HERR INFORMATIK

MANAGED NETWORK DETECTION & RESPONSE (NDR)

TIEFE NETZWERKSICHTBARKEIT & AKTIVE BEDROHUNGSERKENNUNG

Herr Informatik GmbH | Klosterzelgstrasse 1a | 5210 Windisch
+41 56 460 00 60 | info@herr-informatik.ch



Wenn Angreifer die klassische Abwehr überwinden, wir erkennen sie im Netzwerk

Selbst moderne Firewalls oder Endpoint-Sicherheitslösungen können Attacken nicht immer stoppen. Wenn ein Angreifer den Perimeter überwindet, bleibt oft unbemerkt, wie sich die Bedrohung lateral im Netzwerk ausbreitet. Unser Managed NDR schliesst diese Lücke, analysiert den gesamten Netzwerkverkehr proaktiv und reagiert bei Anomalien.

Was ist Managed NDR?

Network Detection & Response (NDR) überwacht kontinuierlich den Netzwerkverkehr sowohl zwischen Netzsegmenten als auch inbound/outbound und nutzt fortschrittliche Analysen, um untypisches Verhalten und versteckte Bedrohungen zu erkennen.

Beim Managed NDR übernehmen wir: Deployment der Sensoren, Betrieb, Alarmierung, Analyse und, falls vereinbart, Unterstützung bei Reaktionen.

Typische Herausforderungen, die wir adressieren

- Verborgene Bedrohungen im Netzwerk selbst wenn der Perimeter übersprungen wird
- Sichtbarkeit von nicht verwalteten Geräten z. B. IoT, OT, Kameras, Drucker
- Erkennung komplexer Angriffsmuster z.B. laterale Bewegung, Datenexfiltration, Command-&-Control
- Alarmflut & Priorisierung zu viele Warnungen, zu wenig Kontext
- Fehlende forensische Tiefe Rückverfolgung von Angriffswegen und Zusammenhängen

Unser Service-Angebot im Detail

- **Netzwerk-Sensor-Deployment & Architektur:** Wir platzieren passive Sensoren, um den Netzwerkverkehr zu erfassen, ohne den regulären Traffic zu stören.
- **Traffic-Analyse & Verhaltensbasierte Erkennung:** Einsatz von Machine Learning, Verhaltensprofilen und Anomalie-Analysen, um Abweichungen gegenüber dem normalen Netzwerkverhalten aufzuspüren.
- **Alarmierung & Analyse-Workflow:** Verdächtige Ereignisse werden priorisiert und mit Kontextdaten (z. B. Gerät, Zeit, betroffene Subnetze) angereichert, um rasche Entscheidungen zu ermöglichen.
- **Incident Response Unterstützung:** Bei bestätigten Vorfällen liefern wir Analysen, Vorschläge zur Eindämmung oder arbeiten mit Ihnen direkt an Reaktionen (z. B. Segment-Isolierung, Netzwerkfilter, Forensik).
- **Spezialexpertise für IoT / OT / Industrie-Netzwerke:** In Produktionsumgebungen, Automatisierung oder sensiblen Netzsegmenten, in denen klassische Agenten nicht eingesetzt werden können, setzen wir NDR-Methoden ein, um Sicherheit zu gewährleisten.

Möchtest du mehr über unsere Dienstleistungen erfahren?



Josip Corkovic
Co-CEO
Head of Dev & Security
+41 56 460 00 60
info@herr-informatik.ch

Technische Eckpunkte & Funktionsweise

- **Datenquelle & Sensoren:** Passive Überwachung über SPAN-Ports, TAPs oder virtuelle Spiegelports ohne Einfluss auf den Echtzeit-Betrieb.
- **Netzwerkverhalten & Baselines:** Das System lernt ein „normales" Kommunikationsverhalten und identifiziert Abweichungen (z. B. ungewöhnlicher Datenverkehr, neue Verbindungen).
- **Erkennungsmethoden:** Kombination aus signaturbasierter Erkennung, Anomalieanalyse und Verhaltensmodellierung (Machine Learning).
- **Automatisierte oder manuelle Reaktion:** Je nach Policy automatische Filterung/blockierende Massnahmen oder manuelle Intervention durch Sicherheitsteams.
- **Forensik & Threat Hunting:** Speicherung relevanter Netzwerkdaten (z. B. Metadaten, Pakete), um nachträglich in Angriffspfade einzutauchen.

Mehrwert mit Managed NDR von HERR INFORMATIK

- Früherkennung & Eindämmung, Bedrohungen erkennen, bevor sie grossen Schaden anrichten
- Netzwerkweite Transparenz, Sicht auf alle Geräte, auch solche ohne Agenten
- Weniger Lärm, mehr Relevanz, Priorisierung und Kontext helfen beim Umgang mit Alarmen
- Schutz kritischer Infrastrukturen, speziell für IoT, OT, Produktionsnetzwerke
- Ausgelagerte Expertise & Ressourcen, du erhältst Spezialwissen, ohne eigenes Team aufbauen zu müssen

Warum HERR INFORMATIK?

- Erfahrung mit Netzwerk-Sicherheitsarchitekturen und modernem Monitoring
- Integration mit bestehenden Sicherheitslösungen (Firewalls, SIEM, EDR etc.)
- Flexibler, regionaler Partner mit direktem Support
- Fokus auf industrielle, heterogene und anspruchsvolle Netzwerke