CROWDSTRIKE

SERVIZI PROATTIVI E DI RISPOSTA AGLI INCIDENTI DI CROWDSTRIKE

Preparati, reagisci e neutralizza le compromissioni in modo rapido ed efficace

SERVIZI PROATTIVI E DI RISPOSTA AGLI INCIDENTI DI CROWDSTRIKE

SCEGLI I SERVIZI CHE MEGLIO SI ADATTANO ALLE TUE ESIGENZE

CrowdStrike® propone servizi di risposta agli incidenti (IR) e soluzioni proattive che svolgono un ruolo cruciale nella realizzazione di una strategia di sicurezza avanzata e nel blocco delle compromissioni. Tutti i servizi sono stati progettati per consentire alle aziende di reagire in modo rapido ed efficace a un incidente di sicurezza informatica, mentre le soluzioni proattive hanno lo scopo di migliorare la capacità di contrasto agli attacchi informatici subiti dai clienti.

Per realizzare questi obiettivi, CrowdStrike utilizza una squadra di professionisti della sicurezza con un background nell'intelligence, nelle forze dell'ordine e nel settore industriale; architetti di sistemi e ingegneri che hanno lavorato per le aziende più tecnologicamente avanzate del mondo e consulenti che hanno indagato sugli attacchi informatici più gravi del pianeta.

Facendo leva sulle funzionalità della piattaforma CrowdStrike Falcon®, questo gruppo di esperti offre un servizio di protezione degli endpoint impareggiabile che si basa sulla risposta agli incidenti in tempo reale, su analisi forensi dettagliate e su attività di threat intelligence grazie a cui nessuna minaccia passa inosservata. Oltre ad aiutare le aziende a prevedere e neutralizzare un'ampia gamma di incidenti di sicurezza e cyberattacchi avanzati e a prevenirne i danni, CrowdStrike Services mette le aziende nella condizione di difendersi dagli attacchi futuri.

I servizi proattivi e di risposta agli incidenti di CrowdStrike possono essere utilizzati singolarmente o combinati tra loro stipulando un contratto di prestazione di servizi flessibile: se le ore riservate ai servizi di risposta agli incidenti restano inutilizzate, CrowdStrike permette di riconvertirle in ore di servizi proattivi, cioè attività volte a migliorare la strategia di sicurezza complessiva.

UNO SGUARDO AI SERVIZI CROWDSTRIKE

I servizi CrowdStrike aiutano a consolidare e a fare evolvere la strategia di sicurezza delle aziende rispondendo a tre interrogativi fondamentali:

HO SUBITO UNA COMPROMISSIONE?

- Servizi di risposta agli incidenti
- Servizi di ripristino degli endpoint
- Valutazione delle compromissioni
- Monitoraggio della sicurezza di rete

QUANT'È MATURA LA MIA STRATEGIA DI SICUREZZA?

- Valutazione della maturità della cybersicurezza
- Valutazione della sicurezza di Active Directory
- Valutazione della sicurezza del cloud
- Valutazione del SOC
- Valutazione dell'integrità IT
- Programma di consolidamento della cybersicurezza
- Programma di sicurezza avanzato
- Sviluppo di un programma di threat intelligence

SONO PRONTO A DIFENDERMI?

- Simulazione di attacco
- Simulazione immersiva
- Esercizio di emulazione dell'attaccante
- Esercizio Red Team / Blue Team
- Servizi di penetration testing

SERVIZI GESTITI, SUPPORTO E FORMAZIONE

- Falcon Complete™
- Supporto operativo di Falcon
- Formazione su Falcon (CrowdStrike University)

SERVIZI PROATTIVI E DI RISPOSTA AGLI INCIDENTI DI CROWDSTRIKE

HO SUBITO UNA COMPROMISSIONE?

SERVIZI DI RISPOSTA AGLI INCIDENTI

- Una panoramica completa sulle attività svolte dall'attaccante consente di accelerare le operazioni di remediation in caso di compromissione e di tornare operativi più velocemente. I servizi IR di CrowdStrike collaborano con la tua azienda per gestire gli incidenti di sicurezza più critici e conducono analisi forensi per risolvere immediatamente gli attacchi e implementare soluzioni di lungo periodo per evitare attacchi futuri.
- Per il team IR di CrowdStrike, le attività di risposta agli incidenti sono vere operazioni di intelligence in cui conoscenze del mondo reale, analisi forensi ed esperienze di remediation si combinano con l'uso della rivoluzionaria piattaforma cloud Falcon per identificare gli attaccanti in modo rapido e preciso ed estrometterli prontamente dall'ambiente. Il team CrowdStrike ha come obiettivo principale il ripristino dell'operatività dei suoi clienti nel minor tempo possibile riducendo l'impatto degli incidenti di sicurezza.

SERVIZI DI RIPRISTINO DEGLI ENDPOINT

- L'offerta Endpoint Recovery Services di CrowdStrike aiuta a tornare rapidamente operativi dopo attacchi avanzati e minacce persistenti senza interruzioni dell'attività.
- Utilizzando la piattaforma tecnologica leader del settore di CrowdStrike, dati di threat intelligence e le competenze di una squadra di esperti professionisti della sicurezza, questa soluzione aiuta a rilevare, analizzare e risolvere gli incidenti di sicurezza conosciuti consentendo una ripresa rapida.

VALUTAZIONE DELLE COMPROMISSIONI

- Il team Compromise Assessment di CrowdStrike esamina le attività di attacco in corso e passate del tuo ambiente di lavoro per rispondere a questo interrogativo: "La mia azienda ha subito una compromissione?"
- Il team vanta anni di esperienza nelle attività di neutralizzazione delle intrusioni operate dagli attaccanti più avanzati. Combinando la potente piattaforma Falcon, dati di threat intelligence all'avanguardia e operazioni di threat hunting ininterrotte, il team è in grado di compiere la valutazione più completa di qualsiasi compromissione.

MONITORAGGIO DELLA SICUREZZA DI RETE

- Servizio che assicura un monitoraggio esteso della rete alla ricerca delle minacce attive presenti nell'ambiente.
- Le sue funzionalità di monitoraggio estese sono al servizio delle attività di rilevamento, risposta e threat hunting. Il servizio si appoggia sia sulle competenze degli analisti di threat hunting di CrowdStrike sia su un'appliance di rete che cerca le minacce attive nell'ambiente di rete.

PERCHÉ SCEGLIERE CROWDSTRIKE?

Competenze comprovate
Una squadra composta da esperti di pronto intervento, ricercatori di malware e professionisti di cyber intelligence risponde rapidamente agli incidenti, esegue analisi forensi, ripristina gli endpoint e offre servizi proattivi.

Informazioni sugli attaccanti
Hai a disposizione informazioni aggiornate all'ultimo minuto su cybercriminali e le tattiche, tecniche e procedure che utilizzano per colpire il tuo ambiente.

Capacità di threat hunting impareggiabili
Attività proattive e ininterrotte di ricerca delle minacce condotte in tutto il tuo ambiente.

Tecnologia di alto livello
La speciale piattaforma CrowdStrike Falcon individua gli attaccanti, li espelle prontamente e li tiene alla larga, assicurando una protezione degli endpoint di livello superiore.

SERVIZI PROATTIVI E DI RISPOSTA AGLI INCIDENTI DI CROWDSTRIKE

QUANT'È MATURA LA MIA STRATEGIA DI SICUREZZA?

VALUTAZIONE DELLA MATURITÀ DELLA SICUREZZA INFORMATICA

- Il team CrowdStrike Services afferma che conformità non equivale a sicurezza. Forte dei suoi anni di esperienza nelle attività di neutralizzazione delle minacce, il team CS valuta attentamente il livello di maturità della strategia di sicurezza anziché limitarsi a considerare la conformità.
- Ben oltre una semplice verifica, il metodo del team prevede l'analisi del livello di protezione informatica dell'azienda considerando la sua capacità di prevenire, rilevare e rispondere agli attacchi più avanzati.

VALUTAZIONE DELLA SICUREZZA DI ACTIVE DIRECTORY

- Esame completo della configurazione Active Directory (AD) e delle policy che ha lo scopo di prevenire gli exploit dell'infrastruttura AD.
- Questa offerta esclusiva di CrowdStrike studia la configurazione e le policy AD per individuare eventuali errori di configurazione che potrebbero essere sfruttati da criminali informatici.
- La valutazione include lo studio di documentazione, incontri con il personale, utilizzo di tool proprietari e verifica manuale della configurazione e delle impostazioni AD. Il risultato è un report dettagliato degli eventuali problemi emersi, del loro impatto e delle misure consigliate per mitigare e risolvere il problema.

VALUTAZIONE DELLA SICUREZZA DEL CLOUD

- Valutazione che genera informazioni fruibili per eliminare gli errori di configurazione e le deviazioni rispetto all'architettura cloud consigliata.
- Forte dell'esperienza maturata da CrowdStrike nella risposta agli incidenti e delle competenze pratiche acquisite dai suoi consulenti da riconosciuti esperti di architetture di sicurezza cloud, questa valutazione indica le azioni prioritarie da intraprendere per migliorare al massimo le capacità di prevenire, rilevare e risolvere gli incidenti cloud.

VALUTAZIONE DELL'INTEGRITÀ IT

- Ricerca proattiva delle vulnerabilità e applicazione di salvaguardie alla rete per prevenire le compromissione.
- La valutazione dell'integrità IT di CrowdStrike assicura migliore visibilità sulle applicazioni, accessibilità e gestione degli account della rete perché mette a disposizione dati contestuali completi sul traffico di rete e le lacune di sicurezza. L'individuazione delle vulnerabilità e delle patch mancanti permette di preservare la sicurezza della rete prima che si verifichi una compromissione.

PROGRAMMA DI CONSOLIDAMENTO DELLA CYBERSICUREZZA

- L'elaborazione e l'implementazione di un programma di consolidamento della cybersicurezza in seguito a una compromissione consente di eliminare le lacune di sicurezza e prevenire intrusioni future.
- Il programma è diretto alle aziende che di recente hanno subito una compromissione e che desiderano essere guidate nell'elaborazione di un piano strategico per migliorare la cybersicurezza attuale e futura.

ALTRE OFFERTE

Valutazione del SOC (Security Operations Center)
Valutazione diretta a migliorare il livello di maturità del SOC tramite l'individuazione delle aree prioritarie di intervento.

Programma di sicurezza avanzato
Studio approfondito dei processi, degli strumenti e delle risorse di cybersicurezza volto a determinare la maturità del programma di sicurezza aziendale.

Sviluppo di un programma di threat intelligence
Elaborazione di un programma per gestire i dati di threat intelligence che tenga conto dell'evoluzione del panorama delle minacce, dei cybercriminali globali e delle loro nuove tattiche, tecniche e procedure.

SERVIZI PROATTIVI E DI RISPOSTA AGLI INCIDENTI DI CROWDSTRIKE

SONO PRONTO A DIFENDERMI?

SIMULAZIONE DI ATTACCO

- La notevole esperienza accumulata dal team CrowdStrike Services durante i suoi interventi di risposta ad incidenti altamente sofisticati rende molto realistici gli esercizi di simulazione degli attacchi.
- Durante gli esercizi viene simulato un attacco mirato contro la tua azienda e i partecipanti – dirigenti o personale tecnico – possono sperimentare, accompagnati, l'esperienza realistica di un incidente senza soffrirne le conseguenze spiacevoli.

SIMULAZIONE IMMERSIVA

- Esercizio ideato per verificare che i collaboratori dell'azienda siano consapevoli del loro ruolo nell'ambito di uno scenario di intervento in caso di incidente.
- Anziché raccontare al gruppo di un ipotetico attacco, il team di CrowdStrike utilizza gli strumenti e i processi di cui dispone l'azienda per rendere la situazione più realistica comunicando informazioni specifiche a determinate persone, cioè esattamente come avverrebbe nel caso di una violazione reale. Il team lascia che il gruppo di partecipanti alla simulazione decida autonomamente come utilizzare le informazioni. Alla fine dell'esercizio, risulteranno chiari i punti deboli della strategia di intervento.

ESERCIZIO DI EMULAZIONE DELL'ATTACCANTE

- Questo esercizio offre il vantaggio di fare l'esperienza di un attacco mirato di alto livello senza doverne sopportare le ripercussioni.
- Un consulente esperto di CrowdStrike mima le tecniche di attacco di un cybercriminale per tentare di accedere alla rete dell'azienda e comprometterne risorse specifiche. Una volta riuscito nel suo intento, il team di CrowdStrike spiega come ha realizzato il suo obiettivo e indica all'azienda le tattiche a cui può ricorrere per prevenire attacchi futuri.

ESERCIZIO RED TEAM / BLUE TEAM

- Questo esercizio prepara i responsabili della cybersicurezza aziendale attraverso uno scontro con i nostri esperti: il team rosso è in attacco e il team blu in difesa.
- Lo scopo dell'esercizio è di migliorare le competenze di threat hunting e i processi che il team aziendale mette in atto per rispondere agli incidenti in uno scenario di attacco preso dal mondo reale.

SERVIZI DI PENETRATION TESTING

- Il team di CrowdStrike individua le lacune di sicurezza dell'azienda ricorrendo a tecniche di hackeraggio etico come simulazione di attacchi autorizzati e penetration testing su vari componenti di sistemi, reti e applicazioni.
- Esistono diverse opzioni di test per soddisfare obiettivi di sicurezza specifici.

SERVIZI GESTITI, SUPPORTO E FORMAZIONE

- **FALCON COMPLETE™:** soluzione completa basata sulla piattaforma Falcon per la protezione degli endpoint e il threat hunting fornita sotto forma di servizio totalmente gestito e pronto all'uso.
- **SUPPORTO OPERATIVO DI FALCON:** supporto operativo che assiste nella configurazione e gestione della piattaforma Falcon per ottimizzarne l'efficacia.
- **FORMAZIONE SU FALCON:** addestramento e servizi di formazione di livello professionale erogati dalla CrowdStrike University (CSU) per migliorare le conoscenze dei team in materia di cybersicurezza e insegnare a sfruttare al meglio l'investimento nella piattaforma Falcon.

INFORMAZIONI SUL TEAM CROWDSTRIKE SERVICES

Il team CrowdStrike Services mette a disposizione delle aziende le misure di protezione e le conoscenze necessarie per difendersi e reagire agli incidenti di sicurezza. Grazie alla piattaforma cloud CrowdStrike Falcon® – che include protezione degli endpoint di livello superiore, raccolta di dati di threat intelligence, opzioni di reportistica e un team di threat hunting attivo 24/7 – il team CrowdStrike Services aiuta i clienti a individuare, sorvegliare e bloccare gli attaccanti in tempo reale. Questo approccio unico consente a CrowdStrike di bloccare più rapidamente gli accessi non autorizzati e di prevenire attacchi futuri. CrowdStrike mette a disposizione anche servizi proattivi con cui le aziende possono migliorare la loro capacità di prevedere le minacce, predisporre le reti e soprattutto di bloccare le compromissioni.

Per maggiori informazioni, visita **www.crowdstrike.com/services/**

E-mail: **services@crowdstrike.com**