Security Information & Event Management (SIEM) as a Service

Echtzeitanalyse aller sicherheitsrelevanten Ereignisse. Automatisierte Alarme und Abwehrmaßnahmen.

Anwendungsfälle

- Änderungen an administrativen Accounts oder Gruppen
- Anmeldungen an kritischen Systemen
- Anmeldungen mit nicht-personalisierten administrativen Accounts
- Exploitversuche auf Basis des Netzwerkverkehrs
- User Behaviour Analytics
- Untypische Anmeldungen und Zugriffe (Zeit, Quell- und Zielsystem, VPN)
- Virusinfektionen in kurzer Zeit auf mehreren Clients
- Zugriff und Änderungen auf kritische Systeme
- Korrelation der Meldungen des IDS und Verwendung im Rahmen der Analysen
- Verfolgung von Malware Kommunikation (Command & Control, CIFS NULL Sessions)
- Auswertung sämtlicher korrelierter Events auf mehreren Korrelationsebenen
- Automatische Alarmierung

Vorteile SIEM as a Service

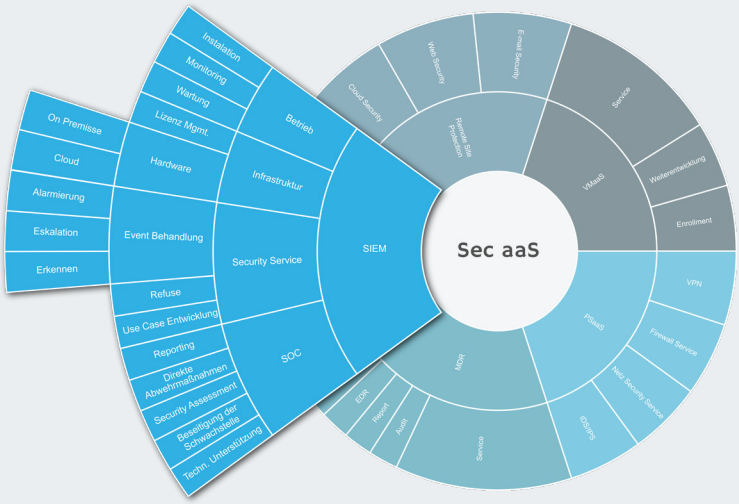
- Entlastung des IT Personals
- Keine eigene Infrastruktur erfolderlich
- Dediziertes Hosting in einem ISO27001 Rechenzentrum
- Patch-, Change- und Incident-Management
- Cyber Security Beratung
- Weiterentwicklung und Erweiterung von von Anwendungsfällen
- Einfache Skalierbarkeit
- Vollständige Ursachendokumentation für weiterführende forensische Untersuchungen

Warum benötigen Sie ein SIEM?

Mit der fortschreitenden Digitalisierung Ihrer Krankenhausprozesse steigt die Anzahl der zu überwachenden Endpunkte exponentiell. Die gesamte Infrastruktur permanent zu überwachen und potenzielle Angriffe auf kritische Daten abzuwehren wird zu einer immer aufwändigeren Aufgabe für Ihre knappen IT-Ressourcen.

Ein SIEM-System korreliert die Log-Daten der angebundenen Quellen in Echtzeit, identifiziert potenziell gefährliche Auffälligkeiten (Events), beurteilt diese hinsichtlich des Risikopotenzials und initiiert bei Bedarf individuell festgelegte Abwehrmaßnahmen. Das SIEM ermöglicht es, die Vielzahl an Quellsystemen - von Infrastrukturkomponenten wie Active Directory, Web-Proxy, VPN-Gateways, Firewalls und Datenbank-Servern bis zu Ihren krankenhausspezifischen Anwendungen - ganzheitlich unter Sicherheitsaspekten zu überwachen. Ein Mehrwert, den ein System allein nie erreichen kann.

omniIT stellt Ihnen ein vollständiges SIEM als Dienstleistung bereit. So müssen Sie keine eigene Infrastruktur aufbauen, das System nicht selbst betreiben oder Mitarbeiter schulen und abstellen. Die Experten von omniIT definieren gemeinsam mit Ihnen die kritischen Anwendungsfälle, identifizieren relevante Quellsysteme und Logs und konfigurieren das SIEM individuell auf Ihre Bedürfnisse. Während des Betriebs übernimmt omniIT die komplette Prozess- und Betriebsverantwortung, inklusive revisionssicherer Backups der Vorfälle und Tickets sowie regelmäßiger Auswertungen und Berichte für Ihre Compliance-Anforderungen.



Modulare Services für jede Sicherheitsanforderung

SIEM Service
- Durchgängiger Schutz kritischer Systeme

Network Security Service
- Kontrollierte und sichere Netzwerke

Vulnerability Management
- Keine Schwachstelle bleibt unentdeckt

Cloud Management
- Sicherheit für Public Cloud Infrastrukturen

Firewall Service
- Die Firewall-Lösung für jeden Bedarf

Endpoint Service
- Überwachte und sichere Endgeräte

Web Security Service
- Sicherer Web-Zugang für Ihre Anwender

E-Mail-Security
- Sichere Kommunikation und Überwachung (DKIM, DMARC)

Erfahren Sie mehr

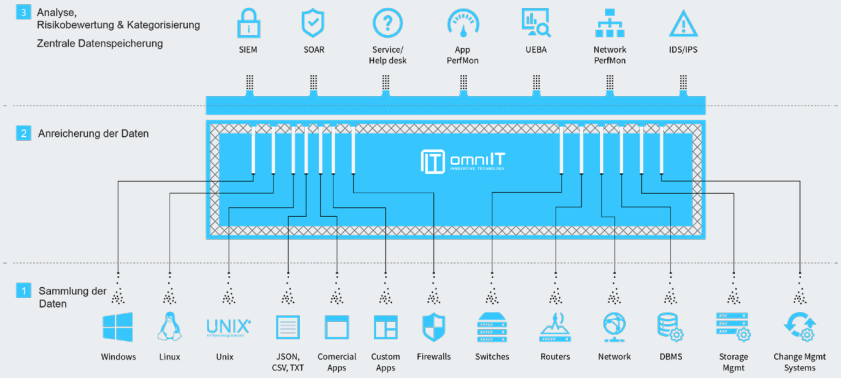
Kontaktieren Sie uns für eine gratis Demo oder individuelle Beratung durch unsere KHZG-zertifizierten Experten.

Michael Ruhdorfer
Tel.: +49 (89) 998 241 920
Mail: secaas@omniit.de

omniIT GmbH
Georg-Hallmaier-Str. 6
81369 München
Telefon +49 89 998 24192 0
E-Mail: info@omniit.de
Web: www.omniit.de
KHZG Webpage: www.khzg.omniit.de
Geschäftsführer: Patryk Wlodarczyk, Marek Chroust

SIEM Überblick

- Analyse von Anomalien im Netzwerk
- Erkennen von Events wie z. B. Attacken durch WannaCry
- Sofortiges Eliminieren von Bedrohungen und Schwachstellen
- Individuell definierte Abwehrstrategien



Ihr Mehrwert

- Proaktive Überwachung der IT-Systeme und kontinuierliche Analyse der aktuellen Bedrohungslage
- Eskalation bei erkannten potentiellen Angriffen mit umsetzbaren Handlungsempfehlungen
- Zentrales Sicherheitsmanagement für die unterschiedlichen Endpunkte
- Regelmäßige Berichte und Auswertungen
- Revisionssichere Backups der Vorfälle und Tickets
- Kontinuierliches Nachschärfen der Auswerteregeln

Wir sind omniIT

Wir aktivieren Ihre digitale DNA!

Als digitaler Komplettanbieter erstreckt sich unser Angebot von IT-Sicherheit über IT-Infrastruktur bis hin zu Software-Entwicklung, Beratungsprojekten und Managed IT-Services.

Unser Team arbeitet für den Erfolg nationaler und internationaler Unternehmen. Wir agieren stets transparent und kommunizieren auf Augenhöhe. Unsere KHZG-zertifizierten Experten begleiten Sie bei Ihren Digitalisierungsprojekten, damit Sie Ihre Ziele im Rahmen Ihrer Zeit- und Budgetvorgaben erreichen.

Unser Portfolio