

Verfahren: 20261023 - Security Managed Services

LISTE DER ÖFFENTLICHEN NACHRICHTEN

Nr.	Frage	Antwort	Gesendet
1	Frage 1 Aufgrund der erheblichen Rechtsfolge eines Ausschlusses müssen sämtliche Ausschlusskriterien für die Bewerber eindeutig, vollständig und zweifelsfrei erkennbar sein. Wir bitten den Auftraggeber daher, alle Ausschlusskriterien einschließlich der jeweils erforderlichen Nachweise, Erfüllungszeitpunkte und etwaigen Nachreichungsmöglichkeiten in einer konsolidierten und abschließenden Übersicht bekanntzugeben. Bitte bestätigen Sie, dass Anforderungen, die in den Vergabeunterlagen nicht ausdrücklich und eindeutig als Ausschlusskriterium gekennzeichnet sind, nicht allein aufgrund einer Nichterfüllung oder eines fehlenden Nachweises zum Ausschluss des Teilnahmeantrags beziehungsweise Angebots führen. Frage 2 Ist es für die Erfüllung der Anforderung zur Zertifizierung nach DIN EN ISO 9001 ausreichend, wenn der Bewerber zum Zeitpunkt der Einreichung des Teilnahmeantrags nachweist, dass er sich bereits in einem verbindlich eingeleiteten Zertifizierungsverfahren bei einer akkreditierten Zertifizierungsstelle befindet, und die erfolgreiche Zertifizierung spätestens zum Beginn der Leistungserbringung nachweist? Bitte bestätigen Sie, dass in diesem Fall das noch nicht vorliegende Zertifikat zum Zeitpunkt des Teilnahmeantrags beziehungsweise der Zuschlagsentscheidung nicht zum Ausschluss führt, sofern das gültige Zertifikat spätestens vor Beginn der Leistungserbringung vorgelegt wird. ?	zu Frage 1 Beiliegende Übersicht "20261023 Auflistung Eignungskriterien SOC" gibt Auskunft darüber, welche Kriterien "K.O."-Kriterien sind und damit bei Nicht-Erfüllung zum Ausschluss aus dem weiteren Verfahren führen und welche Bewertungskriterien mit welcher Max.-Punktzahl belohnt werden. Wenn bei den Bewertungskriterien keine Punkte erreicht werden, dann führt die Nichterfüllung nicht zum Ausschluss, wirkt sich jedoch auf die Rangbildung im Teilnahmewettbewerb aus. Sind mehr als 4 (vier) Teilnehmer geeignet, dann entscheidet die Summe der Punkte aus den Bewertungskriterien über die weitere Teilnahme. Das Verfahren wird mit den Rängen 1 – 4 (höchste Punktzahl absteigend) fortgesetzt. Haben mehrere Teilnehmer die gleiche Punktzahl erreicht, dann entscheidet das Los. zu Frage 2 Antwort wird nachgereicht Anlagen: • 20261023 Auflistung Eignungskriterien SOC.pdf	10.09.2026 13:31:27
2	Frage 3 In Kapitel 4.12 "Abfrage zur Eignung" wird unter	siehe Antwort zu Frage 1	10.09.2026 13:31:27

4.12.2 darauf hingewiesen, dass alle nachfolgenden Kriterien Ausschlusskriterien sind.

*4.12.23. K.O.-Kriterien (Typ A) – Mindestanforderungen
Die nachfolgenden Kriterien sind Ausschlusskriterien. Bewerber, die ein oder mehrere Kriterien nicht erfüllen, werden vom weiteren Verfahren ausgeschlossen. Die Nichterfüllung kann nicht durch besondere Leistungen bei Bewertungskriterien (Typ B) kompensiert werden.*

Die dem Kapitel nachfolgenden Kriterien sind aber sowohl ohne Bewertung (als Ausschluss-Kriterium) als auch mit Punkte-Bewertung (als Bewertungs-Kriterium) ausgeführt.

Beispielsweise ist unter 4.12.5 eine Zertifizierung nach ISO/IEC 20000-1 gefordert, die mit 10 Punkten bewertet wird. Führt nun das Kriterium auch zum Ausschluss, wenn es nicht erfüllt wird, oder wird es nur bewertet?

Wir möchten Sie bitten, klar zu stellen, welche Kriterien zum Ausschluss führen und welche "nur" in die Bewertung einfließen.

3

Frage 6

In der Vergabeunterlage unter 4.12.5 (2a) wird eine gültige Zertifizierung nach ISO/IEC 20000-1 gefordert.

Kann der Auftraggeber auch andere geeignete und nachweisbare Zertifizierungen bzw. Managementsysteme, insbesondere ISO 9001, ISO 27001, ISO 27701 und C5 Typ 2, in Verbindung mit etablierten und nachweislich gelebten IT-Service-Management-Prozessen (gemäß ITIL) als gleichwertigen Nachweis anerkennen und hierfür die vorgesehenen Wertungspunkte vergeben?

Dies würde insbesondere Anbieter berücksichtigen, die durch kombinierte Managementsysteme und langjährige Erfahrung im Betrieb kritischer IT-Services die wesentlichen Anforderungen an ein strukturiertes, qualitätsgesichertes und kontinuierlich verbessertes IT-Service-Management nachweislich erfüllen.

Sehr geehrte Damen und Herren,

Wir lehnen die Anerkennung alternativer Zertifizierungen (wie ISO 9001, 27001) als gleichwertigen Nachweis ab. Der Nachweis einer ISO/IEC 20000-1 Zertifizierung ist zwingend erforderlich.

Ein aktuell noch nicht abgeschlossenes Zertifizierungsverfahren führt im jetzigen Stadium des Verhandlungsverfahrens jedoch nicht zum sofortigen Ausschluss. Das Angebot bleibt im Rahmen der vergaberechtlichen Eignung unter ausdrücklichem Vorbehalt im weiteren Verfahren zugelassen.

Bedingung für diese Zulassung ist ausschließlich, dass die gültige und erfolgreich abgeschlossene Zertifizierung nach ISO/IEC 20000-1 zwingend spätestens zur Angebotsabgabe über das Vergabeportal eingereicht wird.

Liegt das gültige Zertifikat zu diesem Zeitpunkt nicht vor, ist das Angebot zwingend wegen mangelnder Eignung vom weiteren Verfahren ausgeschlossen.

Mit freundlichen Grüßen,

Vergabeabteilung

Abt. 3.3

17.09.2026 10:43:31

4

Sehr geehrte Vergabestelle,

in der Übersicht der KO-Kriterien (pdf) welche am 10.09. zur Verfügung gestellt wurde, ist die ISO 20000-1 eindeutig als Bewertungskriterium definiert. Ihre Bieterantwort von heute sagt: "Der Nachweis

Sehr geehrte Damen und Herren,

wir bedanken uns für Ihren aufmerksamen Hinweis und möchten hiermit eine Korrektur unserer vorherigen Aussage vornehmen. Es lag unsererseits bedauerlicherweise ein Irrtum vor.

17.09.2026 13:51:56

einer ISO/IEC 20000-1 Zertifizierung ist zwingend erforderlich".

Wir bitten um eindeutige Klarstellung, sowie die zeitnahe Beantwortung der noch offenen Bieterfragen.

Die Übersicht der KO-Kriterien vom 10.09. ist korrekt. Bei der Zertifizierung ISO/IEC 20000-1 handelt es sich nicht um ein zwingendes Eignungskriterium. Sondern um ein Bewertungskriterium.

Der Nachweis einer gültigen Zertifizierung ist nicht zwingend für den Verbleib im Vergabeverfahren erforderlich. Ein Fehlen führt nicht zum Ausschluss.

Die Einreichung des Zertifikats dient ausschließlich der Punktevergabe in der Wertung. Sofern das Zertifikat zum Zeitpunkt der Angebotsabgabe nicht vorliegt, können in diesem Bewertungskriterium keine Punkte vergeben werden. Es steht Ihnen frei fehlende Punkte in diesem Kriterium durch entsprechende Leistungen in anderen Bewertungskriterien auszugleichen. Das Nachreichen des Zertifikats zu einem späteren Zeitpunkt ist im Rahmen der Angebotsbewertung nicht vorgesehen und führt auch nicht zu einer nachträglichen Punktevergabe.

Wir bitten, die vorherige missverständliche Kommunikation zu entschuldigen und hoffen die Sache hiermit eindeutig geklärt zu haben. Die Beantwortung der weiteren offenen Fragen erfolgt zeitnah.

Mit freundlichen Grüßen,

Vergabeabteilung

Abt. 3.3

5

Frage 8:

Sehr geehrte Damen und Herren,

zum laufenden Verfahren stellen wir folgende Bieterfrage:

Referenzanforderungen 2 und 3:

Zu den Anforderungen 4.12.12 (9a21) „Referenz 2 – SOC/MDR-Betrieb Krankenhaus 1“ sowie 4.12.14 (9a31) „Referenz 3 – SOC/MDR-Betrieb Krankenhaus 2“ bittet der Bieter um Erweiterung des zulässigen Referenzkreises, so dass für mind. eine der beiden geforderten Referenzen 4.12.12 und 4.12.14 (Bieterfrage bezieht sich nicht auf die Referenzangabe 4.12.11 – SOC/MDR-Betrieb im KRITIS-KH) auch Referenzen von kliniknahen Unternehmen im Gesundheitswesen zulässig sind. Es wird darum gebeten, die Anforderung dahingehend anzupassen, dass auch Referenzen von kliniknahen

zu Frage 8:

Sehr geehrte Damen und Herren,

Die Anforderung bleibt unverändert. Für die Referenzen 2 und 3 sind ausschließlich Referenzen aus Krankenhäusern mit mindestens 500 Betten zugelassen (D2, Ziffer 4.2).

mit freundlichen Grüßen,

Vergabeabteilung

Abt. 3.3

18.09.2026 13:11:35

Unternehmen im Gesundheitswesen als gleichwertig anerkannt werden, sofern die im Rahmen der Referenz erbrachten SOC-/MDR-Leistungen unmittelbar für Krankenhäuser bzw. Krankenhausverbünde, Unternehmen im Gesundheitswesen und der Pharmaindustrie erbracht werden und die zu überwachenden Systeme, Anwendungen und Prozesse dem Krankenhausbetrieb dienen.

6

Sehr geehrte Vergabestelle,
wir haben folgende Fragen:

1) Mit der Beantwortung der letzten Bieterfragen wurde ein BSI C5 Testat zum KO-Kriterium erklärt, sofern es sich nicht um eine On-prem Installation handelt. Da der Ausschreibungsgegenstand aus mehreren technischen Lösungskomponenten und Dienstleistungen besteht, bitten wir um Klarstellung für welche Teile ein BSI C5 Testat gefordert wird. Wird es vom Bieter und/oder den Herstellern der eingesetzten Cloud Lösungen gefordert? Insbesondere bitten wir um Aufklärung wie eine Gleichbehandlung von Bietern möglich ist, wenn eingesetzte Cloud-Lösungen wie bspw. Vectra nach unserem Kenntnisstand kein BSI C5 Testat besitzen, aber im Rahmen der Ausschreibung zur Verlängerung angeboten werden dürfen? Da die Ausschreibungsunterlagen explizit eine Trennung von Lizenz-Eigentümerschaft und Dienstleistung verlangen und es sich bei einem BSI C5 Testat um eine deutsche Zertifizierung für Cloud Dienste handelt, sehen wir aufgrund der sich daraus ergebenden Komplexität die Einhaltung des Gleichbehandlungsprinzips in einer europäischen Ausschreibung als schwierig umsetzbar an und möchten daher die Entfernung eines BSI C5 Testats als KO Kriterium vorschlagen.

2) Für die Realisierung der EDR und ggf SIEM Funktion kommt laut Ausschreibungsunterlage auch eine Microsoft-Lösung in Frage. Unserer Erfahrung nach, ist die Beschaffung der erforderlichen Lizenzen am wirtschaftlichsten, wenn sie sich durch ein oft bereits bestehendes Microsoft Enterprise License Agreement (ELA) erfolgt und somit die entsprechenden Angebotspositionen als optional deklariert werden und aus dem bewerteten Angebotspreis exkludiert werden. Ist diese Anpassung für die Vergabestelle akzeptabel?

Herzlichen Dank und beste Grüße

Sehr geehrte Damen und Herren,

EDR: Die Frage ist in den Vergabeunterlagen bereits geregelt (D1 Kap. 3.2 und 7.2). Stellt der Auftraggeber Microsoft Defender for Endpoint im Rahmen seiner Microsoft-Lizenzierung bereit, sind hierfür keine Produktlizenzen zu kalkulieren; sie sind nicht Bestandteil des wertungsrelevanten EDR-Basispreises.

SIEM: Eine Anpassung erfolgt nicht. Die SIEM-Plattformlizenz (Position LV 4.2, Basis 400 GB/Tag) ist für jede angebotene SIEM-Lösung, auch für Microsoft-basierte Lösungen, vollständig und wertungsrelevant zu bepreisen. Das UKF wird als Lizenznehmer geführt (D1 Kap. 3.2). Über welchen Vertragsweg der Auftraggeber die Lizenzen nach Zuschlag bezieht, bleibt ihm vorbehalten; dies ändert nichts an der Bepreisung im Angebot. Wertungsrelevante Positionen können nicht durch den Bieter als optional erklärt werden.

Der weitere teil Ihrer Frage wird zeitnah beantwortet.

Mit freundlichen grüßen,

Vergabeabteilung

Abt 3.3

7

Frage 10
Datenhoheit:

zu frage 10:

Sehr geehrte Damen und Herren,

18.09.2026 13:15:56

21.09.2026 10:35:11

	Gilt die Anforderung zur Datenhaltung ausschließlich in der EU (Eignungskriterium 4.12.7) rein für die Speicherung der Kundendaten, oder schließt dies auch administrative Support- und Wartungszugriffe durch Herstellerpersonal von Standorten außerhalb der EU (ohne Datenzugriff) aus?	Maßgeblich sind D2, Kriterium „EU-Firmensitz und EU-Datenhoheit“, und D1 Kap. 3.1. Etwaige Herstellerzugriffe sind danach im Angebot nachvollziehbar darzustellen. Mit freundlichen Grüßen, Vergabeabteilung Abt. 3.3	
8	Frage 11 Splunk SIEM: Versteht der Auftraggeber unter dem geforderten BYOL-Modell für das SIEM, dass der Splunk-Tenant direkt auf den Namen des UKF registriert wird, oder soll die Lizenz optional im Preisblatt ausgewiesen und durch den Auftragnehmer im Namen des UKF beschafft werden?	zu Frage 11 Sehr geehrte Damen und Herren, Die SIEM-Plattform wird in einem UKF-eigenen Tenant betrieben, das UKF ist als Lizenznehmer zu führen (D1 Kap. 3.1 und 3.2). Die Lizenz ist im Preisblatt unter LV 4.2 zu bepreisen, siehe auch Antwort zu Frage 5. Mit freundlichen grüßen, Vergabeabteilung Abt.3.3	21.09.2026 10:35:11
9	Frage 12: Log.-Optimierung: Ist der Einsatz einer vorgeschalteten Pipeline-Lösung zur Vorverarbeitung, Filterung und Anreicherung von Logdaten im UKF-Eigenbetrieb gestattet, um das geforderte Zielvolumen von 400 GB/Tag vor der Ingestion in das SIEM einzuhalten?	Zu Frage 12: Sehr geehrte Damen und Herren, Ein Eigenbetrieb durch das UKF ist nicht vorgesehen. Die Optimierung von Logquellen und Filtern zur Erreichung des Zielvolumens von 400 GB/Tag liegt beim Auftragnehmer (D1 Kap. 2.3 und 4.1). Mit freundlichen Grüßen, Vergabeabteilung Abt. 3.3	21.09.2026 10:35:11
10	Frage 14: NDR Ist für den Leistungsbereich NDR ein rein metadatenbasierter Analyseansatz (NetFlow/IPFIX, TLS-Fingerprinting JA3/JA4) ohne Entschlüsselung (TLS-Termination) als vollständig gleichwertig zulässig, oder wird zwingend eine Deep Packet Inspection (DPI) gefordert?	zu Frage 14: Sehr geehrte Damen und Herren, Verschlüsselter Datenverkehr ist ohne TLS-Termination zu analysieren. Maßgeblich sind metadatenbasierte Verfahren (D1 Kap. 5.3). Mit freundlichen Grüßen, Vergabeabteilung Abt. 3.3	21.09.2026 10:35:11
11	Frage 15: PCAP Storage	Zu frage 15: Sehr geehrte Damen und Herren,	21.09.2026 10:35:11

	Sofern eine On-Demand-Erfassung von Paketdaten (PCAP) für gezielte Investigations genutzt wird: Welche konkrete Aufbewahrungsdauer und welches Speichervolumen werden für PCAP-Rohdaten seitens des UKF erwartet?	Speicherort, Aufbewahrungsfristen und Zugriffsrechte werden in der Feinkonzeption festgelegt (D1 Kap. 5.4). Mit freundlichen Grüßen, Vergabeabteilung Abt. 3.3	
12	Frage 16: NDR Automation Werden für die im NDR-Kapitel 5.6 angesprochenen Reaktionen (z. B. Auslösung von Firewall- oder NAC-Sperren) automatisierte Out-of-the-Box-Aktionen verlangt, oder erfolgen sämtliche Maßnahmen ausschließlich regelbasiert über abgestimmte Playbooks im SOC?	zu Frage 16: Sehr geehrte Damen und Herren, Konkrete Aktionen, Freigabewege und Eskalationspfade werden in den Playbooks festgelegt (D1 Kap. 5.6). Automatisierte Reaktionen sind nur innerhalb der vorab abgestimmten Maßnahmenkataloge zulässig und in medizinisch-kritischen Segmenten ausgeschlossen (D1 Kap. 3.3 und 10.7). Mit freundlichen Grüßen, Vergabeabteilung Abt.3.3	21.09.2026 10:35:11
13	Frage 17: Vulnerability Management Welche genaue Bemessungsgrundlage gilt für die Kalkulation des Vulnerability-Management- Lizenztitels im Preisblatt: Die im Ist-Zustand genannten 21.000 IP-Bänder oder die Summe der tatsächlich zu scannenden physischen/virtuellen Assets (ca. 13.400)? Sind nicht-persistente VDI-Desktops (ca. 5.095) als eigenständige Assets zu lizenzieren?	zu frage 17: Sehr geehrte Damen und Herren, Kalkulationsgrundlage für LV 6.2 ist die dort genannte Menge von 21.000 (D1 Kap. 2.1). Der Geltungsbereich umfasst neben Servern, Clients und VDI-Systemen auch Netzwerk- und Sicherheitskomponenten, Webserver, Cloud-Dienste und Identitätsdienste (D1 Kap. 6.1). Die Menge ist unabhängig von der Lizenzmetrik des Bieters abzudecken, VDI-Systeme sind darin enthalten. Mit freundlichen Grüßen Vergabeabteilung Abt.3.3	21.09.2026 10:35:11
14	Frage 18: Vulnerability Management In welchem konkreten Umfang sind über M365 / Entra ID hinaus weitere Cloud-Umgebungen (wie Azure-Subscriptions, SAP S/4HANA Cloud oder ServiceNow) Bestandteil der kontinuierlichen Konfigurations- und Härtingsprüfung im Vulnerability Management?	zu frage 18: Sehr geehrte Damen und Herren, Die Konfigurations- und Härtingsprüfung umfasst die genutzten Cloud-Dienste, insbesondere M365 / Entra ID (D1 Kap. 6.3). Der konkrete Scope wird in der Feinkonzeption festgelegt (D1 Kap. 6.1). mit freundlichen Grüßen, Vergabeabteilung	21.09.2026 10:35:11

15	Frage 19: EDR Lizenzen Stellt das UKF im Falle einer Entscheidung für Microsoft Defender for Endpoint die erforderlichen Produktlizenzen im Rahmen bestehender Microsoft-Verträge (z. B. Enterprise Agreement E3/E5) bei, und wie wird sichergestellt, dass bei der Wertung keine Preisauswirkungsverzerrung gegenüber SentinelOne entsteht?	zu Frage 19: Sehr geehrte Damen und Herren, Es gilt D1 Kap. 7.2: „Sofern der Auftraggeber Microsoft Defender for Endpoint vorgibt, sind die hierfür erforderlichen Microsoft-Produktlizenzen nicht Bestandteil der wertungsrelevanten EDR-Basisleistung, soweit sie durch den Auftraggeber bereitgestellt werden.“ mit freundlichen Grüßen, Vergabeabteilung Abt. 3.3	21.09.2026 10:35:11
16	Frage 20: EDR Eignung Bedeutet die Vorgabe, dass der Bieter beide EDR-Betriebsvarianten (SentinelOne und MS Defender) beherrschen muss, dass für beide Plattformen nachweisbare Zertifizierungen/Referenzen bereits im Teilnahmewettbewerb vorliegen müssen?	zu Frage 20: Sehr geehrte Damen und Herren, Im Teilnahmewettbewerb gelten ausschließlich die Eignungskriterien aus D2. Die Anforderung aus D1 Kap. 7.2 bleibt unberührt. mit freundlichen Grüßen Vergabeabteilung Abt. 3.3	21.09.2026 10:35:11
17	Frage 21: IoMT-Security Trifft die Klarstellung in Kapitel 8.4, dass reine CVE-Listen unzureichend sind, dahingehend zu, dass eine Kombination aus passiver Anomaly-Detection und herstellerbezogenen Risikodaten (z. B. MDS²-Formularen) gefordert ist?	zu Frage 21: Sehr geehrte Damen und Herren, Die Anforderungen an die Risikobewertung ergeben sich aus D1 Kap. 8.4. Die Umsetzung ist im Lösungskonzept darzustellen (D4, Themenfeld 4, Bereich B). mit freundlichen Grüßen, Vergabeabteilung Abt. 3.3	21.09.2026 10:35:11
18	Frage 22: IoMT / NDR Wie ist die fachliche und technische Schnittstelle zwischen der IoMT-Security-Plattform und der NDR-Plattform definiert, um eine Duplizierung von Alarmen zu vermeiden und eine integrierte	zu Frage 22: Sehr geehrte Damen und Herren, Die fachliche Abgrenzung zwischen IoMT und NDR regelt D1 Kap. 8.7. Die Schnittstelle zum SIEM ist im Lösungskonzept darzustellen (D4, Themenfeld 4, Bereich C).	21.09.2026 10:35:11

Korrelation im SIEM sicherzustellen?

mit freundlichen Grüßen,

Vergabeabteilung

Abt.3.3

19

Frage 23:

zu Frage 23:

21.09.2026 10:35:11

Sehr geehrte Damen und Herren,

aus den Vergabeunterlagen geht für uns nicht eindeutig hervor, ob nach Abschluss des Teilnahmewettbewerbs und Einladung zur Angebotsabgabe weiterhin die Möglichkeit besteht, fachliche und vergabebezogene Bieterfragen über die Vergabeplattform einzureichen.

Bitte teilen Sie uns mit, ob in der Angebotsphase eine erneute Fragemöglichkeit vorgesehen ist und ob hierfür gesonderte Fristen veröffentlicht werden.

Sehr geehrte Damen und Herren,
vielen Dank für Ihre Anfrage.
Wir bestätigen, dass es sowohl in der ersten als auch in der nachfolgenden zweiten Angebotsrunde erneute Fragemöglichkeiten über die Plattform geben wird. Da die Eignungsprüfung mit dem Teilnahmewettbewerb abgeschlossen ist, dienen diese Fragerunden ausschließlich für technische und inhaltliche Fragen.

Die genauen Fristen hierfür werden den ausgewählten Bewerbern mit der jeweiligen Aufforderung zur Angebotsabgabe mitgeteilt.

mit freundlichen Grüßen,

Vergabeabteilung

Abt.3.3

20

Mit der Beantwortung der letzten Bieterfragen wurde ein BSI C5 Testat zum KO-Kriterium erklärt, sofern es sich nicht um eine On-prem Installation handelt. Da der Ausschreibungsgegenstand aus mehreren technischen Lösungskomponenten und Dienstleistungen besteht, bitten wir um Klarstellung für welche Teile ein BSI C5 Testat gefordert wird. Wird es vom Bieter und/oder den Herstellern der eingesetzten Cloud Lösungen gefordert? Insbesondere bitten wir um Aufklärung wie eine Gleichbehandlung von Bietern möglich ist, wenn eingesetzte Cloud-Lösungen wie bspw. Vectra nach unserem Kenntnisstand kein BSI C5 Testat besitzen, aber im Rahmen der Ausschreibung zur Verlängerung angeboten werden dürfen? Da die Ausschreibungsunterlagen explizit eine Trennung von Lizenz-Eigentümerschaft und Dienstleistung verlangen und es sich bei einem BSI C5 Testat um eine deutsche Zertifizierung für Cloud Dienste handelt, sehen wir aufgrund der sich daraus ergebenden Komplexität die Einhaltung des Gleichbehandlungsprinzips in einer europäischen Ausschreibung als schwierig umsetzbar an und möchten daher die Entfernung eines BSI C5 Testats als KO Kriterium vorschlagen.

Sehr geehrte Damen und Herren,

Das K.O.-Kriterium Nr. 3 „BSI C5 Typ 2 – Cloud-Sicherheit“ (Kriterienkatalog Ziffer 4.12.6) wird hiermit gestrichen. Mit dem Teilnahmeantrag ist demnach kein C5-Nachweis einzureichen; eine fehlende Vorlage führt nicht zum Ausschluss. Die Anforderung wird stattdessen als Wertungskriterium in die Angebotsphase verlagert (D3, Themenfeld 3), wo das Vorhandensein eines entsprechenden Nachweises positiv berücksichtigt wird. Um der europäischen Ausrichtung des Verfahrens sowie dem Gleichbehandlungsgrundsatz vollumfänglich Rechnung zu tragen, wird klargestellt, dass neben einem Testat nach BSI C5 Typ 2 auch ein gleichwertiger Nachweis zugelassen wird.

Hinsichtlich der angeführten Bestandssysteme gilt zudem: Vom Auftraggeber bereitgestellte oder vorgegebene Systeme sind von dieser Nachweisführung ausgenommen. Ein diesbezüglicher Korrekturzyklus der Vergabeunterlagen wird noch erfolgen.

Mit freundlichen Grüßen,

Vergabeabteilung

Abt. 3.3

21.09.2026 12:50:41

21

Frage 9:

zu Frage 9:

21.09.2026 12:56:35

C5 & Cloud

Sehr geehrte Damen und Herren,

Bezieht sich das geforderte BSI-C5-Typ-2-Testat (Eignungskriterium 4.12.6) ausschließlich auf das Hosting der Cloud-Infrastruktur (IaaS/PaaS-Ebene des Hyperscalers in der EU), oder muss das spezifische SaaS-Produkt des Herstellers über ein eigenes C5-Testat verfügen?

Das K.O.-Kriterium Nr. 3 „BSI C5 Typ 2 – Cloud-Sicherheit“ (Kriterienkatalog Ziffer 4.12.6) wird entfernt. Mit dem Teilnahmeantrag ist kein C5-Nachweis einzureichen, und eine fehlende Vorlage führt nicht zum Ausschluss. Die Anforderung wird in die Angebotsphase verlagert. Für angebotene Cloud-Dienste, in denen Daten des Auftraggebers verarbeitet, gespeichert oder übertragen werden, ist ein Testat nach BSI C5 Typ 2 oder ein gleichwertiger Nachweis vorzulegen. Ein Testat nach BSI C5 Typ 2 wird in der Angebotswertung (D3, Themenfeld 3) positiv berücksichtigt. Vom Auftraggeber bereitgestellte oder vorgegebene Systeme sind ausgenommen. Ein entsprechender Korrekturzyklus wird zeitnah erfolgen.

Mit freundlichen Grüßen,

Vergabeabteilung Abt 3.3

22

Frage 63-80

Sehr geehrte Damen und Herren,

22.09.2026 12:06:10

Sehr geehrte Damen und Herren,

im Rahmen der Prüfung der Ausschreibungsunterlagen haben sich für uns einige Fragen ergeben. Vielen Dank für Ihre Rückmeldung über das Vergabeportal.

zu 63-80:

zu Frage 63:

Frage 63: Kapitel 3.5

Gemäß Kapitel 3.5 ist die Anbindung neuer Standard-Logquellen Bestandteil des Regelbetriebs und löst keine Zusatzkosten aus. Wir bitten um Klarstellung, wie verfahren wird, wenn durch die Aufnahme zusätzlicher Standard-Logquellen eine Erweiterung lizenzabhängiger Plattformkapazitäten (z.B. Datenvolumen, EPS, Asset-Anzahl oder vergleichbare Metriken) erforderlich wird. Sind daraus resultierende Lizenzmehrkosten Bestandteil der Pauschalleistung oder werden diese gesondert vergütet?

Die Anbindung zusätzlicher Standardquellen mit verfügbarem Parser ist Bestandteil des Regelbetriebs und löst keine Zusatzkosten aus (D1 Kap. 3.5 und 4.1). Die SIEM-Plattformlizenz ist für ein Logvolumen von 400 GB/Tag zu bepreisen (Preisblatt LV 4.2). Die Optimierung von Logquellen und Filtern zur Erreichung dieses Zielvolumens liegt beim Auftragnehmer (D1 Kap. 2.3 und 4.1). Für ein darüber hinausgehendes Logvolumen ist der Preis je 100 GB/Tag in Abschnitt 8 des Preisblatts (LV OP.1) anzugeben. Für die übrigen Leistungsbereiche gelten die im Preisblatt genannten Mengen. Weitere lizenzabhängige Metriken, zum Beispiel EPS, begründen keine gesonderte Vergütung.

64: Kapitel 4.12.11 (Kriterienkatalog – Referenz 1)

Wir bitten um Klarstellung, ob für die Referenzanforderung ausschließlich Krankenhäuser akzeptiert werden, die formal als KRITIS-Betreiber nach deutschem Recht eingestuft sind, oder ob gleichwertige Referenzen europäischer Krankenhäuser anerkannt werden. Falls Gleichwertigkeit zugelassen ist, bitten wir um Darstellung der maßgeblichen Bewertungskriterien.

zu Frage 64: Antwort wird nachgereicht

zu Frage 65:

Frage 65: Kapitel 9.4

Wird der Auftraggeber sicherstellen, dass dem künftigen Auftragnehmer sämtliche für den Weiterbetrieb erforderlichen Betriebsartefakte, Konfigurationen, Dokumentationen, Use Cases, Detection-Regeln und Tuning-Anpassungen vollständig und in weiterverwendbarer Form übergeben werden?

Der Auftraggeber koordiniert die Übergabe der beim bisherigen Dienstleister vorhandenen Betriebsartefakte (D1 Kap. 9.5). Eine Zusicherung zu deren Vollständigkeit, Qualität oder Weiterverwendbarkeit gibt der Auftraggeber nicht ab. Der Mindestschutzzumfang zum Cut-over ist in jedem Fall herzustellen, erforderlichenfalls über ein gleichwertiges, dokumentiertes Ersatzregelwerk (D1 Kap. 9.5). Den Umgang mit unvollständiger oder fehlender Dokumentation des bisherigen Dienstleisters stellt der Bieter im Lösungskonzept

Frage 66: Kapitel 9.5

Die Leistungsbeschreibung (LV) sieht die Übernahme der bestehenden Detektionsregeln und Use Cases vor. Wie ist zu verfahren, wenn bei der Übernahme festgestellt wird, dass die bestehenden Regelwerke fachlich nicht ausreichend, nicht ausreichend dokumentiert oder nicht in die Zielarchitektur überführbar sind? Ist deren Neuaufbau Bestandteil der laufenden Transition oder gesondert zu behandeln?

Frage 67: Kapitel 7.2

Die Entscheidung über die Fortführung von SentinelOne oder die Transition zu Microsoft Defender for Endpoint wird vom Auftraggeber spätestens 8 Wochen vor dem Cut-over getroffen. Kann der Auftraggeber eine Tendenz oder Präferenz angeben, um dem Bieter eine zielgerichtetere und wirtschaftlichere Angebotsplanung zu ermöglichen? Betrifft die optionale Transition ausschließlich die technische Migration, oder wird auch eine konzeptionelle Neubewertung der Policy- und Detection-Strategie erwartet?

Zur besseren Kalkulationssicherheit bitten wir um Mitteilung, ob derzeit bereits strategische Vorentscheidungen oder Planungen hinsichtlich einer zukünftigen Nutzung von Microsoft Defender for Endpoint bestehen

Frage 68 Kapitel 4.1

Das Logvolumen von 400 GB/Tag wird als Kalkulationsgrundlage genannt. Wir bitten um Bestätigung, dass dieser Wert die Basis der Angebotsbewertung darstellt und wesentliche Überschreitungen infolge zusätzlicher Systeme, Datenquellen oder regulatorischer Anforderungen nicht Bestandteil des kalkulatorischen Risikos des Auftragnehmers sind. Wie werden daraus resultierende Mehrkosten berücksichtigt?

Frage 69 Kapitel 8

Die Anforderung sieht die passive Analyse des IoMT-Verkehrs vor. Welchen Detaillierungsgrad der Analyse erwartet der Auftraggeber für proprietäre, herstellereigenspezifische klinische Protokolle (z.B. von Herstellern wie Dräger, Siemens Healthineers)? Wird eine reine Analyse von Header-Informationen und Kommunikationsmustern erwartet oder eine tiefgehende Analyse der Protokollinhalte (Deep Packet Inspection auf Applikationsebene)?

Für den Leistungsbereich IoMT werden ca. 5.000 Medizingeräte genannt. Wir bitten um Angabe eines erwarteten Wachstums über die Vertragslaufzeit und um Bestätigung, dass wesentliche Erweiterungen oberhalb dieser Planungsgröße als Leistungsänderung behandelt werden.

Frage 70: Kapitel 12

Die SLA-Kennzahlen (z.B. Time to Contain) setzen eine schnelle Reaktion voraus. Insbesondere bei Reaktionen, die eine Freigabe durch den Auftraggeber erfordern (Human-in-the-Loop, z.B. im IoMT-Umfeld).

dar (D4, Themenfeld 1, Bereich A).

zu Frage 66:

Der Aufbau eines gleichwertigen, dokumentierten Ersatzregelwerks ist Bestandteil der Transition und mit den Positionen des Abschnitts 6 des Preisblatts abgegolten (D1 Kap. 9.5). Der Use-Case- und Detection-Aufbau gehört zur Phase 3 (D1 Kap. 9.1). Der Auftragnehmer bringt einen Standard-Use-Case-Katalog ein und entwickelt ihn fortlaufend weiter (D1 Kap. 4.3 und 10.10). Eine gesonderte Vergütung erfolgt nicht.

zu Frage 67:

Eine Tendenz wird nicht mitgeteilt. Der Auftraggeber legt die Plattform spätestens acht Wochen vor dem Cut-over fest. Bis dahin ist die Planung so auszugestalten, dass beide Szenarien ohne strukturellen Neuaufbau abbildbar sind (D1 Kap. 7.2). Die optionale Transition umfasst mindestens die in D1 Kap. 7.2 und 9.4 genannten Leistungen, einschließlich Policy- und Regelüberführung und Anpassung der Detection- und Response-Prozesse. Bestehende Policies werden übernommen und fachlich überprüft; das Policy- und Konfigurationsmanagement liegt beim Auftragnehmer (D1 Kap. 7.3 und 7.5).

zu Frage 68:

Die 400 GB/Tag sind Kalkulations- und Wertungsgrundlage (D1 Kap. 2.3 und 4.1; Preisblatt LV 4.2). Die Optimierung von Logquellen und Filtern zur Erreichung dieses Zielvolumens liegt beim Auftragnehmer. Wesentliche Abweichungen sind zu dokumentieren und mit ihren Auswirkungen auf Betrieb, Speicherung und Kosten darzustellen (D1 Kap. 2.3). Für ein Logvolumen über 400 GB/Tag gilt der vom Bieter angegebene Preis je 100 GB/Tag (Preisblatt Abschnitt 8, LV OP.1).

zu 69:

Die Anforderungen an Erkennung und Analyse ergeben sich aus D1 Kap. 8.2 und 8.3. Die Erkennung erfolgt herstellerunabhängig. Die genannten Geräteattribute sind mittels Deep Packet Inspection oder gleichwertiger Verfahren zu erfassen, und die in Kap. 8.3 genannten Kommunikationsmuster sind zu erkennen. Wie die Lösung herstellereigenspezifische Protokolle auswertet, stellt der Bieter im Lösungskonzept dar (D4, Themenfeld 4); dies fließt in die Bewertung ein (D3, Themenfeld 4). Klinische Protokollinhalte werden ausschließlich on-premises verarbeitet (D1 Kap. 3.4 und 8.6).

Kalkulationsgrundlage sind 5.000 vernetzte Medizingeräte (D1 Kap. 8.1; Preisblatt LV 8.1 und 8.2). Eine Wachstumsprognose wird nicht gegeben.

Wird die Zeitmessung der SLA (das "Anhalten der Uhr") offiziell pausiert, solange auf eine erforderliche Rückmeldung oder Freigabe durch eine benannte Stelle des UKF gewartet wird, und wird dies im Ticketsystem dokumentiert?

Wir bitten um Beschreibung des aktuellen Reifegrads der ServiceNow-Integration. Existieren bereits definierte APIs, Datenmodelle und Security Incident Workflows oder ist die Konzeption Bestandteil des Projekts?

Frage 71: Kapitel 11.2

Für die Integration in ServiceNow ist die Übergabe von "betroffenen Objekten" vorgesehen. Inwieweit kann der Auftraggeber sicherstellen, dass die hierfür notwendigen Informationen (z.B. eindeutige Asset-IDs, Kritikalität) in der CMDB des UKF konsistent und aktuell gepflegt sind, sodass diese zur automatisierten Anreicherung im SOC-Prozess genutzt werden können?

Frage 72: Kapitel 8.6

Für klinische Protokolle wird eine Anonymisierung vor Cloud-Verarbeitung gefordert. Wir bitten um Konkretisierung, ob eine On-Prem-Komponente für DICOM/HL7/FHIR bereits vorhanden ist oder durch den Auftragnehmer bereitgestellt werden muss.

Frage 73: Kapitel 14.7

Die Unterstützung eines Nachfolgedienstleisters wird als optionale Leistung beschrieben. Wir bitten um Klarstellung, welcher maximale zeitliche Umfang für einen Parallelbetrieb bzw. eine Exit-Transition der Kalkulation zugrunde gelegt werden soll.

Frage 74: Kapitel 10.6

Die Bereitstellung einer 24x7 verfügbaren L3-/DFIR-Kapazität ist Bestandteil des Managed Service; Einsatzaufwände werden jedoch nach Stundenverrechnungssätzen abgerechnet. Wir bitten um Klarstellung, welche Leistungen der DFIR-Kapazität bereits mit der Managed-Service-Pauschale abgegolten sind und ab welchem Punkt eine gesonderte Vergütung erfolgt.

Frage 75: Kapitel 6.1

"Der Geltungsbereich umfasst Server- und Betriebssystemplattformen, Clients und VDI-Systeme, Netzwerk- und Sicherheitskomponenten, Webserver und exponierte Webanwendungen, Cloud-Dienste und Cloud-Konfigurationen, Identitätsdienste sowie sicherheitsrelevante Anwendungen. Der konkrete Scope wird in der Feinkonzeption festgelegt." Da der konkrete Scope erst im Rahmen der Feinkonzeption festgelegt werden soll, bitten wir um Konkretisierung der zum Zeitpunkt der Ausschreibung bekannten Größenordnung der zu überwachenden Assets. Insbesondere bitten wir um Angaben bzw. Schätzwerte zur Anzahl externer Domänen, Webanwendungen und Anzahl je Cloud Asset Typ (z. B. virtuelle Maschinen, Container und virtuelle

Das Mengengerüst ist in der Feinkonzeption zu validieren und bei wesentlichen Abweichungen fortzuschreiben (D1 Kap. 2.1). Die Lösung muss steigende Mengen aufnehmen können (D1 Kap. 3.5). Für Änderungen des Leistungsumfangs nach Vertragsschluss gilt Ziffer 17 der EVB-IT System-AGB.

zu 70:

Zeiten, in denen die Bearbeitung nachweislich ausschließlich wegen einer ausstehenden Mitwirkung oder Freigabe des Auftraggebers ruht, werden nicht auf die Fristen angerechnet. Der Auftragnehmer dokumentiert Beginn und Ende dieser Zeiten im Vorgang (Vertragsanlage § 7 Abs. 5). Bei Guided Response endet die Messung der TTC mit der dokumentierten Übergabe einer konkreten, priorisierten Handlungsempfehlung (Vertragsanlage § 7 Abs. 2).

Zu ServiceNow: Schnittstellenspezifikation, Mapping, Test und Inbetriebnahme erfolgen gemeinsam. Der Auftraggeber stellt die ServiceNow-seitigen Schnittstellen, API-Zugänge, Verbindungsendpunkte, Berechtigungen, Konfigurationen und Mapping-Strukturen bereit (D1 Kap. 11.1 und 13.2). Die Integration auf Seite des Auftragnehmers einschließlich ihrer Konzeption liegt beim Auftragnehmer und ist Bestandteil der Phase 3 (D1 Kap. 9.1).

zu 71:

Eine Zusicherung zur Vollständigkeit oder Aktualität von CMDB-Daten gibt der Auftraggeber nicht ab. Die Bestimmung der betroffenen Objekte und die Anreicherung mit Asset- und Identitätskontext sind Leistungen des Auftragnehmers (D1 Kap. 4.2, 10.2 und 11.2). Verbindliche Grundlage der Kritikalität ist die gemeinsam erarbeitete Asset- und Kritikalitätsklassifizierung (D1 Kap. 9.2). Welche Datenquellen des Auftraggebers dafür angebunden werden, wird im Integrationskatalog festgelegt (D1 Kap. 9.3).

zu 72:

Die On-Premises-Komponente nach D1 Kap. 3.4 ist Bestandteil der angebotenen Lösung und vom Auftragnehmer bereitzustellen (D1 Kap. 3.4 und 8.6). Der Auftraggeber stellt hierfür keine Komponente bei.

zu 73:

sollen Erfahrungswerte einfließen lassen wie lange die aus den vergangenen Projekten dafür gebraucht haben

zu 74:

Netzwerke).

Frage 76: Kapitel 6.3

Das Scanning ist so zu gestalten, dass eine kontinuierliche Sichtbarkeit auf den aktuellen Schwachstellenstand entsteht – nicht nur ein punktueller Scan-Zyklus. Asset-Discovery und das Erkennen neu aufgetauchter, nicht erwarteter Systeme gehören zum Leistungsumfang. Gehen wir richtig in der Annahme, dass das Ausrollen von Agenten und oder Bereitstellen von Zugangsdaten für Netzwerkkomponenten nicht Teil des gewünschten Leistungsumfanges ist sondern durch das operative IT Team erbracht wird?

Frage 77: Kapitel 6.4/9.2

6.4 "Die Priorisierung darf sich nicht ausschließlich auf den CVSS-Wert stützen. Maßgeblich ist eine kombinierte Bewertung folgender Faktoren: [...]"
9.2 "Die Ergebnisse der Klassifizierung sind in einer gemeinsam zugänglichen Dokumentation zu führen und mindestens jährlich sowie anlassbezogen zu überprüfen. Sie dienen als verbindliche Grundlage für Priorisierungsentscheidungen in Detektion, Vulnerability Management, Incident Handling und Reporting."

Gehen wir richtig in der Annahme, dass die Goethe Klinik keine direkte Anbindung der Schwachstelleninformationen an die CMDB erwünscht oder möglichen machen wird und eine Priorisierung anhand Regeln zu Einschätzung der Assetkritikalität (bspw. über Hostname, IP etc.) vorgenommen werden soll?

Frage 78: Kapitel 6.4

"Die Priorisierung darf sich nicht ausschließlich auf den CVSS-Wert stützen. Maßgeblich ist eine kombinierte Bewertung folgender Faktoren: [...]"
Ist die Goethe Klinik bereit Schwachstelleninformationen extern verarbeiten zu lassen oder müssen Daten rein auf System der Goethe Klinik verarbeitet werden?

Frage 79: Kapitel 6.5

"Erkannte und priorisierte Schwachstellen müssen bis zur Bearbeitung, Risikoakzeptanz oder dokumentierten Schließung nachverfolgt werden. Statuswerte umfassen mindestens: neu erkannt, in Bewertung, priorisiert, übergeben, in Bearbeitung, behoben, kompensiert, akzeptiert, zurückgestellt, erneut erkannt, geschlossen [...]"
Nutz die Goethe Klinik neben der aktuellen Schwachstellenscanning Lösung eine ITSM Plattform, in welche solche Informationen integriert sind oder werden sollen? Wenn ja, ist eine solche Plattform (ServiceNow VR, Brinqa etc.) bereits vorhanden oder im Scope?

Frage 80: Kapitel 6.6

"Schwachstellenberichte werden monatlich (operativ) und quartalsweise (strategisch) bereitgestellt. Aktiv ausgenutzte oder besonders kritische Schwachstellen werden anlassbezogen kommuniziert."

Mit den laufenden Managed-Service-Positionen abgegolten sind die Vorhaltung der L3-/DFIR-Kapazität rund um die Uhr sowie sämtliche Leistungen nach D1 Kap. 10.5 bis 10.7, 10.15 und 12.6. Dazu gehören insbesondere die Untersuchung jedes validierten Sicherheitsvorfalls einschließlich Root Cause, Kill Chain und Auswirkungen, die Sicherung forensischer Artefakte bei P1-Vorfällen, die Koordination durch den Incident Response Lead (D1 Kap. 13.1), der Krisenmodus und die Incident-Abschlussbericht e. Nach den DFIR-Stundenätzen (Preisblatt Abschnitt 7) werden ausschließlich darüber hinausgehende forensische Einsätze abgerechnet, die der Auftraggeber gesondert abrechnet.

zu75:

Maßgeblich sind das Mengengerüst (D1 Kap. 2.1) und die Kalkulationsgrundlage von 21.000 für die Plattformlizenz (Preisblatt LV 6.2). Darüber hinausgehende Angaben werden nicht gemacht. Der konkrete Scope wird in der Feinkonzeption festgelegt (D1 Kap. 2.1 und 6.1). Siehe auch Antworten zu Fragen 17 und 18.

zu76:

Nein. Die Erhebung ist einschließlich der hierfür erforderlichen Agenten und Zugangsdaten vom Auftragnehmer zu planen, einzurichten, zu verwalten und zu dokumentieren (D1 Kap. 6.3). Der Auftraggeber stellt die erforderlichen Zugänge und Berechtigungen bereit (D1 Kap. 9.5 und 13.2).

zu 77:

Grundlage der Priorisierung ist die gemeinsam erarbeitete Asset- und Kritikalitätsklassifizierung (D1 Kap. 6.4 und 9.2). Wie sie technisch in die Priorisierung eingebunden wird, legt der Auftragnehmer in der Feinkonzeption fest (D1 Kap. 9.3) und stellt es im Lösungskonzept dar. Eine Anbindung an die CMDB ist weder gefordert noch ausgeschlossen.

zu 78:

Eine Verarbeitung außerhalb der Systeme des Auftraggebers ist zulässig, sofern die Anforderungen aus D1 Kap. 3.1 und 3.2 eingehalten werden, insbesondere Verarbeitung ausschließlich in der EU bzw. im EWR und Darstellung von Datenflüssen, Verarbeitungsorten, Unterauftragnehmern und Herstellerzugriffen im Angebot. Zum Sicherheitsnachweis für Cloud-Dienste siehe Antwort zu Frage 4.

zu79:

Die Übergabe von Maßnahmen an die Betriebsgruppen des Auftraggebers und deren Nachverfolgung erfolgen über die

Ist die Goetheklinik interessiert neben monatlichen / quartalsweisen Berichten ein Live Reporting zu erhalten? Wenn ist die Goetheklinik bereit hierfür eine gängige BI Plattform bereitzustellen? (Bspw. Azure Data Fabric + PowerBI)

ServiceNow-Integration (D1 Kap. 11.2 und 11.3). Das Remediation-Tracking mit den Statuswerten nach D1 Kap. 6.5 verantwortet der Auftragnehmer (D1 Kap. 6.5 und 13.3). Eine zusätzliche Plattform hierfür stellt der Auftraggeber nicht bereit

zu 80:

Gefordert sind die Berichte nach D1 Kap. 6.6 und 12.6. Ein darüber hinausgehendes Live-Reporting ist nicht Gegenstand der Leistung; eine BI-Plattform stellt der Auftraggeber nicht bereit.

mit freundlichen Grüßen

Vergabestelle

Abt. 3.3

23

Frage 62:

zu Frage 62:

22.09.2026 12:10:06

In den Vergabeunterlagen wird als Eignungsnachweis ein BSI APT-Response-Listungsnachweis oder ein gleichwertiger Befähigungsnachweis gefordert. Ist ein entsprechender Nachweis durch einen Link zu einer Website, in dem die Eintragung bzw. Darstellung unseres Unternehmens erfolgt, ausreichend?

Sehr geehrte Damen und Herren,

Ja. Das Produktdatenblatt oder die Herstellererklärung nach D1 Kap. 8.1 ist mit dem Angebot einzureichen, nicht mit dem Teilnahmeantrag.

Gehen wir recht in der Annahme, dass der Teilnahmeantrag in Textform abgegeben werden kann und keine handschriftliche oder qualifizierte elektronische Signatur erforderlich ist?

mit freundlichen Grüßen,

Vergabeabteilung

Abt.3.3.

Der in der Bekanntmachung angegebene Link zu den Eignungskriterien (<https://bieterzugang.deutsche-evergabe.de/.../suitabilitycriteria>) ist nicht erreichbar. Wir bitten um Bereitstellung eines funktionierenden Links bzw. der entsprechenden Informationen.

Wie ist das Dokument im Falle einer vorgesehenen Nachunternehmerschaft bzw. Eignungsleihe einzureichen? Ist es zulässig, die Erklärungen getrennt einzureichen, sodass die nachunternehmer- bzw. eignungsleihespezifischen Angaben in einem separaten Dokument durch den jeweiligen Nachunternehmer ausgefüllt werden?

Ist das vollständige Dokument einschließlich sämtlicher Anlagen mit dem Angebot einzureichen oder sind lediglich die für den Bieter relevanten Bestandteile vorzulegen?

Gehen wir recht in der Annahme, dass die „Anlage zum BMWK-Rundschreiben vom 14.04.2022“ sowie die „Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn“ ausschließlich vom Hauptauftragnehmer auszufüllen und einzureichen sind?

Gelten wir weiterhin als Einzelbewerber, wenn wir beabsichtigen, Nachunternehmer einzusetzen?

In den Vergabeunterlagen wird auf die „Anlage T TNA“ verwiesen. Gehen wir recht in der Annahme, dass darunter das gesamte Dokument "Vergabeunterlagen" fällt?

Gemäß Ziffer 8 "Leistungsbereich Leistungsbereich IoMT-Securitysind" muss die Lösung für den Betrieb in OT- und IoMT-Umgebungen qualifiziert sein. Der Nachweis ist über ein Produktdatenblatt oder eine Herstellererklärung zu erbringen. Gehen wir recht in der Annahme, dass diese erst in der Phase der Angebotsabgabe einzureichen sind.

24	Wichtiger Hinweis zur Übermittlung von Bieterfragen	bitte beachten Sie, dass Bieterfragen einzeln als direkte Nachrichten eingereicht werden müssen. Wir bitten Sie darum, davon abzusehen Fragen in Form von PDF-Dateien oder Excel-Tabellen zu übersenden. Sollten Sie Fragen in Form von Dateien eingereicht haben, bitten wir Sie diese nochmals als einzelne Nachrichten einzusenden. Vielen Dank für Ihr Verständnis. Mit freundlichen Grüßen Vergabestelle Abt 3.3.	23.09.2026 10:49:42
25	Frage 82 Sehr geehrte Damen und Herren, Gemäß §31 Abs2 BSI müssen Betreiber kritischer Anlagen Systeme zur Angriffserkennung einsetzen, die die von den identifizierten Bedrohungen betroffenen IT-Dienste automatisch unterbrechen und vorhandene Lösungen zur Beseitigung anwenden (Playbooks, Automatismen). Automatische Reaktionen sind dort vorgesehen, wo dadurch die kritische Dienstleistung nicht gefährdet wird. Wo eine automatische Reaktion nicht möglich ist, müssen manuelle Prozesse die Reaktion sicherstellen; der Ausschluss automatischer Reaktionen muss nachvollziehbar begründet werden. Außerdem dürfen automatisierte Maßnahmen die kritische Dienstleistung nicht relevant beeinträchtigen. Unserer Gemäß § 31 Abs. 2 BSI sind für die für die Funktionsfähigkeit kritischer Anlagen maßgeblichen informationstechnischen Systeme, Komponenten und Prozesse Systeme zur Angriffserkennung einzusetzen. Die Systeme müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten und sollen Bedrohungen identifizieren und vermeiden sowie geeignete Maßnahmen zur Beseitigung eingetretener Störungen vorsehen. Nach den Anforderungen des BSI sollen bzw. müssen automatisierte Reaktionsmaßnahmen nur dort eingesetzt werden, wo durch diese die kritische Dienstleistung nicht gefährdet wird. Insbesondere bei medizinischen und IoMT-Komponenten kann eine automatisierte Isolation, Unterbrechung der Netzwerkkommunikation oder sonstige automatisierte Reaktion aus Gründen der Patientensicherheit unzulässig oder nicht vertretbar sein. Die technische Ausgestaltung des SOC-/SIEM-/EDR-Services und	zu Frage 82 Sehr geehrte Damen und Herren: Eine Übersicht oder Klassifizierung der IoMT-Komponenten wird im Vergabeverfahren nicht bereitgestellt. Für Planung und Dimensionierung ist von ca. 5.000 vernetzten Medizingeräten auszugehen (D1 Kap. 8.1). Die passive Erkennung der Geräte mit den in D1 Kap. 8.2 genannten Attributen und die Risikobewertung auf Geräteebene (D1 Kap. 8.4) sind Bestandteil der Leistung. Die Asset- und Kritikalitätsklassifizierung erarbeiten Auftragnehmer und UKF gemeinsam im Onboarding (D1 Kap. 9.2). In medizinisch-kritischen Segmenten sind aktive Scans und agentenbasierte Standardbehandlung ausgeschlossen. Sicherheitsrelevante Reaktionsmaßnahmen erfolgen ausschließlich nach dem Human-in-the-Loop-Prinzip mit Freigabe durch den Auftraggeber (D1 Kap. 8.1). Zu automatisierten Reaktionen siehe Antwort zu Frage 16. mit freundlichen grüßen, Vergabeabteilung	23.09.2026 12:11:18

insbesondere die möglichen Detection- und Response-Maßnahmen sind daher wesentlich von Art, Kritikalität und technischen Möglichkeiten der einzubeziehenden IoMT-Komponenten abhängig. Bitte stellen Sie daher eine möglichst vollständige bzw. aggregierte Übersicht der in den **SOC-Service** einzubeziehenden IoMT-Komponenten zur Verfügung. Die Übersicht sollte – soweit vorhanden – mindestens folgende Angaben enthalten:

- IoMT-/Gerätetyp bzw. Gerätekategorie und Hersteller
- Anzahl der jeweiligen Komponenten
- Betriebssystem bzw. Plattform, soweit bekannt
- vorhandene Schnittstellen zur Sicherheitsüberwachung (z. B. EDR-Agent, Syslog, SNMP, API, Netzwerküberwachung)
- Zulässigkeit der Installation eines EDR-/Security-Agenten gemäß Herstellerfreigabe
- Zulässigkeit automatisierter Reaktionsmaßnahmen, insbesondere Isolation bzw. Unterbrechung der Netzwerkkommunikation
- Kritikalität hinsichtlich der medizinischen Versorgung bzw. Patientensicherheit
- bestehende alternative oder kompensierende Sicherheitsmaßnahmen.

Sofern bereits eine entsprechende Klassifizierung vorhanden ist, bitten wir zusätzlich um Zuordnung der Komponenten zu folgenden Überwachungs-/Reaktionsklassen:

Klasse 1 – EDR mit automatisierter Reaktion:

EDR/Agent technisch und regulatorisch zulässig; automatisierte Isolation bzw. Unterbrechung nach definierten Playbooks zulässig.

Klasse 2 – EDR mit eingeschränkter Reaktion:

EDR/Agent zulässig; Detection und Alarmierung möglich, automatisierte Isolation oder Unterbrechung jedoch aus medizinischen, regulatorischen oder betrieblichen Gründen nicht zulässig.

Klasse 3 – Agentenbasierte Überwachung:

Installation eines Monitoring-/Security-Agenten möglich, jedoch keine aktive EDR-Response.

Klasse 4 – Agentenlose Überwachung:

Überwachung ausschließlich über vorhandene Schnittstellen bzw. externe Systeme, z. B. Syslog, Netzwerk-Telemetrie, NDR, SNMP oder API.

Klasse 5 – Keine unmittelbare technische Überwachung:

Eine direkte agentenbasierte oder agentenlose Überwachung ist nicht möglich. Bitte benennen Sie, soweit vorhanden, die vorgesehenen kompensierenden Sicherheitsmaßnahmen.

Sollte eine entsprechende Übersicht oder Klassifizierung derzeit nicht vorliegen, bitten wir um Klarstellung, ob die Erhebung, Bewertung und Klassifizierung der IoMT-Komponenten Bestandteil der ausgeschriebenen Leistung sein soll.

Vielen Dank

26	Frage 84: EU-Datenhoheit bei eigenem Personal außerhalb der EU Die Antwort zu Frage 10 betrifft administrative Support- und Wartungszugriffe durch Herstellerpersonal. Wir bitten um Klarstellung, wie Zugriffe durch Personal des Auftragnehmers selbst beziehungsweise seiner verbundenen Unternehmen von Standorten außerhalb der EU zu behandeln sind, soweit diese ausschließlich der Aufrechterhaltung eines durchgehenden Betriebs dienen, keine Speicherung außerhalb der EU erfolgt und die Zugriffe protokolliert, auf das Erforderliche begrenzt sowie durch Standardvertragsklauseln nach Art. 46 DSGVO und ein Transfer Impact Assessment abgesichert sind. Wir bitten um Bestätigung, dass ein solcher Zugriff das Kriterium (4) nicht verletzt, sofern er im Angebot nachvollziehbar dargestellt wird	zu Frage 84: Eine solche Bestätigung wird nicht erteilt. Das K.O.-Kriterium Nr. 4 „EU-Firmensitz und EU-Datenhoheit“ (Kriterienkatalog Ziffer 4.12.7) verlangt, dass sämtliche im Rahmen der Leistungserbringung verarbeiteten und gespeicherten Daten ausschließlich innerhalb der Europäischen Union verarbeitet und gespeichert werden. Eine Ausnahme für Zugriffe durch Personal des Auftragnehmers oder verbundener Unternehmen von Standorten außerhalb der EU ist nicht vorgesehen, auch nicht bei Absicherung durch Standardvertragsklauseln oder ein Transfer Impact Assessment. Die Antwort zu Frage 10 lässt keine Ausnahme vom K.O.-Kriterium zu.	23.09.2026 12:11:18
27	Frage87: Sehr geehrte Damen und Herren, Für die SIEM-Plattform wird ein Logvolumen von 400 GB/Tag als Kalkulationsgrundlage vorgegeben. Gleichzeitig sind mindestens 12 Monate Aufbewahrung, davon mindestens 90 Tage Hot Storage, gefordert. Es ist nicht eindeutig geregelt, ob die Aufbewahrungspflicht auf das kalkulatorische Zielvolumen von 400 GB/Tag oder auf das tatsächlich nach Implementierung anfallende Sicherheitsdatenvolumen anzuwenden ist. Ist die geforderte Mindestaufbewahrung (12 Monate, davon 90 Tage Hot Storage) auf Basis von 400 GB/Tag oder auf Basis des tatsächlichen produktiven Datenvolumens auszulegen?	zu Frage 87: Die Aufbewahrung nach D1 Kap. 3.1 gilt für die tatsächlich anfallenden sicherheitsrelevanten Log-, Event-, Telemetrie- und Incident-Daten. Zur Kalkulationsgrundlage von 400 GB/Tag und zu einem höheren Volumen siehe Antwort zu Frage 68.	23.09.2026 12:11:18
28	Frage 88: Sehr geehrte Damen und Herren, Die Ausschreibung beschreibt Wachstumsannahmen (z. B. Access Points von 1.208 auf bis zu 3.400). Unklar bleibt, wie zukünftige Mengenzuwächse vergütet werden. Sind Mengenzuwächse innerhalb der in D1 beschriebenen Wachstumsprognosen Bestandteil der Festpreise oder gelten definierte Mengenschwellen, ab deren Überschreitung ein Preisanpassungsmechanismus vorgesehen ist?	zu Frage 88: Das Mengengerüst einschließlich der dort genannten Planwerte ist Planungs- und Kalkulationsgrundlage (D1 Kap. 2.1). Im Übrigen siehe Antwort zu Frage 63. Für Änderungen des Leistungsumfangs nach Vertragsschluss gilt Ziffer 17 der EVB-IT System-AGB	23.09.2026 12:11:18
29	Frage 89: Sehr geehrte Damen und Herren,	zu Frage 89:	23.09.2026 12:11:18

Neue Standardquellen sollen ohne Zusatzkosten angebunden werden. Nicht definiert ist, was als „Standardquelle“ gilt. Nach welchen objektiven Kriterien wird beurteilt, ob eine Quelle als Standardquelle mit vorhandenem Parser einzustufen ist und damit ohne Zusatzkosten eingebunden werden muss?

Siehe Antwort zu Frage 63. Die Kriterien ergeben sich aus D1 Kap. 4.1: Die Aufnahme neuer Quellen über marktübliche Verfahren (Syslog, Webhooks, API, Agent, Forwarder, dateibasiert sowie native Cloud- und Storage-Schnittstelle) ist Bestandteil des Regelbetriebs und löst keinen Sonderaufwand und keine Zusatzbeauftragung aus, soweit ein Standard-Parser verfügbar ist. Für Logs aus Individualsoftware und krankenhausspezifischen Anwendungen setzt der Auftragnehmer die erforderlichen Parser, Normalisierungen und Mappings in der Feinkonzeption um (D1 Kap. 4.2). Erfordert die Aufnahme einer nicht-standardisierten Quelle Parser-Engineering, weist der Auftragnehmer den Aufwand vor Beginn aus und holt die Freigabe des Auftraggebers ein. Abgerechnet wird nach den Stundenverrechnungssätzen (D1 Kap. 3.5; Preisblatt D5, Abschnitt 7).

30 Frage 90: zu Frage 90: 23.09.2026 12:11:18

Sehr geehrte Damen und Herren,

Eine bidirektionale API-Integration wird gefordert. Technische Rahmenbedingungen fehlen. Welche ServiceNow-Version sowie welche relevanten Module (ITSM, SecOps, IRM, CMDB etc.) sind aktuell produktiv im Einsatz und sollen in die E-Bonding-Integration einbezogen werden?

Siehe Antwort zu Frage 70. Die abzudeckenden Vorgangsarten regelt D1 Kap. 11.2. Angaben zu Version und Modulen werden im Vergabeverfahren nicht gemacht.

31 Frage 91: zu Frage 91: 23.09.2026 12:11:18

Sehr geehrte Damen und Herren,

Die Ausschreibung nennt 5.000 Geräte, beschreibt jedoch keine vorhandene Sensorik oder TAP-Infrastruktur. In welchem Umfang sind bereits Mirror-Ports, TAP-Infrastrukturen oder andere geeignete Netzwerkabgriffspunkte in den relevanten medizinischen Netzwerksegmenten vorhanden?

Angaben zu vorhandenen Abgriffspunkten werden im Vergabeverfahren nicht gemacht. Für IoMT-Security ist derzeit keine dedizierte Lösung im Einsatz (D1 Kap. 2.2). Die Lösung muss medizinisch-kritische Segmente ausschließlich passiv und nicht-invasiv erfassen (D1 Kap. 8.1). Der Netzwerkbetrieb des Auftraggebers stellt die relevanten Netz-, Sensorik-, Firewall- und Segmentierungsinformationen bereit (D1 Kap. 13.2). Die technische Anschlussart wird je Quelle im Integrationskatalog festgelegt (D1 Kap. 9.3).

32 Frage 24-32: zu Frage 24-32 23.09.2026 12:25:15

Frage 24:

Frage 24: Frage 1 | Bezug: Veröffentlichungstext / D1 Kapitel 1.2

Der Veröffentlichungstext nennt als Leistungsbeginn den 01.06.2027 bei einer Laufzeit von 60 Monaten und als Vertragsbeginn „schnellstmöglich“. D1 Kapitel 1.2 bestimmt, dass die Vertragslaufzeit von 60 Monaten mit dem Cut-over gemäß Kapitel 9.5 beginnt und der Vertrags- und Projektbeginn spätestens am 01.02.2027 erfolgt. Welches Datum ist für Beginn und Ende der 60-monatigen Laufzeit maßgeblich, und wie verhält sich der Cut-over-Termin 31.05.2027 zum

Die Vertragslaufzeit von 60 Monaten beginnt mit dem Cut-over (D1 Kap. 1.2 und 9.5; Anlage „EVB-IT Exit SLA Vergütung SOC-SIEM“, § 1 Abs. 1). Der Cut-over ist spätestens zum 31.05.2027 herzustellen. Ab dem 01.06.2027 ist die Lizenz- und Betriebsfähigkeit lückenlos sicherzustellen (D1 Kap. 9.4). Der Kalkulation ist der Cut-over zum 31.05.2027 zugrunde zu legen (Preisblatt D5, Deckblatt). Die Zeit zwischen Vertragsbeginn und Cut-over dient der Implementierung und Transition (D1 Kap. 9.1) und zählt nicht zu den 60 Monaten.

Leistungsbeginn 01.06.2027?

Frage 30:

Zum Testat nach BSI C5 siehe Antwort zu Frage 9. Das Produktdatenblatt oder die Herstellererklärung nach D1 Kap. 8.1 ist mit dem Angebot einzureichen, nicht mit dem Teilnahmeantrag; es gilt als ausdrücklich gefordert im Sinne der Verfahrensinformationen

Alle weiteren offenen Fragen werden zeitnah nachgereicht.

Frage 25: 2 | Bezug: Veröffentlichungstext / D1 Kapitel 1.2

D1 Kapitel 1.2 setzt den Vertrags- und Projektbeginn spätestens auf den 01.02.2027. Bitte teilen Sie den vorgesehenen Verfahrenszeitplan mit, insbesondere den geplanten Termin der Aufforderung zur Angebotsabgabe, die Anzahl und den Zeitraum der Verhandlungsrunden sowie den geplanten Zuschlagstermin.

Frage 26: 3 | Bezug: Verfahrensinformationen II. / Bewerbungsbedingungen Nr. 4

Die Verfahrensinformationen schließen Nebenangebote aus, die beigefügten Bewerbungsbedingungen EU enthalten unter Nr. 4 dennoch ausführliche Regelungen zu Nebenangeboten. Bitte bestätigen Sie, dass Nebenangebote in diesem Verfahren zugelassen sind und Nr. 4 der Bewerbungsbedingungen Anwendung findet.

Frage 27: 4 | Bezug: D3 Ziffer 3.2 und 8.2, D4 Ziffer 7

D3 und D4 verweisen mehrfach auf ein „Dokument D2“, in dem Eignung, Referenzen und Umsatz geprüft werden. Ein Dokument mit der Bezeichnung D2 ist in den Vergabeunterlagen nicht enthalten. Ist damit der Kriterienkatalog mit den Eignungskriterien im Bietercockpit gemeint, oder wird D2 noch nachgereicht?

Frage 28:

5 | Bezug: Verfahrensinformationen VI.A

In Abschnitt VI.A der Verfahrensinformationen wird die „Anlage-T Teilnahmeantrag“ genannt, mit der alle geforderten Anlagen und Nachweise abzugeben sind. Ein Formblatt mit dieser Bezeichnung ist in den bereitgestellten Unterlagen nicht enthalten. Wo ist dieses Formblatt abrufbar, oder wird der Teilnahmeantrag ausschließlich über den Kriterienkatalog im Bietercockpit abgegeben?

Frage 29:

6 | Bezug: Verfahrensinformationen D. und III.

Die Verfahrensinformationen verlangen unter D. elektronische Teilnahmeunterlagen „in Schriftform“, erklären das Hochladen zugleich als Signatur und fordern unter III. für die Anlagen BMWK und VT eine gesonderte Signatur durch berechnigte Personen. Welche Signaturform ist für welches Dokument konkret erforderlich, also Textform, fortgeschrittene oder qualifizierte elektronische Signatur?

Frage 30:

7 | Bezug: Verfahrensinformationen VI.C / D1 Kapitel 8.1 / Eignungskriterium

Die Verfahrensinformationen bezeichnen die Abgabe von Prospekten, Broschüren und Datenblättern als nicht erwünscht und weisen auf ein mögliches Ausschlussrisiko hin. Zugleich fordert D1 Kapitel 8.1 als Nachweis der OT-/IoMT-Qualifizierung ein Produktdatenblatt oder eine Herstellererklärung, und das Eignungskriterium zu BSI C5 verlangt den Upload eines Testats. Bitte stellen Sie klar, welche Hersteller- und Produktnachweise einzureichen sind, ohne ein Ausschlussrisiko auszulösen.

Frage 31:

8 | Bezug: Verfahrensinformationen E

Angesichts des Umfangs der Vergabeunterlagen von rund 200 Seiten mit fünf eigenständigen Anlagenwerken und der Vorgabe, jede Bieterfrage einzeln zu stellen, bitten wir um **Verlängerung der Bieterfragefrist um zwei Wochen** und um eine entsprechende Verlängerung der Frist zur Abgabe des Teilnahmeantrags. Ist dies möglich?

Frage 32:

8 | Bezug: Verfahrensinformationen VII

Der Code of Conduct für Lieferanten ist als Dokument benannt, das beim Bieter verbleibt und bei Beauftragung Vertragsbestandteil wird. Bitte bestätigen Sie, dass er im Teilnahmewettbewerb weder zu unterzeichnen noch einzureichen ist.

33

Frage 33-42

zu Frage 33-42:

23.09.2026 12:25:15

zu Frage 35:

Frage 33

Bieterfrage 1 zu Kriterienkatalog Ziffer 4.12.2 bis 4.12.20: Ziffer 4.12.2 kündigt die nachfolgenden Kriterien als K.O.-Kriterien vom Typ A an. Tatsächlich

Anerkannt werden Referenzen über Implementierung und Betrieb, die in den letzten drei Jahren vor Ablauf der Teilnahmefrist erbracht wurden oder noch erbracht werden. Der Auftrag muss nicht mehr laufen.

sind mehrere der Kriterien (1) bis (12) mit Punktwerten hinterlegt und damit erkennbar Bewertungskriterien vom Typ B. Bitte stellen Sie eine eindeutige Zuordnung bereit, welche der Kriterien (1) bis (12) K.O.-Kriterien und welche Bewertungskriterien sind.

Frage 34

Bieterfrage 2 zu Kriterienkatalog Ziffer 4 und 4.12: Bei sämtlichen Bewertungskriterien im Kriterienkatalog ist „Gewichtung: 0,00 %“ hinterlegt, während Abschnitt 4 insgesamt mit „Gewichtung: 100,00 %“ ausgewiesen ist. Wie werden die vergebenen Punkte tatsächlich gewichtet, und wie hoch ist die im Teilnahmewettbewerb maximal erreichbare Gesamtpunktzahl?

Frage 35

Bieterfrage 3 zu Kriterienkatalog Ziffer 4.12.11: Für Referenz 1 über den SOC- beziehungsweise MDR-Betrieb in einem KRITIS-Krankenhaus ist kein Referenzzeitraum angegeben. Welcher Ausführungszeitraum wird anerkannt, beispielsweise Leistungen der letzten drei Jahre entsprechend § 46 Abs. 3 Nr. 1 VgV? Muss der Referenzauftrag zum Zeitpunkt der Abgabe noch laufen?

Frage 36

Bieterfrage 4 zu Kriterienkatalog Ziffer 4.12.11: Wird bei Referenz 1 ein Krankenhaus in einem anderen Mitgliedstaat der Europäischen Union anerkannt, das dort nach nationalem Recht als kritische Einrichtung im Sektor Gesundheit eingestuft ist? Der Begriff KRITIS ist an das deutsche BSIG gebunden

Frage 37

Bieterfrage 5 zu Kriterienkatalog Ziffer 4.12.11: Können bei Referenz 1 die geforderten mindestens 1.000 Betten durch einen Klinikverbund mit mehreren Standorten unter einer gemeinsamen Trägerschaft erfüllt werden, oder muss ein einzelner Standort mindestens 1.000 Betten aufweisen?

Frage 38

Bieterfrage 6 zu Kriterienkatalog Ziffer 4.12.11 bis 4.12.15: Darf die für Referenz 1 benannte Referenz zugleich als Referenz 2 oder Referenz 3 gewertet werden, da ein KRITIS-Krankenhaus mit 1.000 Betten die Anforderung von mindestens 500 Betten ebenfalls erfüllt? Oder sind drei verschiedene Referenzkunden zwingend erforderlich?

Frage 39

zu Frage 37:

Die Mindestzahl von 1.000 Betten muss an einem Krankenhausstandort erreicht werden. Die Addition mehrerer Standorte eines Klinikverbunds ist nicht zulässig.

zu Frage 38:

Es müssen 3 unterschiedliche Referenzen sein.

Alle weiteren Fragen werden zeitnah beantwortet.

Bieterfrage 7 zu Kriterienkatalog Ziffer 4.12.16: Ist Referenz 4 zur IoMT-Security-Plattform ein K.O.-Kriterium oder ein Bewertungskriterium? Kann der Nachweis im Wege der Eignungsleihe durch einen an der Leistungserbringung beteiligten Nachunternehmer oder durch den Hersteller der IoMT-Plattform erbracht werden?

Frage 40

Bieterfrage 8 zu Kriterienkatalog Ziffer 4.12.11 bis 4.12.16: Die Angabe von Ansprechpartnern der Referenzkunden mit Namen, Telefonnummer und E-Mail-Adresse setzt deren Einwilligung voraus. Zahlreiche Kliniken untersagen die namentliche Nennung als Referenz. Akzeptieren Sie anonymisierte Referenzangaben, bei denen der Referenzkunde auf gesondertes Verlangen und nach dessen Freigabe benannt wird?

Frage 41

Bieterfrage 9 zu Kriterienkatalog Ziffer 4.12.17: Zur Anzahl festangestellter Mitarbeitender im direkten MDR-, SOC- und IoMT-Betrieb: Zählen Mitarbeitende verbundener Unternehmen desselben Konzerns sowie Mitarbeitende benannter Nachunternehmer mit? Ist die Angabe als Kopfzahl oder als Vollzeitäquivalent zu verstehen, und welcher Stichtag gilt?

Frage 42

Bieterfrage 10 zu Kriterienkatalog Ziffer 4.12.18 und 4.12.19: Zum Jahresumsatz aus Cybersecurity Managed Services: Ist der Umsatz des bietenden Unternehmens oder des Konzerns maßgeblich? Werden bei einer Bietergemeinschaft die Umsätze der Mitglieder addiert, und kann der Umsatz eines Nachunternehmers im Wege der Eignungsleihe angerechnet werden?

34	Frage 13: SAP S/4HANA Welche konkrete Art der Überwachung und Logquellen-Anbindung wird für die Cloud-Applikation SAP S/4HANA im SIEM-Scope erwartet (z. B. reine Audit-Logs via API oder anwendungsspezifische Security-Events)?	zu Frage 13: Anzubinden sind die sicherheitsrelevanten Audit-Logs von SAP S/4HANA (D1 Kap. 2.1, Einordnung „Cloud-Audit-Logs“, und Kap. 4.1). Die Anbindung ist Bestandteil des Regelbetriebs (D1 Kap. 3.5). Anschlussart, Umfang und Priorität werden im Integrationskatalog festgelegt (D1 Kap. 9.3).	23.09.2026 13:10:12
35	Frage 45: Sehr geehrte Damen und Herren,	zu Frage 45 Gefordert ist die Möglichkeit, Paketdaten für gezielte Untersuchungen anlassbezogen zu	23.09.2026 13:10:12

wir hätten eine weitere Frage bzw. Ergänzung zu dem PCAP Packet-Capture:

(5.4 in Vergabeunterlagen)

erfassen (D1 Kap. 5.4). Eine fortlaufende Aufzeichnung des Netzwerkverkehrs ist nicht gefordert. Ob und in welchem Umfang Paketdaten vorgehalten werden, legt der Auftraggeber in der Feinkonzeption fest, einschließlich Speicherort, Aufbewahrungsfristen und Zugriffsrechten (D1 Kap. 5.4 und 9.1). Es gelten D1 Kap. 3.1 und 3.4.

Ist die Anforderung zwingend als *rein reaktiv ausgelöste* On-Demand-Aufzeichnung zu verstehen, oder ist alternativ auch eine **Ring-Buffer-Lösung** zulässig, bei der Paketdaten kontinuierlich in einen rollierenden Speicher mit begrenzter Vorhaltezeit geschrieben und bei Bedarf rückwirkend extrahiert werden?

36

Frage 47:

BSI C5 Typ 2 bei Cloud-Bestandteilen

Genügt für cloudbasierte Bestandteile, beispielsweise ein SaaS-SIEM oder die SentinelOne-Cloud-Konsole, das BSI-C5-Typ-2-Testat des jeweiligen Cloud-beziehungsweise Plattformanbieters, oder wird zusätzlich ein eigenes BSI-C5-Typ-2-Testat des Bewerbers beziehungsweise Managed-Service-Providers für dessen Betriebsleistung verlangt?

zu Frage 47:

Siehe Antworten zu Fragen 4 und 9. Das K.O.-Kriterium Nr. 3 „BSI C5 Typ 2 – Cloud-Sicherheit“ (Kriterienkatalog Ziffer 4.12.6) ist entfallen. In der Angebotsphase ist für angebotene Cloud-Dienste, in denen Daten des Auftraggebers verarbeitet, gespeichert oder übertragen werden, ein Testat nach BSI C5 Typ 2 oder ein gleichwertiger Nachweis vorzulegen. Maßgeblich ist der Nachweis für den jeweiligen angebotenen Cloud-Dienst. Ein eigener Nachweis des Bieters für seine Betriebsleistung ist nicht gefordert. Bietet der Bieter selbst einen Cloud-Dienst an, gilt die Anforderung auch für diesen. Einzelheiten regeln die Unterlagen zur Angebotsabgabe.

23.09.2026 13:10:12

37

Frage 49:

Lizenzhoheit / BYOL bei SaaS- und Cloud-Plattformen

Ist die Anforderung aus D1 Kap. 3.2 („UKF als Lizenznehmer bzw. nutzungsberechtigte Organisation mit Übertragbarkeit bei Vertragsende“) bei herstellergehosteten SaaS- beziehungsweise Cloud-Plattformen, beispielsweise Microsoft Sentinel oder Defender in einem UKF-eigenen Azure-Tenant, erfüllt, wenn die Plattform in einem UKF-eigenen Tenant beziehungsweise Account auf Grundlage eines unmittelbar auf das UKF lautenden Endkunden-Lizenzvertrags betrieben wird und der Auftragnehmer ausschließlich als betreuender Dienstleister, nicht jedoch als Lizenznehmer, auftritt?

zu Frage 49:

Ja, sofern das UKF Lizenznehmer ist, der Tenant dem UKF gehört und die Weiternutzung bei einem Dienstleisterwechsel ohne Verlust von Lizenzen, Mandanten, Konfigurationen und Daten gewährleistet ist (D1 Kap. 3.1, 3.2 und 14.5). Die Lizenzkosten sind im Preisblatt D5 zu bepreisen (siehe Antworten zu Fragen 5 und 11).

23.09.2026 13:10:12

38

Frage 51:

EDR-Plattformscheidung / Zeitpunkt

zu Frage 51:

Eine Indikation wird nicht gegeben. Es gilt D1 Kap. 7.2: Der Auftraggeber legt die Plattform spätestens acht Wochen vor dem Cut-over fest. Bis dahin ist die Planung so auszugestalten, dass beide Szenarien ohne strukturellen Neuaufbau des Managed Service abbildbar sind.

23.09.2026 13:10:12

Der wertungsrelevante EDR-Basispreis basiert auf SentinelOne; MDE ist gemäß D1 Kap. 7.2 optional. Kann der Auftraggeber eine unverbindliche Indikation zur voraussichtlichen EDR-Zielplattform oder den spätesten Zeitpunkt für die Entscheidung zwischen einer Fortführung von SentinelOne und einer Migration zu MDE benennen, damit die Transitions- und Ressourcenplanung frühzeitig belastbar erfolgen kann?

39

Frage 52:

Microsoft Sentinel / Tenant-Verständnis

Ist ein UKF-eigener Azure-/Sentinel-Tenant, der ausschließlich in einer EU-Region betrieben wird und in dem sämtliche Log-, Detektions- und Falldaten innerhalb der EU verbleiben, mit den Anforderungen an einen „eigenen SIEM-Tenant“ und an die EU-Datenhoheit vereinbar, wenn der Auftragnehmer die administrative Betreuung dieses Tenants übernimmt?

zu Frage 52:

23.09.2026 13:10:12

Ja, sofern der Tenant ein UKF-eigener Tenant ist, das UKF Lizenznehmer ist und Verarbeitung und Speicherung ausschließlich in der EU bzw. im EWR erfolgen (D1 Kap. 3.1 und 3.2). Die administrative Betreuung durch den Auftragnehmer ist zulässig (D1 Kap. 4.5). Ein Betrieb unter alleiniger administrativer Kontrolle des Auftragnehmers ist ausgeschlossen (D1 Kap. 3.1). Herstellerzugriffe und Unterauftragnehmer sind im Angebot darzustellen (D1 Kap. 3.1).

40

Frage 53:

NDR/VM / Bewertungsneutralität

Werden die Fortführung der Bestandsplattformen Vectra AI für NDR und Tenable für Vulnerability Management sowie der Einsatz funktional gleichwertiger Alternativlösungen in der Angebotswertung gleichrangig und bewertungsneutral behandelt, sofern sämtliche funktionalen Anforderungen sowie die Vorgaben zu Datenhoheit, EU-Verarbeitung und Exit-Fähigkeit vollständig erfüllt werden?

zu Frage 53:

23.09.2026 13:10:12

Die Fortführung der Bestandsplattformen und eine alternative Lösung werden nicht unterschiedlich gewichtet (D1 Kap. 5.5 und 6.2). Bewertet wird das Lösungskonzept nach D3 und D4. In den Wertungspreis gehen die Positionen der gewählten Variante ein (Preisblatt D5, Abschnitte 2 und 3).

41

Frage 54:

SLA / Verbindlichkeit und Anpassbarkeit

Sind die SLA-Kennzahlen gemäß D1 Kap. 12.2 und § 7 der Vertragsanlage, einschließlich TTT, TTV, TTC und TTN je Priorität, der monatlichen Zielerreichungsquoten von 99,5 % für P1, 98,5 % für P2 und 95,0 % für P3 sowie der Plattformverfügbarkeit von 99,9 %, als abschließend festgelegte und nicht verhandelbare Mindestvorgaben zu verstehen, oder können sie im Verhandlungsverfahren auf Grundlage belastbarer Betriebserfahrungen aus vergleichbaren KRITIS-Krankenhaus-SOC-Umgebungen differenziert werden? Dies betrifft insbesondere Konstellationen, in denen das geforderte Human-in-the-Loop-Prinzip bei IoMT und patientennahen Systemen eine ausdrückliche Freigabe vor der Eindämmung (TTC) erfordert, sofern Schutzwirkung, Meldefähigkeit und

zu Frage 54:

23.09.2026 13:10:12

Die Service Level nach D1 Kap. 12 und Teil B der Anlage „EVB-IT Exit SLA Vergütung SOC-SIEM“ sind verbindlich. Eine Differenzierung ist nicht vorgesehen. Zeiten, in denen die Bearbeitung nachweislich ausschließlich wegen einer ausstehenden Mitwirkung oder Freigabe des Auftraggebers ruht, werden nicht auf die Fristen angerechnet; der Auftragnehmer dokumentiert Beginn und Ende dieser Zeiten im Vorgang (ebenda, § 7 Abs. 5). Fällt ein Vorfall in die Stufe Guided Response (D1 Kap. 10.7), endet die Messung der TTC mit der dokumentierten Übergabe einer konkreten, priorisierten Handlungsempfehlung an den Auftraggeber (ebenda, § 7 Abs. 2).

Bieterfrage 55-60:

Frage 55:

Bieterfrage 3 unter Punkt: "Kriterienkatalog Ziffer 4.12.6"

- Zum Nachweis nach BSI C5 Typ 2: Genügt das Testat des Cloud- beziehungsweise Plattformherstellers, etwa des SIEM-SaaS-Anbieters oder muss der Bieter selbst über ein eigenes C5-Testat verfügen? Wird ein Testat nach Typ 1 oder ein laufendes Typ-2-Verfahren übergangsweise anerkannt?

Frage 56:

Bieterfrage 4 unter Punkt: "Kriterienkatalog Ziffer 4.12.7 / D1 Kapitel 7.2"

- Das K.O.-Kriterium zur EU-Datenhoheit verlangt, dass sämtliche verarbeiteten und gespeicherten Daten ausschließlich innerhalb der Europäischen Union verarbeitet werden. Zugleich behält sich der Auftraggeber nach D1 Kapitel 7.2 vor, Microsoft Defender for Endpoint vorzugeben, dessen Verarbeitung in der Microsoft-Umgebung des Auftraggebers erfolgt und bei dem Microsoft Support- und Telemetriedatenflüsse außerhalb der EU vorsehen kann. Bezieht sich das K.O.-Kriterium ausschließlich auf die vom Auftragnehmer verantworteten Systeme und Verarbeitungen?

Frage 57:

Bieterfrage 5 unter Punkt: "Kriterienkatalog Ziffer 4.12.9 / D1 Kapitel 10.1"

- Das K.O.-Kriterium fordert, dass der SOC-Betrieb vollständig in deutscher Sprache erfolgt. D1 Kapitel 10.1 lässt dagegen ausdrücklich zu, dass L3-Kapazitäten für tiefgehende forensische Analyse und spezialisierte Incident-Response-Experten in englischer Sprache erbracht werden, sofern eine deutschsprachige Koordinationsrolle auf L2-Ebene besteht. Welche der beiden

zu Bieterfrage 55-60:

Frage 55:

Siehe Antworten zu Fragen 4, 9 und 47. Einzelheiten zu Art und Umfang der Nachweise regeln die Unterlagen zur Angebotsabgabe.

Frage 56:

Das K.O.-Kriterium Nr. 4 „EU-Firmensitz und EU-Datenhoheit“ (Kriterienkatalog Ziffer 4.12.7) erfasst alle Daten, die der Bewerber im Rahmen der Leistungserbringung selbst oder durch Unterauftragnehmer verarbeitet und speichert. Dazu gehören auch die von ihm angebotenen Plattformen, Cloud- und SaaS-Komponenten und die im Preisblatt bepreisten Lizenzen (D1 Kap. 3.1). Nicht erfasst ist die Verarbeitung innerhalb der Microsoft-Umgebung des Auftraggebers, soweit der Auftraggeber Microsoft Defender for Endpoint vorgibt und die Lizenzen selbst bereitstellt (D1 Kap. 2.2 und 7.2). Verarbeitet der Auftragnehmer Daten aus dieser Umgebung, zum Beispiel im SIEM, in der Alarmbearbeitung oder im Reporting, gelten dieses K.O.-Kriterium und D1 Kap. 3.1. Datenflüsse und Herstellerzugriffe der angebotenen Komponenten sind im Angebot darzustellen (D1 Kap. 3.1, siehe Antwort zu Frage 10).

Frage 57:

Beide Regelungen gelten nebeneinander. Das K.O.-Kriterium Nr. 6 „Deutschsprachiger SOC-Betrieb“ (Kriterienkatalog Ziffer 4.12.9) verlangt, dass sämtliche Kommunikations-, Eskalations- und Berichtspflichten gegenüber dem Auftraggeber in deutscher Sprache erfüllt werden. D1 Kap. 10.1 konkretisiert dies für die Tier-Stufen. Die Kommunikation auf L1- und L2-Ebene (Triage, initiale Analyse, Eskalation) erfolgt in deutscher Sprache. L3-Kapazitäten (tiefgehende forensische Analyse, spezialisierte IR-Expertise) können in englischer Sprache erbracht werden, sofern eine deutschsprachige Koordinationsrolle auf L2-Ebene die Kommunikation mit dem UKF sicherstellt. Die Kommunikation mit dem Auftraggeber erfolgt damit in jedem Fall in deutscher Sprache. Das gilt ebenso für Service Delivery Manager, Hotline, Regelkommunikation und Dokumentation (D1 Kap. 3.8 und 10.1).

Alle weiteren Fragen werden zeitnah beantwortet.

23.09.2026 13:10:12

Regelungen gilt?

FRrage 58:

Bieterfrage 6 unter Punkt: "Kriterienkatalog Ziffer 4.8"

- Die geforderte Betriebs- und Berufshaftpflichtversicherung beträgt 2.500.000 Euro pauschal je Schadensfall, einfach maximiert pro Jahr. Bleibt es bei dieser Deckungssumme, oder werden im Vertrag höhere Deckungssummen, eine zweifache Maximierung oder eine gesonderte Cyber- beziehungsweise Vermögensschadenhaftpflicht gefordert?

Frage 59:

Bieterfrage 7 unter Punkt: "Verfahrensinformationen VI.A"

- Die Aufzählung der einzureichenden Unterlagen führt die Anlagen EN1 und EN2, die den Nachunternehmereinsatz betreffen, unter der Überschrift „bei Bietergemeinschaften“ auf. Bitte stellen Sie eine eindeutige Liste der mit dem Teilnahmeantrag einzureichenden Unterlagen bereit, getrennt nach Einzelbewerber, Bietergemeinschaft, Nachunternehmereinsatz und Eignungsleihe.

Frage 60:

Bieterfrage 8 unter Punkt: "Bezug: Verfahrensinformationen IV. und V."

- Ist ein Wechsel oder eine Ergänzung von Nachunternehmern und Eignungsleihgebern zwischen dem Teilnahmeantrag und der Angebotsabgabe zulässig, sofern die Eignung unverändert nachgewiesen bleibt?

43

Frage 92-115:

Nr.

Req-ID

Bezug / Anforderung

Bieterfrage an den AG

Sehr geehrte Damen und Herren,

zu Frage 92:

wird nachgereicht

zu Frage 93:

Siehe Antwort zu Frage 52. Für Export und Löschung gilt D1 Kap. 14.4.

zu Frage 94:

25.09.2026 11:38:54

Frage 92:1	Siehe Antwort zu Frage 52.
REQ-011	zu Frage 95:
Cybersecurity Managed Service als ein Los für SOC/SIEM, NDR, Vulnerability Management, EDR-Management und IoMT-Security erbringen.	Ja. Eine durchgehende Vorhaltung ohne Wiederherstellungsvorlauf erfüllt die Mindestanforderung aus D1 Kap. 3.1.
Kann der AG bestätigen, dass die Leistungsbereiche EDR-Management und IoMT-Security über qualifizierte Unterauftragnehmer/Partner innerhalb eines Loses erbracht werden dürfen, solange der Bieter die Gesamtverantwortung trägt?	zu Frage 96:
Frage 93:	siehe Antwort zu Frage 84.
2	zu Frage 97:
REQ-014	Siehe Antwort zu Frage 49.
Daten & Compliance	zu Frage 98:
Hoheit über Rohdaten, Logs, Telemetrie, Incidents, Reports, Nachweise und Dokumentationen dauerhaft beim UKF belassen.	Die Berichte nach D1 Kap. 12.6 und die Dokumentation sind in deutscher Sprache zu liefern (Kriterienkatalog Ziffer 4.12.9; D1 Kap. 3.8; Ziffer 5.3 EVB-IT System-AGB). Für die Plattformoberfläche besteht keine Sprachvorgabe. Siehe auch Antwort zu Frage 57.
Genügt es dem AG, wenn die Datenhoheit durch jederzeitigen vollständigen Lese- und Exportzugriff (API, CSV/JSON/PDF) sowie vertraglich zugesicherte Herausgabe und Löschung sichergestellt wird, auch wenn die Speicherung in der Hersteller-Cloud (Mandant des UKF) erfolgt?	zu Frage 99:
Frage 94:3	Ja. Syslog und API zählen zu den marktüblichen Verfahren nach D1 Kap. 4.1. Sicherheitsrelevante Alarime, Bewertungen und Kontextdaten müssen an das SIEM übergeben werden (D1 Kap. 8.7). Der Integrationskatalog enthält je Quelle die technische Anschlussart (D1 Kap. 9.3).
REQ-015	zu Frage 100:
Daten & Compliance	Siehe Antwort zu Frage 68. Maßgeblich ist das Logvolumen je Tag (D1 Kap. 2.3; Preisblatt D5, LV 4.2). Eine Durchschnittsbetrachtung mit Lastspitzenausgleich ist nicht vorgesehen.
SIEM in UKF-eigenem Tenant bzw. UKF-eigener Instanz betreiben; alleinige administrative Kontrolle des Auftragnehmers ist ausgeschlossen.	zu Frage 101:
Der SIEM-Betrieb erfolgt bei der angebotenen Lösung in einem dedizierten, UKF-zugeordneten SaaS-Tenant mit UKF-Administratorrechten (Tenant Administrator), jedoch nicht als UKF-eigene Instanz. Kann der AG bestätigen, dass ein dedizierter, mandantentrennter SaaS-Tenant mit vollen UKF-Administrationsrechten die Anforderung erfüllt, oder führt dies zum Ausschluss?	Ja. Die Meldefrist von 30 Minuten nach D1 Kap. 4.2 ist eine vertragliche Pflicht des Auftragnehmers, unabhängig vom Produkt-SLA des Herstellers.
4 Frage 95:	zu Frage 102:
REQ-016	Ja. Das Nachweispaket erstellt der Auftragnehmer (D1 Kap. 4.7, 10.18 und 12.6). Ein standardisiertes Paket des Plattformherstellers ist nicht gefordert. Maßgeblich sind die Anforderungen aus D1 Kap. 4.7.
Daten & Compliance	zu Frage 103:
Sicherheitsdaten mindestens 12 Monate aufbewahren, davon mindestens 90 Tage Hot Storage; Rest innerhalb 24 Stunden wiederherstellbar.	Ja. D1 Kap. 6.2 lässt die Übernahme oder den Neuaufbau von Scan-Profilen zu. Eine herstellerseitig unterstützte Migration wird nicht gefordert. Das Migrationskonzept muss die in D1 Kap. 6.2 genannten Inhalte abdecken.

Ist die Anforderung 'Rest innerhalb 24 Stunden wiederherstellbar' auch erfüllt, wenn die gesamten Sicherheitsdaten über die volle Aufbewahrungsdauer permanent online und ohne Wiederherstellungsvorlauf durchsuchbar vorgehalten werden?

5Frage 96:

REQ-017

Daten & Compliance

Sicherheitsrelevante Daten ausschließlich innerhalb EU/EWR verarbeiten und speichern; Datenflüsse, Orte, Unterauftragnehmer und Herstellerzugriffe transparent darstellen.

Wird die Anforderung der ausschließlichen EU/EWR-Datenhaltung erfüllt, wenn der produktive Mandant in einer EU-Region betrieben wird, Support- und Analysezugriffe durch das 24x7-SOC jedoch im Follow-the-Sun-Modell auch aus Nicht-EU-Standorten erfolgen und dies über Standardvertragsklauseln (SCC) sowie technische Zugriffskontrollen abgesichert wird?

6Frage 97

REQ-019

Daten & Compliance

Kundenbezogene Plattform- und Produktlizenzen im BYOL-Modell auf UKF führen; nicht übertragbare reine MSP-Lizenzmodellen sind ausgeschlossen.

Für die SIEM-Plattform ist ein BYOL-Modell mit dem UKF als Lizenznehmer herstellerseitig nicht vorgesehen; die Lizenzierung erfolgt als Subscription auf den UKF als Vertragspartner. Kann der AG bestätigen, dass eine auf das UKF lautende, kündbare Subscription-Lizenz mit vertraglich gesichertem Datenexport die Anforderung erfüllt?

7Frage 98:

REQ-027

Service Delivery

Operative Service-Kommunikation, Eskalation, Regelkommunikation und Dokumentation gegenüber UKF auf Deutsch erbringen.

Ist es ausreichend, wenn die gesamte operative Kommunikation, Eskalation und Regelkommunikation sowie die Berichtsaufbereitung auf Deutsch erfolgen, die Plattformoberfläche und die systemgenerierten Rohreports jedoch englischsprachig sind?

8Frage 99:

REQ-028

zu Frage 104:

Nach D1 Kap. 6.3 müssen Authenticated Scans, agenten- oder API-basierte Erhebung sowie der Import vorhandener Scan-Ergebnisse unterstützt werden. Das Scanning ist so zu gestalten, dass eine kontinuierliche Sichtbarkeit auf den aktuellen Schwachstellenstand entsteht (D1 Kap. 6.3). Ob vorhandene Scan-Ergebnisse übernommen werden, legt der Auftraggeber in der Feinkonzeption fest

zu Frage 105:

Siehe Antwort zu Frage 18. Ein bestimmtes Werkzeug ist nicht vorgegeben (D1 Kap. 3.6). D1 Kap. 6.3 fordert für die genutzten Cloud-Dienste eine grundlegende Konfigurations- und Härtingsprüfung gegen anerkannte Benchmarks (z. B. CIS, herstellereigene Best Practices). Auswertbare Befunde fließen in die Priorisierung ein. Die Auswertung von Audit-Ereignissen allein erfüllt dies nicht.

zu Frage 106:

Ja, D1 Kap. 7.5 schreibt keine Dokumentation im SIEM vor. Ausnahmen, Ausschlüsse und Konfigurationsänderungen werden über das abgestimmte Berechtigungs- und Freigabemodell behandelt und revisionssicher protokolliert. Policy-Änderungen werden im Change-Management-Prozess geführt (D1 Kap. 7.5). Changes sind Vorgangsarten der ServiceNow-Integration (D1 Kap. 11.2).

zu Frage 107:

Die Anforderungen sind herstellerneutral formuliert (D1 Kap. 3.6). Die Lösung muss D1 Kap. 8 erfüllen, einschließlich des Nachweises nach D1 Kap. 8.1 (siehe Antwort zu Frage 62). Die Lizenz ist auf das UKF zu führen (D1 Kap. 3.2; Preisblatt D5, LV 8.2). Zur Einbindung in das SIEM siehe Antwort zu Frage 99. Der Einsatz von Nachunternehmern richtet sich nach Abschnitt IV der Verfahrensinformationen.

zu Frage 108:

Nein. Schulungen sind in deutscher Sprache durchzuführen, und die Schulungsunterlagen sind in deutscher Sprache geschuldet (Ziffer 2.5 EVB-IT System-AGB; D1 Kap. 9.7). Ergänzend bereitgestellte englischsprachige Herstellerunterlagen ersetzen diese nicht.

zu Frage 109:

Siehe Antwort zu Frage 54. Die Rechtsfolgen bei Überschreitung regelt § 8 der Anlage „EVB-IT Exit SLA Vergütung SOC-SIEM“.

zu Frage 110:

SOC/SIEM

Mindestens Identitätsdienste, Server, Endpunkte, E-Mail, Netzwerk-/Security-Komponenten, Cloud-Dienste und Erkenntnisse aus EDR/NDR/IoMT/VM in das SIEM integrieren.

Können IoMT-Erkenntnisse über eine generische Schnittstelle (Syslog/API einer Drittlösung) in das SIEM integriert werden, sofern keine native IoMT-Integration des Herstellers vorliegt?

9Frage 100:

REQ-029

SOC/SIEM

SIEM für 400 GB sicherheitsrelevantes Logvolumen pro Tag kalkulieren und Quellen/Filter zur Zielerreichung optimieren.

Wird das SIEM-Volumen von 400 GB/Tag als vertraglich fixiertes Gesamtvolumen unabhängig von der Endpunktzahl vereinbart, und ist eine monatliche Durchschnittsbetrachtung mit Lastspitzenausgleich zulässig?

10Frage 101:

REQ-031

SOC/SIEM

Unterbrechungen oder Qualitätsmängel kritischer Logquellen binnen 30 Minuten nach Feststellung melden.

Wird für die Meldung von Logquellen-Unterbrechungen eine vertraglich vereinbarte Frist von 30 Minuten akzeptiert, die außerhalb des Standard-Produkt-SLA individualvertraglich zugesichert wird?

11Frage 102:

REQ-039

SOC/SIEM

Dokumentation für SzA-Nachweis auf RUN-Reifegrad 2 zum Go-Live und Reifegrad 3 spätestens 12 Monate nach Betriebsaufnahme ausrichten.

Wird ein bieterseitig erstelltes SzA-Nachweispaket akzeptiert, das die Reifegradanforderungen mit plattformgenerierten Reports und Prozessdokumentation belegt, ohne dass der Plattformhersteller ein standardisiertes SzA-Paket bereitstellt?

12Frage 103:

REQ-048

Siehe Antwort zu Frage 109.

zu Frage 111:

Siehe Antworten zu Fragen 54 und 109.

zu Frage 112:

Siehe Antwort zu Frage 109.

zu Frage 113:

Die Mindestintervalle nach D1 Kap. 12.4 sind verbindlich (siehe Antwort zu Frage 54).

zu Frage 114:

wird nachgereicht

zu Frage 115:

Gefordert ist ein Löschprotokoll des Auftragnehmers mit Art, Umfang, Speicherorten, Zeitpunkt, Verfahren und verantwortlicher Stelle (D1 Kap. 14.4; Anlage „EVB-IT Exit SLA Vergütung SOC-SIEM“, § 4 Abs. 3). Eine allgemeine Löschbestätigung des Plattformherstellers genügt dafür nicht.

Vulnerability Management

Bei Fortführung Tenable Konfigurationen, Scan-Profile und Asset-Daten übernehmen; bei Alternative Migrationskonzept mit Parallelbetrieb und Vermeidung von Erkennungslücken vorlegen.

Ist bei Variante Ablösung eine Nachbildung der Tenable-Scan-Profile und ein Import der Asset-Daten über die VDR-API ausreichend, oder wird eine native, herstellerseitig unterstützte Migration der Tenable-Konfiguration gefordert?

13Frage 104:

REQ-049

Vulnerability Management

Authenticated Scans, Agent-/API-Erhebung, Import bestehender Ergebnisse, kontinuierliche Sicht sowie Asset Discovery unterstützen.

Ist die Anforderung erfüllt, wenn die Erhebung über authentifizierte Netzwerk-Scans und API-Connectors ohne zusätzlichen Endpunkt-Agenten erfolgt, und kann auf den Import historischer Scan-Ergebnisse aus dem Altsystem verzichtet werden?

14Frage 105:

REQ-050

Vulnerability Management

Webanwendungsprüfungen und grundlegende Cloud-Konfigurations-/Härtungsprüfungen, insbesondere M365/Entra ID, erbringen.

Genügt es, M365/Entra-ID-Härtung über die kontinuierliche Auswertung von Konfigurations- und Audit-Ereignissen im SIEM abzudecken, wenn keine dedizierte CSPM-Prüffunktion im Vulnerability-Management- Werkzeug vorhanden ist?

15Frage 106:

REQ-060

EDR

Baseline-Policies für Server, Client und VDI pflegen; Ausnahmen und Änderungen revisionssicher dokumentieren und Rollback ermöglichen.

Ist es zulässig, die revisionssichere Dokumentation der EDR-Policy-Änderungen im Change-Register des Auftragnehmers und in der jeweiligen EDR-Herstellerkonsole zu führen, statt im SIEM selbst?

16 Frage 107:

REQ-062

IoMT

IoMT-Security für ca. 5.000 vernetzte Medizingeräte dimensionieren und ausschließlich passiv, nicht-invasiv betreiben.

Kann der AG bestätigen, dass die IoMT-Security über eine spezialisierte Drittlösung eines Partners erbracht und deren Erkenntnisse in das SIEM integriert werden dürfen, ohne dass dies zum Ausschluss führt?

17 Frage 108:

REQ-077

Transition

Initial- und Nachschulungen für IT-Betrieb, Informationssicherheit, Medizintechnik und Service-Steuerung durchführen; versioniertes Betriebshandbuch übergeben.

Ist es ausreichend, wenn die Schulungen für IT-Betrieb, Informationssicherheit, Medizintechnik und Service-Steuerung auf Deutsch durchgeführt werden, die herstellerseitigen Schulungsunterlagen und Videos jedoch in englischer Sprache vorliegen?

18 Frage 109:

REQ-089

SLA

TTT einhalten: P1 <=15 Min, P2 <=30 Min, P3 <=60 Min.

Sind die geforderten TTT-Werte (Time-to-Triage: P1 <= 15 Min., P2 <= 30 Min., P3 <= 60 Min.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

19 Frage 110:

REQ-090

SLA

TTV einhalten: P1 <=30 Min, P2 <=60 Min, P3 <=4 Std.

Sind die geforderten TTV-Werte (Time-to-Verify: P1 <= 30 Min., P2 <= 60 Min., P3 <= 4 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche

Sanktionierung?

20 Frage 111:

REQ-091

SLA

TTC einhalten: P1 <=15 Min, P2 <=30 Min, P3 <=4 Std.

Sind die geforderten TTC-Werte (Time-to-Contain: P1 <= 15 Min., P2 <= 30 Min., P3 <= 4 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung? Sofern verbindlich: Wird die Wartezeit auf die gemäß Leitplanke REQ-022 erforderliche UKF-Freigabe aus der Messung herausgerechnet?

21 Frage 112:

REQ-092

SLA

TTN einhalten: P1 <=15 Min, P2 <=60 Min, P3 <=2 Std.

Sind die geforderten TTN-Werte (Time-to-Notify: P1 <= 15 Min., P2 <= 60 Min., P3 <= 2 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

22 Frage 113:

REQ-095

SLA

Statusupdates mindestens P1 alle 30 Min, P2 alle 2 Std, P3 arbeitstäglich und P4 anlassbezogen/Reporting bereitstellen.

Sind die geforderten Update-Intervalle (P1 alle 30 Min., P2 alle 2 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

23 Frage 114:

REQ-098

Reporting

Jährlichen Bericht Angriffserkennung und jährliches sowie anlassbezogenes SzA-Nachweispaket liefern.

Wird ein bieterseitig zusammengestelltes SzA-Nachweispaket akzeptiert, das auf plattformgenerierten Auswertungen und ergänzender Prozessdokumentation beruht?

24 Frage 115:

REQ-102

Exit

Daten und Konfigurationen in marktüblichen Formaten über gesicherten Weg exportieren und nach bestätigter Übergabe nachweisbar löschen.

Wird für den Löschnachweis eine Löschbestätigung des Plattformherstellers auf Basis der dokumentierten Data-Retention-Policy akzeptiert, oder ist ein mandantenspezifisches, technisch verifizierbares Löschprotokoll gefordert?

44

Frage 122

Sehr geehrte Damen Und Herren,

25.09.2026 11:41:48

Sehr geehrte Damen und Herren,

Die genannten Tätigkeiten sind Bestandteil der Leistung des Auftragnehmers (D1 Kap. 7.3 bis 7.5). Die Mitwirkung des Auftraggebers regeln D1 Kap. 13.2 und 13.3

anbei eine weitere Bieterfrage mit der Bitte um Beantwortung:

Mit freundlichen Grüßen,

Vergabeabteilung

Welche fachlichen und administrativen Verantwortlichkeiten sind aus Sicht des Auftraggebers zwingender Bestandteil des zu erbringenden EDR-Managed-Service und welche Tätigkeiten können beim Auftraggeber verbleiben, sofern die geforderte Überwachung, Alarmbewertung, Response-Unterstützung, SIEM-/SOC-Integration, ServiceNow-Integration sowie die Verarbeitung der EDR-Telemetrie vollumfänglich sichergestellt werden? Bitte erläutern Sie insbesondere die erwartete Rollenverteilung für Policy-Management, Plattformadministration, Agentenmanagement, Rollen-/Rechteverwaltung, Plattform-Härtung und Hersteller-Support.

Abt 3.3

Vielen Dank und freundliche Grüße

45

Sehr geehrte Vergabestelle,

zur Sicherstellung einer vollständigen und effizienten Berücksichtigung aller vergaberelevanten Informationen bitten wir die Vergabestelle, die eingegangenen Bieterfragen einschließlich der

Sehr geehrte Damen und Herren, wir möchten uns zunächst dafür entschuldigen, dass die Fragen 92 bis 115 teilweise undeutlich übermittelt bzw. dargestellt wurden. Dies veranschaulicht jedoch exakt den Grund, weshalb wir im Vorfeld ausdrücklich darum gebeten

25.09.2026 12:24:06

jeweiligen Antworten konsolidiert, übersichtlich und in einem bearbeitbaren Format zur Verfügung zu stellen. Wir bitten um entsprechende Bereitstellung, da dies im Sinne aller Teilnehmenden ist.

Danke und beste Grüße

hatten, Bieterfragen einzeln und als reinen Text einzureichen – und nicht in Form von gesammelten PDF-Dokumenten oder Screenshots. Die systemseitige Verarbeitung solcher Dateiformate führt leider unweigerlich zu den aufgetretenen qualitativen Einschränkungen bei der Darstellung. Wir bitten dringend darum, diese Vorgabe für künftige Fragen zu beachten, um eine reibungslose Kommunikation im Sinne aller Beteiligten zu gewährleisten.

Mit freundlichen Grüßen

Vergabeabteilung

Abt 3.3

46

Frage 92

zu 92:

25.09.2026 12:46:00

Cybersecurity Managed Service als ein Los für SOC/SIEM, NDR, Vulnerability Management, EDR-Management und IoMT-Security erbringen. Kann der AG bestätigen, dass die Leistungsbereiche EDR-Management und IoMT-Security über qualifizierte Unterauftragnehmer/Partner innerhalb eines Loses erbracht werden dürfen, solange der Bieter die Gesamtverantwortung trägt?

Antwort wird nachgereicht

zu 93:

Siehe Antwort zu Frage 52. Für Export und Löschung gilt D1 Kap. 14.4.

zu Frage 94:

Siehe Antwort zu Frage 52.

Frage 93:

Hoheit über Rohdaten, Logs, Telemetrie, Incidents, Reports, Nachweise und Dokumentationen dauerhaft beim UKF belassen. Genügt es dem AG, wenn die Datenhoheit durch jederzeitigen vollständigen Lese- und Exportzugriff (API, CSV/JSON/PDF) sowie vertraglich zugesicherte Herausgabe und Löschung sichergestellt wird, auch wenn die Speicherung in der Hersteller-Cloud (Mandant des UKF) erfolgt?

zu Frage 95:

Ja. Eine durchgehende Vorhaltung ohne Wiederherstellungsvorlauf erfüllt die Mindestanforderung aus D1 Kap. 3.1.

zu Frage 96:

Siehe Antwort zu Frage 84.

Frage 94:

SIEM in UKF-eigenem Tenant bzw. UKF-eigener Instanz betreiben; alleinige administrative Kontrolle des Auftragnehmers ist ausgeschlossen. Der SIEM-Betrieb erfolgt bei der angebotenen Lösung in einem dedizierten, UKF-zugeordneten SaaS-Tenant mit UKF-Administratorrechten (Tenant Administrator), jedoch nicht als UKF-eigene Instanz. Kann der AG bestätigen, dass ein dedizierter, mandantentrennter SaaS-Tenant mit vollen UKF-Administrationsrechten die Anforderung erfüllt, oder führt dies zum Ausschluss?

zu Frage 97:

Siehe Antwort zu Frage 49.

Zu Frage 98:

Die Berichte nach D1 Kap. 12.6 und die Dokumentation sind in deutscher Sprache zu liefern (Kriterienkatalog Ziffer 4.12.9; D1 Kap. 3.8; Ziffer 5.3 EVB-IT System-AGB). Für die Plattformoberfläche besteht keine Sprachvorgabe. Siehe auch Antwort zu Frage 57.

Frage 95:

Sicherheitsdaten mindestens 12 Monate aufbewahren, davon mindestens 90 Tage Hot Storage; Rest innerhalb 24 Stunden wiederherstellbar. Ist die Anforderung 'Rest innerhalb 24 Stunden wiederherstellbar' auch erfüllt, wenn die gesamten Sicherheitsdaten über die volle Aufbewahrungsdauer permanent online und ohne Wiederherstellungsvorlauf durchsuchbar vorgehalten werden?

zu Frage 99:

Ja. Syslog und API zählen zu den marktüblichen Verfahren nach D1 Kap. 4.1. Sicherheitsrelevante Alarmer, Bewertungen und Kontextdaten müssen an das SIEM übergeben werden (D1 Kap. 8.7). Der Integrationskatalog enthält je Quelle die technische Anschlussart (D1 Kap. 9.3).

Frage 96:

Sicherheitsrelevante Daten ausschließlich innerhalb EU/EWR verarbeiten und speichern; Datenflüsse, Orte, Unterauftragnehmer und Herstellerzugriffe transparent darstellen. Wird die Anforderung der ausschließlichen EU/EWR-Datenhaltung erfüllt, wenn der produktive Mandant in

einer EU-Region betrieben wird, Support- und Analysezugriffe durch das 24x7-SOC jedoch im Follow-the-Sun-Modell auch aus Nicht-EU-Standorten erfolgen und dies über Standardvertragsklauseln (SCC) sowie technische Zugriffskontrollen abgesichert wird?

Frage 97:

Kundenbezogene Plattform- und Produktlizenzen im BYOL-Modell auf UKF führen; nicht übertragbare reine MSP-Lizenzmodelle sind ausgeschlossen. Für die SIEM-Plattform ist ein BYOL-Modell mit dem UKF als Lizenznehmer herstellerseitig nicht vorgesehen; die Lizenzierung erfolgt als Subscription auf den UKF als Vertragspartner. Kann der AG bestätigen, dass eine auf das UKF lautende, kündbare Subscription-Lizenz mit vertraglich gesichertem Datenexport die Anforderung erfüllt?

Frage 98:

Operative Service-Kommunikation, Eskalation, Regelkommunikation und Dokumentation gegenüber UKF auf Deutsch erbringen. Ist es ausreichend, wenn die gesamte operative Kommunikation, Eskalation und Regelkommunikation sowie die Berichtsaufbereitung auf Deutsch erfolgen, die Plattformoberfläche und die systemgenerierten Rohreports jedoch englischsprachig sind?

Frage 99:

Mindestens Identitätsdienste, Server, Endpunkte, E-Mail, Netzwerk-/Security-Komponenten, Cloud-Dienste und Erkenntnisse aus EDR/NDR/IoMT/VM in das SIEM integrieren. Können IoMT-Erkenntnisse über eine generische Schnittstelle (Syslog/API einer Drittlösung) in das SIEM integriert werden, sofern keine native IoMT-Integration des Herstellers vorliegt?

Frage 100:

SIEM für 400 GB sicherheitsrelevantes Logvolumen pro Tag kalkulieren und Quellen/Filter zur Zielerreichung optimieren. Wird das SIEM-Volumen von 400 GB/Tag als vertraglich fixiertes Gesamtvolumen unabhängig von der Endpunktzahl vereinbart, und ist eine monatliche Durchschnittsbetrachtung mit Lastspitzenausgleich zulässig?

Frage 101:

Unterbrechungen oder Qualitätsmängel kritischer Logquellen binnen 30 Minuten nach Feststellung melden. Wird für die Meldung von Logquellen-Unterbrechungen eine vertraglich vereinbarte Frist von 30 Minuten akzeptiert, die außerhalb des Standard-Produkt-SLA individualvertraglich zugesichert wird?

Frage 102:

Dokumentation für SzA-Nachweis auf RUN-Reifegrad 2 zum Go-Live und Reifegrad 3 spätestens 12 Monate nach Betriebsaufnahme ausrichten. Wird ein bieterseitig erstelltes SzA-Nachweispaket akzeptiert, das die Reifegradanforderungen mit plattformgenerierten Reports und Prozessdokumentation belegt, ohne dass der Plattformhersteller ein standardisiertes SzA-Paket bereitstellt?

Frage 103:

Bei Fortführung Tenable Konfigurationen, Scan-Profile und Asset-Daten übernehmen; bei Alternative Migrationskonzept mit Parallelbetrieb und Vermeidung von Erkennungslücken vorlegen. Ist bei Variante Ablösung eine Nachbildung der Tenable-Scan-Profile und ein Import der Asset-Daten über die

zu Frage 100:

Siehe Antwort zu Frage 68. Maßgeblich ist das Logvolumen je Tag (D1 Kap. 2.3; Preisblatt D5, LV 4.2). Eine Durchschnittsbetrachtung mit Lastspitzenausgleich ist nicht vorgesehen.

zu Frage 101:

Ja. Die Meldefrist von 30 Minuten nach D1 Kap. 4.2 ist eine vertragliche Pflicht des Auftragnehmers, unabhängig vom Produkt-SLA des Herstellers.

zu Frage 102:

Ja. Das Nachweispaket erstellt der Auftragnehmer (D1 Kap. 4.7, 10.18 und 12.6). Ein standardisiertes Paket des Plattformherstellers ist nicht gefordert. Maßgeblich sind die Anforderungen aus D1 Kap. 4.7.

zu Frage 103:

Ja. D1 Kap. 6.2 lässt die Übernahme oder den Neuaufbau von Scan-Profilen zu. Eine herstellerseitig unterstützte Migration wird nicht gefordert. Das Migrationskonzept muss die in D1 Kap. 6.2 genannten Inhalte abdecken.

zu Frage 104:

Nach D1 Kap. 6.3 müssen Authenticated Scans, agenten- oder API-basierte Erhebung sowie der Import vorhandener Scan-Ergebnisse unterstützt werden. Das Scanning ist so zu gestalten, dass eine kontinuierliche Sichtbarkeit auf den aktuellen Schwachstellenstand entsteht (D1 Kap. 6.3). Ob vorhandene Scan-Ergebnisse übernommen werden, legt der Auftraggeber in der Feinkonzeption fest.

Frage 105:

Siehe Antwort zu Frage 18. Ein bestimmtes Werkzeug ist nicht vorgegeben (D1 Kap. 3.6). D1 Kap. 6.3 fordert für die genutzten Cloud-Dienste eine grundlegende Konfigurations- und Härungsprüfung gegen anerkannte Benchmarks (z. B. CIS, herstellereigene Best Practices). Auswertbare Befunde fließen in die Priorisierung ein. Die Auswertung von Audit-Ereignissen allein erfüllt dies nicht.

zu Frage 106:

Ja. D1 Kap. 7.5 schreibt keine Dokumentation im SIEM vor. Ausnahmen, Ausschlüsse und Konfigurationsänderungen werden über das abgestimmte Berechtigungs- und Freigabemodell behandelt und revisionssicher protokolliert. Policy-Änderungen werden im Change-Management-Prozess geführt (D1 Kap. 7.5). Changes sind Vorgangsarten der

VDR-API ausreichend, oder wird eine native, herstellerseitig unterstützte Migration der Tenable-Konfiguration gefordert?

Frage 104:

Authenticated Scans, Agent-API-Erhebung, Import bestehender Ergebnisse, kontinuierliche Sicht sowie Asset Discovery unterstützen. Ist die Anforderung erfüllt, wenn die Erhebung über authentifizierte Netzwerk-Scans und API-Connectors ohne zusätzlichen Endpunkt-Agenten erfolgt, und kann auf den Import historischer Scan-Ergebnisse aus dem Altsystem verzichtet werden?

Frage 105:

Webanwendungsprüfungen und grundlegende Cloud-Konfigurations-/Härtungsprüfungen, insbesondere M365/Entra ID, erbringen. Genügt es, M365/Entra-ID-Härtung über die kontinuierliche Auswertung von Konfigurations- und Audit-Ereignissen im SIEM abzudecken, wenn keine dedizierte CSPM-Prüfung im Vulnerability-Management-Werkzeug vorhanden ist?

Frage 106:

Baseline-Policies für Server, Client und VDI pflegen; Ausnahmen und Änderungen revisionssicher dokumentieren und Rollback ermöglichen. Ist es zulässig, die revisionssichere Dokumentation der EDR-Policy-Änderungen im Change-Register des Auftragnehmers und in der jeweiligen EDR-Herstellerkonsole zu führen, statt im SIEM selbst?

Frage 107:

IoMT-Security für ca. 5.000 vernetzte Medizingeräte dimensionieren und ausschließlich passiv, nicht-invasiv betreiben. Kann der AG bestätigen, dass die IoMT-Security über eine spezialisierte Drittlösung eines Partners erbracht und deren Erkenntnisse in das SIEM integriert werden dürfen, ohne dass dies zum Ausschluss führt?

Frage 108:

Initial- und Nachschulungen für IT-Betrieb, Informationssicherheit, Medizintechnik und Service-Steuerung durchführen; versioniertes Betriebshandbuch übergeben. Ist es ausreichend, wenn die Schulungen für IT-Betrieb, Informationssicherheit, Medizintechnik und Service-Steuerung auf Deutsch durchgeführt werden, die herstellerseitigen Schulungsunterlagen und Videos jedoch in englischer Sprache vorliegen?

Frage 109:

TTT einhalten: P1 <=15 Min, P2 <=30 Min, P3 <=60 Min. Sind die geforderten TTT-Werte (Time-to-Triage: P1 <= 15 Min., P2 <= 30 Min., P3 <= 60 Min.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

Frage 110:

TTV einhalten: P1 <=30 Min, P2 <=60 Min, P3 <=4 Std. Sind die geforderten TTV-Werte (Time-to-Verify: P1 <= 30 Min., P2 <= 60 Min., P3 <= 4 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Regime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

Frage 111:

ServiceNow-Integration (D1 Kap. 11.2).

zu Frage 107:

Die Anforderungen sind herstellerneutral formuliert (D1 Kap. 3.6). Die Lösung muss D1 Kap. 8 erfüllen, einschließlich des Nachweises nach D1 Kap. 8.1 (siehe Antwort zu Frage 62). Die Lizenz ist auf das UKF zu führen (D1 Kap. 3.2; Preisblatt D5, LV 8.2). Zur Einbindung in das SIEM siehe Antwort zu Frage 99. Der Einsatz von Nachunternehmern richtet sich nach Abschnitt IV der Verfahrensinformationen.

zu Frage 108:

Nein. Schulungen sind in deutscher Sprache durchzuführen, und die Schulungsunterlagen sind in deutscher Sprache geschuldet (Ziffer 2.5 EVB-IT System-AGB; D1 Kap. 9.7). Ergänzend bereitgestellte englischsprachige Herstellerunterlagen ersetzen diese nicht.

zu Frage 109:

Siehe Antwort zu Frage 54. Die Rechtsfolgen bei Überschreitung regelt § 8 der Anlage „EVB-IT Exit SLA Vergütung SOC-SIEM“.

zu Frage 110:

Siehe Antwort zu Frage 109.

zu Frage 111:

Siehe Antworten zu Fragen 54 und 109.

zu Frage 112:

Siehe Antwort zu Frage 109.

zu Frage 113:

Die Mindestintervalle nach D1 Kap. 12.4 sind verbindlich (siehe Antwort zu Frage 54).

zu Frage 114:

wir nachgereicht

zu Frage 115:

Gefordert ist ein Löschprotokoll des Auftragnehmers mit Art, Umfang, Speicherorten, Zeitpunkt, Verfahren und verantwortlicher Stelle (D1 Kap. 14.4; Anlage „EVB-IT Exit SLA Vergütung SOC-SIEM“, § 4 Abs. 3). Eine allgemeine Löschbestätigung des Plattformherstellers genügt dafür nicht.

TTC einhalten: P1 <=15 Min, P2 <=30 Min, P3 <=4 Std. Sind die geforderten TTC-Werte (Time-to-Contain: P1 <= 15 Min., P2 <= 30 Min., P3 <= 4 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Reg ime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?
Sofern verbindlich: Wird die Wartezeit auf die gemäß Leitplanke REQ-022 erforderliche UKF-Freigabe aus der Messung herausgerechnet?

Frage 112:

TTN einhalten: P1 <=15 Min, P2 <=60 Min, P3 <=2 Std. Sind die geforderten TTN-Werte (Time-to-Notify: P1 <= 15 Min., P2 <= 60 Min., P3 <= 2 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Reg ime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

Frage 113:

Statusupdates mindestens P1 alle 30 Min, P2 alle 2 Std, P3 arbeitstäglich und P4 anlassbezogen/Reporting bereitstellen. Sind die geforderten Update-Intervalle (P1 alle 30 Min., P2 alle 2 Std.) als vertraglich verbindliche Service Level Agreements mit Pönal-/Service-Credit-Reg ime festzuschreiben, oder versteht der AG diese Werte als Service Level Objectives (Zielwerte) ohne unmittelbare vertragliche Sanktionierung?

Frage 114:

Jährlichen Bericht Angriffserkennung und jährliches sowie anlassbezogenes SzA-Nachweispaket liefern. Wird ein bieterseitig zusammengestelltes SzA-Nachweispaket akzeptiert, das auf plattformgenerierten Auswertungen und ergänzender Prozessdokumentation beruht?

Frage 115:

Daten und Konfigurationen in marktüblichen Formaten über gesicherten Weg exportieren und nach bestätigter Übergabe nachweisbar löschen. Wird für den Löschnachweis eine Löschbestätigung des Plattformherstellers auf Basis der dokumentierten Data-Retention-Policy akzeptiert, oder ist ein mandantenspezifisches, technisch verifizierbares Löschprotokoll gefordert?