SOC-IN-A-BOX

doIT solutions

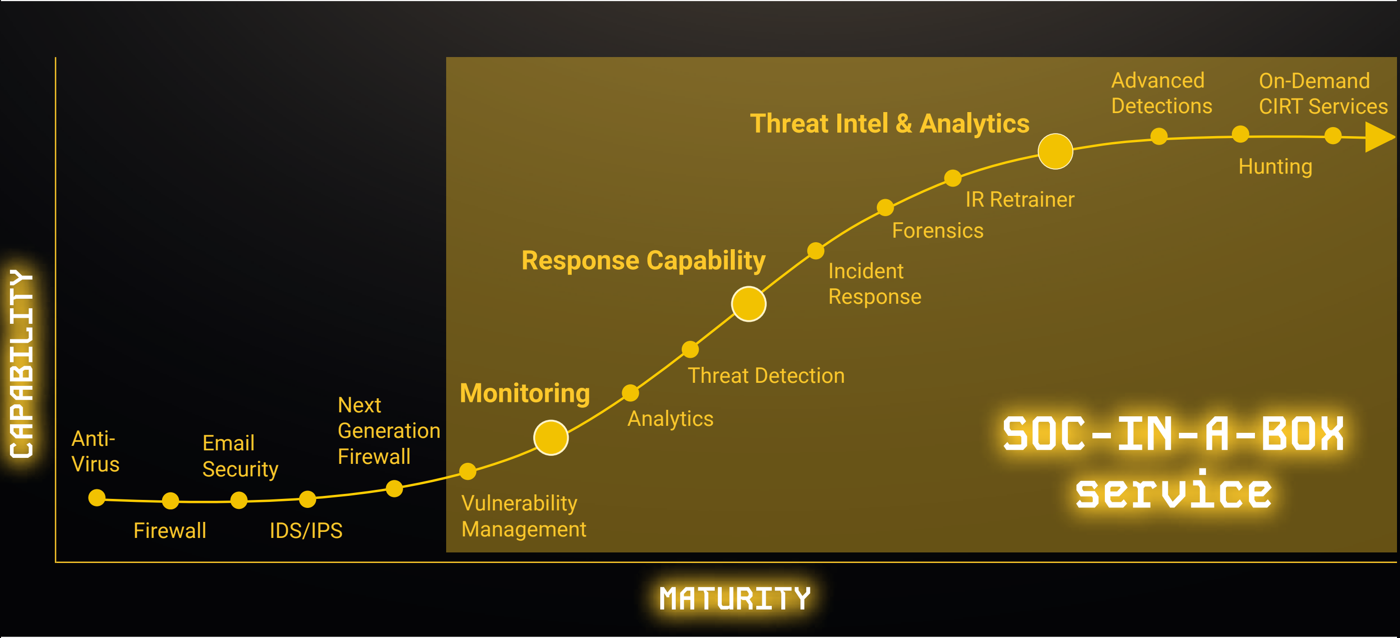
A complete SOC service

IT security still tends to be siloed, with data not being correlated across product boundaries and attacks going undetected because each silo only sees a small part of the attack.

A complete SOC or SOC service brings together processes, technologies and people to provide a comprehensive view of the IT infrastructure.

We have perfected this approach based on decades of experience and developed a complete and modular solution. From practice – for practice.

Our SOC-in-a-Box service accompanies you on your way to comprehensive IT security with a high degree of maturity. No matter where we start together, we are at your side.



A service for all eventualities

Our SOC service is technology-independent, and we are happy to work with your existing tools. If necessary, we can help to supplement missing technologies, and as a managed service provider, we also offer all technologies as an optional managed service.

i

A functioning SOC (Security Operations Centre) provides effective protection against cyber attacks. It is a central unit within an organisation that is responsible for detecting, analysing and responding to security incidents.

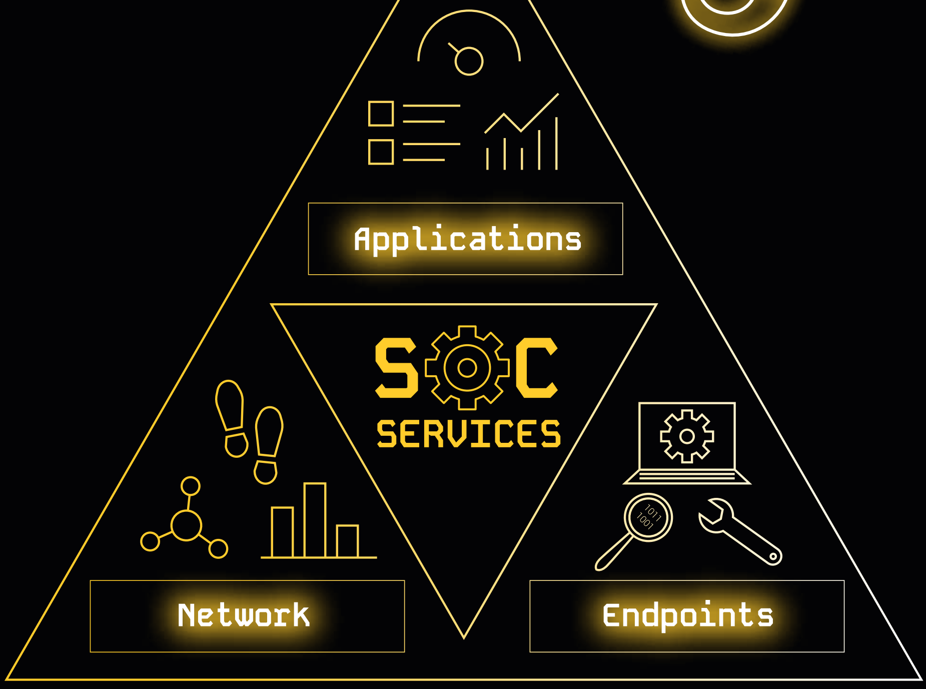
From silo to comprehensive overview

For an IT security strategy to be successful, silos must be broken down and connected with one another. This speeds up analyses and enables attacks to be detected earlier. Our service stands out in particular because it integrates different technologies and implements use cases across technologies and manufacturers.

Light in the darkness

Do you have questions about your security or an incident in your infrastructure? We will not leave you in the dark. As part of the included workshops, we will discuss your current situation, answer questions and talk about improvements to your security.

Regular communication with our security experts ensures continuous development and quality assurance.



Customisable to your needs

Contact

doIT solutions GmbH
Altenhaßlauer Straße 21
63571 Gelnhausen
Germany

+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

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

EDR
Endpoints

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

NDR
OT
Unknowns

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

SIEM
Infrastructure
Applications

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