# 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
- Unabhängige Überwachung Ihrer IT-Landschaft
- 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

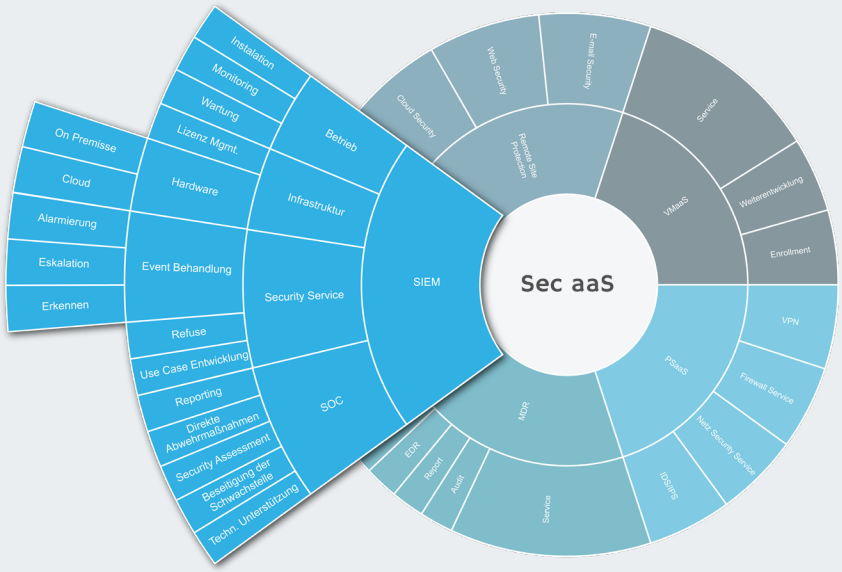
## Warum benötigen Sie ein SIEM?

**Security Information & Event Management (SIEM)** basiert auf einer permanenten real-time Analyse von Informationen aus der zu schützenden IT-Infrastruktur.

SIEM bietet die Voraussetzungen, um unter Sicherheitsaspekten mit ganzheitlicher Sicht auf die IT zu agieren - „all time in real time“. Damit potenziell gefährliche Auffälligkeiten (Events) identifiziert werden, setzt SIEM die Daten verschiedener Log-Quellen in Korrelation.

Zu diesen Quellen zählen zum Beispiel Active Directory, Web-Proxy, VPN-Gateways, Firewalls, Datenbank-Server uvm. Über die universale Log-Analyse im Netzwerk bietet SIEM einen Mehrwert, den ein System allein nie erreichen kann. Jeder identifizierte Event wird sofort auf sein Risikopotential hin beurteilt.

Sollte dabei Gefahr im Verzug drohen, starten ebenso schnell die individuell festgelegten Abwehrmaßnahmen. Um das SIEM nicht selbst betreiben und Mitarbeiter zu schulen und abstellen zu müssen, stellt omniIT ein SIEM as a Service zur Verfügung. Dabei übernehmen die Experten von omniIT die komplette Prozess- und Betriebsverantwortung - inklusive aller einzelnen dafür benötigten Tätigkeiten.



## 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, um eine Demo kostenlos in Ihrem Unternehmen zu testen.

Für weitere Informationen oder Vertriebliche Fragen stehen wir gerne für Sie zur Verfügung:

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

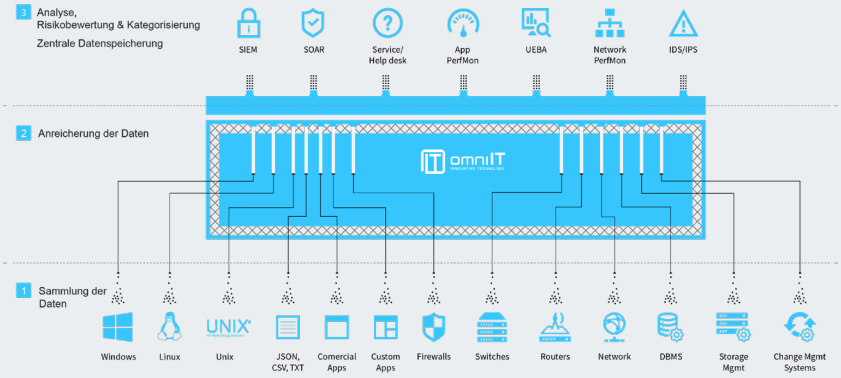
omniIT GmbH
Georg-Hallmaier-Str. 6
81369 München
Telefon +49 89 998 24192 0
E-Mail: info@omniit.de
Web: www.omniit.de
Geschäftsführer: Patryk Wlodarczyk, Marek Chroust



## Fazit

Die Stärken dieses „Frühwarnsystems“ für die IT sind heute unbestritten. Hier dazu nochmal die vier tragenden Säulen jeder SIEM-Lösung:

- 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 laufende Analysen zur aktuellen Bedrohungslage
- Eskalation bei erkannten potentiellen Angriffen mit umsetzbaren Handlungsempfehlung
- Zentrales Sicherheitsmanagement für die unterschiedlichen Endpunkte
- Regelmäßige Berichte und Auswertungen
- Revisionssichere Backups der Vorfälle und Tickets
- Kontinuierliches „Nachschärfen“ der Auswerteregeln zu den Use Cases

## Wir sind omniIT

Wir aktivieren Ihre digitale DNA!

Als Full-Service IT-Dienstleister erstreckt sich unser Angebot von IT-Sicherheit über die ITInfrastruktur bis hin zur Software-Entwicklung, Beratungsprojekten und Managed IT-Services. Nutzen Sie uns als verlängerte Werkbank, um Ihre Ziele zeitnah und mit den erwarteten Ergebnissen zu erreichen.

Unser Team arbeitet für den Erfolg nationaler und internationaler Unternehmen - egal ob Mittelstand oder Großkonzern aus der Technologie-, Automobil-, Finanz- oder Telekommunikationsbranche. Wir agieren stets transparent und kommunizieren auf Augenhöhe.

## Unser Portfolio