

Leistungsbeschreibung

Spot-Consulting

Leistungen im Bereich Elastic Security als SIEM

Vergabe 2026-098-SL

1. Allgemein

Ausgangssituation und Ziel

Die ARGE AOK-Rechenzentrum (ARGE) ist der zentrale Rechenzentrumsbetreiber für die AOK Niedersachsen und AOK Bremen/Bremerhaven. Die ARGE betreibt Elastic Security als zentrale SIEM- und Analyseplattform für die Sammlung, Korrelation, Analyse und Auswertung sicherheitsrelevanter Logs, Events und Alerts aus unterschiedlichen Datenquellen.

Elastic Security unterstützt die Erkennung, Bewertung und Untersuchung sicherheitsrelevanter Ereignisse. Hierzu werden unter anderem Informationen aus Endpunkten, Servern, Netzwerken, Identitäten, Cloud-Diensten und weiteren Security-Produkten zusammengeführt und ausgewertet.

Ziel der Ausschreibung ist der Abschluss eines Kontingentvertrages mit einem geeigneten Dienstleister für Consulting-Leistungen im Umfeld Elastic Security als SIEM. Die Leistungen sollen sowohl für geplante Tätigkeiten als auch für kurzfristige Unterstützungsbedarfe flexibel abrufbar sein.

2. Leistungsumfang

Der Auftraggeber ist berechtigt, während der Vertragslaufzeit bis zum 30.11.2029 Leistungen im Umfang von insgesamt höchstens 40 Personentagen abzurufen. Eine Verpflichtung des Auftraggebers zum Abruf einer bestimmten Mindestmenge oder zur vollständigen Ausschöpfung des Kontingents besteht nicht. Die Vergütung erfolgt ausschließlich für die vom Auftraggeber abgerufenen und vom Auftragnehmer tatsächlich erbrachten Leistungen.

Der Leistungsumfang umfasst insbesondere:

- Technische und fachliche Beratung zu Elastic Security
- Weiterentwicklung und Optimierung der bestehenden SIEM-Umgebung (Self-Managed)
- Integration neuer Datenquellen
- Optimierung von Datenquellen, Pipelines, Parsern und Mappings
- Unterstützung bei Detection Engineering und Erkennungslogiken
- Erstellung, Anpassung und Optimierung von Detection Rules
- Unterstützung bei Dashboards, Visualisierungen und Auswertungen
- Unterstützung bei Alerting, Triage und Use-Case-Entwicklung
- Performance-, Stabilitäts- und Betriebsoptimierungen
- Fehleranalyse und Unterstützung bei technischen Problemen
- Wissenstransfer an interne Mitarbeitende im Rahmen des Kontingentes

Der Auftragnehmer weist die relevanten Erfahrungen / Projekte für die Mitarbeiter nach, welche für die Leistung vorgesehen sind. Eine standardisierte Scorecard ist nicht erforderlich.

Der Auftragnehmer hat sicherzustellen, dass sämtliche für die Leistungserbringung eingesetzten Personen über die für die jeweils übertragenen Tätigkeiten erforderliche fachliche Qualifikation und praktische Erfahrung verfügen.

Jede eingesetzte Person muss über die untenstehenden Kenntnisse und Erfahrungen in folgenden Bereichen verfügen:

- Elastic Security und Elastic Stack
- Elasticsearch, Kibana und Elastic Agent / Fleet
- SIEM-Betrieb und Security Monitoring
- Detection Engineering
- Log Management und Datenquellenintegration
- ECS, Index Templates und Data Streams
- Ingest Pipelines und Datenmodellierung
- Detection Rules und Rule Management
- Dashboards, Visualisierungen und Reporting
- Alerting, Alert-Tuning und False-Positive-Reduzierung
- Rechte- und Rollenkonzepte
- Schnittstellen und API-Nutzung
- Integration von Security-Produkten und Logquellen

Wünschenswert sind zusätzliche Erfahrungen mit typischen Datenquellen wie Endpoint Security (SentinalOne), Netzwerkdaten (Cisco, ExtraHop), Vulnerability Management (Tenable, SUSE Security ehemals NeuVector), Cloud-Security-Logs (Azure, Google Cloud, AWS).

Sprache und Ort der Serviceleistung

Die Leistungserbringung hat in deutscher Sprache zu erfolgen und findet grundsätzlich remote statt. Bei besonderem Bedarf kann eine Leistungserbringung vor Ort am Standort des Auftraggebers in Hannover Vahrenwald vereinbart werden.