

Kontrolle ist gut. Überblick mit SIEM ist besser.



Bekanntlich verweilen Hacker längere Zeit bevor sie zuschlagen. Hacker leben davon, dass Lücken vorhanden sind und keine übergreifenden Überwachungseinrichtungen vorhanden sind. So können sie sich unerkannt bewegen, weil jede Aktion die sie setzen, für sich betrachtet, meist unerkannt bleiben kann.

So unterstützt Sie Managed Service SIEM

Der SIEM Ansatz (Security Information and Event Management) bietet eine ganzheitliche Sicht auf die Sicherheit der IT Ihres Unternehmens. Von Benutzertransaktionen, Useraktivitäten, Maschinenverhalten bis Sicherheitsbedrohungen - ein SIEM Dashboard bringt Überblick über die wesentlichsten Informationen.

Managed Service SIEM ist das perfekte Service bei Ressourcen-Engpässen – wenn nötig sogar sieben Tage die Woche, rund um die Uhr. Es wird die SIEM-Umgebung hinsichtlich Verfügbarkeit und Leistungsfähigkeit überwacht. Gegebenenfalls werden neue Systeme integriert und ständige Detailprüfung von Security Incidents durchgeführt. Im Falle eines Vorfalls erfolgt das Auslösen von vordefinierten Entscheidungswegen. Die Abbildung und Prüfung von unterschiedlichen Security Case Examples (UseCases/Fallbeispielen) sowie die Erstellung von Security Reports erfolgt ebenfalls vom Partner. Sie erhalten laufend Vorschläge zur Verbesserung der SIEM-Lösung und definierte und geprüfte Notfallprozesse mit predictive Decisions. Das Ziel ist: Ihre Mitarbeiter zu entlasten, ohne dass die Security Qualität darunter leidet.

Darum ITdesign

- ✔ Langjährige Erfahrung beim Thema Monitoring
- ✔ Kompetenz in der Analyse und der graphischen Darstellung von großen Datenmengen
- ✔ Langjähriges Know How von ITdesign im Bereich Security und Infrastruktur
- ✔ Langjähriges Betriebs-Know How
- ✔ Verbindung von Technik und Organisation damit IT wirksamer wird

Ihre Erfolgsfaktoren

- ✔ Unterstützung bei der Einhaltung von Compliance Vorgaben
- ✔ Automatisches Sammeln und Indexieren von jeglichen Maschinendaten zur besseren Klassifizierung und Suche
- ✔ Überwachung und Echtzeitwarnungen bei kritischen Systemen
- ✔ Einfache Erstellung von leistungsstarken Berichten und Dashboards
- ✔ Erstellung von Ad-Hoc Berichten
- ✔ Bei Ressourcen-Engpässen als Managed Service zur Verfügung gestellt. Somit entstehen die Aufwände auf Kundenseite erst bei einem Sicherheitsvorfall.
- ✔ professionelle strukturierte Abwicklung von Security Vorfällen