

Vergabenummer: X-KVWL-2026-0014

Vergabeverfahren „Security Operation Center (SOC) & Digital Forensics and Incident Response (DFIR)“



Im Dienst der Medizin.

**Beschränkte Ausschreibung mit Teilnahmewettbewerb gem. UVgO
Security Operation Center (SOC) & Digital Forensics and Incident Response (DFIR)**

**- Vergabeunterlage B / Teilnahmeantrag –
Los 1: Security Operation Center (SOC)**

Name des Bieters/der Bietergemeinschaft:

Mit Abgabe dieses Teilnahmeantrags bewerbe ich mich um die Vergabe des v.g. Auftrags.

Inhaltsverzeichnis

1	Angaben zum Bewerber / zu den Mitgliedern der Bewerbergemeinschaft	3
2	Angaben zur Leistungsfähigkeit des Unternehmens Los 1 – Security Operation Center (SOC).....	4
2.1	Ausschlusskriterien	4
2.2	Bewertungskriterien	5
2.3	Angaben zur personellen Leistungsfähigkeit des Unternehmens	6
2.1	Vertrag	10
2.2	Präsentation.....	13

1 Angaben zum Bewerber / zu den Mitgliedern der Bewerbergemeinschaft

Tabelle 1: Bieterangaben.

Name des Bieters / der Bietergemeinschaft:	
Adresse:	
Ansprechpartner für Rückfragen der Vergabestelle:	
Telefon:	
E-Mail des Ansprechpartners:	

2 Angaben zur Leistungsfähigkeit des Unternehmens Los 1 – Security Operation Center (SOC)

2.1 Ausschlusskriterien

Tabelle 2: Ausschlusskriterien Teilnahmeantrag SOC.

Kriterium	Angabe Ja/Nein
Das Unternehmen ist europäisch und hat einen Standort in Deutschland mit deutschsprachigem Support. Es ist vom Bieter und seinen eingesetzten Unterauftragnehmern sicherzustellen, dass die Verarbeitung gem. Ziffer 1 Abs. 8 AVV erfolgt.	
Das Unternehmen ist nach ISO27001 zertifiziert.	
Das Unternehmen ist nach SOC-CMM zertifiziert.	
Das Unternehmen hat mindestens 30 Mitarbeiter.	
Das Unternehmen hat mindestens 10 erfahrene SOC-Analysten.	
Das Unternehmen hat mindestens 5 Vorfallsbearbeiter.	
Das Unternehmen hat mindestens 2 Account-Manager.	
Das Unternehmen hat 3 Referenzen, die tiefergehende ESET-Kenntnisse und Anbindungsmöglichkeiten nachweisen.	
Das Unternehmen hat mindestens 3 Referenzen, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat.	

* Hinweis zu den Ausschlusskriterien:

Sofern eines dieser Kriterien nicht erfüllt wird, werden Sie nicht für die 2. Stufe ausgewählt werden können und scheiden somit von der weiteren Berücksichtigung im Verfahren aus.

2.2 Bewertungskriterien

Tabelle 3: Bewertungskriterien Teilnahmeantrag SOC.

Oberkriterium	Unterkriterium	Angabe Bieter (Sollte der Platz hier nicht ausreichend sein, kann ein separates Dokument mit entsprechendem Verweis mit Angebotsabgabe eingereicht werden)
Fachliche und Technische Leistungsfähigkeit	Der Bieter hat eine ESET-Partnerschaft.	
	Das Unternehmen arbeitet nach International Threat Intelligence.	
	Das Unternehmen hat ein Prüfdokument der angebotenen Leistung.	

*Hinweis zur Punktevergabe:

Die Vergabe der Punkte für die Ausführungen des Bewerbers zu den jeweiligen Unterkriterien werden wie folgt vergeben:

* volle Punktzahl: Die Aussagen des Bewerbers zum jeweiligen Unterkriterium überzeugen uneingeschränkt.

* 75% der Punktzahl: Die Aussagen des Bewerbers zum jeweiligen Unterkriterium überzeugen größtenteils, weisen aber vereinzelt (d. h. bei einer Teilaussage oder bei wenigen Teilaussagen) kleinere Schwächen bzw. Kritikpunkte auf.

Vergabeverfahren „Security Operation Center (SOC) & Digital Forensics and Incident Response (DFIR)“

* halbe Punktzahl: Die Aussagen des Bewerbers zum jeweiligen Unterkriterium sind insgesamt überwiegend noch überzeugend. Sie weisen aber entweder vereinzelt (d. h. bei einer Teilaussage oder bei wenigen Teilaussagen) deutliche Schwächen bzw. Kritikpunkte oder in größerem Umfang (d. h. bei einer Vielzahl von Teilaussagen) kleinere Schwächen bzw. Kritikpunkte auf.

* 25% der Punktzahl: Die Aussagen des Bewerbers zum jeweiligen Unterkriterium überzeugen nur zum Teil. Sie weisen in größerem Umfang (d. h. bei einer Vielzahl von Teilaussagen) deutliche Schwächen bzw. Kritikpunkte auf oder vereinzelt (d. h. bei einer Teilaussage oder bei wenigen Teilaussagen) deutliche Schwächen bzw. Kritikpunkte und gleichzeitig in größerem Umfang (d. h. bei einer Vielzahl von Teilaussagen) kleinere Schwächen bzw. Kritikpunkte.

* keine Punkte: Die Aussagen des Bewerbers zum jeweiligen Unterkriterium überzeugen in Gänze nicht oder entsprechende Vorschläge fehlen gänzlich.

2.3 Angaben zur personellen Leistungsfähigkeit des Unternehmens

Tabelle 4: Durchschnittliche Anzahl Mitarbeiter, umgerechnet auf Vollzeitstellen.¹

Jahr	2024	2025	aktuell
Gesamt:			
Anzahl erfahrene SOC-Analysten:			
Anzahl Vorfallsbearbeiter:			
Anzahl Account-Manager:			
Anzahl nach BSI zertifizierte (oder vergleichbar) Vorfallsbearbeiter:			
Anzahl nach GIAC Security Operations Certified (oder vergleichbar) zertifiziert:			
Anzahl nach GIAC Security Operations Manager Certification (oder vergleichbar) zertifiziert:			

¹ Bei Bewerbungsgemeinschaften sind jeweils die kumulierten Werte aller Mitglieder anzugeben, ohne dass weitere Hinweise oder Nachweise notwendig sind.

Key Account Manager*in

Tabelle 5: Angaben Key Account Manager*in. Die Angaben sollen durch das beigefügte Profil ergänzt werden.

Key Account Manager*in		Angaben Bieter
Vita	Bitte geben Sie den höchsten Ausbildungsabschluss des zugeordneten Key Account Managers an und nennen Sie die Anzahl der Berufsjahre im IT-/Cybersecurity-Bereich sowie im B2B-Key-Account-Management.	
	Wie viele Jahre Erfahrung hat der Key Account Manager in der Betreuung von SOC- oder Security-Dienstleistungs-Projekten im Gesundheitsumfeld?	
	Haben Sie Referenzen, die tiefergehende ESET-Kenntnisse und Anbindungsmöglichkeiten nachweisen?	
	Haben Sie Referenzen, die nachweist, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	
Fachliche Skills	Beschreiben Sie die Erfahrung des Key Account Managers in der Führung von strategischen Gesprächen mit C-Level-Führungskräften (CISO, CTO, Chief Information Security Officer). Welche Methoden nutzt er/sie, um technische Inhalte verständlich zu kommunizieren?	
	Welche Branchenkenntnisse und Erfahrungen mit regulatorischen Anforderungen (z.B. NIS2, BSI C5, ISO 27001, TISAX) bringt der Key Account Manager mit? In welchen regulierten Branchen hat er/sie bereits SOC-Services betreut?	

	Beschreiben Sie anhand eines konkreten Beispiels, wie der Key Account Manager in einer komplexen Kundensituation (z.B. bei Sicherheitsvorfällen oder Leistungsabweichungen) zur Zufriedenheit und Bindung des Kunden beigetragen hat.	

Vorfallsbearbeiter *in

Tabelle 6: Angaben Vorfallsbearbeiter *in. Die Angaben sollen durch das beigefügte Profil ergänzt werden.

Vorfallsbearbeiter*in		Angaben Bieter
Vita	Bitte nennen Sie die durchschnittliche Anzahl der Berufsjahre im IT-Bereich sowie speziell in der Incident Response / Vorfallsbearbeitung.	
	Wie viele Jahre durchschnittliche Erfahrung haben Ihre Vorfallsbearbeiter in der Bearbeitung von Sicherheitsvorfällen (Incident Response)? Bitte nennen Sie die durchschnittliche Anzahl bearbeiteter Sicherheitsvorfälle pro Jahr. Fokus sollte auf dem Gesundheitsbereich liegen.	
	Haben Sie Referenzen, die tiefergehende ESET-Kenntnisse und Anbindungsmöglichkeiten nachweisen?	
	Haben Sie Referenzen, die nachweist, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	

Vergabeverfahren „Security Operation Center (SOC) & Digital Forensics and Incident Response (DFIR)“

Fachliche Skills	Welche anerkannten Sicherheitszertifizierungen (z.B. CEH, GCIA, GCIH, CompTIA Security+, GIAC Certified Incident Handler) besitzen Ihre Vorfallsbearbeiter? Bitte geben Sie den Prozentsatz der Vorfallsbearbeiter mit mindestens einer relevanten Zertifizierung an.	
	Beschreiben Sie die Fähigkeiten Ihrer Vorfallsbearbeiter in den folgenden Bereichen: Malware-Analyse, Forensik, Netzwerk-Forensik, Log-Analyse und Threat Hunting. Welche Tools setzen Sie hierfür ein?	
	Beschreiben Sie, wie Ihre Vorfallsbearbeiter in High-Pressure-Situationen (z.B. bei kritischen Sicherheitsvorfällen) reagieren. Wie koordinieren Sie Eskalationen und Kommunikation mit dem Kunden während eines aktiven Incidents?	
	Welche regelmäßigen Fort- und Weiterbildungsmaßnahmen absolvieren Ihre Vorfallsbearbeiter? Wie stellen Sie sicher, dass das Team mit neuen Bedrohungen, Angriffsmustern und Technologien Schritt hält?	

SOC-Analysten*in**Tabelle 7: Angaben SOC-Analysten *in.** Die Angaben sollen durch das beigegefügte Profil ergänzt werden.

SOC-Analyst*in		Angaben Bieter
Vita	Bitte nennen Sie die durchschnittliche Anzahl der Berufsjahre im IT-Bereich sowie speziell in der SOC-Überwachung / Security Monitoring.	
	Wie viele Jahre durchschnittliche Erfahrung haben Ihre SOC-Analysten in der Überwachung und Analyse von Sicherheitsereignissen (SIEM, Log Analysis, Threat Detection)?	

Vergabeverfahren „Security Operation Center (SOC) & Digital Forensics and Incident Response (DFIR)“

	Haben Sie Referenzen, die tiefergehende ESET-Kenntnisse und Anbindungsmöglichkeiten nachweisen?	
	Haben Sie Referenzen, die nachweist, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	
Fachliche Skills	Welche anerkannten Sicherheitszertifizierungen (z.B. CompTIA Security+, CEH, GCIA, GCIH, AZ-500) besitzen Ihre SOC-Analysten? Bitte geben Sie den Prozentsatz der SOC-Analysten mit mindestens einer relevanten Zertifizierung an.	
	Mit welchen SIEM-Plattformen und Monitoring-Tools hat Ihr SOC-Team praktische Erfahrung? (z.B. Splunk, Elastic Stack, IBM QRadar, Microsoft Sentinel, Sumo Logic). Bitte beschreiben Sie das Kompetenz-Level pro Plattform und nennen Sie, welche Tools in Ihrem SOC primär eingesetzt werden.	
	Beschreiben Sie die Fähigkeiten Ihrer SOC-Analysten in den folgenden Bereichen: Erkennung von Anomalien, Bewertung von False Positives, Threat Intelligence-Integration, Priorisierung von Sicherheitsereignissen und Korrelation von Events. Wie stellen Sie sicher, dass Alerts effektiv gefiltert und priorisiert werden?	
	Wie dokumentieren und reportieren Ihre SOC-Analysten Sicherheitsereignisse und Trends? Welche Metriken (z.B. Mean Time to Detect, Mean Time to Respond, False Positive Rate) werden regelmäßig gemessen und zur Optimierung genutzt?	

2.1 Vertrag

Der mit den Vergabeunterlagen bereitgestellte Vertragsentwurf muss nicht mit dem Angebot eingereicht werden. Die Konkretisierung erfolgt durch die KVWL nach Zuschlagserteilung entsprechend dem Angebot des erfolgreichen Bieters.

Vergabeverfahren „Security Operation Center (SOC) & Digital Forensics and Incident Response (DFIR)“

Ebenfalls nicht einzureichen ist der mit den Vergabeunterlagen bereitgestellte Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO. Sollte im Rahmen einer Einzelbeauftragung die Verarbeitung von personenbezogenen Daten erforderlich sein, wird der Vertrag im Einzelfall mit dem Auftragnehmer geschlossen.

Sollten Sie einzelne Regelungen des Vertrags für unannehmbar halten, haben Sie die Möglichkeit, hierauf bis zur Frist zur Einreichung der Bieterfragen aufmerksam zu machen. Mit einer solchen Bieterfrage kann auch ein Vorschlag für eine Alternativformulierung verbunden werden.

Grundlage für die Leistungserbringung bildet der Vertrag, andere AGB sind ausgeschlossen.

Mit der Abgabe eines Angebots erklären Sie sich mit den vertraglichen Regelungen einverstanden. Eine nachträgliche Verhandlung über Vertragsinhalte ist unzulässig und wird ausgeschlossen.

Bestätigung des Bieters, dass die vertraglichen Bedingungen zur Kenntnis genommen wurden und akzeptiert werden.

Eine Nicht-Bestätigung führt zum Ausschluss des Angebotes.

Tabelle 8: Ökologische, soziale und umweltbezogene Zuschlagskriterien.

Frage	Angabe Bieter ²
Verfolgen Sie eine nachhaltige Unternehmensführung bzw. wird in Ihrem Unternehmen eine Nachhaltigkeitsstrategie verfolgt (z.B. Umweltmanagement, Energiemanagement, E-Fahrzeuge als Firmenfahrzeuge, Job-Bikes für die Mitarbeite*innen)? (Max. 10 Punkte)	
Zeichnet Ihr Unternehmen ein besonderes ökologisches und soziales Engagement aus? (Kurzbeschreibung ausreichend, ggf. auch Verweis auf separate Anlagen möglich.) (Max. 10 Punkte)	
Inwieweit beachtet Ihr Unternehmen in seinem Handlungsspielraum im Hinblick auf die Geschäftsbeziehungen in den Lieferketten die Einhaltung der Menschenrechte (z. B. keine Zwangsarbeit, keine Kinderarbeit, keine Diskriminierung, Arbeitsschutz) Compliance-Regelungen (Antikorruption und Bestechung) sowie den Schutz der Umwelt? (Max. 10 Punkte)	

² Sofern der Platz nicht ausreicht, können gerne Anlagen zu den Fragestellungen dem Angebot beigelegt werden.

Frage	Angabe Bieter ²
Bitte stellen Sie kurz zu den nachfolgenden Punkten die Umsetzung in Ihrem Unternehmen dar: - Förderung von Frauen - Vereinbarkeit von Beruf und Familie - Förderung / Weiterbildung von Mitarbeitern (Max. 10 Punkte)	

2.2 Präsentation

Zur besseren Koordination geben Sie bitte mindestens zwei Terminvorschläge zwischen dem 05.01.-15.01.2027 an. Wir weisen darauf hin, dass ggf. das Gespräch an einem anderen als von Ihnen vorgeschlagenen Termin stattfindet kann. Mit der Abgabe des Angebots erklären Sie sich bereit, an den u.a. Terminen verfügbar zu sein.

Die konkrete Termineinladung erfolgt gesondert zeitnah nach Ablauf der Angebotsfrist.

Terminvorschläge:	
--------------------------	--