Managed SOC: Endpoint Service

IS4IT KRITIS

ÜBERWACHTE UND SICHERE ENDGERÄTE

Ausgangssituation

- Enorm große Anzahl an Clients und Servern muss laufend überwacht werden
- Unterschiedliche Betriebssysteme erfordern unterschiedliche technische Expertise
- Großer Aufwand zur professionellen Überwachung der Endgeräte

Lösungsansatz Endpoint Service

- Einführung der Lösung inkl. Anpassung an die Umgebung in einem Vorprojekt
- Nutzung von Agents auf Basis von Microsoft Windows oder Linux zur automatisierten Kontrolle und zum automatisierten Schutz der Endgeräte vor Befall mit Schadsoftware
- Protokollierung aller abgewehrten Vorfälle
- Umsetzung von Maßnahmen nach Kritikalität
- Einbindung in SIEM-Service-Plattform

Leistungsumfang Endpoint Service

- Inbetriebnahme der zentralen Komponenten, Agenten werden durch Kunden installiert
- Regelmäßiger Report über Anzahl der Agenten sowie sicherheitstechnisch bedeutsame Meldungen
- Konstante Überwachung durch IS4IT
- Umgehende Eskalation bei Problemen wie Nichterreichbarkeit einer größeren Zahl von Agenten oder möglichem Malware-Ausbruch
- Updates der Agenten eigenständig oder durch IS4IT
- Regelmäßige Aktualisierung der Analysealgorithmen bei Verbindung des Endpoints mit dem zentralen System
- Monatlich vier Service Requests inkludiert
- 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

Organisatorische Sicherheitsmerkmale

- Betrieb durch ständig geschulte Sicherheitsexperten der IS4IT
- Auswahl der Technologie auf dem aktuellen Stand der Technik durch IS4IT
- Regelmäßige Aktualisierung der Lösung nach Technologie-Entwicklung
- Implementierung von Sensoren auf kritischen Endgeräten zur Erhöhung des Schutzniveaus (optional)

Nutzen für den Kunden

- Automatisierung der Überwachung reduziert Kosten
- Konstante und professionelle Kontrolle der Endgeräte minimiert das Risiko erfolgreicher Angriffe
- Ausgereifte und modernste Technologie mit optimiertem Preis-Leistungs-Verhältnis

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

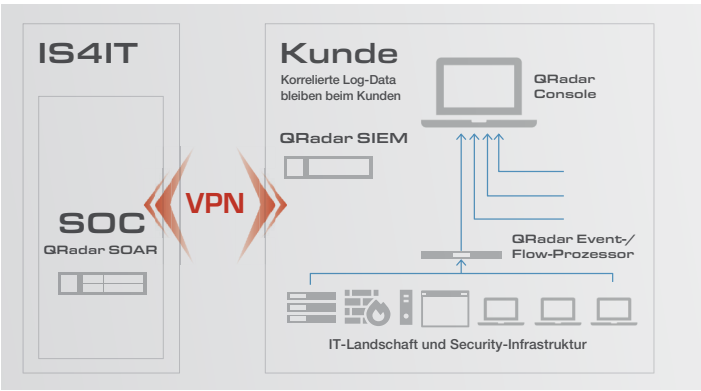
- SIEM Service
- SOAR Service
- Firewall Service
- Web Security Service
- E-Mail-Service
- Vulnerability Management & CSIRT Service
- Endpoint Service
- Network Security Service

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