SOC-IN-A-BOX

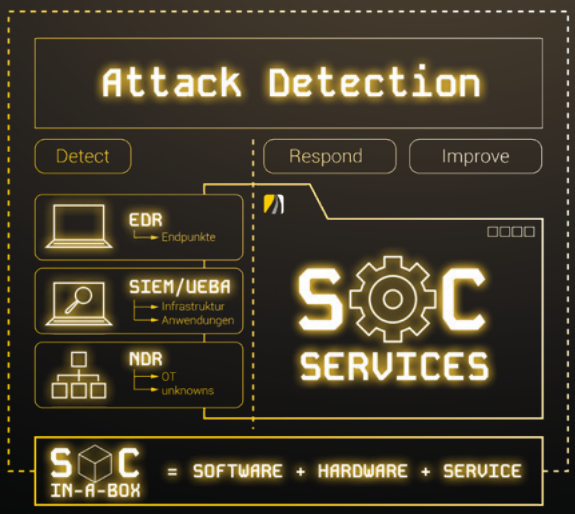
The only truly comprehensive SOC service

doIT solutions

A comprehensive SOC integrates processes, technologies, and people to ensure the security of your IT infrastructure.

Based on decades of experience, we have perfected this approach developing a complete and modular solution – worked out in practice, for use in practice.

We continue where others stop. While our SOC-in-a-Box is the perfect solution for detecting attacks and incidents, our SOC Services respond to these attacks and incidents. Thus, the detected data doesn't get lost in tables and logs, but is actively used to optimize and proactively enhance your IT security.



i

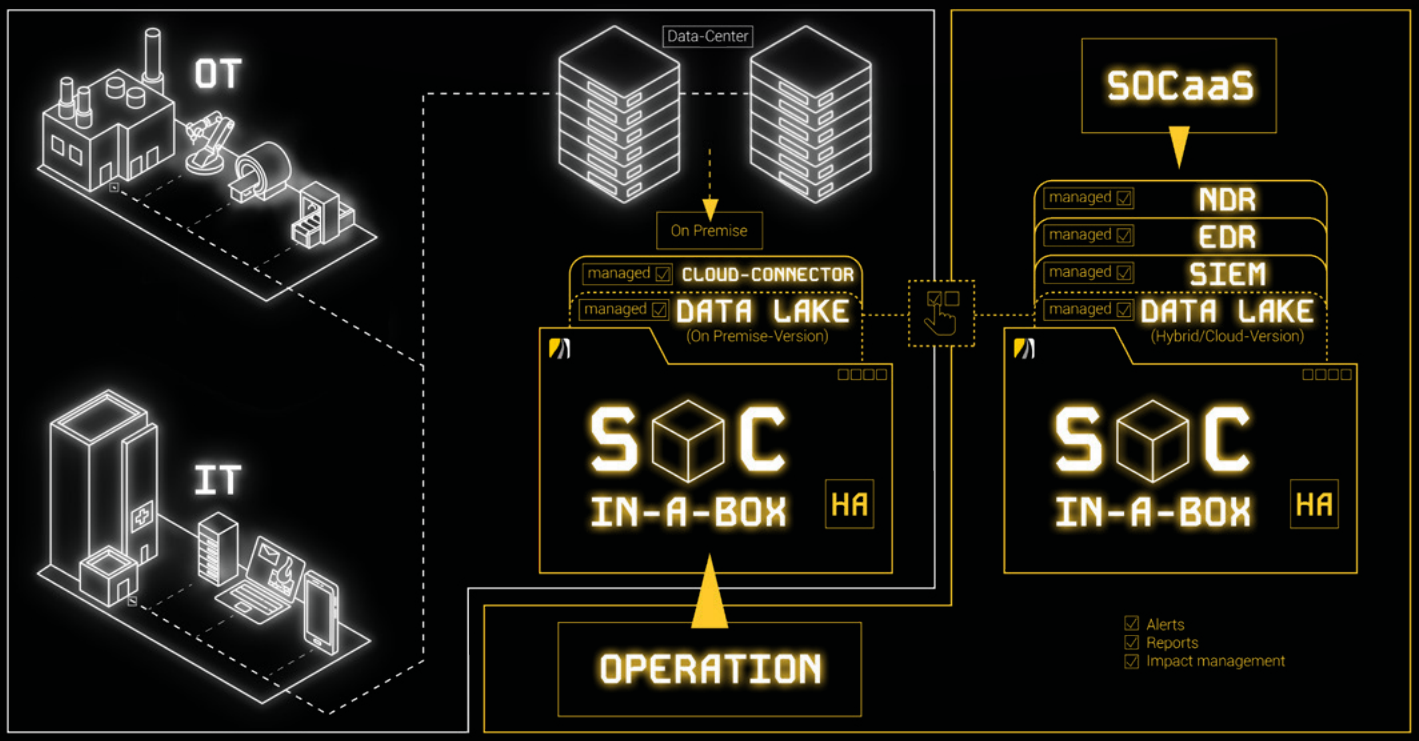
A functioning Security Operations Center (SOC) provides efficient protection against cyberattacks. Responsible for monitoring, detecting, analyzing, and responding to security incidents it is a central unit within an organization.

All tools included, but not just a tool

Without the right tools, even an expert is powerless. Therefore, our concept includes a combination of various enterprise software modules to be well prepared for all kinds of threats.

Comes with infrastructure, but not just a server

When attacked, a SOC must be able to act independently of the IT in order to remain operational. Therefore, our SOC-in-a-Box provides a standalone infrastructure. Whether at your data center or as a cloud service: autonomous, powerful, and highly available.



Fully managed, but not just a service

Our credo: A proactive approach

We are capable of proactively identifying and preventing threats within the SOC before they become major issues. This requires a deep understanding of the threat landscape and the specific vulnerabilities of each system. We actively support you in your daily business with our SOC services.

Cloud - but not cloud only

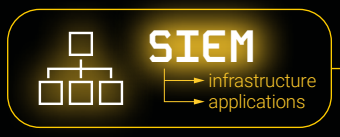
Cloud services are indispensable in modern IT.

Therefore, SOC-in-a-Box supports all common cloud services. This is crucial in order to get an exhaustive image and avoid blind spots.

Modular and flexible, but not just customized

doIT solutions

We offer you two versions of our solution, perfectly tailored to your needs. You can either opt for SOC-in-a-Box as an all-inclusive package in the Foundation version at the best price, or choose our Enterprise version — modular, customizable, and comprehensive.



	CLOUD	ENTERPRISE
SOCAAS		
Deployment Type: On-prem	NO	YES
Hybrid SOC	YES	YES
Multidatacenter Deployment	YES	optional
Reporting	Custom	Custom
Alerting	Service Portal & E-Mail	Service Portal & E-Mail
Custom Ticket System API Integration	YES	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
Regular Security Workshops	YES	YES
Additional Security Consulting (on-demand)	24h max response time	4h max response time
Indicator Enrichment	YES	YES
doIT Threat Intelligence Service	included	optional
Customer Access to SOC instance (SIEM, EDR, NDR)	YES	YES
Access to SOAR Tenant	NO	optional
Use Cases for IT and OT Infrastructure	YES	YES
SOCaaS for customer owned tools (BYO)	YES	YES
TECHNOLOGY EDR		
Max Capacity (Endpoints)	unlimited	10000
Min Capacity (Endpints)	200	500
Agent Monitoring	YES	YES
Response Workflows	Custom	Custom
TECHNOLOGY NDR		
Max Capacity (Gbit/s)	unlimited	10
Min Capacity (Gbit/s)	1	1
Dataflow Monitoring	YES	YES
Response Workflows	Custom	Custom
Usecase Deployment	Standard	Custom
IDS (Intrusion/Detection)	YES	YES
TECHNOLOGY SIEM		
Logmanagment	YES	YES
Max Capacity (GB/day)	unlimited	1000
Min Capacity (GB/day)	10	100
Data Source Monitoring	YES	YES
Response Workflows	Custom	Custom
Usecase Deployment	Standard	Custom
Datasourcetypes for Usecases	Custom	Custom
DATA LAKE		
High Availability	YES	YES
Data retention – default	30 Days + optional	370 Days
Data retention – optional	unlimited	5 Years

Contact

doIT solutions GmbH
Altenhaßlauer Str. 21 | 63571 Gelnhausen

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

Support

In need of our services?
We're there for you, supporting you 24/7.

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