SOC-Solution Packages

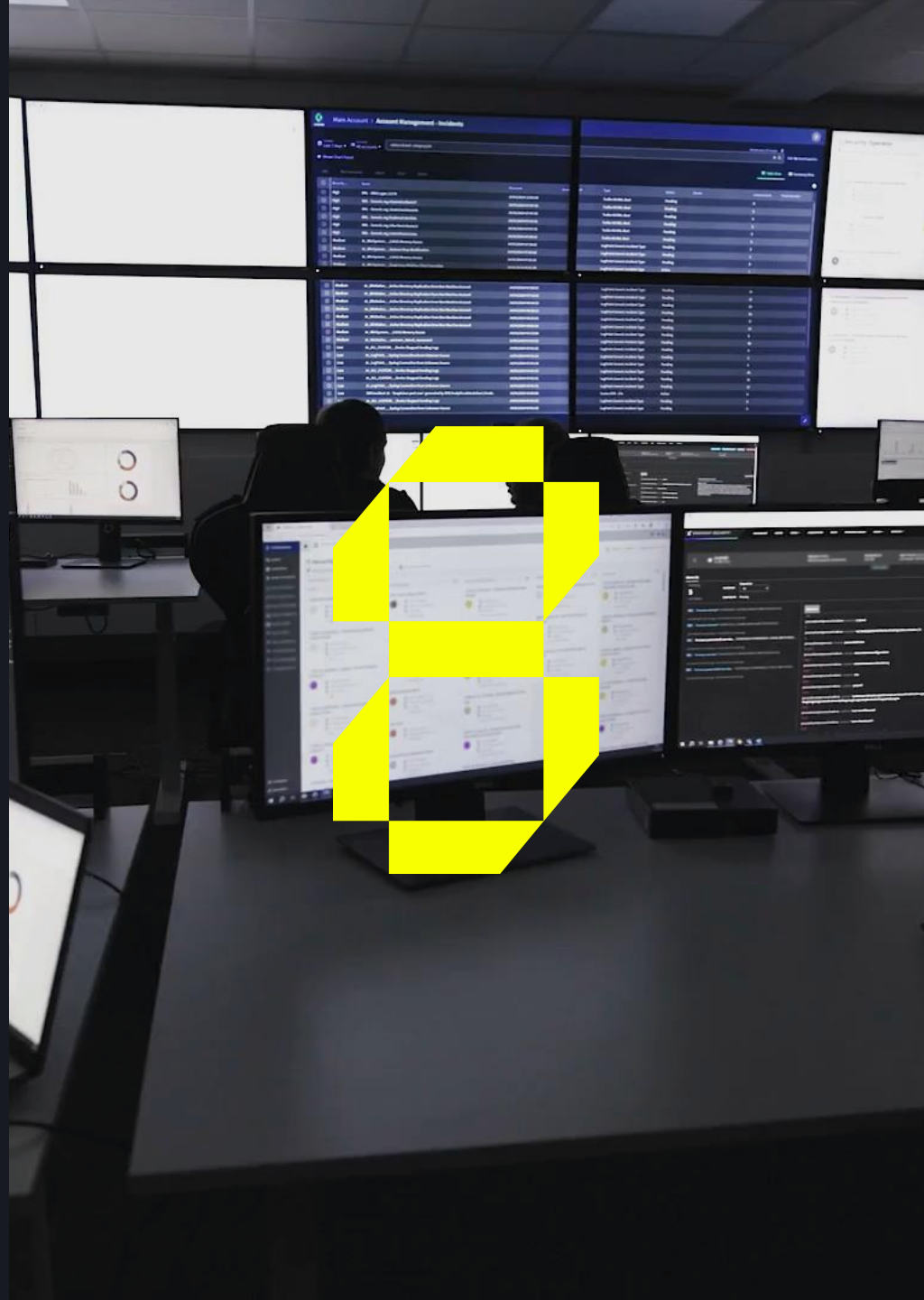
8COM CYBER SECURITY

Optimal vorbereitet

Cyberangriffe erkennen und sofort stoppen.

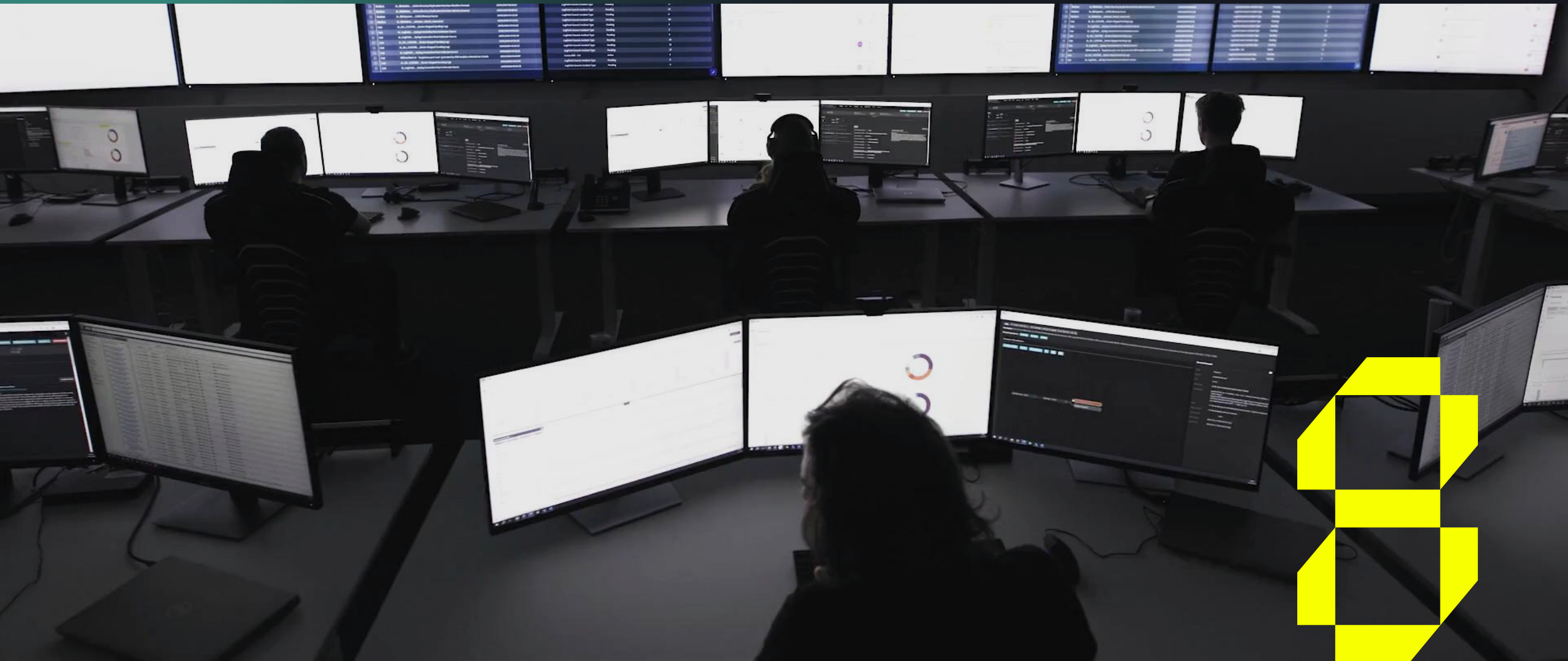
Wir schützen Unternehmen und Behörden mit kompromissloser Qualität und modernster Technologie — 24 Stunden am Tag, 365 Tage im Jahr.

8COM
CYBER SECURITY



Security Operations Center
24/7/365

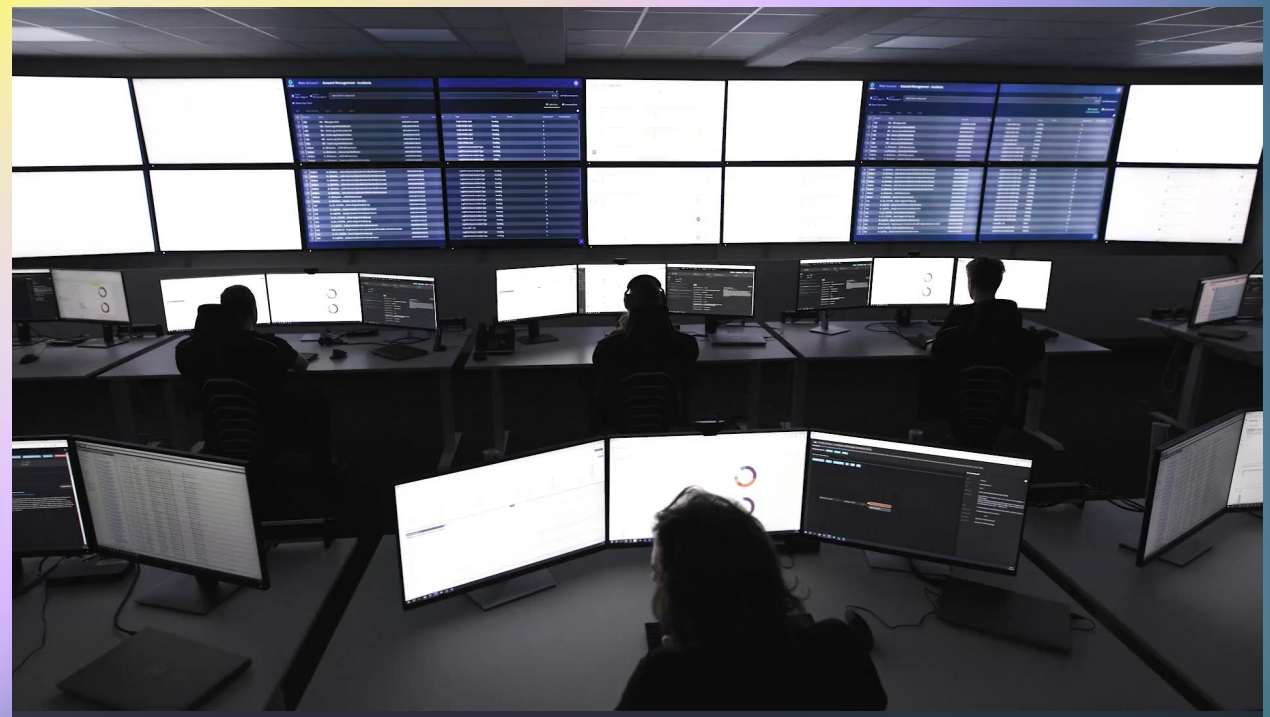
8COM



8COM

Security Operations Center 24/7/365

- 2004 gegründet
- Seit 2011 SOC as a Service
- 120 Mitarbeitende (festangestellt)
- 128 SOC-Kunden



Trust Seal
www.teletrust.de/itsmig
SecurITy made in Germany

Bundesamt für Sicherheit in der Informationstechnik
ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz
Zertifikat Nummer:
BSI-IGZ-0693-2025
Gültig bis:23.06.2028

2025: 8com SOC Ecosystem

„Best of breed“

8COM

Supported only (Anbindung über XSOAR)

SIEM andere | xDR andere | NDR andere

Fully Managed

ISO 27001 Security certificate
ISO 27701 Privacy certificate

ISO 27017 Security certificate
ISO 27018 Privacy certificate
(Für cloud service provider)

SOC 2 Type 1 & 2

Common Criteria

Agence nationale de la sécurité des systèmes d'information (ANSSI) **NGFW certification**

Cloud Computing Compliance Controls Catalogue (C5)
BSI - Bundesamt für Sicherheit in der Informationstechnik

SIEM Logpoint MS Sentinel (Q2/2026)	Vulnerability Management Qualys + Tenable	SAP Security Monitoring securityBridge	Darknet Monitoring DarkOwl	Phishing Playbook inkl. Sandboxing PAN XSOAR
XDR Palo Alto Cortex MS-Defender	OT Security Nozomi	DFIR Asgard + Thor	CTEM XM-Cyber	Threat Hunting PAN XSOAR, BlueLiv

Palo Alto Cortex xSOAR

8com SOC

LOGPOINT | Qualys. | NOZOMI NETWORKS | Security Bridge | XM Cyber | CORTEX BY PALO ALTO NETWORKS

Ein SOC – drei Einstiege. Flexibel, sicher, kompromisslos.

Immer dabei: 24/7/365 SOC, BSI IT Grundschutz-zertifiziert, Made in Germany.

8COM

CORE
sicherer Start

Managed-SOC aus DE
BSI IT-Grundschutz zertifiziert

Alle SOC Analysten sind professionell ausgebildet und nach SANS zertifiziert

Echtes 24/7/365 Security Monitoring
Clients/Server/Smartphones/Tablets

24/7/365 Threat Analyzes und Hunting

Flatrate für unbegrenzte Alarmbearbeitung

Marktführende Technologie:
Palo Alto Cortex XDR (Best of Breed) oder kostengünstiger Einstieg mit MS-Defender Technologie-Stack

Orchestrierung und Automatisierung durch Palo Alto xSOAR

Weitere Add-ONs wie Vuln-Mgmt etc.

ADVANCED
umfassender Schutz Core inklusive

Erweiterte Sicherheit durch Integration:

- Firewalls
- VPN-Server
- Cloud-Tenants wie Microsoft 365, AWS und GCP
  Identity Provider (AD, Entra ID etc.)

Darknet Monitoring

Individuelle Aufbewahrungsdauer von Logfiles (relevant für spätere Forensische Analysten etc.)

Optionaler Einsatz von SIEM Lösungen

Diverse weitere Add-Ons

- OT-Security Monitoring mit Nozomi
- CTEM
- . . .

INFINITY
Premium Detektion & Response

Vollständig flexibel und individuell anpassbar

2 „named“ SOC-Analysten als feste Ansprechpartner

SIEM mit über 400 proprietäre

- Use-Cases für beste Detektionsleistung
- Weitere individuelle Use-Cases können schnell integriert werden
- Beste Preise für Incident-Response und Forensik Stunden

Diverse weitere Add-ONs

- SAP-Security Monitoring
- Application Security Monitoring wie z.B. Fachanwendungen, SalesForce . . .
- . . .

8COM
CYBER SECURITY

Read for SOC?

Wann dürfen wir Sie als neuen SOC-Kunden der 8com begrüßen?

Gerne laden wir Sie zu einer SOC-Besichtigung ein!