IT-Planwerk GmbH
Hindenburgstraße 27
88361 Altshausen

Beantwortung Bieterfragen
SIEM & SOC System

04.07.2025

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.