SECUREIQ | MANAGED SECURITY

Angriffe erkennen, bevor Schaden entsteht.

SOC & SIEM als Managed Service für KMU, Kommunen und öffentliche Auftraggeber.

Analysten-Triage · Definierte Eskalationswege · Auditfähiges Reporting

DIE OPERATIVE LÜCKE

Logs allein erkennen keinen Angriff.

Viele Organisationen sammeln Protokolldaten, doch niemand bewertet sie kontinuierlich. Für ein eigenes 24/7-Team fehlen Personal, Erfahrung oder Budget. Gleichzeitig sieht NIS2 bei erheblichen Sicherheitsvorfällen eine Frühwarnung innerhalb von 24 Stunden nach Kenntnis vor. Entscheidend ist deshalb ein klarer Weg vom Signal zur bewerteten und dokumentierten Reaktion.

8x5 oder 24x7	Hosting in Deutschland	Mandantengetrennt
Passend zu Risiko und Betriebsmodell	Datenhoheit nachvollziehbar geregelt	Technische und organisatorische Trennung

LEISTUNGSBAUSTEINE

Vom Ereignis zur Entscheidung.

Technik, Analysten und Reaktionsprozesse greifen als ein Service ineinander. Sie erhalten priorisierte Informationen und behalten klare Zuständigkeiten.

01

Log-Erfassung und Normalisierung

Endpoint, Firewall, Cloud, Active Directory und weitere relevante Quellen werden zentral angebunden und in ein einheitliches Format überführt.

02

Korrelation und Alarmierung

Ein gepflegtes Regelwerk verbindet einzelne Signale zu bewertbaren Angriffsmustern und priorisiert sie nach Risiko.

03

Triage durch Analysten

Analysten prüfen Kontext, Plausibilität und Dringlichkeit, bevor ein Alarm eskaliert wird.

04

Incident Response

Definierte Eskalationswege, Ansprechpartner und vorbereitete Maßnahmen schaffen Handlungsfähigkeit.

05

Nachweisbares Reporting

Berichte für Geschäftsführung, Audit und Aufsicht zeigen Ereignisse, Reaktionszeiten und Trends.

TECHNOLOGIE UND DATENHOHEIT

Elastic-basierte Plattform mit Hosting in Deutschland. Mandanten werden technisch und organisatorisch getrennt; eine Weitergabe der Sicherheitsdaten an Dritte ist nicht Bestandteil des Betriebsmodells. Datenquellen, Aufbewahrungsdauer, Zugriffe und Löschung werden vor dem Onboarding dokumentiert.

SERVICEMODELL UND SLA

Transparente Planungsbasis.

Leistungsmerkmal	8x5 Managed Detection	24x7 Managed Detection
Servicezeit	Mo-Fr, 08:00-18:00 Uhr	24 Stunden, 365 Tage
Reaktionsziel P1	bis 60 Minuten innerhalb der Servicezeit	bis 15 Minuten rund um die Uhr
Reaktionsziel P2	bis 4 Stunden innerhalb der Servicezeit	bis 60 Minuten rund um die Uhr
Onboarding	typisch 4-6 Wochen	typisch 6-8 Wochen
Ansprechpartner	Service Manager und benannte Analysten	Service Manager, Schichtteam und Rufbereitschaft
Betriebsreview	monatlich	monatlich, bei Bedarf häufiger

Die Zielwerte sind eine Planungsbasis. Finale Einstufung, Zeiten und Eskalationswege werden passend zu Risiko und Scope vertraglich vereinbart.

ONBOARDING

Vier Schritte bis zum Go-Live.

1	Assessment 3-5 Arbeitstage Schutzbedarf, Werkzeuge, Quellen, Use Cases und Eskalationswege klären.
2	Quellen anbinden 1-3 Wochen Konnektoren einrichten, Datenqualität und Aufbewahrung prüfen.
3	Tuning 2-3 Wochen Regeln abstimmen, Alarmrauschen reduzieren und Playbooks testen.
4	Go-Live ab Woche 4-7 Service übernehmen, SLA messen und Ergebnisse im Review besprechen.

COMPLIANCE-MAPPING

Kontrollen werden im Betrieb nachweisbar.

Rahmenwerk	Anforderung	Beitrag des Services	Nachweis
NIS2 Art. 21/23	Incident Handling, Erkennung, Meldung	Triage, Zeitstempel, Eskalation	Tickets, Zeitlinie, Protokoll
ISO 27001 A.8.15	Logging	Erfassung, Normalisierung, Schutz, Retention	Quelleninventar, Retention-Konzept
ISO 27001 A.8.16	Monitoring activities	Use Cases, Korrelation, Analystenbewertung	Regelkatalog, Alarmhistorie
BSI IT-Grundschutz	OPS.1.1.5, DER.1, DER.2.1	Protokollierung, Detektion, Incident-Behandlung	Betriebskonzept, Playbooks, Berichte

Der Service unterstützt technische und organisatorische Anforderungen. Er ersetzt nicht die Gesamtverantwortung der Organisation oder eine individuelle rechtliche Bewertung.

KOSTENMODELL

Ein belastbarer Preis braucht Kontext.

Die Kalkulation berücksichtigt Zahl und Art der Quellen, tägliches Log-Volumen, Aufbewahrungsdauer, Servicezeit und Reaktionsziele. Nach einem kompakten Assessment erhalten Sie einen klar beschriebenen Scope und einen nachvollziehbaren Preis.

Nächster Schritt	30 Minuten Orientierungsgespräch: aktuelle Log-Quellen, Servicebedarf und realistischen Einstieg klären.

KONTAKT

Stefan Schiechl

SecureIQ · München · +49 (0)151/57676030 · kontakt@secureiq.de · www.secure-iq.de