Leistungsbeschreibung (Leistungsverzeichnis)
als Bestandteil des Angebots für: Managed Extended Detect and Response (MXDR)

Bestandteil dieser Ausschreibung sind die Anlage „Zusatzvereinbarung Datensouveränität / CLOUD Act“ (im Folgenden: Zusatzvereinbarung) sowie die Anlagen 1 (Service Level), 2 (Bewertungsmatrix), 3 (Mindestinhalte Auftragsverarbeitungsvertrag) und 4 (Funktionsmatrix Betriebssysteme) zu diesem Leistungsverzeichnis. Angebote, bei denen Änderungen oder Ergänzungen an den Vergabeunterlagen vorgenommen worden sind, werden gemäß § 42 Abs. 1 Satz 2 Nr. 4 UVgO ausgeschlossen. Keine Änderung in diesem Sinne sind der vom Bieter vorzulegende Auftragsverarbeitungsvertrag, soweit er die Mindestinhalte nach „Anlage zum Leistungsverzeichnis: Mindestinhalte des Auftragsverarbeitungsvertrags“ erfüllt, sowie Angaben nach Ziffer 4a der Zusatzvereinbarung.

			vom Bieter auszufüllen	
Lfd. Nr.	Bezeichnung der Leistung, Kennzeichnung, technische Angaben, mit dem Angebot vorzulegende Nachweise	Menge bzw. Einheit	Preise je Einheit EUR	Gesamt-betrag EUR
1	**Managed Extended Detect and Response für Clients und Server** Kennzeichnung der Anforderungen: **[A]** = Mindestanforderung; wird sie nicht erfüllt, wird das Angebot ausgeschlossen. **[B1] bis [B10]** = Wertungskriterium; die Erfüllung wird nach der Bewertungsmatrix (Anlage zum Leistungsverzeichnis: Bewertungsmatrix) bewertet. Laufzeit: 12 Monate ab Laufzeitbeginn 31.12.2026 mit Option zur zweimaligen Verlängerung um jeweils 12 Monate (1+1+1). Die Option übt der Auftraggeber durch einseitige Erklärung in Textform spätestens drei Monate vor Ablauf der jeweiligen Laufzeit aus. Die Preise der Optionsjahre sind mit dem Angebot verbindlich anzugeben (Pos. 3). Der Auftragnehmer erbringt Überwachung und Management rund um die Uhr (24/7/365). Der Auftraggeber erhält Einsicht in alle Erkennungen und kann selbst Ausnahmen anlegen – oder anlegen lassen; vom Auftraggeber angelegte Ausnahmen prüft der Auftragnehmer auf Plausibilität. **[A]** Plattformunterstützung: - **[A]** Unterstützung folgender Betriebssysteme und Versionen: Windows 11, Windows Server 2019-2025 (inklusive Exchange Server SE und SQL Server 2019-2025), Ubuntu 24.04, Ubuntu 26.04, Debian 12, Debian 13, SUSE SLES 15 & 16 - **[A]** Folgende Kernfunktionen stehen auf allen unterstützten Windows- und Linux-Systemen zur Verfügung: Malware-Prävention (NGAV), EDR-Telemetrie, Isolierung aus der Ferne und Remote Response. Abweichungen im Funktionsumfang je Betriebssystem sind in der Funktionsmatrix („Anlage zum Leistungsverzeichnis: Funktionsmatrix Betriebssysteme“) vollständig anzugeben. - **[B1]** Funktionsumfang unter Linux nach der Funktionsmatrix („Anlage zum Leistungsverzeichnis: Funktionsmatrix Betriebssysteme“); Bewertung nach der Bewertungsmatrix - **[A]** Steuerbare Updates: Funktionsupdates der Agents werden in Abstimmung mit dem Auftraggeber gestaffelt ausgerollt (zunächst Testgruppe, dann Gesamtbestand); mindestens die Vorversion (N-1) ist wählbar und wird unterstützt. Erkennungs-Content-Updates werden schnellstmöglich verteilt.	**410 Endgeräte davon 70 Server 340 Clients** **Preise siehe Pos. 1.1 bis 6**		

	Bedrohungserkennung und -verhinderung: - **[A]** Erkennung und Blockierung bekannter und unbekannter Schadsoftware (u. a. Viren, Trojaner, Würmer, Spyware, Rootkits) durch signaturunabhängige Verfahren (z. B. Machine Learning, Verhaltensanalyse) in Kombination mit Heuristiken - **[A]** Verhaltensbasierter Schutz gegen Ransomware einschließlich Erkennung und Unterbindung von Massenverschlüsselung sowie Schutz vor der Ausnutzung unbekannter Schwachstellen (Zero-Day) - **[B2]** Ergebnisse in unabhängigen Tests der letzten 24 Monate (z. B. AV-TEST, AV-Comparatives) - **[A]** Verhindern der Malware-Ausführung mithilfe eines lokalen Erkennungsmodells auch ohne Cloudanbindung (beispielsweise bei Geräten ohne Internetzugang) - **[A]** Automatisierte Reaktionen zur Eindämmung und Behebung (z. B. Prozess beenden, Datei in Quarantäne verschieben, Änderungen zurücknehmen) - **[A]** Isolierung von Endpunkten aus der Ferne, wobei die Verbindung zur Management-Plattform und vom Auftraggeber festgelegte Ausnahmen (z. B. Fernwartung) erhalten bleiben - **[A]** Mehrschichtiger Ansatz mit NGAV-, EDR- und XDR-Funktionen XDR-Funktionen (mindestens): 1. **[A]** Korrelation von Ereignissen aus mehreren Quellen zu Vorfällen. Im Leistungsumfang enthaltene Datenquellen: die Endpunkte sowie die Firewall-Logs des Check-Point-Management-Servers (Export per Syslog/CEF über den Check Point Log Exporter; Umfang: ca. 45 GB pro Tag, Spitzenwert ca. 1500 Ereignisse pro Sekunde, Umfang der exportierten Logs: Firewall, zugelassene Verbindungen (Accept) 53 % Site-to-Site-VPN (Encrypt/Decrypt, Key-Exchange) 43 % Firewall, verworfen/abgewiesen (Drop/Reject) 3 % Threat Prevention: nur IPS (Detect/Prevent/Reject) 0,4 % Remote-Access-VPN (An-/Abmeldung, auch fehlgeschlagene), Identity Awareness < 0,1 % Administrations-/Audit-Logs (SmartConsole, WEB_API: Anmeldungen der Administratoren, Änderungen) < 0,1 % Identitätsquellen siehe [B9] und [B10]. Für die Anbindung erforderliche Komponenten beim Auftraggeber (z. B. Log-Collector als virtuelle Maschine) sind mit ihren Systemanforderungen im Angebot anzugeben. Weitere vom Anbieter unterstützte Datenquellen sind im Angebot ohne Preisangabe aufzulisten; sie werden nicht gewertet. 2. **[A]** Automatische Anreicherung von Ereignissen mit IOC-Daten und Risikokontext (Threat Intelligence Enrichment) 3. **[A]** Zuordnung von Erkennungen zu Taktiken und Techniken nach MITRE ATT&CK 4. **[A]** Automatisierte Reaktionsabläufe für gängige Bedrohungsszenarien, sodass nicht jeder Vorfall manuelles Eingreifen erfordert 5. **[A]** Dokumentierte Reaktionsabläufe (z. B. Playbooks), die dem Auftraggeber zugänglich sind			

	Identitätsüberwachung: - **[B9]** Überwachung der Identitäten in Microsoft 365 / Entra ID (470 Benutzerkonten): Erkennung identitätsbasierter Angriffe (z. B. verdächtige Anmeldungen, Token-Diebstahl, MFA-Ermüdungsangriffe, Änderungen an privilegierten Rollen) und automatisierte Reaktion (z. B. Konto sperren, Sitzungen widerrufen). Gewertet wird nur, wenn die Leistung in den Preisen der Pos. 1.1, 1.2 und 3.1 bis 3.4 enthalten ist; Einzelheiten zu Leistungsumfang und Preisbezug in der Bewertungsmatrix. Voraussetzungen auf Seiten des Auftraggebers (z. B. bestimmte Microsoft-Lizenzen) sind im Angebot anzugeben. - **[B10]** Überwachung des lokalen Active Directory (2 Domänencontroller): Erkennung typischer Angriffe auf das Active Directory (z. B. Kerberoasting, DCSync, Pass-the-Hash, Golden Ticket, Änderungen an privilegierten Gruppen) und automatisierte Reaktion (z. B. Konto deaktivieren). Gewertet wird nur, wenn die Leistung in den Preisen der Pos. 1.1, 1.2 und 3.1 bis 3.4 enthalten ist; Einzelheiten zu Leistungsumfang und Preisbezug in der Bewertungsmatrix. Voraussetzungen auf Seiten des Auftraggebers (z. B. Sensoren auf den Domänencontrollern, Dienstkonten, Lizenzen) sind im Angebot anzugeben. Vorfallreaktion und -behebung: - **[A]** Der Auftragnehmer übernimmt die Vorfallbehandlung und meldet nicht nur. Im Pauschalpreis (Pos. 1) enthalten sind: Triage und Bewertung jeder Erkennung, Eindämmung (z. B. Isolierung, Prozessbeendigung, Sperrung), Bereinigung per Fernzugriff sowie eine Abschlussdokumentation je Vorfall. - **[A]** Incident-Response-Grundkontingent: Für Leistungen über den Pauschalumfang hinaus hält der Auftragnehmer je Vertragsjahr ein Grundkontingent von 40 Stunden vor (Pos. 5.1). Dazu gehören insbesondere forensische Untersuchungen, Einsätze vor Ort, Neuaufbau und Wiederherstellung von Systemen sowie Unterstützung bei der Kommunikation mit Behörden und Versicherern. Der Auftraggeber ruft das Kontingent in Textform ab. Der Auftragnehmer beginnt innerhalb von 4 Stunden nach Abruf mit der Leistung per Fernzugriff und ist bei Bedarf innerhalb von 24 Stunden vor Ort. Die verbrauchten Stunden weist er im Vorfallbericht aus. - **[A]** Erweiterung des Kontingents: Reicht das Grundkontingent nicht aus, kann der Auftraggeber es nach Abstimmung mit seinem Cyberversicherer zu den Stundensätzen der Pos. 5.2 erweitern. Der Auftragnehmer zeigt an, wenn 80 % des Kontingents verbraucht sind. Darüber hinausgehende Leistungen erbringt er nur nach Freigabe in Textform. Unaufschiebbare Maßnahmen zur Schadensabwehr setzt er bis zur Freigabe fort, höchstens jedoch für 8 Stunden. Benennt der Cyberversicherer einen eigenen Incident-Response-Dienstleister, arbeitet der Auftragnehmer mit diesem zusammen und übergibt ihm alle relevanten Erkenntnisse und Daten. - **[A]** Nicht verbrauchte Stunden des Grundkontingents kann der Auftraggeber bis zum Ende des Vertragsjahres für vorbeugende Leistungen abrufen (z. B. Notfallübung, Compromise Assessment); danach verfallen sie.			

	- **[A]** Eskalationsmatrix: Der Auftragnehmer darf Clients und als „unkritisch“ gekennzeichnete Server ohne vorherige Rücksprache isolieren. Vom Auftraggeber als „kritisch“ gekennzeichnete Server werden erst nach Freigabe isoliert, es sei denn, der Auftraggeber ist innerhalb von 15 Minuten nicht erreichbar und eine Ausbreitung droht. Die Matrix wird beim Onboarding gemeinsam festgelegt. - **[A]** Einhaltung der Service Level nach „Anlage zum Leistungsverzeichnis: Service-Level“ - **[A]** Export von Alarmen und Ereignissen in ein SIEM des Auftraggebers über eine dokumentierte Schnittstelle (z. B. Syslog, REST-API); das Format oder die unterstützten SIEM-Lösungen (z. B. Elastic, Wazuh, Splunk, IBM QRadar) sind im Angebot zu benennen. Bereitstellung, Management und Integration: - **[B3]** Anpassbare Dashboards und Berichte - **[A]** Zentrale Management-Konsole mit rollenbasierter Zugriffskontrolle (RBAC) und Mehr-Faktor-Authentifizierung - **[A]** Automatische Priorisierung von Alarmen, um Fehlalarme (False Positives) zu reduzieren und eine Alarmflut zu vermeiden - **[A]** Monatlicher Bericht über Erkennungen, Vorfälle, Einhaltung der Service Level und Status der Agenten - **[A]** Fernzugriffe auf Endpunkte (z. B. Remote Shell) werden vollständig protokolliert; Zugriffe auf kritische Server erfolgen nach der Eskalationsmatrix. - **[A]** Kompatibilität mit dem internen Schwachstellenscanner des Auftraggebers (derzeit Greenbone; bei einem Wechsel ein gleichwertiges Produkt): Für den Scanner lassen sich Ausnahmen auf Hostebene konfigurieren (z. B. über IP-Adresse oder Hostnamen), sodass authentifizierte und nicht authentifizierte Scans weder blockiert werden noch zur Isolierung des gescannten Endpunkts führen. Die Ausnahmen lassen sich auf einzelne Endpunkte oder Endpunktgruppen beschränken und gelten nur für den Scanner; der Schutz gegenüber allen anderen Quellen bleibt unverändert. Die Scan-Aktivitäten werden weiterhin protokolliert, aber nicht als Vorfall eskaliert. Scanzeiten und Ausnahmen werden beim Onboarding gemeinsam festgelegt. Leistung und Skalierbarkeit: - **[A]** Geringe Belastung der Endpunkte: im Normalbetrieb mit aktivem Echtzeitschutz (ohne laufenden Vollscan) durchschnittlich höchstens 5 % CPU-Last und 500 MB Arbeitsspeicher, gemessen über 24 Stunden auf dem Referenzsystem „ThinkBook 16 G7 ARP (AMD Ryzen 5 7535HS, 16GB DDR5-4800MT/s)“. Der Auftraggeber kann die Einhaltung während des Rollouts prüfen. - **[A]** Skalierbarkeit auf mindestens 2.500 Endpunkte ohne Wechsel der Plattform Datenverarbeitung, Datensouveränität und Ausschluss von Drittstaatenzugriffen (insbesondere U.S. CLOUD Act): Es gelten die Begriffsbestimmungen der Zusatzvereinbarung, insbesondere für „Drittstaat“ und „Vertragsdaten“. - **[A]** Verarbeitung, Speicherung und Sicherung sämtlicher Vertragsdaten ausschließlich in Rechenzentren innerhalb der EU/des EWR; Zugriffe auf Vertragsdaten von außerhalb der			

	EU/des EWR nur nach Ziffer 3 und 7 der Zusatzvereinbarung - **[A]** Datei-Samples werden nur an Analysedienste innerhalb der EU/des EWR übermittelt; Funktionen, die Vertragsdaten an Stellen außerhalb der EU/des EWR übermitteln, sind deaktivierbar und standardmäßig deaktiviert. - **[A]** Keine Nutzung von Vertragsdaten für eigene Zwecke des Auftragnehmers oder des Herstellers, insbesondere nicht zum Training von KI-Modellen; ausgenommen sind anonymisierte Erkennungsmerkmale ohne Personenbezug (z. B. Hashwerte, IOCs) - **[A]** Zusicherung zum Ausschluss von Drittstaatenzugriffen nach Ziffer 4 der Zusatzvereinbarung oder, soweit diese nicht abgegeben werden kann, Darlegung gleichwertiger Ersatzmaßnahmen nach Ziffer 4a der Zusatzvereinbarung. Die Inanspruchnahme von Ziffer 4a ist kein Ausschlussgrund; die Maßnahmen werden nach [B4] bis [B6] bewertet. - **[B4]** Weder der Bieter noch der Hersteller der eingesetzten Plattform noch ein wesentlicher Unterauftragsverarbeiter wird von einem Unternehmen mit Sitz in einem Drittstaat beherrscht. Begriffsbestimmungen und Bewertung nach der Bewertungsmatrix. - **[A]** Offenlegung sämtlicher Unterauftragsverarbeiter (insbesondere Hersteller der EDR-/XDR-Plattform, Hosting, Log-Speicherung, Threat-Intelligence-Zulieferer) einschließlich Sitz, Konzernzugehörigkeit und Verarbeitungsort - **[A]** Offenlegung der Standorte des SOC-Personals mit administrativem oder inhaltlichem Zugriff auf Vertragsdaten, einschließlich der jeweils anwendbaren Rechtsordnung - **[B5]** Zugriff auf Vertragsdaten ausschließlich durch Personal von Gesellschaften mit Sitz in der EU/im EWR, das keinen Weisungen einer Gesellschaft mit Sitz in einem Drittstaat unterliegt (einschließlich Hersteller-Support) - **[B6]** Schlüsselhoheit des Auftraggebers oder eines von ihm benannten, in der EU ansässigen Treuhänders (Bring/Hold Your Own Key) für die gespeicherten Vertragsdaten - **[A]** Meldung von Sicherheitsvorfällen beim Auftragnehmer oder seinen Unterauftragsverarbeitern (z. B. Kompromittierung der MDR-Plattform) und von Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung. Für Angriffe auf die Systeme des Auftraggebers gelten die Service Level nach „Anlage zum Leistungsverzeichnis: Service-Level“. - **[B7]** Kürzere Meldefrist als 24 Stunden für die vorgenannten Vorfälle - **[A]** Zugriff auf Inhaltsdaten (z. B. Dateiinhalte, E-Mails, Dokumente) – im Unterschied zu Metadaten und Telemetrie (z. B. Prozess-, Netzwerk- und Dateiereignisse, Hashwerte) – nur im begründeten Einzelfall zur Aufklärung eines konkreten Sicherheitsvorfalls; jeder solche Zugriff wird protokolliert und dem Auftraggeber im Vorfallbericht offengelegt. - **[A]** Unterzeichnung der Zusatzvereinbarung und Vorlage eines Auftragsverarbeitungsvertrags (AVV) nach Art. 28 DSGVO, der die Mindestinhalte nach „Anlage zum Leistungsverzeichnis: Mindestinhalte des Auftragsverarbeitungsvertrags“ erfüllt			

	Aufbewahrung von Daten: - **[A]** Vorhaltung der Telemetrie-Rohdaten für mindestens 90 Tage, durchsuchbar in der Konsole - **[A]** Vorhaltung von Alarmen, Vorfällen und Vorfallberichten für mindestens 12 Monate Compliance und Zertifizierungen des Anbieters: - **[A]** Für die genutzte Cloud-Infrastruktur und die MDR-Plattform: BSI-C5-Testat (Typ 1 oder Typ 2) oder ein gleichwertiger Nachweis, insbesondere ein ISO/IEC-27001-Zertifikat, dessen Geltungsbereich die angebotene Leistung umfasst, ausgestellt von einer nach ISO/IEC 17021-1 akkreditierten Stelle; Ausstellungsdatum bzw. Ende des Prüfzeitraums nicht älter als 24 Monate - **[B8]** BSI-C5-Testat Typ 2 oder gleichwertiger Nachweis; Bewertung nach der Bewertungsmatrix - **[A]** Zertifizierung nach ISO/IEC 27001 für den SOC-Betrieb des Auftragnehmers oder gleichwertiger Nachweis - **[A]** Penetrationstests der MDR-Plattform durch unabhängige Dritte mindestens jährlich; eine Zusammenfassung der Ergebnisse wird auf Anforderung vorgelegt - **[A]** Jährlicher Transparenzbericht zu behördlichen Anordnungen von Drittstaaten nach Ziffer 9 der Zusatzvereinbarung Reaktion und menschliche Unterstützung: - **[A]** Security Operations Center (SOC) rund um die Uhr (24/7/365) telefonisch erreichbar, einschließlich Fernwartungsfunktionen - **[A]** Unterstützung bei Onboarding und Rollout: Die Verteilung der Agenten übernimmt der Auftraggeber mit seinem Softwareverteilungswerkzeug „ACMP“. Der Auftragnehmer stellt die Installationspakete bereit (Option für „Silent install“ ohne Benutzerinteraktion muss vorhanden sein), erstellt gemeinsam mit dem Auftraggeber Richtlinien und eine sichere Grundkonfiguration nach Herstellerempfehlung und begleitet die Inbetriebnahme. Der Rollout ist spätestens sechs Wochen nach Laufzeitbeginn abzuschließen; bis dahin bleibt die bisherige Schutzlösung des Auftraggebers in Betrieb. - **[A]** Isolierung und Sperrung (Lockdown) betroffener Geräte nach der Eskalationsmatrix - **[A]** Fester Ansprechpartner (Account-Manager) und regelmäßige Security Reviews per Videokonferenz mit Sicherheitsfachleuten des Auftragnehmers (mindestens vierteljährlich) Exit-Management: - **[A]** Die Exit-Phase beginnt mit Zugang einer Kündigung, spätestens jedoch drei Monate vor dem regulären Vertragsende bzw. vor Ablauf der zuletzt ausgeübten Option. - **[A]** Auf Verlangen des Auftraggebers führt der Auftragnehmer den Betrieb über das Vertragsende hinaus für bis zu drei Monate zu den Preisen der Pos. 6 fort (Übergangsbetrieb). - **[A]** Datenexport der Alarme, Vorfälle und Vorfallberichte der letzten 12 Monate sowie der vorhandenen Telemetrie in einem offenen, maschinenlesbaren Format (z. B. JSON, CSV, STIX) mit Feldbeschreibung			

	- **[A]** Herausgabe der für den Auftraggeber konfigurierten Richtlinien, Playbooks und Ausnahmeregelungen in einem offenen, maschinenlesbaren Format; Standard-Playbooks des Herstellers sind ausgenommen - **[A]** Übergabe der Daten spätestens vier Wochen nach Beginn der Exit-Phase, bei außerordentlicher Kündigung spätestens vier Wochen nach Zugang der Kündigung; Aktualisierung zum Vertragsende bzw. zum Ende des Übergangsbetriebs - **[A]** Löschung sämtlicher Vertragsdaten beim Auftragnehmer und seinen Unterauftragsverarbeitern innerhalb von 30 Tagen nach Bestätigung des vollständigen Datenempfangs durch den Auftraggeber; Bestätigung der Löschung in Textform - **[A]** Bereitstellung von Werkzeugen bzw. Anleitung zur rückstandsfreien Deinstallation der Agenten einschließlich Deaktivierung des Manipulationsschutzes **Mit dem Angebot vorzulegende Unterlagen (zwingend; die Nachforderung richtet sich nach § 41 UVgO):** - Eigenerklärung zum Verarbeitungsort (EU/EWR) sämtlicher Vertragsdaten einschließlich Datei-Samples und Threat-Intelligence-Abgleichen - Software Bill of Materials (SBOM) für den Endpunkt-Agenten im Format CycloneDX oder SPDX; ersatzweise verbindliche Erklärung, dass die SBOM dem Auftraggeber nach Zuschlag unter Vertraulichkeitsvereinbarung bereitgestellt wird - Nur wenn nicht vollständig beim Auftraggeber On-Premise betrieben (im Sinne von [B8] Buchstabe (c) der Bewertungsmatrix): BSI-C5-Testat oder gleichwertiger Nachweis gemäß Abschnitt „Compliance und Zertifizierungen“ (nicht älter als 24 Monate) - ISO/IEC-27001-Zertifikat für den SOC-Betrieb oder gleichwertiger Nachweis - Liste der eingesetzten Unterauftragsverarbeiter mit Sitz, Konzernzugehörigkeit und Verarbeitungsort - Konzern- und Beteiligungsübersicht des Bieters und des Plattform-Herstellers; bei Konzernbezug zu Drittstaaten mit Angabe der beherrschenden Gesellschaft - Standortübersicht des SOC-Personals mit Zugriffsrechten auf Vertragsdaten - Ausgefüllte Funktionsmatrix Betriebssysteme (Anlage zum Leistungsverzeichnis: Funktionsmatrix Betriebssysteme) mit Erläuterung jeder Angabe „E“ - Beschreibung des Update-Verfahrens (gestaffelte Auslieferung, wählbare Agent-Versionen) - Auftragsverarbeitungsvertrag des Bieters, der die Mindestinhalte nach „Anlage zum Leistungsverzeichnis: Mindestinhalte des Auftragsverarbeitungsvertrags“ erfüllt - Unterzeichnete Zusatzvereinbarung Datensouveränität / CLOUD Act; soweit der Bieter die Zusicherung nach deren Ziffer 4 nicht abgeben kann, zusätzlich die Darlegung nach Ziffer 4a - Erklärungen und Nachweise zu den Wertungskriterien [B1] bis [B10]			
1.1	Managed Extended Detect and Response (MXDR) gemäß Pos. 1 – **Server**, 1. Vertragsjahr (01.01.–31.12.2027), Preis je Endgerät und Jahr	**70 Stück**		

1.2	Managed Extended Detect and Response (MXDR) gemäß Pos. 1 – **Clients**, 1. Vertragsjahr, Preis je Endgerät und Jahr	**340 Stück**		
2	Onboarding: Einrichtung, Richtlinien, Begleitung des Rollouts gemäß Pos. 1 (einmalig)	**1 pauschal**		
3.1	**Option** 2. Vertragsjahr – Server, Preis je Endgerät und Jahr	**70 Stück**		
3.2	**Option** 2. Vertragsjahr – Clients, Preis je Endgerät und Jahr	**340 Stück**		
3.3	**Option** 3. Vertragsjahr – Server, Preis je Endgerät und Jahr	**70 Stück**		
3.4	**Option** 3. Vertragsjahr – Clients, Preis je Endgerät und Jahr	**340 Stück**		
4.1	Unterjährige Erweiterung – zusätzlicher Server, Preis je Endgerät und angefangenem Monat; höchstens ein Zwölftel des Einheitspreises der Pos. 1.1 bzw. im Optionsjahr der Pos. 3.1 oder 3.3 (kein Abnahmeanspruch)	**1 Gerät**		
4.2	Unterjährige Erweiterung – zusätzlicher Client, Preis je Endgerät und angefangenem Monat; höchstens ein Zwölftel des Einheitspreises der Pos. 1.2 bzw. im Optionsjahr der Pos. 3.2 oder 3.4 (kein Abnahmeanspruch)	**1 Gerät**		
5.1	Incident-Response-Grundkontingent gemäß Pos. 1 (40 Stunden je Vertragsjahr einschließlich eventueller Reise- und Nebenkosten), pauschal je Vertragsjahr; der Preis gilt auch für die Optionsjahre	**3 Vertrags-jahre**		
5.2	Erweiterung des Incident-Response-Kontingents nach Pos. 5.1, auf Abruf, je Stunde einschließlich Reise- und Nebenkosten (Schätzmenge, kein Abnahmeanspruch)	**40 Stunden**		
6	**Option**: Übergangsbetrieb nach Vertragsende (Exit), alle Endgeräte, je Monat (Schätzmenge)	**3 Monate**		
			Netto-Angebots-summe (alle Pos.):	
			19 % MwSt.	
			Angebots-summe (brutto):	

Anmerkung:
Eventuelle Preisnachlässe sowie Skonti sind im Angebotsvordruck gesondert anzubieten. Die Netto-Angebotssumme aller Positionen einschließlich Optionen, Schätz- und Bedarfspositionen ist die Wertungssumme für das Kriterium Preis (Bewertungsmatrix). Aus Options- und Bedarfspositionen ergibt sich kein Anspruch auf Abnahme.

Rechtsfolgen bei Nichteinhaltung der Leistungsanforderungen
Die in der Anlage „Service Level" vorgesehenen Gutschriften bei Nichteinhaltung der vereinbarten Service Levels stellen eigenständige vergütungsbezogene Rechtsfolgen dar. Sie werden auf die Vertragsstrafe gemäß Nr. 10 der Zusatzvereinbarung nicht angerechnet.
Die Begrenzung der Vertragsstrafe gemäß Nr. 10 der Zusatzvereinbarung auf 10 % der Jahresvertragssumme gilt ausschließlich für die dort geregelte Vertragsstrafe. Die Begrenzung der Gutschriften auf 15 % der jeweiligen monatlichen Vergütung gemäß Anlage „Service Level" bleibt hiervon unberührt.
SLA-Gutschriften und Vertragsstrafe können bei Vorliegen der jeweiligen Voraussetzungen nebeneinander geltend gemacht werden. Die gesetzlichen und vertraglichen Voraussetzungen im Übrigen bleiben unberührt.

Anlage zum Leistungsverzeichnis: Service Level

Die Fristen beginnen mit der Erzeugung des Alarms in der Plattform und laufen rund um die Uhr, sofern nicht „Werktag“ angegeben ist (Werktage: Montag bis Freitag außer gesetzliche Feiertage in Schleswig-Holstein). Die Einstufung erfolgt durch den Auftragnehmer nach den folgenden Kategorien; der Auftraggeber kann eine höhere Einstufung verlangen.

Priorität	Beispiele	Benachrichtigung des Auftraggebers	Beginn der Eindämmung	Statusmeldungen
Kritisch	Aktive Kompromittierung, Ransomware, laterale Bewegung, Angriff auf kritische Server	15 Minuten (telefonisch und in Textform)	30 Minuten	stündlich bis zur Eindämmung
Hoch	Bestätigte Schadsoftware ohne Ausbreitung, kompromittiertes Benutzerkonto	1 Stunde	4 Stunden	alle 4 Stunden
Mittel	Verdächtige Aktivität, unerwünschte Anwendung mit Risiko	4 Stunden	nächster Werktag	im Vorfallbericht
Niedrig	Richtlinienverstöße, potenziell unerwünschte Programme	nächster Werktag (Sammelmeldung zulässig)	nach Absprache	im Monatsbericht

Weitere Service Level

- Verfügbarkeit der Management-Konsole und der Erkennungsplattform: mindestens 99,5 % im Kalendermonat, ausgenommen angekündigte Wartungsfenster von insgesamt höchstens 4 Stunden im Monat außerhalb Montag bis Freitag 7 bis 16 Uhr
- Telefonische Erreichbarkeit des SOC: rund um die Uhr; Rückruf spätestens nach 30 Minuten
- Nachweis: Der Auftragnehmer weist die Einhaltung im Monatsbericht anhand der Zeitstempel aus Plattform und Ticketsystem nach.

Gutschriften bei Nichteinhaltung

- Je Überschreitung einer Frist der Priorität „Kritisch“: 2 % der monatlichen Vergütung
- Je Überschreitung einer Frist der Priorität „Hoch“: 1 % der monatlichen Vergütung
- Verfügbarkeit unter 99,5 %: 2 % der monatlichen Vergütung je angefangene 0,5 Prozentpunkte Unterschreitung

Die Gutschriften sind auf 15 % der monatlichen Vergütung begrenzt. Weitergehende Ansprüche bleiben unberührt; Gutschriften werden auf Schadensersatzansprüche angerechnet. Überschreitet der Auftragnehmer in drei aufeinanderfolgenden Monaten jeweils eine Frist der Priorität „Kritisch“, kann der Auftraggeber den Vertrag aus wichtigem Grund kündigen.

Verhältnis zu sonstigen vertraglichen Rechtsfolgen

Die SLA-Gutschriften gemäß dieser Anlage gelten unabhängig von der Vertragsstrafe gemäß Nr. 10 der Zusatzvereinbarung. Im Übrigen gilt die Regelung zum Verhältnis von SLA-Gutschriften und Vertragsstrafe im Leistungsverzeichnis.

Anlage zum Leistungsverzeichnis: Bewertungsmatrix

Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt (§ 43 UVgO). Gewertet werden nur Angebote, die alle Mindestanforderungen [A] erfüllen.

- Preis: 60 Punkte
- Qualität/Leistung: 40 Punkte

Preiswertung (maximal 60 Punkte)
Grundlage der Preiswertung ist die Wertungssumme des Angebots in Euro netto (ohne Umsatzsteuer).
Das Angebot mit der niedrigsten Wertungssumme erhält 60 Punkte. Für die übrigen Angebote wird die Preisabweichung zum Bestpreis ermittelt und ins Verhältnis zum Bestpreis gesetzt. Der daraus resultierende Punktabzug wird von der Höchstpunktzahl abgezogen.

Formel:
Punktabzug = (Preisabweichung × 60) ÷ Bestpreis
Preiswertung = 60 − Punktabzug
Die Preiswertung beträgt **mindestens 0 Punkte**.

Beispiel:

- Bieter A: 40.000 € netto (Bestpreis)
- Bieter B: 55.000 € netto
- Preisabweichung: 15.000 €

Berechnung des Punktabzugs für Bieter B: 15.000 € × 60 Punkte ÷ 40.000 € = 22,5 Punkte

Preiswertung Bieter B: 60 Punkte − 22,5 Punkte = **37,5 Punkte**

Bieter A erhält 60 Punkte, Bieter B erhält 37,5 Punkte.

Qualitätswertung (maximal 40 Punkte)
Die Qualität bzw. Leistung wird anhand der Kriterien B1 bis B10 bewertet. Die Kriterien werden zunächst gemäß der nachfolgenden Bewertungsmatrix mit insgesamt maximal 100 Bewertungspunkten bewertet.
Die erreichte Punktzahl wird anschließend mit dem Faktor 0,4 multipliziert. Damit können maximal 40 Qualitätspunkte erreicht werden.

Nr.	Kriterium	max. Punkte	Bewertungsmaßstab
B1	Funktionsumfang unter Linux nach Funktionsmatrix (Anlage zum Leistungsverzeichnis: Funktionsmatrix Betriebssysteme)	10	Für jede Linux-Spalte der Funktionsmatrix (Ubuntu, Debian, SUSE SLES) wird ein Erfüllungsgrad berechnet. Jede der Funktionen 1 bis 18 erhält für die Angabe „J“ 1 Punkt, für „E“ 0,5 Punkte und für „N“ 0 Punkte. Der Erfüllungsgrad ist die Summe dieser Punkte geteilt durch 18. Maßgeblich ist die Spalte mit dem niedrigsten Erfüllungsgrad. Der Erfüllungsgrad wird nicht gerundet. 10 = mindestens 90 %; 5 = mindestens 75 % und weniger als 90 %; 2 = mindestens 50 % und weniger als 75 %; 0 = weniger als 50 % Eine Angabe „E“ ohne Erläuterung wird wie „N“ gewertet. Unterscheiden sich die Versionen innerhalb einer Spalte (z. B. Ubuntu 24.04 und 26.04), ist die jeweils ungünstigere Angabe einzutragen und zu erläutern. Beispiel: 15 × J, 2 × E, 1 × N → (15 + 1) ÷ 18 = 88,9 % → 5 Punkte **Nachweis:** ausgefüllte Funktionsmatrix mit Erläuterung jeder Angabe „E“
B2	Unabhängige Testergebnisse (letzte 24 Monate)	5	Anerkannt werden Tests und Zertifizierungen von AV-TEST, AV-Comparatives und SE Labs sowie gleichwertigen Prüfinstituten. Gleichwertig ist ein Institut, das mit dem Hersteller nicht verbunden ist (§ 15 AktG) und Prüfmethodik und Ergebnisse öffentlich zugänglich macht. Vom Hersteller in Auftrag gegebene Einzelgutachten (Auftragsstudien) und die MITRE ATT&CK Evaluations werden nicht gewertet. Maßgeblich ist das Veröffentlichungsdatum; es darf höchstens 24 Monate vor Ablauf der Angebotsfrist liegen. 5 = das angebotene Produkt (gleiche Produktlinie) wurde in einem Test für Unternehmensprodukte zertifiziert oder hat ihn bestanden; 2 = zertifiziert bzw. bestanden hat nur ein anderes Produkt des Herstellers mit derselben Erkennungs-Engine (z. B. Privatkundenprodukt) oder nur eine einzelne Komponente; 0 = sonst, insbesondere bloße Teilnahme ohne Zertifizierung oder Bestehen **Nachweis:** Link zum Testbericht und Angabe der Fundstelle
B3	Anpassbare Dashboards und Berichte	5	5 = der Auftraggeber kann selbst, ohne Mitwirkung des Auftragnehmers, (a) eigene Dashboards mit frei wählbaren Kennzahlen bzw. Elementen und Filtern (mindestens Zeitraum, Gerätegruppe, Schweregrad) anlegen, (b) eigene Berichte mit frei wählbaren Inhalten erstellen und (c) Berichte zeitgesteuert erzeugen und als PDF oder CSV exportieren; 2 = nur vordefinierte Dashboards bzw. Berichte, die mindestens nach Zeitraum und Gerätegruppe gefiltert werden können, oder Anpassungen nur durch den Auftragnehmer auf Anforderung; 0 = sonst **Nachweis:** Produktdokumentation oder Screenshots; Prüfung in der Teststellung vorbehalten

Nr.	Kriterium	max. Punkte	Bewertungsmaßstab
B4	Keine Beherrschung durch Unternehmen mit Sitz in einem Drittstaat	20	**Beherrschung:** Ein Unternehmen wird beherrscht, wenn ein anderes Unternehmen unmittelbar oder mittelbar (a) die Mehrheit der Anteile oder Stimmrechte hält, (b) die Mehrheit der Mitglieder des Leitungs- oder Aufsichtsorgans bestellen kann oder (c) auf andere Weise beherrschenden Einfluss im Sinne des § 17 AktG ausüben kann (z. B. durch einen Beherrschungsvertrag). Zu betrachten ist die gesamte Beteiligungskette bis zur obersten Muttergesellschaft. Ein Unternehmen hat seinen Sitz in einem Drittstaat, wenn sein satzungsmäßiger Sitz oder seine Hauptverwaltung in einem Drittstaat liegt. **Hersteller:** der Inhaber der Rechte an der angebotenen EDR-/XDR-Plattform und, falls abweichend, der Betreiber ihres Cloud-Backends. **Wesentlicher Unterauftragsverarbeiter:** jeder Unterauftragsverarbeiter, der Vertragsdaten speichert, Zugriff auf Vertragsdaten im Klartext hat oder Systeme mit Vertragsdaten administriert, insbesondere Hosting bzw. Rechenzentrumsbetrieb, Log-Speicherung, ausgelagerter SOC-Betrieb und Sample-Analyse. Nicht wesentlich sind Unterauftragsverarbeiter, die ausschließlich anonymisierte Erkennungsmerkmale im Sinne der Ziffer 2 der Zusatzvereinbarung erhalten. 20 = weder Bieter noch Hersteller noch ein wesentlicher Unterauftragsverarbeiter wird von einem Unternehmen mit Sitz in einem Drittstaat beherrscht; 8 = der Bieter nicht, jedoch der Hersteller und/oder mindestens ein wesentlicher Unterauftragsverarbeiter; 0 = der Bieter selbst. Bei Bietergemeinschaften gilt jedes Mitglied als Bieter. Ist der Bieter zugleich Hersteller, wird er als Bieter gewertet. **Nachweis:** Konzern- und Beteiligungsübersicht bis zur obersten Muttergesellschaft, Eigenerklärung, Liste der Unterauftragsverarbeiter
B5	Zugriff ausschließlich durch Personal in der EU/im EWR ohne Weisungsbindung an Drittstaaten-Gesellschaften	20	**Personal ohne Drittstaaten-Weisungsbindung:** Personen, die (a) bei einer Gesellschaft mit Sitz in der EU/im EWR beschäftigt sind, (b) sich beim Zugriff in der EU/im EWR aufhalten und (c) hinsichtlich des Zugriffs auf Vertragsdaten keinen fachlichen oder disziplinarischen Weisungen einer Gesellschaft mit Sitz in einem Drittstaat unterliegen. Die Konzernzugehörigkeit wird allein in B4 bewertet; der Bieter legt dar, wie die Weisungsfreiheit nach (c) vertraglich und organisatorisch abgesichert ist. Ziffer 7 der Zusatzvereinbarung regelt nur den Aufenthaltsort des Personals; B5 bewertet zusätzlich den Sitz des Arbeitgebers und die Weisungsfreiheit. **Hersteller-Support:** jede Tätigkeit von Personal des Herstellers oder seiner Dienstleister mit Zugriff auf Vertragsdaten, insbesondere 2nd/3rd-Level-Support und Fehleranalyse. **Plattformbetrieb:** Betrieb und Administration der Systeme, in denen Vertragsdaten gespeichert oder verarbeitet werden. **Einzelfreigabe:** vorherige Zustimmung einer vom Auftraggeber benannten Person in Textform für einen konkreten Supportfall, beschränkt auf die erforderlichen Daten und auf höchstens 72 Stunden. Ohne Freigabe ist der Zugriff technisch nicht möglich (z. B. Just-in-Time-Zugriff oder Customer Lockbox). Jeder Zugriff wird nach Ziffer 7 der Zusatzvereinbarung protokolliert. 20 = sämtliche Zugriffe durch SOC, Plattformbetrieb und Hersteller-Support erfolgen ausschließlich durch Personal ohne Drittstaaten-Weisungsbindung; 10 = SOC und Plattformbetrieb erfüllen dies, Hersteller-Support durch anderes Personal erfolgt nur nach Einzelfreigabe; 0 = alle übrigen Fälle (z. B. SOC mit Schichtbetrieb außerhalb der EU/des EWR) **Nachweis:** Standortübersicht des SOC-Personals, Beschreibung von Plattformbetrieb und Hersteller-Support einschließlich Freigabeverfahren, Darlegung zur Weisungsfreiheit

Nr.	Kriterium	max. Punkte	Bewertungsmaßstab
B6	Schlüsselhoheit beim Auftraggeber oder EU-Treuhänder	10	**Schlüsselhoheit:** Die Vertragsdaten werden im gespeicherten Zustand so verschlüsselt, dass der Schlüssel zur Entschlüsselung (Master- bzw. Key-Encryption-Key) ausschließlich in einem Schlüsselmanagementsystem oder HSM liegt, das der Auftraggeber oder ein Treuhänder betreibt. Weder Bieter noch Hersteller noch deren Unterauftragsverarbeiter können den Schlüssel im Klartext auslesen oder exportieren. Die Verarbeitung im Arbeitsspeicher während des Betriebs ist ausgenommen. **Treuhänder:** ein Unternehmen mit Sitz in der EU, das weder mit dem Bieter oder Hersteller verbunden ist (§ 15 AktG) noch nach B4 von einem Unternehmen mit Sitz in einem Drittstaat beherrscht wird und das gegenüber dem Auftraggeber weisungsgebunden ist. Ein solcher Treuhänder ist dem Auftraggeber gleichgestellt. **Jederzeitige Sperrbarkeit:** Der Auftraggeber (oder der Treuhänder auf seine Weisung) kann den Schlüssel ohne Mitwirkung des Auftragnehmers sperren. Spätestens 1 Stunde nach der Sperrung können Auftragnehmer, Hersteller und Unterauftragsverarbeiter die betroffenen Daten nicht mehr entschlüsseln. 10 = Schlüsselhoheit mit jederzeitiger Sperrbarkeit für alle gespeicherten Vertragsdaten, d. h. Telemetrie-Rohdaten, Alarme, Vorfälle und Vorfallberichte, Datei-Samples, Konfigurationsdaten sowie alle Sicherungen und Replikate; 5 = Schlüsselhoheit mit jederzeitiger Sperrbarkeit mindestens für die Telemetrie-Rohdaten und die Datei-Samples einschließlich ihrer Sicherungen; 0 = sonst. Werden sämtliche Vertragsdaten ausschließlich auf Infrastruktur des Auftraggebers gespeichert, gilt die Schlüsselhoheit als gegeben. Gewertet wird nur, wenn die Kosten für Schlüsselverwaltung und gegebenenfalls Treuhänder in den Preisen enthalten sind. Erforderliche Komponenten beim Auftraggeber sind anzugeben. **Nachweis:** Architekturbeschreibung mit abgedeckten Datenkategorien, Schlüsselhierarchie, eingesetztem KMS bzw. HSM und Ablauf der Sperrung
B7	Meldefrist für Vorfälle beim Auftragnehmer	5	Bewertet wird die verbindlich zugesagte Frist für die Erstmeldung der im Leistungsverzeichnis genannten Vorfälle (Sicherheitsvorfälle beim Auftragnehmer oder seinen Unterauftragsverarbeitern sowie Verletzungen des Schutzes personenbezogener Daten). Die Frist beginnt mit Kenntniserlangung, also dem Zeitpunkt, zu dem beim Auftragnehmer oder einem Unterauftragsverarbeiter hinreichende tatsächliche Anhaltspunkte für einen solchen Vorfall vorliegen; der Abschluss der Untersuchung ist nicht abzuwarten. Die Kenntnis eines Unterauftragsverarbeiters wird dem Auftragnehmer zugerechnet. Die Erstmeldung erfolgt telefonisch und in Textform und enthält mindestens die bekannten Umstände, die möglicherweise betroffenen Vertragsdaten und einen Ansprechpartner. 5 = höchstens 4 Stunden; 3 = mehr als 4 bis höchstens 12 Stunden; 0 = mehr als 12 bis höchstens 24 Stunden. Eine Frist von mehr als 24 Stunden erfüllt die Mindestanforderung nicht. Die angebotene Frist wird Vertragsbestandteil. **Nachweis:** verbindliche Erklärung im Angebot

Nr.	Kriterium	max. Punkte	Bewertungsmaßstab
B8	BSI-C5-Testat Typ 2 oder gleichwertiger Nachweis	5	5 = eine der folgenden Voraussetzungen ist erfüllt: (a) Es liegt ein BSI-C5-Testat Typ 2 nach C5:2020 oder C5:2026 vor, dessen Geltungsbereich die MDR-Plattform und die genutzte Cloud-Infrastruktur umfasst. Deckt ein Testat nur einen Teil ab, sind für die übrigen Teile weitere Nachweise nach (a) oder (b) vorzulegen. Das Ende des Prüfzeitraums liegt höchstens 24 Monate vor Ablauf der Angebotsfrist. (b) Es liegt ein gleichwertiger Nachweis vor. Gleichwertig ist ein Nachweis, der kumulativ (1) von einem unabhängigen, für die Prüfung qualifizierten Prüfer ausgestellt ist, (2) die Wirksamkeit der Kontrollen über einen Prüfzeitraum von mindestens 6 Monaten bestätigt, (3) Kriterien zugrunde legt, die die Basiskriterien und Umfeldparameter des C5 inhaltlich abdecken, und (4) als Prüfbericht mit Beschreibung der geprüften Kontrollen und etwaiger Abweichungen vorgelegt wird. Der Bieter weist die Gleichwertigkeit mit dem Angebot nach, z. B. durch eine Zuordnung zu den C5-Kriterien. Als gleichwertig gelten insbesondere eine mit dem C5 kombinierte SOC-2-Typ-2-Prüfung, eine gültige SecNumCloud-Qualifizierung der ANSSI und eine CSA STAR Level 2 Attestation (SOC-2-Typ-2-Prüfung ergänzt um die Cloud Controls Matrix); für diese entfällt die Darlegung nach Satz 2. Die Anforderungen an Geltungsbereich und Aktualität nach (a) gelten entsprechend. (c) Vollständiger On-Premise-Betrieb: Sämtliche Komponenten, die Vertragsdaten speichern oder verarbeiten (Management-Server, Telemetriespeicher, Analyse und Korrelation, Sample-Analyse, Log-Collector), laufen auf Infrastruktur des Auftraggebers. Vertragsdaten verlassen diese Infrastruktur nicht; ausgenommen sind der Fernzugriff des SOC, anonymisierte Erkennungsmerkmale und der Bezug von Updates. 0 = sonst. Nicht gleichwertig sind insbesondere C5-Testate Typ 1, Zertifikate nach ISO/IEC 27001, 27017 oder 27018 (auch in Verbindung mit der Cloud Controls Matrix, z. B. CSA STAR Level 2 Certification), SOC-2-Typ-2-Berichte ohne Ergänzung um C5 oder die Cloud Controls Matrix sowie hybride Betriebsmodelle ohne Nachweis nach (a) oder (b) für den Cloud-Anteil. **Nachweis:** Testat bzw. Prüfbericht einschließlich Beschreibung des Geltungsbereichs; bei (b) zusätzlich die Darlegung der Gleichwertigkeit, soweit kein genanntes Beispiel vorliegt; bei (c) Architekturbeschreibung

Nr.	Kriterium	max. Punkte	Bewertungsmaßstab
B9	Überwachung der Identitäten in Microsoft 365 / Entra ID	10	**Erkennung identitätsbasierter Angriffe:** Die Plattform des Auftragnehmers wertet die Anmelde-, Audit- und Risikoprotokolle aus Entra ID und Microsoft 365 laufend aus; die Alarme fließen in die Vorfallbehandlung des SOC einschließlich der Service Level ein. Erkannt werden mindestens: (1) verdächtige Anmeldungen (z. B. unmögliche Reise, anonymisierte IP-Adressen, Password Spraying), (2) Token- bzw. Sitzungsdiebstahl (z. B. AiTM-Phishing, Token-Replay), (3) MFA-Ermüdungsangriffe, (4) Änderungen an privilegierten Rollen und Rollenzuweisungen. Microsoft-eigene Erkennungen dürfen als Datenquelle genutzt werden, wenn sie korreliert und vom SOC triagiert werden; die bloße Weiterleitung genügt nicht. **Automatisierte Reaktion:** Die Reaktion wird nach den beim Onboarding festgelegten Regeln ohne manuellen Einzelschritt ausgelöst. Sie umfasst mindestens das Sperren des Kontos und den Widerruf aller Sitzungen und Refresh-Tokens. 10 = alle Szenarien werden erkannt, mit automatisierter Reaktion; 5 = alle Szenarien werden erkannt, die Reaktion erfolgt manuell durch das SOC innerhalb der Service Level; 0 = sonst **Preisbezug:** Gewertet wird nur, wenn die Leistung für alle 470 Benutzerkonten in den Preisen der Pos. 1.1, 1.2 und 3.1 bis 3.4 enthalten ist und keine weiteren Entgelte des Auftragnehmers oder Herstellers anfallen; die einmalige Einrichtung kann in Pos. 2 enthalten sein. Der Auftraggeber verfügt derzeit über Lizenzen für Microsoft Entra ID P1. Setzt die Leistung beim Auftraggeber weitere Lizenzen oder nutzungsabhängige Cloud-Kosten voraus (z. B. für die Datenaufnahme in einen Microsoft-Sentinel-Arbeitsbereich des Auftraggebers), wird sie mit 0 Punkten bewertet. **Nachweis:** Liste der Erkennungsregeln bzw. Dokumentation mit Zuordnung zu jedem geforderten Szenario; Prüfung in der Teststellung vorbehalten
B10	Überwachung des lokalen Active Directory	10	**Typische AD-Angriffe:** mindestens Kerberoasting, AS-REP-Roasting, DCSync, Pass-the-Hash, Pass-the-Ticket, Golden Ticket, Password Spraying bzw. Brute Force gegen AD-Konten sowie Änderungen an privilegierten Gruppen (mindestens Domänen-Admins, Organisations-Admins, Schema-Admins, Administratoren). **Über die EDR-Telemetrie hinausgehende Überwachung:** eine eigene AD-spezifische Erkennungslogik, die die Kerberos-, NTLM-, LDAP- und Replikationsaktivität beider Domänencontroller auswertet (über deren Ereignisprotokolle oder den Netzwerkverkehr). Die allgemeine Prozess- und Dateitelemetrie des EDR-Agenten auf den Domänencontrollern genügt nicht, auch wenn sie einzelne Angriffswerkzeuge erkennt. **Automatisierte Reaktion:** wie bei B9, mindestens die automatische Deaktivierung des betroffenen Kontos im lokalen Active Directory. 10 = alle Szenarien werden erkannt, mit automatisierter Reaktion; 5 = alle Szenarien werden erkannt, ohne automatisierte Reaktion; 0 = sonst **Preisbezug:** wie bei B9 (Pos. 1.1, 1.2 und 3.1 bis 3.4; einmalige Einrichtung in Pos. 2). Setzt die Leistung beim Auftraggeber weitere Lizenzen oder nutzungsabhängige Cloud-Kosten voraus (z. B. für die Datenaufnahme in einen Microsoft-Sentinel-Arbeitsbereich des Auftraggebers), wird sie mit 0 Punkten bewertet. **Nachweis:** wie bei B9

Grundlage der Bewertung sind die mit dem Angebot vorgelegten Erklärungen und Nachweise. Nicht belegte Angaben werden mit 0 Punkten bewertet. Maßgeblich für alle Wertungskriterien ist der Sachstand bei Ablauf der Angebotsfrist. Welche Nachweise je Kriterium vorzulegen sind, ist im jeweiligen Bewertungsmaßstab angegeben. Begriffe, die in der Zusatzvereinbarung bestimmt sind (insbesondere „Drittstaat“, „Vertragsdaten“, „Zugriff“), gelten auch für die Bewertungsmatrix. Die Angaben zu [B4] bis [B6] werden Vertragsbestandteil (Ziffer 4a der Zusatzvereinbarung).

Gesamtwertung

Die Gesamtpunktzahl ergibt sich aus der Summe der Preiswertung und der gewichteten Qualitätswertung.

Gesamtpunkte = Preiswertung + (Qualitätspunkte × 0,4)

Es können insgesamt maximal 100 Punkte erreicht werden.

Bei Punktgleichheit erhält das Angebot mit der niedrigeren Wertungssumme den Zuschlag.

Anlage zum Leistungsverzeichnis: Mindestinhalte des Auftragsverarbeitungsvertrags

Der Bieter legt mit dem Angebot einen Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO vor. Der AVV muss mindestens die folgenden Inhalte enthalten; erfüllt er einen Mindestinhalt nicht, gilt dies als Nichterfüllung einer Mindestanforderung [A]. Redaktionelle Anpassungen und Konkretisierungen, die die Mindestinhalte nicht unterschreiten, können nach Zuschlag vereinbart werden.

- Pflichtinhalte nach Art. 28 Abs. 3 DSGVO: Gegenstand und Dauer, Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen, Weisungsgebundenheit, Vertraulichkeit, Unterstützung bei Betroffenenrechten und bei den Pflichten nach Art. 32 bis 36 DSGVO, Löschung bzw. Rückgabe, Nachweise und Kontrollen
- Ausdrückliche Benennung der Datenkategorien des MDR-Dienstes: Telemetrie (Prozess-, Netzwerk-, Datei- und Anmeldeereignisse), Benutzer- und Gerätekennungen, Datei-Samples sowie Inhaltsdaten im Einzelfall
- Technische und organisatorische Maßnahmen als Anlage, mindestens im Umfang der Ziffer 7 der Zusatzvereinbarung
- Liste der Unterauftragsverarbeiter als Anlage; Austausch oder Hinzuziehung nur mit vorheriger Zustimmung des Auftraggebers in Textform nach Ziffer 8 der Zusatzvereinbarung
- Kontrollrechte einschließlich Prüfungen vor Ort durch den Auftraggeber oder von ihm beauftragte Dritte
- Meldung von Verletzungen des Schutzes personenbezogener Daten spätestens innerhalb von 24 Stunden nach Kenntniserlangung
- Verarbeitung ausschließlich in der EU/im EWR; Übermittlung in Drittstaaten nur mit vorheriger Zustimmung des Auftraggebers im Einzelfall in Textform
- Keine Verarbeitung zu eigenen Zwecken des Auftragnehmers oder des Herstellers (z. B. Produktverbesserung, Training von KI-Modellen), ausgenommen anonymisierte Erkennungsmerkmale ohne Personenbezug
- Löschung innerhalb von 30 Tagen nach Vertragsende bzw. nach Bestätigung des Datenempfangs mit Löschbestätigung in Textform
- Keine Haftungsbeschränkungen, Vergütungsregelungen oder Verweise auf Allgemeine Geschäftsbedingungen, die die Pflichten nach Art. 28 DSGVO oder nach der Zusatzvereinbarung einschränken; Vorrang der Zusatzvereinbarung nach deren Ziffer 12

Anlage zum Leistungsverzeichnis: Funktionsmatrix Betriebssysteme

Der Bieter trägt für jede Funktion und jedes Betriebssystem ein: **J** = vollständig verfügbar, **E** = eingeschränkt verfügbar, **N** = nicht verfügbar. Jede Angabe „E“ ist in der Tabelle „Erläuterungen zu Angaben ‚E‘“ im Anschluss an die Funktionsmatrix zu erläutern. Reicht der Platz nicht aus, können Zeilen ergänzt oder ausführliche Erläuterungen als Anlage beigefügt werden, auf die in der Tabelle verwiesen wird. Die Angaben werden Vertragsbestandteil.

Der Auftraggeber behält sich vor, die Angaben vor Zuschlag in einer Teststellung bei den bestplatzierten Bietern sowie während des Rollouts zu prüfen. Erweisen sich Angaben vor Zuschlag als unzutreffend, kann das Angebot ausgeschlossen werden; nach Zuschlag ist der Auftraggeber zur außerordentlichen Kündigung berechtigt.

Bewertung nach [B1]: Die Berechnung ergibt sich abschließend aus der Bewertungsmatrix. Unterscheiden sich die Versionen innerhalb einer Spalte (z. B. Ubuntu 24.04 und 26.04), ist die jeweils ungünstigere Angabe einzutragen und zu erläutern. Eine Angabe „E“ ohne Erläuterung wird wie „N“ gewertet.

Nr.	Funktion	Windows 11	Windows Server 2019–2025	Ubuntu 24.04 & 26.04	Debian 12 & 13	SUSE SLES 15 & 16
1	Malware-Prävention in Echtzeit (signaturbasiert und Machine Learning)					
2	Verhaltensbasierte Erkennung von Prozessaktivitäten					
3	Erkennung und Blockierung ohne Cloudanbindung (lokales Erkennungsmodell)					
4	Schutz vor Ransomware einschließlich Wiederherstellung verschlüsselter Dateien					
5	Exploit- und Speicherschutz					
6	EDR-Telemetrie: Prozess-, Datei-, Netzwerk- und Anmeldeereignisse					
7	Threat Hunting (Abfragen über die gespeicherte Telemetrie)					
8	Isolierung des Endpunkts aus der Ferne					
9	Remote Response (Remote Shell, Dateien abrufen, Prozesse beenden)					
10	Automatisierte Eindämmung und Bereinigung (z. B. Quarantäne, Prozess beenden)					
11	Manipulationsschutz des Agenten (Tamper Protection)					
12	Integritätsüberwachung kritischer System- und Konfigurationsdateien					
13	Software- und Schwachstelleninventar (installierte Software, bekannte Schwachstellen)					
14	Gerätesteuerung (USB- und Wechseldatenträger)					
15	Verwaltung der Host-Firewall					
16	Gestaffelte Agent-Updates und Wahl der Agent-Version (mindestens N-1)					
17	Agent-Updates ohne Neustart des Systems					
18	Unterstützung neuer Kernel-Versionen ohne manuelle Anpassung (nur Linux)	–	–			

Erläuterungen zu Angaben „E“

Für jede Angabe „E“ in der Funktionsmatrix ist eine eigene Zeile auszufüllen. Gilt dieselbe Einschränkung für mehrere Betriebssysteme, genügt eine Zeile mit Angabe aller betroffenen Betriebssysteme. Anzugeben ist, worin die Einschränkung gegenüber der vollständigen Verfügbarkeit besteht. Die Erläuterungen werden Vertragsbestandteil.

Nr. der Funktion	Betroffene Betriebssysteme und Versionen	Art und Umfang der Einschränkung (was fehlt oder ist eingeschränkt, ggf. Verweis auf Anlage)