ANLX
SECURE CLOUD

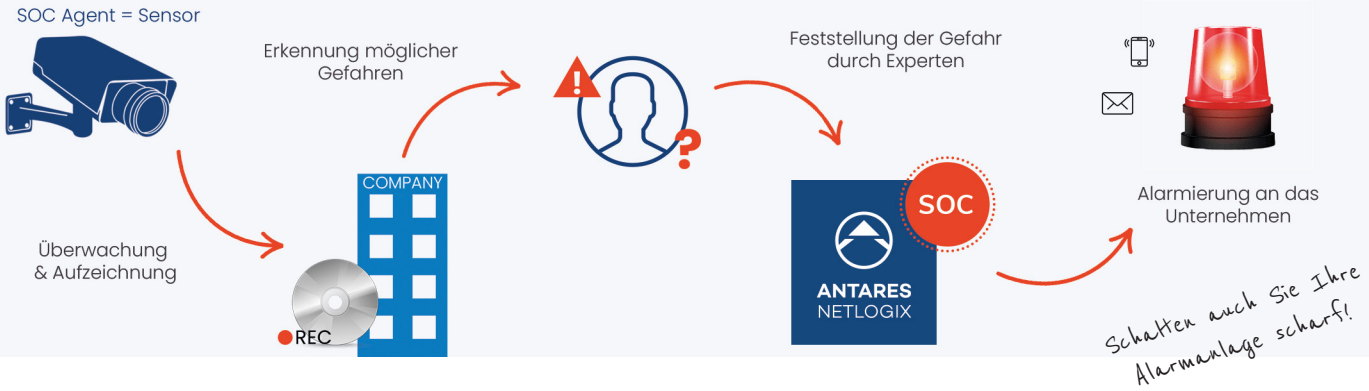
ANTARES NETLOGIX
INDIVIDUAL

ANLX.CLOUD SOC AS A SERVICE

Mit dem ANLX.Cloud SOC as a Service erhalten Sie eine ganzheitliche Verteidigungsstrategie und proaktive 360°-Security-Plattform. Mit unserem Service können Sie also sicher sein, dass Ihre gesamte Netzwerkumgebung von unseren Cybersecurity-Analysten in Hinblick auf neue Bedrohungen kontinuierlich überwacht wird. Reduzieren Sie Ihre Schwachstellen und erhöhen Sie Ihr Sicherheitsniveau mit hochqualifizierten Experten und im Notfall effizient funktionierenden Prozessen. Erkennen Sie Bedrohungen frühzeitig und minimieren Sie somit die Auswirkungen.

UNSER **SOC** IST DIE **ALARMANLAGE** FÜR IHRE IT

Genauso wie ein Firmengebäude mit einer Alarmanlage geschützt ist, wird Ihre IT mit unserem Service gesichert.



Unser SOC Agent überwacht den Normalbetrieb Ihres Unternehmens und sammelt Log-Daten. Bei ungewöhnlichen Aktionen wird nicht sofort ein Alarm ausgelöst, sondern eine Analyse des Problems von unseren Experten durchgeführt. Wird tatsächlich eine Bedrohung festgestellt, erreicht Sie ein Alarm in Form eines Tickets per Mail oder als Anruf. Somit werden Fehlalarme vermieden und die Problemlösung kann sofort eingeleitet werden.

UNSER SERVICE FÜR IHRE **SICHERHEIT**

So ist unser Service aufgebaut* :

1 - LOG MANAGEMENT

- Basisbetrieb der Security Appliance inhouse oder im Antares-Rechenzentrum
- Monatlicher Report & tägliche Status-Mail zu den Security-Alarmen (E-Mail)
- Security Dashboard für den Kunden
- DSGVO-konformes Monitoring
- File Integrity Monitoring
- Windows Enhanced Security Monitoring (PowerShell- & Prozessüberwachung etc.)
- Online-Daten für 14 Tage
- Log-Archiv für bis zu 365 Tage
- Add on: Compliance Reporting

2 - ANLX.CLOUD SOC SERVICE

- basierend auf dem Log Management
- zentrale Aufbereitung der Logdaten in der ANLX. Cloud mittels Anomaly Detection
- täglicher Review und Statusreport durch Antares Cybersecurity-Analysten
- Security Ticketing für Ihre IT

3 - INCIDENT RESPONSE SUPPORT

Unsere SOC-Kunden genießen die volle Unterstützung durch unser **Incident Response Team.** Dabei ist die Incident-Response-Reaktionszeit mit dem SOC-Service gleichgeschaltet.
(Wählen Sie zwischen 9x5- oder 9x7 -Unterstützung.)

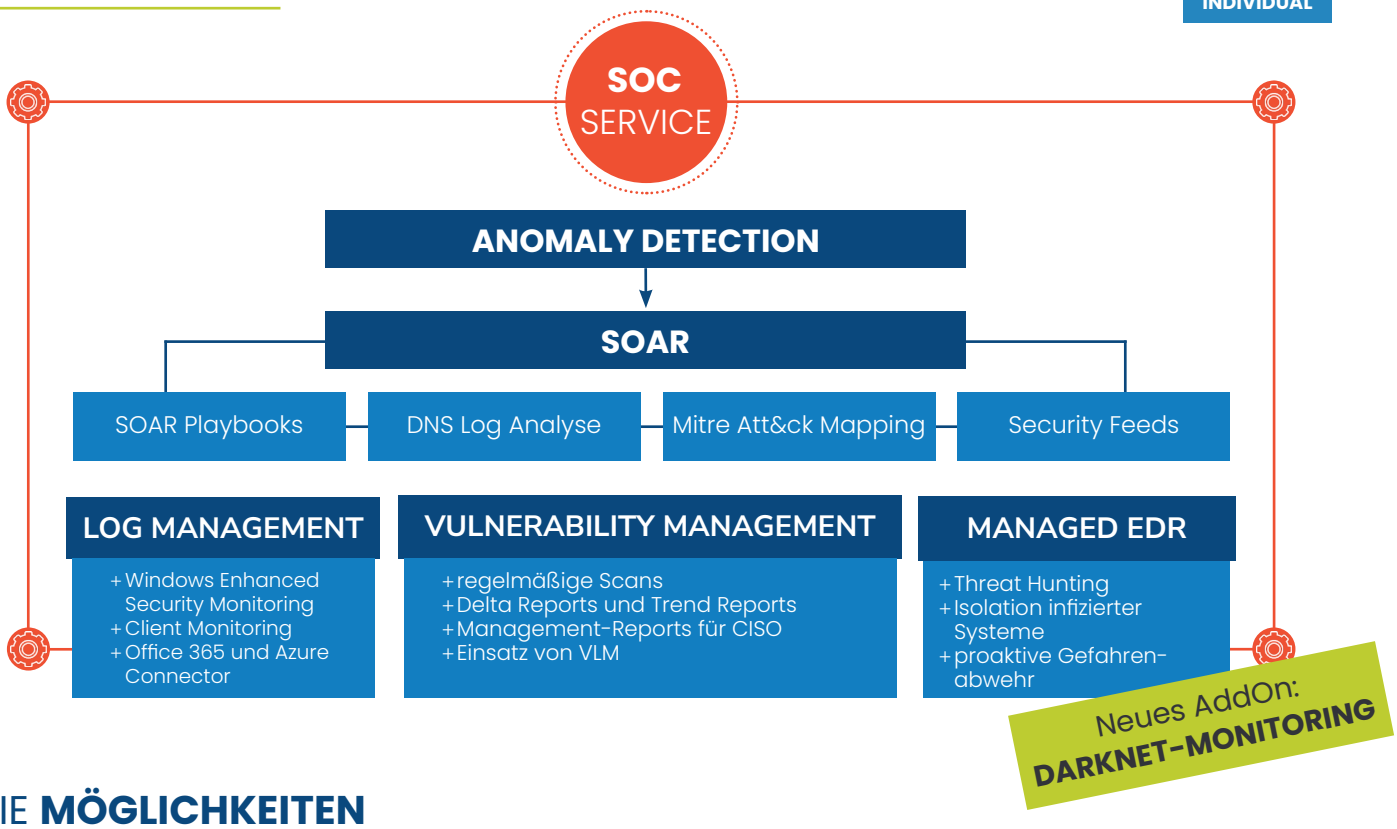
* das Log Management stellt die Basis des Services dar, der Incident Response Support und die ANLX.Cloud SOC Services basieren auf dem Logging.

CLOUD CONNECTOREN: Gerne übernehmen wir für Sie auch den Betrieb folgender Cloud Connectoren: Office 365 Connector, Azure Connector und AWS Connector.

ANTARES NETLOGIX
INDIVIDUAL

DAS STECKT DRIN

ANLX.Cloud SOC as a Service



DIE **MÖGLICHKEITEN**

- **Minimierung der Aktionszeit** von Hackern und anderen Verbrechern
- Verlässliche und individuelle **Alarmierung** im Falle einer erkannten Gefahr
- Einfache und rasche **Rekonstruktion** des Vorfalls bis ins Detail möglich

DAS SAGEN UNSERE **EXPERTEN**

„In unserem SOC kombinieren wir intelligente Technologen, Software und Hardware mit Expertenwissen. So schaffen wir die Grundlage für die bestmögliche Sicherheit unserer Kunden. Wir überwachen die gesamte IT-Infrastruktur beginnend beim Client über den Server bis hin zu den Firewall-Systemen und Infrastrukturkomponenten im Netzwerk. Wir verhindern Vorfälle, indem wir auf nahezu alle Eventualitäten vorbereitet sind und im Notfall die richtigen Entscheidungen treffen."

Bernhard Hochauer (Security Operations Center)

ISO 27001 Information Security Management Services
ISO 27018 Data Protection for Cloud Services

UNSERE **VORTEILE**

Vertrauen Sie auf unsere Expertise

HÖCHSTE SICHERHEIT: Schnellere Schadensminderung mittels proaktiver Überwachung und zeitnaher Alarmierung durch unsere Cybersecurity-Analysten.

RASCH IMPLEMENTIERT: Unser Know-how ermöglicht eine schnelle Integration und Einbindung Ihrer Systeme in unser Security Operations Center.

COMPLIANCE: Alle sicherheitsrelevanten Ereignisse werden von uns dokumentiert und manipulationssicher archiviert. So erfüllen Sie auch Ihre Compliance-Anforderungen.