

# 8com Security Operations Center

## Bedrohungserkennung

### HIGHLIGHTS

- Fehlertolerante Threat-Erkennung**  
 Umfassende Sichtbarkeit garantiert, dass Angriffe mehrfach erkannt werden können.
- Validere Erkennung durch Daten-korrelation**  
 Umfassende Korrelation einer Vielzahl von Security Events zur besseren Bedrohungserkennung.
- Erkennung in Echtzeit und Retrospektiv**  
 Echtzeitalarmierung und der Blick auf zurückliegende Sicherheitsereignisse sind ein entscheidender Vorteil, um Advanced Persistent Threats zu begegnen.
- Kontinuierliche Optimierung der Sichtbarkeit**  
 Die Architekten unseres SOC entwickeln unsere Services permanent weiter, um die Sichtbarkeit zu optimieren.
- Individueller Technologieeinsatz:**  
 SIEM, Machine Learning, Endpoint Detection and Response, Threat Feeds, Honeypots u. v. m.
- Bewährt und sicher**  
 Ausgezeichnete Technologien und hohe Sicherheitsstandards.
- Hochskalierbar und kostentransparent**  
 Die Bedrohungserkennung kann jederzeit der gewachsenen Infrastruktur angepasst werden. Unangenehme Kostenexplosionen sind durch unser transparentes Kostenmodell ausgeschlossen.



Bei der Bedrohungserkennung von 8com setzen wir auf umfassende Transparenz und Sichtbarkeit. Das bedeutet, dass an das SIEM unseres Technologiepartners alle relevanten Datenquellen angebunden werden (Firewall, Proxy, VPN, AV, Switches, DCs, Memberserver, DMZ-Systeme, Clients, u. v. m.).

Dadurch können Cyberangriffe, die an einer Datenquelle nicht oder zu spät erkannt werden, an anderer Stelle entdeckt und abgewehrt werden.

Durch umfassende Korrelation einer Vielzahl von Security Events unterschiedlicher Datenquellen erkennen wir nicht nur klassische Hacking-Angriffe sondern Veränderungen und Manipulationen jeglicher Art.

Die Ergebnisse aus der Analyse von False Positives, aktuelle Threat- und Bedrohungsinformationen und die Erkenntnisse anderer Fachabteilungen (bspw.: Penetration Testing) werden von den Architekten unseres SOC berücksichtigt, um die Sichtbarkeit unserer Services weiterzuentwickeln.

Die SOC-Architekten modellieren für unsere Kunden individuelle Sicherheitsstrategien und berücksichtigen branchenspezifische Anforderungen.

Wir setzen dabei immer auf ausgezeichnete und zertifizierte Technologien unterschiedlicher Anbieter und zahlreiche Threat Feeds.

### 8com GmbH & Co. KG

Europastraße 32  
 67433 Neustadt a. d. Weinstraße  
 Germany

☎ +49 89 413270707

✉ [soc@8com.de](mailto:soc@8com.de)

🌐 [www.8com.de/soc](http://www.8com.de/soc)