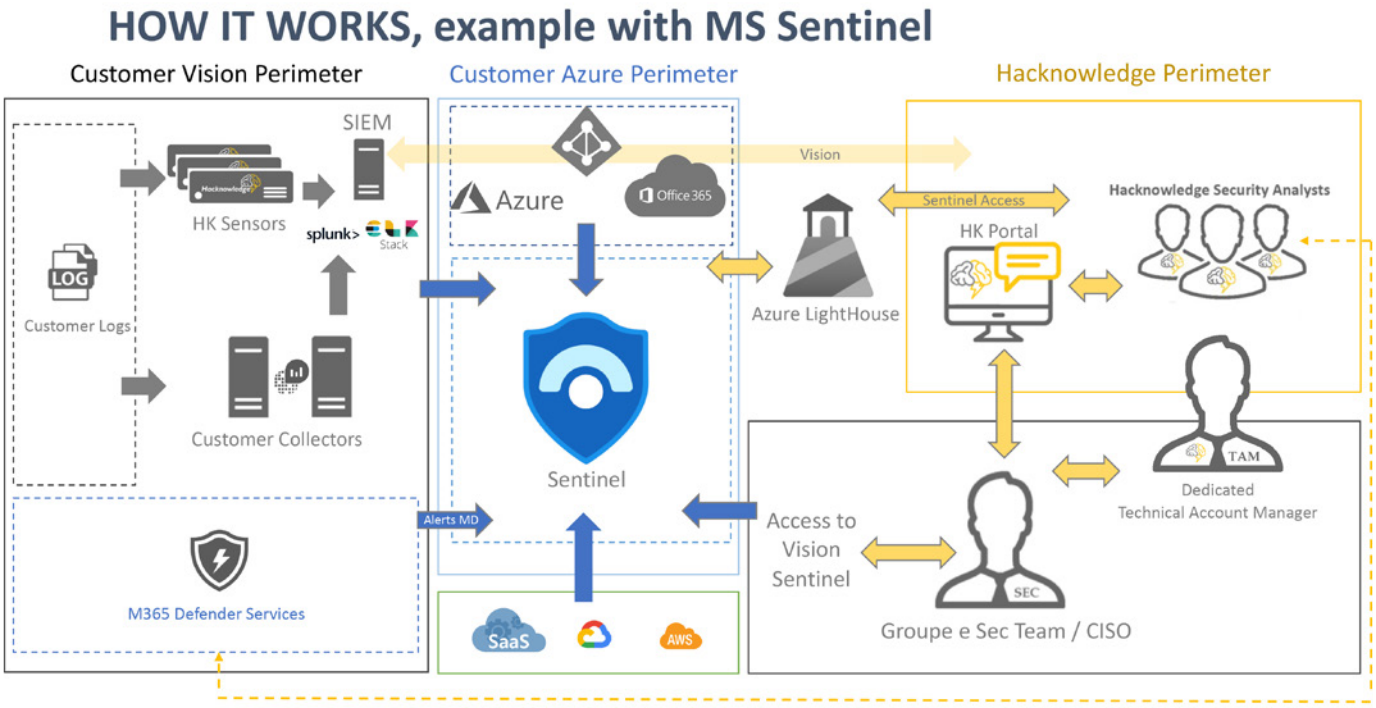
Monitoraggio della cibersicurezza
Ridurre il tempo che intercorre tra una violazione di sicurezza e il suo rilevamento

La cibercriminalità non è fantascienza, ma un vero pericolo per le aziende. Le aziende colpite devono far fronte a richieste di riscatto, periodi di interruzione e riparazioni costose. Ci vogliono in media circa 100 giorni perché un'organizzazione scopra una violazione o ne venga informata. Ciò rende ancora più importante il monitoraggio continuo di tutti i sistemi. Il servizio gestito da Hacknowledge, specialista in cibersicurezza, mira a ridurre questo tempo al minimo e ad aiutare i clienti ad agire per prevenire qualsiasi attività di hacking nella propria rete.

Security Operations Center (SOC)

Hacknowledge fornisce un SOC gestito e una soluzione SIEM (Security Incident and Event Management) gestita per recuperare i log se non sono disponibili. È un prodotto tutto incluso, che tuttavia si adatta alle esigenze del cliente. Il servizio è svizzero, semplice ed efficiente. Per «svizzero» si intende che tutti i dati rimangono sempre in Svizzera. «Semplice» significa sfruttare l'ambiente di sicurezza IT esistente ed «efficiente» enfatizza la capacità del servizio di adattarsi al contesto del cliente.



I vostri vantaggi

– Monitoraggio 24/7 della vostra infrastruttura: gli esperti ingegneri di sicurezza rilevano le minacce e vi reagiscono grazie alle soluzioni all'avanguardia di VISION Cyber Management™.

– Segnalazione di incidenti di sicurezza qualificati e assistenza al vostro team della sicurezza affinché si concentri sugli eventi importanti: ci occupiamo di gestire i log per voi, così da fornirvi più tempo per lavorare sugli incidenti qualificati.

– Soluzione basata in Svizzera: tutti i dati sono conservati in Svizzera, tutti gli ingegneri lavorano in Svizzera e non riscontrerete nessun problema dovuto alle frontiere per quanto riguarda dati riservati o personali.

– Hacknowledge è certificato dalla norma ISO 27001 (senza alcuna eccezione) ed è conforme alle norme GDPR.

– Azienda indipendente: avete la garanzia di ricevere supporto da un fornitore di servizi indipendente.

– La soluzione è trasparente e avete accesso completo ai vostri dati (ad es. log ed eventi di sicurezza) in qualsiasi momento.

– I servizi secondari coprono l'intero campo della cibersicurezza, dai test d'intrusione (penetration testing), alla scienza forense (forensics) e alla sensibilizzazione del personale.

Monitorare. Rilevare. Reagire.

1) Il primo passo è definire il perimetro da coprire, sia in termini di ambiente IT sia dei casi d'uso. È meglio partire in piccolo e crescere.

2) Hacknowledge può schierare un SIEM per consolidare e correlare i log di sicurezza. Se esiste già un SIEM, Hacknowledge può connettersi adesso per fornire il servizio SOC.

3) Hacknowledge aiuta il cliente a recuperare i log e segnalarli al SIEM. I sensori possono aiutare ad arricchire e analizzare i log più vicini alla fonte, evitando il rumore nella rete e ottimizzando la quantità di dati inviati al GIES.

4) Hacknowledge implementa i casi d'uso uno per uno per garantire un monitoraggio funzionale ed efficace. Testeremo insieme i casi e filtreremo i falsi positivi.

5) In aggiunta alla segnalazione quanto più rapida degli incidenti di sicurezza, Hacknowledge fornisce regolarmente dei report di sicurezza per garantire il continuo miglioramento della collaborazione.

Adattabile e flessibile

Il SOC supporta nativamente tre SIEM: SPLUNK, Microsoft Sentinel e Vision (Kibana e la stack ELK). Hacknowledge è molto adattabile e flessibile, perché permette di implementare il monitoraggio di sicurezza nel vostro ambiente IT e OT in modo semplice ed efficiente.

Posta CH Comunicazione SA
E-Government
Wankdorfallee 4
3030 Berna
Svizzera

E-mail egovernment@posta.ch
posta.ch/e-government