

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 2: Digital Forensics and Incident Response (DFIR)**

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 2 – Digital Forensics and Incident Response (DFIR)	4
2.1	Ausschlusskriterien	4
2.2	Bewertungskriterien	5
2.3	Angaben zur personellen Leistungsfähigkeit des Unternehmens	6
2.1	Vertrag	15
2.2	Präsentation.....	17

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 2 – Digital Forensics and Incident Response (DFIR)

2.1 Ausschlusskriterien

Tabelle 2: Ausschlusskriterien Teilnahmeantrag DFIR.

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 ein nachgewiesener BSI-APT Response Dienstleister.	
Das Unternehmen hat mindestens 4 Experten im Bereich forensischer Analysen (Linux, Netzwerk, Windows).	
Das Unternehmen hat eine 24/7 Erreichbarkeit.	
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 DFIR.

Oberkriterium	Unterkriterium	Angabe Bieter (Sollte der Platz hier nicht ausreichend sein, kann ein separates Dokument mit entsprechendem Verweis mit Angebotsabgabe eingereicht werden)
Fachlich Technische Leistungsfähigkeit	Umwandelbarkeit des Kontingents.	
	Das Unternehmen hat folgende Zertifizierungen: BSI Pentestlabor oder gleichwertige Zertifizierungen.	
Personelle Leistungsfähigkeit	Partnernetzwerk oder eigene Experten in verschiedenen Bereichen	

*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.

* 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.

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

* 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 Teil-aussagen) 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 Experten im Bereich forensischer Analysen:			
Anzahl nach GIAC Certified Forensic Analyst (oder vergleichbar) zertifiziert:			
Anzahl nach GIAC Certified Forensic Examiner (oder vergleichbar) zertifiziert:			
Anzahl nach GIAC Certified Incident Handler (oder vergleichbar) zertifiziert:			
Anzahl nach GIAC Network Forensic Analyst (oder vergleichbar) zertifiziert:			
Anzahl nach GIAC Reverse Engineering Malware (oder vergleichbar) zertifiziert:			
Anzahl nach BSI Certified Pentester (oder vergleichbar) zertifiziert:			
Anzahl nach OSCP (oder vergleichbar) zertifiziert:			

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

Risikomanager*in

Tabelle 5: Angaben Risikomanager*in. Die Angaben sollen durch das beigefügte Profil ergänzt werden.

Risikomanager*in		Angaben Bieter
Vita	Bitte nennen Sie die Anzahl der Berufsjahre im Risikomanagement sowie speziell im IT-Risikomanagement / Cybersecurity-Risikomanagement.	
	Wie viele Jahre Erfahrung hat der Risikomanager in der Durchführung von Cybersecurity-Risikoanalysen, Risikobewertungen und der Entwicklung von Risikominderungsstrategien? Bitte nennen Sie mindestens zwei Referenzkunden mit ähnlichem Projektumfang.	
	Haben Sie Referenzen, die nachweisen, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	
Fachliche Skills	Welche anerkannten Zertifizierungen im Bereich Risikomanagement oder IT-Sicherheit besitzt der Risikomanager? (z.B. CISSP, CISM, CRISC, CCSK, ISO 27001 Lead Auditor). Bitte beschreiben Sie zudem seine/ihre Expertise in Cybersecurity Risk Frameworks (NIST Cybersecurity Framework, ISO 27001/27002, BSI C5).	
	Beschreiben Sie die Fähigkeiten des Risikomanagers in der Anwendung von Risikobewertungsmethoden (z.B. Quantitative/Qualitative Risikoanalyse, Threat Modeling, Vulnerability Assessment). Welche Erfahrungen hat der Risikomanager mit	

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

	regulatorischen Anforderungen und Standards im Bereich Gesundheitswesen? (z.B. NIS2, TISAX, BSI C5, ISO 27001, GDPR, branchenspezifische Regulierungen)	
	Beschreiben Sie, wie der Risikomanager Sicherheitsvorfälle und deren potenzielle Auswirkungen bewertet. Wie koordiniert er/sie die Kommunikation zwischen SOC-Team, Geschäftsführung und Stakeholdern bei kritischen Incidents? Bitte geben Sie ein konkretes Beispiel.	
	Wie erstellt und kommuniziert der Risikomanager Risikoreporte für verschiedene Stakeholder (CRO, CISO, Geschäftsführung)? Welche KPIs und Metriken nutzt er/sie zur Messung und Überwachung von Cybersecurity-Risiken? Wie trägt er/sie zur Weiterentwicklung der Sicherheitsstrategie bei?	

Forensiker*in

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

Forensiker*in		Angaben Bieter
Vita	Bitte nennen Sie die Anzahl der Berufsjahre im IT-Bereich sowie speziell in der digitalen Forensik und Incident Response Forensics.	
	Wie viele Jahre Erfahrung haben die Forensiker in der Durchführung von Forensik-Untersuchungen bei Sicherheitsvorfällen im Durchschnitt? Bitte nennen Sie die durchschnittliche Anzahl bearbeiteter Forensik-Cases pro Jahr im Bereich Gesundheitswesen.	
	Haben Sie Referenzen, die nachweisen, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	
Fachliche Skills	Welche anerkannten Forensik-Zertifizierungen besitzt der Forensiker? (z.B. GCFE, GCIA, GCIH, CCFE, CEH, EnCE, ENCE). Bitte beschreiben Sie zudem seine/ihre Expertise in Netzwerk-Forensik, Host-Forensik, Malware-Analyse und Cloud-Forensik.	
	Beschreiben Sie die Fähigkeiten des Forensikers in der forensischen Analyse von: Windows-Systemen, Linux/Unix-Systemen, macOS, Netzwerk-Traffic-Analyse (Packet Analysis), Log-Analyse und Cloud-Umgebungen (AWS, Azure, Google Cloud). Bitte geben Sie Kompetenz-Level pro Bereich an.	

	Beschreiben Sie die Fähigkeiten des Forensikers in der Analyse von Malware, Ransomware und Advanced Persistent Threats (APTs). Verfügt er/sie über Kenntnisse in Reverse Engineering oder Code-Analyse? Bitte geben Sie konkrete Beispiele aus durchgeführten Analysen.	
	Wie stellt der Forensiker sicher, dass bei Forensik-Untersuchungen die Beweisintegrität und forensische Standards (z.B. Chain of Custody) eingehalten werden? Wie dokumentiert und reportet er/sie Findings für potenzielle rechtliche Verfahren? Bitte beschreiben Sie seine/ihre Erfahrung mit Strafverfolgungsbehörden oder Rechtsanwälten.	

Tabelle 7: Angaben Penetrationstester*in. Die Angaben sollen durch das beigefügte Profil ergänzt werden.

Penetrationstester*in		Angaben Bieter
Vita	Bitte nennen Sie die Anzahl der Berufsjahre im IT-Bereich sowie speziell in Penetrationstests und Vulnerability Assessments.	
	Wie viele Jahre Erfahrung hat der Penetrationstester in der Durchführung von Penetrationstests und Security-Assessments? Bitte nennen Sie die durchschnittliche Anzahl durchgeführter Penetrationstest-Projekte pro Jahr und geben Sie Beispiele aus dem Gesundheitsbereich und Umgebungen (On-Premise, Cloud, Hybrid) an.	
	Haben Sie Referenzen, die nachweisen, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	
Fachliche Skills	Welche anerkannten Zertifizierungen im Bereich Penetrationstesting besitzt der Pentester? (z.B. CEH, OSCP, GPEN, eJPT, eCPPT, GWAPT). Bitte beschreiben Sie zudem seine/ihre Expertise in verschiedenen Angriffsszenarien: WebApp Testing, Netzwerk, Active Directory, Backup	
	Beschreiben Sie die Fähigkeiten des Pentesters in der Sicherheitsbewertung von: Windows-Umgebungen, Linux/Unix-Systemen, Netzwerk-Infrastruktur (Firewall, Router, VPN), Web-Anwendungen und Cloud-Plattformen. Bitte geben Sie Kompetenz-Level pro Bereich an.	
	Wie erstellt und kommuniziert der Pentester Pentest-Berichte für verschiedene Stakeholder (technisches Team, CISO, Geschäftsführung)? Wie detailliert sind die Remediation Recommendations und wie wird Priorisierung durchgeführt?	

Vergabenummer: X-KVWL-2026-0014

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

	Bitte beschreiben Sie seinen/ihren Erfahrung in der Nachbetreuung und Retest-Durchführung nach behobenen Findings.	
--	--	--

Tabelle 8: Angaben ISMS Berater*in. Die Angaben sollen durch das beigegefügte Profil ergänzt werden.

ISMS Berater*in		Angaben Bieter
Vita	Bitte nennen Sie die Anzahl der Berufsjahre im IT-Bereich sowie speziell in Information Security Management Systemen (ISMS) und Compliance-Beratung.	
	Wie viele Jahre Erfahrung hat der ISMS Berater in der Implementierung, Auditierung und Optimierung von ISMS nach ISO 27001 und anderen Standards? Bitte nennen Sie die Anzahl durchgeführter ISMS-Projekte in den letzten 3 Jahren und geben Sie Beispiele aus der Gesundheitsbranche an.	
	Haben Sie Referenzen, die nachweisen, dass eine Zusammenarbeit im öffentlichen Bereich stattgefunden hat?	
Fachliche Skills	Welche anerkannten Zertifizierungen im Bereich ISMS und Information Security besitzt der ISMS Berater? (z.B. ISO 27001 Lead Auditor, CISM, CISSP, CCSK, ISMS Foundation, ISMS Practitioner). Bitte beschreiben Sie zudem seine/ihre Expertise in relevanten Standards und Frameworks (ISO 27001/27002, NIS2, TISAX, BSI C5, NIST Cybersecurity Framework).	
	Beschreiben Sie die Fähigkeiten des ISMS Beraters in: Gap-Analysen, Risikoanalysen nach ISO 27005, Implementierung von Controls, interne Audits und Vorbereitung auf externe Zertifizierungsaudits. Welche methodischen Ansätze und Tools nutzt er/sie? Bitte geben Sie Beispiele aus durchgeführten Projekten.	

	Welche Erfahrungen hat der ISMS Berater mit regulatorischen Anforderungen und branchenspezifischen Standards? (z.B. NIS2, TISAX, BSI C5, GDPR, Datenschutz, Gesundheitswesen, Behörden). In welchen Branchen hat er/sie bereits ISMS-Projekte durchgeführt?	
	Beschreiben Sie die Fähigkeiten des ISMS Beraters in: Dokumentation von Sicherheitsrichtlinien und Prozessen, Prozessmodellierung, Erstellung von Kontrollmatrizen und Change Management bei ISMS-Implementierungen. Verfügt er/sie über Erfahrung mit ISMS-Softwarelösungen? Welche hat er/sie bereits eingesetzt?	
	Wie kommuniziert der ISMS Berater mit verschiedenen Stakeholdern (CISO, IT-Leitung, Geschäftsführung, Mitarbeiter)? Wie gestaltet er/sie den Übergang vom Audit zum operativen Betrieb? Beschreiben Sie seine/ihre Erfahrung in der Unterstützung von Verbesserungsprozessen und der Auffrischung von ISMS-Zertifizierungen.	

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.

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 9: 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:	
--------------------------	--