KREISVERWALTUNG
Rhein-Hunsrück Kreis

Funktionale Leistungsbeschreibung

Die Kreisverwaltung des Rhein-Hunsrück-Kreises ist öffentliche Auftraggeberin. Im Rahmen eines offenen Verfahrens nach VgV bitten wir Sie um Abgabe eines Angebots für die Beschaffung eines MDR (Managed, Detect and Response) – Services. Als Menge wird hierbei eine Summe von **3.500 Clients inkl. Server** und **13.000 User Identitäten** angenommen.

Ende der Angebotsfrist:	18. August 2026 um 9 Uhr
Abgabe:	elektronisch
Zuschlagskriterium:	100 % Preis
Ende der Fragefrist:	11. August 2026

Die Vertragslaufzeit beträgt 4 Jahre und läuft vom 28.09.2026 bis 27.09.2030. Es besteht die Option, den Vertrag zweimal um jeweils ein Jahr zu verlängern.

Bitte reichen Sie uns mit Ihrem Angebot einen EVB-IT Vertrag ein. Der Vertrag muss auf die Anforderungen der ausgeschriebenen Leistung und der dazugehörigen funktionalen Leistungsbeschreibung abgestimmt sein.

Folgende Leistungen bzw. Vorrausetzungen müssen in Ihrem Angebot aufgeschlüsselt und erfüllt werden:

Nr.	Leistung
1.	Vertragslaufzeit von 4 Jahren (28.09.2026 bis 27.09.2030)
2.	Der Preis für 48 Monate muss in 4 gleichen Zahlungen und jährlich möglich sein
3.	Alle Endpunkte, Systeme, Module und Kommunikation mit dem MDR Service sind in einer Konsole enthalten
4.	Es ist kein Aufbau eines eigenen Sicherheitsteams auf Seiten der KV notwendig
5.	24/7/365 Monitoring, Threat Hunting & Reaktionsfähigkeit
6.	Log Investigation bis zu 30GB pro Tag für forensische Zwecke
7.	Speicherung der Sys-Log-Daten revisionssicher für mindestens 30 Tage beim Anbieter
8.	Fähigkeit zur Malware-Analyse

9.	Schnittstelle (API) zur vorhandenen Fortinet Firewall
10.	Neben der Erkennung per Künstlicher Intelligenz (KI) immer eine zwingende Beurteilung durch einen Cyber Security-Experten des Anbieters erforderlich
11.	Software, die auf granularer Ebene (pro Gerät) Maßnahmen treffen kann
12.	Bearbeitender Zugriff auf alle Module
13.	ISO 27001-Zertifizierung -> Zertifikatsnachweis
14.	Unterstützung von älteren Betriebssystemen (bis Server 2012 R2, Windows 7)
15.	Die Lösung erfüllt die Anforderungen gem. DSGVO, die Daten sind innerhalb von Deutschland gespeichert
16.	Quartalsweise Jour-Fix-Termine und Security Reports
17. 18.	Im Bedarfsfall Einsatz beim Auftraggeber vor Ort möglich, Anfahrt <2h
	Umfangreiche Unterstützung von Linux
19.	Dauer der Implementierungsphase bis zum „Go Live“ des MDR-Services beträgt maximal 2 Wochen
20.	Der MDR Service umfasst den 24x7 Schutz der Active Directory Umgebung und Entra ID Umgebung zum Schutz vor identitätsbasierten Bedrohungen und Angriffsszenarien (13.000 User Identitäten)
21.	Das Data Center für den Managed Service befindet sich in der EU
22.	Der MDR Service bietet die Möglichkeit zur direkten Kommunikation mit den Security-Analysten
23.	Der MDR Service muss einen persönlichen Ansprechpartner für kritische Fälle bereitstellen
24.	Reaktionszeit <= 60 Minuten nach Erkennung eines kritischen Incidents
25.	Die durchschnittliche Reaktionszeit des SLA muss die Analyse, Triage und Gegenmaßnahmen umfassen, nicht nur die Benachrichtigung über einen Vorfall
26.	Der AN hat im 24x7 Model dedizierte "Threat Hunting" Analysten im Einsatz um Rohdaten - anlassunabhängig der üblichen Detektionen - manuell auf Ausfälligkeiten die auf Angreiferaktivitäten hindeuten zu untersuchen
27.	Die Lösung darf sich nicht ausschließlich auf Signaturen oder Hash-Lookups zur Malware-Prävention stützen, sondern eine verhaltensbasierte Erkennung wird verwendet
28.	Die Plattform muss Seitwärtsbewegungen („Lateral Movement“) erkennen und mit beteiligten Endpunkten, zeitlichem Ablauf sowie Angriffstechniken gemäß MITRE ATT&CK darstellen
29.	Die Plattform muss die Möglichkeit bieten, aus der Ferne eine Verbindung zu den Zielsystemen herzustellen, um zusätzliche forensische Beweise zu sammeln (Speicherauszüge, Registry,

	Dateien usw.). Alle Betriebssysteme müssen hier unterstützt werden und die Plattformspezifischen Scriptingumgebungen bereitstellen
30.	Die Lösung muss die Möglichkeit bieten, Dateien auf entfernte Systeme zu übertragen, Dateien auszuführen, Skripte zu starten, Prozesse zu beenden, Registrierungsschlüssel zu ändern und andere Aufgaben durchzuführen, die während der Reaktion auf einen Vorfall erforderlich sind
31.	Die Lösung muss kompromittierte Passwörter im Active Directory und EntraID erkennen
32.	Die Lösung detektiert Attacken auf das Active Directory und EntraID
33.	Die Installation, Update oder Downgrade des Sensors/Agenten erfordert keinen System-Neustart. Der EDR Schutz und auch MDR Service muss bereits ohne Neustart vollumfänglich zur Verfügung stehen
34.	Alle Sensoren müssen in einem Agenten vorhanden sein
35.	Die Lösung beinhaltet eine SOAR Komponente, durch die im No-Code Verfahren Workflows gebaut werden können
36.	Die Lösung muss ein SIEM mit integrierter SOAR Lösung beinhalten
37.	Es muss einen MDR Service geben, der 3rd Party Detections bearbeitet und dessen Informationen mit anderen Detection korreliert (z.B. Fortinet, VMWare, Veeam)
38.	Die Lösung muss einen eigenen Log-Kollektor zur Verfügung stellen zur sicheren Weiterleitung von u.a. On-Premise Logs in das SIEM
39.	Der AN benennt mindestens zwei feste Ansprechpartner die vom Hersteller der Lösung zertifiziert sind
40.	Der AN bietet Unterstützung bei der Bereitstellung und beim Onboarding
41.	Der AN bietet während der Geschäftszeiten (Werktags 08:00-17:00 ausgenommen gesetzliche Feiertage in Rheinland-Pfalz) einen deutschsprachigen support und bietet die Möglichkeit, Level 1 und Level 2 Supportanfragen telefonisch zu bearbeiten

Bitte reichen Sie Ihr Angebot im PDF-Format schriftlich und unterschrieben auf Ihrem Briefbogen ein.

Das Angebot ist als Pauschalpreissumme in netto und brutto anzugeben. Die Mehrwertsteuer ist gesondert auszuweisen. Die Laufzeit von 4 Jahren ist im Pauschalpreis zu berücksichtigen.

Nachlässe/Rabatte sind gesondert auszuweisen.

Der günstigste Bieter erhält den Zuschlag.

Bitte beachten Sie, dass der Angebotspreis alle anfallenden Finanzierungs- und Zinskosten enthalten muss.