SOC-IN-A-BOX

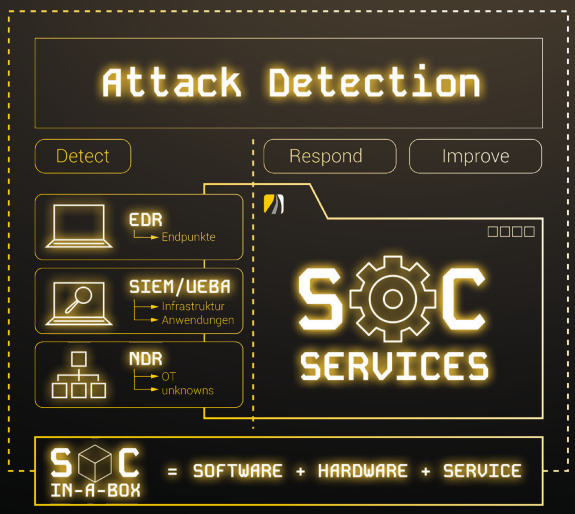
Der einzig wirklich vollständige SOC Service

doIT solutions

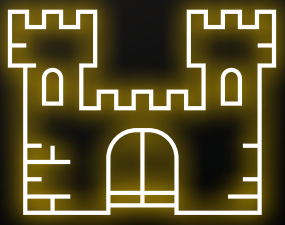
Ein vollständiges SOC bringt Prozesse, Technologien und Menschen zusammen, um die Sicherheit der IT-Infrastruktur zu gewährleisten.

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

Wir machen dort weiter, wo andere aufhören. Während unser SOC-in-a-Box die perfekte Lösung zur Erkennung von Angriffen und Vorfällen darstellt, reagieren unsere SOC Services auf diese Angriffe und Vorfälle. So gehen die erkannten Daten nicht in Tabellen und Logs unter, sondern es wird aktiv mit ihnen gearbeitet, um Ihre IT-Sicherheit zu optimieren und proaktiv weiterzuentwickeln.



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 überwachen, zu erkennen, zu analysieren und darauf zu reagieren.

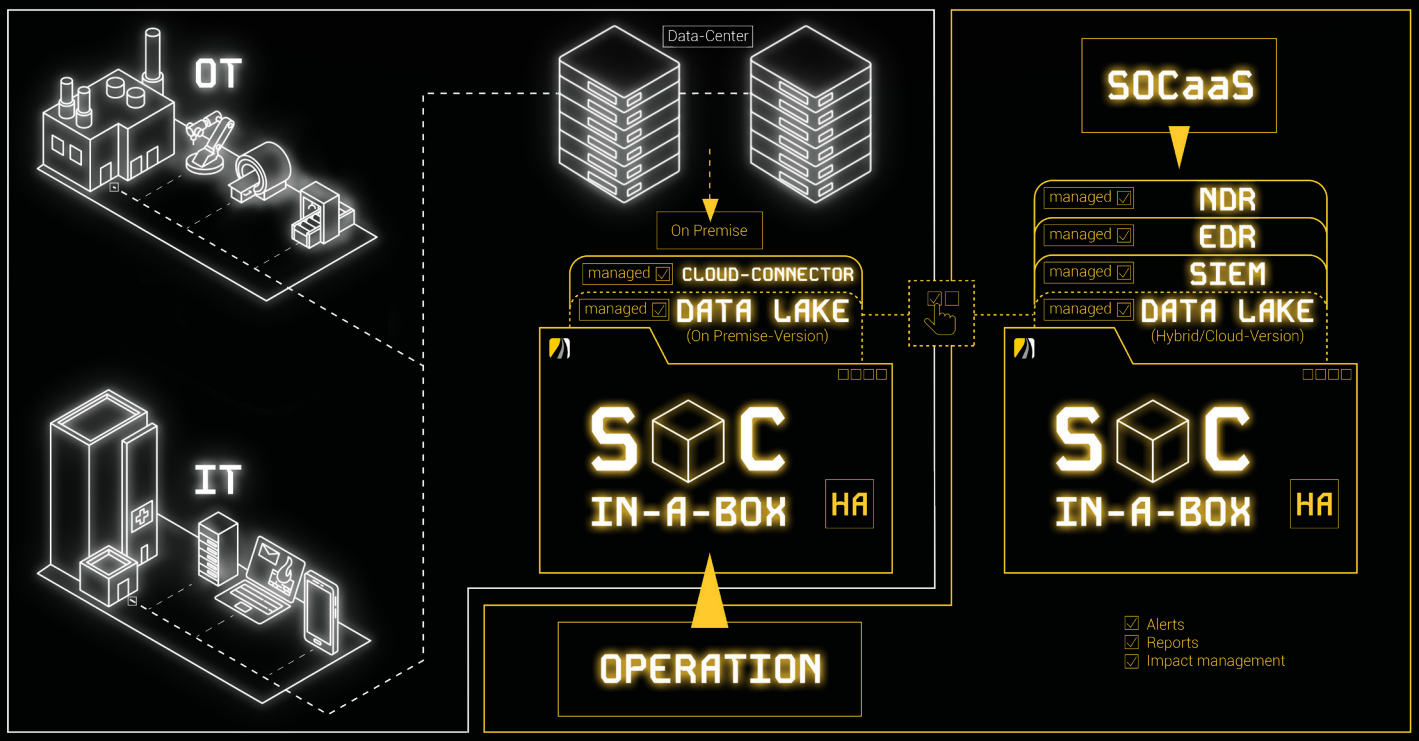


All tools included, but not just a tool

Ohne das richtige Werkzeug ist jeder Experte machtlos. Daher enthält unser Konzept eine Kombination aus verschiedenen Enterprise Software Modulen, um für alle Bedrohungen bestmöglich gerüstet zu sein.

Comes with infrastructure, but not just a server

Bei einem Angriff bleibt ein SOC nur handlungsfähig, wenn es von der IT unabhängig agieren kann. Daher stellt unser SOC-in-a-Box eine eigenständige Infrastruktur dar. Bei Ihnen im Rechenzentrum oder als Cloud Service. Autark, leistungsstark und hochverfügbar.



Fully managed, but not just a service

Unser Credo: Proaktives Handeln

Wir sind in der Lage, im SOC Bedrohungen proaktiv zu erkennen und zu verhindern, bevor sie zu größeren Problemen werden. Dies erfordert ein tiefes Verständnis der Bedrohungslandschaft und der spezifischen Schwachstellen des jeweiligen Systems. Wir unterstützen Sie mit unseren SOC Services aktiv in Ihrem Tagesgeschäft.

Cloud - but not cloud only

Cloud Dienste sind aus einer modernen IT nicht mehr wegzudenken. Daher unterstützt SOC-in-a-Box alle üblichen Cloud Services. Dies ist notwendig, um ein vollständiges Bild zu erhalten und keine blinden Flecken entstehen zu lassen.

Modular and flexible, but not just customized

doIT solutions

Wir bieten Ihnen zwei Versionen unserer Lösung, die perfekt auf Ihre Bedürfnisse zugeschnitten sind. Entweder haben Sie die Option, SOC-in-a-Box als Rundum-sorglos-Paket in der Foundation Version zum besten Preis zu erhalten. Oder aber unsere Enterprise Version – modular, anpassbar und kompromisslos.

EDR
Endpunkte

NDR
OT
Unknowns

SIEM
Infrastruktur
Anwendungen

	FOUNDATION	ENTERPRISE
GENERAL		
Deployment Type: On-prem	YES	YES
Deployment Type: Cloud / Hybrid	YES	YES
Multidatacenter Deployment	NO	optional
Reporting	Standard	Custom
Alerting	Service Portal & E-Mail	Service Portal & E-Mail
Ticket System Integration	NO	YES
SOAR enhanced Security	YES	YES
24/7 Level I + 10/5 Level 2	YES	YES
24/7 Level 2 Erweiterung	optional	optional
Level 1 maximale Reaktionszeit	30 min	30 min
Level 2 maximale Reaktionszeit	4 h	2 h
SOC Service aus Deutschland	YES	YES
Handlungsempfehlung bei Incidents	YES	YES
Security Consulting (on-demand)	48h max. response time	48h max. response time
Included Security Workshops per year	1	2
Additional Security Workshops (on-demand)	YES	YES
Indicator Enrichment	YES	YES
doIT Threat Intelligence Service	optional	optional
Customer Access to SOC instance (SIEM, EDR, NDR)	YES	YES
Access to SOAR Tenant	NO	optional
EDR		
Max Capacity (End points)	1500	4000+
Agent Monitoring	YES	YES
Custom Response Workflows	Standard	Custom
NDR		
Max Capacity (Gbit/s)	3	10+
Dataflow Monitoring	YES	YES
Response Workflows	Standard	Custom
Usecase Deployment	Standard	Custom
IDS (Intrusion/Detection)	YES	YES
SIEM		
Logmanagment	YES	YES
Max Capacity (GB/Tag)	150	400+
Data Source Monitoring	YES	YES
Response Workflows	Standard	Custom
Usecase Deployment	Standard	Custom
Datasources for Usecases	Standard	Custom
INFRASTRUKTUR		
Minimum Log Volume Size	50 GB / Tag	100 GB / Tag
SOCaaS for customer owned tools	NO	YES

Kontakt

doIT solutions GmbH
Altenhaßlauer Str. 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