

FIGHTING CYBERCRIME

# Security Operations Center

 **Advanced**

Mehr Sichtbarkeit. Mehr Reaktion. Mehr Sicherheit.





PROAKTIV STATT REAKTIV

## Erweiterte Bedrohungsanalyse

# 24/7 Detection & Response und Darknet Monitoring



**8COM betreibt das einzige  
SOC im DACH-Raum  
mit ISO 27001 nach  
BSI-IT-Grundschutz.**

C5-testierte Technologie.  
Betrieb in einem deutschen  
RC4-Hochsicherheitsbereich.  
24/7/365 sind hochqualifizierte  
SOC-Analysten vor Ort für Sie  
im Einsatz – in Ihrer Sprache  
(Deutsch/Englisch).

# SOC Solution Package | Advanced

## XDR as a Service

Extended Detection & Response mit Palo Alto Cortex XDR Pro (C5-testiert) oder Microsoft Defender. 24/7/365 Schutz für Endpunkte, Cloud/SaaS, Identitäten & Firewalls/VPNs. Inklusive XSOAR, DFIR und Flatrate für Alarmbearbeitung, Service & Support.

## Best of Breed

Unsere Technologieauswahl im SOC orientiert sich an unabhängigen Wirksamkeitstests wie den MITRE ATT&CK® Evaluations. Technisch, organisatorisch und strategisch auf Herz und Nieren geprüft für kompromisslose Qualität.

## Extended Threat Hunting (XTH)

Hypothesengetriebenes Threat Hunting zur proaktiven Suche nach versteckten oder fortgeschrittenen Bedrohungen, die nicht durch klassische Erkennungsmethoden auffallen.

## Identity Threat Detection & Response (ITDR)

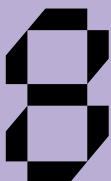
Schutz vor Insider-Bedrohungen, Credential Theft und Lateral Movement durch die tiefgehende Analyse von Benutzer- und Host-Aktivitäten.

## Darknet Monitoring

Überwachung und Analyse digitaler Identitäten auf Basis der weltweit größten kommerziell verfügbare Darknet-Datenbank mit DarkOwl zum Schutz zur frühzeitigen Erkennung kompromittierter Informationen.

## Optionale SIEM-Integration

Die optionale SIEM-Integration erweitert die Überwachungsmöglichkeiten von Cortex XDR Pro um zusätzliche Systeme, beispielsweise Firewall-Systeme von Sophos und Watchguard sowie weitere VPN- und Remote-Access-Lösungen.



**Mehr Tiefe. Mehr Integration. Mehr Schutz.  
Zukunftssicher aufgestellt.**

SOC Advanced erweitert den Core-Schutz um Identity Monitoring (inkl. Darknet), Cloud Security und die Überwachung von Firewalls & VPNs – perfekt für komplexe IT-Umgebungen.

# 20 Jahre Vorsprung – 20 Jahre Cyber Security Expertise



Seit über zwei Jahrzehnten beschäftigen wir uns ausschließlich mit Cyber Security – mit eigener Infrastruktur, exklusiven Zertifizierungen und methodischer Tiefe.

Unser SOC ist das Ergebnis langer Erfahrung und kontinuierlicher Weiterentwicklung. Wir stehen für einen Sicherheitsanspruch, der im Ernstfall hält, was andere versprechen.

## Sicherheit, die weiterdenkt.

Jetzt SOC Advanced kennenlernen und Bedrohungen abwehren, bevor sie Schaden anrichten.



Mehr Details finden Sie hier:  
[www.8com.de/soc](http://www.8com.de/soc)

**8com GmbH & Co. KG**  
Europastraße 32  
67433 Neustadt/Weinstraße

**E-Mail:** [info@8com.de](mailto:info@8com.de)  
**Telefon:** +49 6321 48446-0

**8COM**