SOC-IN-A-BOX

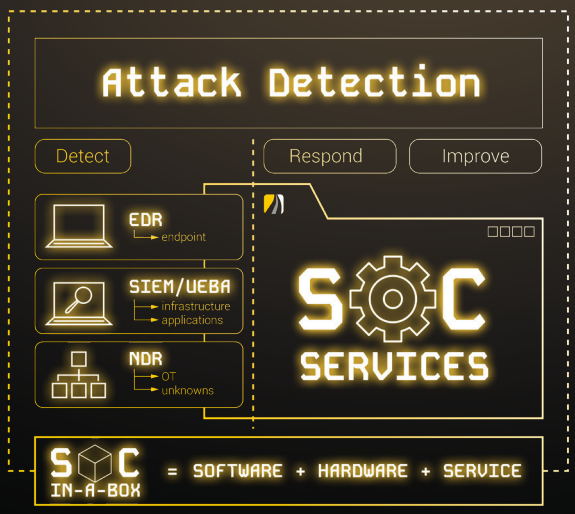
The only truly comprehensive SOC service

doIT solutions

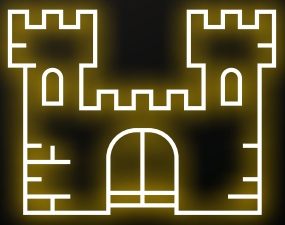
A comprehensive SOC integrates processes, technologies, and people to ensure the security of your IT infrastructure.

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.



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.

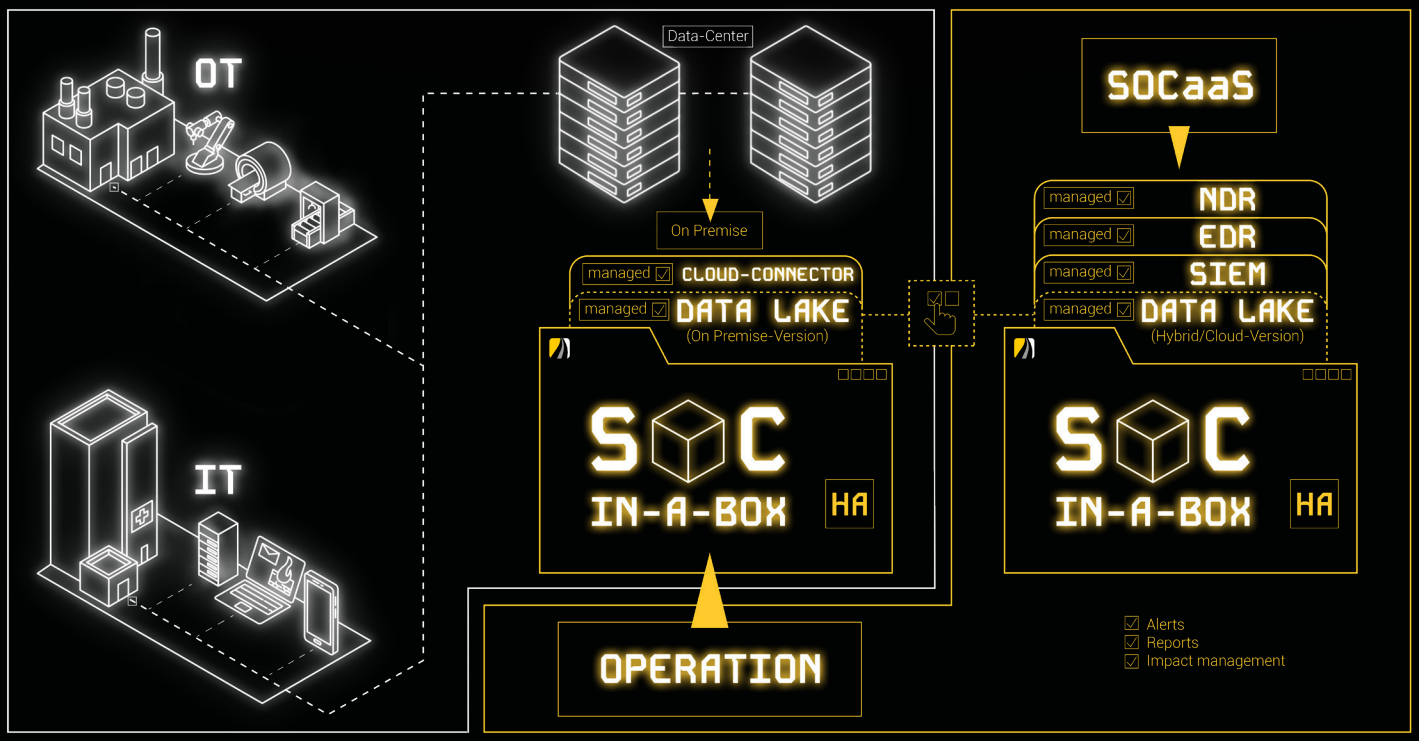


All tools included, but not just a tool

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.

EDR
endpoints

NDR
OT
unknowns

SIEM
infrastructure
applications

	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 add-on	optional	optional
Level 1 maximum response time	30 min.	30 min.
Level 2 maximum response time	4 h	2 h
SOC service from Germany	YES	YES
Actionable recommendations for incidents	YES	YES
Security consulting (on-demand)	48h maximum response time	48h maximum 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		
Log managment	YES	YES
Max capacity (GB/day)	150	400+
Data source monitoring	YES	YES
Response workflows	standard	custom
Usecase deployment	standard	custom
Datasources for usecases	standard	custom
INFRASTRUCTURE		
Minimum log volume size	50 GB / day	100 GB / day
SOCaaS for customer owned tools	NO	YES

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