SCHEDA TECNICA

Servizi di risposta agli eventi

Indagare, contenere e risolvere gli eventi critici per la sicurezza in modo veloce, scalabile ed efficiente

CASO DI STUDIO: I SERVIZI DI RISPOSTA AGLI EVENTI DI MANDIANT IN AZIONE

Una multinazionale attiva nel settore dei servizi professionali, con decine di migliaia di computer in tutto il mondo, si è rivolta a Mandiant per reagire a una potenziale violazione di dati critici dei clienti.

Giorno 1 – I consulenti Mandiant hanno avviato l'implementazione della sua tecnologia endpoint basata su cloud entro quattro ore dalla notifica su 18.000 sistemi.

- L'indagine è iniziata il giorno stesso.
- Prova materiale della violazione individuata entro quattro ore dall'inizio dell'indagine.

Giorno 6 – La maggior parte del lavoro investigativo è stato concluso. Analisi svolta su oltre 18.000 endpoint, analizzando in modo approfondito la risposta dal vivo su 80 sistemi.

Giorno 7 – Contenimento eseguito senza interruzione dell'attività. Gli esperti Mandiant hanno continuato a monitorare la rete per garantire l'assenza di ulteriori tentativi di violazione da parte dell'aggressore.

Giorno 11 - Il cliente è tornato alle sue attività lavorative come al solito.

Tutto il lavoro è stato effettuato da remoto.

FireEye Mandiant è in prima linea nello sviluppo di soluzioni per la sicurezza e l'intelligence informatica dal 2004. I nostri esperti di sicurezza hanno contrastato le violazioni più complesse in ogni angolo 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.

Abbiamo solide competenze di indagine e di risoluzione, acquisite reagendo a migliaia di incidenti con le informazioni sulle minacce e con la tecnologia all'avanguardia di FireEye, leader del settore per quanto riguarda le reti e gli endpoint.

Il lavoro di Mandiant sugli eventi più estesi e più noti attribuisce un ruolo di primo piano ai nostri esperti nell'assistere i clienti in tutti gli aspetti della risposta agli eventi: dalla reazione tecnica alla gestione della crisi.

Aiutiamo i clienti a indagare e a risolvere i problemi in modo più veloce ed efficiente, affinché possano dedicarsi a ciò che è più importante: la loro attività.

Panoramica

L'utilizzo del cloud e delle soluzioni on premise consente di avviare immediatamente le indagini, gestendo al contempo i problemi relativi alla riservatezza dei dati del cliente. Gli esperti di sicurezza di Mandiant possono iniziare in poche ore ad analizzare il traffico di rete e le informazioni provenienti da migliaia di endpoint. L'accesso privilegiato alle informazioni sulle minacce direttamente dalla prima linea di ricerca sull'attacco e da altre fonti di informazioni fornisce ai team di risposta agli eventi di Mandiant informazioni sulle ultime tattiche, tecniche e procedure (TTP) di chi attacca.

Gli esperti di Mandiant sanno bene che una risposta completa agli eventi e alle violazioni va oltre l'indagine tecnica, il contenimento e il ripristino. Prestiamo, quindi, assistenza anche nella comunicazione esecutiva e nella gestione delle crisi, per quanto riguarda gli aspetti legali, normativi e delle pubbliche relazioni. La gestione delle crisi è un fattore critico per limitare i danni alla reputazione e la responsabilità legale.

Tabella 1. Tipi di incidenti che generalmente trattiamo.

Furto di proprietà intellettuale	Furto di segreti commerciali o di altre informazioni riservate.
Reati finanziari	Furto dei dati delle carte di pagamento, bonifici e trasferimenti di denaro illeciti, estorsione e ransomware.
Informazioni di identificazione personale (IIP)	Divulgazione di informazioni utilizzate per l'identificazione univoca delle persone.
Informazioni sanitarie riservate (Protected Health Information, PHI)	Divulgazione di informazioni riservate relative all'assistenza sanitaria.
Minacce interne	Attività inappropriate o illegali svolte da dipendenti, fornitori e altri operatori all'interno dell'azienda.
Attacchi distruttivi	Attacchi con l'unico scopo di mettere in difficoltà l'organizzazione che rendono inutilizzabili i sistemi informatici o le informazioni.

MANDIANT: LA DIFFERENZA

- **Esperienza investigativa:** gli investigatori di Mandiant hanno affinato le proprie competenze affrontando le indagini più estese e più complesse del mondo e risolvendone i problemi.
- **Informazioni sulle minacce:** informazioni leader del settore, ottenute combinando dati di prima linea sulla risposta agli incidenti, scoperta e ricerca dettagliate di tecniche tradizionali di attacco attraverso fonti di dati di terze parti, informazioni FireEye Dynamic Threat Intelligence acquisite tramite le tecnologie FireEye e da altre fonti di informazioni sulle FireEye Threat Intelligence.
- **Tecnologia:** gli esperti Mandiant utilizzano l'innovativo cloud di FireEye e le tecnologie on premise consentendo di avviare le indagini immediatamente. Le nostre tecnologie offrono una risposta rapida su larga scala, rendendo visibile il traffico di rete e gli endpoint con Microsoft Windows, Linux e macOS X.
- **Gestione delle crisi:** gli esperti che rispondono agli eventi vantano anni di esperienza nella consulenza sugli incidenti legati alla comunicazione, come la comunicazione esecutiva, le pubbliche relazioni e i requisiti di divulgazione.
- **Analisi del malware:** gli esperti FireEye di reverse engineering analizzano i malware e scrivono decoder e parser personalizzati per fornire informazioni sulle capacità e i TTP utilizzati dagli aggressori.
- **Copertura 24x7 le risposte agli incidenti:** analisi 24x7 sull'attività dell'aggressore durante le indagini e le soluzioni fornite da FireEye Managed Defense.

Il nostro approccio

Le indagini di Mandiant comprendono analisi a livello di host e di rete e basate sugli eventi per una valutazione completa e olistica dell'ambiente. Le nostre reazioni sono studiate appositamente per aiutare i clienti a reagire agli eventi e a riprendersi, gestendo al contempo i requisiti normativi e i danni alla reputazione. Durante le indagini, i consulenti Mandiant di solito identificano:

- Applicazioni, reti, sistemi e account utente coinvolti
- Software dannoso e vulnerabilità sfruttate
- Informazioni violate o rubate

Analisi dell'evento

1. **Installazione delle risorse tecnologiche/analisi degli elementi iniziali:** installiamo la tecnologia più appropriata per una risposta agli eventi veloce e completa. Indaghiamo sugli elementi iniziali forniti dal cliente per iniziare a costruire gli indicatori di compromissione (Indicators of Compromise, IOC) che individueranno l'attività dell'aggressore, esaminando al contempo l'ambiente per rilevare tutti gli indicatori di attività dannose.
2. **Pianificazione della gestione delle crisi:** collaboriamo con i manager, gli uffici legali, i dirigenti aziendali e il personale di sicurezza di alto livello per sviluppare un piano di gestione della crisi.
3. **Determinazione della portata dell'evento:** monitoriamo l'attività dell'aggressore in tempo reale e ricerchiamo prove forensi della sua attività precedente, per determinare la portata dell'evento.
4. **Analisi approfondita:** analizziamo le azioni intraprese dall'aggressore per determinare il vettore di attacco iniziale, stabilire la cronologia delle attività e individuare l'estensione del danno. Queste operazioni possono includere:
   - Analisi della risposta in tempo reale
   - Analisi forense
   - Analisi del traffico di rete
   - Analisi dei log
   - Analisi del malware
5. **Valutazione dei danni:** individuiamo i sistemi colpiti, le strutture, le applicazioni e il livello di divulgazione delle informazioni.
6. **Risoluzione:** sviluppiamo una strategia di contenimento e di risoluzione personalizzata a seconda delle azioni dell'aggressore, in base alle esigenze dell'attività, con l'obiettivo di impedire l'accesso all'aggressore e rafforzare le condizioni di sicurezza dell'ambiente, per prevenire o limitare i danni di eventuali attacchi futuri.

Elementi forniti

Report esecutivi, di indagine e di risoluzione per l'esame minuzioso da parte di terzi.

- **Sintesi esecutiva:** riepilogo di alto livello che descrive le tempistiche e il processo investigativo, i principali risultati ottenuti e le attività di contenimento/eradicazione.
- **Report di indagine:** dettagli sulle tempistiche dell'attacco e sul percorso critico (in che modo l'aggressore ha agito nell'ambiente). I report includono un elenco dei computer coinvolti, la loro ubicazione, gli account utente e le informazioni rubate o a rischio.
- **Report di risoluzione:** dettagli delle misure di contenimento/eradicazione adottate, con consigli strategici per rafforzare le condizioni di sicurezza dell'organizzazione.

Sospettate una violazione? Inviateci un'e-mail a **investigations@mandiant.com** o visitate **https://www.fireeye.com/company/incident-response.html**

FireEye Italia Srl.
Piazza IV Novembre, 7. 20124 Milano, Italy
+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.

FIREEYE™