SOLUTION BRIEF

Accelera al massimo i tempi di rilevamento e interruzione, indagine e correzione con la soluzione per le operazioni di sicurezza di Fortinet

Executive Summary

Non è insolito che gli autori delle minacce abbiano spesso molto tempo a disposizione all'interno di un'organizzazione per raggiungere i propri obiettivi prima di essere scoperti Secondo una ricerca, il team di sicurezza medio impiega da 16 a 204 giorni per rilevare un incidente di sicurezza in corso.[1] E il 75% dei professionisti della sicurezza afferma che l'attuale panorama delle minacce è il più complesso degli ultimi cinque anni.[2]

La soluzione per le operazioni di sicurezza di Fortinet utilizza l'intelligenza artificiale e le analisi avanzate per monitorare le attività di utenti, dispositivi, reti, e-mail, applicazioni, file e registri e rilevare azioni anomale o dannose che l'uomo potrebbe facilmente ignorare. In aggiunta, le integrazioni native del Fortinet Security Fabric tra i diversi componenti favoriscono lo scambio di informazioni esclusive per attuare il contenimento automatico, al fine di anticipare e mitigare i rischi. Di conseguenza, i team di sicurezza hanno più tempo per condurre un'indagine completa e porre rimedio ad ogni incidente in modo automatizzato e orchestrato, migliorando l'efficienza e la coerenza.

La metà delle organizzazioni dichiara di investire in intelligenza artificiale e machine learning per rilevare più rapidamente le minacce. Il 44% dichiara di utilizzare soluzioni SIEM e SOAR per migliorare i tempi di risposta.[4]

In generale, i clienti che adottano la soluzione per le operazioni di sicurezza di Fortinet hanno ridotto il tempo necessario per individuare e contenere gli attacchi da una media di 180 ore a meno di un'ora, spesso in pochi minuti, e successivamente per condurre l'indagine e apportare le correzioni in un intervallo di tempo compreso tra i 10 e i 15 minuti.[3]

L'evoluzione delle minacce e l'ampliamento della superficie di attacco comportano violazioni più complesse (e costose)

Da un panorama di minacce in costante evoluzione e una superficie di attacco in continua espansione a una significativa carenza di professionisti qualificati, i team di sicurezza devono affrontare quotidianamente molte problematiche. Di conseguenza, anche i gruppi più preparati di professionisti esperti faticano a proteggere le reti aziendali con un approccio efficace. Secondo il team di risposta agli incidenti di FortiGuard (un gruppo spesso chiamato a indagare sugli attacchi informatici), gli autori delle minacce sono rimasti inosservati sulle reti aziendali per una media di 36 giorni.[5] E questo è molto meno dei 204 giorni dichiarati in un recente report di IBM.[6] In entrambi i casi, è chiaro che gli autori delle minacce hanno in genere molto tempo per raggiungere i loro obiettivi.

Inoltre, le violazioni di sicurezza di successo stanno diventando sempre più costose da mitigare. Secondo un recente sondaggio, l'84% delle organizzazioni ha subito una o più violazioni negli ultimi 12 mesi e il 48% ha subito incidenti informatici la cui risoluzione ha richiesto un esborso finanziario di almeno 1 milione di dollari.[7]

La soluzione per le operazioni di sicurezza di Fortinet accelera il rilevamento e la risposta agli incidenti

Di conseguenza, le organizzazioni affermano di dare priorità agli investimenti in tecnologie avanzate come intelligenza artificiale e machine learning per rilevare i segnali di intrusione in tempi più rapidi, tecnologie centralizzate come SIEM e SOAR per accelerare la risposta agli incidenti di sicurezza e prodotti di sicurezza integrati per ridurre la complessità.[8]

Ecco perché la soluzione per le operazioni di sicurezza di Fortinet è fondamentale per le organizzazioni aziendali, in quanto offre:

- La più ampia gamma di sensori basati sul comportamento, distribuiti all'interno di un dominio specifico o tra domini diversi, per il rilevamento precoce e la prevenzione delle intrusioni informatiche
- Automazione centralizzata della sicurezza per aggregare, arricchire e analizzare le informazioni sulla sicurezza provenienti da questi e altri sensori, nonché per visualizzare, orchestrare e automatizzare le indagini e la risposta agli incidenti
- Una serie di servizi SOC aggiuntivi per valutare e migliorare la prontezza dei team e delle tecnologie interne, per accrescere tali team con risorse ad hoc o in modo costante e per fornire assistenza in caso di situazioni critiche

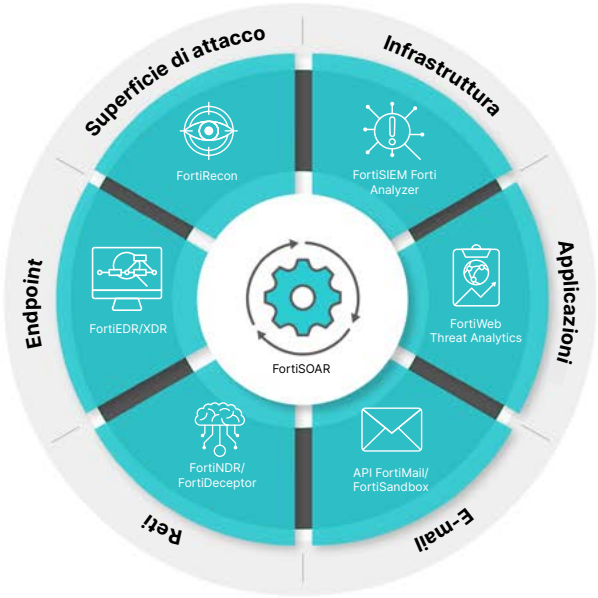

Figura 1: la soluzione per le operazioni di sicurezza di Fortinet

- Assistenza basata sull'IA generativa integrata per informare e accelerare le azioni degli analisti nelle indagini sulle minacce, nella strategia di risposta e in altre attività chiave

L'integrazione consente l'automazione con la soluzione per le operazioni di sicurezza di Fortinet

La soluzione per le operazioni di sicurezza di Fortinet è un'offerta integrata superiore alla somma delle sue parti Oltre a fornire un rilevamento efficace, i suoi componenti condividono automaticamente la threat intelligence e intervengono per aiutare le organizzazioni a passare da un modello di difesa informatica reattivo a uno proattivo. Di seguito sono riportati alcuni esempi di come la soluzione per le operazioni di sicurezza di Fortinet si integra con altri prodotti Fortinet e migliora la sicurezza dell'organizzazione.

- **FortiEDR:** Dopo aver effettuato la rilevazione basata sul comportamento di attività sospette o dannose in tempo reale su un dispositivo endpoint e bloccando azioni ad alto rischio come la crittografia dei file o l'instaurazione di una connessione di rete, l'integrazione nativa del tessuto tra FortiEDR e FortiGate NGFW consente la condivisione peer-to-peer, bidirezionale dell'intelligence sulle minacce.
- **FortiNDR:** Dopo aver individuato un comportamento sospetto o dannoso basato sulla rete da un dispositivo, FortiNDR può acquisire informazioni sul dispositivo da FortiEDR e persino attivare una quarantena del dispositivo di origine grazie alla sua integrazione fabric-native.
- **FortiRecon:** dopo aver valutato gli asset rivolti all'esterno, l'integrazione fabric-native di FortiRecon consente di ricevere ulteriori asset dai FortiGate NGFW da includere nell'inventario e nella scansione degli asset.
- **FortiDeceptor:** dopo aver rilevato l'intrusione di un autore di minacce, l'integrazione fabric-native consente a FortiDeceptor di indirizzare gli NGFW FortiGate a bloccare l'accesso ad altri dispositivi, restituendo al contempo le risposte previste per continuare a coinvolgere l'aggressore inconsapevole.
- **FortiSandbox:** dopo aver effettuato una valutazione del rischio basata sul comportamento, FortiSandbox può condividere tale valutazione con molti dispositivi Fortinet, tra cui NGFW FortiGate e FortiMail, per il blocco in tempo reale prima della distribuzione.
- **FortiAnalyzer:** l'integrazione nativa con l'intero portfolio Fortinet consente alle organizzazioni di impostare trigger di eventi e risposte di automazione.
- **FortiSIEM:** dopo che una ricca serie di analisi, comprese quelle di un workbench di machine learning, ha effettuato i rilevamenti, gli incidenti possono essere gestiti attraverso azioni di correzione abilitate da oltre 300 integrazioni tecnologiche o trasferiti senza problemi a FortiSOAR per una solida orchestrazione e automazione.
- **FortiSOAR:** una volta che FortiSOAR riceve gli avvisi di attività sospette, possono essere eseguite azioni di playbook automatizzati, come la distribuzione di strumenti di raggiro nella posizione giusta per ingannare e bloccare l'autore della minaccia.

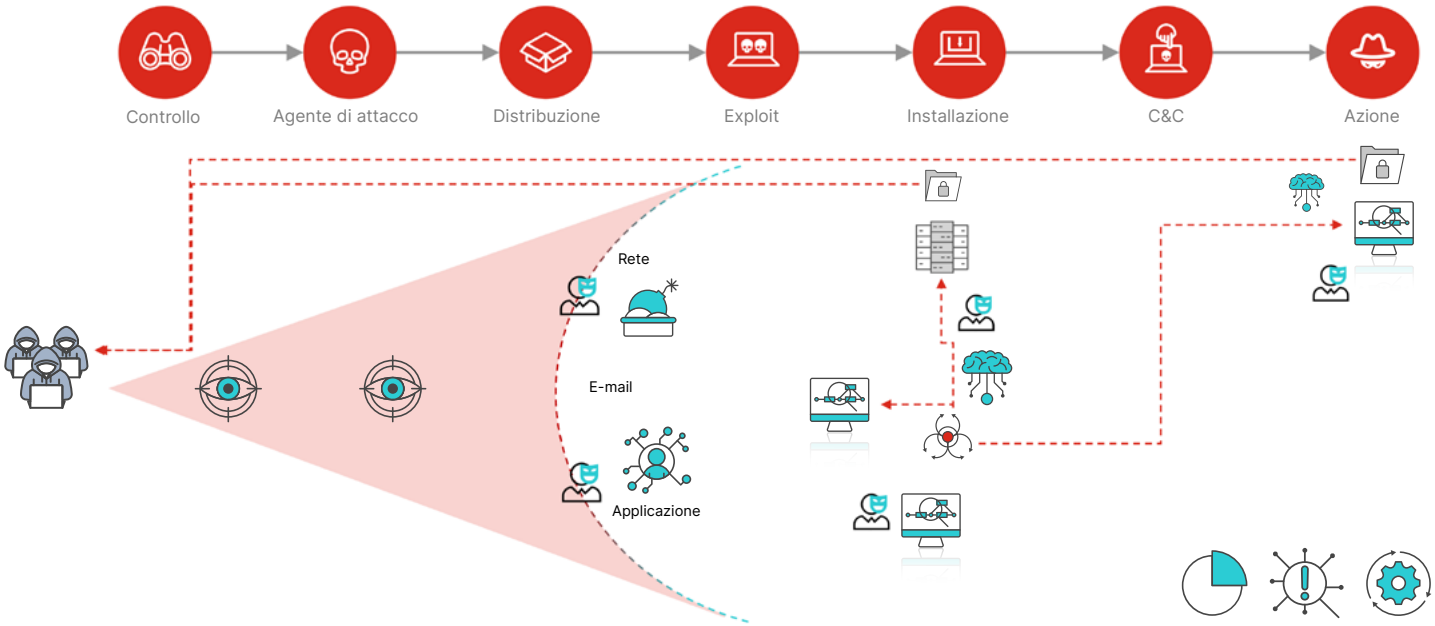

Figura 2: Componenti della soluzione per le operazioni di sicurezza di Fortinet applicati lungo la catena di attacco cibernetico.

I clienti che utilizzano la soluzione per le operazioni di sicurezza di Fortinet registrano un ritorno sull'investimento del 597%[9]

È stato dimostrato che investire nei componenti della soluzione per le operazioni di sicurezza di Fortinet riduce notevolmente i tempi di attesa, il rischio informatico e l'impegno nelle operazioni di sicurezza. Nello specifico:

- Prima di investire in sensori di rilevamento precoce e prevenzione, i clienti Fortinet hanno segnalato che, in media, i loro team impiegavano 21 giorni per rilevare le intrusioni informatiche e un altro giorno e mezzo per contenerle,[10] Dopo aver distribuito prodotti come FortiEDR, FortiNDR, FortiDeceptor e altri, i clienti hanno affermato di essere in grado di rilevare e contenere le attività degli autori delle minacce entro un'ora (e in pochi minuti nella maggior parte dei casi).[11]
- Prima di distribuire i componenti della soluzione per le operazioni di sicurezza di Fortinet, le organizzazioni segnalavano che l'indagine e la correzione degli avvisi richiedevano da due a tre giorni.[12] Dopo l'implementazione di componenti quali FortiAnalyzer, FortiSIEM, FortiSOAR o altri, le indagini potevano essere completate in 10-15 minuti.[13]
- Inoltre, i clienti hanno riferito che un team di sei persone (o addirittura di tre, in un caso) poteva gestire il lavoro di 12, con un netto miglioramento dell'efficienza operativa.[14]

Figura 3: Benefici quantificati dell'implementazione dei componenti delle operazioni di sicurezza di Fortinet.

ESG Research ha quantificato il valore di questi miglioramenti in termini di riduzione del rischio e di benefici finanziari attesi. La ricerca dimostra che un'organizzazione media ha quasi il 30% di probabilità di subire una violazione in un determinato anno, con un costo annuale previsto di 1,4 milioni di dollari.[15] In combinazione con i tempi più rapidi per il rilevamento e l'interruzione, l'indagine e la correzione, ESG Research ha calcolato un risparmio annuale di 1,39 milioni di dollari in termini di riduzione dei costi previsti per le violazioni implementando i componenti della soluzione per le operazioni di sicurezza di Fortinet.[16]

Inoltre, grazie all'aumento della produttività dopo l'implementazione della soluzione, i team di sicurezza hanno risparmiato in media 1,9 milioni di dollari sui costi del personale.[17] In definitiva, ESG Research stima un ritorno sull'investimento del 597% per le organizzazioni che investono nella soluzione per le operazioni di sicurezza di Fortinet, con un periodo di recupero dell'investimento inferiore a due mesi.[18]

Conclusioni

La soluzione per le operazioni di sicurezza di Fortinet consente alle organizzazioni di introdurre potenti funzionalità di rilevamento basate sull'intelligenza artificiale in tutta l'organizzazione digitale e di integrarsi con i controlli di sicurezza esistenti per ridurre notevolmente il tempo necessario per interrompere gli attacchi informatici lungo la Cyber Kill Chain. La soluzione consente inoltre ai team di sicurezza di orchestrare, automatizzare e aumentare le attività centralizzate di indagine e correzione degli incidenti, per una risposta più rapida e coerente. Infine, sono disponibili ulteriori servizi di esperti per valutare la predisposizione delle operazioni di sicurezza e assistere nella risposta agli incidenti di sicurezza, se necessario. L'ampiezza della copertura e la profondità dell'integrazione della soluzione per le operazioni di sicurezza di Fortinet aiutano i team di sicurezza a passare dall'approccio "rileva e rispondi", che richiede molto tempo, a un paradigma più rapido "rileva e interrompi, quindi procedi con l'indagine e la correzione" per una difesa informatica attiva.

1 Cost of a Data Breach Report 2023, IBM, 24 luglio 2023.

2 How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, ISC2, 31 ottobre 2023.

3 ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, 1 agosto 2023.

4 2023 Global Ransomware Report, Fortinet, 20 aprile 2023.

5 FortiGuard Labs, ultimo accesso: 21 novembre 2023.

6 Cost of a Data Breach Report 2023, IBM, 24 luglio 2023.

7 2023 Global Cybersecurity Skills Gap Report, Fortinet, 21 marzo 2023.

8 2023 Global Ransomware Report, Fortinet, 20 aprile 2023.

9 ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, 1 agosto 2023.

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

16 Ibid.

17 Ibid.

18 Ibid.

Copyright © 2024 Fortinet, Inc. Tutti i diritti riservati. Fortinet®, FortiGate®, FortiCare® FortiGuard® e altri marchi sono marchi registrati di Fortinet, Inc. Anche altri nomi Fortinet qui citati possono essere marchi registrati e/o marchi di diritto comune di Fortinet. Tutti gli altri nomi di prodotti o società possono essere marchi registrati dei rispettivi proprietari. I dati riportati relativi a prestazioni e altre caratteristiche sono stati ottenuti con prove interne di laboratorio in condizioni ideali e, pertanto, le prestazioni effettive e altri risultati possono variare. Variabili di rete, diversità degli ambienti di rete e altre condizioni possono influenzare i risultati in termini di prestazioni. Nulla di quanto qui contenuto rappresenta un impegno vincolante per Fortinet, e Fortinet esclude qualsiasi garanzia, esplicita o implicita, eccetto quelle previste da un contratto scritto, firmato da un rappresentante legale di Fortinet, che garantisca esplicitamente all'acquirente che le prestazioni del prodotto indicato saranno conformi a determinati dati esplicitamente indicati. In tal caso, solo gli specifici dati prestazionali esplicitamente identificati in tale contratto scritto saranno vincolanti per Fortinet. Per chiarezza, qualsiasi garanzia è limitata alle prestazioni ottenute nelle stesse condizioni ideali delle prove interne di laboratorio di Fortinet. Fortinet esclude in toto qualsiasi convenzione, rappresentanza e garanzia, esplicita o implicita, sulla base del presente documento. Fortinet si riserva il diritto di cambiare, modificare, trasferire o comunque revisionare questa pubblicazione senza alcun preavviso. La versione applicabile della presente pubblicazione è quella più recente.

febbraio 19, 2024 10:59 AM

2431037-0-0-IT