



ANTARES
NETLOGIX



MANAGED SERVICES

ANLX.CLOUD

MANAGED ENDPOINT DETECTION & RESPONSE

Managed Endpoint Detection and Response (EDR) unterstützt Unternehmen bei der Suche nach Bedrohungen und der Reaktion auf diese, sobald sie entdeckt werden. Unser Service bietet Ihnen sowohl die Tools als auch den Zugang zu unseren Security-Analysten, welche für die **verhaltensbasierte Überwachung von Netzwerken, die Analyse von Vorfällen und die Reaktion auf Sicherheitsvorfälle zuständig sind.**



MANAGED ENDPOINT DETECTION & RESPONSE

KOSTENGÜNSTIG & EINFACH

Ein oft übersehenes Problem, wenn es um Cyber-Sicherheit geht, ist die große Anzahl an Warnungen und Sicherheitsmeldungen, die IT-Teams regelmäßig erhalten. **Viele Vorgänge können nicht ohne Weiteres als bösartig identifiziert und müssen einzeln geprüft werden.** Das kann kleine Security Teams schnell überfordern.



Unsere Security-Analysten übernehmen diese Aufgabe und korrelieren die Bedrohungen, um Angriffe zeitnah zu erkennen.



Es ist heute unmöglich, als österreichisches mittelständisches oder sogar internationales Unternehmen „dagegenzuhalten“. Setzen Sie auf Antares-Netlogix! Wir sind ein vertrauensvoller Partner der immer zur Stelle ist, wenn Not am Mann ist.

IHR VORTEIL

kostengünstig, einfach & sicher

- + Profitieren Sie von der langjährigen Erfahrung unseres Security-Teams im Bereich der Bedrohungsanalysen. Wir haben das Know-how, im Ernstfall einen Rollout innerhalb von Stunden umzusetzen.
- + Unser SOC-Team ist immer up-to-date.
 - + Profitieren Sie von zeitnahen Informationen über aktuelle Bedrohungslagen.
- + Im Krisenfall steht das Team bereit um Sie mit einem erweiterten Incident Response Service (Incident Response Koordinator, SOC EDR Service etc.) zu unterstützen.

ALLE LEISTUNGEN IM DETAIL

Managed Endpoint Detection & Response

Bleiben Sie auf der sicheren Seite und nutzen Sie unseren Service und unser umfangreiches Know-how. Wir bieten Ihnen umfassende Leistungen für Ihr Incident Response Management.

Leistungsumfang:

- + Zentrales Hosting der EDR-Lösung innerhalb der EU
- + Zentrale Administration
- + Betrieb und Konfiguration der EDR-Agents auf den Kundensystemen
- + Regeländerungen
- + Anpassung der Sicherheits-Profile
- + „Killen“ von Prozessen
- + Entfernen von Persistenz-Mechanismen
- + Malops lokalisieren und terminieren
- + Threat Hunting

Abdeckung aller Tätigkeiten des Incident Response Managements. Zum Beispiel:

- + Annahme und Bearbeitung von Incidents und Service Requests über das Antares Operations Center Portal
- + Isolierung infizierter Systeme
- + Im Krisenfall zusätzliche Erreichbarkeit via Telefon

Abdeckung aller Tätigkeiten des Problem-Managements. Zum Beispiel:

- + Analyse und Behebung reproduzierbarer Device-Probleme
- + Fehleranalyse gemeinsam mit den zuständigen Kundenadministratoren

Optional:
Integration in das Antares SOC



SICHERHEIT & DATENSCHUTZ

Der Betrieb unserer Services erfolgt ausschließlich innerhalb der EU. Somit sind unsere Services nur österreichischem und EU-Recht unterworfen.

Unsere Mitarbeiter werden regelmäßigen **Sicherheitsüberprüfungen** unterzogen, haben **Vertraulichkeits-erklärungen** zu unterfertigen und werden jährlich in die entsprechenden **Sicherheitsstandards** unterwiesen (PCI DSS, DSGVO, ISO27001, Grundschriftbuch, etc.).

Seitens Antares-Netlogix werden **keine Daten** (die über das administrativ Unumgängliche hinausgehen, wie z. B. Lizenzdaten) an inländische oder ausländische Behörden bzw. Unternehmen **weitergegeben**.

Wir garantieren Ihnen ein **Höchstmaß an Sicherheit!**



„Wir leben aktive Sicherheit in jeder Sekunde.
Das bedeutet vor allem eines:
Zero Trust – Vertraue keinem Netzwerk!“

Bernhard Hochauer
Cyber Security Analyst | Antares-Netlogix

Managed Endpoint Detection & Response

Interesse?

Kontaktieren Sie uns einfach per E-Mail office@netlogix.at oder wenden Sie sich direkt an Ihren persönlichen Ansprechpartner.



Antares-Netlogix Netzwerkberatung GmbH

Feldstraße 13, A-3300 Amstetten

T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at