Leistungsverzeichnis zur Ausschreibung: 006/26

Managed SoC (Security Operations Center)

1. Kurzportrait UKD

Das Universitätsklinikum Düsseldorf (UKD) ist das größte Krankenhaus in der Landeshauptstadt und eines der wichtigsten medizinischen Zentren in NRW. Die 9.300 Mitarbeiterinnen und Mitarbeiter in UKD und Tochterfirmen setzen sich dafür ein, dass jährlich über 45.000 Patientinnen und Patienten stationär behandelt und 270.000 ambulant versorgt werden können.
Das UKD steht für internationale Spitzenleistungen in Krankenversorgung, Forschung und Lehre, sowie für innovative und sichere Diagnostik, Therapie und Prävention. Patientinnen und Patienten profitieren von der intensiven interdisziplinären Zusammenarbeit der 60 Kliniken und Institute. Die besondere Stärke der Uniklinik ist die enge Verzahnung von Klinik und Forschung zur sicheren Anwendung neuer Methoden.

2. Struktur der Leistungsbeschreibung und der Anforderungen

Die Anforderungen sind in diesem Dokument durch folgende Struktur gekennzeichnet:
ID: Kürzel zur leichteren Identifikation sowie inhaltliche Angaben zur Anforderung/ **Kurzbeschreibung der Anforderung.** Die Anforderungen werden wie folgt differenziert:

- **MUSS-Anforderung:** Entspricht einem Ausschlusskriterium i.S.e. Mindestanforderung. Das Angebot des Auftragnehmers muss diese Anforderung erfüllen. Die Nichterfüllung einer als Ausschlusskriterium gekennzeichneten Anforderung führt zwingend zum Ausschluss des Angebotes.
- **SOLL-Anforderung:** Entspricht einem Bewertungskriterium. Der Auftragnehmer beschreibt in seinem Angebot, ob und wie er die entsprechende Anforderung erfüllt. Die Erfüllung wird bewertet. Soweit dies nicht vom Auftraggeber anders verlangt wird, ist diese Anforderung dann im Auftragsfall vom Auftragnehmer seiner Beschreibung entsprechend ebenso umzusetzen, wie eine MUSS-Anforderung. Die Bewertung der SOLL-Anforderungen sind in der Bewertungsmatrix aufgeführt.

Enthalten die Vergabeunterlagen nach Auffassung des Bieters Unklarheiten, Unvollständigkeiten oder Fehler, so hat er unverzüglich die Vergabestelle schriftlich über das Vergabeprotal per Bieterfrage darauf hinzuweisen. Bitte geben Sie bei Bieterfragen zur Leistungsbeschreibung die ID, zum Bespiel DEF-SENT-01, an.

3. Auftragsgegenstand und Zielsetzung

Ziel dieser Ausschreibung ist die Auswahl eines qualifizierten Dienstleisters zur Einführung und Integration von Microsoft Defender für Endpoint auf allen relevanten Client- und Server-Systemen der Organisation. Das UKD ist eine KRITIS-Einrichtung gemäß BSI Gesetz. Im Rahmen des Auftrages ist dieser Sachverhalt zu berücksichtigen. Die Maßnahme umfasst:

- Installation und Konfiguration von Microsoft Defender auf Clients und Servern gemäß Best Practices.
- Anbindung an Microsoft Sentinel zur zentralisierten Sicherheitsüberwachung und Ereignisanalyse.
- Betrieb eines Managed Security Operations Center (SOC) zur kontinuierlichen Überwachung, Analyse und Reaktion auf sicherheitsrelevante Vorfälle.

Die Managed SOC-Dienstleistung umfasst folgende Mengen:
- Clients: 10.000
- Server: 1.500

Die Vertragslaufzeit beträgt 12 Monate mit der Option auf Verlängerung um jeweils weitere 12 Monate. Die Maximale Laufzeit beträgt 48 Monate. Die Verlängerung erfolgt ausschließlich durch den Auftraggeber zu den angebotenen Konditionen.

Lizenzen für Microsoft Defender und Microsoft Sentinal sind nicht Bestandteil dieser Ausschreibung und werden separat durch den Auftraggeber bereitgestellt.

4. Anforderungen Einführung Microsoft Defender und Sentinel

ID: DEF-SENT-01 Einführung und Integration Microsoft Defender & Sentinel [MUSS]
Installation und Konfiguration von Microsoft Defender for Endpoint auf allen definierten Clients und Servern gemäß Microsoft Best Practices.

ID: DEF-SENT-02 Anbindung an Microsoft Sentinel [MUSS]
Vollständige Anbindung der Defender-Telemetrie an Microsoft Sentinel inkl. Einrichtung von Datenconnectors, Workbooks und Alerts.

ID: DEF-SENT-03 Übernahme bestehender Sophos-Konfiguration [MUSS]
Funktionale Überführung der bestehenden Sophos-Konfiguration inkl. Richtlinien, Ausnahmen und Ausschlüsse in die neue Defender-Umgebung, technisch entsprechende Umsetzungen soweit dies möglich ist.

ID: DEF-SENT-04 Berücksichtigung von Client-Ausnahmen [MUSS]
Definierte Ausnahmen in der Sophos Konfiguration für Clients müssen in der neuen Konfiguration berücksichtigt und dokumentiert werden.

ID: DEF-SENT-05 Berücksichtigung von Server-Ausnahmen [MUSS]
Definierte Ausnahmen für Server müssen in der neuen Konfiguration berücksichtigt und dokumentiert werden.

ID: DEF-SENT-06 Dokumentation der Sicherheitskonfiguration [SOLL]
Bereitstellung einer vollständigen technischen Dokumentation der Konfiguration und Anbindung inkl. übernommener bzw. eigenerstellter Richtlinien und Automatisierungen.

ID: DEF-SENT-07 Schulung & Übergabe [SOLL]
Durchführung einer Schulung für Administratoren sowie strukturierte Übergabe der Lösung.

5. Anforderungen an das Managed SOC

ID: SOC-TECH-01 Zentrale Ereigniskorrelation [MUSS]
Das SOC muss sicherheitsrelevante Ereignisse aus Microsoft 365, Azure, Entra zentral korrelieren.

ID: SOC-TECH-02 Zentrale Ereigniskorrelation [MUSS]

Das SOC muss sicherheitsrelevante Ergebnisse von On-Premise Systemen vor Ort sammeln und in Ihre Lösung sicher übertragen und zentral korrelieren. Die Umsetzung muss technisch dargelegt werden. On-Premise Systeme aus denen Daten gesammelt werden müssen sind mindestens: Server-Systemen (Windows/Linux), Endponits, Firewalls, Syslog, AD, DNS, Proxy

ID: SOC-TECH-03 Integration zusätzlicher Datenquellen [MUSS]
Zusätzliche Datenquellen müssen über Konnektoren, APIs oder Syslog angebunden werden können.

ID: SOC-TECH-04 Detection Rules (KQL) [MUSS]
Erstellung und Pflege von KQL-basierten Detection Rules zur Erkennung bekannter und unbekannter Bedrohungen.

ID: SOC-TECH-05 Automatisierte Reaktionen [MUSS]
Automatisierte Reaktionen über Playbooks (z. B. Benutzer sperren, Geräte isolieren, Tickets erstellen) müssen möglich sein. Die Erstellung von 10 Playbooks ist zu inkludieren. Diese werden gemeinsam erstellt, können auf Basis von Playbooks des Bieters basieren und werden zusammen finalisiert. Hierbei sind Playbooks für Client- und Serverereignisse, Veränderung kritischer Berechtigungen im Tagesbetrieb, Flächenbetroffenheit, Verdacht auf Ransomware (Client) und Verdacht auf Ransomware (Server / zentrales Filesystem) zu erstellen.

ID: SOC-TECH-06 Dashboards und Reports [SOLL]
Bereitstellung von Dashboards und Reports für verschiedene Zielgruppen (Security-Team, IT-Leitung, Management).

ID: SOC-TECH-07 Langzeitarchivierung [MUSS]
Sicherstellung der Langzeitarchivierung gemäß BSI Empfehlung von Logs (min. 6 Monate) gemäß geltenden Compliance-Vorgaben muss gewährleistet sein.

ID-SOC-TECH-08 ITSM-Integration [MUSS]
Anbindung an bestehende ITSM-Systeme (z. B. ServiceNow) muss erfolgen.

ID:SOC-TECH-09 Erweiterte Datenquellenintegration [MUSS]
Integration zusätzlicher Systeme wie Firewalls (Fortinet, Check Point, Palo Alto) und NDR-Systeme (z. B. Armis) zur Erkennung von lateralem Bewegungsverhalten und Netzwerk-Anomalien.

SOC-ORG-01 Rollen und Verantwortlichkeiten [MUSS]
Klare Definition von Rollen und Verantwortlichkeiten (z. B. Analyst, Incident Manager, Threat Hunter) im SOC-Betrieb.

ID: SOC-ORG-02 Dokumentierte Prozesse [MUSS]
Dokumentierte Prozesse für Incident Response, Eskalation, Reporting und Lessons Learned müssen vorhanden sein.

ID: SOC-ORG-03 Use-Case-Entwicklung [MUSS]
Regelmäßige Entwicklung und Anpassung von Playbooks zur Reaktion auf neue Bedrohungslagen.

ID: SOC-ORG-04 Schulungen und Awareness [SOLL]
Durchführung von Schulungen und Awareness-Maßnahmen für interne Teams.

ID: SOC-ORG-05 Betriebszeiten [MUSS]
24/7 -Betrieb muss gewährleistet sein. Hierbei kann zwischen bedientem Betrieb und Betrieb nach Alarmierung unterschieden werden.

6. Allgemeine Anforderungen

ID: SOC-Allg-01 Einhaltung von gesetzlichen Vorschriften, Standards, Leitfäden und Richtlinien [MUSS]
Der Auftragnehmer MUSS die Umsetzung der jeweils aktuellen gesetzlichen Regelungen zum Datenschutz und Informationssicherheit für UK Düsseldorf im Rahmen der Umsetzungs- und Betriebsphase sicherstellen.

ID: SOC-Allg-02 Der Anbieter muss über folgende Zertifizierungen, personenbezogene Nachweise bzw. Referenzen verfügen. [MUSS]

- Nachweis einer Firmenzertifizierung nach ISO9001, ISO27001, BSI-IT-Grundschutz oder vergleichbarer Standard
- Nachweis der Qualifikation der Mitarbeiter hinsichtlich ITIL.V4 bzw. COBIT,
- Referenz von 4 Unternehmen als externes SOC im hier beschriebenen Umfang, hierbei mindestens 1 Unternehmen im Gesundheitswesen.

Für jedes benannte Unternehmen müssen mindestens ein Ansprechpartner benannt werden. Für die Rückfrage an diese ist jeweils mindestens ein Kontaktweg anzugeben. Die Kontakterlaubnis wird als „vorhanden“ unterstellt.

ID: SOC-Allg-03 AV-Vertrag [MUSS]
Notwendigkeit eines Abschlusses eines Auftragsverarbeitungsvertrages (AV-V) nach Artikel 28 DSGVO (insbesondere im Fall der (Fern-)Wartung) MUSS der Vertrag des UK Düsseldorf verwendet werden.

ID: SOC-Allg-04 Qualifikation in Defender & Sentinel [MUSS]
Alle Personen, die für die Konfiguration, Administration oder Überwachung von Microsoft Defender und Microsoft Sentinel verantwortlich sind, MÜSSEN über eine nachweisbare Qualifikation oder Zertifizierung verfügen. Anerkannt werden insbesondere Microsoft-Zertifizierungen wie:

- SC-200: Microsoft Security Operations Analyst

ID: SOC-Allg-05 Deutschsprachiger Support [MUSS]
Für alle sicherheitsrelevanten Systeme und Dienste (einschließlich Microsoft Defender und Microsoft Sentinel) muss ein deutschsprachiger Support verfügbar sein. Dies umfasst:

- Incident Response: Unterstützung bei Sicherheitsvorfällen in deutscher Sprache.
- Technischer Support: Hilfe bei Konfiguration, Betrieb und Fehlerbehebung.
- Dokumentation: Bereitstellung relevanter Anleitungen und Richtlinien in deutscher Sprache.

Der Support muss 24/7 erreichbar sein und darf keine Verzögerungen aufgrund von Sprachbarrieren verursachen.

ID: SOC-Allg-06 Betriebskonzept [MUSS]
Der Anbieter MUSS ein vollständiges Betriebskonzept für den Betrieb des Security Operations Centers (SOC) einreichen. Das Betriebskonzept muss mindestens folgende Inhalte umfassen:

- Organisationsstruktur
- Serviceumfang und Leistungsbeschreibung
- Betriebszeiten und Erreichbarkeit
- Prozesse und Workflows
- Sicherheits- und Compliance-Anforderungen
- Monitoring und Reporting
- Qualifikation des Personals
- Technische Architektur

7. Bewertung & Zuschlagskriterien

Kriterium	Gewichtung
Qualität des Betriebskonzepts	30 %
Erfüllung der Soll Kriterien	20 %
Preisgestaltung (Angebotspreis gemäß Anlage 1, als Berechnungsbasis gilt jeweils der Betrag einschließlich in Deutschland geltender Mehrwertsteuer)	50 %

Siehe Anlage 2 – Zuschlagskriterien und Bewertungsmatrix

8. Sonstige Vereinbarungen

Mit der Beteiligung an der Ausschreibung sowie die Auftragsannahme verpflichtet sich der Auftragsnehmer vorrangig die Einkaufsbedingungen des Universitätsklinikum Düsseldorf (Stand Mai 2019) anzunehmen.

Vor Beauftragung, innerhalb der Bindefrist, hat der Bieter einen entsprechenden EVB-IT Dienstvertrag (Langfassung) an den Auftraggeber, mit den Angaben aus dieser Vergabe an den Ansprechpartner des UKD zu übermitteln.

Die Rechnungslegung erfolgt je Quartal im Voraus.

Zahlungskonditionen: Gemäß Einkaufsbedingungen des Universitätsklinikums Düsseldorf