerare la risposta.
		Managed Defense per la tecnologia operativa (operational technology, OT)	Un servizio 24 ore su 24, 7 giorni su 7 che sfrutta le competenze specialistiche per identificare i rischi e accelerare la risposta per i sistemi di controllo industriale (ICS) e la tecnologia operativa (OT).	Migliorare il livello di difesa dell'ambiente ICS/OT e ridurre l'impatto degli eventi di sicurezza.

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.