Managed SOC: SOAR Service

IS4IT KRITIS

DURCHGÄNGIGER SCHUTZ IHRER SYSTEME

Ausgangssituation

- Reduktion der Varianz bei der Bearbeitung von Incident-Response-Prozessen
- Gewährleistung der definierten Abarbeitung von Response-Prozessen
- Sammlung von Daten über Sicherheitsbedrohungen aus einer Vielzahl interner und externer Anwendungen
- Höhere Effektivität aller Sicherheitsoperationen durch Implementierung von Incident-Response-Prozessen
- Priorisierung, Standardisierung und Automatisierung von Vorfallsreaktionen
- Entlastung der Spezialisten von manuellen Tätigkeiten für komplexe Analysen

Lösungsansatz Managed SOAR Service

- Toolbasierte Unterstützung bei Planung, Ablauforganisation, Nachverfolgung und Koordination der Reaktion bei Security Events
- Erfassung und Kodifizierung etablierter Incident-Response-Prozesse in dynamischen Playbooks
- Unterstützung der Sicherheitsoperationen durch Automatisierung und Orchestrierung von Abläufen, Prozessen, der Richtlinienumsetzung sowie des Berichtswesens
- Standardisierte Workflow-, Berichts- und Kollaborationsfunktionen
- Definiertes Vorgehen bei meldepflichtigen Datenschutzverletzungen (Art. 33 DSGVO)
- Integration mit anderen Sicherheitstools

Leistungsumfang Managed SOAR Service

- Definition der Playbooks in Abstimmung mit den Kunden
- Implementierung der Playbooks in der SOAR-Umgebung
- Bereitstellung aller Sicherheitsvorfälle in Echtzeit
- Incident Management bis zur Erledigung eines Vorfalls
- Life-Dashboards zur aktuellen Sicherheitslage
- Integriertes Fallmanagement bis zum Abschluss
- Anlassabhängige Vorschläge für Service-Meetings zur Optimierung der Sicherheitslage
- Steigerung der Organisationsresilienz durch Simulationen von Security Incidents im SOAR
- Vermeidung von Pönalen durch Einhaltung der DSGVO-Vorgaben
- Optionale Integration eines Ticketsystems beim Kunden
- 8x5 Rufbereitschaft im Fehlerfall

Organisatorische Aufgaben mit kundenseitiger Mitwirkung

- Anbindung an SIEM-System
- Implementierung der VPN-Verbindungen
- Konfiguration der Firewalls für die Kommunikation zwischen SIEM und SOAR-System
- Archivierung aller Informationen gemäß Aufbewahrungsfristen
- Etablierung weiterer Schnittstellen zur Automatisierung von Event-Reaktionen oder zur Anreicherung von Kontext-Informationen
- Zeitnahe Entscheidung bzw. Freigabe der Handlungsempfehlungen aus den Vorfällen
- Einbindung Datenschutz für DSGVO-Meldungen

Nutzen für den Kunden

- Sicherheitslösung für alle Systeme und Applikationen
- Schnellere und gezieltere Reaktion auf Sicherheitsvorfälle
- Minimierung von Dauer und Auswirkungen von Cyberattacken
- Optimiertes Bedrohungs- und Schwachstellenmanagement
- Einhaltung hoher Qualitätsstandards dank einheitlicher Bearbeitung der Sicherheitsvorfälle
- Aktuelle Sicherheitslage immer im Blick dank Live-Dashboard
- Risikomanagement in Bezug auf DSGVO-Vorfälle

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

IS4IT KRITIS

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

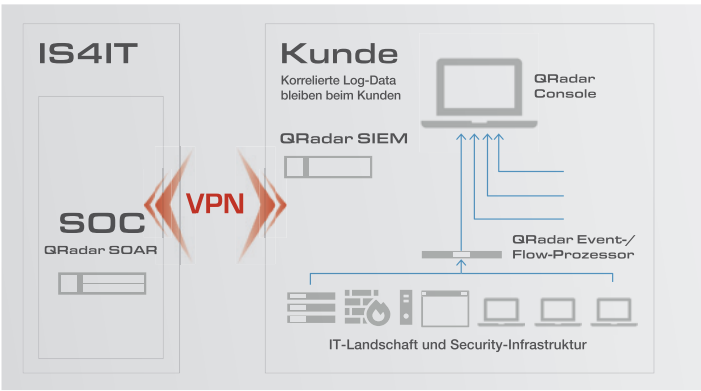
- SIEM Service
- SOAR Service
- Firewall Service
- Web Security Service
- E-Mail-Service
- Vulnerability Management & CSIRT Service
- Endpoint Service
- Network Security Service

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