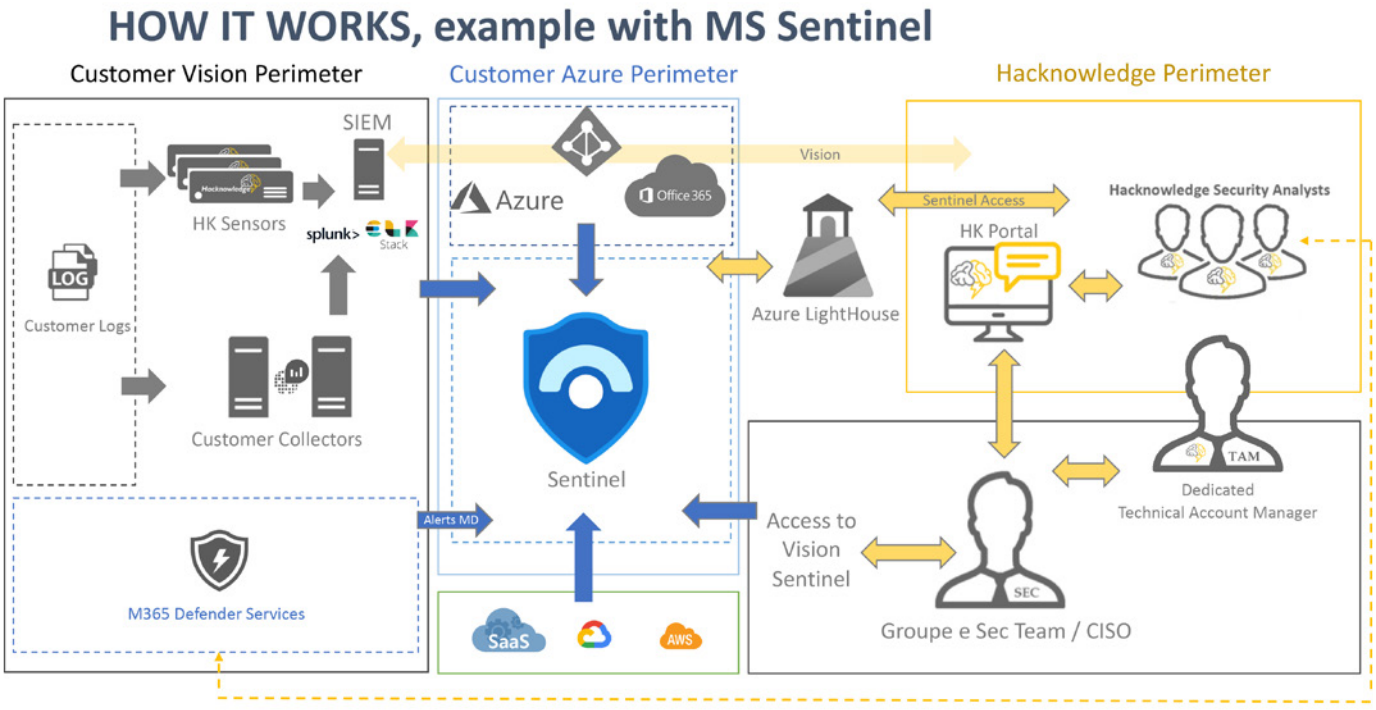
Cybersecurity-Monitoring
Sicherheitsverletzungen schneller entdecken

Cyberkriminalität ist keine Science-Fiction, sondern eine echte Bedrohung für Unternehmen. Betroffene Unternehmen sehen sich bald einmal mit Lösegeldforderungen, Produktionsausfällen und teuren Behebungsarbeiten konfrontiert. Es dauert im Schnitt etwa 100 Tage, bis ein Unternehmen eine Sicherheitsverletzung entdeckt oder darüber informiert wird. Deshalb ist fortlaufendes Monitoring umso wichtiger. Der Managed Service der Cybersicherheits-Spezialistin Hacknowledge zielt darauf ab, die Zeit bis zur Entdeckung einer Sicherheitsverletzung auf ein Minimum zu verringern und den Kunden dabei zu helfen, Massnahmen zu ergreifen und Hackerangriffe auf ihr Netzwerk zu verhindern.

Security Operations Center (SOC)

Hacknowledge bietet bei Bedarf ein Managed SOC und ein Managed SIEM (Security Incident and Event Management) zur Sammlung von Logs. Es ist ein All-in-One-Produkt, das sich sehr gut an die Umgebung des Kunden anpassen lässt. Der Service ist Schweiz-basiert, einfach und effizient. «Schweiz-basiert» bedeutet, dass die Daten jederzeit in der Schweiz bleiben. «Einfach» bedeutet, dass unsere Lösung die bestehende IT-Sicherheitsumgebung optimal ausnutzt, und «effizient» unterstreicht die Fähigkeit des Service, sich an die Bedürfnisse des Kunden anzupassen.



Ihre Vorteile

– Monitoring Ihrer Infrastruktur rund um die Uhr: Die Sicherheitsexpertinnen und -experten erkennen Bedrohungen und reagieren darauf mit Hilfe der hochmodernen «VISION Cyber Management™»-Lösungen.

– Meldung relevanter Sicherheitsvorfälle und Entlastung Ihres Sicherheitsteam, damit sich dieses auf die wichtigsten Dinge konzentrieren kann: Wir übernehmen die Logbearbeitung für Sie und schaffen so mehr Zeit für die Bearbeitung relevanter Sicherheitsvorfälle.

– Schweiz-basierte Lösung: Alle Daten werden in der Schweiz gespeichert, alle Techniker arbeiten in der Schweiz, vertrauliche und persönliche Daten gelangen nicht ins Ausland.

– Hacknowledge ist nach ISO 27001 zertifiziert (ohne Ausnahme) und komplett DSGVO-konform.

– Herstellerunabhängiges Unternehmen: Sie werden mit 100-prozentiger Sicherheit von einem unabhängigen Dienstleister unterstützt.

– Die Lösung ist transparent und Sie haben und behalten immer die volle Kontrolle über Ihre Daten (u. a. über Sicherheitslogs und -vorfälle).

– Die Nebenservices decken das gesamte Spektrum der Cybersicherheit ab, von Pentests über Forensik bis hin zur Mitarbeitendenschulung.

Überwachen. Erkennen. Reagieren.

1) Der erste Schritt besteht darin, den Umfang zu definieren, der abgedeckt werden soll – sowohl in Bezug auf die IT-Umgebung als auch auf die Use Cases. Es ist besser, klein anzufangen und dann kontinuierlich mehr abzudecken.

2) Hacknowledge kann ein SIEM einrichten, um die Sicherheitslogs zu konsolidieren undkorrelieren. Wenn bereits ein SIEM vorhanden ist, kann Hacknowledge sich mit diesem verbinden, um den SOC-Service bereitzustellen.

3) Hacknowledge unterstützt den Kunden bei der Sammlung der Logs und deren Übermittlung an das SIEM. Sensoren helfen dabei, die Logdaten näher an der Quelle anzureichern zu parsen. Auf diese Weise werden irrelevante Logs aus dem Netzwerk herausgefiltert und die Daten, die dem SIEM übermittelt werden, optimiert.

4) Hacknowledge setzt jeden Use Case einzeln um, um ein funktionierendes und effizientes Monitoring zu gewährleisten. Die verschiedenen Szenarien werden zusammen getestet und falsche Alarme herausgefiltert.

5) Hacknowledge meldet nicht nur Sicherheitsvorfälle so früh wie nötig, sondern liefert auch regelmässig Sicherheitsberichte, um die Zusammenarbeit kontinuierlich zu verbessern.

Anpassungsfähig und flexibel

Drei SIEMs werden vom SOC nativ unterstützt: Splunk, Microsoft Sentinel und Vision (Kibana und ELK Stack). Hacknowledge ist sehr anpassungsfähig und flexibel, sodass das Monitoring der Cybersicherheit in Ihrer IT- und OT-Umgebung reibungslos und effizient umgesetzt werden kann.

Post CH Kommunikation AG
Digital Business
Wankdorfallee 4
3030 Bern
Schweiz

E-mail digital-business@post.ch
post.ch/hacknowledge-business