DTS
Security Operations Center (SOC)

Security Operations Center

Cyber attacks are increasingly sophisticated, multi-layered and can take place at any time. In addition to the sophistication of the threats, a lack of visibility, alert fatigue and, last but not least, insufficient expertise also play a part. The most important advancement in cyber security to meet the increased demands of professional cyber security is the Security Operations Center (SOC).

An SOC consisting of highly qualified IT security experts continuously monitors IT infrastructures and data. Not every company can build such a team and operate it around the clock, however, as it is expensive and time-consuming. The keyword is: “SOC services”.

Our DTS SOC and DTS SOC Services are the ideal solution. We provide you with a central IT security control center for 24/7/365 protection of your IT environment. The DTS SOC fully monitors your IT infrastructure, collects, processes and analyzes data, looks for anomalies and attacks and manages possible countermeasures. We help you on two levels at once: both proactive and preventive detection and response!

- Highly qualified SOC specialists, continuously on duty 24/7/365
- Certified operation in Europe
- Fusion of technology & manpower
- Fast detection and analysis of anomalies and provision of defense recommendations
- Use of central DTS SOC Threat Intelligence
- Visibility in your IT infrastructure
- Compliance through documentation of events & measures
- Vulnerability analysis & continuous optimization
- Regular reporting – as a basis for further security decisions
- German & English-speaking project team, English-speaking analyst teamy

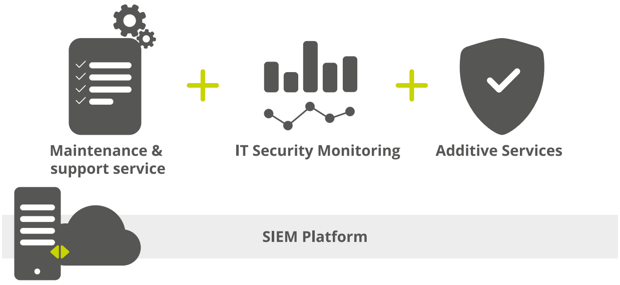
Every company and every IT landscape benefits from an SOC. No matter what form and scale a cyber attack takes, if it is detected too late, massive damage can result. Moreover, attackers always have the opportunity to reuse access details and data, cause damage and launch follow-up attacks at a later date. This makes a combination of cyber security expertise, visibility, diagnosis, analysis and defense all the more important. In addition, all circumstances of the individual IT infrastructure should be taken into account. Technical competence therefore also plays an essential role. Attacks can take place around the clock. For organizations of all sizes, ensuring continuous operation of the SOC to guard against this is a difficult challenge.

The highly qualified team of the DTS SOC is always on duty. It combines automatic detection of attacks, active monitoring by cyber security experts, rapid detection of potential cyber attacks and timely initiation of appropriate measures. In doing so, DTS provides all the benefits of a world-class 24/7/365 SOC without the high cost, complexity and challenges associated with building, properly staffing and operating your own SOC. We relieve the burden on you significantly so that you can concentrate on your core business. We offer the following SOC services: managed security services, active monitoring & analysis of your IT systems, detection and removal of IT vulnerabilities, central security management, alerts & initiation of defensive measures, security assessments, event and log management, compliance, reporting and much more.

DTS SOC Services consist of a variety of services and modules and are far more than the sum of their parts. All modules are provided as a monthly service after an initial planning and implementation phase. Depending on your requirements, we offer several methods of provisioning: on the one hand, IT security monitoring (SIEM-based), on the other via MDR services (Cortex XDR-based).

SOC services based on LogRhythm SIEM

The foundation of SIEM-based SOC services is LogRhythm's XDR stack. Potentially dangerous anomalies are identified, documented and reported centrally via this technology. This gives companies a holistic view of their security posture. In addition, SIEM solutions help to prove conformity with statutory and compliance requirements and to monitor operational events. Building on this system, we offer various service modules to map your requirements in the best possible way. From implementation, deployment as a managed SIEM, full SOC service to additional services such as vulnerability management, DTS has the right service to provide optimal support for you.



Advantages:

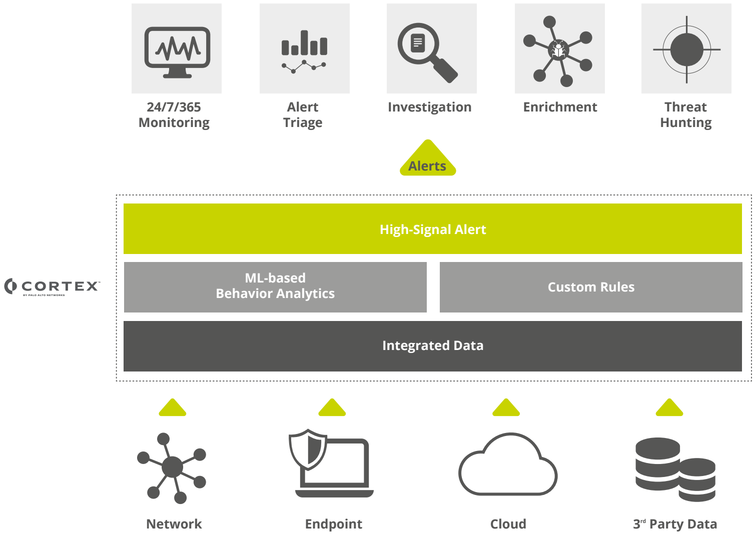
- 24/7/365 service
- Platform management on-premises or in the cloud
- Threat & risk correlation & evaluation of your log files
- Use of DTS best practices & custom use cases
- Detection of security incidents by the certified DTS SOC analysts
- Immediate information on incidents via defined reporting channels, including reports & relevant information, such as incident information, recommendations for remediation and containment
- Monthly jour fixe to discuss & review service
- Reporting, including on threats, coordinated activities, IT security events and recommendations
- Specific reports on regulatory requirements and audits
- Quarterly reports on analysis of the overall threat situation and presentation, including recommendation of counter measures

Use cases from SOC services based on LogRhythm SIEM:

- SIEM platform management
- IT security monitoring
- Compliance management
- Operational information

MDR service based on Cortex XDR

The DTS Managed Detection and Response (MDR) service significantly increases the sophistication of your IT security in terms of threat detection and response. The secret is a combination of highly skilled expertise and first-class technology to detect dynamic threats across your IT ecosystem rapidly. Our service provides active 24/7/365 threat monitoring and defense by trained SOC experts, based on Palo Alto Networks' Cortex XDR platform. We combine automated detection, analysis and response based on state-of-the-art technologies with proactive and continuous threat hunting, data forensics and incident mitigation in one service.



Advantages:

- 24/7/365 managed detection, monitoring of Cortex XDR platform events & actions
- Proactive & continuous threat searches
- Automated technology-based analysis & response
- Root cause analysis, process containment & remediation
- Threat detection based on the information of leading threat intelligence platforms
- Digital forensic investigations
- Health, status & availability system management

Use cases from MDR service based on Cortex XDR:

- Detection & analysis based on endpoint information
- Response to incidents via the Cortex XDR platform
- Detection & analysis based on endpoint, network, cloud & 3rd party information with IT security focus

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de