

# SIEMOC

## Das SIEM von COMPRISE

Komfortabel, Erweiterbar, Integrierbar, Flexibel – leistbares Security Information und Event Management auf Enterprise Niveau



### UEBA

User and Entity Behavior Analytics



### Threat Intelligence

Automatische Nutzung von Sicherheitsinformationen



### Endpoint Protection

Signaturlose Malware-Erkennung



### Compliance

Zur Erfüllung höchster Compliance Standards



### Preiswert

Attraktives Lizenzmodell mit planbaren Kosten



### Flexibel

Umfangreiche Erweiterungsmöglichkeiten



### Überschaubar

Vorgefertigte Regelwerke und Auswertungen



### Alarmierung

Automatische Alarmierung bei Cyberangriffen



### Machine Learning

Automatisierte Anomaliedetektion



### Skalierbar

Unbegrenzte Skalierbarkeit

## SIEMOC – Security und Compliance einfach erreicht

### Beginnen Sie innerhalb von Minuten mit dem Erkennen von Sicherheitsbedrohungen in Echtzeit

Eine einheitliche Kommandozentrale für Echtzeit-Kontrolle und Einblick in alle System-, Anwendungs- und Benutzeraktivitäten. Konformitätsnachweis bei reduzierten Betriebskosten und Minimierung des Aufwands für Audit, Forensik und Betrugserkennung.

Zunehmende Vorschriften und Geschäftspartnern zwingen immer mehr zur Bewertung von Sicherheitsrisiken und zur Planung und Umsetzung umfassender Sicherheitsstrategien. Meistens findet man dabei eine wesentliche Lücke im Bereich der automatisierten Sicherheitsüberwachung, Alarmierung, Forensik und Berichterstattung.

SIEMOC füllt diese Lücke und bietet ein kostengünstigeres SIEM mit den Kernfunktionen, die von Vorschriften und Profis gefordert werden. Auf der bewährten Technologie von LOMOC aufbauend bietet es die Logsammlung von Sicherheits- und Netzwerkgeräten, Servern, Clients, Cloud-Servern und -Apps sowie Unternehmensanwendungen. Einmal erfasst, werden diese analysiert, korreliert und mit Warnmeldungen und forensischen Funktionen versehen. Wir bieten dies für Sie auch gerne als ein komplett verwaltetes Service an – so dass Sie kein Experte in dieser fortschrittlichen Technologie werden müssen!

SIEMOC erhöht durch durchdachte Integration verschiedenster Datenquellen die Transparenz Ihrer IT-Landschaft. Die Nutzung vordefinierter Mechanismen zur Anomalieerkennung und die Einbeziehung öffentlich verfügbare Erkennungsregeln. Leistungsfähige Untersuchungsfunktionen und ein integriertes Case-Management beschleunigen Ihre Gefahrenbekämpfung erheblich. Mit der einheitlichen Verfügbarkeit aller Funktionalitäten in einer einzigen modernen Oberfläche bewahren Sie immer die Übersicht und reagieren rasch auf sich ändernde Rahmenbedingungen.

Log-Daten sind die schwer entzifferbare „Golden Records“ der digitalen Forensik. Mit SIEMOC reagieren Sie schneller als sich ein Angreifer ausbreiten kann – mit den Analyse-möglichkeiten sammeln Sie Beweise und vollziehen Angriffe nach so einfach wie noch nie.

Eine All-in-One-SIEM-Lösung für die Erfassung, Speicherung, Analyse und Berichterstellung von Protokollen, die Ihre IT-Profis dabei unterstützt, Cyber-Bedrohungen zu erkennen und darauf zu reagieren und die Einhaltung von Vorschriften nachzuweisen.

### Key Features

- **Einfache Benutzerführung.** Durchsuchen Sie rasch riesige Datenmengen auf verdächtige Muster und visualisieren übersichtlich Zusammenhänge.
- **Out-of-the-Box Sicherheit.** Vordefinierte Korrelationsregeln ermöglichen automatisch bei möglichen Sicherheitsverletzungen zu alarmieren.
- **Echtzeit-Korrelation.** Echtzeit-Protokoll- und Ereigniskorrelationen durch vorgelagerte Normalisierung von Protokolldaten.
- **Threat Intelligence.** Ergänzung der Korrelationsregeln durch voll integrierte Aktualisierung von Threat Intelligence Feeds.
- **Unlimitierte Protokollierung.** Sammlung und Indizierung von System- und Anwendungsprotokollen aus beliebigen Quellen.
- **MITRE ATT&CK.** Integration einer weltweiten Knowledge-Base von aktuellen Angriffstaktiken und -techniken für eine effektive Abwehr.

# SIEMOC

## Das SIEM von COMPRISE

Komfortabel, Erweiterbar, Integrierbar, Flexibel

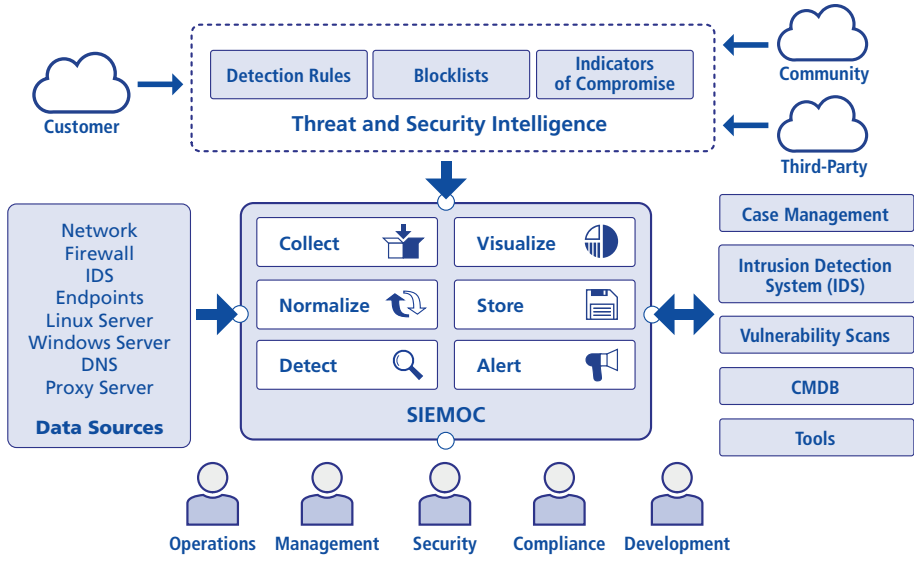
– leistungsfähiges Security Information und Event Management auf Enterprise Niveau



**Bedrohung effektiv abwehren**  
– rasch und einfach

**Vorschriften effektiv erfüllen –**  
bei geringeren Kosten

**Sicherheits-Management –**  
mit Support aus Europa



**Sicher.** Die Sicherheitsfunktionen von SIEMOC sorgen dafür, dass auch nur Zugriff erhält, wer zugreifen darf. Entscheiden Sie sich für die Gewissheit, dass in SIEMOC gespeicherten Daten auch sicher und geschützt sind.

**Bewährt.** Robust, skalierbar, flexibel und preiswert durch die Technologiebasis LOMOC von COMPRISE.

**Zuverlässig.** Hohe Erkennungsrate durch hohe Automation und modernste Machine-Learning Algorithmen.

**Sicherheit einfach erhöht mit SIEMOC von COMPRISE**

### Impressum

Medieninhaber: COMPRISE GmbH  
Wiedner Hauptstraße 76, 1040 Wien, Austria (Europe)  
info@comprise.world | www.comprise.world | Firmenbuch: FN 523846m | Handelsgericht Wien UID: ATU75083847



Stand April 2023