IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Beantwortung Bieterfragen
SIEM & SOC System

15.07.2025

Klinikum Mittelbaden gGmbH
Balger Str. 50
76532 Baden-Baden

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Bieterfrage 1

Betrifft Ziffer 3 (1) der LTMG-BW: Nach Ziffer 3 soll der Auftragnehmer dem Auftraggeber bei einer Kontrolle die Entgeltabrechnungen, und andere Geschäftsunterlagen des Auftragnehmers vorlegen. Erklärt sich der Auftraggeber damit einverstanden, dass etwaige Unterlagen und Nachweise über Entgeltzahlungen unter Beachtung des Datenschutzrechts auch in anonymisierter bzw. pseudonymisierter Form zu Kontrollzwecken vorgelegt werden können?

Antwort Bieterfrage 1

Ein Austausch von anonymisierten Daten ist ausreichend.

Bieterfrage 2

Aus der Vorankündigung können wir entnehmen, dass Sie für das Projekt im genannten Zeitraum ein Budget von 560 000,00€ angesetzt haben. Gehen wir Recht in der Annahme, die zur Verfügung zu stellende Angebote diesen Wert nicht überschreiten sollten?

Antwort Bieterfrage 2

Der von Ihnen genannte Betrag basiert auf dem Schätzwert aus unserer Markterkundung im Vorfeld der Ausschreibung. Bitte beachten Sie, dass wir im Rahmen des Vergabeverfahrens keine Aussagen zur individuellen Kalkulation einzelner Bieter treffen oder Vorgaben hierzu machen können. Jeder Bieter ist angehalten, seine Angebotskalkulation eigenständig und unter Berücksichtigung der Ausschreibungsunterlagen vorzunehmen.

Bieterfrage 3

Sie verlangen als A-Kriterium "SOC 2 Type II oder vergleichbar zertifiziert". Die außerhalb der USA international und im europäischen Raum anerkannte Alternative SOC 2 Type II ist ISO/IEC 27001. Im Gegensatz zu SOC 2, das auf Prinzipien basiert, ist ISO 27001 prozessorientiert und verlangt ein vollständiges ISMS und ist damit sogar hochwertiger anzusehen.
Dennoch verlangen Sie zusätzlich auch noch die ISO 27001 als separates A-Kriterium, welches einen Wiederspruch in sich darstellet. Gehen wir Recht in der Annahme, dass mit der Erfüllung der ISO27001 gleichzeitig die Forderung "SOC 2 Type II oder vergleichbar zertifiziert" vollumfänglich erfüllt ist

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Antwort Bieterfrage 3

Aufgrund der Ähnlichkeit dieser Zertifizierungen, wird eine ISO 27001 für Informationssicherheit als vergleichbar akzeptiert.

Bieterfrage 4

Gehen wir Recht in der Annahme, dass SOC-Provider sämtliche Lizenzen als Reseller selbst bereitstellen muss, oder können diese auch separat, beispielsweise direkt über die Lösungsanbieter oder Cloud-Marktplätze wie Azure Market Place, vom Klinikum Mittelbaden bezogen werden?

Antwort Bieterfrage 4

Ja, der Auftragnehmer muss die Lizenzen als Reseller bereitstellen.

Bieterfrage 5

Bis wann können Bieterfragen gestellt werden?

Antwort Bieterfrage 5

Bieterfragen können bis einschließlich 09.07.2025 gestellt werden.

Bieterfrage 6

Ist der Auftraggeber damit einverstanden, dass für die Anbindung an unsere Systeme bestimmte Forwarder eingesetzt werden? Wenn ja: Gibt es eine Umgebung, wo z.B. virtuelle Maschinen installiert werden können?

Antwort Bieterfrage 6

Nein, eine Installation auf der ESX-Umgebung ist nicht vorgesehen.

Bieterfrage 7

Möchten Sie neben dem Reporting auch Zugriff auf unsere Kundenoberfläche? Wenn ja, für wie viele Benutzer?

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Antwort Bieterfrage 7

Es wird im Lastenheft unter Kriterium A03-28 ein „zentrales Dashboard zur Suche von Ereignissen (Self Service Dashboard)" als A-Kriterium gefordert.
Der Zugriff auf das Dashboard muss min. für zwei gleichzeitige Benutzer möglich sein.

Bieterfrage 8

Ist ein Verweis im Lastenheft (Datei "Lastenheft SIEM") auf eine z.B. erläuternde Präsentation zulässig? Wenn ja: gibt es hierfür Einschränkungen? Gilt dies im Sinne "Leistungsbeschreibung" nach den einzureichenden Anlagen?

Antwort Bieterfrage 8

Ja, Erläuterungen zum Lastenheft sind zulässig und können als Anlage beigelegt werden.

Bieterfrage 9

Im Formular "Angebot für Dienstleistungen - 25003 KOMM EU ANG" wird der EVB-IT als Bestandteil genannt. Ist dieser vorausgefüllt dem Angebot beizufügen oder wird er erst mit der Zuschlagerteilung notwendig?

Antwort Bieterfrage 9

Der Vertrag wird mit der Zuschlagserteilung mit den korrekten Daten befüllt und gegenseitig gezeichnet.

Bieterfrage 10

Im Leistungsverzeichnis wird auf eine Trennung von IT und OT hingewiesen: Soll die angefragt Leistung beide Bereiche abdecken? Können Sie mehr Details zur Trennung der Segmente geben?

Antwort Bieterfrage 10

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Ja, es sollen beide Bereiche abgedeckt werden.
Die Netze IT, OT und MT sind durch Firewalls in separate VLANs aufgeteilt.

Bieterfrage 11

Gibt es eine bestehende Verantwortlichkeitenmatrix (RACI-Matrix) für die IT-Auslagerungen? Und ist hier schon die SOC-Dienstleistung mit integriert? Falls ja, können Sie uns diese zur Verfügung stellen?

Antwort Bieterfrage 11

Nein, ist aktuell nicht vorhanden.
Dies soll im Rahmen des Workshops erarbeitet werden.

Bieterfrage 12

Inwiefern sollen externe Dienstleister in der bestehenden Servicelandschaft mit überwacht werden? Gibt es "You build it, you run it"-Systeme oder andere durch externe Dienstleister betriebene Systeme, die durch einen speziellen Serviceschnitt besondere Beachtung finden müssen? Oder können wir davon ausgehen, dass alle eingesetzten Geräte dem Klinikum auch gehören und dort Agents oder Sensoren installiert werden können?

Antwort Bieterfrage 12

Sensoren und Agents können überall installiert werden.

Bieterfrage 13

Welche Erwartungshaltung besteht bezüglich der Nutzung des Ticketsystems Matrix42?

Antwort Bieterfrage 13

Schaffung einer Schnittstelle zum eigenen System muss gegeben sein.

Bieterfrage 14

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Inwieweit existieren bereits Playbooks oder Erfahrungen mit diesen?

Antwort Bieterfrage 14

Es existieren aktuell keine Playbooks.

Bieterfrage 15

Inwiefern wird erwartet, dass der SOC-Dienstleister in bestehende Notfallübungen, Alarmübungen o.ä. involviert wird?

Antwort Bieterfrage 15

Der SOC Dienstleister soll an Notfallübungen und Alarmübungen vollumfänglich teilnehmen.

Bieterfrage 16

Für die Security Awareness: Inwiefern existieren bereits Regelungen oder Informationen für z.B. "Verhalten bei Cyberangriffen" o.ä.? Wurden bereits Schulungen durchgeführt?

Antwort Bieterfrage 16

Aufgrund der Vorgaben des ISB wurden bereits kleinere Schulungen durchgeführt.

Bieterfrage 17

In den Vergabeunterlagen wird von „Hersteller" gesprochen. Gehen wir recht in der An-nahme, das mit Hersteller auch ein Managed Security Service Provider (MSSP) gemeint ist?

Antwort Bieterfrage 17

Ja der Hersteller kann auch ein MSSP sein

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Bieterfrage 18

Gehen wir recht in der Annahme, dass ein MSSP-Angebot zulässig ist?

Antwort Bieterfrage 18

Ja das ist zulässig

Bieterfrage 19

Im Preisblatt wird unter den Positionen 1.1.1–1.1.2 „keine Kapazitätsbegrenzung" angege-ben. Bedeutet dies, dass Lösungen zur Ingest Data (Datenaufnahme/-import) nicht berück-sichtigt werden sollen? Falls Ingest Data-Lösungen zulässig sind: Können Sie bitte bestäti-gen, dass für die Angebotskalkulation eine angenommene Datenmenge von ca. 50 TB pro Jahr als Vergleichsmaßstab verwendet werden kann? Sollte eine andere Mengenvorgabe maßgeblich sein, bitten wir um entsprechende Angabe, um eine ordnungsgemäße und vergleichbare Kalkulation sicherzustellen.

Antwort Bieterfrage 19

Es wird davon ausgegangen das eine Datenmenge von mindesten 50TB Logdaten auf der Cloudplatform des Dienstleisters belegt wird.
Hierbei handelt es sich um eine Schätzung, welche stark von dem genutzten System und der Effizienz des LOG-Transport und der Speicherung abhängt.
Enthalten sein muss der Datentransport zum Dienstleister aus den verschiedenen Quellsystemen sowie die Aufbewahrung der Daten.

Bieterfrage 20

In der Anforderung A01-3 wird abgefragt, dass der Hersteller eine Kontaktaufnahme 24*7 erfüllt. Wenn wir MSSP-Leistungen anbieten, reicht es dem Klinikum, wenn dies durch den Serviceprovider sichergestellt wird?

Antwort Bieterfrage 20

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Ja das ist zulässig

Bieterfrage 21

Bezug A01-10: Wir betreiben ein eigenes Ticketingsystem, halten jedoch eine Anbindung an Ihr bestehendes Ticketingsystem für den sinnvolleren Ansatz, um eine zentrale, transpa-rente und effiziente Bearbeitung zu gewährleisten. Geht das Klinikum mit dieser Einschät-zung mit und welche technischen Anforderungen oder Präferenzen bestehen für eine sol-che Integration? Im Falle von Matrix42 haben wir dies bereits in anderen Kundenkonstella-tionen umgesetzt.

Antwort Bieterfrage 21

Hierbei wird lediglich abgefragt, ob ein Ticketsystem betrieben wird.
Eine Integration in Matrix 42 wird an dieser Stelle nicht gefordert.

Bieterfrage 22

A02-12: In Ihrem Lastenheft fragen Sie, ob SOC-Expert:innen stets physisch am SOC-Standort anwesend sind. In der modernen Arbeitswelt ist dies nicht mehr durchgängig der Fall, da auch für unsere Security-Expert:innen flexible Arbeitsmodelle wie Homeoffice eine wichtige Rolle spielen. Unsere SOC-Mitarbeitenden greifen im Homeoffice ausschließlich über eine mehrstufig abgesicherte, MFA-geschützte Jump-Umgebung auf die relevanten Systeme (z. B. SIEM) zu. Damit stellen wir sicher, dass höchste Anforderungen an Daten-schutz und Datensicherheit eingehalten werden. Falls dies Ihren Sicherheitsanforderungen entspricht, würden wir die Frage im Fragebogen mit „Ja" beantworten. Sollten Sie jedoch eine durchgehende physische Präsenz in einem dedizierten Gebäude fordern, müssten wir dies verneinen.

Antwort Bieterfrage 22

Es wird eine physische Präsenz von Experten am SOC-Standort gefordert.

Bieterfrage 23

A02-16: Es ist der Nachweis eines Bedrohungsanalyseteams von mindestens 10 Perso-nen gefordert. Wie soll dies nachgewiesen werden bzw. welche Art des Nachweises wird akzeptiert?

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Antwort Bieterfrage 23

Der Nachweis kann z.B. mittels geeigneten Zertifikaten (z.B. CISSP, CEH, OSCP) / Rollenprofilen mit Nachweis / Aus-/Fortbildungsbescheinigungen erfolgen.

Bieterfrage 24

A03-9: In Ihrem Lastenheft fordern Sie eine Nachbearbeitung von Sicherheitsvorfällen ohne etwaige Mehrkosten (A-Kriterium). Um Missverständnisse zu vermeiden, bitten wir um Präzisierung: Bezieht sich diese Anforderung ausschließlich auf die Bereitstellung der im Rahmen des Incident-Managements erfassten Daten und Standard-Reports? Oder er-warten Sie darüberhinausgehende, individuell angepasste Berichte und Analysen, die auf Wunsch des Kunden jederzeit und flexibel, nach vom Kunden definierten Anforderungen erstellt werden sollen? Eine Klärung wäre für uns wichtig, um unser Angebot entsprechend Ihrer Erwartungen gestalten und die Kostenstruktur transparent darstellen zu können.

Antwort Bieterfrage 24

Es wird die Nachbereitung von durch den SOC detektierten sicherheitsrelevanten Vorfällen gefordert.
Mindestens die Erstellung von Incident-Reports und der resultieren Handlungsempfehlungen, ist Bestandteil der Dienstleistung und erfolgt ohne zusätzliche Vergütung.

Bieterfrage 25

A03-18: Was ist mit dieser Anforderung gemeint? Bitte erläutern Sie wie der ausgeschrie-bene Service bzw. die ausgeschriebene Technologie (SIEM) in bestehende Security Tools und Cloud Dienste integriert werden soll

Antwort Bieterfrage 25

Es wird abgefragt ob das SIEM / SOC Logs, Events oder Kontextinformationen aus bereits vorhandenen Sicherheitslösungen wie z.B. Virenscanner, VMware Systemen oder etwaigen Cloud-Diensten auslesen und verarbeiten kann.

Bieterfrage 26

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

A03-21: Sie schreiben "Network Detection and Response inkludiert". Was verstehen Sie genau unter diesem Punkt und welche Dienstleistungen fragen Sie konkret an? Gehen wir recht in der Annahme, dass ein Network Detection and Response System nicht durch den Auftragnehmer bereitzustellen und zu betreiben ist? Gehen wir ferner recht in der An-nahme, dass mit diesem Punkt ausschließlich die Anbindung eines durch den Auftragge-ber gestellten Network Detection and Response System an das SIEM System möglich sein muss?

Antwort Bieterfrage 26

Dieses Kriterium bezieht sich auf die LV POS 1.1.7 in der ein physischer Sensor gefordert wird.
Dieser muss den Datenverkehr unter anderem von den mehr als 300 vorhanden Netzwerkkomponenten analysieren und Risiken erkennen können.

Bieterfrage 27

A03-22: Was verstehen Sie konkret unter Guided Incident Response?

Antwort Bieterfrage 27

Es wird geforderte das der Auftragnehmer oder das SOC den Auftraggeber gezielt durch den Prozess der Reaktion auf einen Sicherheitsvorfall führt mit strukturierten Anleitungen und Handlungsempfehlungen

Bieterfrage 28

Wir bitten um Konkretisierung, ob die geforderten Referenzen zwingend aus dem Gesundheits- bzw. Kliniksektor stammen müssen oder ob auch branchenunabhängige, rein leistungsbezogene Referenzen zugelassen sind.

Antwort Bieterfrage 28

Referenzen können rein Leistungsbezogen (Branchenunabhängig) angegeben werden.

Bieterfrage 29

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Ist vorgesehen, dass die derzeit eingesetzte XDR-Lösung „Cybereason" vollständig abgelöst wird, oder soll diese weiterhin in die bestehende Sicherheitsarchitektur integriert bleiben?

Antwort Bieterfrage 29

Die bestehende Sicherheitsarchitektur bleibt erhalten.

Bieterfrage 30

Ist die Lösung Cybereason aktuell vollumfänglich auf sämtlichen Servern und Clients ausgerollt? Diesbezüglich bitten wir um eine Bestätigung, insbesondere in Bezug auf die Positionen gemäß Leistungsverzeichnis „25003 LV", Punkte 1.1.1 bis 1.1.2. Nur bei einer Ablösung von Cybereason könnten wir für die dort genannten Positionen Preise für ein alternatives XDR-Produkt anbieten

Antwort Bieterfrage 30

Cybereason ist vollständig ausgerollt und soll nicht durch ein alternatives Produkt ersetzt werden

Bieterfrage 31

Sofern die bestehende XDR-Lösung (Cybereason) alle Clients und Server abdeckt, ist davon auszugehen, dass bereits ein hoher Schutz besteht. Dürfen wir davon ausgehen, dass eine zusätzliche Überwachung der ca. 3.000 Clients über das SIEM nicht zwingend erforderlich ist? Oder sollen die Clients ausdrücklich in den SIEM-Scope mit aufgenommen werden? Wir bitten um eine klare Rückmeldung.

Antwort Bieterfrage 31

Es sind sämtliche Clients in das SIEM zur Überwachung einzubinden.
Hierzu ist auch eine Anbindung an die vorhandene XDR von Cybereason möglich.

Bieterfrage 32

Im Leistungsverzeichnis werden 3.000 Clients genannt, während in den ergänzenden Unterlagen von 1.650 PC-Arbeitsplätzen und Notebooks die Rede ist. Wir bitten um

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Klärung, wie diese Zahlen zueinanderstehen und welche Gesamtanzahl für die Kalkulation verbindlich zugrunde zu legen ist.

Antwort Bieterfrage 32

Für die Kalkulation ist die Anzahl in der Position 1.1.1, 1.1.2 im LV entscheidend.

Bieterfrage 33

- Wie viele der insgesamt 250 Switches sind als Core-Switches im Einsatz?
- Wird die Fortinet-Umgebung (15 Firewalls) mit FortiManager und FortiAnalyzer betrieben?
- Beziehen sich die 20 Server mit ca. 350 VMs ausschließlich auf die im Dokument „Aktuelle Umgebung" beschriebenen Systeme?
- Welche Storage-Lösung ist im Einsatz (z. B. SAN-System, Veeam)?
- Existieren zusätzliche Kerninfrastrukturkomponenten wie Domain Controller, E-Mail-Archivierung, Jumphosts etc., oder sind diese innerhalb der genannten 20 Server und 350 VMs enthalten?

Antwort Bieterfrage 33

- 4 Switche sind im Datacenter als „Core Switches" im Einsatz
- Ja, der Fortimanager ist für die Komponenten(FortiGate/FortiAnalyzer/FortiAuthenticator) im Einsatz
- Das Klinikum betreibt derzeit 20 Physische Server auf denen insgesamt 350 Virtuelle Maschinen in Betrieb sind
- Es ist ein Storage des Herstellers Netapp im Einsatz
- Diese Systeme sind in der genannten Anzahl enthalten

Bieterfrage 34

Im Leistungsverzeichnis wird mehrfach auf „Cloud-Plattformen" verwiesen. Wir bitten um Konkretisierung, ob damit eine reine Cloud-basierte SIEM-Lösung gefordert ist oder ob alternativ auch eine On-Premises-Lösung innerhalb der eigenen Infrastruktur oder bei einem Host-Provider ihrer Wahl zulässig ist.

Antwort Bieterfrage 34

Eine OnPremise Installation im Rechenzentrum des Klinikum ist nicht zulässig, eine Installation in einem externen Rechenzentrum wäre zulässig jedoch zwingend als

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

vollständige Lösung welchen den Aufbau, Betrieb und Service von Soft- und Hardwarekomponenten durch den Auftragnehmer vollständig abdeckt.

Bieterfrage 35

Ist es korrekt, dass im Leistungsverzeichnis Positionen 1.1.7 und 1.1.8 auch OT-Komponenten (Operational Technology) mit umfasst sind und mit überwacht werden sollen? Falls ja, bitten wir um detaillierte Angaben zu den betreffenden OT-Komponenten.

Antwort Bieterfrage 35

Nein, im Rahmen der Ausschreibung nicht vorgesehen.

Bieterfrage 36

In den Unterlagen wird ein EVB-IT Cloudvertrag bereitgestellt. Unsere SIEM-Lösung ist jedoch als On-Premises-Lösung ausgelegt, bei der die Datenhaltung vollständig im Rechenzentrum des Auftraggebers verbleibt. Daher wäre aus unserer Sicht der EVB-IT Servicevertrag die geeignete Vertragsgrundlage. Wir bitten um Bestätigung, ob in diesem Fall die Verwendung des EVB-IT Servicevertrags möglich ist.

Antwort Bieterfrage 36

Eine On-Premise Installation ist nicht vorgesehen, daher ist der EVB-IT Servicevertrag nicht passend.

Bieterfrage 37

Wir bitten um Erläuterung des Hintergrunds und der konkreten Anforderungen an den Vor-Ort-Support, insbesondere vor dem Hintergrund, dass bei einem Managed SOC Service typischerweise eine zentrale, remote erbrachte Überwachung und Reaktion vorgesehen ist. Welche Leistungen oder Tätigkeiten sollen nach Ihrer Vorstellung zwingend vor Ort erbracht werden? Gibt es spezifische Einsatzszenarien (z. B. Hardware-Tausch, forensische Sofortmaßnahmen, persönliche Beratungstermine), die Vor-Ort-Präsenz erforderlich machen?

Antwort Bieterfrage 37

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Mögliche VorOrt Einsätze könnten z.B. die Unterstützung nach einem Incident bei großflächigen Störungen, den Tausch von physischen Bauteilen oder ergänzende Beratungen sein.

Bieterfrage 38

Unser Unternehmen betreibt selbst kein eigenes Rechenzentrum, da wir als reiner SOC-Dienstleister mit einer On-Premises-SIEM-Lösung arbeiten, welche standardmäßig innerhalb der Infrastruktur des Auftraggebers implementiert wird. Optional besteht die Möglichkeit, die Lösung über unseren Partner in deren zertifiziertem Rechenzentrum (Tier 3+ bzw. kombinierter Betrieb Tier 4) zu hosten. Wir bitten um Bestätigung, ob die Bereitstellung und der Betrieb des SIEM-Systems in einem nachweislich Tier 3+ oder Tier 4 zertifizierten Rechenzentrum eines Partnerunternehmens als gleichwertig angesehen wird und damit den Anforderungen gemäß A02-3 und A02-4 entspricht.

Antwort Bieterfrage 38

Die Kriterien A02-3 und A02-4 wären mit der vollständigen Bereitstellung und dem Betrieb aus einem Rechenzentrum der Klasse Tier3+ oder Tier 4 vollständig erfüllt.

Bieterfrage 39

Unser SOC ist nach ISO 27001 auf Basis BSI IT-Grundschutz zertifiziert. Die Kernprozesse (SIEM/XDR/EDR) werden ausschließlich in unserem eigenen SOC Deutschland betrieben.
Das SOC arbeitet in einem vollwertigen 3-Schicht-Betrieb (7/24/365) mit Präsenzpflicht für das Level 1 (kein Homeoffice, kein Outsourcing). Die gesamte Dienstleistung wird zentral in Deutschland erbracht, ohne den Einsatz von Unterauftragnehmern.
Wir bitten um Bestätigung, dass mit dieser zentralen Betriebsstruktur die Anforderungen aus A02-6 (Europa) und A02-7 (Deutschland) vollumfänglich erfüllt sind und die volle Punktzahl erreicht wird.

Antwort Bieterfrage 39

Die Kriterien A02-6 und A02-7 wären mit dieser Form der Bereitstellung erfüllt

Bieterfrage 40

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Bitte konkretisieren Sie, welcher Form der Nachweis zur Teamgröße und Qualifikation gefordert wird:
• Reicht eine anonymisierte Übersicht mit Anzahl, Funktion und Zertifizierungen der Mitarbeiter (z. B. in Tabellenform oder als Organigramm)?
• Müssen darüber hinaus weitere Nachweise (z. B. Kopien von Zertifikaten oder eine namentliche Auflistung der Fachkräfte) eingereicht werden?
Analog bitten wir um verbindliche Klärung für die Anforderungen an A05-1 (mindestens 10 ausgebildete Personen für das SOC) sowie A05-2 (Nachweis der Anzahl der Fachtechniker für das SOC mit Bewertungsstufen).
Wir bitten um verbindliche Klarstellung, um die Nachweisführung für alle genannten Punkte (A02-16, A05-1, A05-2) entsprechend den Anforderungen korrekt und prüfbar vorbereiten zu können.

Antwort Bieterfrage 40

Der Nachweis kann z.B. mittels geeigneter Zertifikate (z.B. CISSP, CEH, OSCP) / Rollenprofilen mit Nachweis / Aus-/Fortbildungsbescheinigungen erfolgen.

Bieterfrage 41

In der Ausschreibung für das Klinikum Mittelbaden handelt es sich um eine SOC/SIEM-Ausschreibung. Laut Lastenheft wird NDR als Muss-Kriterium definiert. Nach unserem Verständnis ist NDR jedoch eine eigenständige Lösung, die sich auf Netzwerk-Traffic-Analyse und -Erkennung spezialisiert und nicht Teil einer klassischen SIEM-Lösung ist.
Daher bitten wir um verbindliche Klärung, ob im Rahmen dieser Ausschreibung tatsächlich die Implementierung und der Betrieb einer vollständigen, eigenständigen NDR-Lösung zusätzlich zur SIEM-Lösung gefordert ist, oder ob es ausreicht, wenn die SIEM-Lösung über Netzwerk-Datenquellen korrelieren und auswerten kann

Antwort Bieterfrage 41

Die Lösung muss die Netzwerk Datenquellen auslesen und auswerten können hierzu soll eine Überwachung von Netzwerkverkehr Layer 2-7 (Verbindungen, Protokolle, verdächtige Muster) möglich sein

Bieterfrage 42

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Nach unserem Verständnis beschreibt A03-22 eine uneingeschränkte Flatrate ohne Limitierung von Stunden oder Anzahl an Incidents, bei der Guided Incident Response pauschal abgedeckt ist.
Aus unserer Erfahrung sind Incident-Response-Fälle grundsätzlich nicht plan- oder vorhersehbar, können je nach Art und Schwere stunden-, tage- oder sogar wochenlange intensive Maßnahmen erfordern und sind daher nicht pauschalierbar.
Unser Modell basiert daher auf einem jährlichen, inkludierten Stundenkontingent, das explizit auch Tätigkeiten wie, Incident-Response-Leistungen, Beratung und Unterstützung bei Sicherheitsvorfällen abdeckt. Dieses Kontingent wird vertraglich fest vereinbart (z. B. 100 oder 200 Stunden) und kann bei Bedarf flexibel erweitert werden.
Wir bitten um verbindliche Bestätigung, ob dieses Modell mit inkludiertem Jahresstundenkontingent als gleichwertig zur geforderten Flatrate anerkannt wird oder ob zwingend eine uneingeschränkte Flatrate ohne Stundengrenze gefordert ist.

Antwort Bieterfrage 42

Es wird eine Flatrate gefordert, welche in den Kosten enthalten sein muss. Ein Stundenkontingent, welches immer wieder nachgefordert werden muss, ist nicht zulässig

Bieterfrage 43

Nach unserem Verständnis beschreibt A03-26 eine forensische Analyse, die pauschal und vollständig kostenfrei im Rahmen des Incident-Response-Prozesses enthalten ist, unabhängig von Aufwand und Dauer.
Aus unserer Erfahrung sind forensische Analysen grundsätzlich nicht plan- oder vorhersehbar, da diese je nach Art und Umfang des Vorfalls stunden-, tage- oder sogar wochenlange Detailuntersuchungen mit hochspezialisierten Ressourcen erfordern können. Diese Leistungen sind daher nicht pauschalierbar.
Unser Modell basiert auf einem jährlichen, inkludierten Stundenkontingent, das Incident-Response-Leistungen, forensische Analysen, Beratung und Unterstützung bei Sicherheitsvorfällen abdeckt. Dieses Kontingent wird vertraglich fest vereinbart (z. B. 100 oder 200 Stunden) und kann bei Bedarf flexibel erweitert werden. Nach Verbrauch erfolgt eine transparente Abrechnung nach Aufwand.
Wir bitten um verbindliche Bestätigung, ob dieses Modell mit inkludiertem Jahresstundenkontingent als gleichwertig zur geforderten pauschalen und kostenfreien forensischen Analyse anerkannt wird oder ob zwingend eine uneingeschränkte, komplett kostenfreie Leistung ohne Stundengrenze gefordert ist.

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Antwort Bieterfrage 43

Sofern Sie das B-Kriterium mit A03-26 „Forensiche Analyse nach Incident Kostenfrei enthalten" mit JA bestätigen ist dies kostenfrei zu liefern, ein Stundenkontingent ist dann nicht zulässig

Bieterfrage 44

Heute wurde ein neues Lastenheft hochgeladen, jedoch ohne Hinweis auf Änderungen oder Ergänzungen. Könnten Sie uns bitte mitteilen, welche konkreten Änderungen vorgenommen bzw. welche Ergänzungen hinzugefügt wurden?

Antwort Bieterfrage 44

Das Befüllen der Felder G24-G28 war in der Datei nicht möglich

Bieterfrage 45

Nach unserem Verständnis wird unter A01-2 sowie in Position 1.1.9 gefordert, dass der Vor-Ort-Support und die Inbetriebnahmeleistungen direkt durch den Anbieter erbracht werden.
Wir sind ein spezialisierter Cyber-Security-Dienstleister mit Fokus auf Managed SOC-, SIEM-, XDR-, MDR- und Awareness-Services. Tätigkeiten wie Vor-Ort-Support (z. B. Montage, physische Hardware-Installationen, Verkabelung) oder Dienstleistungen zur Inbetriebnahme fallen nicht in unseren originären Leistungsbereich.
Unser SOC stellt Ihnen eine virtuelle NIDS-Appliance bereit. Sie müssen lediglich die benötigte Hardware für die NIDS-Appliance beschaffen und in Ihrem Rechenzentrum gemäß Anleitung montieren. Unsere Kunden übernehmen diese Montage eigenständig.
Sobald das System angebunden ist (Strom, Netzwerk), unterstützen wir Sie bei der Implementierung, Konfiguration und Integration des Systems in unser SOC.
Warum wird diese Tätigkeit (Vor-Ort-Support und physische Inbetriebnahme) als A-Kriterium in einer SIEM-Ausschreibung definiert?
Solche Leistungen sind üblicherweise nicht Bestandteil einer Cyber-Security-Dienstleistung, sondern werden entweder durch ein IT-Systemhaus oder durch das interne IT-Team des Kunden übernommen.
Wir bitten um schnellstmögliche Rückmeldung, welche Optionen wir in diesem Zusammenhang hätten (z. B. Übernahme durch den Kunden selbst), ohne dass dies die Bewertung oder Vergabeentscheidung negativ beeinflusst.

Antwort Bieterfrage 45

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Die physisch zu liefernden Komponenten sind durch den Auftragnehmer oder einen möglichen benannten Nachunternehmer fachgerecht im System des Klinikums zu Integrieren. Hierbei unterstützt das Klinikum mit sämtlichen erforderlichen Leistungen wie z.B. Zugang zu den Räumlichkeiten oder Freischaltung von Ports.

Bieterfrage 46

Welche konkreten Geräte verbergen sich hinter den genannten 3.000 Clients & Endgeräten?
Verstehen wir es richtig, dass sich darunter die 1.680 PC-Arbeitsplätze und Notebooks befinden?
Falls ja, wie setzt sich die Differenz zu den insgesamt 3.000 Geräten zusammen?
Handelt es sich hierbei um medizinische Geräte, mobile Endgeräte, Drucker oder weitere Spezialsysteme?

Antwort Bieterfrage 46

Die detaillierte Aufschlüsselung der Geräte ist wie folgt: (siehe LV)

Folgende Geräte (ca. 3000 gesamt) sind aktuell Bestandteil der Umgebung:

- ca. 1650 Clients/Notebooks
- ca. 250 Switches, davon 4 DC Switches
- ca. 15 Firewalls (4x Large, 4x Medium und 7x Small)
- ca. 20 Server mit insgesamt ca. 350 VM´s
- Storage
- ca. 300 Access Points

+weitere Geräte (Medigeräte, Sandbox,...)

Bieterfrage 47

Sie geben an, dass die Lösung CyberReason vollumfänglich auf allen Clients und Servern ausgerollt ist.

Gilt dies gleichermaßen für die verbleibenden 1.350 Clients (Differenz zu den insgesamt 3.000 Clients), sodass auch diese vollständig über CyberReason abgesichert sind?

Zudem bitten wir um Präzisierung, welche Systeme oder Gerätetypen sich konkret hinter diesen 1.350 Clients verbergen, nach Abzug der 1.650 PC-Arbeitsplätze und

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Notebooks.
Diese Information ist für die genaue Definition des Schutzumfangs und die technische Planung essenziell.

Antwort Bieterfrage 47

Die detaillierte Aufschlüsselung der Geräte ist wie folgt: (siehe LV)

Folgende Geräte (ca. 3000 gesamt) sind aktuell Bestandteil der Umgebung:

- ca. 1650 Clients/Notebooks
- ca. 250 Switches, davon 4 DC Switches
- ca. 15 Firewalls (4x Large, 4x Medium und 7x Small)
- ca. 20 Server mit insgesamt ca. 350 VM´s
- Storage
- ca. 300 Access Points

+weitere Geräte (Medigeräte, Sandbox,...)

Bieterfrage 48

Was genau erwarten Sie mit der Anlage „Leistungsbeschreibung bzw. selbst gefertigte Kurzfassung oder Abschrift des Leistungsverzeichnisses mit den darin verlangten Angaben und Erklärungen"? Ist hier gegebenenfalls unsere eigene Leistungsbeschreibung gemeint?

Antwort Bieterfrage 48

Es ist hier nicht eine vom Auftragnehmer verfasste Leistungsbeschreibung gefordert. Eine Leistungsbeschreibung kann als Anhang beigelegt werden.
Erläuterung zu „Leistungsbeschreibung bzw. selbst gefertigte Kurzfassung oder Abschrift des Leistungsverzeichnisses mit den darin verlangten Angaben und Erklärungen":
Bieter haben die Möglichkeit für die Angebotsabgabe eine selbstgefertigte Abschrift oder Kurzfassung des Leistungsverzeichnisses zu benutzen, wenn sie den vom Auftraggeber verfassten Wortlaut des Leistungsverzeichnisses im Angebot als allein verbindlich anerkennen; Kurzfassungen müssen jedoch die Ordnungszahlen (Positionen) vollzählig, in der gleichen Reihenfolge und mit den gleichen Nummern wie in dem vom Auftraggeber verfassten Leistungsverzeichnis wiedergeben.

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Bieterfrage 49

Gehen wir Recht in der Annahme, dass ein Logdatenvolumen von maximal 750 GB/Tag realistisch ist? Aus unserer Erfahrung mit Krankenhäusern unterschiedlicher Größenordnung liegt der tatsächliche Wert wahrscheinlich eher darunter. Diese Information ist wichtig, um eine belastbare Kalkulation erstellen zu können.

Antwort Bieterfrage 49

Das tägliche Logdatenvolumen kann derzeit nicht detailliert angegeben werden da dies stark von der zu Implementierenden Lösung und deren Funktionalitäten zur Datenübertragung, Optimierung und Speicherung abhängig ist.
Es wird ein gesamter Speicherverbrauch im Rechenzentrum von ca. 50TB beim Dienstleister geschätzt.

Bieterfrage 50

Wir bitten weiterhin um eine Präzisierung, ob die 1650 PC-Arbeitsplätze und Notebooks in den genannten 3000 Clients enthalten sind.

Antwort Bieterfrage 50

Die detaillierte Aufschlüsselung der Geräte ist wie folgt: (siehe LV)

Folgende Geräte (ca. 3000 gesamt) sind aktuell Bestandteil der Umgebung:

- ca. 1650 Clients/Notebooks
- ca. 250 Switches, davon 4 DC Switches
- ca. 15 Firewalls (4x Large, 4x Medium und 7x Small)
- ca. 20 Server mit insgesamt ca. 350 VM´s
- Storage
- ca. 300 Access Points

+weitere Geräte (Medigeräte, Sandbox,...)

Bieterfrage 51

Gehen wir Recht in der Annahme, dass es eine Bieterpräsentation mit den drei bestplatzierten Anbietern geben wird, dass danach zur Abgabe eines finalen

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Angebotes aufgefordert wird und daher das derzeitige, erste Angebot nicht bezuschlagt wird?

Antwort Bieterfrage 51

Es werden die besten 3 Bieter nach Auswertung von Preis und Lastenheft zum Bietergespräch eingeladen. (Siehe Dokument Bewertungskriterien)
Den Zuschlag erhält der Bieter mit der besten Bewertung aus Preis 50% /Lastenheft 20% /Bietergespräch 30% auf das Erstangebot.
Es wird kein zusätzliches „Finales Angebot" vom Auftraggeber angefordert.

Bieterfrage 52

Sie fordern im Dokument "KOMM EU BB" unter Punkt 6., dass Leistungen von Unterauftragnehmern/ Eignungsleihern im Dokument "Komm EU (D) Erkl Andere/Unter" zu benennen sind. Wir bitten Sie diese Dokument zur Verfügung zu stellen

Antwort Bieterfrage 52

Haben wir als Nachtrag zur Verfügung gestellt.

Bieterfrage 53

Gehen wir mit unserer Annahme richtig, dass Sie mit der Position gemäß Lastenheft A03-22 „Flatrate für Guided Incident Response, Anzahl Fälle und zeitlicher Aufwand" sowie A03-26 „Forensische Analyse nach Incident kostenfrei enthalten" in erster Linie die grundsätzliche Verfügbarkeit der Incident-Response- und Forensik-Teams sicherstellen möchten?
Oder erwarten Sie hier explizit eine uneingeschränkte Flatrate ohne Begrenzung der Stunden, Fälle oder Aufwände, die ein Cyber-Vorfall verursacht?
In unserer SOC-Basisgebühr ist die Verfügbarkeit/Bereitschaft von L1-L3-Analysten (IR-Team/Forensik-Team) 24/7/365 inkludiert. Ist somit die Anforderung der Pos. A03-22 + A03-26 erfüllt?

Antwort Bieterfrage 53

Eine reine Verfügbarkeit der Techniker erfüllt das Kriterium nicht.
Im Kriterium A03-22 wird eine Flatrate für Anzahl der Fälle inkl. Arbeitszeit gefordert

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Sofern Sie das B Kriterium A03-26 „Forensische Analyse nach Incident kostenfrei enthalten" mit „JA" beantworten muss die Forensische Analyse nach einem Vorfall kostenfrei enthalten sein in der angebotenen Leistung.

Bieterfrage 54

Bezugnehmend auf Ihre Antwort zu unserer Bieterfrage 34, in der Sie erläutern, dass das SIEM-System nicht im Rechenzentrum des Klinikums Mittelbaden implementiert werden soll, sondern extern (z. B. in der Cloud), möchten wir hierzu eine ergänzende Klärung zum NDR-System einholen.
Bezieht sich diese Aussage ebenfalls auf das NDR-System?
Konkret: Soll das NDR-System in der Infrastruktur des Klinikums Mittelbaden (On-Premises) implementiert werden, oder ist – analog zum SIEM-System – auch hier eine externe (z. B. Cloud-)Implementierung vorgesehen?

Antwort Bieterfrage 54

Aufgrund der Tatsache das auf die im LV beschriebenen Switche, Firewalls oder Server Onboard Management Controllern im Regelfall keine Software/App installierbar ist, werden physische Sensoren zur Aufnahme und übertragen der Daten an das anzubietende Cloud System im Leistungsverzeichnis_V3 „LV Positionen 1.1.8 und 1.1.9" gefordert. Die Auswertung sowie die Aufbewahrung der LOG-Daten sollen im Cloud Rechenzentrum durch den Auftragnehmer/Dienstleister erfolgen.

Bieterfrage 55

Wie ist seitens des Klinikums Mittelbaden der Projektablauf für die Implementierung der Lösungen SIEM und NDR geplant? Aus unserer Erfahrung starten wir in solchen Projekten grundsätzlich mit der Einführung des SIEM-Systems, um zunächst eine umfassende Sicht auf die Infrastruktur zu gewinnen, alle relevanten Logs zu normalisieren und erste Use Cases aufzubauen.
Basierend auf diesen Erkenntnissen und der etablierten Log-Normalisierung erfolgt anschließend die Implementierung und Konfiguration des NDR-Systems, um eine tiefere Netzwerküberwachung und zusätzliche Schutzebenen aufzubauen.
Entspricht dieses gestufte Vorgehen auch dem gewünschten Ablauf seitens Klinikum Mittelbaden, oder ist explizit gefordert, beide Lösungen (SIEM und NDR) parallel einzuführen?
Aus technischer und organisatorischer Sicht empfehlen wir ausdrücklich, zunächst das SIEM-System vollständig umzusetzen, bevor das NDR-System ergänzt wird

Antwort Bieterfrage 55

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Die detaillierte Ausarbeitung der einzelnen Installationsschritten wird in dem in der Dienstleistung (Pos.1.1.10) geforderten Workshop zwischen Auftragnehmer und Auftraggeber erarbeitet.
Eine schrittweise Einführung ist möglich.

Bieterfrage 56

wir haben hier noch eine Frage zum Thema NDR.

- Wie viele IP-Adressen sollen insgesamt über das NDR abgedeckt werden?

- Um wie viele Standorte handelt es sich insgesamt?

- Wie viele lokale Breakouts (Internetanschlüsse) gibt es pro Standort?

Antwort Bieterfrage 56

Es handelt sich um zwei Standorte mit jeweils zwei Internet-Breakouts. Die genaue Anzahl der IP-Adressen wird im Rahmen des Workshops gemeinsam erarbeitet. Die Preiskalkulation erfolgt auf Basis der angegebenen Geräte und User.

Bieterfrage 57

In den Positionen LV 1.1.7 – 1.1.8 wird beschrieben, dass das NDR-System Logdaten von Endpoints, Firewalls, Servern, Switches etc. abfragen soll. Nach unserer Erfahrung und gängiger Praxis übernimmt diese Aufgaben jedoch in erster Linie ein SIEM-System, nicht ein NDR-System.
Wir bitten daher um eine Präzisierung, wie diese Anforderungen mit einem NDR-System in Zusammenhang stehen und ob hier ggf. eine Verwechslung oder ein Missverständnis vorliegt.

Darüber hinaus möchten wir anmerken, dass wir aus fachlicher Sicht empfehlen, zunächst ein SIEM-Projekt umzusetzen, um die Grundlagen für eine spätere NDR-Einführung zu schaffen. Erst im Anschluss sollte ein Proof of Concept (PoC) für ein NDR-System durchgeführt werden, um auf dieser Basis ein belastbares Sizing sowie eine belastbare Kostenplanung erstellen zu können.

Ein vorzeitiger Erwerb eines NDR-Systems birgt aus unserer Sicht das Risiko, dass der Kunde bereits für Lizenzen und Support zahlt, bevor die Implementierung sinnvoll beginnen kann (z. B. erst nach Abschluss des SIEM-Projekts), was einen

IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

erheblichen Nachteil darstellen würde.

Wir bitten daher um eine eindeutige Klarstellung zu diesen Punkten sowie um eine Bestätigung, ob die von uns vorgeschlagene Vorgehensweise (zunächst SIEM, anschließend NDR-PoC) im Sinne des Auftraggebers ist.

Antwort Bieterfrage 57

Die physischen Sensoren (LV 1.1.8 und 1.1.9) sollen Log Daten von den Hardwareprodukten abfragen können, auf denen keine Software installiert werden kann.

Details zur finalen Umsetzung können im Bietergespräch sowie dem vorgeschalteten Workshop besprochen werden.