

**SCHEDA TECNICA**

# Ransomware Defense Assessment

**VANTAGGI**

- Individuare le risorse più esposte ad attacchi da parte di ransomware
- Identificare i punti deboli della tua sicurezza, bersaglio dei ransomware
- Identificare controlli di accesso facilitati sulle condivisioni dei file
- Riconoscere mancanze operazionali nella gestione delle attività di ransomware
- Ricevere suggerimenti e linee guida altamente pratici per limitare gli attacchi ransomware

**Perché FireEye Mandiant**

FireEye Mandiant è in prima linea nello sviluppo di soluzioni per la sicurezza e l'intelligence informatica sin dal 2004. I nostri esperti di sicurezza contrastano le violazioni più complesse in ogni angolo del mondo. Conosciamo bene gli aggressori e le loro tattiche, tecniche e procedure (TTPs) in rapida evoluzione poiché facciamo leva sulle fonti di informazioni combinate di avversari, computer e vittime.

Il servizio Ransomware Defense Assessment è il frutto dell'esperienza maturata nel rispondere e nel risolvere incidenti di ransomware, nonché nel raccogliere informazioni sulle minacce relative a ransomware emergenti e in evoluzione.

**Panoramica**

Ransomware Defense Assessment di FireEye Mandiant valuta l'efficacia della capacità di un'azienda di prevenire, rilevare, contenere e risolvere un attacco ransomware. Gli esperti Mandiant sono in grado di analizzare elementi tecnici e non tecnici del tuo programma di sicurezza per capire in che modo il tuo team risponderà a un attacco ransomware.

Gli esperti Mandiant valutano l'impatto tecnico che un attacco ransomware potrebbe avere sulla tua rete interna, scoprono quali dati potrebbero essere compromessi o andare persi e testano i punti di forza e di debolezza dei tuoi controlli di sicurezza nel rilevare e rispondere a un attacco ransomware.

**Metodologia**

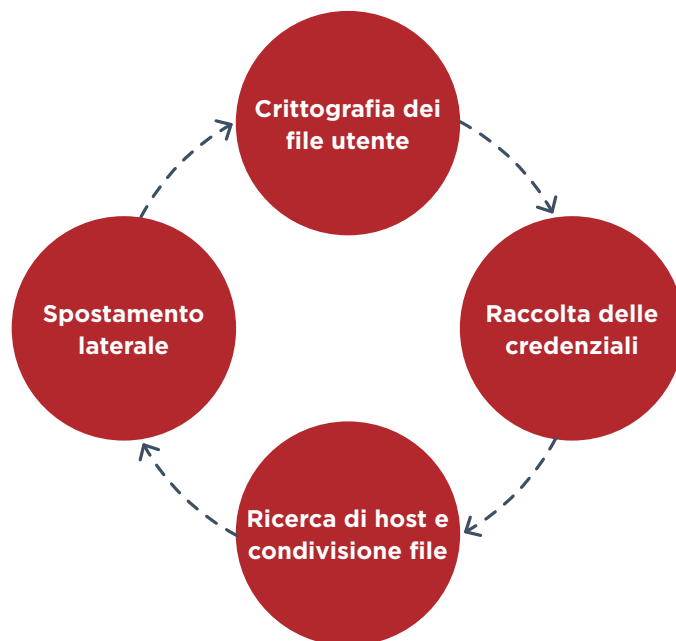
Il servizio Ransomware Defense Assessment include la revisione della documentazione, l'analisi della configurazione di accesso, workshop di approfondimento e simulazioni di comportamento degli attacchi ransomware nel mondo reale.

Il servizio Ransomware Defense Assessment si concentra su quattro competenze fondamentali in materia di ransomware:

- **Architettura di sicurezza.** Le tecnologie, le reti e i controlli di sicurezza necessari a difendersi da un attacco ransomware e per continuare a lavorare.
- **Risposta.** La capacità di un'azienda di rispondere rapidamente a un attacco ransomware e di contenerlo.
- **Comunicazione.** Processi di comunicazione interna ed esterna utilizzati per consegnare i messaggi aziendali ai principali stakeholder. Comprende il coordinamento con l'assicurazione e la consulenza legale informatiche.
- **Ripristino.** I processi e l'approccio per correggere o ripristinare un attacco ransomware.

Le nostre simulazioni di attacchi ransomware reali:

- Scansione delle vulnerabilità di Windows sfruttate dal ransomware
- Scansione di condivisioni di file accessibili attraverso ransomware
- Simulare il movimento laterale del ransomware cercando di sfruttare le vulnerabilità scoperte o riutilizzare le credenziali raccolte
- Testare la segmentazione tra le reti per determinare se il ransomware può diffondersi in altri ambienti, come ad esempio:
  - Reti di produzione e impianti
  - Reti di infrastrutture di backup
  - Reti del mondo retail
  - Altre reti di sicurezza
- Simulare il comportamento di crittografia ransomware, utilizzando uno strumento di emulazione ransomware personalizzato e non distruttivo per simulare la crittografia di massa dei file
- Eseguire le tecniche utilizzate dagli aggressori per distribuire i ransomware



#### Durata e risultati finali

La valutazione Ransomware Defense Assessment richiede in genere una settimana. Può essere consegnata in loco o da remoto.

Dopo l'operazione, Mandiant fornisce un report che include:

- Sintesi con punti di forza e aree da migliorare
- Informazioni tecniche sul processo di testing
- Risultati dettagliati, classificati per gravità
- Executive briefing

Per ulteriori informazioni su FireEye, visita il sito Web [www.FireEye.com](http://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.

