SOC-IN-A-BOX

Ein vollständiger SOC-Service

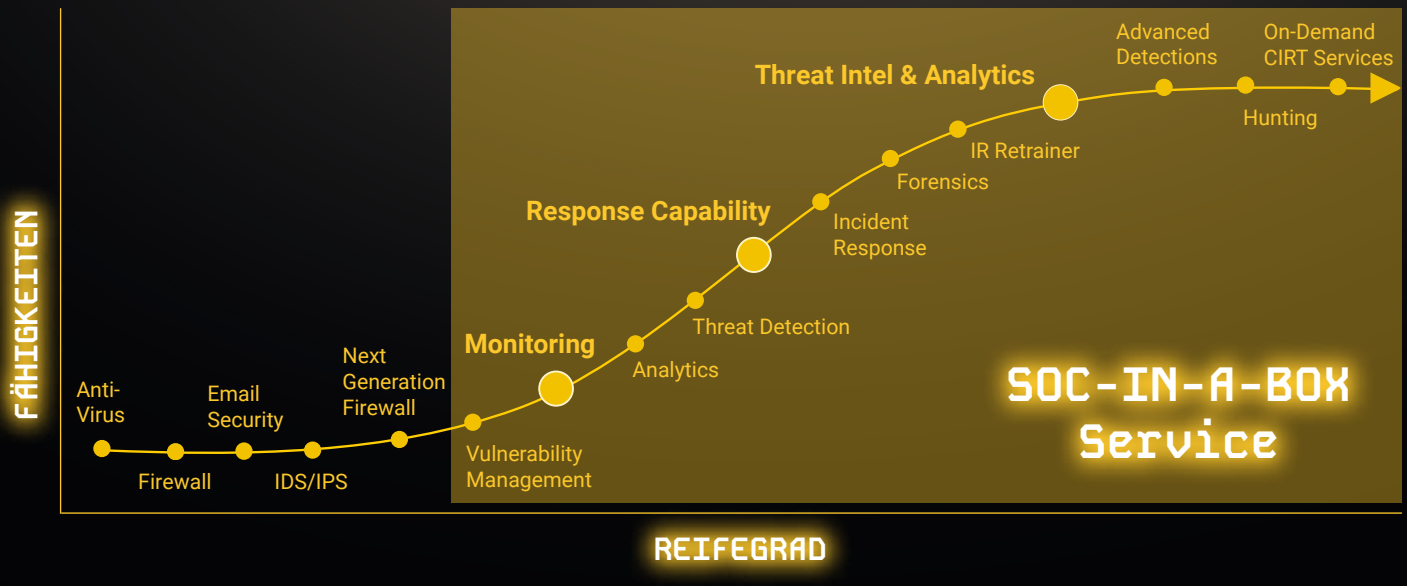
doIT solutions

IT Security findet auch heute noch meist in Silos statt, Daten werden nicht über die Produktränder miteinander korreliert und Angriffe nicht erkannt, weil jedes Silo nur einen kleinen Teil des Angriffs sieht.

Ein vollständiges SOC oder SOC-Service bringt Prozesse, Technologien und Menschen zusammen, um einen umfassenden Blick auf die IT-Infrastruktur zu bekommen.

Genau dies haben wir auf Basis jahrzehntelanger Erfahrung perfektioniert und daraus eine vollständige und modulare Lösung entwickelt. Aus der Praxis – für die Praxis.

Unser SOC-in-a-Box Service begleitet Sie auf ihrem Weg zu einer umfassenden IT-Sicherheit mit hohem Reifegrad. Egal wo wir gemeinsam starten. Wir sind an Ihrer Seite.



Ein Service für alle Fälle

Unser SOC-Service ist Technologie unabhängig, gerne arbeiten wir mit Ihren bestehenden Tools. Wenn nötig können wir helfen, fehlende Technologien zu ergänzen, und als Managed Service Provider bieten wir alle Technologien auch optional verwaltet an.

Vom Silo zum umfassenden Überblick

Für eine erfolgreiche IT-Sicherheitsstrategie müssen Silos aufgebrochen und miteinander verbunden werden. Das beschleunigt die Analysen und ermöglicht es, Angriffe früher zu erkennen. Unser Service zeichnet sich insbesondere dadurch aus, dass er unterschiedliche Technologien integriert und Use Cases technologie- und herstellerübergreifend umsetzt.

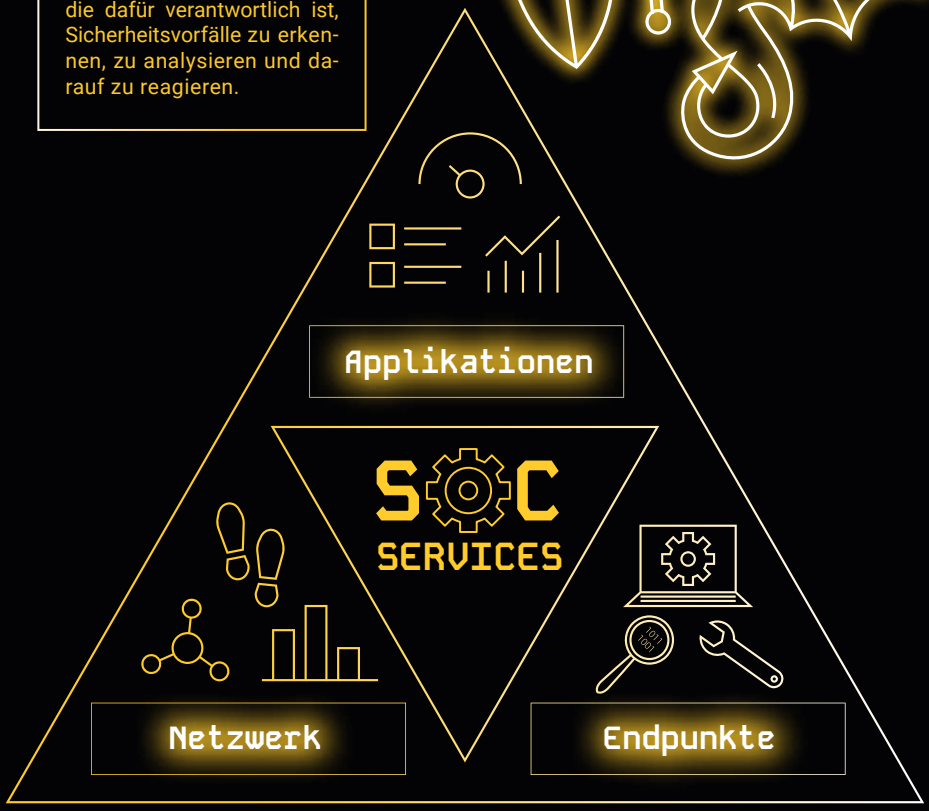
Licht im Dunkeln

Sie haben Fragen zu Ihrer Sicherheit oder einen Vorfall in Ihrer Infrastruktur? Wir lassen Sie auf keinen Fall im Dunkeln stehen. Im Rahmen von inkludierten Workshops besprechen wir Ihre aktuelle Lage, beantworten Fragen und sprechen über Verbesserungen Ihrer Sicherheit.

Durch den regelmäßigen Austausch mit unseren Security Experten wird eine kontinuierliche Weiterentwicklung und Qualitätssicherung sichergestellt.

i

Ein funktionierendes SOC (Security Operations Center) bietet einen effizienten Schutz vor Cyberangriffen. Es ist eine zentrale Einheit innerhalb einer Organisation, die dafür verantwortlich ist, Sicherheitsvorfälle zu erkennen, zu analysieren und darauf zu reagieren.



Anpassbar auf Ihre Bedürf-nisse

Kontakt

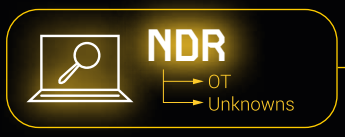
doIT solutions GmbH
Altenhaßlauer Straße 21
63571 Gelnhausen

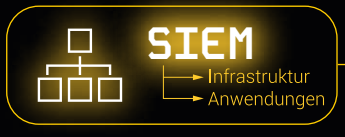
+49 6051 60196 0
info@doit-solutions.de

Support

Sie brauchen uns jetzt?
Wir sind für Sie da.
Gerne auch rund um die Uhr!

+49 6051 60196 80
support@doit-solutions.de





SOC AS A SERVICE		
Gerneral		
SOC Service made in Germany	✓	
Support for On-Prem SOC deployments	✓	
Support for Cloud-based SOC deployments	✓	
Use Cases for IT and OT Infrastructure	✓	
SOC as a Service for customer owned tools (BYO)	✓	
Security Consulting workshops (2/year)	✓	
Additional Consulting workshops	optional	
Standard Reporting	✓	
Custom Reporting	optional	
Response		
Alerting via Service Portal & E-Mail & SMS	✓	
Custom Ticket System integration	optional	
Active Remediation	✓	
Standard Response Workflows	✓	
Custom Reponse Workflows	optional	
10/5 standard SLA (SLA L1: 30min / L2:4h / L3: 4h)	✓	
10/5 extended SLA I (SLA L1: 30min / L2:1h / L3: 2h)	optional	
10/5 extended SLA II (SLA L1: 15min / L2:30min / L3: 1h)	optional	
24/7 standard SLA : Level 1 Response (SLA L1: 30min)	✓	
24/7 extended SLA I : Level 2 + 3 Response (10/5 SLA + 30 min; critical incidents only)	optional	
24/7 extended SLA II : Level 2 + 3 Response (10/5 SLA + 15 min)	optional	
Service Addons		
Indicator Enrichment	✓	
Threat Intelligence Service	optional	
Threat Intelligence Service additional Darkweb Monitoring	optional	
Vulnerability Management Service	optional	
Threat Hunting Service	optional	
Deception Service + Honeypots	optional	
Incident Response Retainer	optional	
Customer Success Manager	optional	
Security Awareness Service	optional	
Attack Surface Management Service	optional	
Audit Access to doIT Case Management System	optional	
TECHNOLOGY EDR		
	Cloud	On-Prem
Min Capacity (Endpoints)	200	500
High Availability	✓	✓
Agent Monitoring	✓	✓
Technology Access	✓	✓
Default Data Retention	31	180
Additional Data Retention	optional	optional
TECHNOLOGY NDR		
	Cloud	On-Prem
Min Capacity (Gbit/s)	1	1
High Availability	✓	✓
Dataflow & Sensor Monitoring	✓	✓
IDS (Intrusion Detection)	✓	✓
Technology Access	✓	✓
Default Data Retention	31	180
Additional Data Retention	optional	optional
TECHNOLOGY SIEM		
	Cloud	On-Prem
Min Capacity (GB/day)	10	50
High Availability	✓	✓
Logmanagment & Data Source Monitoring	✓	✓
Technology Access	✓	✓
Default Data Retention	31	180
Additional Data Retention	optional	optional