MDR Service – Leistungsbeschreibung

Unser MDR Service (Managed Detection & Response) bietet umfassenden Schutz durch kontinuierliche Bedrohungserkennung, Analyse und schnelle Reaktion auf Sicherheitsvorfälle. Dabei stehen zwei Servicestufen zur Auswahl – Essential und Advanced – abgestimmt auf unterschiedliche Schutzbedarfe.

Hinweis: MDR-Kunden können das Incident Response Service-Paket zu einem stark vergünstigten Preis als optionalen Zusatzbaustein buchen. Dies ermöglicht bei Bedarf eine koordinierte Vor-Ort-Reaktion und vertiefte Analyse durch unser Experten-Team – ohne hohe Zusatzkosten.

🔹 MDR Essential – Grundschutz

Zielgruppe: Unternehmen mit mittlerem Schutzbedarf, die auf Erkennung und Reaktion während der Geschäftszeiten setzen.

Leistung	Details
Monitoring & Detection	24/7 automatisiertes Monitoring, manuelle Analystensichtung 10x5
Verfügbarkeit	Montag–Freitag, 08:00–18:00 Uhr (werktags)
Reaktionszeit	Remote-Reaktion innerhalb von 4 Stunden (während Servicezeiten)
Incident Response Paket	Optional zubuchbar (vergünstigt für MDR-Kunden)
Reporting	Monatlicher Überblick über erkannte Bedrohungen & Maßnahmen
Kommunikationskanäle	Ticket-System + E-Mail
Threat Intelligence	Basis-Feeds inkludiert

🔸 MDR Advanced – Vollschutz

Zielgruppe: Unternehmen mit kritischen Systemen oder hohem Schutzbedarf, die durchgängig Überwachung und sofortige Reaktion benötigen.

Leistung	Details
Monitoring & Detection	24/7 kontinuierlich mit aktiver, manueller Threat Hunting
Verfügbarkeit	Rund um die Uhr, 24x7
Reaktionszeit	Remote-Reaktion innerhalb von 1 Stunde, jederzeit

Incident Response Paket	Optional zubuchbar (vergünstigt für MDR-Kunden)
Reporting	Monatlicher Security-Report + Ad-hoc-Berichte bei kritischen Vorfällen
Kommunikationskanäle	Ticket, E-Mail, Telefon-Hotline + dedizierter Ansprechpartner
Threat Intelligence	Erweiterte Feeds + Kontexterkennung
Jährlicher Review	Security-Workshop & Lessons Learned inklusive

✅ Gemeinsame Vorteile

• Vertraglich garantierte SLAs

• Monatlich planbare Fixpreise

• Vorrangige Behandlung sicherheitsrelevanter Vorfälle

• Optional erweiterbar: Forensik, Awareness-Trainings, Playbooks, SIEM-Integration