Servizi gestiti: EDR (Endpoint Detection and Response)

Riesce dove le soluzioni tradizionali non funzionano. Scopri tutta la potenza di un servizio con le funzionalità integrate per una resilienza aziendale senza confronti.

Le sfide

Oltre il 60% delle violazioni avviene tramite una forma di accesso non autorizzato e le aziende devono adottare controlli di sicurezza avanzati per difendersi da minacce sempre più sofisticate.

Spinti dal profitto economico, i criminali informatici puntano ai dati sensibili. I settori altamente regolamentati, tra cui quelli sanitario, finanziario e governativo, diventano così un obiettivo strategico dei loro attacchi.

Tuttavia, a causa della complessità e del costo delle tecnologie EDR, che hanno un time-to-value di lungo periodo anche per i team SOC più grandi, la maggior parte dei servizi di sicurezza avanzati per gli endpoint, che possono aiutare le piccole e medie imprese a contrastare queste minacce, presenta ancora sfide significative, ad esempio:

- Costi elevati, superiori al budget destinato all'IT
- Ore, se non giorni, per le attività di analisi e di incident response
- Le soluzioni tradizionali non sono in grado di bloccare le minacce avanzate
- Correzione dei problemi limitata, che non garantisce la continuità operativa e la protezione dei dati
- Rischio di ritardi nella creazione dei report di conformità o mancanza di supporto per il disaster recovery

Vantaggi principali

Accesso a competenze nell'IT e nella sicurezza

- Riduzione delle assunzioni e delle esigenze di formazione
- Operazioni più semplici e in linea con i trend più recenti

Convenienza

- Costi più prevedibili basati su SLA
- Passaggio da spese di capitale (CapEx) a costi di esercizio (OpEx)

Assistenza e supporto su base continua

- Dati e sistemi aziendali sono monitorati 24 ore su 24

Scalabilità rapida

- Incremento o riduzione delle risorse ai ritmi e ai costi desiderati

La soluzione: i servizi gestiti EDR (Endpoint Detection and Response)

Sia che la tua azienda collabori con un provider su progetti per la sicurezza altamente specializzati oppure esternalizzi l'intero comparto IT, siamo in grado di offrirti servizi EDR (Endpoint Detection and Response) estremamente efficaci e convenienti.

Ci impegniamo a mantenere la tua azienda operativa, produttiva, sicura e protetta, nel rispetto del budget che hai destinato all'IT.

Perché

Analisi e prioritizzazione degli incidenti ottimizzate	Sicurezza, backup e ripristino integrati	Soluzione di Cyber Protection completa
• Velocizza le indagini sugli attacchi dando priorità ai potenziali rischi e riducendo l'eccesso di avvisi • Analizza gli eventi in pochi minuti e su vasta scala grazie alla correlazione automatizzata e alle interpretazioni guidate e basate su AI degli attacchi • Ottieni più visibilità in tutte le fasi MITRE ATT&CK® con un'analisi rapida dell'attacco e del suo impatto e informazioni su come la minaccia si è infiltrata, sui danni che ha causato e su come può essersi diffusa • Creazione rapida di report sugli incidenti di sicurezza	• Le funzionalità di backup e ripristino integrate offrono una resilienza reale (a differenza delle soluzioni di sicurezza mirate), basata su rollback specifico in base all'attacco, ripristino a livello di file o di immagine e disaster recovery • Risoluzione e ripristino rapidi e con un solo clic per eseguire indagini, correggere i problemi, recuperare i dati e chiudere le falle che rendono i tuoi sistemi vulnerabili • Protezione completa e integrata secondo i principi del framework NIST	• Avvia rapidamente i nuovi servizi di Cyber Protection con un solo agente e un'unica console, velocizzando il deployment e l'onboarding • Estendi con facilità i servizi a più clienti e nel contempo mantieni ottimi margini e riduci i costi operativi, dal momento che non dovrai più fare affidamento su un ampio team di personale altamente qualificato

Funzionalità principali

Rilevamento delle minacce avanzate e degli attacchi in corso

Il servizio monitora e correla gli eventi sospetti tra gli endpoint per rilevare e neutralizzare minacce complesse e difficili da identificare, in grado di superare altri livelli di protezione degli endpoint, come il ransomware, gli attacchi zero-day, le minacce persistenti avanzate (APT) o gli attacchi fileless.

Maggiore conformità alle normative

Protezione dalle minacce dei dati sensibili soggetti a normative quali GDPR, HIPAA e PCI-DSS; la visibilità dei dati sensibili interessati da problemi aiuta a creare i report di conformità.

Una risposta olistica alle minacce, che garantisce la continuità operativa dell'azienda

Assicuriamo la continuità operativa della tua azienda con il ripristino rapido dei dati e il rollback delle modifiche apportate ai sistemi dopo un attacco. A differenza di altri servizi di sicurezza avanzati per gli endpoint basati esclusivamente su soluzioni di Cyber Security, il nostro servizio gestito di sicurezza degli endpoint offre funzionalità integrate per tutte le fasi del framework di Cyber Security NIST, garantendo una continuità operativa reale alla tua azienda.

Protezione degli endpoint premiata

Editors' choice

Partecipante e vincitore del test di AV-TEST

Certificazione Endpoint Anti-Malware di ICSA Labs

Certificazione AV-Comparatives

Certificazione VB100

Identificazione

Devi conoscere a fondo i dati di cui disponi per poterli esaminare e proteggere. Il nostro servizio prevede strumenti per l'inventario e la classificazione dei dati per comprendere meglio le superfici di attacco.

Protezione

Garantisci la protezione proattiva degli endpoint grazie ai feed informativi sulle minacce, la correzione delle falle aperte, il blocco delle minacce note e la gestione delle policy per consolidare ulteriormente le misure di difesa.

Rilevamento

Adotta il monitoraggio continuo contro le minacce con motori basati sull'analisi comportamentale e sulle firme, filtraggio degli URL e correlazione degli eventi.

Risposta

Effettua indagini rapide sugli incidenti di sicurezza utilizzando la connessione remota e i dati forensi. Risolvi i problemi velocemente isolando gli endpoint, arrestando i processi, applicando la quarantena e avviando rollback specifici in base all'attacco.

Ripristino

Utilizza le nostre soluzioni per il backup e il ripristino, completamente integrate e leader di mercato, per garantire una continuità operativa senza precedenti dei sistemi, dei dati e dell'attività aziendale.

info@acts.com
+390444800235
www.acts.com+390444800235