482683-2025 - Wettbewerb

Deutschland – IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung – SWA_MS SOC_SIEM_TNW
OJ S 139/2025 23/07/2025
Auftrags- oder Konzessionsbekanntmachung – Standardregelung
Dienstleistungen

1. Beschaffer

1.1. Beschaffer

Offizielle Bezeichnung: Stadtwerke Achim AG
E-Mail: alexandra.losch@hlp-rae.de
Rechtsform des Erwerbers: Öffentliches Unternehmen
Tätigkeit des Auftraggebers: Erzeugung, Fortleitung oder Abgabe von Gas oder Wärme

2. Verfahren

2.1. Verfahren

Titel: SWA_MS SOC_SIEM_TNW
Beschreibung: Ausschreibung zum Abschluss eines Rahmenvertrages über den Betrieb eines Managed Security Service über den Betrieb eines Security Information and Event Management (SIEM) sowie ein Security Operation Center (SOC) als full-managed Service auf Basis einer Cloudlösung inkl. weiterer Dienstleistungen Los 1: Corporate- und Office-IT (IT-Infrastruktur) Los 2: Operational Technologie (OT-Infrastruktur)
Kennung des Verfahrens: 77348f1e-5c67-4d42-9896-48205364ec13
Interne Kennung: SWA_MS SOC_SIEM_TNW
Verfahrensart: Verhandlungsverfahren mit vorheriger Veröffentlichung eines Aufrufs zum Wettbewerb/Verhandlungsverfahren
Das Verfahren wird beschleunigt: nein
Zentrale Elemente des Verfahrens: Im ersten Verfahrensabschnitt werden die Interessenten zur Abgabe eines Teilnahmeantrages aufgefordert. Im Anschluss daran prüft die Vergabestelle die Eignung der Bewerber anhand der eingereichten Nachweise. Sodann werden pro Los max. 4 Bewerber ausgewählt, die eingeladen werden, erste indikative Angebote einzureichen, über die dann verhandelt wird. Nach Abschluss der Verhandlungsphase erhalten alle Bieter, die ein indikatives Erstangebot eingereicht und an den Verhandlungen teilgenommen haben, die Aufforderung zur Einreichung der verbindlichen finalen Angebote, die nach Maßgabe der bekannt gegebenen Zuschlagskriterien bewertet werden.

2.1.1. Zweck

Art des Auftrags: Dienstleistungen
Haupteinstufung (cpv): 72000000 IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung
Zusätzliche Einstufung (cpv): 72220000 Systemberatung und technische Beratung

2.1.2. Erfüllungsort

Postanschrift: Gaswerkstraße 7
Stadt: Achim
Postleitzahl: 28832

Land, Gliederung (NUTS): Verden (DE93B)
Land: Deutschland

2.1.3. Wert

Geschätzter Wert ohne MwSt.: 4 000 000,00 EUR
Höchstwert der Rahmenvereinbarung: 4 000 000,00 EUR

2.1.4. Allgemeine Informationen

Zusätzliche Informationen: Bekanntmachungs-ID: CXP4YHS5GAL Der maximale Auftragswert für Los 1 wie für Los 2 beträgt 2 Mio EURO.
Rechtsgrundlage:
Richtlinie 2014/25/EU
sektvo -

2.1.5. Bedingungen für die Auftragsvergabe

Bedingungen für die Einreichung:
Höchstzahl der Lose, für die ein Bieter Angebote einreichen kann: 2
Auftragsbedingungen:
Höchstzahl der Lose, für die Aufträge an einen Bieter vergeben werden können: 2

2.1.6. Ausschlussgründe

Quellen der Ausschlussgründe: Auftragsunterlagen

5. Los

5.1. Los: LOT-0001

Titel: Full-managed SOC/SIEM IT
Beschreibung: Die Stadtwerke Achim AG (nachfolgend "SWA" oder "Auftraggeber" oder "Vergabestelle" genannt), Gaswerkstraße 7, 28832 Achim, leitet mit der Auftragsbekanntmachung ein europaweites Ausschreibungsverfahren mit dem Ziel ein, die IT-Sicherheit durch die Einführung und den Betrieb eines Managed Security Information and Event Management (SIEM) und Security Operations Center (SOC) zu verbessern. Der Ausschreibungsgegenstand besteht innerhalb jedes Loses aus vier Phasen. Die ersten drei Phase erfassen die Implementierung und die Stabilisierungsphase und werden auch als "Einführungsprojekt" bezeichnet. Die vierte Phase erfasst den Ausbau und die Entwicklung. Leistungen werden jeweils bedarfsentsprechend abgerufen. Im Rahmen des Einführungsprojektes ist die angebotene SIEM-Lösung inklusive des SOC als full-managed Service nach Maßgabe der Leistungsbeschreibung bereit zu stellen. Bestandteil des full-managed-Service ist die Entwicklung und Bereitstellung eines voll funktionsfähigen Basissatzes an sicherheitsrelevanten Use Cases sowie standardisierten Incident-Response-Playbooks. Ziel dieser Phase ist es, schnellstmöglich ein tragfähiges Sicherheitsniveau zu erreichen, das auf die aktuelle Infrastruktur und die vorliegenden Bedrohungslagen abgestimmt ist. Mit dem Zuschlag werden die Leistungen des Einführungsprojektes beauftragt. Der Auftraggeber ist während der Vertragslaufzeit berechtigt, weitere Leistungen abzurufen, die Bestandteil der Phase 4 Ausbau und Weiterentwicklung sind. Ziel dieser Phase 4 ist der Ausbau und die kontinuierliche Weiterentwicklung der Lösung mitsamt weiterer Use Cases und Playbooks, die auf Grundlage der im Betrieb gewonnenen Erkenntnisse, aktueller Bedrohungsanalysen sowie branchenspezifischer Anforderungen entwickelt werden. Innerhalb des Loses 1 IT liegt ein Schwerpunkt auf der schrittweisen Automatisierung von Reaktionsprozessen im Sinne eines SOAR-Ansatzes (Security Orchestration, Automation and Response). Dies beinhaltet die Integration automatisierter Abläufe zur schnelleren und

konsistenteren Behandlung sicherheitsrelevanter Ereignisse sowie die Verknüpfung mit weiteren IT-Sicherheits- und Betriebssystemen. Damit wird eine kontinuierliche Reifegradsteigerung der Sicherheitsorganisation angestrebt - von der initialen, manuell gesteuerten Reaktion hin zu einem automatisiert unterstützten, hoch effizienten Sicherheitsbetrieb. Die SWA versorgt als Eigentümerin des Strom- und Gasnetzes die Stadt Achim im Rahmen der Grundversorgung gemäß § 36 Abs. 2 Energiewirtschaftsgesetzes (EnWG) mit Strom und Gas. Daneben beliefert sie die Gemeinde Oyten sowie die Flecken Ottersberg und Langwedel als Grundversorger mit Gas über die in ihrem Eigentum befindlichen Gasversorgungsnetze. Seit 2018 hat die SWA das Stromnetz in der Gemeinde Oyten von der Netzgesellschaft Oyten GmbH gepachtet und versorgt seit 2019 bis einschließlich 2024 die Gemeinde Oyten im Rahmen der Grundversorgung mit Strom. Zudem können Kunden deutschlandweit durch den Energievertrieb mit Strom und Gas versorgt werden. Nach § 6b Abs. 3 Satz 2 EnWG ergeben sich für die SWA die beiden Tätigkeitsbereiche Elektrizitätsverteilung und Gasverteilung. Daneben übernimmt sie die Elektrizitäts- und Gasverteilung, das Stromvertriebsgeschäft, das Gasvertriebsgeschäft, das Betreiben von Wärmeversorgungsanlagen einschließlich des Vertriebs von Wärme, der moderne Messstellenbetrieb, die Unterhaltung der Straßenbeleuchtungsanlagen in der Stadt Achim sowie die kaufmännische Betriebsführung der Gesellschaft, die das Netz in Oyten betreibt, der NOG. Die Operational Technology (OT), also die IT-Infrastruktur, die für die kritische Infrastruktur und den operativen Betrieb der Anlagen für den Betrieb des Strom- und Gasnetzes erforderlich sind, sind Gegenstand des Loses 2. Ziel der eingeleiteten Ausschreibung ist der Abschluss eines Rahmenvertrages über - die Feinkonzeption, - die Bereitstellung - die Anbindung, - den Betrieb sowie - der Ausbau und die Weiterentwicklung der ausgeschriebenen Leistungen als "Managed Security Service" nach Maßgabe der Vergabeunterlagen und insbesondere der Leistungsbeschreibung und des Rahmenvertrages. Die ausgeschriebene und anzubietende Leistung ist durch einen Managed Security Service Provider (MSSP) auf Basis des Bereitstellungsmodells "Managed Service" in einer durch den Auftragnehmer (AN) betriebenen bzw. bereitgestellten Cloud Infrastruktur zu erbringen. Den Vergabeunterlagen für den Teilnahmewettbewerb beigefügt ist jeweils losbezogen das Dokument "Leistungsbeschreibung Teilnahmewettbewerb" (Anlage 1 a und Anlage 1 b), das die jeweils ausgeschriebenen Leistungen zusammenfasst. Nach Abschluss des Teilnahmewettbewerbs wird den ausgewählten Bietern jeweils pro Los eine verdichtete Fassung der Leistungsbeschreibung elektronisch bereitgestellt. Interessenten sind aufgefordert, einen Teilnahmeantrag einzureichen und anzugeben, für welches Los der Teilnahmeantrag eingereicht wird.
Interne Kennung: 1

5.1.1. Zweck

Art des Auftrags: Dienstleistungen
Haupteinstufung (cpv): 72000000 IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung

5.1.2. Erfüllungsort

Postanschrift: Gaswerkstraße 7
Stadt: Achim
Postleitzahl: 28832
Land, Gliederung (NUTS): Verden (DE93B)
Land: Deutschland

5.1.3. Geschätzte Dauer

Laufzeit: 4 Jahre

5.1.4. Verlängerung

Maximale Verlängerungen: 4
Weitere Informationen zur Verlängerung: 4 x 1 Jahr bis maximal 8 Jahre

5.1.5. Wert

Geschätzter Wert ohne MwSt.: 2 000 000,00 EUR

5.1.6. Allgemeine Informationen

Vorbehaltene Teilnahme:
Teilnahme ist nicht vorbehalten.
Auftragsvergabeprojekt nicht aus EU-Mitteln finanziert
Die Beschaffung fällt unter das Übereinkommen über das öffentliche Beschaffungswesen: nein
Diese Auftragsvergabe ist auch für kleine und mittlere Unternehmen (KMU) geeignet: nein
Zusätzliche Informationen: Ferner sind die Erklärung zur Einhaltung des gesetzlichen Mindestlohns (Formblatt 8) und die Eigenerklärung i.S.d. Art 5k Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren (Formblatt 7) einzureichen. Weiterhin sind in der Angebots- und Verhandlungsphase der für das Gesamtprojekt verantwortliche Beschäftigte und dessen Vertretung namentlich sowie mit Kontaktdaten (Anschrift, Telefon, E-Mail) zu benennen. Die Vergabestelle erwartet, dass die für das Projekt verantwortliche Person oder dessen Vertretung an den Vergabeverhandlungen teilnehmen.

5.1.7. Strategische Auftragsvergabe

Ziel der strategischen Auftragsvergabe: Keine strategische Beschaffung

5.1.9. Eignungskriterien

Quellen der Auswahlkriterien: Bekanntmachung
Kriterium: Maßnahmen zur Sicherstellung der Qualität
Beschreibung des Auswahlkriteriums: Unternehmensdarstellung (Name, Anschrift, Rechtsform, organisatorische Gliederung, Leistungsspektrum, Gründungsdatum, Niederlassungen), (Formblatt - Angaben zum Unternehmen (Versicherung/Umsatz)

Kriterium: Eintragung in das Handelsregister
Beschreibung des Auswahlkriteriums: Angabe der Eintragung in ein Handelsregister, alternativ eine Angabe nach Maßgabe der Rechtsvorschriften des Landes, in dem der Bewerber ansässig ist.

Kriterium: Maßnahmen zur Sicherstellung der Qualität
Beschreibung des Auswahlkriteriums: Eigenerklärung über das Nichtvorliegen von Ausschlussgründen gemäß § 123 f. GWB (Formblatt - Erklärung zum Nichtvorliegen von Ausschlussgründen) - (Im Fall der Bildung einer Bewerbergemeinschaft für alle Mitglieder einzureichen!).

Kriterium: Berufliche Risikohaftpflichtversicherung
Beschreibung des Auswahlkriteriums: Einzureichen ist ein Nachweis einer Betriebshaftpflichtversicherung für Personen- sowie für Sach- und Vermögensschäden (inkl. Mietsachschäden) über mindestens 3 Mio. EUR, welche bei einem in der EU zugelassenen Versicherer abgeschlossen ist; es genügt die Erklärung über die Bereitschaft, im Zuschlagsfall eine entsprechende Versicherung abzuschließen sowie die Bestätigung eines Versicherungsunternehmens zum Abschluss einer entsprechenden Versicherung.

Kriterium: Allgemeiner Jahresumsatz
Beschreibung des Auswahlkriteriums: Eigenerklärung über die Gesamtumsätze der letzten drei Geschäftsjahre und der Umsätze der letzten drei Geschäftsjahre, die mit der ausgeschriebenen Leistung vergleichbar sind

Kriterium: Zertifikate von unabhängigen Stellen über Umweltmanagementsysteme oder -standards
Beschreibung des Auswahlkriteriums: a) Eigenerklärung darüber, dass der Bewerber in der Lage ist, die jeweils angebotene Leistung in einer Umgebung zu hosten, die eine Zertifizierung nach DIN ISO/IEC 27001:2022 in Bezug auf das gesamte Unternehmen oder eine gleichwertige Bescheinigung, wie etwa die Zertifizierung gem. BSI Grundschutz oder vergleichbare Zertifizierungen von akkreditierten Stellen in anderen Mitgliedstaaten aufweist (zugleich Mindestanforderung). b) Eigenerklärung darüber, dass der Bewerber in der Lage ist, die jeweils angebotene Leistung in einer Umgebung zu hosten, die eine nach DIN ISO/IEC 27017: aufweist (die Zertifizierung eines Mitglieds einer Bewerbergemeinschaft genügt, wenn das zertifizierte Mitglied das Rechenzentrum betreibt, in dem die anzubietende Lösung gehostet wird) (Mindestanforderung). c) Darstellung zur Unternehmensorganisation und der Unternehmensprozesse, die eine hinreichende Systemqualität sicherstellt, alternativ kann eine Zertifizierung des Unternehmens nach DIN ISO 9001 oder eine gleichwertige Bescheinigung von akkreditierten Stellen in anderen Mitgliedstaaten eingereicht werden

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: d) Referenzliste über vergleichbare und abgeschlossene Leistungen der letzten drei (3) Jahre. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 800 Events per Second (EPS) mit einem 24/7-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird. Anzugeben sind: - Projektinhalt mit Angaben zu Zeitdauer und Charakteristik, Projektziel, insbesondere zu Implementierung und Dauer des Betriebs von SOC, - Auftraggeber inkl. Ansprechpartner und Telefonnummer, - Leistungszeitraum, - Kurzbeschreibung der durchgeführten Dienstleistungen, insbesondere Angabe zum erbrachten Support/Service und zu dem betreuten SIEM-Tool. Mindestanforderung: Nachweis über mindestens zwei vergleichbare und abgeschlossene Referenzprojekte der letzten drei Jahre, davon mindestens eine vergleichbare Referenz, die für einen Akteur, der eine kritische Infrastruktur betreibt, erbracht wurde. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 800 Events per Second (EPS) mit einem 24/7/365-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird.

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: Nachweis über mindestens zwei vergleichbare und abgeschlossene Referenzprojekte der letzten drei Jahre, davon mindestens eine vergleichbare Referenz, die für einen Akteur, der eine kritische Infrastruktur betreibt, erbracht wurde. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer

Ereignisrate von mindestens 800 Events per Second (EPS) mit einem 24/7/365-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird. Anzugeben sind: - Projektinhalt mit Angaben zu Zeitdauer und Charakteristik, Projektziel, insbesondere zu Implementierung und Dauer des Betriebs von SOC, - Auftraggeber inkl. Ansprechpartner und Telefonnummer, - Leistungszeitraum, - Kurzbeschreibung der durchgeführten Dienstleistungen, insbesondere Angabe zum erbrachten Support/Service und zu dem betreuten SIEM-Tool.

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: Für die Auswahl entscheidend ist zu 60 % die nachgewiesene Kompetenz und Erfahrung anhand der Vergleichbarkeit eingereichten Referenzen über die mit der ausgeschriebenen Leistung vergleichbar erbrachten Leistungen nach Maßgabe der nachfolgend definierten Anforderungen. Die Vergabestelle beschränkt die Zahl der einreichbaren Referenzen auf sechs (6) Referenzen pro Bewerber /Bewerbergemeinschaft. Jede der eingereichten Referenz wird anhand des nachstehenden Punktesystems wie folgt bewertet: 15 Punkte bei Vorliegen folgender Voraussetzungen: (1) Referenz über 1.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 1000 EPS im Produktivbetrieb. 1.2. Bereitstellung als hochverfügbare Lösung (? 99,9 % Verfügbarkeit) 1.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 1.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 1.5. Einsatz von Incident Response-Mechanismen sowie automatisierten Abläufen im Sinne eines SOAR-Ansatzes (Security Orchestration, Automation and Response) oder vergleichbare Interventionsmöglichkeiten 1.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 1.7. Die Referenz muss sich auf einen Auftraggeber im Bereich Energiewirtschaft und/oder im Bereich kritischer Infrastruktur (KRITIS) beziehen 1.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 1.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 13 Punkte: 2.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 1000 EPS im Produktivbetrieb. 2.2. Bereitstellung als hochverfügbare Lösung (? 99,9 % Verfügbarkeit) 2.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 2.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 2.5. Einsatz von Incident Response-Mechanismen sowie automatisierte Abläufe im Sinne eines SOAR-Ansatzes (Security Orchestration, Automation and Response) oder vergleichbare Interventionsmöglichkeiten 2.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 2.7. Die Referenz muss sich auf einen Auftraggeber im Bereich Energiewirtschaft und/oder im Bereich kritischer Infrastruktur (KRITIS) beziehen 2.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 2.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 11 Punkte 3.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 800 EPS im Produktivbetrieb. 3.2. Bereitstellung als hochverfügbare Lösung (? 98,5 % Verfügbarkeit) 3.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 3.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 3.5. Einsatz von Incident Response-Mechanismen oder vergleichbare

Interventionsmöglichkeiten 3.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 3.7. Die Referenz muss sich auf einen vergleichbaren Auftraggeber im Bereich Energiewirtschaft und/oder kritische Infrastruktur (KRITIS) beziehen 3.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 3.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 8 Punkte 4.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 800 EPS im Produktivbetrieb. 4.2. Bereitstellung als hochverfügbare Lösung (? 98,5 % Verfügbarkeit) 4.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 4.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 4.5. Einsatz von Incident Response-Mechanismen oder vergleichbare Interventionsmöglichkeiten 4.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 4.7. Die Abnahme /Produktivsetzung liegt mindestens 12 Monate zurück 4.8. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 5 Punkte: 5.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 800 EPS im Produktivbetrieb. 5.2. Bereitstellung als hochverfügbare Lösung (? 98,5 % Verfügbarkeit) 5.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1 /2/3) 5.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 5.5. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 5.6. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider)
Anhand der Kriterien werden die Bewerber ausgewählt, die zur zweiten Phase des Verfahrens eingeladen werden sollen
Gewichtung (Prozentanteil, genau): 60,00

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: Bestandteil der Vergabeunterlagen ist das Formblatt - Erklärung zur Kundenzufriedenheit, das von dem jeweiligen Auftraggeber einer eingereichten Referenz auszufüllen ist. Es dürfen nur ausgefüllte Formblätter von Auftraggebern zu eingereichten vergleichbaren und abgeschlossenen Referenzprojekten eingereicht werden. Gewertet wird jeweils nur der Grad der nachgewiesenen Zufriedenheit über vergleichbare Referenzprojekte. Die durch einen Auftraggeber abgegebene ausgefüllte Erklärung zur Kundenzufriedenheit wird wie folgt bewertet: Ein Bewerber erhält für jeden sehr zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung, die einen verbindlichen Fertigstellungstermin umfasste, pro ausgefülltem Formblatt 15 Punkte. Ein Bewerber erhält für jeden sehr zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung pro ausgefülltem Formblatt 12 Punkte. Ein Bewerber erhält für jeden zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung, die einen verbindlichen Fertigstellungstermin umfasste, pro ausgefülltem Formblatt 8 Punkte. Ein Bewerber erhält für jeden zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung pro ausgefülltem Formblatt 6 Punkte. Ein Bewerber erhält für jeden teilweise zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung, die einen verbindlichen Fertigstellungstermin umfasste, pro ausgefülltem Formblatt 4 Punkte. Ein Bewerber erhält für jeden teilweise zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung pro ausgefülltem Formblatt 2 Punkte. Die erreichten Punkte werden

mit dem o.g. Gewichtungsfaktor (50 %) multipliziert. Die sechs (6) Bewerber mit den insgesamt höchsten Punktzahlen (Summe aus "Kompetenz und Erfahrung" und "Grad der Kundenzufriedenheit") werden zur Angebotsabgabe ausgewählt. Sollten mehrere Bewerber die gleiche Punktzahl erhalten, behält sich die ÜSTRA vor, die abschließende Auswahl und Reduzierung des Bieterkreises durch Losverfahren herbeizuführen.
Anhand der Kriterien werden die Bewerber ausgewählt, die zur zweiten Phase des Verfahrens eingeladen werden sollen
Gewichtung (Prozentanteil, genau): 40,00

Kriterium: Durchschnittliche jährliche Belegschaft
Beschreibung des Auswahlkriteriums: e) Eigenerklärung gem. § 46 Abs. 3 Nr. 2 VgV und Angabe des jährlichen Mittelwertes der in den letzten drei Jahren im Unternehmen angestellten Personen, jeweils aufgegliedert in die Bereiche Support zu SOC/SIEM und Entwicklung des SOC. Mindestanforderung: Eigenerklärung, dass der Bewerber/die Bewerbergemeinschaft über verfügbares Personal von mindestens zehn (10) Beschäftigten im Bereich SOC, die alle drei Support-Levels bearbeiten, davon mindestens jeweils zwei (2) Beschäftigte im Level 3-Support verfügt (Antrag auf Teilnahme).
Informationen über die zweite Phase eines zweiphasigen Verfahrens:
Mindestzahl der zur zweiten Phase des Verfahrens einzuladenden Bewerber: 1
Höchstzahl der zur zweiten Phase des Verfahrens einzuladenden Bewerber: 4
Das Verfahren wird in mehreren aufeinanderfolgenden Phasen durchgeführt. In jeder Phase können einige Teilnehmer ausgeschlossen werden

5.1.10. Zuschlagskriterien

Kriterium:
Art: Preis
Bezeichnung: Angebotspreis
Beschreibung: Das der Angebotsaufforderung beigefügte Preisblatt ist ausgefüllt mit dem Angebot einzureichen. Der niedrigste Gesamtpreis gem. Preisblatt bildet den Referenzpreis, der die volle Bewertungspunktzahl von 45 Punkten erhält. Die Punktzahl der weiteren Angebote ergibt sich nach folgender Formel: Bewertungspunkte = 45 X (Referenzpreis dividiert durch Angebotspreis). Der Bieter hat seine Preiskalkulation auf einer gesonderten Anlage zu erläutern.
Kategorie des Gewicht-Zuschlagskriteriums: Gewichtung (Prozentanteil, genau)
Zuschlagskriterium — Zahl: 45
Kriterium:
Art: Qualität
Bezeichnung: Leistung
Beschreibung: Weiteres Bewertungskriterium ist die Qualität der angebotenen Leistungen, die anhand des einzureichenden Umsetzungskonzeptes und des einzureichenden Servicekonzeptes entsprechend der Bewertungsmatrix bewertet wird. Das Umsetzungskonzept wird mit 65% und das Servicekonzept mit 35% gewichtet.
Kategorie des Gewicht-Zuschlagskriteriums: Gewichtung (Prozentanteil, genau)
Zuschlagskriterium — Zahl: 55

5.1.11. Auftragsunterlagen

Sprachen, in denen die Auftragsunterlagen offiziell verfügbar sind: Deutsch
Frist für die Anforderung zusätzlicher Informationen: 14/08/2025 23:59:59 (UTC+02:00) Osteuropäische Zeit, Mitteleuropäische Sommerzeit

Internetadresse der Auftragsunterlagen: https://www.dtvp.de/Satellite/notice/CXP4YHS5GAL/documents

Ad-hoc-Kommunikationskanal:

URL: https://www.dtvp.de/Satellite/notice/CXP4YHS5GAL

5.1.12. Bedingungen für die Auftragsvergabe

Verfahrensbedingungen:

Voraussichtliches Datum der Absendung der Aufforderungen zur Angebotseinreichung: 12/09/2025

Bedingungen für die Einreichung:

Elektronische Einreichung: Erforderlich

Adresse für die Einreichung: https://www.dtvp.de/Satellite/notice/CXP4YHS5GAL

Sprachen, in denen Angebote oder Teilnahmeanträge eingereicht werden können: Deutsch

Elektronischer Katalog: Nicht zulässig

Varianten: Nicht zulässig

Die Bieter können mehrere Angebote einreichen: Nicht zulässig

Frist für den Eingang der Teilnahmeanträge: 21/08/2025 10:00:00 (UTC+02:00) Osteuropäische Zeit, Mitteleuropäische Sommerzeit

Informationen, die nach Ablauf der Einreichungsfrist ergänzt werden können:

Nach Ermessen des Käufers können einige fehlenden Bieterunterlagen nach Fristablauf nachgereicht werden.

Zusätzliche Informationen: Die Vergabestelle behält sich vor, gem. § 51 SektVO auch im Teilnahmewettbewerb nach sachgerechtem Ermessen fehlende Unterlagen, Erklärungen und Angaben binnen einer Frist von drei (3) Werktagen nachzufordern. Unterlagen, Erklärungen und/oder Nachweise, die nach Fristablauf eingereicht werden, werden nicht berücksichtigt. Der Teilnahmeantrag wird in der dann vorliegenden Fassung geprüft und die Eignung des Bewerbers bewertet. Zwingende Voraussetzung für die Wertbarkeit eines Teilnahmeantrags ist ein fristgerecht eingegangener, rechtswirksam unterschriebener Teilnahmeantrag.

Auftragsbedingungen:

Die Auftragsausführung muss im Rahmen von Programmen für geschützte Beschäftigungsverhältnisse erfolgen: Nein

Bedingungen für die Ausführung des Auftrags: Zwingende Voraussetzungen sind die Akzeptanz und Zeichnung folgender Unterlagen durch den Wettbewerbsteilnehmer: - Vereinbarung zur Auftragsverarbeitung (AVV) inklusive der Mindestanforderungen an die technischen und organisatorischen Maßnahmen (TOM) sowie - Vertraulichkeitsvereinbarung, - Vereinbarung über die Verarbeitung im Auftrag gemäß Art. 28 DSGVO zu diesem Vergabeverfahren gemäß der Anlage 3, Auftragsverarbeitungsvertrag - Geheimhaltungsvereinbarung - Verpflichtung zur Einhaltung der Vorgaben des MiLoG - Zeichnung der SanktVO 833

Elektronische Rechnungsstellung: Zulässig

Aufträge werden elektronisch erteilt: ja

Zahlungen werden elektronisch geleistet: ja

Von einer Bietergemeinschaft, die den Zuschlag erhält, anzunehmende Rechtsform: gesamtschuldnerisch haftend mit bevollmächtigtem Vertreter

Finanzielle Vereinbarung: gem. Vergabeunterlagen

5.1.15. Techniken

Rahmenvereinbarung:

Rahmenvereinbarung ohne erneuten Aufruf zum Wettbewerb

Höchstzahl der Teilnehmer: 1

Informationen über das dynamische Beschaffungssystem:
Kein dynamisches Beschaffungssystem

5.1.16. Weitere Informationen, Schlichtung und Nachprüfung

Überprüfungsstelle: Vergabekammer Niedersachsen beim Nds. Ministerium für Wirtschaft, Verkehr, Bauen und Digitalisierung
Informationen über die Überprüfungsfristen: Wettbewerbsteilnehmern steht der vergaberechtliche Rechtsschutz gemäß den §§ 160 ff. GWB zur Verfügung. Ein Nachprüfungsverfahren ist nur auf Antrag zulässig. Antragsbefugt ist gemäß § 160 Abs. 2 GWB jedes Unternehmen, das ein Interesse an dem öffentlichen Auftrag hat und eine Verletzung in seinen Rechten nach § 97 Abs. 6 GWB durch Nichtbeachtung von Vergabevorschriften geltend macht. Dabei ist darzulegen, dass dem Unternehmen durch die behauptete Verletzung der Vergabevorschriften ein Schaden entstanden ist oder zu entstehen droht. Der Antrag ist gemäß § 160 Abs. 2 GWB unzulässig, soweit: 1) Der Antragsteller den geltend gemachten Verstoß gegen Vergabevorschriften vor Einreichen des Nachprüfungsantrags erkannt und gegenüber dem Auftraggeber nicht innerhalb einer Frist von 10 Kalendertagen gerügt hat; der Ablauf der Frist nach § 134 Abs. 2 bleibt unberührt, 2) Verstöße gegen Vergabevorschriften, die aufgrund der Bekanntmachung erkennbar sind, nicht spätestens bis zum Ablauf der in der Bekanntmachung benannten Frist zur Bewerbung gegenüber dem Auftraggeber gerügt werden, 3) Verstöße gegen Vergabevorschriften, die erst in den Vergabeunterlagen erkennbar sind, nicht spätestens bis zum Ablauf der Frist zur Bewerbung oder Angebotsabgabe gegenüber dem Auftraggeber gerügt werden, 4) Mehr als 15 Kalendertage nach Eingang der Mitteilung des Auftraggebers, einer Rüge nicht abhelfen zu wollen, vergangen sind. Satz 1 gilt nicht bei einem Antrag auf Feststellung der Unwirksamkeit des Vertrags nach § 135 Satz 1 Nr. 2. § 134 Abs. 1 Satz 2 GWB bleibt unberührt.
Organisation, die zusätzliche Informationen über das Vergabeverfahren bereitstellt: Stadtwerke Achim AG
Organisation, die Teilnahmeanträge entgegennimmt: Stadtwerke Achim AG

5.1. Los: LOT-0002

Titel: Full-managed SOC/SIEM OT
Beschreibung: Es gelten nachstehende Anforderungen in Bezug auf die technische Eignung: Referenzliste über vergleichbare und abgeschlossene Leistungen der letzten drei (3) Jahre. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 1500 Events per Second (EPS) mit einem 24/7/365-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird. Anzugeben sind: - Projektinhalt mit Angaben zu Zeitdauer und Charakteristik, Projektziel, insbesondere zu Implementierung und Dauer des Betriebs von SOC, - Auftraggeber inkl. Ansprechpartner und Telefonnummer, - Leistungszeitraum, - Kurzbeschreibung der durchgeführten Dienstleistungen, insbesondere Angabe zum erbrachten Support/Service und zu dem betreuten SIEM-Tool. Mindestanforderung: Nachweis über mindestens zwei vergleichbare und abgeschlossene Referenzprojekte der letzten drei Jahre, davon mindestens eine vergleichbare Referenz, die für einen Akteur erbracht wurde, der eine kritische Infrastruktur betreibt. Vergleichbar sind Referenzen über Betriebsleistungen eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 1500 Events per Second (EPS) mit einem 24/7/365-Support in allen drei Support-Level-Klassen (1/2/3), die sich auf die IT-Infrastruktur bezogen, mit der der Bereich der kritischen Infrastrukturen (KRITIS) betrieben wird

/wurde (Operational IT - nachfolgend "OT") und Logs sowie sicherheitsrelevante Ereignisse aus einer OT-Umgebung bzw. OT-Infrastruktur verarbeitet hat. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird. Weiter erfolgt die Punktevergabe im Auswahlprozess in Bezug das Kriterium "Referenzen des Bewerbers Kompetenz und Erfahrung" wie folgt: 15 Punkte Referenz über 1.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 3000 EPS im Produktivbetrieb. 1.2. Bereitstellung als hochverfügbare Lösung (? 99,9 % Verfügbarkeit) 1.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 1.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 1.5. Einsatz von Incident Response-Mechanismen oder vergleichbare Interventionsmöglichkeiten 1.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen) 1.7. Die Referenz muss sich auf einen Auftraggeber aus dem Bereich der kritischen Infrastrukturen (KRITIS) im Bereich der Energiewirtschaft gem. ENWG beziehen. Gegenstand der Referenz muss der Einsatz eines SIEM-Systems sein, das Logs und sicherheitsrelevante Ereignisse aus einer OT-Umgebung bzw. OT-Infrastruktur verarbeitet hat. 1.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 1.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) Der Einsatz des SIEM-Systems bezog sich maßgeblich auf OT-Infrastrukturen (z. B. Produktionsnetzwerke, industrielle Steuerungsanlagen, SCADA, ICS). Die Referenz muss den Umfang der Projektleistung im Hinblick auf die OT-spezifischen Herausforderungen (z. B. Segmentierung, Protokollvielfalt, Echtzeit-Anforderungen) erkennbar machen. 13 Punkte Referenz über 2.1 Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 2500 EPS im Produktivbetrieb. 2.2. Bereitstellung als hochverfügbare Lösung (? 99,9 % Verfügbarkeit) 2.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 2.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 2.5. Einsatz von Incident Response-Mechanismen oder vergleichbare Interventionsmöglichkeiten 2.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 2.7. Die Referenz muss sich auf einen Auftraggeber aus dem Bereich der kritischen Infrastrukturen (KRITIS) im Bereich der Energiewirtschaft gem. ENWG beziehen. Gegenstand der Referenz muss der Einsatz eines SIEM-Systems sein, das Logs und sicherheitsrelevante Ereignisse aus einer OT-Umgebung bzw. OT-Infrastruktur verarbeitet hat. 2.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 2.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) Der Einsatz des SIEM-Systems bezog sich maßgeblich auf OT-Infrastrukturen (z. B. Produktionsnetzwerke, industrielle Steuerungsanlagen, SCADA, ICS). Die Referenz muss den Umfang der Projektleistung im Hinblick auf die OT-spezifischen Herausforderungen (z. B. Segmentierung, Protokollvielfalt, Echtzeit-Anforderungen) erkennbar machen. Das Bewertungssystem ist in der Bewerberinformation in Abschnitt III, Ziffer 5.5. definiert.
Interne Kennung: 2

5.1.1. Zweck

Art des Auftrags: Dienstleistungen
Haupteinstufung (cpv): 72000000 IT-Dienste: Beratung, Software-Entwicklung, Internet und Hilfestellung

5.1.2. Erfüllungsort

Postanschrift: Gaswerkstraße 7
Stadt: Achim
Postleitzahl: 28832
Land, Gliederung (NUTS): Verden (DE93B)
Land: Deutschland

5.1.3. Geschätzte Dauer

Laufzeit: 4 Jahre

5.1.4. Verlängerung

Maximale Verlängerungen: 4
Weitere Informationen zur Verlängerung: 4 x 1 Jahr bis maximal 8 Jahre

5.1.5. Wert

Geschätzter Wert ohne MwSt.: 2 000 000,00 EUR

5.1.6. Allgemeine Informationen

Vorbehaltene Teilnahme:
Teilnahme ist nicht vorbehalten.
Auftragsvergabeprojekt nicht aus EU-Mitteln finanziert
Die Beschaffung fällt unter das Übereinkommen über das öffentliche Beschaffungswesen: nein
Diese Auftragsvergabe ist auch für kleine und mittlere Unternehmen (KMU) geeignet: nein
Zusätzliche Informationen: Ferner sind die Erklärung zur Einhaltung des gesetzlichen Mindestlohns (Formblatt 8) und die Eigenerklärung i.S.d. Art 5k Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren (Formblatt 7) einzureichen. Weiterhin sind in der Angebots- und Verhandlungsphase der für das Gesamtprojekt verantwortliche Beschäftigte und dessen Vertretung namentlich sowie mit Kontaktdaten (Anschrift, Telefon, E-Mail) zu benennen. Die Vergabestelle erwartet, dass die für das Projekt verantwortliche Person oder dessen Vertretung an den Vergabeverhandlungen teilnehmen.

5.1.7. Strategische Auftragsvergabe

Ziel der strategischen Auftragsvergabe: Keine strategische Beschaffung

5.1.9. Eignungskriterien

Quellen der Auswahlkriterien: Bekanntmachung
Kriterium: Maßnahmen zur Sicherstellung der Qualität
Beschreibung des Auswahlkriteriums: Unternehmensdarstellung (Name, Anschrift, Rechtsform, organisatorische Gliederung, Leistungsspektrum, Gründungsdatum, Niederlassungen), (Formblatt - Angaben zum Unternehmen (Versicherung/Umsatz)

Kriterium: Eintragung in das Handelsregister
Beschreibung des Auswahlkriteriums: Angabe der Eintragung in ein Handelsregister, alternativ eine Angabe nach Maßgabe der Rechtsvorschriften des Landes, in dem der Bewerber ansässig ist.

Kriterium: Maßnahmen zur Sicherstellung der Qualität

Beschreibung des Auswahlkriteriums: Eigenerklärung über das Nichtvorliegen von Ausschlussgründen gemäß § 123 f. GWB (Formblatt - Erklärung zum Nichtvorliegen von Ausschlussgründen) - (Im Fall der Bildung einer Bewerbergemeinschaft für alle Mitglieder einzureichen!).

Kriterium: Berufliche Risikohaftpflichtversicherung
Beschreibung des Auswahlkriteriums: Einzureichen ist ein Nachweis einer Betriebshaftpflichtversicherung für Personen- sowie für Sach- und Vermögensschäden (inkl. Mietsachschäden) über mindestens 3 Mio. EUR, welche bei einem in der EU zugelassenen Versicherer abgeschlossen ist; es genügt die Erklärung über die Bereitschaft, im Zuschlagsfall eine entsprechende Versicherung abzuschließen sowie die Bestätigung eines Versicherungsunternehmens zum Abschluss einer entsprechenden Versicherung.

Kriterium: Allgemeiner Jahresumsatz
Beschreibung des Auswahlkriteriums: Eigenerklärung über die Gesamtumsätze der letzten drei Geschäftsjahre und der Umsätze der letzten drei Geschäftsjahre, die mit der ausgeschriebenen Leistung vergleichbar sind

Kriterium: Zertifikate von unabhängigen Stellen über Umweltmanagementsysteme oder -standards
Beschreibung des Auswahlkriteriums: a) Eigenerklärung darüber, dass der Bewerber in der Lage ist, die jeweils angebotene Leistung in einer Umgebung zu hosten, die eine Zertifizierung nach DIN ISO/IEC 27001:2022 in Bezug auf das gesamte Unternehmen oder eine gleichwertige Bescheinigung, wie etwa die Zertifizierung gem. BSI Grundschutz oder vergleichbare Zertifizierungen von akkreditierten Stellen in anderen Mitgliedstaaten aufweist (zugleich Mindestanforderung). b) Eigenerklärung darüber, dass der Bewerber in der Lage ist, die jeweils angebotene Leistung in einer Umgebung zu hosten, die eine nach DIN ISO/IEC 27017: aufweist (die Zertifizierung eines Mitglieds einer Bewerbergemeinschaft genügt, wenn das zertifizierte Mitglied das Rechenzentrum betreibt, in dem die anzubietende Lösung gehostet wird) (Mindestanforderung). c) Darstellung zur Unternehmensorganisation und der Unternehmensprozesse, die eine hinreichende Systemqualität sicherstellt, alternativ kann eine Zertifizierung des Unternehmens nach DIN ISO 9001 oder eine gleichwertige Bescheinigung von akkreditierten Stellen in anderen Mitgliedstaaten eingereicht werden

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: d) Referenzliste über vergleichbare und abgeschlossene Leistungen der letzten drei (3) Jahre. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 800 Events per Second (EPS) mit einem 24/7-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird. Anzugeben sind: - Projektinhalt mit Angaben zu Zeitdauer und Charakteristik, Projektziel, insbesondere zu Implementierung und Dauer des Betriebs von SOC, - Auftraggeber inkl. Ansprechpartner und Telefonnummer, - Leistungszeitraum, - Kurzbeschreibung der durchgeführten Dienstleistungen, insbesondere Angabe zum erbrachten Support/Service und zu dem betreuten SIEM-Tool. Mindestanforderung: Nachweis über mindestens zwei vergleichbare und abgeschlossene Referenzprojekte der letzten drei Jahre, davon mindestens eine vergleichbare Referenz, die für einen Akteur, der eine kritische Infrastruktur betreibt, erbracht wurde. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center

(SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 800 Events per Second (EPS) mit einem 24/7/365-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird.

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: Nachweis über mindestens zwei vergleichbare und abgeschlossene Referenzprojekte der letzten drei Jahre, davon mindestens eine vergleichbare Referenz, die für einen Akteur, der eine kritische Infrastruktur betreibt, erbracht wurde. Vergleichbar sind Leistungen über den Betrieb eines Security Operations Center (SOC) inklusive eines Security Information and Event Management (SIEM) mit einer Ereignisrate von mindestens 800 Events per Second (EPS) mit einem 24/7/365-Support in allen drei Support-Level-Klassen (1/2/3) umfassen. Als abgeschlossen gelten Referenzprojekte, deren Implementierung abgeschlossen ist und die SIEM-/SOC-Lösung seit mindestens zwölf (12) Monaten produktiv betrieben wird. Anzugeben sind: - Projektinhalt mit Angaben zu Zeitdauer und Charakteristik, Projektziel, insbesondere zu Implementierung und Dauer des Betriebs von SOC, - Auftraggeber inkl. Ansprechpartner und Telefonnummer, - Leistungszeitraum, - Kurzbeschreibung der durchgeführten Dienstleistungen, insbesondere Angabe zum erbrachten Support/Service und zu dem betreuten SIEM-Tool.

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: Für die Auswahl entscheidend ist zu 60 % die nachgewiesene Kompetenz und Erfahrung anhand der Vergleichbarkeit eingereichten Referenzen über die mit der ausgeschriebenen Leistung vergleichbar erbrachten Leistungen nach Maßgabe der nachfolgend definierten Anforderungen. Die Vergabestelle beschränkt die Zahl der einreichbaren Referenzen auf sechs (6) Referenzen pro Bewerber /Bewerbergemeinschaft. Jede der eingereichten Referenz wird anhand des nachstehenden Punktesystems wie folgt bewertet: 15 Punkte bei Vorliegen folgender Voraussetzungen: (1) Referenz über 1.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 1000 EPS im Produktivbetrieb. 1.2. Bereitstellung als hochverfügbare Lösung (? 99,9 % Verfügbarkeit) 1.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 1.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 1.5. Einsatz von Incident Response-Mechanismen sowie automatisierten Abläufen im Sinne eines SOAR-Ansatzes (Security Orchestration, Automation and Response) oder vergleichbare Interventionsmöglichkeiten 1.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 1.7. Die Referenz muss sich auf einen Auftraggeber im Bereich Energiewirtschaft und/oder im Bereich kritischer Infrastruktur (KRITIS) beziehen 1.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 1.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 13 Punkte: 2.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 1000 EPS im Produktivbetrieb. 2.2. Bereitstellung als hochverfügbare Lösung (? 99,9 % Verfügbarkeit) 2.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 2.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 2.5. Einsatz von Incident Response-Mechanismen sowie automatisierte Abläufe im Sinne eines SOAR-Ansatzes (Security Orchestration, Automation and Response)

oder vergleichbare Interventionsmöglichkeiten 2.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 2.7. Die Referenz muss sich auf einen Auftraggeber im Bereich Energiewirtschaft und/oder im Bereich kritischer Infrastruktur (KRITIS) beziehen 2.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 2.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 11 Punkte 3.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 800 EPS im Produktivbetrieb. 3.2. Bereitstellung als hochverfügbare Lösung (? 98,5 % Verfügbarkeit) 3.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 3.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 3.5. Einsatz von Incident Response-Mechanismen oder vergleichbare Interventionsmöglichkeiten 3.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 3.7. Die Referenz muss sich auf einen vergleichbaren Auftraggeber im Bereich Energiewirtschaft und/oder kritische Infrastruktur (KRITIS) beziehen 3.8. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 3.9. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 8 Punkte 4.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 800 EPS im Produktivbetrieb. 4.2. Bereitstellung als hochverfügbare Lösung (? 98,5 % Verfügbarkeit) 4.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1/2/3) 4.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 4.5. Einsatz von Incident Response-Mechanismen oder vergleichbare Interventionsmöglichkeiten 4.6. Durchführung forensischer Analysen im Rahmen von Sicherheitsvorfällen (in der Referenzbeschreibung darzustellen 4.7. Die Abnahme /Produktivsetzung liegt mindestens 12 Monate zurück 4.8. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider) 5 Punkte: 5.1. Konzeption, Integration und Betrieb einer SIEM-Lösung mit mindestens 800 EPS im Produktivbetrieb. 5.2. Bereitstellung als hochverfügbare Lösung (? 98,5 % Verfügbarkeit) 5.3. 24/7/365-Überwachung durch ein SOC mit vollständiger Abdeckung der Supportklassen (1 /2/3) 5.4. Umsetzung oder Nutzung eines anerkannten Frameworks zur Angriffserkennung, z. B. MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework (MITRE ATT&CK(R)), Lockheed Martin Cyber Kill Chain(R)) 5.5. Die Abnahme/Produktivsetzung liegt mindestens 12 Monate zurück 5.6. Die Lösung befindet sich nachweislich im aktiven Betrieb durch den MSSP (Managed Security Service Provider)
Anhand der Kriterien werden die Bewerber ausgewählt, die zur zweiten Phase des Verfahrens eingeladen werden sollen
Gewichtung (Prozentanteil, genau): 60,00

Kriterium: Referenzen zu bestimmten Dienstleistungen
Beschreibung des Auswahlkriteriums: Bestandteil der Vergabeunterlagen ist das Formblatt - Erklärung zur Kundenzufriedenheit, das von dem jeweiligen Auftraggeber einer eingereichten Referenz auszufüllen ist. Es dürfen nur ausgefüllte Formblätter von Auftraggebern zu eingereichten vergleichbaren und abgeschlossenen Referenzprojekten eingereicht werden. Gewertet wird jeweils nur der Grad der nachgewiesenen Zufriedenheit über vergleichbare Referenzprojekte. Die durch einen Auftraggeber abgegebene ausgefüllte Erklärung zur Kundenzufriedenheit wird wie folgt bewertet: Ein Bewerber erhält für jeden sehr zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung, die einen verbindlichen Fertigstellungstermin umfasste, pro ausgefülltem

Formblatt 15 Punkte. Ein Bewerber erhält für jeden sehr zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung pro ausgefülltem Formblatt 12 Punkte. Ein Bewerber erhält für jeden zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung, die einen verbindlichen Fertigstellungstermin umfasste, pro ausgefülltem Formblatt 8 Punkte. Ein Bewerber erhält für jeden zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung pro ausgefülltem Formblatt 6 Punkte. Ein Bewerber erhält für jeden teilweise zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung, die einen verbindlichen Fertigstellungstermin umfasste, pro ausgefülltem Formblatt 4 Punkte. Ein Bewerber erhält für jeden teilweise zufriedenen Referenzkunden über vergleichbare Referenzleistungen in Bezug auf die erbrachte Gesamtleistung pro ausgefülltem Formblatt 2 Punkte. Die erreichten Punkte werden mit dem o.g. Gewichtungsfaktor (50 %) multipliziert. Die sechs (6) Bewerber mit den insgesamt höchsten Punktzahlen (Summe aus "Kompetenz und Erfahrung" und "Grad der Kundenzufriedenheit") werden zur Angebotsabgabe ausgewählt. Sollten mehrere Bewerber die gleiche Punktzahl erhalten, behält sich die ÜSTRA vor, die abschließende Auswahl und Reduzierung des Bieterkreises durch Losverfahren herbeizuführen.
Anhand der Kriterien werden die Bewerber ausgewählt, die zur zweiten Phase des Verfahrens eingeladen werden sollen
Gewichtung (Prozentanteil, genau): 40,00

Kriterium: Durchschnittliche jährliche Belegschaft
Beschreibung des Auswahlkriteriums: e) Eigenerklärung gem. § 46 Abs. 3 Nr. 2 VgV und Angabe des jährlichen Mittelwertes der in den letzten drei Jahren im Unternehmen angestellten Personen, jeweils aufgegliedert in die Bereiche Support zu SOC/SIEM und Entwicklung des SOC. Mindestanforderung: Eigenerklärung, dass der Bewerber/die Bewerbergemeinschaft über verfügbares Personal von mindestens zehn (10) Beschäftigten im Bereich SOC, die alle drei Support-Levels bearbeiten, davon mindestens jeweils zwei (2) Beschäftigte im Level 3-Support verfügt (Antrag auf Teilnahme).
Informationen über die zweite Phase eines zweiphasigen Verfahrens:
Mindestzahl der zur zweiten Phase des Verfahrens einzuladenden Bewerber: 1
Höchstzahl der zur zweiten Phase des Verfahrens einzuladenden Bewerber: 4
Das Verfahren wird in mehreren aufeinanderfolgenden Phasen durchgeführt. In jeder Phase können einige Teilnehmer ausgeschlossen werden

5.1.10. Zuschlagskriterien

Kriterium:
Art: Preis
Bezeichnung: Angebotspreis
Beschreibung: Das der Angebotsaufforderung beigefügte Preisblatt ist ausgefüllt mit dem Angebot einzureichen. Der niedrigste Gesamtpreis gem. Preisblatt bildet den Referenzpreis, der die volle Bewertungspunktzahl von 45 Punkten erhält. Die Punktzahl der weiteren Angebote ergibt sich nach folgender Formel: Bewertungspunkte = 45 X (Referenzpreis dividiert durch Angebotspreis). Der Bieter hat seine Preiskalkulation auf einer gesonderten Anlage zu erläutern.
Kategorie des Gewicht-Zuschlagskriteriums: Gewichtung (Prozentanteil, genau)
Zuschlagskriterium — Zahl: 45
Kriterium:
Art: Qualität
Bezeichnung: Leistung

Beschreibung: Weiteres Bewertungskriterium ist die Qualität der angebotenen Leistungen, die anhand des einzureichenden Umsetzungskonzeptes und des einzureichenden Servicekonzeptes entsprechend der Bewertungsmatrix bewertet wird. Das Umsetzungskonzept wird mit 65% und das Servicekonzept mit 35% gewichtet.
Kategorie des Gewicht-Zuschlagskriteriums: Gewichtung (Prozentanteil, genau)
Zuschlagskriterium — Zahl: 55

5.1.11. Auftragsunterlagen

Sprachen, in denen die Auftragsunterlagen offiziell verfügbar sind: Deutsch
Frist für die Anforderung zusätzlicher Informationen: 14/08/2025 23:59:59 (UTC+02:00) Osteuropäische Zeit, Mitteleuropäische Sommerzeit
Internetadresse der Auftragsunterlagen: https://www.dtvp.de/Satellite/notice/CXP4YHS5GAL/documents

Ad-hoc-Kommunikationskanal:

URL: https://www.dtvp.de/Satellite/notice/CXP4YHS5GAL

5.1.12. Bedingungen für die Auftragsvergabe

Verfahrensbedingungen:

Voraussichtliches Datum der Absendung der Aufforderungen zur Angebotseinreichung: 12/09/2025

Bedingungen für die Einreichung:

Elektronische Einreichung: Erforderlich
Adresse für die Einreichung: https://www.dtvp.de/Satellite/notice/CXP4YHS5GAL
Sprachen, in denen Angebote oder Teilnahmeanträge eingereicht werden können: Deutsch
Elektronischer Katalog: Nicht zulässig
Varianten: Nicht zulässig
Die Bieter können mehrere Angebote einreichen: Nicht zulässig
Frist für den Eingang der Teilnahmeanträge: 21/08/2025 10:00:00 (UTC+02:00) Osteuropäische Zeit, Mitteleuropäische Sommerzeit

Informationen, die nach Ablauf der Einreichungsfrist ergänzt werden können:

Nach Ermessen des Käufers können einige fehlenden Bieterunterlagen nach Fristablauf nachgereicht werden.
Zusätzliche Informationen: Die Vergabestelle behält sich vor, gem. § 51 SektVO auch im Teilnahmewettbewerb nach sachgerechtem Ermessen fehlende Unterlagen, Erklärungen und Angaben binnen einer Frist von drei (3) Werktagen nachzufordern. Unterlagen, Erklärungen und/oder Nachweise, die nach Fristablauf eingereicht werden, werden nicht berücksichtigt. Der Teilnahmeantrag wird in der dann vorliegenden Fassung geprüft und die Eignung des Bewerbers bewertet. Zwingende Voraussetzung für die Wertbarkeit eines Teilnahmeantrags ist ein fristgerecht eingegangener, rechtswirksam unterschriebener Teilnahmeantrag.

Auftragsbedingungen:

Die Auftragsausführung muss im Rahmen von Programmen für geschützte Beschäftigungsverhältnisse erfolgen: Nein
Bedingungen für die Ausführung des Auftrags: Zwingende Voraussetzungen sind die Akzeptanz und Zeichnung folgender Unterlagen durch den Wettbewerbsteilnehmer: - Vereinbarung zur Auftragsverarbeitung (AVV) inklusive der Mindestanforderungen an die technischen und organisatorischen Maßnahmen (TOM) sowie - Vertraulichkeitsvereinbarung, - Vereinbarung über die Verarbeitung im Auftrag gemäß Art. 28 DSGVO zu diesem Vergabeverfahren gemäß der Anlage 3, Auftragsverarbeitungsvertrag - Geheimhaltungsvereinbarung - Verpflichtung zur Einhaltung der Vorgaben des MiLoG - Zeichnung der SanktVO 833

Elektronische Rechnungsstellung: Zulässig
Aufträge werden elektronisch erteilt: ja
Zahlungen werden elektronisch geleistet: ja
Von einer Bietergemeinschaft, die den Zuschlag erhält, anzunehmende Rechtsform: gesamtschuldnerisch haftend mit bevollmächtigtem Vertreter
Finanzielle Vereinbarung: gem. Vergabeunterlagen

5.1.15. Techniken

Rahmenvereinbarung:
Rahmenvereinbarung ohne erneuten Aufruf zum Wettbewerb
Höchstzahl der Teilnehmer: 1
Informationen über das dynamische Beschaffungssystem:
Kein dynamisches Beschaffungssystem

5.1.16. Weitere Informationen, Schlichtung und Nachprüfung

Überprüfungsstelle: Vergabekammer Niedersachsen beim Nds. Ministerium für Wirtschaft, Verkehr, Bauen und Digitalisierung
Informationen über die Überprüfungsfristen: Wettbewerbsteilnehmern steht der vergaberechtliche Rechtsschutz gemäß den §§ 160 ff. GWB zur Verfügung. Ein Nachprüfungsverfahren ist nur auf Antrag zulässig. Antragsbefugt ist gemäß § 160 Abs. 2 GWB jedes Unternehmen, das ein Interesse an dem öffentlichen Auftrag hat und eine Verletzung in seinen Rechten nach § 97 Abs. 6 GWB durch Nichtbeachtung von Vergabevorschriften geltend macht. Dabei ist darzulegen, dass dem Unternehmen durch die behauptete Verletzung der Vergabevorschriften ein Schaden entstanden ist oder zu entstehen droht. Der Antrag ist gemäß § 160 Abs. 2 GWB unzulässig, soweit: 1) Der Antragsteller den geltend gemachten Verstoß gegen Vergabevorschriften vor Einreichen des Nachprüfungsantrags erkannt und gegenüber dem Auftraggeber nicht innerhalb einer Frist von 10 Kalendertagen gerügt hat; der Ablauf der Frist nach § 134 Abs. 2 bleibt unberührt, 2) Verstöße gegen Vergabevorschriften, die aufgrund der Bekanntmachung erkennbar sind, nicht spätestens bis zum Ablauf der in der Bekanntmachung benannten Frist zur Bewerbung gegenüber dem Auftraggeber gerügt werden, 3) Verstöße gegen Vergabevorschriften, die erst in den Vergabeunterlagen erkennbar sind, nicht spätestens bis zum Ablauf der Frist zur Bewerbung oder Angebotsabgabe gegenüber dem Auftraggeber gerügt werden, 4) Mehr als 15 Kalendertage nach Eingang der Mitteilung des Auftraggebers, einer Rüge nicht abhelfen zu wollen, vergangen sind. Satz 1 gilt nicht bei einem Antrag auf Feststellung der Unwirksamkeit des Vertrags nach § 135 Satz 1 Nr. 2. § 134 Abs. 1 Satz 2 GWB bleibt unberührt.
Organisation, die zusätzliche Informationen über das Vergabeverfahren bereitstellt: Stadtwerke Achim AG
Organisation, die Teilnahmeanträge entgegennimmt: Stadtwerke Achim AG

8. Organisationen

8.1. ORG-0001

Offizielle Bezeichnung: Stadtwerke Achim AG
Registrierungsnummer: DE 116739835
Postanschrift: Gaswerkstraße 7
Stadt: Achim
Postleitzahl: 28832
Land, Gliederung (NUTS): Verden (DE93B)
Land: Deutschland

E-Mail: alexandra.losch@hlp-rae.de
Telefon: +511262938-0
Rollen dieser Organisation:
Beschaffer
Organisation, die zusätzliche Informationen über das Vergabeverfahren bereitstellt
Organisation, die Teilnahmeanträge entgegennimmt

8.1. ORG-0002

Offizielle Bezeichnung: Vergabekammer Niedersachsen beim Nds. Ministerium für Wirtschaft, Verkehr, Bauen und Digitalisierung
Registrierungsnummer: t:04131153308
Postanschrift: Auf der Hude 2
Stadt: Lüneburg
Postleitzahl: 21339
Land, Gliederung (NUTS): Lüneburg, Landkreis (DE935)
Land: Deutschland
E-Mail: vergabekammer@mw-niedersachsen.de
Telefon: 00494131 152943
Rollen dieser Organisation:
Überprüfungsstelle

8.1. ORG-0003

Offizielle Bezeichnung: Datenservice Öffentlicher Einkauf (in Verantwortung des Beschaffungsamts des BMI)
Registrierungsnummer: 0204:994-DOEVD-83
Stadt: Bonn
Postleitzahl: 53119
Land, Gliederung (NUTS): Bonn, Kreisfreie Stadt (DEA22)
Land: Deutschland
E-Mail: noreply.esender_hub@bescha.bund.de
Telefon: +49228996100
Rollen dieser Organisation:
TED eSender

Informationen zur Bekanntmachung

Kennung/Fassung der Bekanntmachung: cc9c6ff2-0ea5-4954-80aa-01055aedd311 - 01
Formulartyp: Wettbewerb
Art der Bekanntmachung: Auftrags- oder Konzessionsbekanntmachung – Standardregelung
Unterart der Bekanntmachung: 17
Datum der Übermittlung der Bekanntmachung: 21/07/2025 15:16:41 (UTC+02:00) Osteuropäische Zeit, Mitteleuropäische Sommerzeit
Sprachen, in denen diese Bekanntmachung offiziell verfügbar ist: Deutsch
Veröffentlichungsnummer der Bekanntmachung: 482683-2025
ABl. S – Nummer der Ausgabe: 139/2025
Datum der Veröffentlichung: 23/07/2025