Aufforderung zur Angebotsabgabe: Cloud Security Monitoring und Analyse Lösung

Inhaltsübersicht

1. Einführung und Hintergrund
2. Ziele des Projekts
3. Umfang der Arbeiten
4. Technische Anforderungen
5. Funktionale Anforderungen
6. Anforderungen an KI und erweiterte Analytik
7. Qualifikationen des Anbieters
8. Kriterien für die Bewertung
9. Leitlinien für die Einreichung
10. Zeitleiste

1. Einleitung und Hintergrund

Die Organisation benötigt eine umfassende Cloud-Sicherheitsüberwachungs- und Analyselösung zur Verbesserung der Cybersicherheitsinfrastruktur. Diese Ausschreibung umreißt die Anforderungen an ein robustes System, das kontinuierliche Überwachung, Bedrohungserkennung und umfassende Analyse von Sicherheitsereignissen in Cloud-Umgebungen bietet.

1.1 Überblick über die Organisation

- Multi-Cloud-Infrastruktur unter Verwendung von AWS-, Azure- und GCP-Diensten
- Hybride Cloud-Architektur mit Rechenzentren vor Ort
- Globale Aktivitäten in mehreren geografischen Regionen

- Anforderungen für den Einsatz auf Unternehmensebene
- Kritischer Datenschutzbedarf

1.2 Derzeitige Sicherheitslage

- Vorhandene SIEM- und Protokollverwaltungstools
- Systeme zur Überwachung der Netzsicherheit
- Plattformen zum Schutz von Endgeräten
- Cloud-basierte Sicherheits-Tools
- Aktuelle Herausforderungen der Integration

1.3 Ziele des Projekts

- Verbesserte Transparenz der Cloud-Infrastruktur und der Sicherheitsereignisse
- Verbesserung der Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen in allen Umgebungen
- Gewährleistung der Einhaltung von Branchenvorschriften und -standards
- Optimieren Sie Sicherheitsabläufe durch fortschrittliche Analytik
- KI-gesteuerte Sicherheitsautomatisierung implementieren
- Einrichtung einer umfassenden Sicherheitsüberwachung

2. Projektziele

2.1 Zentrale Sicherheitsziele

- Implementierung einer umfassenden Cloud-Sicherheitsüberwachung für alle Umgebungen
- Erkennung von Bedrohungen und Reaktionsmöglichkeiten in Echtzeit
- Verbesserung der Funktionen zur Überwachung der Einhaltung von Vorschriften und der Berichterstattung
- Verbesserung der Untersuchung von Sicherheitsvorfällen und der Forensik
- Erweiterte Sicherheitsanalysen einführen

- Automatische Reaktion auf Bedrohungen ermöglichen

2.2 Ziele der Analytik und Intelligenz

- Einsatz erweiterter Analysen für die Korrelation von Sicherheitsereignissen
- Implementierung von KI-gestützter Bedrohungserkennung und -analyse
- Aufbau von Fähigkeiten zur vorausschauenden Sicherheit
- Automatische Reaktion auf Sicherheitsvorfälle ermöglichen
- Integration von Bedrohungsdaten entwickeln
- Schaffen Sie verwertbare Erkenntnisse zur Sicherheit

2.3 Operative Ziele

- Rationalisierung der Sicherheitsabläufe durch Automatisierung
- Weniger Ermüdungserscheinungen durch intelligente Priorisierung von Alarmen
- Verbesserung der Effizienz von Sicherheitsuntersuchungen
- Proaktive Funktionen zur Bedrohungssuche aktivieren
- Verbesserung der Arbeitsabläufe bei der Reaktion auf Vorfälle
- Optimieren Sie die Ressourcennutzung

3. Umfang der Arbeit

3.1 Implementierungsdienste

- Vollständige Umweltbewertung und Lückenanalyse
- Entwurf und Dokumentation der Lösungsarchitektur
- Integration in bestehende Sicherheitstools und -plattformen
- Verfahren zur Systemprüfung und -validierung
- Produktionseinsatz und -optimierung
- Wissenstransfer und Ausbildung

3.2 Implementierung der Kernfunktionalität

- Systeme zur Datenerhebung und -aggregation
- Rahmenwerke zur Sicherheitsüberwachung
- Systeme zur Verwaltung von Warnmeldungen
- Arbeitsabläufe für die Reaktion auf Vorfälle
- Instrumente zur Überwachung der Einhaltung der Vorschriften
- Berichts- und Analyseplattformen

3.3 Implementierung erweiterter Analysen

- Einsatz von KI und maschinellen Lernmodellen
- Prädiktive Analysefunktionen
- Automatisierte Antwortsysteme
- Integration von Bedrohungsdaten
- Implementierung der Verhaltensanalyse
- Entwicklung kundenspezifischer Analysen

4. Technische Anforderungen

4.1 Datenerfassung und -integration

- Multi-Cloud-Dateneingabefunktionen für AWS, Azure und GCP
- Log-Aggregation und Normalisierung in Echtzeit
- Umfassender Rahmen für die API-Integration
- Echtzeit-Datenverarbeitungsfunktionen
- Unterstützung für benutzerdefinierte Datenquellen
- Skalierbare Datenspeicherlösungen

4.2 Überwachung der Sicherheit

- Kontinuierliche Überwachung der Sicherheitslage
- Analyse des Netzwerkverkehrs in Echtzeit

- Erweiterte Analyse des Nutzer- und Unternehmensverhaltens
- Überwachung von Cloud-Konfiguration und Compliance
- Ermittlung von Vermögenswerten und Bestandsverfolgung
- Überwachung und Bewertung von Schwachstellen

4.3 Erkennung von Bedrohungen

- Mehrschichtige signaturbasierte Erkennung
- Fortgeschrittene Verhaltensanalytik
- Auf maschinellem Lernen basierende Erkennung von Bedrohungen
- Identifizierung von Zero-Day-Bedrohungen
- Überwachung von Insider-Bedrohungen
- Erstellung benutzerdefinierter Erkennungsregeln

5. Funktionale Anforderungen

5.1 Kernfunktionalitäten

5.1.1 Datenerfassung und -aggregation

Effiziente Datenerfassung und -aggregation bilden die Grundlage für die Überwachung der Cloud-Sicherheit. Konzentrieren Sie sich auf eine umfassende Abdeckung aller Cloud-Assets und die Möglichkeit, Daten aus verschiedenen Quellen für eine einheitliche Analyse zu normalisieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Quellen für die Datenerhebung	Sammeln von Daten aus Cloud-Protokollen		
	Sammeln von Daten aus dem Netzwerkverkehr		
	Erfassen von Daten aus Endpunktaktivitäten		

	Unterstützung der Integration benutzerdefinierter Datenquellen		
Sichtbarkeit	Umfassende Transparenz der Cloud-Umgebung		
	Ermöglicht Echtzeit-Überwachungsfunktionen		
	Unterstützung der Analyse historischer Daten		
Datenverarbeitung	Unterstützung der Datennormalisierung in Echtzeit		
	Ermöglichung von Datenfilterung und -klassifizierung		
	Bereitstellung von Datenanreicherungsfunktionen		

5.1.2 Erkennung von Bedrohungen

Eine wirksame Erkennung von Bedrohungen erfordert einen mehrschichtigen Ansatz, der signaturbasierte Erkennung, Verhaltensanalyse und maschinelles Lernen kombiniert.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennungsmethoden	Implementierung der signaturbasierten Erkennung		
	Einsatz von Algorithmen für maschinelles Lernen		
	Aktivieren Sie die Verhaltensanalyse		
	Unterstützung benutzerdefinierter Erkennungsregeln		

Abdeckung von Bedrohungen	Identifizierung bekannter Bedrohungen		
	Zero-Day-Bedrohungen erkennen		
	Überwachung auf Insider-Bedrohungen		
	Aufspüren fortschrittlicher, hartnäckiger Bedrohungen		
Umsetzung	Unterstützung eines mehrstufigen Erkennungsansatzes		
	Fähigkeiten zur Bedrohungssuche aktivieren		
	Integration von Bedrohungsdaten bereitstellen		

5.1.3 Reaktion auf Vorfälle

Die Geschwindigkeit und Effektivität der Reaktion auf Vorfälle wirkt sich direkt auf Ihre Sicherheitslage aus. Konzentrieren Sie sich auf Automatisierungsfunktionen und behalten Sie gleichzeitig die menschliche Kontrolle über wichtige Entscheidungen bei.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Reaktion Maßnahmen	Aktivieren der Systemisolierung		
	Unterstützung der Verkehrssperrung		
	Einleitung einer Untersuchung zulassen		
	Automatisierte Antwortmöglichkeiten bereitstellen		

	Aktivieren Sie die Fernsanierung von Systemen		
Spielbücher	Unterstützung benutzerdefinierter Antwort-Playbooks		
	Automatisierung von Arbeitsabläufen ermöglichen		
	Playbook-Testfunktionen bereitstellen		
Dokumentation	Lebenszyklus von Vorfällen verfolgen		
	Aufrechterhaltung von Antwortprüfpfaden		
	Berichte über Vorfälle generieren		

5.1.4 Priorisierung von Alarmen

Eine intelligente Priorisierung von Alarmen ist entscheidend für die effiziente Verwaltung von Sicherheitsvorgängen und die Verringerung der Alarmmüdigkeit.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
System der Prioritätensetzung	Implementierung einer auf Kritikalität basierenden Prioritätensetzung		
	Berücksichtigung des Vermögenswertes bei der Prioritätensetzung		
	Einbeziehung des Bedrohungskontexts in die Bewertung		
	Unterstützung benutzerdefinierter Priorisierungsregeln		

Management von Warnmeldungen	Intelligente Filterung von Warnmeldungen bereitstellen		
	Alarmweiterleitung und -eskalation aktivieren		
	Unterstützung der Korrelation von Warnmeldungen		
	Benutzerdefinierte Alarmkategorien zulassen		

5.1.5 Verwaltung der Einhaltung der Vorschriften

Umfassende Compliance-Management-Funktionen sind für die Einhaltung von Vorschriften und Sicherheitsstandards in Cloud-Umgebungen unerlässlich.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verwaltung der Politik	Durchsetzung von Compliance-Richtlinien		
	Unterstützung mehrerer Compliance-Rahmenwerke		
	Aktivieren der Erstellung benutzerdefinierter Richtlinien		
	Bereitstellung von Funktionen zum Testen von Richtlinien		
Überwachung	Einführung einer kontinuierlichen Überwachung der Einhaltung der Vorschriften		
	Verfolgung von Richtlinienverstößen		
	Generierung von Konformitätswarnungen		
	Unterstützung automatisierter Bewertungen		

Berichterstattung	Automatisierte Berichte über die Einhaltung von Vorschriften erstellen		
	Detaillierte Prüfpfade aufrechterhalten		
	Unterstützung der Erstellung benutzerdefinierter Berichte		
	Aktivieren Sie geplante Berichte		

5.1.6 Skalierbarkeit

Cloud-Sicherheitslösungen müssen effizient mit dem Unternehmenswachstum skalieren und gleichzeitig die Leistung und Zuverlässigkeit in allen Regionen und Umgebungen aufrechterhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Skalierung der Infrastruktur	Unterstützung der horizontalen Skalierung		
	Vertikale Skalierung einschalten		
	Bewältigung größerer Datenmengen		
	Unterstützung der Bereitstellung in mehreren Regionen		
Leistung	Aufrechterhaltung der Verarbeitungsgeschwindigkeit unter Last		
	Unterstützung der verteilten Verarbeitung		
	Aktivieren des Lastausgleichs		
Unterstützung des Wachstums	Anpassung an das Wachstum der Organisation		
	Skaliertes Lizenzierungsmodell		

	Unterstützung der Integration neuer Technologien		

5.1.7 Integrationsfähigkeiten

Die nahtlose Integration in bestehende Sicherheitsinfrastrukturen und -tools ist entscheidend für die Aufrechterhaltung der betrieblichen Effizienz und einer umfassenden Sicherheitsabdeckung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Integration von Sicherheitstools	Verbindung mit SIEM-Systemen		
	Integration mit EDR-Plattformen		
	Unterstützung der SOAR-Integration		
	Ermöglichung der Integration von Identitätsmanagement		
Integration der Entwicklung	Unterstützung der Integration von CI/CD-Pipelines		
	Ermöglichung von DevSecOps-Workflows		
	Bereitstellung von Automatisierungsschnittstellen		
API-Unterstützung	Umfassende REST-APIs anbieten		
	Unterstützung von Webhook-Implementierungen		
	Ermöglichung der Entwicklung benutzerdefinierter Integration		

5.1.8 Verwaltung des Datenschutzes

Ein robustes Datenschutzmanagement ist für den Schutz sensibler Informationen und die Einhaltung gesetzlicher Vorschriften in Cloud-Umgebungen unerlässlich.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Datenschutz	Implementierung der Verschlüsselung von Daten im Ruhezustand		
	Aktivieren Sie die Verschlüsselung bei der Übertragung		
	Unterstützung der Datenmaskierung		
	Anonymisierung von Daten ermöglichen		
Klassifizierung	Unterstützung der automatischen Datenklassifizierung		
	Aktivieren Sie benutzerdefinierte Klassifizierungsregeln		
	Erstellung von Klassifizierungsberichten		
Zugangskontrolle	Implementierung einer rollenbasierten Zugriffskontrolle		
	Aktivieren Sie die attributbasierte Zugriffskontrolle		
	Unterstützung des Prinzips der geringsten Privilegien		
	Verfolgung von Datenzugriffsaktivitäten		

5.2 KI-gestützte Fähigkeiten

5.2.1 Generative KI-Assistenten

KI-Assistenten sollten die Sicherheitsabläufe durch natürlichsprachliche Interaktion und intelligente Automatisierung verbessern und dabei Genauigkeit und Relevanz beibehalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Sprachverarbeitung	Bearbeitung von Abfragen in natürlicher Sprache		
	Unterstützung kontextbezogener Antworten		
	Aktivieren Sie die Unterstützung mehrerer Sprachen		
Sicherheitsaufgaben	Automatisieren Sie Routinevorgänge		
	Einblicke in die Sicherheit generieren		
	Anleitung zur Abhilfe geben		
Integration	Unterstützung der Workflow-Integration		
	Aktivieren Sie die benutzerdefinierte Automatisierung		
	Prüfpfade beibehalten		

5.2.2 Integration von Bedrohungsdaten

Eine fortschrittliche Integration von Bedrohungsdaten sollte verwertbare Erkenntnisse liefern und gleichzeitig Daten aus verschiedenen Quellen automatisch korrelieren, um die Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen zu verbessern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Geheimdienstliche Analyse	Verarbeiten Sie mehrere Bedrohungs-Feeds		
	Korrelieren Sie Bedrohungsindikatoren		

	Erzeugen von Schauspielerprofilen		
	Folgenabschätzung bereitstellen		
Automatisierung	Automatisierte Aufnahme von Futtermitteln ermöglichen		
	Unterstützung der Erstellung benutzerdefinierter Informationen		
	Erkennungsregeln automatisch aktualisieren		
Integration	Verbindung mit externen Plattformen		
	Unterstützung der Formate STIX/TAXII		
	Funktionen zur gemeinsamen Nutzung von Bedrohungen aktivieren		

5.2.3 Code-Analyse

Die KI-gestützte Code-Analyse sollte umfassende Möglichkeiten zur Sicherheitsbewertung bieten und gleichzeitig die Zahl der Fehlalarme minimieren und klare Anleitungen für Abhilfemaßnahmen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Analysefunktionen	Statische Code-Analyse durchführen		
	Aktivieren der dynamischen Codeanalyse		
	Unterstützung mehrerer Sprachen		
	Identifizierung von Sicherheitsschwachstellen		

Automatisierung	Automatisieren der Scan-Planung		
	Ermöglichung der CI/CD-Integration		
	Abhilfeschritte generieren		
Berichterstattung	Detaillierte Ergebnisse vorlegen		
	Verfolgung von Schwachstellen-Trends		
	Unterstützung benutzerdefinierter Berichte		

5.2.4 Intelligente Cloud-Erkennung und -Reaktion (CDR)

CDR-Funktionen sollten KI für die frühzeitige Erkennung von Bedrohungen nutzen und gleichzeitig automatische Reaktionsmaßnahmen und eine klare Visualisierung der Angriffskette ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Aufdeckungsfähigkeiten	Ermöglicht die frühzeitige Erkennung von Angriffen		
	Cloud-Dienste überwachen		
	Identifizierung von Angriffsmustern		
	Seitliche Bewegung der Spur		
Antwortfunktionen	Erste Reaktion automatisieren		
	Unterstützung benutzerdefinierter Playbooks		
	Eindämmung von Zwischenfällen ermöglichen		
Analytik	Korrelieren Sie Sicherheitsereignisse		

	Angriffsvisualisierung bereitstellen		
	Folgenabschätzung generieren		

5.2.5 Adaptive Sicherheit

Adaptive Sicherheitsrahmen sollten kontinuierlich weiterentwickelt werden, um neuen Bedrohungen zu begegnen und gleichzeitig die Sicherheitskontrollen auf der Grundlage einer Risikobewertung in Echtzeit automatisch anzupassen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Adaptiver Rahmen	Implementierung dynamischer Kontrollen		
	Echtzeit-Überwachung ermöglichen		
	Unterstützung der Anpassung der Politik		
	Risikobasierte Anpassung vorsehen		
Lernfähigkeiten	Aktivieren Sie die Mustererkennung		
	Unterstützung des Verhaltenslernens		
	Aktualisierung der Sicherheitsgrundlagen		
Automatisierung	Sicherheitsregeln anpassen		
	Ändern der Zugangskontrollen		
	Erkennungskriterien aktualisieren		

5.2.6 Prädiktive Analytik

Prädiktive Analysefunktionen sollten historische Daten und aktuelle Bedrohungsdaten nutzen, um potenzielle Sicherheitsvorfälle vorherzusagen und eine proaktive Schadensbegrenzung zu ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Vorhersage	Vorhersage von Sicherheitsvorfällen		
	Potenzielle Bedrohungen identifizieren		
	Berechnung der Risikowerte		
	Trends bei Projektangriffen		
Analyse	Historische Daten verarbeiten		
	Analysieren von Bedrohungsmustern		
	Risikofaktoren evaluieren		
Berichterstattung	Erstellung von Prognoseberichten		
	Bereitstellung von Trendanalysen		
	Risikobewertungen erstellen		

5.2.7 Automatisierte Sicherheitsmaßnahmen

Die Sicherheitsautomatisierung sollte die Abläufe rationalisieren und gleichzeitig die Transparenz aufrechterhalten und die menschliche Kontrolle über kritische Entscheidungen ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Aufgaben-Automatisierung	Automatisieren Sie Routineaufgaben		
	Verwalten von Sicherheitswarnungen		
	Reaktion auf Vorfälle bewältigen		
	Prozess-Schwachstellenmanagement		

Arbeitsablauf-Management	Automatisierte Arbeitsabläufe erstellen		
	Aktivieren Sie die benutzerdefinierte Automatisierung		
	Unterstützung der menschlichen Aufsicht		
Berichterstattung	Automatisierte Aktionen verfolgen		
	Audit-Protokolle führen		
	Effektivitätsberichte generieren		

5.2.8 Intelligente Zugangskontrolle

Zugangskontrollsysteme sollten KI nutzen, um dynamische Entscheidungen zu treffen und dabei ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit zu wahren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verhaltensanalyse	Benutzeraktivitäten überwachen		
	Zugriffsmuster verfolgen		
	Anomalien erkennen		
	Profil Benutzerverhalten		
Zugangsverwaltung	Dynamische Berechtigungen festlegen		
	Implementierung eines risikobasierten Zugangs		
	Just-in-time-Zugang ermöglichen		
Schutz	Unbefugten Zugang verhindern		
	Verdächtige Aktivitäten blockieren		

	Durchsetzung von Zugriffsrichtlinien		

5.2.9 KI-gestützte Datenverlustprävention

DLP-Funktionen sollten KI nutzen, um sensible Daten genau zu identifizieren und zu schützen und gleichzeitig Geschäftsunterbrechungen zu minimieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennung von Daten	Identifizierung sensibler Daten		
	Informationstypen klassifizieren		
	Datenbewegung überwachen		
	Datennutzung verfolgen		
Prävention	Unerlaubte Freigabe blockieren		
	Verschlüsseln Sie sensible Daten		
	Durchsetzung von DLP-Richtlinien		
Verwaltung	Benutzerdefinierte Regeln erstellen		
	DLP-Berichte generieren		
	Verfolgung von Richtlinienverstößen		

5.2.10 AI Security Posture Management (AI-SPM)

AI-SPM sollte einen umfassenden Einblick in die Sicherheit von KI-Diensten bieten und gleichzeitig die automatische Behebung von erkannten Problemen ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI Service Sicherheit	Überwachen von AI-Workloads		

	Bewertung der LLM-Sicherheit		
	Zugriff auf AI-Modelle verfolgen		
	Auswertung der KI-Datennutzung		
Verwaltung	Sicherheitsüberprüfungen automatisieren		
	Aktivieren von Abhilfemaßnahmen		
	Aufrechterhaltung der Sicherheitsgrundlagen		
Berichterstattung	Berichte über die Körperhaltung generieren		
	Verfolgung von Sicherheitsmetriken		
	Dokumentieren Sie den Stand der Einhaltung		

5.2.11 GenAI-gestützte SaaS-Sicherheit

SaaS-Sicherheit sollte generative KI nutzen, um den Schutz zu verbessern und gleichzeitig umfassende Transparenz und Kontrolle zu gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
SaaS-Schutz	SaaS-Anwendungen überwachen		
	Kontrolle des Datenzugriffs		
	Schutz sensibler Informationen		
	Benutzeraktivitäten verfolgen		
Integration	CASB-Funktionen unterstützen		
	Aktivieren Sie die DLP-Integration		
	Bereitstellung von API-Sicherheit		

Verwaltung	Einblicke in die Sicherheit generieren		
	Automatisieren Sie die Durchsetzung von Richtlinien		
	Erstellung von Compliance-Berichten		

6. Qualifikationen des Anbieters

6.1 Informationen zum Unternehmen

- Mindestens 5 Jahre Erfahrung im Bereich Cloud-Sicherheit
- Nachgewiesene Erfolgsbilanz bei Sicherheitslösungen für Unternehmen
- Starke finanzielle Stabilität und Wachstum
- Industriezertifizierungen und Partnerschaften
- Globale Unterstützungsmöglichkeiten

6.2 Technisches Fachwissen

- Umfassende Erfahrung mit Cloud-Sicherheit
- Erweiterte Analyse- und KI-Funktionen
- Erfahrung mit der Integration wichtiger Plattformen
- Entwicklungs- und Anpassungsmöglichkeiten
- Sicherheitsforschung und Bedrohungsanalyse

6.3 Unterstützungsfähigkeiten

- 24/7/365 technische Unterstützung
- Mehrere Support-Kanäle
- Umfassende Schulungsprogramme
- Verfügbarkeit professioneller Dienstleistungen
- Regelmäßige Produktaktualisierungen und -verbesserungen

7. Kriterien für die Bewertung

7.1 Technische Verdienste (40%)

- Vollständigkeit der Lösung
- Technische Innovation
- AI/ML-Fähigkeiten
- Integrationsfähigkeit
- Skalierbarkeit und Leistung
- Wirksamkeit der Sicherheit

7.2 Funktionale Fähigkeiten (30%)

- Zentrale Sicherheitsmerkmale
- Erweiterte Analytik
- Fähigkeiten zur Automatisierung
- Berichterstattung und Sichtbarkeit
- Benutzererfahrung
- Anpassungsmöglichkeiten

7.3 Qualifikationen des Anbieters (20%)

- Erfahrung im Unternehmen
- Technisches Fachwissen
- Kundenreferenzen
- Unterstützung der Infrastruktur
- Fahrplan für Innovation
- Marktstellung

7.4 Kosten (10%)

- Preisgestaltung der Lösung
- Kosten der Durchführung
- Laufende Wartung

- Ausbildungskosten
- Zusätzliche Dienstleistungen
- Gesamtbetriebskosten

8. Anforderungen an die Einreichung

Die Anbieter müssen einreichen:

1. Detaillierte technische Lösungsbeschreibung
2. Methodik der Umsetzung und Integration
3. Projektzeitplan mit wichtigen Meilensteinen
4. Vollständige Preisstruktur
5. Qualifikation und Erfahrung des Unternehmens
6. Mindestens drei Unternehmensreferenzen
7. Support- und Wartungspläne
8. Ausbildung und Wissenstransfer
9. Musterberichte und Dokumentation
10. Produktfahrplan und künftige Entwicklungspläne

9. Zeitleiste

- RFP-Freigabe:
- Fragen sind fällig:
- Fälligkeit der Vorschläge:
- Bewertungszeitraum:
- Präsentationen von Anbietern:
- Auswahl des Anbieters:
- Projektstart:
- Durchführungsphase 1:

- Durchführungsphase 2:
- Abschluss des Projekts:

Alle Vorschläge sind einzureichen bei:

Technischer Kontakt:

Kontakt für die Beschaffung: