ENGINSIGHT
UNITE. SECURE. PROTECT.

ENGINSIGHT MDR

SERVICE-BESCHREIBUNG

Für Enginsight Managed Detection & Response

enginsight.com

V.1.0.0

Inhaltsverzeichnis

Executive Summary

Cyberangriffe haben den Mittelstand erreicht – als organisierte, mehrstufige und industrialisierte Bedrohung, die sich nicht mehr mit einzelnen Sicherheitswerkzeugen abwehren lässt. Was fehlt, ist ein Sicherheitsbetrieb: Menschen, Prozesse und Technologie, die rund um die Uhr zusammenwirken. Genau das liefert Enginsight MDR.

Was Enginsight MDR leistet

Wir überwachen Ihre IT-Landschaft 24 Stunden am Tag, validieren jeden sicherheitsrelevanten Alarm durch einen Analysten und greifen aktiv ein, bevor aus einem Vorfall ein Schaden wird. Der Service folgt drei klaren Prioritäten:

- **Unterbrechen** kompromittierter Systeme innerhalb von Minuten
- **Aufklären** der Ursache und des Ausmaßes innerhalb von Stunden
- **Verbessern** Ihres Schutzniveaus mit jedem Vorfall, kontinuierlich

Was Sie erhalten

- **24/7-SOC** mit deutschsprachigen Analysten
- **15-Minuten-First-Response** rund um die Uhr 24/7
- **Eigenentwickelte Security Operations Plattform** – Attack Surface, Detection, Reaction – Made in Germany
- **Ready to Detect MDR-Pakete**, sowie individuelle Services aus unserem SOC nach Bedarf
- **Compliance-tauglich** für NIS2, DORA, ISO 27001, TISAX und B3S
- **Onboarding ab 4 Wochen** je nach Umgebungsgröße

Was Sie von uns erwarten dürfen

Datenhoheit als Designprinzip. Telemetrie und Logs bleiben in Ihrer Umgebung – on-premises bei Ihnen oder in einem deutschen Rechenzentrum. Keine Cloud außerhalb Europas, keine CLOUD-Act-Risiken.

Plattform und Service aus einer Hand. Wir entwickeln die Sicherheitsplattform selbst und betreiben den Service mit unserem Premium-Partner. Eine Roadmap, ein Vertragspartner, klare Verantwortung.

Bekenntnis zu europäischen Sicherheitsstandards. Enginsight hat sich schriftlich zu den Anforderungen der ENISA verpflichtet, der EU-Agentur für Cybersicherheit. Plattform-Entwicklung und Service-Design folgen ihren Leitlinien – Ihre Compliance-Bemühungen und unsere Plattform-Roadmap arbeiten in dieselbe Richtung (s. Kapitel 10.6).

Mittelstands-Nähe. Persönliche Ansprechpartner, pragmatische Onboarding-Prozesse, Verträge ohne unverständliche Konzern-Klauseln. Wir sind so groß, wie wir sein müssen, um zuverlässig zu liefern – und so nah, wie der Mittelstand es braucht.

1. Die Bedrohungslage – warum Sie das jetzt betrifft

Cyberangriffe sind kein abstraktes Risiko mehr, das Großkonzerne und Behörden trifft. Sie sind im Mittelstand angekommen – und sie haben sich verändert. Wer Sicherheitsstrategien aus den letzten fünf Jahren weiterführt, schützt sich gegen die falschen Angreifer.

1.1 Wie Angreifer heute arbeiten

Drei Entwicklungen prägen die aktuelle Bedrohungslage – und keine davon lässt sich mit einer einzelnen Sicherheitslösung beantworten.

Angriffe sind industrialisiert. Hinter den meisten Vorfällen stehen heute keine Einzeltäter, sondern organisierte Gruppen. Ransomware-as-a-Service-Modelle haben den Zugang zu Angriffswerkzeugen demokratisiert: Wer früher technisches Spezialwissen brauchte, mietet heute fertige Infrastruktur und teilt das Lösegeld mit dem Plattformbetreiber. Das Ergebnis: deutlich mehr Angriffe, deutlich tiefere Reichweite.

Angriffe skalieren nach unten. Ziele sind nicht mehr nur die Konzerne mit hohem Lösegeld-Potenzial. Automatisierung und KI machen es wirtschaftlich, auch mittelständische Unternehmen anzugreifen – Hersteller, Dienstleister, Kommunen, Krankenhäuser, Steuerberater. Die Annahme „uns trifft das nicht, wir sind zu klein" stimmt nicht mehr.

Angriffe verlaufen mehrstufig. Ein moderner Angriff beginnt selten mit verschlüsselten Festplatten am ersten Tag. Typisch ist ein Schleichweg: Initialer Zugang über kompromittierte Anmeldedaten oder eine ungepatchte Schwachstelle, dann Tage oder Wochen unauffälliges Erkunden des Netzwerks, Privilegien-Eskalation, Exfiltration sensibler Daten – und erst danach die eigentliche Erpressung. Wer den Angriff erst beim Lösegeldschreiben bemerkt, hat alle Frühphasen verpasst.

1.2 Warum klassische Schutzmaßnahmen Lücken lassen

Die meisten mittelständischen Unternehmen haben in den vergangenen Jahren in Cybersicherheit investiert: Firewalls, Antivirus-Lösungen, oft auch ein SIEM oder eine Endpoint-Protection-Plattform. Diese Werkzeuge sind notwendig – aber sie haben prinzipielle Grenzen.

Sie erkennen, ohne zu reagieren. Eine Firewall protokolliert verdächtigen Datenverkehr. Ein Antivirus blockiert bekannte Schadsoftware. Ein SIEM sammelt Logs und korreliert Ereignisse. Was alle drei nicht leisten: die Bewertung, ob ein konkreter Vorfall in Ihrer Umgebung gerade gefährlich ist – und die Entscheidung, was dagegen zu tun ist. Diese Bewertung erfordert einen Menschen, der die Daten liest.

Sie produzieren mehr Alarme, als ein Inhouse-Team verarbeiten kann. Eine durchschnittliche Sicherheitsplattform meldet hunderte Ereignisse pro Tag. Die meisten sind unkritisch, einige sind verdächtig, wenige sind echte Angriffe. Wer diese Differenzierung im laufenden IT-Betrieb leisten muss, übersieht das Kritische zwischen dem Rauschen – nicht aus Nachlässigkeit, sondern weil die Aufgabe rund-um-die-Uhr-Aufmerksamkeit verlangt.

Sie schützen nicht nachts und am Wochenende. Angreifer wissen, wann IT-Abteilungen schlafen. Die Mehrheit erfolgreicher Angriffe wird außerhalb der Bürozeiten ausgelöst – Freitagabend, Samstagnacht, an Feiertagen. Ein Sicherheitskonzept, das nur werktags von 8 bis 17 Uhr verteidigt, schützt nur ein Drittel der Zeit.

Sie verkürzen die Reaktionszeit nicht. Zwischen dem Erstzugriff eines Angreifers und der Auslösung des eigentlichen Schadens liegen oft Stunden, manchmal Tage. Diese Zeitspanne ist Ihre Chance –

aber nur, wenn jemand die Erkennung in Reaktion übersetzt. Ohne diesen Zwischenschritt verstreicht das Zeitfenster ungenutzt.

1.3 Was die Regulierung fordert

Die regulatorische Landschaft hat auf die veränderte Bedrohungslage reagiert. Mehrere Rahmenwerke fordern heute explizit, was vor wenigen Jahren noch als Best Practice galt.

NIS2 verpflichtet einen erweiterten Kreis mittelständischer Unternehmen zu kontinuierlichem Sicherheitsmonitoring, definierten Reaktionsprozessen und kurzen Meldefristen bei Vorfällen. Wer nicht selbst über die Kapazitäten verfügt, muss diese nachweislich beschaffen – Untätigkeit ist keine Option mehr und kann persönliche Haftung der Geschäftsführung auslösen.

DORA stellt für den Finanzsektor und seine IKT-Dienstleister vergleichbare Anforderungen. ISO 27001 verlangt in der aktuellen Fassung ausdrücklich Detection-, Response- und Reporting-Fähigkeiten. TISAX erwartet von Automotive-Zulieferern denselben Standard. B3S definiert ihn für Krankenhäuser und KRITIS-Betreiber.

Allen gemeinsam: Sie verlangen nicht „eine Firewall" oder „einen Virenscanner". Sie verlangen einen Sicherheitsbetrieb – eine Organisation, die Bedrohungen erkennt, bewertet, behandelt und dokumentiert. Wer diesen Betrieb nicht aufbauen will oder kann, braucht einen Partner, der ihn leistet.

2. Warum Erkennung allein nicht reicht

Kapitel 1 hat die Lücke beschrieben. Diese Lücke entsteht nicht, weil Unternehmen zu wenig in Sicherheit investiert hätten – sie entsteht, weil Erkennung und Reaktion unterschiedliche Disziplinen sind. Dieses Kapitel erklärt, was Managed Detection & Response leistet, und worauf bei der Wahl eines MDR-Anbieters wirklich ankommt.

2.1 Was Managed Detection & Response leistet

Managed Detection & Response (MDR) ist die Antwort auf die Erkenntnis, dass Cybersicherheit ein Betriebsmodell braucht: Menschen, Prozesse und Technologie im Zusammenspiel, rund um die Uhr. Ein MDR-Dienstleister übernimmt die Aufgabe, die im eigenen Haus selten leistbar ist: die kontinuierliche Bewertung von Sicherheitsereignissen und die Einleitung von Gegenmaßnahmen, bevor aus einem Vorfall ein Schaden wird.

Ein guter MDR-Service folgt drei klaren Prioritäten:

Unterbrechen – im Bereich von Minuten und Stunden. Sobald ein Angriff erkannt wird, geht es nicht um Aufklärung, sondern um Tempo. Kompromittierte Systeme werden isoliert, verdächtige Sitzungen unterbrochen, die Ausbreitung verlangsamt. Der Angreifer verliert die Initiative.

Aufklären – im Bereich von Stunden bis Tagen. Ist der Angriff unterbrochen, beginnt die Analyse: Eintrittspunkt, betroffene Systeme, Ausmaß. Das Ergebnis ist die Grundlage für die Bereinigung und stellt sicher, dass kein erneuter Einbruch über denselben Weg möglich ist.

Verbessern – im Bereich von Tagen bis Wochen. Jeder Vorfall liefert Erkenntnisse über Schwachstellen, Konfigurationen und Prozesse. Diese Erkenntnisse werden zurück in das Sicherheitskonzept geführt – damit das Schutzniveau mit jedem Vorfall steigt.

2.2 Worauf es bei der Wahl eines MDR-Anbieters ankommt

Der MDR-Markt wächst. Internationale Anbieter werben mit globaler Reichweite, KI-Versprechen und beeindruckenden Marketing-Auftritten. Was im Ernstfall zählt, sind andere Kriterien. Die folgenden sieben Fragen entscheiden, ob ein MDR-Service Ihrem Unternehmen wirklich hilft – oder ob Sie im Sicherheitsfall feststellen, dass entscheidende Voraussetzungen fehlen.

Wo liegen Ihre Daten? Viele MDR-Anbieter zentralisieren Telemetrie, Logs und Vorfall-Informationen in Cloud-Plattformen außerhalb Europas – häufig unter der Jurisdiktion des US-amerikanischen CLOUD Act. Dort gespeicherte Daten können ausländischen Behörden offengelegt werden, ohne dass Ihr Unternehmen davon erfährt. Wer sensible Geschäftsdaten, Kundendaten oder Compliance-relevante Informationen schützt, braucht europäische Datenhaltung – idealerweise on-premises in der eigenen Umgebung.

Wer beantwortet Ihren Anruf um drei Uhr morgens? Im Ernstfall zählen Sprache, Erreichbarkeit und Kontextwissen. Ein Analyst, der in einer anderen Zeitzone sitzt und Ihre Umgebung nicht kennt, verzögert die Reaktion – auch dann, wenn das SLA formal eingehalten wird. Deutschsprachige Analysten mit Verständnis für die DACH-IT-Landschaft sind keine Komfort-Funktion, sondern eine harte Anforderung an die Reaktionsqualität.

Wie tief geht die Erkennung – und kann sie wachsen? Ein MDR-Service, der nur Endpunkte überwacht, sieht nur einen Teil eines mehrstufigen Angriffs. Wer heute mit Endpoint-Schutz startet, sollte den Service später um Identitäten, Cloud-Dienste und beliebige weitere Datenquellen erweitern können – ohne den Anbieter zu wechseln und ohne in eine neue Plattform zu investieren.

Gehört Plattform und Service aus einer Hand? Manche MDR-Anbieter betreiben fremde Sicherheitsplattformen. Das bedeutet: zwei Lieferanten, zwei Roadmaps, zwei Vertragsverhältnisse. Funktionsänderungen am Security-Produkt liegen außerhalb der Kontrolle des MDR-Dienstleisters. Wer Plattform und Betrieb aus einer Hand bezieht, bekommt einen abgestimmten Service – mit klaren Verantwortlichkeiten und einer Roadmap, die zur Service-Strategie passt.

Bleibt der Service hersteller-unabhängig? Ein MDR-Service, der ausschließlich auf einer fremden Endpoint-Plattform aufsetzt, bindet Sie an deren Lizenzmodell und deren Roadmap. Eine eigene Plattform, die zugleich offen für die Anbindung Ihrer bestehenden Sicherheitstools ist, verbindet das Beste aus beiden Welten: tiefe Integration der eigenen Komponenten und Flexibilität bei der Einbindung dessen, was bei Ihnen bereits im Einsatz ist.

Wer trägt die Verantwortung – rechtlich und operativ? Bei vielen internationalen Anbietern liegen Vertragspartner, Datenverarbeiter und SOC-Standort in verschiedenen Ländern. Im Streitfall ist unklar, welcher Gerichtsstand gilt, welches Datenschutzrecht greift und welche Behörde zuständig ist. Ein deutscher Vertragspartner mit europäischem SOC schafft hier Klarheit – und ist im NIS2- und DORA-Kontext der einfachere Compliance-Nachweis.

Wie nah ist der Anbieter an Ihrer Größe? Mittelständische Unternehmen brauchen einen Anbieter, der Mittelstand versteht: pragmatische Onboarding-Prozesse, persönliche Ansprechpartner, Verträge ohne Konzern-Klauseln. Ein Anbieter, dessen Standardkunde ein Fortune-500-Konzern ist, behandelt mittelständische Vorfälle nicht mit derselben Aufmerksamkeit – egal was im SLA steht.

Wie Enginsight diese sieben Anforderungen erfüllt, beschreibt das folgende Kapitel.

2.3 Wie Enginsight diese Anforderungen erfüllt

Was Sie brauchen	Was Enginsight liefert
Daten in Europa	Plattform on-premises in Ihrer Umgebung oder in einem deutschen Rechenzentrum. Telemetrie und Logs verlassen Ihre Hoheit nicht.
Erreichbarkeit im Ernstfall	24/7-SOC mit deutschsprachigen Analysten. First Response innerhalb von 15 Minuten für jeden Alarm, unabhängig vom Schweregrad.
Skalierbare Erkennungstiefe	Zwei MDR-Pakete von der Endpoint- bis zur Identity-Überwachung – erweiterbar um individuelle Datenquellen und Use Cases, ohne Plattform-Migration.
Plattform und Service aus einer Hand	Eigenentwickelte Plattform, eigener Service. Eine Roadmap, ein Ansprechpartner, ein Vertrag.
Hersteller-Unabhängigkeit	Eigene Plattform mit offenen Schnittstellen für Ihre bestehenden Sicherheitstools – Microsoft 365, Active Directory, Firewalls, Endpunktschutz Dritter.
Klare Verantwortung	Deutscher Vertragspartner, deutsches Recht, Service-Erbringung in Deutschland und der Schweiz. NIS2- und DORA-konformer Nachweis.
Mittelstands-Nähe	Made in Germany, gewachsen mit dem deutschen Mittelstand. Persönliche Ansprechpartner, pragmatische Onboarding-Prozesse, Vertragslaufzeiten ab 12 Monaten.

3. Enginsight MDR auf einen Blick

Cyberangriffe lassen sich nicht mehr verhindern – aber sie lassen sich rechtzeitig erkennen, unterbrechen und aufarbeiten. Genau das leistet Enginsight MDR: Wir überwachen Ihre IT-Landschaft rund um die Uhr, validieren jeden Alarm und greifen aktiv ein, bevor aus einem Vorfall ein Schaden wird.

3.1 Wer was beiträgt

Enginsight MDR funktioniert als Zusammenspiel aus drei Komponenten. Keine davon ersetzt die anderen:

Layout-Hinweis: Diese Tabelle soll im finalen Dokument als Drei-Spalten-Schaubild dargestellt werden – analog zur Folie „Enginsight MDR – Partnership". Bis zur grafischen Umsetzung folgt die tabellarische Darstellung.

Enginsight-SOC-Team	Enginsight-Technologie	Ihr IT-Team
24/7-Überwachung Ihrer Umgebung durch deutschsprachige Analysten	**Pulsar Agent** für Endpunkt-Erkennung mit Schwachstellen-Scan, IDS, File Integrity Monitoring und APT-Erkennung	Gesamtverantwortung für die Sicherheit Ihres Unternehmens

Validierung, Triage und Klassifizierung jedes Alarms	**SIEM mit Data Lake** für Korrelation aller sicherheitsrelevanten Ereignisse	Unternehmens- und Umgebungswissen, das kein Externer haben kann
Aktive Eindämmungsmaßnahmen im Ernstfall	**Pulsar Shield** für aktive Eindämmung – Quarantäne kompromittierter Hosts und Blockierung verdächtiger Verbindungen	Definition der eigenen Schutzbedürfnisse und Eskalationswege
Konkrete Handlungsempfehlungen und Threat Hunting	**Workflows & SOAR** zur automatisierten Ausführung der vom SOC-Team definierten Reaktionsregeln	Umsetzung von Anpassungs- und Bereinigungsmaßnahmen in der eigenen Infrastruktur
Service Review (bei MDR Endpoint + Identity, halbjährlich)	**Souveräne Plattform** – Made in Germany, on-premises bei Ihnen oder in deutschem Rechenzentrum	Ansprechpartner während Sicherheitsvorfällen

3.2 Was Enginsight MDR von anderen Lösungen unterscheidet

Made in Germany, betrieben in Europa. Die Enginsight-Plattform ist deutsche Eigenentwicklung, EU-patentiert und ohne Abhängigkeit vom CLOUD Act. Ihre Daten verlassen Ihre Umgebung nicht – die Plattform läuft on-premises bei Ihnen oder in einem deutschen Rechenzentrum.

Souveräne Datenhaltung als Designprinzip. Andere MDR-Anbieter sammeln Telemetrie und Log-Daten in zentralen Cloud-Plattformen außerhalb Europas. Bei Enginsight bleiben die Daten in Ihrer Hoheit – die Plattform läuft on-premises bei Ihnen oder in einem deutschen Rechenzentrum. Das SOC-Team greift über eine kontrollierte API-Verbindung zu, ohne dass Ihre Logs Ihre Umgebung verlassen müssen.

24/7 mit deutschsprachigen Analysten. Im Ernstfall sprechen Sie mit jemandem, der Ihre Umgebung versteht – fachlich und sprachlich. Keine Tickets in Englisch, keine Eskalationen über drei Zeitzonen.

Reaktion in Minuten, nicht in Stunden. Jeder Alarm wird innerhalb von 15 Minuten durch einen SOC-Analysten gesehen und eingeordnet, rund um die Uhr – auch nachts, am Wochenende und an Feiertagen. Im Ernstfall steht zusätzlich ein 24×7-Bereitschaftsteam für Incident Response abrufbar zur Verfügung: Tier-2- und Tier-3-Spezialisten, die einen schweren Vorfall sofort übernehmen können, ohne dass Sie erst nach einem Dienstleister suchen müssen. Die Bereitschaft ist im Servicepreis enthalten – die tatsächliche Bearbeitung wird nach Aufwand abgerechnet.

Compliance-tauglich. Enginsight MDR erfüllt die Anforderungen führender Rahmenwerke an Detection, Response und Reporting – als zentraler Baustein Ihrer Compliance-Strategie für NIS2, DORA, ISO 27001, TISAX und B3S.

4. Service-Pakete

Enginsight MDR ist als modulares Angebot aufgebaut: Sie wählen eines von zwei MDR-Paketen für den Schutz Ihrer Endpunkte und Identitäten – und können diesen Schutz bei Bedarf um die Anbindung weiterer individueller Datenquellen erweitern. Allen Paketen gemeinsam sind die zugesicherten Reaktionszeiten, das 24×7-Monitoring sowie die 24×7-Bereitschaft eines Incident-Response-Teams.

4.1 Die zwei MDR-Pakete im Vergleich

	MDR Endpoint	MDR Endpoint + Identity
Erkennung		
Endpoint-Überwachung (Clients und Server) via Pulsar Agent	✓	✓
Identity-Überwachung (Microsoft AD und Entra ID)	–	✓
Anzahl InfoGuard EDR Threat Detection Use Cases	ca. 50	ca. 150
Kontinuierliche Use-Case-Optimierung auf Basis aktueller Gegebenheiten durch das SOC	✓	✓
Automatisierte Host-Isolation für definierte kritische Use Cases	✓	✓
Reaktion (First Response, 24×7)		
Critical / High / Normal / Low	15 Min	15 Min
Reaktion (Extended Investigation)		
Critical (24×7)	60 Min	60 Min
High (10×5)	4 Stunden	4 Stunden
Normal (10×5)	8 Stunden	8 Stunden
Low (10×5)	24 Stunden	24 Stunden
Service-Leistungen		
Standardisierte Incident-Benachrichtigung inkl. Handlungsempfehlung	✓	✓
Monatlicher Standard-Report (Alarmvolumen, Kritikalität, Trends)	✓	✓
Service Review Meeting	–	halbjährlich
24×7-Bereitschaft eines Incident-Response-Teams	✓	✓

4.2 Welches Paket passt zu Ihnen?

MDR Endpoint überwacht Ihre Endpunkte – Clients und Server – durch den Pulsar Agent. Endpunkte sind das wichtigste Frühwarnsystem: Hier zeigen sich verdächtige Prozesse, ungewöhnliche Aktivitätsmuster und Persistenz-Mechanismen. Der Service umfasst rund 50 ausgewählte InfoGuard Threat Detection Use Cases, die typische Endpoint-Angriffs- und Ransomware-Muster früh sichtbar machen. Für definierte kritische Use Cases wird der betroffene Host automatisch isoliert – noch bevor sich ein Angreifer seitwärts ausbreiten kann.

> *Geeignet für Sie, wenn: Ihre IT primär aus Office-Arbeitsplätzen und Servern besteht, Sie Microsoft 365 nicht zentral nutzen oder Identitätsschutz bereits anderweitig abgedeckt ist und Sie einen klar abgegrenzten Einstieg in die 24×7-Überwachung suchen.*

MDR Endpoint + Identity erweitert die Endpunkt-Überwachung um Ihre Identitätssysteme. Microsoft Entra ID und Active Directory sind zentrale Ziele moderner Angriffe – kompromittierte Zugangsdaten und Privilegien-Eskalationen lassen sich auf Endpunkten allein oft nicht erkennen. Der Service umfasst rund 150 Use Cases über Endpunkte und Identitäten hinweg und beinhaltet die kontinuierliche Weiterentwicklung des Use-Case-Sets durch das SOC: Erkenntnisse aus realen Vorfällen, neue Threat Intelligence und veränderte Angriffstaktiken fließen laufend in die Erkennung Ihrer Umgebung ein.

> *Geeignet für Sie, wenn: Sie Anmelde-, Berechtigungs- und Privilegien-Anomalien systematisch in die Überwachung einbeziehen möchten.*

Use Cases statt Detection Rules – warum die Zahl nicht alles ist

Manche Anbieter werben mit tausenden Detection Rules. Das klingt nach Sicherheit – ist aber das Gegenteil. Detection Rules sind isolierte Trigger: Jede Regel feuert, wenn ihre Bedingung erfüllt ist, unabhängig vom Kontext. Das Ergebnis: Tausende Alarme pro Tag, von denen die meisten irrelevant sind. Wer alle ernst nimmt, ertrinkt. Wer keinen ernst nimmt, übersieht den entscheidenden.

Wir arbeiten anders. Ein Use Case ist eine durchdachte, mit Ihnen abgestimmte Erkennung einer vollständigen Angriffstaktik – über mehrere Phasen, mit Kontext und mit definierter Reaktion. Hinter jedem Use Case stehen mehrere Detection Rules, korrelative Logik und eine klare Antwort auf die Frage: Was bedeutet das für genau Ihre Umgebung? Use Cases werden in Workshops mit Ihnen erarbeitet, kontinuierlich verfeinert und gemeinsam priorisiert.

Das Ergebnis ist nicht weniger Sicherheit, sondern mehr: Sie werden nur dann informiert, wenn wirklich etwas Kritisches passiert. Kein Alarm-Spam. Keine Müdigkeit durch False Positives. Sondern gezielte, qualifizierte Information – genau dann, wenn sie zählt.

4.3 Optionale Erweiterung: Individuelle Use Cases

Individuelle Use Cases sind jederzeit als Erweiterung zu beiden MDR-Paketen buchbar. Die Standard-Pakete decken Endpunkte und Identitäten ab. Individuelle Anforderungen erweitern den Service um die Anbindung beliebiger weiterer Datenquellen, für die individuelle Use Cases entwickelt werden.

Was Sie damit anbinden können

- **Netzwerk-Komponenten:** Firewalls, Web-Proxies, VPN-Gateways
- **Cloud-Plattformen:** Microsoft Azure, AWS, Google Cloud (jenseits der Identity-Komponenten)
- **Sicherheitstools:** Antivirus-Lösungen, EDR-Drittanbieter, E-Mail-Security

- **Geschäftsanwendungen:** ERP-, CRM- und Branchensysteme mit eigener Log-Schnittstelle
- **OT- und IoT-Systeme:** Industriesteuerungen, Produktions- und Gebäudeleittechnik
- **Custom-Quellen:** Eigene Anwendungen und individuelle Log-Formate

Anders als bei den Standard-MDR-Paketen, die auf einem vordefinierten Use-Case-Katalog basieren, erfordern individuelle Datenquellen auch individuelle Use Cases. Diese werden in gemeinsamen Workshops mit Ihrem Team entwickelt und im SIEM implementiert.

1. Individuelle Use Cases werden gemeinsam in Workshops entwickelt
2. Anbindung und Normalisierung der vereinbarten Datenquellen
3. Inbetriebnahme, Tuning und Pflege der individuellen Use Cases im laufenden Betrieb

> *Geeignet für Sie, wenn: Sie als KRITIS-Unternehmen oder unter NIS2-, DORA- oder TISAX-Auflagen einen Nachweis vollständiger Erkennung benötigen, eine heterogene IT- und OT-Landschaft betreiben oder regulatorische Anforderungen wie ISO 27001 oder B3S ein zentrales Security Monitoring vorgeben.*

Abrechnung: Jeder Use Case wird nach tatsächlichem Aufwand abgerechnet. Was als ein Use Case bzw. eine Datenquelle zählt, wird im Onboarding gemeinsam mit Ihnen festgelegt. Das individuelle Angebot erstellen wir auf Basis Ihrer geplanten Datenquellen und der Komplexität der Anbindung. Dies kann direkt im Onboarding erfolgen oder zu jedem beliebigen Zeitpunkt der Zusammenarbeit.

4.4 Was in beiden MDR-Paketen enthalten ist

Unabhängig vom gewählten Paket erhalten Sie:

- **24×7-Überwachung** durch das SOC-Team mit deutschsprachigen Analysten
- **First Response innerhalb von 15 Minuten** bei jedem Alarm, unabhängig von der Kritikalitätsstufe
- **Validierung der Alarme** durch das SOC-Team
- **Aktive Eindämmungsmaßnahmen** – etwa die Quarantäne kompromittierter Endpunkte
- **Konkrete Handlungsempfehlungen** nach Vorfällen, sodass Sie die Risiken verstehen und beheben können.
- **Service Review** mit Vorfall-Übersicht, SLA-Report und Optimierungsempfehlungen – halbjährlich bei MDR Endpoint + Identity
- **Kontinuierliche Optimierung der Erkennungsregeln** auf Basis von Vorfällen in Ihrer Umgebung
- **24×7-Bereitschaft eines Incident-Response-Teams** – Tier-2- und Tier-3-Analysten stehen im Ernstfall rund um die Uhr abrufbar zur Verfügung (siehe Kapitel 6.1)

4.5 Servicezeiten und Vertragslaufzeit

Servicezeiten. Critical-Vorfälle werden 24×7 bearbeitet – das gesamte Jahr, an allen Tagen, zu jeder Uhrzeit. Die First Response von 15 Minuten gilt für alle Kritikalitätsstufen rund um die Uhr. Die vertiefte Bearbeitung der Schweregrade High, Normal und Low läuft 10×5 (Montag bis Freitag, 8:00 bis 18:00 Uhr) – mit den entsprechenden Reaktionszeiten aus der Tabelle in 4.1, sowie SLA-Beschreibungen unter 9.

Vertragslaufzeit und Konditionen. Die kommerziellen Rahmenbedingungen – Vertragslaufzeit, Kündigungsfrist, Rechnungsstellung und Angebotsgültigkeit, sind in Kapitel 12 (Geschäftsbedingungen) zusammengefasst.

5. Was im Service enthalten ist

Enginsight MDR ist das Zusammenspiel aus drei Bestandteilen: einer Sicherheitsplattform, die Daten erhebt und Reaktionen ausführt, einem SOC-Team, das diese Daten interpretiert und entscheidet, und definierten Prozessen, die beides verbinden. Dieses Kapitel beschreibt, was jeder Bestandteil leistet – und was nicht enthalten ist.

5.1 Die Plattform – die technische Grundlage

Die Enginsight-Plattform ist eine deutsche Eigenentwicklung und läuft on-premises in Ihrer Umgebung oder in einem Rechenzentrum Ihrer Wahl. Sie sammelt sicherheitsrelevante Daten, korreliert sie und führt automatisierte Reaktionen aus. Die zentralen Komponenten für den MDR-Service:

Pulsar Agent – Erkennung und Eindämmung am Endpunkt

Der Pulsar Agent läuft auf Servern und Clients. Er erhebt Daten direkt am Endpunkt und führt dort Reaktionsmaßnahmen aus. Pulsar liefert tiefe Einblicke in das reale Verhalten eines Endpunkts: Prozess- und Aktivitätsmuster, sicherheitsrelevante Systemereignisse sowie Kontextinformationen, die in klassischen, rein log-basierten Sensoriken oft fehlen oder erst spät sichtbar werden. Über die automatisierte Host-Isolation kann ein kompromittiertes System unmittelbar isoliert werden – noch bevor sich ein Angreifer seitwärts ausbreitet.

Über den MDR-Service hinaus umfasst Pulsar weitere Sicherheitsfunktionen: hostbasiertes Intrusion Detection System (IDS), File Integrity Monitoring (FIM), kontinuierliche Schwachstellen-Scans und Software-Inventarisierung. Diese Funktionen stehen Ihnen unabhängig vom MDR-Service als Teil der Enginsight-Plattform zur Verfügung – auch für eigene Auswertungen durch Ihr IT-Team oder einen externen IT-Partner. Details siehe docs.enginsight.com.

Pulsar ist kein Antivirus-Produkt. Er ergänzt Ihre bestehende Endpunktsicherheit um die für MDR notwendige Telemetrie und Reaktionsfähigkeit. Welche Voraussetzungen Ihr Endpunktschutz erfüllen muss, beschreibt Kapitel 8.1.

SIEM mit Data Lake – zentrale Korrelation

Das Enginsight-SIEM bringt sicherheitsrelevante Ereignisse aus den angebundenen Quellen zusammen, normalisiert sie und macht sie korrelierbar. Im Data Lake werden Log-Daten zentral indexiert und über Event Streams für Erkennungsregeln zugänglich gemacht. Cockpits stellen die Sicherheitslage Ihres Unternehmens visuell dar.

Playbooks – automatisierte Reaktionen

Playbooks führen die vom SOC-Team definierten Reaktionsregeln aus: Sie isolieren Hosts, erstellen Tickets oder benachrichtigen Verantwortliche – automatisiert, in Sekunden, rund um die Uhr. Die Logik wird vom SOC-Team gepflegt und kontinuierlich an neue Bedrohungslagen angepasst.

5.2 Die SOC-Leistung – was das Team liefert

Technologie allein erkennt Muster. Das SOC-Team entscheidet, ob aus einem Muster ein Vorfall wird – und was dann passiert.

24×7-Sicherheitsüberwachung

Unser SOC-Team überwacht Ihre Umgebung kontinuierlich auf Basis definierter SLA-Parameter: Triage, Klassifizierung und Eskalation. Jeder Alarm wird durch einen Analysten gesehen – kein automatisiertes Pass-through. Die Analysten sind deutschsprachig.

Threat Detection Use Cases

Im MDR Endpoint sind rund 50 InfoGuard EDR Threat Detection Use Cases aktiv, die typische Endpoint-Angriffs- und Ransomware-Muster abdecken. Im MDR Endpoint + Identity erweitert sich das Set auf rund 150 Use Cases über Endpunkte und Identitäten hinweg. Die Use Cases basieren auf einem vordefinierten Katalog, der gemeinsam mit Ihnen im Onboarding-Workshop konkretisiert wird – auf Basis Ihrer kritischsten Assets und Ihrer spezifischen Umgebung.

First Response, Validierung und Triage

Bei einem Alarm beginnt die Bearbeitung sofort. Innerhalb von 15 Minuten erfolgt die First Response: Der Alarm wird gesehen, eingeordnet und mit einer vorläufigen Einschätzung versehen. Danach beginnt – je nach Kritikalität – die Extended Investigation. Die genauen Reaktionszeiten und Servicezeiten sind in Kapitel 9 beschrieben.

Automatisierte Host-Isolation

Für definierte, besonders kritische Use Cases kann das SOC den betroffenen Host automatisch in Quarantäne setzen – sofern Sie diese Reaktion vorab für den jeweiligen Use Case freigegeben haben (CSOP*).

** Customer Standard Operating Procedure: vorab gemeinsam abgestimmte Vorgehensweisen für die Eindämmung. Sie definieren pro Use Case, welche automatisierten Reaktionen das SOC ohne Rückfrage ausführen darf.*

Standardisierte Kundenkommunikation

Alarm- und Incident-Benachrichtigungen erfolgen über die im Onboarding vereinbarten Kanäle – Portal, E-Mail oder Ihr eigenes ITSM-System. Jede Benachrichtigung enthält die Klassifizierung, die Einschätzung des SOC und eine konkrete Handlungsempfehlung.

Periodisches Reporting und Service Reviews

Sie erhalten einen monatlichen Standard-Report mit Alarmvolumen, Kritikalitätsverteilung und Trendindikatoren. Die Häufigkeit der gemeinsamen Service Reviews richtet sich nach dem gewählten Paket: halbjährlich bei MDR Endpoint + Identity (siehe Kapitel 9.6).

5.3 Wie ein Vorfall typischerweise abläuft

Um das Zusammenspiel von Plattform und SOC greifbar zu machen, ein typisches Szenario: Auf einem Server in Ihrer Umgebung führt ein Prozess plötzlich PowerShell-Befehle aus, die auf das Auslesen von Anmeldeinformationen hindeuten.

Zeitpunkt	Was passiert
T+0 Sekunden	Der Pulsar Agent erkennt das verdächtige Verhalten und meldet es an das SIEM
T+30 Sekunden	Das SIEM korreliert das Ereignis und stuft es als kritisch ein
innerhalb 15 Minuten	**First Response:** Ein SOC-Analyst hat den Alarm gesehen, eingeordnet und eine vorläufige Einschätzung mit Threat-Hypothese erstellt. Sofern für diesen Use Case vorab freigegeben: Pulsar isoliert den Host automatisch
innerhalb 60 Minuten	**Extended Investigation (Critical, 24×7):** Das SOC liefert die vertiefte Analyse mit bestätigtem Vorfallsumfang und konkreter Handlungsempfehlung

Was Sie nicht in der Tabelle sehen: das Threat Hunting, das parallel läuft – also die Suche nach weiteren Spuren desselben Angreifers in Ihrer Umgebung. Bei Vorfällen niedrigerer Kritikalität verschiebt sich die Extended Investigation in die jeweilige Servicezeit (siehe Kapitel 9).

5.4 Was nicht enthalten ist

Im Sinne einer ehrlichen Erwartungssteuerung: Folgende Leistungen gehören nicht zum Standard-Umfang von Enginsight MDR. Einige können als Add-on hinzugebucht werden (siehe Kapitel 6), andere bleiben in Ihrer Verantwortung.

Bereinigung in Ihrer Infrastruktur. Nach einem Vorfall isolieren wir kompromittierte Hosts und liefern eine Handlungsempfehlung. Die eigentliche Wiederherstellung – Neuaufsetzen, Patchen, Härten – erfolgt durch Ihr IT-Team oder Ihren IT-Dienstleister.

Custom Detection Engineering. Die MDR-Pakete basieren auf einem vordefinierten Use-Case-Katalog. Individuelle, kundenspezifische Erkennungsregeln für eigene Anwendungen oder Geschäftslogiken sind im Standardumfang nicht enthalten (sie können als individuelle Use Cases jederzeit hinzugebucht werden). Unabhängig davon wird der Use-Case-Katalog regelmäßig auf Basis der neusten Erkenntnisse aus Markt- und Kunden-Erfahrungen aktualisiert.

Vollumfängliche Incident Response und Forensik. Die Bereitstellung des Incident-Response-Teams ist im Service enthalten (24×7-Bereitschaft, Tier 2 und 3). Die tatsächliche Bearbeitung eines schweren Vorfalls inkl. Vor-Ort-Unterstützung wird als Professional Service nach Aufwand abgerechnet (siehe Kapitel 6.1).

Endpunktschutz im engeren Sinn (Antivirus). Pulsar Agent erkennt verdächtiges Verhalten und reagiert darauf, ersetzt aber kein klassisches Antivirenprodukt. Ein verhaltensbasierter Endpunktschutz muss in Ihrer Umgebung vorhanden und während der MDR-Servicezeit aktiv sein. Diese Beistellpflicht ist Voraussetzung für den Service.

Der Grund dafür ist die unterschiedliche Aufgabenteilung beider Technologien: Ein klassisches EDR- bzw. Antivirenprodukt arbeitet auf Dateiebene – es scannt, blockiert und bereinigt Schadcode direkt auf dem Endgerät. Pulsar Agent setzt eine Ebene darüber an: Er überwacht das Systemverhalten, korreliert Ereignisse und leitet Informationen an das SIEM weiter. Beide Ansätze greifen ineinander – EDR schließt die Lücke auf Dateiebene, Pulsar Agent liefert den Kontext für die übergeordnete Angriffserkennung. Zusammen decken sie damit zwei komplementäre Schutzschichten ab, die sich gegenseitig verstärken, aber nicht ersetzen.

6. Optionale Add-ons

Enginsight MDR deckt den Sicherheitsbetrieb für Endpunkte und Identitäten umfassend ab. In bestimmten Situationen sind darüber hinaus spezialisierte Leistungen erforderlich – etwa bei einem schweren Sicherheitsvorfall oder wenn ein Alarm intensiv untersucht werden muss. Für diese Anforderungen stehen zwei modulare Add-ons zur Verfügung. Sie können vorab vertraglich vereinbart oder im Bedarfsfall auf Anfrage aktiviert werden.

6.1 Incident Response & Recovery

Bei einem schweren Sicherheitsvorfall – etwa Ransomware, Datenabfluss oder einem mehrstufigen Angriff – reicht die Eindämmung allein nicht aus. Es braucht spezialisierte Incident Responder, die den Angriff vollständig aufklären, den Angreifer aus dem Netzwerk entfernen, die Wiederherstellung absichern und die Erkenntnisse für die Zukunft nutzbar machen.

Was im MDR Paket bereits enthalten ist – die 24×7-Bereitschaft

Der Incident-Response-Retainer ist in allen MDR-Paketen enthalten. Er hält die Bereitschaft vor, dass im Ernstfall Tier-2- und Tier-3-Analysten – einschließlich Forensik-Spezialisten – rund um die Uhr abrufbar zur Verfügung stehen. Diese Bereitschaft ist die Grundlage dafür, dass die Reaktion bei einem schweren Vorfall ohne Verzögerung beginnen kann.

Was nach Aufwand abgerechnet wird – die tatsächliche Bearbeitung

Wird ein schwerer Vorfall festgestellt, prüft das Tier-2-Team zunächst Lage und Umfang. Auf Basis dieser ersten Einschätzung wird gemeinsam mit Ihnen entschieden, welche Bearbeitungstiefe notwendig ist und welche Leistungen erbracht werden. Die tatsächliche Bearbeitung wird nach Aufwand abgerechnet, getrennt nach Tier-Stufe.

Was die Bearbeitung umfassen kann

- Übernahme des Krisenstabs und Coaching der Geschäftsführung
- Forensische Untersuchung der betroffenen Systeme
- Eindämmung der Situation und sichere Wiederherstellung der Infrastruktur
- Unterstützung bei der Einbindung von Behörden und der Krisenkommunikation
- Verhandlung mit Erpressern und Unterstützung bei rechtlichen Fragen
- Lessons Learned und Übergabe an den laufenden MDR-Service

IR-Readiness als Vorbereitung

Wer den IR-Service tatsächlich nutzen muss, gewinnt entscheidende Stunden, wenn er vorbereitet ist. Im Rahmen des MDR Onboarding-Workshops werden Ihre Infrastruktur, Eskalationswege und Schlüsselpersonen vorab erfasst – damit das IR-Team im Vorfall keine Zeit mit Grundlagenklärung verliert. Die Details zum IR-Readiness-Workshop besprechen wir auf Anfrage.

6.2 Threat Analysis

Nicht jeder Alarm lässt sich automatisiert abschließend bewerten. Manche Ereignisse erfordern menschliches Urteilsvermögen, etwa bei mehrdeutigen Indicators of Compromise, auffälligem Verhalten privilegierter Konten oder bei

der Frage, ob ein bestätigter Alarm Teil eines größeren Angriffszusammenhangs ist.

Was die Threat Analysis leistet

- Vertiefte Analyse durch einen Tier-2- oder Tier-3-Spezialisten direkt am betroffenen System
- Identifikation noch unbekannter Indikatoren (Custom IOCs)
- Untersuchung möglicher Querverbindungen zu anderen Vorfällen oder Bedrohungsakteuren
- Schriftlicher Untersuchungsbericht mit Empfehlung, ob eine Eskalation in den Full-IR-Modus sinnvoll ist

Wann sie sinnvoll ist

Wenn ein Standard-Alarm validiert wurde, aber Unsicherheit über das Ausmaß bleibt – etwa „Ein Domänen-Administrator hat sich um drei Uhr morgens angemeldet, war es kompromittiert oder berechtigte Wartung?" Threat Analysis liefert die Antwort, bevor ein vollständiger Incident Response notwendig wird.

Abrechnung

Threat Analysis wird nach tatsächlichem Aufwand auf Basis einer vorab abgestimmten Aufwandsschätzung abgerechnet. Sie erhalten eine Preis- und Zeitschätzung zur Freigabe, bevor die Untersuchung beginnt.

7. So läuft das Onboarding ab

Vom Vertragsabschluss bis zum vollwertigen Schutzbetrieb vergehen je nach Größe Ihrer Umgebung zwischen vier und zwanzig Wochen. Das Onboarding folgt einem klar strukturierten Vier-Phasen-Modell – mit definierten Aktivitäten pro Phase und drei parallellaufenden Arbeitsströmen.

7.1 Vor Vertragsabschluss

Bevor das Onboarding offiziell startet, gibt es zwei vorbereitende Schritte:

Vertrag und Auftragsbestätigung. Nach Auftragseingang erhalten Sie binnen zwei Werktagen eine Auftragsbestätigung. Wir benennen Ihre festen Ansprechpartner für Onboarding und späteren Service-Betrieb.

Initiale Kontaktaufnahme. Innerhalb von sieben Werktagen meldet sich Ihr Onboarding-Manager und versendet die Vorbereitungsunterlagen für den Kick-off.

7.2 Die vier Onboarding-Phasen im Überblick

Das eigentliche Onboarding läuft in vier aufeinander folgenden Phasen:

1. **Initialisierung**
   In der Initialisierungsphase werden die Grundlagen gelegt: organisatorisch, technisch, personell.
2. **Realisation**
   In der Realisation-Phase wird die technische Plattform aufgebaut und mit dem SOC verbunden.

3. **Baselining**
   Im Baselining wird das System produktiv geschaltet. Schwellwerte werden an Ihre Umgebung angepasst, False Positives reduziert, der Übergabepunkt an den SOC-Betrieb formell vollzogen.
4. **Operations**
   Mit der Operations-Phase beginnt der Regelbetrieb. Ab hier laufen alle Service-Leistungen aus Kapitel 5 und die SLAs aus Kapitel 9.

In jeder Phase laufen drei Arbeitsströme parallel:

- **Governance** – die organisatorische Struktur: Rollen, Prozesse, Eskalationswege
- **Stream EDR** – die Endpunkt-Erkennung mit Pulsar Agent
- **Stream SIEM** – die Anbindung der Logquellen und Rule-Tuning

> *Hinweis: Der Umfang des SIEM-Streams hängt von Ihrem gewählten Paket ab. Bei MDR Endpoint umfasst er nur die für die Endpunkt-Erkennung notwendigen SIEM-Funktionen. Bei MDR Endpoint + Identity kommen die Identitäts-Datenquellen hinzu. Bei individuellen Use Cases wird der Stream auf weitere, individuell vereinbarte Datenquellen erweitert.*

7.3 Wie lange dauert das Onboarding?

Die Gesamtdauer hängt primär von der Größe und Heterogenität Ihrer Umgebung ab. Als Orientierung:

Umgebungsgröße	Typische Dauer Onboarding
Bis 500 Endpunkte	30 bis 60 Tage
Bis 1.000 Endpunkte	30 bis 90 Tage
Über 1.000 Endpunkte	60 bis 120 Tage

Diese Zahlen gehen von einer mittleren IT-Komplexität und üblicher Mitwirkungsfähigkeit Ihrerseits aus. Komplexe Multi-Standort-Umgebungen, schwer dokumentierte Bestandssysteme oder eine erhöhte Anzahl an Datenquellen können die Projektdauer verlängern.

8. Voraussetzungen & Mitwirkungspflichten

Enginsight MDR entfaltet seine Wirkung nur in einer dafür vorbereiteten Umgebung. Dieses Kapitel zeigt, was das konkret bedeutet: welche Voraussetzungen vor dem Onboarding zu schaffen sind, was wir im Onboarding und im laufenden Betrieb gemeinsam leisten – und was Sie von uns erwarten können.

8.1 Technische Voraussetzungen

Damit das Onboarding starten kann, müssen folgende Voraussetzungen in Ihrer Umgebung erfüllt sein:

Verhaltensbasierter Endpunktschutz (Beistellpflicht)

Auf allen Systemen, die in den MDR-Service einbezogen werden, muss eine Endpunktschutzlösung mit verhaltensbasierter Erkennung installiert und aktiv sein – während der gesamten Servicezeit. Diese Lösung erkennt und blockiert sowohl bekannte Schadsoftware als auch verhaltensbasierte Angriffsmuster. Pulsar Agent ergänzt diese Endpunktsicherheit um die für MDR notwendige Telemetrie und Reaktionsfähigkeit – er ersetzt sie nicht.

Eine reine Signatur-basierte Antivirenlösung erfüllt die Anforderung nicht. Üblicherweise abgedeckt durch Microsoft Defender (in den verhaltensbasierten Konfigurationen ab Windows 11 Pro/Enterprise) oder vergleichbare Produkte führender Hersteller.

Pulsar-Agent-fähige Endpunkte

Die zu schützenden Clients und Server müssen den Enginsight Pulsar Agent ausführen können. Unterstützt werden aktuelle Versionen von Windows, Linux und macOS. Die genauen Systemanforderungen finden Sie unter docs.enginsight.com.

Netzwerk- und Firewall-Freigaben

Für die Kommunikation zwischen den Pulsar Agents und Ihrer zentralen Enginsight-Plattform sowie für die Anbindung an das SOC sind definierte Netzwerk- und Firewall-Freigaben erforderlich. Die konkreten Ports und Verbindungswege werden im Onboarding gemeinsam festgelegt.

Wartungsverbindung zum SOC

Die Verbindung zwischen Ihrer Enginsight-Plattform und dem SOC wird über redundante Site-to-Site-VPNs hergestellt, die in geo-separierten Rechenzentren terminieren (siehe Kapitel 9.5). Die Einrichtung erfolgt im Onboarding.

Hosting der Enginsight-Plattform

Die Enginsight-Plattform läuft entweder on-premises in Ihrer Umgebung oder in einem Rechenzentrum Ihrer Wahl. Die dafür benötigten Server-Ressourcen (virtuelle Maschinen, Speicher, Netzwerkbandbreite) liegen in Ihrer Verantwortung.

8.2 So bereiten Sie sich auf das Onboarding vor

Das Onboarding läuft erfolgreich, wenn folgende Informationen und Dokumente bereits vor dem Kick-off vorliegen:

- **Asset-Liste** mit allen in den Service einzubeziehenden Systemen (Server, Clients, virtuelle Maschinen) inklusive Betriebssystem, Standort und Verantwortlichkeit
- **Netzwerk-Dokumentation** mit Standorten, Segmentierung, Firewall-Übergängen und Internet-Anbindung
- **Liste besonders schützenswerter Systeme und Datenbestände**, deren Kompromittierung erhebliche Geschäftsauswirkungen hätte
- **Liste der Datenquellen** (bei MDR Endpoint + Identity und/oder individuellen Use Cases): Welche Identitätssysteme, Sicherheitstools, Cloud-Plattformen oder weitere Quellen sollen angebunden werden?
- **Übersicht des eingesetzten Endpunktschutzes** mit Versionsstand und Verteilungslogik
- **Definition der Eskalationswege**: Wer wird bei welchem Vorfalltyp informiert, wer ist 24×7 erreichbar, wer trifft technische Entscheidungen?

Diese Informationen erfassen wir gemeinsam in einem strukturierten Onboarding, das wir mit Ihnen nach der Auftragsbestätigung durchführen.

8.3 Ihre laufenden Mitwirkungspflichten

Während des laufenden Service-Betriebs benötigen wir von Ihnen folgende Mitwirkung:

Informationsbereitstellung

Sie stellen alle für die Erbringung des Service erforderlichen Informationen zeitnah zur Verfügung – insbesondere bei Rückfragen aus der Vorfall-Bearbeitung. Verzögerungen bei Rückfragen können die Bearbeitung kritischer Vorfälle behindern.

Aufrechterhaltung der Systemvoraussetzungen

Sie halten Ihre IT-Infrastruktur aktuell und stellen sicher, dass die in 8.1 beschriebenen Voraussetzungen kontinuierlich erfüllt sind. Dazu gehören regelmäßige Updates der Plattform-Komponenten, des Endpunktschutzes und der Betriebssysteme. Die Wartung Ihrer Server-Infrastruktur und der Plattform-Komponenten liegt in Ihrer Verantwortung oder der eines von Ihnen beauftragten IT-Dienstleisters.

Zugriffs- und Berechtigungsverwaltung

Sie stellen sicher, dass die für den Service notwendigen Zugriffsrechte für unsere SOC-Analysten erteilt und aktuell gehalten werden. Personalwechsel auf Ihrer oder unserer Seite werden zeitnah kommuniziert, damit Berechtigungen entsprechend angepasst werden können.

Transparenz zu Architektur-Änderungen

Wenn sich Ihre Umgebung verändert – etwa durch neue Server-Pools, eine VDI-Einführung oder neue Admin-Tools – informieren Sie uns rechtzeitig. Damit können die Erkennungsregeln sauber angepasst werden und Service-Unterbrechungen vermieden werden.

Kooperation bei Tests und Updates

Im Rahmen geplanter Updates, Konfigurationsänderungen oder Tests stellen Sie die notwendigen Informationen, Systemzugänge und Ansprechpartner bereit. Sie nehmen an Planungssitzungen teil und liefern zeitnahes Feedback zu Testergebnissen.

Meldung von Störungen und Änderungen

Störungen, Probleme oder Ausfälle, die die Serviceerbringung beeinträchtigen können, melden Sie unverzüglich an unser Service-Management. Geplante Änderungen an Ihrer IT-Umgebung, die den Service betreffen, melden Sie idealerweise zwei Wochen vor Umsetzung (siehe Kapitel 9.7 zu Change Requests).

Reaktion auf Handlungsempfehlungen

Nach jedem validierten Sicherheitsvorfall erhalten Sie von uns eine konkrete Handlungsempfehlung. Die Umsetzung dieser Empfehlungen liegt in Ihrer Verantwortung. Wir empfehlen, einen verbindlichen Prozess für die zeitnahe Bearbeitung dieser Empfehlungen zu etablieren – sonst entsteht eine Lücke zwischen Erkennung und Behebung, die unnötiges Risiko erzeugt.

8.4 Was wir Ihnen bereitstellen

Im Gegenzug erhalten Sie von uns:

- **Onboarding-Formular** zur strukturierten Erfassung aller benötigten Informationen, mit Auftragsbestätigung
- **Dokumentation Ihrer Service-Konfiguration**: angebundene Systeme, aktive Use Cases, vereinbarte Customer Standard Operating Procedures, Eskalationskontakte
- **Zugang zur Security Management Plattform** mit Echtzeit-Übersicht über Sicherheitslage, Tickets und Dashboards (siehe Kapitel 9.5)
- **Schulung Ihrer technischen Ansprechpartner** im Umgang mit der Plattform, im Rahmen des Onboardings
- **Regelmäßige Information** über Veränderungen der Bedrohungslage und über neue Erkennungsregeln, die für Ihre Umgebung aktiviert werden
- **Persönliche Ansprechpartner** für Onboarding, SOC und Service Management – mit Vertretungsregelung

9. SLAs, Service Management & Kommunikation

Dieses Kapitel beschreibt, was Sie im laufenden Service-Betrieb von uns erwarten dürfen, und wie wir mit Ihnen kommunizieren. Im Zentrum stehen die zugesicherten Reaktionszeiten bei Sicherheitsvorfällen, das Kunden-Portal als Ihre transparente Schnittstelle zum SOC.

9.1 First Response – 15 Minuten, unabhängig vom Schweregrad

Wenn das SOC einen Alarm erhält (egal ob durch eigene Erkennung oder durch Ihre Meldung) beginnt unsere Bearbeitung sofort. Die First Response ist der Zeitpunkt, an dem ein Analyst den Alarm gesehen, eingeordnet und die initiale Triage durchgeführt hat. Sie ist die wichtigste Zusicherung, die ein MDR-Service geben kann: Sie schließt das Zeitfenster, in dem Angreifer unbemerkt agieren können.

Kritikalität	Servicezeit	First Response	Ergebnis
Critical/High/Normal/ Low	24×7	15 Minuten	Vorläufige Einschätzung, Threat-Hypothese

Die First-Response-Zusicherung gilt rund um die Uhr, an jedem Tag des Jahres, für jede Kritikalitätsstufe. Innerhalb dieser 15 Minuten hat das SOC den Alarm geprüft und eine erste Bewertung erstellt: Liegt eine Bedrohungslage vor, welche Indikatoren weisen darauf hin, welche Hypothese verfolgen wir weiter?

9.2 Extended Investigation – die vertiefte Bearbeitung

Im zweiten Schritt vertieft das SOC die Analyse: Ist die Hypothese bestätigt? Wie groß ist der Vorfall? Welche Systeme sind betroffen? Welche Handlungsempfehlung folgt daraus? Die Servicezeit und die Reaktionszeit für diese Phase richten sich nach der Kritikalität des Vorfalls.

Kritikalität	Servicezeit	Extended Investigation Response
Critical	24×7	60 Minuten
High	10×5 (Mo–Fr 8:00–18:00)	4 Stunden
Normal	10×5 (Mo–Fr 8:00–18:00)	8 Stunden
Low	10×5 (Mo–Fr 8:00–18:00)	24 Stunden

Critical-Vorfälle werden rund um die Uhr in die Extended Investigation übernommen – also auch Nachts, am Wochenende und an Feiertagen. Bei den übrigen Kritikalitätsstufen erfolgt die vertiefte Bearbeitung während der Geschäftszeiten. Die First-Response-Bewertung selbst (inklusive der vorläufigen Einschätzung und der Threat-Hypothese) liegt Ihnen aber immer innerhalb von 15 Minuten vor, auch außerhalb der Geschäftszeiten.

9.3 Klassifizierung der Schweregrade

Die Einstufung eines Vorfalls als Critical, High, Normal oder Low erfolgt durch das SOC anhand zweier Dimensionen:

Use Case Criticality. Wie schwer wiegt das erkannte Bedrohungsmuster? Wo im Angriffszyklus befindet sich der Angreifer? Welche Folgeschritte sind möglich, wenn nicht eingegriffen wird? Ein Use Case, der frühe Aufklärung erkennt, hat eine niedrigere Kritikalität als einer, der laufende Datenexfiltration anzeigt.

Asset Criticality. Welche Bedeutung hat das betroffene System für Ihren Geschäftsbetrieb? Ein Verwaltungsclient hat eine andere Kritikalität als ein produktiver Server oder ein System mit besonders sensiblen Daten.

Aus der Kombination beider Dimensionen ergibt sich die Gesamtkritikalität eines Vorfalls. Welche Ihrer Systeme als besonders kritisch gelten, definieren Sie gemeinsam mit uns im Onboarding. Die Klassifizierungslogik wird im Service Review fortlaufend an Ihre Umgebung angepasst.

9.4 Übergabepunkt der Servicequalität

Die zugesicherten Service-Level beziehen sich auf den Übergabepunkt des SOC – also den Punkt, an dem das SOC-System eine Verbindung zum Internet bzw. zur Übergabeinfrastruktur des Rechenzentrums herstellt. Verzögerungen, die durch Ausfälle bei Telekommunikationsanbietern, in Ihrer Internet-Verbindung oder in Ihrer eigenen Infrastruktur entstehen, liegen außerhalb der Verantwortung des SOC und werden in den SLA-Messungen nicht berücksichtigt.

9.5 Ihr Zugang zum SOC – das Kunden-Portal

Ein Sicherheitsservice ist nur so wertvoll, wie er für Sie transparent ist. Sie wollen wissen, was das SOC sieht, welche Alarme bearbeitet werden und in welchem Status Ihre Anfragen stehen. Dafür stellen wir Ihnen mit der Security Management Plattform (SMP) ein Kunden-Portal zur Verfügung.

Was Sie im Portal sehen

Verschiedene Dashboards zeigen Service-Visualisierungen Ihrer Sicherheitslage. Ihre Tickets sind mit Status jederzeit ersichtlich und abrufbar. Sie sehen, welche Aktion das SOC wann durchgeführt

hat, welche Empfehlungen ausgesprochen wurden und in welcher Bearbeitungsphase sich ein Vorfall befindet.

Anbindung an Ihre Systemlandschaft

Im Service ist eine E-Mail-basierte Schnittstelle für die Anbindung Ihres Ticketing- oder Case-Management-Systems enthalten. Wenn das SOC einen Sicherheitsvorfall startet, werden Sie informiert. Aktionen sind erst dann von Ihrer Seite erforderlich, wenn das SOC Ihre Rückmeldung benötigt*.

** Im Idealfall liegt die Eigenlöserate des SOC bei 100 % – das heißt, der Vorfall wird vollständig vom SOC bearbeitet, ohne dass Sie aktiv eingreifen müssen.*

Konnektivität

Die Verbindung zwischen Security Management Plattform und Ihrer Infrastruktur wird über redundante Site-to-Site-VPNs gewährleistet. Die redundanten VPN-Verbindungen terminieren in geo-separierten Rechenzentren, um eine Verfügbarkeit von 99,9 % zu sichern. Alle Services aus dem SOC werden redundant über beide Rechenzentren betrieben. Bei Ausfall eines Rechenzentrums werden die Services nach Wiederherstellung über das zweite Rechenzentrum bereitgestellt.

9.6 Service Management – die laufende Zusammenarbeit

Über die operative Vorfall-Bearbeitung hinaus pflegen wir mit Ihnen eine strukturierte Zusammenarbeit, damit der Service nicht nur funktioniert, sondern sich kontinuierlich verbessert.

Service Review Meetings

Im Paket MDR Endpoint + Identity finden Service Reviews mit folgendem Inhalt statt:

Übersicht aller Sicherheitsvorfälle des Berichtszeitraums (Anzahl, Kritikalität, Status)

- Einhaltung der SLAs (First Response und Extended Investigation je Kritikalitätsstufe)
- Konkrete Handlungsempfehlungen aus den Vorfällen
- Veränderungen der Bedrohungslage und Anpassungen der Use Cases
- Optimierungspotenziale am Service-Setup

Teilnehmerkreis

Pflicht-Teilnehmer auf Ihrer Seite: ein technischer Verantwortlicher, der Entscheidungen über Konfigurationsanpassungen treffen kann. Empfohlen: IT-Sicherheitsverantwortliche/r, Informationssicherheitsbeauftragte/r oder CISO. Auf Wunsch sind Geschäftsführung, Datenschutzbeauftragte oder externe Berater willkommen.

Ad-hoc-Kommunikation zwischen den Reviews

Bei Sicherheitsvorfällen oder dringenden Rückfragen ist das SOC rund um die Uhr über die im Onboarding vereinbarten Kanäle erreichbar – Portal, E-Mail und Telefon. Für nicht-zeitkritische Anliegen steht Ihnen das Service-Management während der Geschäftszeiten zur Verfügung.

Eskalation

Sind Sie mit der Bearbeitung eines Vorfalls oder mit dem Service insgesamt nicht zufrieden, steht Ihnen ein definierter Eskalationspfad zur Verfügung. Erstkontakt ist Ihr Service-Manager; bei

ungelösten Themen erfolgt die Eskalation in die Leitung Service Delivery und in die Geschäftsführung. Die genauen Kontaktdaten finden Sie in Kapitel 14.

9.7 Änderungen an Ihrer Umgebung – Change Requests

Änderungen an Ihrer eigenen IT-Umgebung, die die Funktionsfähigkeit des MDR-Service betreffen, liegen in Ihrer Verantwortung. Dazu gehören etwa die Migration auf eine neue Firewall-Generation, die Einführung einer neuen Identitätsplattform, die Veränderung der Netzwerksegmentierung oder größere Software-Rollouts.

Hier informieren Sie uns bitte: Sie melden geplante Änderungen, die den Service betreffen können, vorab an unser Service-Management – idealerweise zwei Wochen vor Umsetzung. Damit können wir prüfen, ob Anpassungen an der Konfiguration der Plattform oder der Erkennungslogik nötig sind, und Service-Unterbrechungen vermeiden.

Was wir nicht übernehmen: Die Planung, Durchführung und Dokumentation von Änderungen an Ihrer Umgebung ist nicht Bestandteil des MDR-Service. Wir konfigurieren ausschließlich die Komponenten der Enginsight-Plattform und unsere Erkennungs- und Reaktionsregeln. Anpassungen, die durch eine Änderung Ihrer Umgebung notwendig werden, können einen zusätzlichen Aufwand darstellen, der je nach Umfang als Service Request abgewickelt oder gesondert beauftragt wird.

9.8 Service Requests

Über das Incident Handling hinaus können Sie standardisierte Anpassungen am Service beauftragen – etwa die Erstellung eines neuen Dashboards, die Anpassung eines bestehenden Use Cases oder die Justierung von Schwellwerten. Solche Service Requests werden 10×5 bearbeitet. Die Definitionen, Bearbeitungszeiten und der genaue Prozess sind in Anhang A4 beschrieben.

10. Datenschutz & Datenverarbeitung

Enginsight MDR verarbeitet Daten, die zum Schutz Ihrer IT-Umgebung notwendig sind – darunter Telemetrie von Endpunkten, Log-Daten und Informationen zu Sicherheitsvorfällen. Dieses Kapitel beschreibt, in welchen Rollen wir mit diesen Daten arbeiten, wo sie verarbeitet werden und wie sie geschützt sind. Die rechtlich verbindlichen Details regelt die Auftragsverarbeitungsvereinbarung (AVV) gemäß Art. 28 DSGVO, die als separates Dokument Bestandteil Ihres Vertrags wird.

10.1 Rollen und Verantwortlichkeiten

Sie sind im Sinne der DSGVO Verantwortlicher für die in Ihrer Umgebung erhobenen Daten. Sie entscheiden über Zweck und Mittel der Datenverarbeitung. Sie definieren, welche Systeme in den MDR-Service einbezogen werden, welche Datenquellen angebunden werden und welche personenbezogenen Daten dabei verarbeitet werden.

Die Enginsight GmbH ist Auftragsverarbeiter. Wir verarbeiten Ihre Daten ausschließlich auf Ihre dokumentierte Weisung und im Rahmen des vertraglich definierten Service-Umfangs. Eigene Verarbeitungszwecke verfolgen wir nicht.

Zur Erbringung der 24×7-SOC-Leistungen setzen wir InfoGuard als Unter-Auftragsverarbeiter ein. Die Datenverarbeitung durch InfoGuard ist vertraglich auf den Umfang dieser Auftragsverarbeitung beschränkt und entspricht den Anforderungen der DSGVO. Ihre Einwilligung in den Einsatz dieses Unter-Auftragsverarbeiters ist Voraussetzung für die Service-Erbringung und wird mit der AVV

erklärt. Weitere Unter-Auftragsverarbeiter werden ohne Ihre vorherige Information nicht eingebunden.

10.2 Welche Daten verarbeitet werden

Im Rahmen des MDR-Service werden folgende Datenkategorien verarbeitet:

Telemetrie- und Log-Daten von Endpunkten: Systeminformationen, Software-Inventar, Prozess- und Netzwerkaktivitäten, Schwachstellen-Befunde, sicherheitsrelevante Ereignisse aus Betriebssystemen und Anwendungen.

Identitäts- und Anmeldedaten: Anmelde- und Berechtigungsereignisse aus Active Directory oder Microsoft Entra ID – Benutzernamen, Zeitstempel, Quell-IP-Adressen, Authentifizierungsstatus. Klartextpasswörter werden zu keinem Zeitpunkt verarbeitet.

Log-Daten weiterer Datenquellen: Inhalte abhängig von der jeweiligen Quelle – etwa Firewall-Verbindungslogs, Cloud-Plattform-Audit-Logs, Sicherheitstool-Warnungen.

Vorfall-Daten: Im Rahmen der SOC-Analyse erhobene Informationen zu erkannten Sicherheitsvorfällen, einschließlich Bewertung, Klassifikation, Reaktionsmaßnahmen und Empfehlungen.

Kontaktdaten Ihrer benannten Ansprechpartner: Name, Funktion, Telefonnummer, E-Mail-Adresse – zur Kommunikation im Rahmen des Service-Betriebs.

Personenbezogene Daten werden nur in dem Umfang verarbeitet, in dem sie für die Erkennung von Sicherheitsvorfällen erforderlich sind. Wo technisch möglich, werden Identifikatoren obfuskiert oder pseudonymisiert.

10.3 Wo Daten verarbeitet werden

Die Enginsight-Plattform mit dem Data Lake läuft entweder on-premises in Ihrer Umgebung oder in einem deutschen Rechenzentrum unter Ihrer Verantwortung. Telemetrie und Log-Daten verlassen Ihre Hoheit nicht.

Für die SOC-Analyse greifen die Analysten über eine kontrollierte, verschlüsselte Verbindung auf Ihre Plattform zu. Es werden keine Bulk-Daten exportiert; der Zugriff erfolgt lesend auf die für die Analyse erforderlichen Einzelereignisse. Vorfall-bezogene Daten werden in den SOC-Systemen von InfoGuard verarbeitet, die in Deutschland und der Schweiz betrieben werden – beides Länder mit Angemessenheitsentscheidung der EU-Kommission bzw. innerhalb des EWR.

Eine Übermittlung von Daten in Drittländer außerhalb von EU/EWR/Schweiz findet im Rahmen des Service nicht statt. Die Enginsight-Plattform unterliegt keinem US-amerikanischen Recht, insbesondere nicht dem CLOUD Act, da weder Enginsight noch InfoGuard Tochtergesellschaften US-amerikanischer Konzerne sind und keine Datenverarbeitung auf US-Servern stattfindet.

10.4 Wer Zugriff auf Ihre Daten hat

Zugriff auf Ihre Daten haben ausschließlich:

- Namentlich benannte und vertraulichkeitsverpflichtete SOC-Analysten und Incident Responder von Enginsight und InfoGuard
- Im Bedarfsfall: Service-Management-Verantwortliche zur Bearbeitung von Eskalationen
- Im Audit-Fall: durch Sie autorisierte Dritte (etwa externe Auditoren)

Die genauen Zugriffsrollen und das Berechtigungskonzept werden im Onboarding dokumentiert. Personalwechsel auf unserer Seite werden so gehandhabt, dass ausscheidende Mitarbeitende ihre Zugriffsrechte unmittelbar verlieren. Wechsel können auf Anfrage durch Sie nachvollzogen werden.

Alle Zugriffe auf Ihre Daten werden in einem revisionsfähigen Audit-Log protokolliert. Sie können auf Anfrage einen Auszug dieser Logs erhalten – etwa für eigene Audit-Zwecke oder zur Nachweisführung gegenüber Aufsichtsbehörden.

10.5 Aufbewahrungsfristen

Die Aufbewahrungsfristen für Aufzeichnungen und Dokumentationen im Rahmen des MDR-Service sind wie folgt festgelegt:

3 Monate für:

- Logs und Event-Informationen im SOC
- Security-Incident-Tickets innerhalb der Security Management Plattform
- Zusätzliche Incident-Response-Dokumentation und -Evidenzen

12 Monate für:

- Informationen innerhalb des Kunden-Portals
- Kundenreporte und Service-Berichte

Telemetrie- und Log-Daten in Ihrer Enginsight-Plattform werden davon unabhängig nach den von Ihnen konfigurierten Aufbewahrungseinstellungen gespeichert – diese unterliegen Ihrer eigenen Aufbewahrungsrichtlinie.

Kontaktdaten werden für die Dauer des Vertragsverhältnisses und für die Dauer gesetzlicher Aufbewahrungsfristen verarbeitet.

Die genauen Löschkonzepte und Ausnahmen sind in der AVV geregelt.

10.6 Schriftliches Bekenntnis zu europäischen Sicherheitsstandards

Enginsight hat sich am 4. Dezember 2024 schriftlich zu den Anforderungen und Empfehlungen der Europäischen Agentur für Cybersicherheit (ENISA) bekannt – konkret zum ENISA-Dokument „Indispensable baseline security requirements for the procurement of secure ICT products and services". Die Bekennungsurkunde, unterzeichnet durch unsere Geschäftsführung, ist auf Anfrage einsehbar.

Mit dieser Bekennung verpflichten wir uns:

- die Empfehlungen und Anforderungen der ENISA für die Entwicklung und den Betrieb unserer Cybersicherheits-Lösung umzusetzen,
- die ENISA Best Practices in unsere internen Prozesse zu überführen,
- kontinuierlich zur Verbesserung der Cybersicherheitsstandards innerhalb unserer Organisation beizutragen.

Warum das für Sie relevant ist. Die ENISA gestaltet die europäischen Rahmenwerke mit, die Sie als Unternehmen einhalten müssen – die NIS2-Richtlinie, den Cyber Resilience Act, den EU Cybersecurity Act. Wer seine Sicherheitsplattform und seinen Service an diesen Leitlinien ausrichtet, schafft die operative Grundlage für deren Erfüllung. Ihre Compliance-Bemühungen und unsere Plattform-Roadmap arbeiten in dieselbe Richtung.

Diese Ausrichtung ist Teil unseres Selbstverständnisses als deutscher Hersteller: Wir positionieren uns bewusst innerhalb der europäischen Cybersicherheits-Governance – nicht in dem internationaler Konzerne, die ihre eigenen, oft US-zentrierten Standards setzen.

10.7 Auftragsverarbeitungsvereinbarung

Die rechtlich verbindlichen Regelungen zur Auftragsverarbeitung – einschließlich der vollständigen Liste der Datenkategorien, der technisch-organisatorischen Maßnahmen (TOM), der Subunternehmer-Liste und der Regelungen zur Datenträgerentsorgung – sind in der Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO festgehalten. Die AVV wird gemeinsam mit dem Servicevertrag und diesem Service-Beschreibung unterzeichnet.

Die in diesem Kapitel beschriebenen Punkte geben einen Überblick. Bei Abweichungen oder Lücken zwischen diesem Kapitel und der AVV gilt der Wortlaut der AVV.

11. Beendigung des Services

Anders als bei vielen anderen MDR-Anbietern endet mit der Beendigung des Enginsight-MDR-Service nicht der Zugang zu Ihrer Sicherheitsplattform. Die Enginsight-Plattform und alle darin gespeicherten Daten gehören Ihnen – unabhängig davon, ob Sie den SOC-Service weiter beziehen oder nicht.

11.1 Vertragslaufzeit und Kündigung

Die MDR-Pakete haben eine Mindestlaufzeit von 12 Monaten. Der Servicevertrag verlängert sich automatisch um jeweils 12 weitere Monate, sofern er nicht drei Monate vor Ablauf des jeweiligen Leistungszeitraums schriftlich gekündigt wird.

Eine außerordentliche Kündigung aus wichtigem Grund bleibt für beide Vertragsparteien unberührt und richtet sich nach den gesetzlichen Bestimmungen.

11.2 Was endet, was bleibt

Mit dem Ende des MDR-Service enden die folgenden Leistungen:

- 24×7-Überwachung Ihrer Umgebung durch das SOC-Team
- Validierung, Triage und aktive Eindämmung von Sicherheitsvorfällen
- Service Reviews und SLA-Berichte
- Zugriff der SOC-Analysten auf Ihre Enginsight-Plattform
- 24×7-Bereitschaft des Incident-Response-Teams

Was bestehen bleibt:

- Ihre Enginsight-Plattform-Lizenz – vorausgesetzt, der Softwarelizenz-Vertrag besteht weiter
- Alle in Ihrem System gespeicherten Telemetrie- und Log-Daten
- Alle im SIEM eingerichteten Erkennungsregeln und Workflows
- Alle Dashboards, Cockpits und Reports
- Alle angebundenen Datenquellen und Konfigurationen

Sie verlieren weder Daten noch Funktionalität der Plattform. Was Sie ab dem Ende des MDR-Service nicht mehr haben, ist der menschliche Sicherheitsbetrieb – die Plattform selbst bleibt voll

funktionsfähig und kann von Ihrem eigenen Team oder einem Enginsight-Partner weiter betrieben werden.

11.3 Datenrückgabe und -löschung

Da Ihre Daten ohnehin in Ihrer Plattform bleiben, ist eine separate Datenrückgabe nicht erforderlich. Eine Ausnahme bilden vorfall-bezogene Daten, die in den SOC-Systemen verarbeitet wurden (siehe Kapitel 10.5): Diese werden gemäß den in der Auftragsverarbeitungsvereinbarung geregelten Fristen aufbewahrt und anschließend gelöscht.

Möchten Sie eine frühere Löschung oder einen vollständigen Export dieser Daten, kontaktieren Sie unser Service-Management. Eine vorzeitige Löschung erfolgt unter Wahrung gesetzlicher Aufbewahrungspflichten.

11.4 Beendigung der Zugriffe

Mit dem Ende des Servicevertrags werden die Zugriffsrechte der SOC-Analysten auf Ihre Enginsight-Plattform deaktiviert. Die kontrollierte Site-to-Site-VPN-Verbindung zwischen Ihrer Plattform und dem SOC wird zurückgebaut. Sie behalten die volle administrative Kontrolle über Ihre Umgebung.

12. Geschäftsbedingungen

Dieses Kapitel beschreibt die kommerziellen Rahmenbedingungen für den Bezug von Enginsight MDR. Die rechtlich verbindlichen Regelungen – einschließlich Allgemeiner Geschäftsbedingungen, Haftung und Gewährleistung – sind im Servicevertrag zwischen Ihnen und der Enginsight GmbH festgehalten.

12.1 Preise und Rechnungsstellung

Preise

Alle Preise im Rahmen dieses Service-Angebots verstehen sich netto, zuzüglich der gesetzlichen Mehrwertsteuer. Die konkreten Preise für die gewählten MDR-Pakete und die optionalen Zusatzleistungen (z.B. individuelle Use Cases) werden Ihnen im individuellen Angebot ausgewiesen.

Einmalige Gebühren – Service Initialisierung

Die Service Initialisierung (Initialisierung, Realisation und Baselining – siehe Kapitel 7) wird als einmalige Gebühr abgerechnet. Die genaue Höhe ergibt sich aus Umfang und Komplexität Ihrer Umgebung und wird im individuellen Angebot ausgewiesen.

Wiederkehrende Gebühren – Servicebetrieb

Die laufenden Gebühren für den MDR-Service werden in einem regelmäßigen Rhythmus im Voraus in Rechnung gestellt. Der konkrete Abrechnungsmodus wird im Servicevertrag geregelt.

Aufwandsbasierte Leistungen

Leistungen, die nach tatsächlichem Aufwand abgerechnet werden – etwa die Nutzung des Incident-Response-Teams, Threat Analysis oder zusätzliche Custom Detection Rules, werden nach erbrachter Leistung in Rechnung gestellt. Auf Wunsch erhalten Sie vor Aufnahme der Tätigkeit eine Aufwandsschätzung zur Freigabe.

12.2 Vertragslaufzeit

Die MDR-Pakete haben eine Mindestlaufzeit von 12 Monaten. Der Servicevertrag verlängert sich automatisch um jeweils 12 weitere Monate, sofern er nicht drei Monate vor Ablauf des jeweiligen Leistungszeitraums schriftlich gekündigt wird. Details zur Beendigung des Services finden Sie in Kapitel 11.

12.3 Gültigkeit des Angebots

Ein Ihnen vorgelegtes individuelles Angebot ist 90 Tage ab Angebotsdatum gültig. Nach Ablauf der Gültigkeit können sich Konditionen ändern – etwa durch zwischenzeitliche Anpassungen der Preisliste, Änderungen Ihrer Umgebung oder neue regulatorische Anforderungen. Eine Verlängerung der Angebotsgültigkeit ist auf Anfrage möglich.

12.4 Vertragsabschluss und Bestellung

Der Vertragsabschluss erfolgt durch beidseitige Unterzeichnung des Servicevertrags und seiner Anlagen. Zu den Anlagen gehören insbesondere:

- Dieser Service-Beschreibung
- Das individuelle Angebot mit Preiskalkulation
- Die Auftragsverarbeitungsvereinbarung (AVV) gemäß Art. 28 DSGVO

Die formale Bestellung erfolgt im Rahmen des Vertragsabschlusses. Ein separates Bestellformular ist nicht erforderlich.

12.5 Vertragspartner und Vertragsverhältnis

Ihr Vertragspartner ist die Enginsight GmbH, eingetragen im Handelsregister beim Amtsgericht Jena unter HRB 51280

8. Alle vertraglichen Beziehungen – einschließlich Rechnungsstellung, Vertragsänderungen und Eskalation kommerzieller Themen – bestehen ausschließlich mit Enginsight. Die operative Service-Erbringung durch unseren Premium-Partner ist Bestandteil dieses Vertrags und wird durch Enginsight verantwortet (siehe Kapitel 13).

13. Vertrauen & Erfahrung

Ein MDR-Service ist nur so gut wie die Menschen und Organisationen, die ihn erbringen. Dieses Kapitel beschreibt, wer hinter Enginsight MDR steht: Enginsight als Plattform-Hersteller und Ihr Vertragspartner – und InfoGuard als unser Premium-Partner für den operativen 24/7-SOC-Betrieb.

13.1 Enginsight – die Plattform aus Deutschland

Die Enginsight GmbH ist ein deutscher Cybersecurity-Spezialist mit Sitz in Jena, Thüringen. Wir entwickeln seit Gründung des Unternehmens unsere Sicherheitsplattform vollständig in Deutschland – als Eigenentwicklung, ohne Anbindung an internationale Konzerne und ohne Abhängigkeit von ausländischen Cloud-Anbietern.

Was uns auszeichnet

- **Made in Germany** – Plattform-Entwicklung und Hosting in Deutschland

- **EU-patentierte Technologie** in Kernbereichen der Erkennungs- und Reaktionslogik
- **ISO 27001-zertifiziert** für die eigene Informationssicherheit
- **Schriftliches Bekenntnis zur ENISA** seit Dezember 2024 (Details in Kapitel 10.6)
- **Souveräne Datenhaltung** – kein CLOUD Act, keine Datenverarbeitung außerhalb EU/EWR/Schweiz
- **Unabhängig und eigentümergeführt** – keine Konzernmutter, keine US-Investoren, keine Übernahmerisiken
- **Spezialisiert auf den deutschen Mittelstand** – Plattform und Service sind auf die Realität mittelständischer IT-Organisationen ausgelegt

Die Enginsight-Plattform schützt heute mehrere hundert Endkundenumgebungen mit insgesamt über 100.000 überwachten Systemen. Zu unseren Kunden zählen Industrie- und Handelsunternehmen, Energieversorger, Kommunen, Gesundheitseinrichtungen und Behörden.

13.2 InfoGuard – unser Premium-Partner für den 24/7-SOC-Betrieb

Den 24/7-Betrieb des SOC-Teams für Enginsight MDR erbringen wir gemeinsam mit unserem Premium-Partner InfoGuard. InfoGuard ist seit über 25 Jahren als Cybersecurity-Spezialist aktiv und gehört im deutschsprachigen Raum zu den etablierten Anbietern für Cyber Defence und Incident Response.

Was InfoGuard mitbringt

- **Über 25 Jahre Cybersecurity-Expertise** und durchgehende Spezialisierung auf Managed Detection & Response, Incident Response und Cyber Defence
- **Zwei Security Operation Center** mit 24/7-Betrieb – in der Schweiz und in Deutschland, mit durchgehend personeller Besetzung
- **Über 90 hochspezialisierte Analysten und Incident Responder** im SOC und CSIRT
- **Über 450 SOC-Kunden** aus unterschiedlichen Branchen – darunter Industrie, Banken, Versicherungen, Energieversorger, Krankenhäuser und Behörden
- **BSI-qualifizierter APT-Response-Dienstleister** für die Bearbeitung von Advanced Persistent Threats
- **Mitglied des FIRST** (Forum of Incident Response and Security Teams), dem internationalen Verbund führender Incident-Response-Teams
- **Incident-Response-Partner und Schadensabwickler** führender Versicherungen wie Allianz, Zürich und Marsh

InfoGuard ist ein eigentümergeführtes Unternehmen mit Sitz in Baar (Schweiz) und Standorten in Frankfurt, München, Düsseldorf und Wien – durchgehend innerhalb des deutschsprachigen Raums und der EU/EWR-/Schweiz-Datenschutzräume.

13.3 Die Mechanik der Partnerschaft

Für Sie als Kunde bedeutet die Partnerschaft konkret:

- **Ein Vertragspartner**: Sie schließen einen Vertrag mit der Enginsight GmbH. Die Service-Erbringung – einschließlich des SOC-Betriebs durch InfoGuard – ist Teil dieses Vertrags. Es gibt keine separaten Vertragsbeziehungen mit InfoGuard.

- **Eine Auftragsverarbeitung**: Die DSGVO-konforme Datenverarbeitung ist über die Auftragsverarbeitungsvereinbarung mit Enginsight geregelt, InfoGuard agiert als Unter-Auftragsverarbeiter (siehe Kapitel 10).
- **Eine Eskalationskette**: Bei Vorfällen ist das SOC-Team Ihre erste Adresse. Bei vertraglichen Themen oder strategischen Fragen ist Enginsight Ihr Ansprechpartner.

13.4 Warum diese Konstellation für Sie funktioniert

Die Verbindung aus Enginsight-Plattform und InfoGuard-Servicebetrieb verbindet zwei Stärken, die einzelne Anbieter selten gemeinsam haben:

Tiefe Plattform-Integration durch den Hersteller selbst. Enginsight entwickelt die Plattform, die Erkennungsmechanismen und die Reaktionswerkzeuge. Veränderungen in der Bedrohungslage fließen direkt in die Plattform-Roadmap, ohne Umweg über fremde Hersteller. Sie bekommen einen MDR-Service auf einer Plattform, die für diesen Service entworfen wurde.

Operative Service-Reife durch einen etablierten Partner. InfoGuard hat über Jahre einen 24/7-SOC-Betrieb auf Premium-Niveau aufgebaut – mit erfahrenen Analysten, etablierten Prozessen und einer Skalierbarkeit, die ein einzelnes mittelständisches Unternehmen nicht in vergleichbarer Qualität abbilden kann. Sie bekommen die operative Stärke eines spezialisierten SOC-Dienstleisters, ohne die Anonymität eines internationalen Konzerns.

Die Partnerschaft ist langfristig angelegt und vertraglich abgesichert. Sie investieren in einen Service, der nicht von einer einzelnen Personalentscheidung oder einem Standort-Wechsel abhängt.