Managed SOC: SIEM Service

IS4IT KRITIS

DURCHGÄNGIGER SCHUTZ KRITISCHER SYSTEME

Ausgangssituation

- Unverzichtbarer Schutz unternehmenskritischer Systeme inklusive industrieller Steuerungssysteme und eingebetteter Software in Geräten mit Befall von Schadsoftware, Spionage oder missbräuchlicher Nutzung
- Erkennung und Abwehr von Angri en anhand definierter Maßnahmen
- Gewährleistung der Einhaltung eines klar definierten Sicherheitsniveaus

Lösungsansatz SIEM Service

- Analyse und Definition der Sicherheitsanforderungen und des Netzwerks
- Installation einer vorkonfigurierten Appliance für Eventkorrelation und/oder Netzwerk-Flow-Überwachung im RZ des Kunden
- Betrieb aller notwendigen Appliances über abgesicherten Fernzugri im IS4IT SOC
- Umsetzung auf Basis vereinbarter SLAs

Leistungsumfang SIEM Service

- Bereitstellung aller Sicherheitsdaten in Echtzeit
- Überwachung und Korrelation der eingegangenen Events und des analysierten Netzwerk-Tra cs, Auswertung durch geschulte IT-Security-Experten
- Regelmäßige Aktualisierung der Datenbanken bezüglich schädlicher URLs und IP-Adressen
- Incident Management bis zur Erledigung eines Vorfalls
- Regelmäßige Dokumentationen und Auswertungen
- Kontrollierte Ticketverarbeitung je nach Art der Sicherheitsvorfälle
- Anlassabhängige Vorschläge für Service-Meetings zur Optimierung der Sicherheitslage
- 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 und Service-Level zwischen 30 Minuten und 24 Stunden

Organisatorische Aufgaben mit kundenseitiger Mitwirkung

- Bereitstellung von VMware-Umgebung
- Implementierung der VPN-Verbindungen
- Konfiguration der Firewalls für die Weiterleitung der Events zur Appliance
- Implementierung der Regeln der Event-Weiterleitung
- Umgehende Meldung von Ereignissen, die die Nutzbarkeit der Lösung oder Sicherheit des Betriebs beeinträchtigen
- Archivierung aller Informationen gemäß Aufbewahrungsfristen

Nutzen für den Kunden

- Zeitgleiche Überwachung sämtlicher Unternehmensnetzwerke
- Maximale Sicherheit für unternehmenskritische Systeme
- Gewährleistung eines ungestörten Produktivbetriebs

IS4IT KRITIS GmbH Kraichgaublick 13 74847 Obrigheim telefon +49 6261 31944-0 fax +49 6261 31944-9 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

Lösungsansatz Managed SOC

- Security-Analysten betreuen mehrere Unternehmen parallel
- Optimale Infrastrukturnutzung Mandantenfähigkeit und virtuelle Server

Leistungsumfang Managed SOC

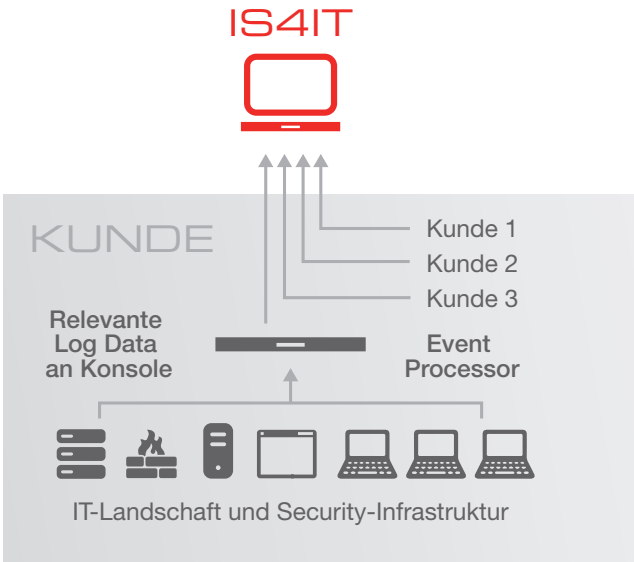
- SIEM Service
- SOAR Service
- E-Mail-Service
- Vulnerability Management
- Endpoint Service
- Network Security Service

Warum Informationssicherheit mit IS4IT?

- Schneller Return on Investment
- Klare Aufgabentrennung zwischen Betrieb und Sicherheit

Nutzen für den Kunden

- Monatlicher Festpreis, halbjährige Kündigungsfrist,
- Mindestlaufzeit von 12 oder 36 Monaten
- Rechtlich abgesicherte Sicherheitskonzepte und revisionssichere Datenhaltung



IS4IT KRITIS GmbH Kraichgaublick 13 74847 Obrigheim telefon +49 6261 31944-0 fax +49 6261 31944-9 info@is4it-kritis.de www.is4it-kritis.de