IT-Planwerk GmbH
88361 Altshausen **Hindenburgstr. 27** **+49(7584)640 96-0** **info@it-planwerk.de**

LEISTUNGSVERZEICHNIS

Lang- und Kurztexte

Alle Positionen

Projekt-Nr. :	25003
Bauvorhaben :	Klinikum Mittelbaden gGmbH Dr.-Rumpf-Weg 7 76530 Baden Baden
Auftraggeber :	Klinikum Mittelbaden gGmbH Dr.-Rumpf-Weg 7 76530 Baden Baden
Leistungsumfang :	SiEM & SOC System
Ausschreibung vom :	13.06.2025
Ausführungsfrist :	01.09.2025 - 31.08.2028
Aufklärungsfragen bis :	09.07.2025
Angebotsabgabe bis :	16.07.2025
Angebotsabgabe an :	elektronisch
Zuschlagsfrist:	01.09.2025
Laufzeit des Vertrages:	**3 Jahre**
Bieter:	.....
	.....
	.....
	.....
Angebotssumme netto :	EUR .....
.....% MWSt :	EUR .....
Angebotssumme brutto :	EUR

(Stempel und rechtsverbindliche Unterschrift) (Datum)

INHALTSVERZEICHNIS zum LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM

Umfang: SiEM & SOC System

Ausgabeumfang: Alle Positionen

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.	Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre

1 SiEM & SOC System

Leistungsbeschreibung

die Klinikum Mittelbaden gGmbH beabsichtigt, im Rahmen ihrer strategischen Weiterentwicklung der IT- und Informationssicherheit, eine Ausschreibung zur Vergabe von Dienstleistungen im Bereich Security Information and Event Management (SIEM) sowie Security Operation Center (SOC) durchzuführen.
Ziel der Ausschreibung ist es, einen leistungsfähigen und zuverlässigen Partner zu gewinnen, der die Klinikum Mittelbaden gGmbH bei der kontinuierlichen Überwachung, Analyse und Bewertung sicherheitsrelevanter Ereignisse unterstützt und einen wesentlichen Beitrag zur nachhaltigen Absicherung der IT-Infrastruktur leistet.
Die Leistungen sollen sich dabei eng an dem bestehenden Information-Security-Framework der Klinikum Mittelbaden gGmbH orientieren und integraler Bestandteil eines ganzheitlichen Sicherheitskonzepts sein.

Die Klinikum Mittelbaden gGmbH (nachfolgend „Klinikum Mittelbaden“ oder „KMB“) ist ein kommunales Gesundheitsunternehmen in gemeinsamer Trägerschaft der Stadt Baden-Baden und des Landkreises Rastatt. Das KMB betreibt zwei Akutkliniken mit mehreren Standorten, insgesamt rund 890 akutmedizinischen Betten, mehrere medizinische Versorgungszentren (MVZ), Pflegeeinrichtungen, ein Demenzzentrum, einen ambulanten Pflegedienst, ein Palliativzentrum sowie ein Hospiz.
Mit insgesamt etwa 3.500 Beschäftigten in den Akutkliniken, MVZs, Pflegeheimen sowie den Tochtergesellschaften zählt das KMB zu den bedeutenden Gesundheitsdienstleistern der Region. Als Akademisches Lehrkrankenhaus der Medizinischen Fakultät der Ruprecht-Karls-Universität Heidelberg bietet das KMB ein umfassendes medizinisches Versorgungsspektrum mit modernen Diagnose- und Therapieverfahren.

Folgende Geräte sind aktuell Bestandteil der Umgebung:
- ca. 3000 Clients
- ca. 250 Switches, davon 4 DC Switches
- ca. 15 Firewalls (4x Large, 4x Medium und 7x Small)
- ca. 20 Server mit insgesamt ca. 350 VM´s
- Storage

weitere Informationen zur aktuellen Umgebung:

PC-Arbeitsplätze und Notebooks	1650
IT-Abteilung	ca. 20 Mitarbeiter*innen Ausrichtung als steuernde IT operative Tätigkeiten
IT-Auslagerungen	verbundene Sourcing Partner für fast alle operativen Dienste Gewerke werden aktuell neu verteilt auch auf neue Partner
Cloud-Computing	Cisco Webex, SDWorks (HR), Medigate, Cybereason
Informationssicherheitsmanagement	Trennung OT und IT ISB ist außerhalb der IT angesiedelt
IT-Compliance	Regelwerke bauen auf ISO 27001 und Betriebsvereinbarungen auf

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.	Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre

Ticketsystem	- Matrix42ist führendes Ticketsystem, für alle operativen IT Services für zerntralen Überblick und Auswertungsbasis, sowie Steuerungszentrale. - Matrix42 wird basierend auf ITIL eingesetzt.
IT-Servicelandschaft	- Gewachsene, heterogene IT-Service-/ und Systemlandschaft - Vier externe Dienstleister erbringen in unterschiedlichen Ausprägungen und Verantwortlichkeiten die entsprechenden Services. - Die Implementierungsreihenfolge der Services, IT-Systeme (siehe Quellsysteme, Mengengerüste) sowie Applikationen können entsprechend in der Konzeption berücksichtigt werden.
Server (Produktion)	Windows Server, Citrix, AD, LDAP
Arbeitsplatzrechner	Ja
HTTP- und FTP-Proxy	Proxy: Fortinet Reverse Proxys: Ja SSL VPN: Fortigate
Mailgateway/ SMTP-Proxy/ PGP-Mailgateway	Ja, diverse
DNS-Proxy	Ja
Firewalls	FW: Fortigate
VPN Gateway	s.o.
Schutz gegen Schadsoftware/ Antivirus	Cyberreason
Web-Application- Systeme	Ja
Datenbanken	Oracle, MS-SQL, SAP DB2
Netzwerkmanagement und Netzwerkkomponenten	Cisco LAN und WLAN
Netzzugangskontrolle	Fortinet
PKI	Ja
Exchange	Exchange on Prem/ Exchange Online
Telefonie- und Videokonferenzsystem	Unify (Telefonie), Cisco WebEx
Sicheres Drucken/ SafeCom Secure Print	Über DL Multifunktionsgeräte
IT-Betriebswerkzeuge	Ticketing: Matrix42

Implementierung:
1 Die Implementierung der Systeme erdolgt Schrittweise über die gesamte Laufzeit bis zur geschätzen maximalen Systemanzahl.
2 Eine Verpflichtung zur Abnahme der Gesamtmenge resultiert daraus nicht.

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System

Ausgabeumfang: Alle Positionen OZ / Pos.-Nr.	Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre

Lizenzbedarf und Abrechnung:
1 Der Auftragnehmer ist verpflichtet, einmal jährlich den tatsächlich in Anspruch genommenen Leistungsumfang zu ermitteln. Die Ermittlung erfolgt jeweils zum Stichtag [31.12. eines Kalenderjahres] auf Basis der tatsächlichen Nutzung im abgelaufenen Vertragsjahr
2 Die auf dieser Grundlage ermittelte Nutzeranzahl bzw. Nutzungsmengen dienen als Berechnungsgrundlage für die Jahresrechnung des Folgejahres.
3 Der Auftragnehmer übermittelt dem Auftraggeber bis spätestens [15. Januar] eines jeden Jahres eine detaillierte Übersicht der Nutzung und die darauf basierende Abrechnung.

Vertragsverlängerung:
1 Die Vertragslaufzeit beträgt zunächst 36 Monate ab dem vereinbarten Vertragsbeginn.
2 Der Auftraggeber kann den Vertrag einmalig um bis zu 12 Monate verlängern, sofern dies dem Auftragnehmer spätestens drei Monate vor Ablauf der regulären Vertragslaufzeit schriftlich mitgeteilt wird.
3 Eine weitere Verlängerung um bis zu 12 Monate ist möglich, wenn die erste Verlängerung in Anspruch genommen wurde und der Auftraggeber dies dem Auftragnehmer ebenfalls mindestens drei Monate vor Ablauf der verlängerten Laufzeit schriftlich mitteilt.
4 Die maximale Gesamtlaufzeit des Vertrags beträgt 60 Monate. Die Entscheidung über die Inanspruchnahme der Verlängerungsoptionen erfolgt nach Bedarf des Auftraggebers.

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.		Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre

Abstimmung von Eventualpositionen vor Beauftragung

Bevor Eventualpositionen beauftragt werden, muss der Auftragnehmer diese gemeinsam mit dem IT-Planer und dem Auftraggeber technisch und wirtschaftlich prüfen. Die Ausführung darf erst nach schriftlicher Freigabe erfolgen.

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System
1 Managed Detection und Response

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.		Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre

1.1 Managed Detection und Response

Laufzeit/Preis

Die kalkulierte Laufzeit beträgt 3 Jahre

Bitte geben Sie wie folgt an:
Einheitspreis = jährlicher Preis
Gesamtbetrag = Jahrespreis x Laufzeit

Lizenzierung

Falls einer der Optionen nicht zutrifft, bitte 0€ eintragen!
Genaue Anzahl der User/Geräte muss im Workshop final aufgenommen werden.

Die Abrechnung der Lizenzen erfolgt jährlich nach tatsächlicher Nutzung. Hierzu muss jährlich eine Auswertung der aktiven Systeme als Grundlage der Berechnung durchgeführt werden.

1.1.1 **MDR User Lizenzen**

- Managed Detection & Response Lizenz je User
- Aufbewahrung der Log Daten für 90 Tage ohne Kapazitätsbeschränkung

3000 St/J _____ _____

Alternativposition .

1.1.2 **MDR Geräte Lizenzen**

- Managed Detection & Response Lizenz je Gerät
- Aufbewahrung der Log Daten für 90 Tage ohne Kapazitätsbeschränkung

2000 St/J _____ **NEP**

1.1.2 **MDR Server Lizenzen**

- Managed Detection & Response Lizenz je Server
- Aufbewahrung der Log Daten für 90 Tage ohne Kapazitätsbeschränkung

410 St/J _____ _____

1.1.3 **Grundkosten bereitgestellte Cloud Plattform**

- bereitgestellte Cloud Plattform

1 St/J _____ _____

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System
1 Managed Detection und Response

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.		Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre
1.1.4	**Zugriffslizenzen/Anbindung Cloud Plattform** • Zugriffslizenz für Server und User an Cloud Plattform	3410	St/J		
1.1.5	**First Response** • First Response • inkl. Reaktionszeit laut Lastenheft • automatisches Isolieren von Geräten durch SOC • Isolieren von Geräten nach Workflow • Fachunterstützung durch Security Experten • bevorzugten Zugriff auf Layer 2 und 3 Service Experten bei Bedarf	1	St/J		
1.1.6	**Incident Response inkl. Forensische Analyse** • Incident Response • Reaktionszeiten laut Lastenheft • Incident Response inkl. Forensischen Analysen • nach tatsächlichem Aufwand	1	Std		
1.1.7	**physischer MDR Sensor** • zur Erfassung und verschlüsselten Übertragung Daten mit 1 GB • Abfrage der Log Daten von Endpoints, Firewall, Server, Switches etc. • Überwachung von Netzwerkverkehr Layer 2-7 (Verbindungen, Protokolle, verdächtige Muster) • Aufbewahrung der Log Daten für 90 Tage ohne Kapazitätsbeschränkung	2	St/J		
1.1.8	**physischer MDR Sensor 10G** • zur Erfassung und verschlüsselten Übertragung Daten mit 10 GB • Abfrage der Log Daten von Endpoints, Firewall, Server, Switches etc. • Überwachung von Netzwerkverkehr Layer 2-7 (Verbindungen, Protokolle, verdächtige Muster) • Aufbewahrung der Log Daten für 90 Tage ohne Kapazitätsbeschränkung	2	St/J		

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System
1 Managed Detection und Response

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.		Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre
1.1.9	**Dienstleistung Inbetriebnahme** • Workshop zum Projektkickoff • Workshop zur technischen Inbetriebnahme mit den Fach Ansprechpartnern • Inbetriebnahme physischer Appliances vor Ort • Installation und Konfiguration der einzelnen Sensoren/Agenten • Überprüfung und Konfiguration/Erfassung der Log-Quellen, Firewalls, AD, Endgeräte etc. • Anbindung an Cloud Plattform • Bereitstellen Zugänge zur Cloud Plattform • Einrichtung der verschlüsselten Übertragung ins Rechenzentrum unter Beachtung der Lastverteilung • Festlegung des Log Speicher Zyklus • Generierung von Workflows für Client und virtuelle Server Systeme zur Definition der Vorgehensweise bei Incidents • Schulung der Administratoren • Festlegung der mind. Quartalsweisen Workshops (siehe Lastenheft) • Anpassungen nach Kundenwunsch • Testbetrieb vor Go-Live • Anpassungen vor Go-Live • Go-Live		1	psch	_____	_____
1.1.10	**Versandkosten Hardware**		1	psch	_____	_____
	Eventualpos. ohne GP					
1.1.11	**Aufpreis erweiterte Speicherung Log Daten von 90 Tagen auf 180 Tage** • Aufbewahrung der Log Daten für 180 Tage ohne Kapazitätsbeschränkung		1	St/J	_____	**NEP**
	Eventualpos. ohne GP					
1.1.12	**Aufpreis erweiterte Speicherung Log Daten von 90 Tagen auf 365 Tage** • Aufbewahrung der Log Daten für 365 Tage ohne Kapazitätsbeschränkung		1	St/J	_____	**NEP**
1.1	**Managed Detection und Response**			**Summe:**		_____

LEISTUNGSVERZEICHNIS

Projekt: 25003 Klinikum Mittelbaden - SIEM
1 SiEM & SOC System
2 Security Awareness

Ausgabeumfang: Alle Positionen

OZ / Pos.-Nr.		Menge	Einheit	Einheitspreis (pro Jahr)	Gesamtbetrag 3 Jahre
1.2	**Security Awareness**				
	Laufzeit/Preis Die kalkulierte Laufzeit beträgt 3 Jahre Bitte geben Sie wie folgt an: Einheitspreis = jährlicher Preis Gesamtbetrag = Jahrespreis x Laufzeit				
	Eventualpos. mit GP				
1.2.1	**Security Awareness je User** • Mitarbeitereinbindung/Schulung • regelmäßig simulierte Phishing Attacken • Auswertungen über Mitarbeiterkenntnisee hinsichtlich Trainingsstand • Auswertung zu den Phishing Attacken • Auswertung der Probleme • kontinuirliche Weiterbildung	3000	St/J	_____	_____
	Eventualpos. mit GP				
1.2.2	**Dienstleistung Inbetriebnahme** • Erfassung der Mitarbeiter • Vorbereitung der Maßnahmen • Umsetzung	1	psch	_____	_____
1.2	**Security Awareness**			**Summe:**	_____

LEISTUNGSVERZEICHNIS

Projekt:	25003	Klinikum Mittelbaden - SIEM
	1	SiEM & SOC System

Ausgabeumfang:	Alle Positionen	Gesamtbetrag
OZ		in EUR

Zusammenstellung

1.1	Managed Detection und Response	
1.2	Security Awareness	
1	Summe	
	+ 19 % MwSt.	
	Bruttosumme SiEM & SOC System	