MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

Managed Cyber Security per la sua azienda

Con Managed Extended Detection and Response (MxDR) le offriamo un supporto professionale per proteggere la sua infrastruttura IT dalle minacce informatiche più sofisticate. Utilizzando strumenti di analisi automatizzati, basati sull'IA e in continua evoluzione, i nostri esperti di sicurezza monitorano costantemente i suoi sistemi e le sue reti IT per identificare i potenziali rischi e proporre contromisure nel modo più rapido possibile.

La risposta alle minacce informatiche di oggi
I sistemi tradizionali di protezione delle infrastrutture IT non sono più sufficienti a contrastare le nuove minacce informatiche sempre più sofisticate e, nella maggior parte dei casi, le organizzazioni non dispongono delle risorse necessarie per eseguire in autonomia analisi di sicurezza complete e individuare le minacce tempestivamente. Con MxDR, questo compito lo svolgiamo noi: mediante l'analisi continua di tutti i log della sua infrastruttura IT, il team di esperti rileverà eventuali minacce nei sistemi e, laddove necessario, proporrà prontamente le contromisure adeguate.

Security Monitoring professionale
Grazie a MxDR, i log dei sistemi IT vengono acquisiti, compressi e trasmessi al sistema MxDR in forma codificata per l'analisi su base continua. I nostri esperti di sicurezza verificano i risultati delle attività critiche, classificano gli eventi e li confrontano con i sistemi globali di analisi e notifica. Infine, nel portale MxDR, gli esperti MxDR mettono regolarmente a disposizione del cliente analisi dettagliate, informazioni riguardo a nuove minacce, punti deboli dell'infrastruttura IT e raccomandazioni in merito alle misure da adottare. In questo modo, MxDR garantisce una risposta efficiente ed efficace agli attuali incidenti di sicurezza.

Servizio completo
MxDR si occuperà di sorvegliare le aree interessate da attacchi informatici quali PC, componenti di rete e servizi cloud (SaaS), affinché lei possa dedicarsi completamente alle sue attività commerciali. Grazie al monitoraggio continuo dei sistemi con le tecnologie più all'avanguardia, le anomalie vengono identificate rapidamente e le minacce vengono affrontate in modo tempestivo.

Ulteriori servizi di sicurezza
Offriamo anche servizi come scansione delle vulnerabilità, test di penetrazione, training per la sensibilizzazione al phishing e servizi di Incident Response che permettono di identificare i potenziali rischi, aumentare la consapevolezza sulla sicurezza nella sua organizzazione e rispondere adeguatamente agli eventuali attacchi informatici.

Accenture: il nostro partner per la sua sicurezza
Per il monitoraggio della sua infrastruttura IT, ci affidiamo al servizio MxDR leader sul mercato e al know how in materia di sicurezza di Accenture. Grazie alla clientela internazionale, gli esperti di Accenture vantano una conoscenza approfondita dello stato attuale delle minacce informatiche globali e sono sempre informati per tempo sulle nuove minacce, cosicché lei possa proteggere la sua infrastruttura IT anche dalle più attuali minacce.

Sunrise
BUSINESS

Caratteristiche standard

Service Features	**Analisi dei dati:** identificazione di eventi rilevanti e relativa correlazione in base alla fonte IP **Alert Monitoring 24/7:** identificazione ed escalation degli incidenti tramite analisi delle minacce specifiche del settore e del cliente **Analisti e team altamente qualificati:** analisti di sicurezza certificati GIAC (Global Information Assurance Certification) **Servizio personalizzabile:** notifica degli incidenti di sicurezza su misura per le esigenze della clientela, rilevamento della gravità degli incidenti **Riconoscimento delle anomalie:** diagnosi di traffico dati insolito, Data Mining e creazione di analisi statistiche **Portale clienti semplice e intuitivo (portale MxDR):** con una dashboard unificata e funzionalità avanzate di reporting **Mid-Market Threat Intelligence:** panoramica delle minacce che hanno un impatto su settori simili e in determinate regioni
Prestazioni	Monitoraggio Edge-to-Endpoint Il team MxDR Delivery è a sua disposizione 24/7 per rispondere a qualsiasi domanda e offrirle consulenza in caso di guasti Onboarding dei dispositivi: Baselining della piattaforma Log Collection, accesso sicuro e configurazione della raccolta Analisi in tempo reale dei protocolli di sicurezza e relativa correlazione degli eventi Convalida e notifica in tempo reale in caso di incidenti di sicurezza Monitoraggio dei protocolli dei dispositivi e notifica in caso di anomalie del protocollo Accesso sicuro del portale web al portale MxDR Reporting mensile con panoramica della situazione delle minacce L'acquisizione dei log sulla piattaforma MxDR di Accenture è altamente flessibile e si adatta sia all'ambiente IT che alle esigenze specifiche dell'organizzazione
Servizi e assistenza	Monitoraggio della sicurezza, analisi e report in tempo reale 24/7 Tempi di risposta di dieci minuti in caso di emergenza o grave incidente

Ulteriori servizi di sicurezza

Phishing Awareness Service	Campagne personalizzate sul phishing Sensibilizzi i suoi dipendenti sui rischi degli attacchi di phishing e verifichi la vulnerabilità della sua organizzazione rispetto ad attacchi di questo tipo. • Attacchi di phishing simulati tramite e-mail • Tipi di e-mail e linguaggi personalizzati in base alle sue esigenze specifiche • Test realistici per sensibilizzare i dipendenti • Rapporto dettagliato e anonimo dei risultati
Scansioni delle vulnerabilità	Scansione delle vulnerabilità dell'ambiente IT interno ed esterno Per verificare la vulnerabilità di tutti i dispositivi (server, workstation, stampanti, scanner, telefoni, router, switch, hypervisor e dispositivi wireless) e sistemi (versioni delle patch, sistemi operativi) collegati alla rete, viene impiegata la soluzione software professionale Tenable Nessus®. Il rapporto di valutazione delle vulnerabilità fornisce una panoramica prioritaria di tutte le vulnerabilità identificate, oltre a raccomandazioni concrete per intervenire. Quindi, nel corso di un incontro con il team tecnico di esperti, vengono presentati i risultati dettagliati.
Test di penetrazione	Protegga la sua organizzazione identificando tempestivamente le potenziali vulnerabilità nella sua infrastruttura IT, prima che i criminali informatici possano attaccare. Gli attacchi informatici simulati ai suoi sistemi IT da parte di Penetration Tester esperti forniscono informazioni preziose sui possibili pericoli. • Condizioni quadro chiare e definite in anticipo • Generalmente, vengono testati tutti i dispositivi collegati alla rete (ad eccezione delle applicazioni) • Discussione conclusiva dettagliata e di persona con il Penetration Tester • Il rapporto completo sui risultati include le misure consigliate per ottimizzare la sicurezza
Incident Response Service	In caso di attacco informatico o di guasto del sistema, è fondamentale agire tempestivamente. I nostri team di esperti di Incident Response conducono indagini immediate e accurate su dispositivi elettronici, reti e sistemi per determinare la causa, l'origine e la portata dell'incidente. Ciò avviene non solo virtualmente ma, laddove necessario, anche in loco, 24 ore su 24, 365 giorni all'anno. Quindi, lavoriamo insieme al suo team per contenere l'attacco e ripristinare le operazioni il più rapidamente possibile.

Ci contatti telefonicamente per ricevere maggiori informazioni.

Sunrise Sagl
Thurgauerstrasse 101B
8152 Glattpark (Opfikon)

Infoline 0800 555 552

sunrise.ch/business

10.2024