IL VANTAGGIO DEL DIFENSORE

SINTESI GENERALE

MANDIANT

Il Vantaggio del difensore è l'idea della difesa che le aziende eseguono contro gli attacchi che avvengono nel loro ambiente. Fornisce un vantaggio cruciale per il fatto che hanno il controllo del territorio in cui incontreranno i loro avversari. Le aziende fanno fatica ad approfittare di tale vantaggio.

7,5

Le aziende che si abbonano a una media di feed per informazioni sulle minacce*

66,5%

Il 66,5% sparge ancora la CTI tramite e-mail, ppt, fogli di lavoro, documenti**

43%

Solo il 43% possiede requisiti di CTI documentati**

Ogni giorno, le aziende si ritrovano a fronteggiare una nuova ondata di cyber attacchi sempre più sofisticati. Con attacchi significativi come ransomware ed estorsioni sfaccettate che dominano la scena, i leader della sicurezza si dimenano nel trovare soluzioni mentre affrontano nuovi requisiti di sicurezza informatica imposti da legislatori e dirigenti aziendali che vogliono risposte. La realtà con la quale si confrontano i team sulla sicurezza potrebbe sembrare una battaglia difficile, con molti che perdono terreno nei confronti degli avversari a causa della mancanza di risorse e competenze, più strumenti mal configurati.

Attività di sicurezza disorganizzate, scoordinate o di conservazione non possono fornire risposte alle tante domande poste dai dirigenti aziendali e dagli azionisti, né possono dare fiducia a livello di reattività. Concentrandosi su come le persone usano gli strumenti a disposizione e sviluppano le capacità per proteggere l'attività, le aziende hanno ampliato l'orizzonte al di là del SOC al più vasto ambito della Difesa informatica.

*Forrester Wave ETIS D', 2021
**Sondaggio 2021 CTI SANS

I ruoli della difesa informatica

Intelligence
Guida

Cacciare
Caccia alle minacce e stime sulle compromissioni

Rilevare
Monitoraggio e investigazionedegli allarmi

Rispondere
Risposta e recupero sugli incidenti

Convalidare
Test e controlli di convalida sugli obiettivi

Comandare e controllare
Mantenere la missione

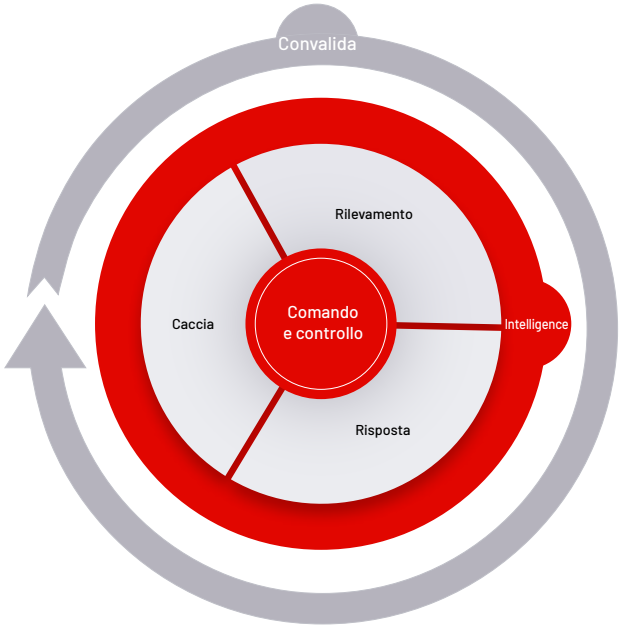
La Difesa informatica è uno dei quattro domini integrati della Sicurezza informatica, con gli altri che sono la Governance di sicurezza, l'Architettura di sicurezza e la Gestione del rischio di sicurezza. Composta da sei funzioni, la Difesa informatica consente alle aziende di continuare a operare nonostante le minacce.

Ciascuna funzione di Difesa informatica rappresenta differenti attività, azioni o responsabilità concentrate su diversi obiettivi, collettivamente lavorando per identificare e rispondere alle minacce nei confronti dell'azienda. Serve un cambio di paradigma per muoversi da tecnologie sul pezzo ad attivare tali funzioni; unificarle per ridurre in modo significativo il rischio e l'impatto di cyber attacchi a un'azienda.

Quando interamente ottimizzata e attivata, la Difesa informatica permette alle aziende di rispondere a domande come:

- Chi ci sta bersagliando e cosa vogliono?
- Siamo stati compromessi?
- Sapremmo di essere stati compromessi?
- Siamo pronti a rispondere a una violazione?
- I nostri investimenti sulla sicurezza sono efficaci?

Figura 1: i ruoli della Difesa informatica in azione



> Il Profilo sulle minacce informatiche è forse il documento più importante per un programma di cyber intelligence. La maggior parte dei programmi o non ne ha uno o non lo usa per portare avanti le proprie operazioni.

Andrew Close, Consulente principale, Intelligence Capability Development, Mandiant

Il ruolo di intelligence

Il sangue della Difesa informatica si basa sull'intelligence sulle minacce informatiche (CTI), che si collega a ogni funzione della difesa informatica. Quando viene implementata in modo efficace, la CTI fornisce informazioni sulle tattiche, tecniche e procedure (TTP) degli aggressori, sui loro obiettivi e moventi, oltre ad aiutare a scoprire possibili vulnerabilità all'interno dell'ambiente di un'azienda. Può esplorare la possibilità di un attacco e anche determinare l'impatto aziendale in caso avvenga.

I team di sicurezza possono investire in decine dei "migliori" abbonamenti di intelligence; tuttavia, anche la miglior intelligence è sprecata se non usata correttamente. È dunque importante capire chi consumerà l'intelligence, cosa ci faranno e come verrà comunicato prima di prendere decisioni d'acquisto.

Il ruolo di caccia

Il ruolo di caccia usa l'intelligence per identificare potenziali prove di una compromissione in corso o precedente all'interno dell'ambiente di un'azienda. Usando informazioni su un avversario specifico, i team di caccia adottano la mentalità di un minacciatore per sviluppare ipotesi su come egli potrebbe aver compromesso le difese di sicurezza dell'azienda, setacciando l'ambiente, raccogliendo più dati, analizzando i risultati e comunicando i risultati. Quando la caccia alla minaccia viene attivata come ruolo nella Difesa informatica, le aziende beneficiano di una capacità di risposta aumentata, miglioramenti di sicurezza, un'intelligence arricchita su minacce interne, più nuovi metodi di rilevamento delle minacce.

Il ruolo di rilevamento

Il ruolo di rilevamento identifica comportamenti malevoli in base all'attività od osservazione degli allarmi. L'intelligence sulle minacce si trova al centro del rilevamento effettivo, contestualizzando e categorizzando incidenti, report e feed di dati per generare informazioni che possono definire l'obiettivo e la metodologia di un aggressore. Queste informazioni vengono usate per dare precedenza ad analisi e risoluzione delle minacce che pongono il rischio maggiore.

Molti team SOC tradizionali affrontano volumi di allarmi insostenibili per l'analisi a causa di troppi feed di dati, tuttavia i team SOC moderni unificano allarmi simili usando l'automazione, segnalando casi di alta precisione per un'investigazione più approfondita.

> Avere una comprensione approfondita delle TTP basata su un'intelligence sulle minacce affidabile è vitale per gli analisti SOC. Una comprensione delle violazioni passate aiuta gli analisti a predire l'attività futura degli aggressori a un singolo sistema e a un incidente aziendale.

David Lindquist, Managed Defense Operations Manager, Mandiant

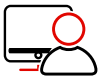
Il ruolo di risposta

Il ruolo di risposta nell'ambito della Difesa informatica si occupa della risposta e rimedio alle compromissioni all'interno dell'ambiente di un'azienda. Dopo l'identificazione dell'attività sospetta da parte dei ruoli di rilevamento e caccia, il team di risposta conferma se quest'attività sia malevola e prende provvedimenti che includono: capire la compromissione a fondo, minimizzare l'impatto all'attività, consentirgli di tornare alle normali operazioni e rimuovere la minaccia dall'ambiente.

Per prevenire la ripetizione di incidenti, il ruolo di risposta deve anche identificare le lezioni imparate e comunicare miglioramenti al team responsabile del comando e controllo.

Il ruolo di convalida

Il ruolo di convalida assicura che l'ecosistema di controllo di sicurezza funzioni a dovere e protegga i beni vitali. La convalida di sicurezza può essere mirata, basata su missione, obiettivo o parte di una continua valutazione di controllo, fornendo dati quantitativi per guidare il processo decisionale su potenziali investimenti e risparmi. Attraverso l'uso dell'attività simulata, persone, processi e tecnologie di un'azienda vengono testati in sicurezza con attacchi attivi autentici per valutarne l'efficacia e identificare aree dove migliorare.



Il ruolo di comando e controllo

Il gruppo Comando e controllo si occupa di mantenere la missione e orchestrare tutte le altre funzioni per dare priorità alle risorse di Difesa informatica. Un compito importante di Comando e controllo consiste nel facilitare il flusso di informazioni tra ogni ruolo. In molti casi, le aziende sviluppano solide capacità e strumenti di rilevamento, ma mostrano scarsa risposta agli incidenti per una mancanza di procedure consolidate e documentate. Durante un grosso incidente, Comando e controllo si occupa principalmente di comunicare e coordinare le attività di investigazione e rimedio.

> È comune per le aziende eseguire per conto proprio la risposta agli incidenti in preda al panico e tentare di ottenere un rimedio prematuro. Spesso saltano direttamente al rimedio e introducono cambiamenti che complicano l'investigazione. Questo approccio acchiappa la talpa allungherà l'investigazione, causando sforzi di rimedio incompleti e porta ad attacchi ripetuti.

Eric Scales, Vicepresidente, Mandiant

Attivare la Difesa informatica per capitalizzare sul Vantaggio del difensore

I ruoli di Difesa informatica non devono solo essere stabiliti, ma anche attivati e resi operativi contro gli aggressori. I ruoli di Difesa informatica non devono essere attivati tutti assieme. Le capacità possono essere costruite e maturate nel tempo. Per accelerare l'attivazione delle capacità di Difesa informatica, le aziende sfruttano SaaS e servizi gestiti selezionati in modo strategico al fine di fornire una copertura di Difesa informatica completa, microservizi per necessità mirate e risorse esperte per implementazione interna e sviluppo delle operazioni. Le aziende devono concentrarsi sulle aree che contano di più e impiegare acceleratori per galvanizzare il loro vantaggio del difensore.

Nel Vantaggio del difensore, Mandiant fornisce consigli completi passo dopo passo su come portare avanti le capacità di sicurezza di un'azienda per costruire un programma di sicurezza completo e solido, consentendo loro di prendere in mano il proprio ambiente e contrattaccare gli aggressori.

Ottieni la tua copia gratuita de **Il Vantaggio del difensore** oggi stesso
www.mandiant.com/defenders-advantage

Se vuoi galvanizzare le tue difese informatiche, gli esperti di Mandiant sono disponibili per fornire guida, aiuto e supporto. **Clicca qui per iniziare la conversazione oggi stesso.**
www.mandiant.com/contact-us

Informazioni su Mandiant

La sicurezza effettiva si basa sulla giusta combinazione di competenza, intelligence e tecnologia. Dal 2004, Mandiant è un leader di fiducia nel settore della sicurezza per le aziende che non possono permettersi di perdere. Oggi, Mandiant offre decenni di conoscenze di prima linea su scala attraverso soluzioni SaaS per aziende di tutte le dimensioni. Le offerte vanno da consulenza, difesa automatizzata, rilevamento gestito a risposta, intelligence sulle minacce e convalida di sicurezza per una Difesa informatica dimostrabile e trasformativa.

Per saperne di più, visita il sito **www.mandiant.com/managed**

Mandiant
601 McCarthy Blvd. Milpitas, CA95035
+1.408.321.6300
+1.833.3MANDIANT (362.6342)
info@mandiant.com

MANDIANT

©2021 Mandiant, Inc. Tutti i diritti riservati. Mandiant è un marchio registrato di Mandiant, Inc.
Altri marchi, nomi di prodotti e servizi sono o possono essere rivendicati come proprietà di terzi.