Managed SOC: Network Security Service

IS4IT KRITIS

KONTROLLIERTE UND SICHERE NETZWERKE

Ausgangssituation

- Unkontrollierter Netzwerkverkehr erhöht die Risiken
- Hoher Bedarf an kompetenten Mitarbeitern zur Überwachung
- Keine Ressourcen zur permanenten Überwachung verfügbar
- Tool-Unterstützung oft unzureichend
- Hochleistungsfähige Tools für kleinere Organisationen zu teuer
- Mangelnde Integration in einer unternehmensweiten Sicherheitslösung

Lösungsansatz Network Security Service

- Einsatz der Advanced-Security-Analysis-Plattform von finally safe
- Analyse des Traffics in festgelegten Bereichen
- Umsetzung von Maßnahmen nach Kritikalität
- Einbindung in SIEM-Service-Plattform

Leistungsumfang Network Security Service

- Inbetriebnahme des Sensors vor Ort beim Kunden mittels VPN-Verbindung
- Monatliche Reports über die Sicherheitslage sowie Sicherheitsvorfälle
- Reaktionszeit auf Incidents je nach vereinbartem Service-Level und vereinbarter Servicezeit
- Servicezeit je nach Paket von 08:00 bis 17:00 Uhr, 06:00 bis 22:00 Uhr oder rund um die Uhr
- Rufbereitschaft außerhalb der Servicezeit
- Reaktionszeiten je nach Kritikalität zwischen 30 Minuten und 24 Stunden
- Hardware-Austausch vor Ort je nach Kritikalität zwischen vier Stunden und fünf Arbeitstagen

Technische Sicherheitsmerkmale

- Automatisiertes Aufdecken veralteter OS und Browser
- Automatisiertes Aufdecken fehlender oder schwacher Verschlüsselungen
- Intelligentes Lernen des Netzwerkverhaltens
- Automatisiertes Aufdecken von Anomalien
- Aufdeckung von Systemfreigabe- und Policy-Verstößen
- Meldung bei Aufdecken von versteckten Kommunikationskanälen
- Forensik zu Betriebs- und Sicherheitsvorfällen
- Automatisiertes Aufdecken von Advanced Persistent Threats
- Botnetzerkennung und Aufdeckung versteckter Steuerkanäle
- Erkennung von Manipulationen von Netzwerkverbindungen

Nutzen für den Kunden

- Automation der Überwachung reduziert Kosten
- Konstante und professionelle Überwachung des Netzwerks minimiert das Risiko erfolgreicher Angriffe
- Ausgereifte und modernste Technologie mit optimiertem Preis-Leistungs-Verhältnis

finally safe

IS4IT KRITIS GmbH Kraichgaublick 13 74847 Obrigheim telefon +49 6262 9262594 fax +49 6262 9262595 info@is4it-kritis.de www.is4it-kritis.de

Security Operations Center (SOC): Im Überblick

MANAGED SERVICES ENTLASTEN IHR TEAM

Ausgangssituation

- Bedrohungslage nimmt ständig zu und wird immer aggressiver
- Neue Regularien und Gesetze (EU-DSGVO, KRITIS etc.)
- Strafen drohen – Bußgelder bis zu 4 % des Umsatzes bzw. bis zu 20 Mio. Euro
- Kronjuwelen des Unternehmens bewerten und schützen
- Security-Analysten und Forensik-Experten sind teuer
- Bedarf an Schulungen, Zertifizierungen & Weiterbildung

Lösungsansatz Managed SOC

- Security-Analysten betreuen mehrere Unternehmen parallel
- Optimale Infrastrukturnutzung ➔ Mandantenfähigkeit und virtuelle Server (optional Hardware-Appliances)
- Vorkonfiguriertes SIEM für typische Anforderungen zur schnellen Einführung
- Abgestimmte und definierte Kommunikationswege und Notfallpläne

Leistungsumfang Managed SOC

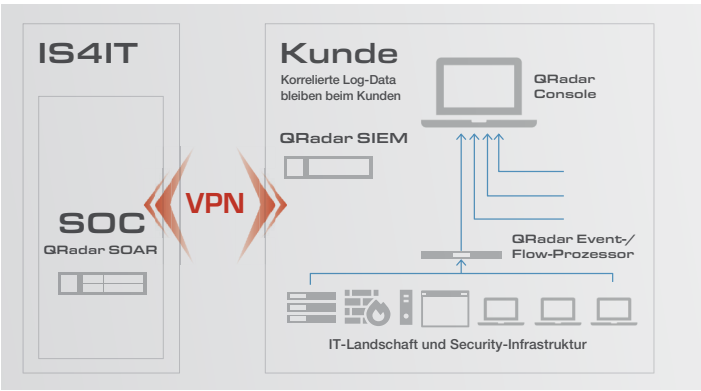
- SIEM Service
- SOAR Service
- Firewall Service
- Web Security Service
- E-Mail-Service
- Vulnerability Management & CSIRT Service
- Endpoint Service
- Network Security Service

Warum Informationssicherheit mit IS4IT?

- Schneller Return on Investment
- Unsere vorkonfigurierte Shared Infrastructure sorgt für schnelle Umsetzung
- Sichere Datenhaltung auf mandantenfähigem Server in nach ISO 27001 zertifiziertem Rechenzentrum, nur über deutsche DE-CIX-Leitungen angeschlossen (keine Weitergabe an Drittländer, z. B. USA)
- Keine eigenen Security-Operations-Center-Experten für den 24 x 7-Betrieb notwendig
- Klare Aufgabentrennung zwischen Betrieb und Sicherheit

Nutzen für den Kunden

- Monatlicher Festpreis, halbjährige Kündigungsfrist, inkl. Lizenzmanagement und Hardware
- Mindestlaufzeit von 12 Monaten bei 24 x 7-Betrieb
- Schnelle Realisierung vom Proof of Concept zum Produktivbetrieb
- Rechtlich abgesicherte Sicherheitskonzepte und revisionssichere Datenhaltung
- Kosteneinsparung bei Audits und Compliance-Prüfungen



IS4IT KRITIS GmbH Kraichgaublick 13 74847 Obrigheim telefon +49 6262 9262594 fax +49 6262 9262595 info@is4it-kritis.de www.is4it-kritis.de