Kommunale Wasserwerke Leipzig GmbH · Postfach 10 03 53 · 04003 Leipzig

An Alle Bieter

versendet via www.evergabe.de

Es schreibt Ihnen: Christopher Rudolph
Team Vergabe

Sitz: Berliner Str. 25
E-Mail Christopher.Rudolph2@L.de

15.05.2024

SOC für die Kommunale Wasserwerke Leipzig GmbH
Vergabe-Nr.: 24-019-003

Bewerberfragen 1-21

Sehr geehrte Damen und Herren,

anbei erhalten Sie die Bewerberfragen mit den entsprechenden Antworten fortlaufend.
Die Bewerberfragen 18 - 21 sind neu.

Bewerberfrage 1 vom 26.04.2024
Leistungsschein 1 SOC Seite 4 - Leistung "Vollständige Analyse aller auftretender Alarme im SIEM des AG: In Ihren Unterlagen haben Sie beschrieben, dass Sie sich bereits im Aufbau eines SIEM befinden. Aus unserer Sicht ist es nicht optimal, das SOC eines anderen Anbieters als den des SIEM zu nutzen (unser SOC arbeitet auf Basis unserer eigenen SIEM-Lösung). Wäre es für Sie denkbar, unsere unternehmenseigene SIEM-Lösung anstelle der aktuell im Aufbau befindlichen Lösung zu nutzen?
Antwort Bewerberfrage 1:
Die Analyse der Alarme durch das SOC soll auf Basis des SIEM des AG (Kommunale Wasserwerke Leipzig GmbH) erfolgen. Eine direkte Anbindung der SIEM Lösung des AN an die IT-Infrastruktur des AG ist nicht vorgesehen.

Bewerberfrage 2 vom 30.04.2024
Können Sie bitte spezifizieren, welches Security Information and Event Management (SIEM) System für die Analyse der Alarme durch das Security Operations Center (SOC) der Kommunalen Wasserwerke Leipzig GmbH eingesetzt wird?
Antwort Bewerberfrage 2:
Zum Einsatz kommt das SIEM System „Splunk“

Bewerberfrage 3 vom 30.04.2024
Leistungsschein 1 SOC Seite 4 Welche technischen Voraussetzungen muss der AN schaffen, um auf die SIEM-Umgebung des AN zuzugreifen?
Antwort Bewerberfrage 3:
Die detaillierten technischen Voraussetzungen werden im Rahmen der detaillierten Transitionsplanung ermittelt. Es kann jedoch - nicht abschließend - davon ausgegangen werden, dass Zugangsvoraussetzungen zu den Netzen des AG zu schaffen sind (z.B. Netzkopplung/ -zugriff per VPN) und alle weiteren Voraussetzungen, damit der AN auf das SIEM und die weiteren Systeme des AG zugreifen kann. Die Schaffung weiterer technischer Voraussetzungen wie z.B. der Einsatz von AG-Hardware ist nicht vorgesehen.

Bewerberfrage 4 vom 30.04.2024
Leistungsschein 1 SOC Seite 5 Wer trägt die Kosten für den Zugriff der SOC-Mitarbeiter des AG auf das SIEM des AN?
Antwort Bewerberfrage 4:
So wie die Frage gestellt ist kann sie nicht beantwortet werden, da es keine SOC-Mitarbeiter des AG gibt und geben wird und ein evtl. vorhandenes SIEM des AN nicht zum Einsatz kommt. Das SIEM wird vollständig durch den AG bereitgestellt. Unter der Annahme, dass die Frage lautet, wer die Kosten für den Zugriff der AN-Mitarbeiter auf das SIEM des AG trägt, lautet die Antwort, dass evtl. dafür benötigte Lizenzen durch den AG getragen werden, evtl. auftretende Kosten für den Zugriff innerhalb der Netze des AG trägt ebenfalls der AG. Alle weiteren Kosten für den Zugriff trägt der AN.

Bewerberfrage 5 vom 30.04.2024
Leistungsschein 1 SOC Seite 6 Welche Software inkl. Version ist derzeit für die Funktion SIEM beim AN im Betrieb?
Antwort Bewerberfrage 5:
Siehe Antwort zu Bewerberfrage 2 vom 30.04.2024

Bewerberfrage 6 vom 30.04.2024
Leistungsschein 1 SOC Seite 7 Werden seitens des AG Voraussetzungen (Schulungen, Zertifizierungen, etc.) bezogen auf die eingesetzte SIEM-Lösung vorausgesetzt?
Antwort Bewerberfrage 6:
Nein, Vorerfahrungen sind hier allerdings wünschenswert.

Bewerberfrage 7 vom 30.04.2024
Leistungsschein 1 SOC Seite 8 Wer betreibt die SIEM-Lösung anhand, welcher SLA-Parameter?
Antwort Bewerberfrage 7:
Der Betrieb des SIEM erfolgt komplett durch den AG bzw. durch den AG beauftragte Dienstleister und ist nicht Teil der Ausschreibung. SLA Parameter sind nicht definiert.

Bewerberfrage 8 vom 30.04.2024
Leistungsschein 1 SOC Seite 9 Wer pflegt das Regelwerk der SIEM-Lösung?
Antwort Bewerberfrage 8:
Die Pflege im Sinne der Anpassung von Regeln erfolgt komplett im Rahmen des Betriebes der SIEM-Lösung durch den AG (siehe Antwort auf Bewerberfrage 7 vom 30.04.2024). Es ist allerdings Teil dieser Ausschreibung (siehe Leistungsschein 1 SOC, 5.1, Pflege des IT-Services), den Regelsatz initial durch den AN zu erstellen und kontinuierlich zu verbessern und anzupassen. Die Umsetzung der Verbesserung erfolgt dann im Rahmen der Zusammenarbeit über das Ticketsystem des AG.

Bewerberfrage 9 vom 30.04.2024
Leistungsschein 1 SOC Seite 10 Welchen Einfluss haben hat das SOC des AN auf das Regelwerk der SIEM-Lösung des AG?
Antwort Bewerberfrage 9:
Siehe Antwort Bewerberfrage 8 vom 30.04.2024

Bewerberfrage 10 vom 30.04.2024
Mit Abgabe des Teilnahmeantrags müssen die Bewerber eine Vielzahl an Referenzen einreichen. Gem. dem Referenzformblatt müssen die Bieter den Namen des Auftraggebers und einen Ansprechpartner benennen. Bei sicherheitskritischen Themen wie SOC wollen Referenzgeber sowie die Ansprechpartner erfahrugnsgemäß nicht namentlich genannt werden. Eine Lösung wäre die Anonymisierung der Referenzen mit der Möglichkeit, dass über den Bewerber im Bedarfsfall der Kontakt vermittelt werden kann. Der Auftraggeber fordert für die spätere Angebotsabgabe ohnehin gem. Bewerbungs- und Ausschreibungsbedingungen S. 15: "Nennung von mindestens zwei Referenzkunden mit ähnlicher Größe und Branche, welche für Referenzgespräche zur Verfügung stehen" Spätestens zu diesem Zeitpunkt wird der AG einen Teil der Referenzen überprüfen. Dadurch ist es unserer Ansicht nach nicht notwendig, mit dem Teilnahmeantrag Kundennamen und Namen von Ansprechpartner der Referenzgeber zu nennen. Wir bitten Sie daher auch anonymisierte Referenzen zuzulassen.
Antwort Bewerberfrage 10:
Grundsätzlich sind anonymisierte Referenzen im Rahmen des Teilnahmewettbewerbs dann zulässig, wenn aus der Referenz erkennbar wird, warum sie für die LWW als AG relevant ist, und der Bewerber zusichert, dass im Bedarfsfall die Referenz komplett genannt und im Rahmen der Angebotsabgabe offengelegt wird.

Bewerberfrage 11 vom 30.04.2024
Welcher SIEM-Hersteller wird vom Auftraggeber eingesetzt?
Antwort Bewerberfrage 11:
Siehe Antwort zu Bewerberfrage 2 vom 30.04.2024

Bewerberfrage 12 vom 02.05.2024
In Abschnitt 8 des Rahmenvertrags fordert der Auftraggeber neben einer ISO/IEC-27001-Zertifizierung auch den Nachweis einer Zertifizierung nach ISAE 3402, Typ II. Im Teilnahmewettbewerb wird jedoch zunächst nur eine ISO/IEC-27001-Zertifzierung als Eignungsnachweis gefordert. Der Bieter und/oder sein Subunternehmer kann zahlreiche Referenzen für SOC- und CERT-Dienstleistungen im KRITIS-Sektor nachweisen. Da eine entsprechende ISAE-3402-Zertizierung mit erheblichen (finanziellen) Aufwänden verbunden ist, bittet der Bewerber um Streichung der Anforderung, so dass ein Nachweis des ISO/IEC 27001 Zertifikates, wie im TNA gefordert, ausreichend ist. Aus Sicht des Bieters ist die ISAE-3402 Zertifizierung relevant, wenn ein Unternehmen Prozesse auslagert, die für die Buchführung und Rechnungslegung relevant sind, was hier eindeutig nicht der Fall ist.
Antwort Bewerberfrage 12:
Der Hinweis ist korrekt, eine Zertifizierung nach ISAE-3402 ist wünschenswert und wird im Rahmen der Zuschlagserteilung nach Angebotsabgabe wertend berücksichtigt, ist allerdings kein Eignungskriterium und somit optional.

Bewerberfrage 13 vom 02.05.2024
In der Antwort auf die Bewerberfrage 1 vom 26.04.2024 werden 2 wesentliche Punkte geklärt: Das SIEM des AG soll genutzt werden und eine direkte Anbindung einer SIEM Lösung eines AN an die IT Infrastruktur des AG ist nicht vorgesehen. Da der Einsatz der SIEM-Lösung des Bieters damit ausgeschlossen ist, wäre es zwingend erforderlich zu wissen, welche SIEM Lösung aktuell bei dem AG eingesetzt wird. Es wird unter anderem gefordert, dass der AN "regelmäßige Verbesserungsmaßnahmen und -vorschläge für die Optimierung und Verbesserung des SIEM des AG" einbringt. Dies ist nach Ermessen des Bieters nur mit einer gewissen technischen Expertise für die eingesetzte Lösung möglich. Welche SIEM-Lösung wird beim AG eingesetzt?
Antwort Bewerberfrage 13:
Siehe Antwort zu Bewerberfrage 2 vom 30.04.2024

Bewerberfrage 14 vom 03.05.2024
Auf S. 30 der Bewerbungs- und Ausschreibungsbedingungen sollen die Bewerber "Angaben zu Zertifizierungen" machen. Abgesehen von der ISO27001 gibt es unserer Auffassung nach keine Mindestanforderung diesbezüglich. Der "Auswertungsmatrix Teilnahmeanträge" können wir keine Angabe entnehmen, dass es positiv bewertet wird, wenn ein Unternehmen über bestimmte weitere Zertifizierungen verfügt. Gehen wir daher recht in der Annahme, dass die Bewerber darstellen sollen, über welche für den Auftrag relevanten Unternehmenszertifizierungen sie verfügen?
Antwort Bewerberfrage 14:
Ja, hierbei ist auch Antwort zu Bewerberfrage 12 vom 03.05.2024 zu berücksichtigen.

Bewerberfrage 15 vom 03.05.2024
Auf S. 34 der Bewerbungs- und Ausschreibungsbedingungen sollen die Bewerber "Angaben zu Systempartnerschaften" machen. Als Hinweis ist vermerkt, dass es sich dabei sowohl um ein Ausschluss- als auch um ein Bonuskriterium handelt. Der "Auswertungsmatrix Teilnahmeanträge" können wir in Zeile 22 lediglich entnehmen, dass es sich um ein Bonuskriterium handelt. Gehen wir daher recht in der Annahme, dass es sich auf S. 34 der Bewerbungs- und Ausschreibungsbedingungen um ein redaktionelles Versehen handelt und dass die Angabe zu Systempartnerschaften lediglich ein Bonuskriterium ist?
Antwort Bewerberfrage 15:
Ja, korrekter Hinweis. Es handelt sich hier um einen redaktionellen Fehler, es handelt sich ausschließlich um ein Bonuskriterium.

Bewerberfrage 16 vom 03.05.2024
In der "Auswertungsmatrix Teilnahmeanträge" fordern Sie als Ausschlusskriterium unter "Sicherheits- und Geschäftsfortführung": "Grundlegende Anforderungen an das Vorliegen eines Sicherheits- und Geschäftsfortführungskonzepts und -plans für Dienstleister mit KRITIS-Bezug sind erfüllt oder übererfüllt" Ist damit ein Cybernotfallhandbuch inkl. Wiederanlaufkonzept gemeint, das vom Auftragnehmer im Zuschlagsfall erstellt werden soll? Falls nein, bitte konkretisieren Sie, was genau damit gemeint ist. Bitte konkretisieren Sie weiterhin, in welcher Form die Bewerber im Rahmen des TNA die Einhaltung der Anforderung nachweisen sollen. Wäre eine Eigenerklärung ausreichend?
Antwort Bewerberfrage 16:
Nein, es handelt sich hier um das Cybernotfallhandbuch des Bieters. Hierbei sollte der Bieter generell darstellen, dass ein entsprechender Prozess existiert und dokumentiert ist, und einen für Dritte nachvollziehbaren Überblick zu wesentlichen Merkmalen geben.

Bewerberfrage 17 vom 03.05.2024
In der "Auswertungsmatrix Teilnahmeanträge" fordern Sie als Ausschlusskriterium unter "Referenzen / Erfahrung CERT": "Mindestens 3 Referenzen für die Erbringung von CERT-Leistungen mit jeweils mindestens 3 Einsätzen / CERT-Aktivierungen pro Jahr" Unserer Ansicht nach bestätigen solche Referenzen nicht zwingend die Eignung eines Bewerbers. Wenn es zu drei Einsätzen im Jahr kommt, würden wir Handlungsbedarf bei der SOC-Lösung sehen. In Bezug auf die Eignung zum Thema CERT-Leistungen würden wir auf die APT-Response-Dienstleister-Zertifizierung des BSI verweisen wollen. Gehen wir recht in der Annahme, dass der Nachweis einer APT-Response-Dienstleister-Zertifizierung des BSI das Einreichen von "Referenzen / Erfahrung CERT" obsolet macht?
Antwort Bewerberfrage 17:
Nein, der Nachweis alleine genügt nicht. Mithilfe der Referenzabfrage wollen wir die praktischen Erfahrungen der vorgehaltenen CERT-Ressourcen überprüfen. Alternativ zur geforderten Referenznennung ist die Angabe der Gesamtzahl von mit CERT-Dienstleistungen betreuten Kunden (mind. 3) und die für alle Kunden des Bieters durchgeführten CERT-Aktivierungen pro Jahr zulässig (mind. 9). Es sind somit nicht zwingend 3 Aktivierungen pro betreutem Kunden notwendig.

Bewerberfrage 18 vom 14.05.2024
Dokument "24-019-003-200_Rahmenvertrag.pdf" Kapitel 17 Punkt 17.1 "Beachtung des technologischen Fortschritts": Ist der AN für das Patching des SIEMS inkl. Apps und Add Ons sowie des Betriebssystems verantwortlich?
Antwort Bewerberfrage 18:
Nein, der Betrieb des SIEM liegt in der Verantwortung des AG.

Bewerberfrage 19 vom 14.05.2024
Leistungsschein 1 SOC Seite 4 - Leistung "Vollständige Analyse aller auftretender Alarme im SIEM des AG: Darf eine Weiterleitung der Alarme (keine Events, Logs etc.) in eine zentrale Instanz des AN erfolgen?
Antwort Bewerberfrage 19:
Ja, eine Weiterleitung von Alarmen kann über ein vorhandenes SMS / Voice Gateway des Auftraggebers erfolgen.

Bewerberfrage 20 vom 14.05.2024
Inhaltliche Frage: Soll der SOC Service (Bewertung, Bearbeitung etc.) 24x7 oder 5x9 erfolgen?
Antwort Bewerberfrage 20:
Der SOC Service soll 24x7 erfolgen.

Bewerberfrage 21 vom 14.05.2024
In der Anlage I.1 Eigenerklärung zur Eignung inkl. Anlagen I.1a - I.1c ist geschrieben, dass bzgl. der Berufshaftpflichtversicherung eine Mindestsumme pro Schadensfall in Höhe von 5 Millionen EUR verlangt wird. Dies können wir nicht abdecken, sondern nur bis 3 Millionen. Ist dies ein Ausschlusskriterium, wenn dies nicht erfüllt ist, oder kann das Angebot trotzdem mit dem Hinweis eingereicht werden, dass die Summe weniger ist.
Antwort Bewerberfrage 21:
Sofern die derzeitige Haftpflichtversicherung die geforderte Deckung nicht enthält, ist es alternativ möglich, dass mit dem Teilnahmeantrag eine Eigenerklärung eingereicht wird. Aus dieser muss hervorgehen, dass im Auftragsfall eine Anpassung des Versicherungsschutzes in vollem geforderten Umfang erfolgen wird.

Diese Nachricht wird Bestandteil der Vergabeunterlagen und ist bei der Erstellung der Teilnahmeanträge zu beachten.

Freundliche Grüße
Kommunale Wasserwerke Leipzig GmbH

Dieses Dokument wurde maschinell erstellt und ist ohne Unterschrift gültig.