

Ausschreibung eines Managed Security Operations Center (SOC) an der Universität zu Lübeck

Feld	Angabe
Dokumententyp	Leistungsbeschreibung / Leistungsverzeichnis
Auftraggeber	Universität zu Lübeck (nachfolgend „Auftraggeber“ oder „UzL“)
Vergabestelle	Referat IV/1/500 Finanzen/Controlling/Einkauf
Vergabenummer / Verfahrenskennung	20260653 / Managed Security Operations Center (SOC) und Cisco Security Enterprise Agreement
Verfahrensart	Offenes Verfahren
Version	2.0
Stand	04.08.2026
Vertragslaufzeit	60 Monate
Verbindliche Verfahrenssprache	Deutsch

Inhaltsverzeichnis

1	Allgemeine Angaben	3
1.1	Auftraggeber und Vergabestelle	3
1.2	Gegenstand und Zweck des Verfahrens.....	3
2	Ausgangslage und Zielsetzung.....	3
2.1	Ausgangslage.....	3
2.2	Zielsetzung	4
2.3	Bestehende Systemlandschaft (Serviceobjekt)	4
2.4	Zielarchitektur (Mengengerüst)	5
2.5	Bestandsbezogenheit und Investitionsschutz.....	5
3	Gegenstand der Leistung.....	6
3.1	Leistungsumfang im Überblick.....	6
3.2	Lizenzbeschaffung, -verlängerung und Pflege	7
3.3	Zusätzlich zu erbringende Fähigkeiten.....	7
3.4	Nicht Gegenstand der Leistung	8
4	Leistungserbringung und Service Level Agreements	9
4.1	Service Level Agreements (SLAs).....	9
4.2	Serviceverfügbarkeit	9
4.3	Reaktions- und Lösungszeiten.....	9
4.4	Sprache und Serviceort	9
4.5	Servicebereiche	10
4.5.1	Service Design & Transition	10
4.5.2	Lizenzmanagement – SOC-Produkte.....	11
4.6	Service Operation.....	11
4.6.1	Vorfallerkennung (Detection)- Cisco XDR	11
4.6.2	Incident Response - Automatisierte Workflows	11
4.6.3	Threat Hunting & Threat Intelligence	12
4.6.4	Monitoring, Reporting und Steuerung.....	12
4.7	Continual Service Improvement (CSI)	13
5	Schnittstellen und Rollen.....	14
5.1	Grundsätze der Zusammenarbeit	14
5.2	Zusammenarbeit	14
5.3	Halbjährliches Service-Recap und Innovationsworkshop	15
6	Leistungsfähigkeit des Anbieters.....	15
7	Ergänzende Regelungen	16
7.1	Datenschutz und Auftragsverarbeitung	16
7.2	Erweiterte Wiederherstellungsunterstützung (optionale Abrufleistung).....	16

1 Allgemeine Angaben

1.1 Auftraggeber und Vergabestelle

Auftraggeber ist die Universität zu Lübeck (nachfolgend „Auftraggeber“ oder „UzL“). Die Universität zu Lübeck ist eine Stiftung des öffentlichen Rechts.

1.2 Gegenstand und Zweck des Verfahrens

Gegenstand dieses Verfahrens ist die Erbringung eines Managed Security Operations Center (nachfolgend „Managed SOC“) als Dienstleistung, einschließlich der Bereitstellung, Verlängerung und Pflege von erforderlichen Softwarelizenzen. Der zu beschaffende Lizenzumfang ergibt sich abschließend aus dem Mengengerüst in Kapitel 2.4.

Es handelt sich um einen gemischten Auftrag aus Dienstleistungs- und Lieferanteilen. Der Lizenzanteil ist dieser Dienstleistung funktional zugeordnet.

Zweck des Verfahrens ist die Sicherstellung eines durchgehend (24 Stunden an 7 Tagen der Woche einschließlich Sonn- und Feiertagen) betriebenen Sicherheitsbetriebs mit definierten Reaktions- und Lösungszeiten.

2 Ausgangslage und Zielsetzung

2.1 Ausgangslage

Der Auftraggeber entwickelt seine Informationssicherheit kontinuierlich weiter, insbesondere auch im Bereich der Cyberresilienz. Cyberresilienz bezeichnet die Widerstandsfähigkeit der IT-Systeme im Zusammenspiel von Prävention, Detektion und Reaktion.

Angeichts der zunehmenden Bedrohungslage durch Advanced Persistent Threats (APT), Ransomware und staatlich unterstützte Angriffe ist die Weiterentwicklung eines durchgehenden Überwachungs- und Reaktionssystems erforderlich. Der Auftraggeber begegnet diesen Herausforderungen mit einer zentralen Sicht und Orchestrierung.

Der Auftraggeber hat daher ein Managed Security Operations Center eingeführt. Ein Security Operations Center ist eine organisatorische Einheit, in der qualifiziertes Personal sicherheitsrelevante Informationen aus verschiedenen Quellen zusammenführt, analysiert und bewertet, um Bedrohungen und Sicherheitsvorfälle zu erkennen, einzuordnen und zu beantworten. Hierzu werden Technologien wie Security Information and Event Management (SIEM), Systeme zur Angriffserkennung und -abwehr (IDS/IPS), Endpoint beziehungsweise Extended Detection and Response (EDR/XDR) sowie forensische Werkzeuge eingesetzt.

Daten aus Netzwerkverkehr, Protokolldateien und Nutzungsverhalten werden erhoben, aggregiert und korreliert. Verdächtige Aktivitäten werden identifiziert und Angriffe blockiert, eingegrenzt und beseitigt. Den Betrieb dieser Systeme kann der Auftraggeber weder personell noch wirtschaftlich 7x24x365 in Eigenleistung sicherstellen. Die Leistung wird daher extern beschafft.

2.2 Zielsetzung

Mit der ausgeschriebenen Leistung verfolgt der Auftraggeber folgende Ziele:

- durchgehender Betrieb der Detektions- und Reaktionsfähigkeit mit einem SLA von 24x7x365 Tagen im Jahr
- vollständige Nutzung der bereits getätigten Lizenzinvestitionen (Investitionsschutz)
- Erweiterung der Erkennungstiefe um Endpunkt-, Netzwerk-, E-Mail- und Identitäts-Telemetrie durch automatische Korrelation der bestehenden Systeme
- Aufbau- und Wissenstransfer an die IT-Organisation des Auftraggebers

2.3 Bestehende Systemlandschaft (Serviceobjekt)

Der Auftraggeber betreibt eine Sicherheitsplattform mit den folgenden Bestandskomponenten:

- Cisco XDR (Extended Detection & Response) - zentrale Korrelations- und Analyseplattform inkl. Response-Instanz
- Cisco Secure Endpoint - Gewährleistung des Endpunktschutzes und der EDR-Funktionalität
- Cisco Duo - Zero-Trust-Plattform, Multifaktor-Authentifizierung und -verwaltung
- Cisco Umbrella - DNS-Sicherheit
- Cisco Secure Email Gateway - E-Mail-Sicherheit
- Cisco ISE - Sicherheitsplattform für das Netzwerkmanagement
- Tenable - Schwachstellenmanagement und Scanning
- Splunk Enterprise - Log Management

Der Auftragnehmer erbringt zukünftig die Leistung auf Basis der unter Ziffer 2.4. genannten Zielarchitektur. Hierzu gehören die erforderliche Anpassung, Aktualisierung und Weiterentwicklung der bestehenden Komponenten sowie die Integration der in Ziffer 2.4 zusätzlich vorgesehenen Komponenten und Funktionalitäten. Die in Ziffer 2.4 ausgewiesene Zielarchitektur bildet den für die Leistungserbringung maßgeblichen technischen und mengenmäßigen Zielzustand.

Eine Ablösung oder Ersetzung dieser Komponenten durch Produkte anderer Hersteller ist nicht Gegenstand dieses Verfahrens.

Der Einsatz ergänzender Werkzeuge des Auftragnehmers (zum Beispiel für Ticketing, Automatisierung, Reporting oder ergänzende Bedrohungsdaten) ist zulässig, sofern Interoperabilität, Datenschutzkonformität und Auditierbarkeit gewahrt bleiben und dem Auftraggeber hierdurch keine zusätzlichen Kosten entstehen.

2.4 Zielarchitektur (Mengengerüst)

Die nachstehenden Angaben zum Mengengerüst der Zielarchitektur sind Grundlage der Kalkulation.

Pos.	Komponente	Lizenzmetrik	Anzahl / Volumen	Laufzeitende der Be- standslicenz
1	Cisco XDR Advantage	Nutzende	2000	[31.10.2026]
2	Secure Network Analytics	Flow Rate	4000	[31.10.2026]
3a	Cisco Secure Endpoint Education Student Adv	Endpunkte	5	[31.10.2026]
3b	Cisco Secure Endpoint Education Faculty Adv	Endpunkte	2000	[31.10.2026]
4	Cisco Duo Advantage for Education Faculty	Nutzende	10300	[31.10.2026]
5a	Cisco Secure Access DNS EDU Essentials	Nutzende	2000	[31.10.2026]
5b	Cisco Support Std. for Sec Acc EDU Ess - SPA Ess		1	[31.10.2026]
6	Cisco Secure Email Essential	Postfächer	2600	[31.10.2026]
7	Cisco Secure SMA Centralized Email Management	Postfächer	2600	[31.10.2026]
8	Cisco ISE Essentials	Endpunkte	4000	[31.10.2026]
9	Secure Client Premier		6000	[31.10.2026]
10	Splunk On-Prem Enterprise	Datenvolumen pro Tag (GB)	256 GB	[31.10.2026]
11	Splunk On-Prem Enterprise Security Essential	Datenvolumen pro Tag (GB)	150 GB	[31.10.2026]
12	Tenable One Foundation	Assets	3000	[31.10.2026]

2.5 Bestandsbezogenheit und Investitionsschutz

Gegenstand der Ausschreibung ist der Betrieb, die Verwaltung und die Weiterentwicklung der bereits produktiv eingesetzten Sicherheitsplattform. Die Ausschreibung dient nicht der Auswahl oder Einführung einer neuen Technologie, sondern der Sicherstellung des kontinuierlichen Betriebs der vorhandenen Systemlandschaft.

Der wesentliche Investitionswert liegt nicht in den Restlaufzeiten der bestehenden Lizenzen, sondern in den innerhalb der Plattform aufgebauten und validierten Konfigurationsständen. Hierzu zählen insbesondere Korrelationsregeln, Playbooks, Automatisierungen, Systemintegrationen, Datenmodelle, Anlernstände sowie etablierte Betriebs-, Monitoring-, Troubleshooting- und Incident-Response-Prozesse. Diese Werte bestehen über die jeweilige Lizenzlaufzeit hinaus und bilden die Grundlage für die Funktions- und Reaktionsfähigkeit des laufenden Sicherheitsbetriebs.

Die bestehende Sicherheitsarchitektur verbindet Cisco XDR als übergeordnete Managementplattform mit Cisco Secure Endpoint, Cisco Duo, Cisco Umbrella, Cisco Secure E-Mail Gateway, Cisco ISE, Tenable sowie mit Splunk Enterprise. Die erforderlichen Schnittstellen sind eingerichtet und aktiv. Die Systeme ermöglichen eine übergreifende Korrelation sicherheitsrelevanter Informationen sowie automatisierte Abläufe bei der Bearbeitung und Eindämmung von Bedrohungen.

Eine alternative Plattform wäre nur dann tatsächlich gleichwertig, wenn sie diese vollständige Integrations- und Prozesskette abbilden könnte. Hierfür müssten die Verfügbarkeit geeigneter Schnittstellen geprüft, sämtliche Anbindungen neu umgesetzt sowie Datenmodelle, Korrelationsregeln, Playbooks, Automatisierungen und Betriebsprozesse neu aufgebaut, getestet und validiert werden. Auch bei Nutzung standardisierter APIs wäre jede Integration plattformspezifisch anzupassen.

Während einer solchen Migration bestünde das Risiko einer eingeschränkten Erkennungs- und Reaktionsfähigkeit. Ein Parallelbetrieb würde dieses Risiko nicht vollständig beseitigen, da zusätzliche Schnittstellen und parallele Betriebswege entstünden. Bis zur vollständigen Übernahme und Validierung aller Funktionen wäre keine durchgehend einheitliche Sicht auf die Bedrohungslage gewährleistet.

Ein Plattformwechsel wäre daher kein einfacher Produktaustausch, sondern ein Neuaufbau wesentlicher Teile der produktiven Sicherheitsarchitektur. Dies würde zusätzliche Aufwände für Planung, Migration, Integration, Implementierung, Tests, Validierung, Schulung und Übergangsbetrieb verursachen.

Die Fortführung der bestehenden Plattform ist somit technisch und wirtschaftlich erforderlich, um die vorhandenen Konfigurations- und Integrationswerte zu erhalten, die Interoperabilität der eingesetzten Komponenten sicherzustellen und den sicheren sowie kontinuierlichen Betrieb der Sicherheitsarchitektur ohne Einschränkung der Erkennungs- und Reaktionsfähigkeit zu gewährleisten.

3 Gegenstand der Leistung

3.1 Leistungsumfang im Überblick

Der Auftragnehmer erbringt über die gesamte Vertragslaufzeit ein Managed SOC („Security Operation Center as a Service“) auf Basis der genannten Bestandsplattform, gemäß den nachstehend aufgeführten Leistungsbestandteilen.

Er nutzt die Fähigkeiten der bestehenden Plattform und Systemarchitektur im vorgenannten Umfang (Zielarchitektur) und integriert diese sowie zukünftig zu beschaffenden Fähigkeiten in ein proaktives, rund um die Uhr (24x7x365) arbeitendes SOC-Betriebsmodell.

Der Auftragnehmer setzt die Kernprinzipien Defense-in-Depth, Zero-Trust-Kompatibilität, Privacy-by-Design und Auditierbarkeit innerhalb der nativen Funktionen der bestehenden SOC-Plattform und Systemarchitektur um.

Es muss eine Vertragslaufzeit von 60 Monaten angeboten werden bei jährlicher Zahlweise (s. Preisblatt).

Der Auftragnehmer erbringt den SOC-Service mit einem SLA von 24x7x365 (Details siehe Anlage A_Kriterienkatalog) und erfüllt die Anforderungen.

Der Leistungsumfang umfasst:

- Aufnahme der Assets und der Alarmierungsprozesse im Rahmen des Onboardings
- Konfiguration, Pflege und kontinuierliche Optimierung sämtlicher in Kapitel 2.4 genannter

Komponenten der Zielarchitektur

- Betrieb der XDR-Plattform als zentrale Datenbasis und Orchestrierungsschicht des SOC
- Proaktive Überwachung, Analyse und Bewertung sicherheitsrelevanter Ereignisse im 24x7x365-Betrieb sowie die mit dem Auftraggeber abgestimmte Reaktion auf Sicherheitsvorfälle
- Beschaffung und Pflege der für den Betrieb erforderlichen Lizenzen
- Integration weiterer Systemquellen des Auftraggebers in die bestehende Plattform und Systemarchitektur sowie Integration der in Kapitel 3.3 genannten zusätzlichen Fähigkeiten
- Regelmäßige, automatisierte Schwachstellenanalyse der IT-Landschaft der Universität zu Lübeck: 4 Schwachstellenscans pro Monat, 1 Report pro Woche, Priorisierung der festgestellten Schwachstellen sowie ein Auswertungsgespräch mit der Universität zu Lübeck zur Behebung
- Berichtswesen, Teilnahme an Steuerungsgremien und kontinuierliche Serviceverbesserung.

3.2 Lizenzbeschaffung, -verlängerung und Pflege

Der Lizenzumfang wird wie folgt geregelt:

- Alle Lizenzen des Mengengerüsts 2.4 inkl. Renewals und Support sind Bestandteil der Grundvergütung bzw. der Lizenzpositionen des Preisblatts.
- Bei EOL/EOS schuldet der AN die Umstellung auf das funktionale Nachfolgeprodukt desselben Herstellers zu den vereinbarten Konditionen; Mehrkosten reiner Programmumbenennungen gehen nicht zulasten des Auftraggebers
- Herstellerwechsel ist nicht Vertragsgegenstand (Ziffer 2.5).
- Die Beschaffung höherwertiger Lizenzstufen oder zusätzlicher Produkte, die über das Mengengerüst nach Kapitel 2.4 hinausgeht, ist nicht Gegenstand dieses Vertrags. Dem Bieter steht es frei, die geforderten Lizenzen im Wege einer gebündelten Lizenzierung (z. B. über ein Enterprise-Agreement-Modell) anzubieten, sofern der geforderte Leistungsumfang vollständig abgedeckt und die Preisbildung transparent und nachvollziehbar dargestellt wird.
- Die Lizenzen sind über vom jeweiligen Hersteller autorisierte Vertriebswege zu beziehen und auf den Auftraggeber als Endkunden zu registrieren. Der Auftragnehmer weist Bezugsberechtigung und Laufzeit auf Verlangen nach.

3.3 Zusätzlich zu erbringende Fähigkeiten

Die nachstehenden Fähigkeiten sind ergänzend zum Bestand bereitzustellen. Die Anforderungen sind funktional zu verstehen; die Auswahl der Lösung zur Umsetzung obliegt dem Bieter. Soweit eine Bestandskomponente die Anforderung bereits abdeckt, ist dies im Angebot darzustellen. Eine Doppelbeschaffung ist nicht erwünscht.

- Analyse von Netzwerkdatenströmen auf Basis von Flussdaten (zum Beispiel NetFlow, IPFIX) zur Erkennung anomalen Netzwerkverhaltens, einschließlich der Anbindung an die bestehende Plattform
- Erweiterte, verhaltensbasierte Erkennung und Abwehr von Phishing-, Malware- und Spoofing-Angriffen im E-Mail-Verkehr, die über den Funktionsumfang der bestehenden E-Mail-Sicherheitslösung hinausgeht

- Erweiterte Detektions- und Schutzfunktionalität mit SIEM-Charakteristik für Dienste, die durch die Bestandskomponenten nicht abgedeckt sind, insbesondere Verzeichnisdienste (Microsoft Active Directory beziehungsweise Entra ID) und Virtualisierungsplattformen (zum Beispiel Nutanix, VMware vCenter). Der Bieter stellt dar, in welchem Umfang hierfür die vorhandene Protokollhaltung genutzt wird
- Absicherung des Internetzugriffs und der Web-Kommunikation über ein Secure Internet Gateway, soweit über die vorhandene DNS-Sicherheitslösung hinausgehend
- Erkennung sicherheitsrelevanter Ereignisse in genutzten Cloud-Diensten (Microsoft 365 und weitere nach Angabe des Auftraggebers)

3.4 Nicht Gegenstand der Leistung

Zur Abgrenzung des Leistungsumfangs sind die folgenden Leistungen ausdrücklich nicht Gegenstand dieses Vertrags:

- Der Betrieb der allgemeinen IT-Infrastruktur des Auftraggebers (Administration, Patch- und Release-Management von Clients, Servern, Netzwerk, Verzeichnisdiensten, Anwendungen) ist nicht Gegenstand der Leistung. Hiervon unberührt bleibt die sicherheitsseitige Überwachung dieser Systeme (Einbindung der Protokoll- und Telemetriedaten, Detektion, Alarmierung) nach Ziffer 3.3.
- Die Behebung von Schwachstellen in Systemen des Auftraggebers, soweit sie nicht über die im Rahmen dieses Vertrags betriebenen Sicherheitskomponenten erfolgen kann; der Auftragnehmer beschränkt sich insoweit auf Priorisierung, Handlungsempfehlung und Nachverfolgung
- Forensische Gutachten für gerichtliche Zwecke sowie Verhandlungen mit Angreifern; diese können gesondert beauftragt werden
- Die Erbringung von Leistungen im Rahmen der Arbeitnehmerüberlassung

4 Leistungserbringung und Service Level Agreements

4.1 Service Level Agreements (SLAs)

Es gelten die in Anlage A_Kriterienkatalog definierten Serviceverfügbarkeit, Reaktions- und Lösungszeiten sowie die dort geregelten Alarmierungspflichten. Die SLA-Messung erfolgt auf Basis vollständiger Kalendertage.

4.2 Serviceverfügbarkeit

Der Service ist an 24 Stunden pro Tag und 7 Tagen pro Woche einschließlich Sonn- und gesetzlicher Feiertage verfügbar.

Details sind der Anlage A_Kriterienkatalog zu entnehmen.

4.3 Reaktions- und Lösungszeiten

Die nachstehend definierten Zeiten sind als verbindliche Fristen ab dem Eintritt des Sicherheitsvorfalls zu verstehen. Als Zeitpunkt des Eintritts gilt der Zeitpunkt der automatisierten Erkennung durch die Cisco XDR-Plattform.

Priorität	Reaktionszeit	Lösungszeit (Handlungsempfehlung)
Prio 1 (Kritisch)	15 Minuten (24x7)	2 Stunden
Prio 2 (Hoch)	30 Minuten (24x7)	4 Stunden
Prio 3 (Mittel)	2 Stunden (Mo-Fr 08 – 18 Uhr)	12 Stunden (Mo-Fr 08 – 18 Uhr)
Prio 4 (Niedrig)	24 Stunden (Mo-Fr 08 – 18 Uhr)	–

**Details sind in der Anlage A_Kriterienkatalog zu entnehmen*

4.4 Sprache und Serviceort

Für die Erbringung der Leistungen gelten folgende verbindliche Vorgaben hinsichtlich der Kommunikationssprache und des geografischen Leistungsorts:

- **Vertragssprache**

Die Vertragssprache ist Deutsch, im operativen Betrieb sowie für die vom Bieter eigenständig erstellten technischen Dokumentationen. Die deutsche Vertragssprache ist erforderlich, da der operative Betrieb eng mit den überwiegend deutschsprachigen Fachbereichen und der IT-Organisation des Auftraggebers abgestimmt werden muss, um sicherheitskritische Meldungen ohne Zeitverlust verständlich zu

kommunizieren. Das mit der Kommunikation zum Auftraggeber betraute Personal (insbesondere Service Manager/SPOC sowie die Ansprechpartner für Vorfälle der Prioritätsstufen 1 und 2) verfügt über Deutschkenntnisse von mindestens Niveau C1 des Gemeinsamen Europäischen Referenzrahmens für Sprachen (GER). Für die übrigen im SOC eingesetzten Fachkräfte sind Deutschkenntnisse erforderlich, die eine reibungslose technische Zusammenarbeit und das Verständnis sicherheitsrelevanter Dokumentation gewährleisten.

- **Berichterstattung**

Alle anzufertigenden Berichte, Handlungsempfehlungen sowie SLA-Dokumente sind in deutscher Sprache abzufassen und dem Auftraggeber bereitzustellen.

- **Serviceort**

Die Dienstleistung wird primär im Remote-Betrieb oder in den Räumlichkeiten des Auftragnehmers erbracht. Ein physischer Zugang zum Standort des Auftraggebers ist bei Bedarf oder auf explizite Anforderung des Auftraggebers zu gewährleisten. Der Auftraggeber stellt keine Räumlichkeiten zur Verfügung. Tätigkeiten im Rahmen des Arbeitnehmerüberlassungsgesetzes (AÜG) sind nicht vorgesehen.

- **Rechenzentrumsstandorte**

Im SOC-Betrieb werden fortlaufend personenbezogene Daten von Studierenden und Beschäftigten verarbeitet, darunter Identitäts-, Anmelde-, Netzwerk- und Kommunikationsmetadaten in erheblichem Umfang. Diese Daten erlauben detaillierte Verhaltensprofile und betreffen die Funktionsfähigkeit der Sicherheitsinfrastruktur des Auftraggebers. Eine Verarbeitung in Drittländern würde zusätzliche Übermittlungs- und Zugriffsrisiken (Art. 44 ff. DSGVO) begründen, die der Auftraggeber angesichts der Sensibilität der Daten und seiner Stellung als öffentliche Einrichtung nicht eingeht. Sämtliche Verarbeitungsprozesse und Rechenzentrumsstandorte haben daher innerhalb der EU zu liegen.

4.5 Servicebereiche

Der Auftragnehmer hat folgende Kernleistungen auf Basis der in Kapitel 2.4 beschriebenen Zielarchitektur des Auftraggebers zu erbringen. Die in diesem Kapitel sowie in den nachfolgenden Kapiteln 4.6 und 4.7 beschriebenen Servicebereiche und Leistungsanforderungen sind dabei entsprechend den Vorgaben und Servicebereichen gemäß Kapitel 2.5 zu berücksichtigen. Für jeden Leistungsbereich sind das Leistungsziel (Was), die technische Umsetzungsmethode auf der Plattform und Systemarchitektur (Wie) sowie der daraus resultierende Mehrwert für den Auftraggeber (Nutzen) gemäß der Normativen Referenz wie folgt zu definieren:

4.5.1 Service Design & Transition

Was: Aufbau eines qualitätsgesicherten Betriebsmodells und Optimierung der bestehenden Architektur für den Produktivbetrieb.

Wie: Der Auftragnehmer analysiert die vorhandene Cisco-Lizenz- und Konfigurationssituation, erstellt ein Optimierungskonzept und verbessert den Betriebszustand.

Nutzen: Der Auftraggeber erhält ein vollständig betriebsbereites, dokumentiertes SOC-Stack mit klarer Verantwortungszuordnung. Die vorhandenen Lizenzen werden von Beginn an vollständig genutzt.

Normative Referenz: ISO/IEC 27001:2022 (Anhang A.8.1, A.13.1); ITIL 4 (Service Design Practice); BSI IT-Grundschutz ORP.2

4.5.2 Lizenzmanagement – SOC-Produkte

Was: Kontinuierliche Überwachung von Lizenzstatus und End-of-Life-Situationen aller inventarisierten Komponenten im Rahmen der SOC-Plattform.

Wie: Der Auftragnehmer überwacht kontinuierlich die Lizenzlaufzeiten sowie EOL-/EOS-Ankündigungen für alle lizenzierten SOC-Produkte. Lizenz-Renewals werden rechtzeitig (mind. 90 Tage vor Ablauf) kommuniziert und in Abstimmung mit dem Auftraggeber initiiert. Die Beschaffung zusätzlicher oder höherwertiger Lizenzen ist nicht Gegenstand dieses Vertrags und erfolgt bei Bedarf gesondert. Patch- und Release-Management der SOC-Komponenten sowie der Betrieb der IT-Infrastruktur (Clients, Netzwerk, Server, etc.) erfolgen durch den Auftraggeber.

Nutzen: Keine ungenutzten oder abgelaufenen Lizenzen; frühzeitige Planungssicherheit bei Vertragsverlängerungen; keine Betriebsunterbrechungen durch überraschende Laufzeitenden.

Normative Referenz: ITIL 4 (Service Level Management); BSI IT-Grundschutz OPS.1.1.3

4.6 Service Operation

4.6.1 Vorfallerkennung (Detection)-Cisco XDR

Was: Automatisierte Erkennung von Sicherheitsvorfällen durch die Cisco XDR-Plattform inkl. plattformseitiger False-Positive-Filterung und Priorisierung.

Wie: Der Auftragnehmer betreibt und optimiert kontinuierlich die Cisco XDR-Korrelationsregeln, Playbooks und Automatisierungen. Security-Events aus Cisco Secure Endpoint, Secure Network Analytics, Secure Access und Secure Email Threat Defense werden in Echtzeit in Cisco XDR aggregiert, normalisiert und bewertet. Zusätzliche Datenquellen (z. B. Cloud-Dienste) sind über Cisco XDR-native Integrationen eingebunden. Erkannte Ereignisse werden nach Prio 1–4 klassifiziert und an das Ticketsystem des Auftraggebers gemeldet.

Nutzen: Drastische Reduzierung der Mean Time to Detect (MTTD) durch native Cisco XDR-Telemetrie; lückenloser 24/7-Schutz ohne personellen Mehraufwand beim Auftraggeber; optimale Ausnutzung der erworbenen Cisco-Lizenzen.

Normative Referenz: ISO/IEC 27035-2:2023; NIST SP 800-94 (IDPS); BSI BSI-CS 134

4.6.2 Incident Response - Automatisierte Workflows

Was: Definition von Handlungsempfehlungen und Bereitstellung automatisierter Cisco XDR Response-Workflows zur proaktiven Gefahreneindämmung.

Wie: Für jede Prioritätsklasse werden Cisco XDR Response-Workflows mit dem Auftraggeber abgestimmt, konfiguriert und betrieben, die dann automatisiert ausgelöst werden. Automatisierte Maßnahmen umfassen Cisco Secure Endpoint-Isolierung, Cisco Secure Access Blockierungen (DNS/IP), Cisco Secure Firewall-Regeln sowie Konto-Deaktivierungen via IDM/AD-Integration. Für komplexe Vorfälle bereitet der Auftragnehmer strukturierte Handlungsempfehlungen vor und stellt diese innerhalb der vereinbarten Lösungszeit bereit.

Umfang und Eingriffstiefe automatisierter Response-Maßnahmen werden im Onboarding je Maßnahmen-typ schriftlich vereinbart (Rules-of-Engagement Dokument). Ohne Einzelfreigabe zulässig sind reversible Eindämmungsmaßnahmen nach abgestimmten Playbooks (insbesondere Endpoint-Isolierung, DNS-/IP-Blockierung). Eingriffsintensive Maßnahmen (insbesondere Konto-Deaktivierungen, Firewall-Regeländerungen) sind nur nach Freigabe durch den AG oder auf Grundlage einer in der Freigabematrix (Rules-of-Engagement Dokument) ausdrücklich erteilten Vorab-Autorisierung zulässig. Jede automatisierte Maßnahme wird protokolliert und im Servicebericht ausgewiesen.

Nutzen: Minimierung des Schadenspotenzials durch sofortige Eindämmung mit vorhandenen Cisco-Werkzeugen; vollständige Dokumentation für forensische Zwecke und regulatorische Meldepflichten (NIS2 Art. 23, DSGVO Art. 33).

Normative Referenz: NIST SP 800-61 Rev. 2; ISO/IEC 27035-3:2020; BSI IT-Grundschutz DER.2.1

4.6.3 Threat Hunting & Threat Intelligence

Was: Gezielte Suche nach Bedrohungen auf Basis aktueller Cisco Talos-Veröffentlichungen sowie Nutzung der in Cisco XDR integrierten Threat-Intelligence-Feeds, ergänzt um Log-Korrelation in Splunk Enterprise Security und Expositionsbeurteilung in Tenable.

Wie: Das Team des Auftragnehmers wertet relevante Cisco Talos Blog-Posts und Advisories aus und leitet daraus gezielte Hunting-Hypothesen ab. Diese werden mit den nativen Hunting-Funktionen von Cisco XDR sowie Cisco Secure Endpoint überprüft. Zusätzlich werden auf Basis derselben Talos-Erkenntnisse (TTPs, IOCs) entsprechende Suchabfragen (SPL) in Splunk Enterprise Security gegen die dort aggregierten Log-Quellen ausgeführt, um Indikatoren auch außerhalb der Cisco-Telemetrie zu identifizieren. Sofern Talos-Advisories konkrete CVEs referenzieren, erfolgt ein Abgleich mit der Asset- und Schwachstellenbasis in Tenable, um die tatsächliche Exposition betroffener Systeme im Kundenumfeld zu bewerten. Grundlage der Bedrohungserkennung sind ausschließlich die integrierten Threat-Intelligence-Feeds (Cisco Talos Intelligence) sowie die vorhandenen Bestandsdaten in Splunk ES und Tenable. Eine Anbindung zusätzlicher externer Feeds ist nicht Bestandteil dieser Leistung.

Nutzen: Frühzeitige Erkennung aktueller Bedrohungen auf Basis praxisnaher Talos-Erkenntnisse. Ganzheitliche Bewertung über Netzwerk-/Endpoint-Ebene (Cisco), Log-Korrelation (Splunk ES) und Schwachstellenexposition (Tenable). Maximaler Nutzen der bereits lizenzierten Cisco Talos-Subscription sowie der vorhandenen SIEM- und Exposure-Management-Plattformen ohne zusätzlichen Integrationsaufwand. Strategische Risikoinformation für das Management.

Normative Referenz: MITRE ATT&CK Framework (aktuelle Version); ISO/IEC 27002:2022 (Kontrolle 5.7)

4.6.4 Monitoring, Reporting und Steuerung

Was: Regelmäßiges Reporting aus der vorhandenen SOC-Plattform heraus, Teilnahme an Steuerungsgremien und Besetzung definierter Rollen im Serviceprozess in Form von wöchentlichen Kurz-Jour-fixes.

Wie: Der Auftragnehmer erstellt monatliche Service-Reports, die mindestens folgende Inhalte umfassen: SLA-Kennzahlen je Prioritätsstufe, Mean Time to Acknowledge (MTTA), Mean Time to Resolve (MTTR), False-Positive-Rate sowie eine Trendanalyse auf Basis der nativen Cisco-XDR-Daten. Alle Berichte werden in deutscher Sprache erstellt. Änderungen im Rahmen des CSI-Prozesses sind auf die Ergänzung einzelner

Kennzahlen und die Anpassung der Darstellung beschränkt und mit der Grundvergütung abgegolten. Zusätzliche Berichtsformate, neue Gremien oder eine erhöhte Berichtsfrequenz sind gesondert zu beauftragende Leistungen.

Nutzen: Vollständige Transparenz über den Sicherheitsstatus der SOC-Plattform; messbare SLA-Erfüllung; fundierte Entscheidungsgrundlage für künftige Cisco-Lizenz- und Sicherheitsinvestitionen.

Normative Referenz: ITIL 4 (Service Reporting); ISO/IEC 27001:2022 (Anhang A.5.35, A.5.36); DSGVO Art. 5 (Rechenschaftspflicht)

4.7 Continual Service Improvement (CSI)

Was: Kontinuierliche Verbesserung der vorhandenen SOC-Plattformkonfiguration und der Servicequalität durch formale Review-Prozesse und messbare Optimierungsmaßnahmen.

Wie: Service-Reviews im Rahmen der geforderten Service-Recap und Innovationsworkshops (siehe Kapitel 5.3) auf Basis definierter KPIs (MTTA, MTTR, False-Positive-Rate, SLA-Compliance-Rate). Identifizierte Optimierungsmaßnahmen – z. B. neue Cisco XDR-Korrelationsregeln, Policy-Anpassungen – werden in einem CSI-Register erfasst und priorisiert bearbeitet. Mit der Grundvergütung abgegolten sind Optimierungsmaßnahmen innerhalb der Bestandsplattform, insbesondere Pflege und Neuanlage von Korrelationsregeln und Playbooks sowie Policy-Anpassungen. Maßnahmen, die zusätzliche Lizenzen, Hardware oder darüber hinausgehende Datenquellen erfordern, werden als gesonderte Leistung zum Tagessatz des Preisblatts angeboten und vom AG beauftragt.

Nutzen: Nachhaltige Qualitätssteigerung; Nachweis kontinuierlicher Verbesserung gegenüber Regulatoren; proaktive Anpassung an neue Bedrohungslagen innerhalb der bestehenden Plattform und Systemarchitektur.

Normative Referenz: ITIL 4 (Continual Improvement Practice); ISO/IEC 27001:2022 (Kap. 10); ISO 9001:2015 (KVP)

5 Schnittstellen und Rollen

5.1 Grundsätze der Zusammenarbeit

Die Zusammenarbeit soll sich als ein kooperativer, vertrauensvoller Prozess zwischen Auftraggeber und Auftragnehmer gestalten.

5.2 Zusammenarbeit

Die Zusammenarbeit zwischen den Vertragspartnern erfolgt auf Basis der klar definierten RACI-Matrix (Responsible, Accountable, Consulted, Informed). Die primären Kommunikationswege sind wie folgt festgelegt:

- Das etablierte ITSM-Ticketsystem des Auftraggebers für die Dokumentation und Nachverfolgung von Anfragen
- Proaktive Push-Benachrichtigungen zur Information über relevante Systemereignisse
- Direkte telefonische Erreichbarkeit des Auftraggebers bei Vorfällen der Prioritätsstufe 1 (Prio 1) und Prioritätsstufe 2 (Prio 2)

Die Zuordnung der Rollen und Verantwortlichkeiten ist in der nachstehenden Tabelle definiert:

Partei	Rolle	Verantwortlichkeiten
Auftraggeber (AG)	Security-Owner	Strategische Entscheidungen, Lizenzgenehmigungen, Freigaben, Eskalationsmanagement, Vertragssteuerung
Auftraggeber (AG)	Support Coordination	Koordination interner Ressourcen, Kommunikation mit Fachbereichen
Auftragnehmer (AN)	Service Manager (SPOC)	Single Point of Contact, SLA-Monitoring, Service-Reporting, Lizenzmanagement, Review-Koordination
Auftragnehmer (AN)	Plattform Engineer	Administration, Konfiguration und Optimierung aller Komponenten
Auftragnehmer (AN)	SOC-Team	Detection, Analyse, Incident Response (Automation) & Threat Hunting
Extern	Cisco TAC / Account Team	Herstellersupport bei Plattform & Systemarchitektur Problemen sowie Lizenz-Support

5.3 Halbjährliches Service-Recap und Innovationsworkshop

Der Auftragnehmer führt zweimal je Kalenderjahr, jeweils zum Ende eines Kalenderhalbjahres, ein Service-Recap durch. Gegenstand ist die Rückschau auf die im abgelaufenen Halbjahr erbrachte Leistung auf Basis der Kennzahlen und der Serviceberichte.

Unmittelbar im Anschluss an jedes Service-Recap führt der Auftragnehmer einen Innovationsworkshop durch. Gegenstand sind Weiterentwicklungsthemen des Managed SOC sowie angrenzende, infrastrukturnahe Themen des Auftraggebers.

Service-Recap und Innovationsworkshop finden an einem gemeinsamen Termin mit einer Dauer von acht Stunden statt. Der Termin wird mindestens 20 Werktage im Voraus abgestimmt.

Veranstaltungsort sind vorrangig die Räumlichkeiten des Auftraggebers. Eine Durchführung als Videokonferenz ist zulässig, wenn der Auftraggeber dies verlangt oder ihr zustimmt. Die Entscheidung trifft der Auftraggeber.

Der Auftragnehmer stellt die Agenda mindestens 10 Werktage vor dem Termin bereit und übermittelt innerhalb von 10 Werktagen die gezeigten Inhalte.

Die Leistung ist mit dem monatlichen Festpreis abgegolten. Eine gesonderte Vergütung, auch für Vorbereitungs- und Reiseaufwand des Auftragnehmers, erfolgt nicht.

6 Leistungsfähigkeit des Anbieters

Der Auftraggeber verlangt gemäß § 46 VgV den Nachweis, dass der Bieter über die für den Betrieb der aus geschriebenen Leistungen erforderliche fachliche Leistungsfähigkeit verfügt. Bei der Beurteilung der fachlichen Leistungsfähigkeit kommt es auf die nachgewiesene technische Kompetenz, die Qualifikation des eingesetzten Personals, die einschlägige Projekterfahrung und die organisatorische Leistungsfähigkeit des Bieters an.

Der Bieter muss nachweisen, dass er über Erfahrung im Betrieb von XDR- oder EDR-Lösungen verfügt. Der Nachweis kann insbesondere erbracht werden durch einschlägige Herstellerqualifikationen, Personenzertifizierungen der für die Leistung vorgesehenen Fachkräfte oder sonstige geeignete Nachweise, aus denen die erforderliche fachliche Kompetenz hervorgeht.

Die Nachweise sind der Anlage A_Kriterienkatalog zu entnehmen.

Zusätzliche Qualitätsnachweise können bei der Beurteilung der fachlichen Leistungsfähigkeit berücksichtigt werden, soweit sie ein durch den Hersteller oder eine unabhängige Stelle überprüfbares Qualitätsniveau des angebotenen Managed Services belegen.

Hierzu zählen beispielsweise auditierte Managed-Service-Programme der Hersteller. Maßgeblich ist nicht die Bezeichnung des Programms, sondern der Nachweis, dass insbesondere Betriebsprozesse, Servicequalität, organisatorische Leistungsfähigkeit, Qualifikation des eingesetzten Personals sowie die technischen Voraussetzungen für den Betrieb vergleichbarer Managed Services überprüft wurden.

Die Anforderungen aus dem Kriterienkatalog stellen einen möglichen Nachweis dar. Gleichwertige Nachweise anderer Hersteller oder unabhängiger Prüfstellen werden in gleicher Weise berücksichtigt, sofern sie hinsichtlich des Inhalts, Prüfungsumfang und Aussagekraft vergleichbar sind.

7 Ergänzende Regelungen

7.1 Datenschutz und Auftragsverarbeitung

Da der Betrieb des Security Operations Centers (SOC) zwangsläufig die Verarbeitung personenbezogener Daten erfordert, wird der Auftragnehmer im Rahmen dieser Leistung als Auftragsverarbeiter tätig. Der Auftraggeber erwartet, dass der Auftragnehmer über die im Markt für professionelle SOC-Dienstleister üblichen datenschutzrechtlichen Grundlagen verfügt. Dies kann beispielsweise durch eine Zertifizierung nach ISO/IEC 27001 oder ein vergleichbares Managementsystem nachgewiesen werden. Dies umfasst insbesondere:

- **Auftragsverarbeitungsvertrag (AVV):** Der Auftragnehmer verpflichtet sich, vor Inbetriebnahme der Leistungen einen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO zu unterzeichnen.
- **Technische und Organisatorische Maßnahmen (TOMs):** Der Auftragnehmer legt vor Vertragschluss seine technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO verbindlich vor und passt sie auf den Betrieb der eingesetzten Plattformen und die Verarbeitung von Telemetriedaten an. Der Nachweis eines Informationssicherheits-Managementsystems (z. B. nach ISO/IEC 27001 oder gleichwertig) gilt als geeigneter Beleg des Sicherheitsniveaus.
- **Datenort:** Alle Verarbeitungsprozesse müssen innerhalb der Europäischen Union stattfinden, um die Vorgaben der DSGVO (insb. Art. 44 ff.) einzuhalten.

Sollten im Zuge der konkreten Umsetzung Anpassungen der TOMs erforderlich werden, erfolgt dies in enger Abstimmung mit dem Auftraggeber.

7.2 Erweiterte Wiederherstellungsunterstützung (optionale Abrufleistung)

Zur Unterstützung bei der Wiederherstellung von Systemen und Services, die von einem Sicherheitsvorfall betroffen sind, stellt der Auftragnehmer auf gesonderten Abruf des Auftraggebers qualifiziertes Personal gemäß dem Personalprofil "Senior Security Engineer" (Anforderungen siehe Preisblatt) bereit. Die Abrufleistung umfasst Wiederherstellungsarbeiten, die über die nach Ziffer 4.6.2 und den vereinbarten Service Levels geschuldete Eindämmung und Handlungsempfehlung hinausgehen. Der Abruf erfolgt in Textform. Forensische Gutachten für gerichtliche Zwecke sowie Verhandlungen mit Angreifern sind nach Ziffer 3.4 nicht Gegenstand der Leistung. Die Gesamtverantwortung für die IT-Systeme des Auftraggebers bleibt unberührt. Der Auftragnehmer wird unterstützend tätig.