MEDIALINE

IT Security

Managed Attack Defense Sensor (MADS)

Angriffserkennung in Echtzeit: automatisiert, proaktiv, managed.

Wir überwachen Ihren Netzwerkverkehr rund um die Uhr, erkennen Angriffsmuster in Echtzeit und stoppen Bedrohungen, bevor Schaden entsteht. Der Sensor analysiert passiv, arbeitet ohne Infrastruktur-Umbau und ist ab Tag 1 einsatzbereit.

Wie schnell erkennen und stoppen Sie Angriffe?

Wissen Sie, ob kompromittierte Systeme in Ihrem Netzwerk bereits mit Angreifern kommunizieren? Fehlen Ihrem Security-Team die Ressourcen, um Bedrohungen rund um die Uhr zu erkennen und zu bewerten? Und wie schnell können Sie heute auf einen aktiven Angriff reagieren?

Bedrohungen erkennen, bewerten, stoppen

Wir analysieren Ihren gesamten Netzwerkverkehr mit über 100.000 Erkennungsregeln, alarmieren Sie innerhalb weniger Minuten und blockieren auf Wunsch Angreifer automatisiert an der Firewall, bei planbaren monatlichen Kosten.

Erkannte Angriffsindikatoren

Der Managed Attack Defense Sensor erkennt unter anderem:

- Command-and-Control-Kommunikation
- Exploit-Kits und Botnets
- Exploits bekannter Schwachstellen (CVE)
- DDoS und DoS Angriffe
- SCADA/OT-Protokollverletzungen
- Credential Phishing
- Kryptominer
- Netzwerk-Anomalien
- Spyware-Downloads

Echtzeit-Angriffserkennung

Verdächtige Aktivitäten und Ransomware-Kommunikation erkennen, bevor Schaden entsteht.

Managed Detection & Response

Unsere Experten betreiben, optimieren und analysieren. Ihr Team wird entlastet.

Automatische Blockierung

Erkannte Angreifer-IPs werden in Echtzeit an der Firewall gesperrt (Optimal-Paket).

Unsere Leistungen

	Basis	Business	Optimal
Appliance (optional Redundanz)	Single	Single / HA-Cluster	Single / HA-Cluster
Automatisierte Alarmierung 24/7	✓	✓	✓
Monatlicher Report	✓	✓	✓
Alarmnachverfolgungen pro Monat	5	10	unlimitiert
Firewall-Deflektor (aktive Blockierung)	✗	✗	✓

Basis: Single Appliance

Ein Sensor analysiert Ihren gesamten Netzwerkverkehr passiv über Port-Mirror oder TAP, ohne Eingriff in den Datenfluss. Über 100.000 Erkennungsregeln in mehr als 40 Kategorien arbeiten ab Tag 1. Sie erhalten Transparenz, Echtzeit-Alarmierung und die Analyse von fünf Vorfällen pro Monat. Ideal für den schnellen Einstieg oder kleinere Umgebungen.

Business: Hochverfügbarer Sensor

Redundante Sensoren garantieren unterbrechungsfreie Erkennung. Regeln, Tuning und Reporting werden über ein gemeinsames Management synchronisiert. Zusätzlich erhalten Sie zehn inkludierte Alarm-Analysen pro Monat. Die richtige Wahl für produktive Netzwerke mit hohen Anforderungen an Ausfallsicherheit und Compliance.

Optimal: Firewall-Deflektor mit aktiver Blockierung

Der Deflektor erweitert die Sensorarchitektur um automatisierte Gegenmaßnahmen: Erkannte Angreifer-IPs, C2-Verbindungen oder kompromittierte Hosts werden in Echtzeit über dynamische Firewall-Regeln blockiert. Der Datenverkehr fließt weiterhin durch Ihre Firewall, nicht durch den Sensor. So entsteht ein vollwertiges IPS-Szenario ohne Inline-Risiko. Inklusive Alarmierungs-Flatrate.

Warum Managed Security?

Cyberbedrohungen entwickeln sich schneller als interne Teams reagieren können. Ihr Mehrwert: Entlastung Ihrer Security-Ressourcen, permanente Angriffserkennung durch Experten und planbare Kosten statt ungeplanter Incident-Aufwände.

Lassen Sie uns gemeinsam prüfen, wie gut Ihr Netzwerk heute geschützt ist. Wir begleiten Sie vom Erstgespräch über die Integration bis zum laufenden Betrieb, mit klaren Reaktionszeiten, spezialisierten Analysten und planbaren Kosten. Sprechen Sie uns an unter **sales@medialine.ag**.

Stand: 04/2026