

Verfahren: 65/26/12 - Einführung und der Betrieb EDR/XDR & Managed Security Operations Center (SOC)

LISTE DER ÖFFENTLICHEN NACHRICHTEN

Nr	Frage	Antwort	Gesendet
1	Sehr geehrte Vergabestelle, leider können wir die Anlage 1 und somit den Kriterienkatalog für den Teilnahmewettbewerb nicht ausfüllen (ab Position A3). Können Sie bitte ein bearbeitungsfähiges Dokument bereitstellen?	In der Anlage 1 Kriterienkatalog war leider eine Dateiüberprüfung aktiviert, diese ist nun entfernt. Die Datei wurde ausgetauscht.	19.05.2026 09:37:37
2	Können Sie bitte die Position A5 in Anlage 1 näher spezifizieren?	<p>Das Dokument „Anlage 1 - Kriterienkatalog TNW_NEU.xlsx“ ist fehlerhaft und wurde ausgetauscht.</p> <p>In der Excel „Anlage 1 - Kriterienkatalog TNW.xlsx“ steht im Blatt „Mindestkriterien“ in der Zeile zu „A5“ als Text ein „c5“.</p> <p>Dort sollte jedoch folgender Text anstatt dem „c5“ hinterlegt sein:</p> <p>Sämtliche im Rahmen der Leistungserbringung verarbeiteten sicherheitsrelevanten Daten sind ausschließlich innerhalb des EWRs, der Schweiz oder Großbritannien zu speichern und zu verarbeiten. Dies gilt auch für sämtliche Unterauftragnehmer und sonstige Dritte, die Zugriff auf diese Daten erhalten.</p>	21.05.2026 06:48:15
3	<p>In den Vergabeunterlagen wird gefordert, dass das Managed SOC Netzwerk-Logs sammelt und analysiert.</p> <p>Wir bitten um Klarstellung, ob diese Anforderung zwingend ist oder ob alternative Telemetriequellen als erfüllungsgleich anerkannt werden können.</p> <p>Begründung: Die Erhebung und Auswertung von Netzwerk-Logs ist in modernen IT-Umgebungen häufig nicht mehr möglich oder nicht mehr zielführend, da:– verschlüsselte Kommunikation (TLS 1.3, E2E-Verschlüsselung) den Inhalt und Kontext von Netzwerkverkehr weitgehend unzugänglich macht– Cloud-basierte Dienste (SaaS, IaaS, Zero Trust) keinen Zugriff auf interne Netzwerkdaten erlauben– Remote-Arbeitsplätze und mobile Endgeräte oft außerhalb des Unternehmensnetzwerks operieren– Segmentierte oder SD-WAN-Architekturen keinen vollständigen, zentral erfassbaren Netzwerkverkehr mehr</p>	<p>Die Anforderung ist zwingend und wird NICHT durch alternative Telemetriequellen als alleinige Erfüllung anerkannt.</p> <p>Die Sammlung und Analyse von Netzwerk-Logs ist neben Endpoint- und Identitätsdaten eine unverzichtbare Säule einer umfassenden Sicherheitsüberwachung ("SOC Visibility Triad").</p> <p>Wir präzisieren und bestätigen unser Verständnis von "Netzwerk-Logs" im Kontext dieser Ausschreibung wie folgt:</p> <p>Der Begriff umfasst eine Vielfalt an Telemetrie-Quellen, die sicherheitsrelevante Ereignisse auf der Netzwerkebene dokumentieren. Dazu zählen insbesondere, aber nicht ausschließlich:</p> <p>-Logs von Netzwerk-Security-Komponenten: Dies schließt Firewalls (On-Premise und Cloud), Web</p>	21.05.2026 06:48:15

erzeugen– sicherheitsrelevante Aktivitäten zunehmend auf Identitäts- und Endpoint-Ebene stattfinden und dort wesentlich präziser erkennbar sind.

Application Firewalls (WAF), Proxies, VPN-Gateways, Intrusion Detection/Prevention Systeme (IDS/IPS) und DNS-Server ein. Die Analyse dieser Log-Daten (z.B. blockierte/erlaubte Verbindungen, erkannte Angriffsmuster, DNS-Anfragen) ist fundamental für die Erkennung von Bedrohungen.
-Logs aus Cloud-Umgebungen: Wir erwarten explizit die Integration und Analyse von nativen Netzwerk-Log-Quellen der genutzten Cloud-Provider (z.B. AWS VPC Flow Logs, Azure NSG Flow Logs, Google Cloud VPC Flow Logs).
-Logs von Remote-Access-Lösungen: Dies umfasst Logs von VPN-Konzentratoren sowie von modernen SASE/SSE/Zero-Trust-Netzwerk-Access (ZTNA)-Plattformen.
-Flussdaten (Metadaten): Die Analyse von Netzwerkflussdaten (z.B. NetFlow, sFlow, IPFIX) aus zentralen Netzwerkkomponenten zur Erkennung von Anomalien im Kommunikationsverhalten (wer spricht mit wem, wann, wie viel), auch wenn der Dateninhalt verschlüsselt ist.

Ihre Begründung hebt die Herausforderungen durch Verschlüsselung und moderne Architekturen hervor. Wir sind uns dieser Entwicklungen bewusst. Ein leistungsfähiges Managed SOC muss jedoch gerade in der Lage sein, mit diesen Gegebenheiten umzugehen und den maximalen sicherheitsrelevanten Informationsgehalt aus den verbleibenden Metadaten und den genannten Log-Quellen zu extrahieren.

Eine alleinige Fokussierung auf Endpoint- und Identitätsdaten ist für die Erfüllung des Sicherheitsbedarfs des Auftraggebers nicht ausreichend, da hierdurch kritische Blind Spots (z.B. bei der Erkennung von kompromittierten IoT-Geräten ohne Endpoint-Agent oder bei umgangener Endpoint-Security) entstehen würden.

Wir bitten Sie, in Ihrem Angebot darzulegen, wie Ihr Managed SOC-Service die Fähigkeit zur Sammlung, Korrelation und Analyse der oben genannten Vielfalt an Netzwerk-Logs sicherstellt, um ein umfassendes und resilientes Sicherheitsmonitoring zu gewährleisten.

4

Wir haben eine Frage zu Anlage 1, Position A7. Im Rahmen der Ausschreibung wird für die Analyseleistungen im SOC ein Deutschniveau C1 gefordert.

Wir bitten um Klarstellung, ob die Leistungserbringung im Bereich Analyse auch in englischer Sprache zulässig ist, sofern die fachliche Qualität, Dokumentation sowie Kommunikation mit definierten Ansprechpartnern sichergestellt werden können.

Die in der Ausschreibung geforderte Beherrschung der deutschen Sprache auf dem Niveau C1 des Gemeinsamen Europäischen Referenzrahmens (GER) ist eine zwingende Anforderung für alle Leistungen mit direktem oder indirektem Kundenkontakt.

Wir erkennen an, dass die interne Kommunikation zwischen Ihren Analysten, die Nutzung von Fachtools und die Recherche in internationalen

21.05.2026 14:07:06

Hintergrund der Frage ist, dass im Bereich Cyber Security und SOC-Analyse international etablierte Fachbegriffe, Analysewerkzeuge, Threat-Intelligence-Quellen sowie Herstellerkommunikation überwiegend englischsprachig sind. Darüber hinaus sind hochqualifizierte SOC-Analysten häufig international tätig und arbeiten standardmäßig in englischer Sprache.

Eine Öffnung für englischsprachige Analyseleistungen könnte den Kreis geeigneter Fachkräfte erweitern und damit die Verfügbarkeit spezialisierter Expertise sowie die Qualität der Leistungserbringung erhöhen.

Quellen in englischer Sprache erfolgen kann und oft auch zweckmäßig ist. Dies steht nicht im Widerspruch zu unseren Anforderungen.

Jedoch muss zwingend sichergestellt sein, dass sämtliche nach außen gerichteten und für uns als Auftraggeber relevanten Kommunikations- und Dokumentationsprozesse vollständig in deutscher Sprache auf dem geforderten C1-Niveau erbracht werden.

Dies umfasst insbesondere, aber nicht ausschließlich:

Vorfalldokumentation und Incident Reports
Ticket-System: Erstellung, Bearbeitung und Kommentierung von Tickets
Mündliche Kommunikation: Telefonate, Videokonferenzen und Präsentationen mit unseren Ansprechpartnern
Schriftliche Berichte: Regelmäßige Reports (z.B. wöchentlich, monatlich) und Ad-hoc-Berichte
Dashboards und Benutzeroberflächen:
Beschriftungen, Erläuterungen und bereitgestellte Inhalte
Die Anforderung stellt sicher, dass alle relevanten Informationen, insbesondere in kritischen Situationen, präzise, unmissverständlich und ohne Verzögerung durch Übersetzungen für unsere Mitarbeiter und Stakeholder verständlich sind.

Die Verantwortung für die Sicherstellung der sprachlichen Qualität auf dem geforderten Niveau liegt vollumfänglich beim Auftragnehmer.

5

1. Welche Betriebssysteme müssen clientseitig unterstützt werden (Windows 10/11, macOS, Linux)?

2. Welche Betriebssysteme müssen serverseitig unterstützt werden (Microsoft Server, Linux Distributionen)?

3. Ist Microsoft Sentinel und LogAnalytics bereits im Einsatz oder ist es geplant einzuführen?

zu 1.
Clientseitig müssen Windows 10/11 (Windows 10 ist stark in der Ablösung) unterstützt werden. macOS und Linux ist hier nicht im Einsatz.

zu 2.
Serverseitig müssen
-Windows Server ab 2019 (letzte 2012er Systeme noch in der Ablösung)
und
-aktuelle Linux OS zu (Debian, CentOS, SuSELinux, Ubuntu LTS)
unterstützt werden, wobei Ubuntu LTS der zukünftige Standard für Linux Server werden soll.

zu 3.
Die angesprochenen Systeme von Microsoft sind nicht im Einsatz und es ist noch nichts geplant. Durch die Ausschreibung wird ergebnisoffen ein System zur Sicherheitsinformations- und Ereignisüberwachung mit Vorfallreaktion/Incident Response gesucht (XDR/SIEM). Die Ausgestaltung des Angebots obliegt dem Bieter.

21.05.2026 16:13:00