Aufforderung zur Angebotsabgabe: Cloud Infrastructure Entitlement Management (CIEM) Software-Lösung

Inhaltsübersicht

1. Einleitung und Hintergrund

Cloud Infrastructure Entitlement Management (CIEM) ist eine spezialisierte Sicherheitslösung für die Verwaltung und Sicherung von Zugriffsberechtigungen in Cloud-Umgebungen. Sie konzentriert sich auf die Überwachung und Kontrolle von Berechtigungen - Berechtigungen und Privilegien, die menschlichen und maschinellen Identitäten zugewiesen werden -, um sicherzustellen, dass der Zugriff auf Cloud-Ressourcen nach dem Prinzip der geringsten Privilegien erfolgt.

Unser Unternehmen ist auf der Suche nach einer umfassenden CIEM-Lösung, um unsere Cloud-Sicherheit zu verbessern und die Zugriffsverwaltung in unserer Cloud-Infrastruktur zu optimieren.

2. Projektziele

1. **Verbesserte Cloud-Sicherheit**
    - Verwalten und sichern Sie Zugriffsberechtigungen in Cloud-Umgebungen
    - Umsetzung einer umfassenden Verwaltung der Ansprüche
    - Proaktive Erkennung und Reaktion auf Bedrohungen ermöglichen
    - Sicherstellung der Durchsetzung des Grundsatzes des geringsten Rechtsanspruchs
2. **Einhaltung von Vorschriften**
    - Erfüllung spezifischer Compliance-Anforderungen (z. B. GDPR, HIPAA)
    - Automatisierte Compliance-Berichterstattung ermöglichen
    - Pflege von Prüfpfaden und Dokumentation
    - Umsetzung einheitlicher Zugangsrichtlinien
3. **Operative Effizienz**
    - Rationalisierung der Prozesse zur Verwaltung von Ansprüchen
    - Automatisieren Sie routinemäßige Zugriffsüberprüfungen und Zertifizierungen
    - Reduzieren Sie manuelle Eingriffe in die Rechteverwaltung
    - Optimieren Sie die Ressourcenzuweisung
4. **Umfassende Sichtbarkeit**
    - Vollständige Transparenz beim Zugriff auf Cloud-Ressourcen
    - Überwachung der Nutzungsmuster von Ansprüchen
    - Änderungen und Anomalien verfolgen

- Ermöglicht detaillierte Audit-Funktionen

3. Funktionale Anforderungen

3.1 Umfassende Datenerhebung und -analyse

Tipp: Effektive CIEM-Lösungen erfordern robuste Datenerfassungsfunktionen über mehrere Cloud-Plattformen hinweg. Konzentrieren Sie sich auf Echtzeit-Aggregation, umfassende Erkennung und KI-gestützte Analyse, um einen vollständigen Einblick in Ihre Cloud-Berechtigungslandschaft zu gewährleisten. Die Lösung sollte historische Daten für Trendanalysen aufbewahren und gleichzeitig umsetzbare Erkenntnisse liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Daten-Aggregation	Daten von mehreren Cloud-Plattformen zusammenfassen		
	Datenerfassung und -verarbeitung in Echtzeit		
	Unterstützung für alle wichtigen Cloud-Anbieter		
Entdeckung	Automatisierte Erkennung von Cloud-Entitäten		
	Kontinuierliche Überwachung der Kontoaktivitäten		
	Abbildung von Ressourcenbeziehungen		
Inventarverwaltung	Erstellung einer umfassenden Bestandsaufnahme der Ansprüche		
	Aktualisierung des Bestands in Echtzeit		
	Änderungen und Modifikationen verfolgen		
AI/ML-Analyse	Algorithmen zur Mustererkennung		

	Nutzungsanalyse und Trendbestimmung		
	Erkennung von Anomalien		

3.2 Erweiterte Erkennung von Bedrohungen

Tipp: Erweiterte Funktionen zur Erkennung von Bedrohungen sollten maschinelles Lernen und Verhaltensanalysen nutzen, um potenzielle Sicherheitsrisiken zu erkennen, bevor sie sich zu Vorfällen entwickeln. Suchen Sie nach Lösungen, die mehrere Erkennungsmethoden mit automatischen Reaktionsmöglichkeiten kombinieren, um einen umfassenden Schutz vor Bedrohungen zu bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Maschinelles Lernen - Erkennung	Mustererkennung für ungewöhnliche Verhaltensweisen		
	Festlegung des Grundverhaltens		
	Dynamische Schwellenwertanpassung		
Erkennung von Anomalien	Überwachung von Transaktionen in Echtzeit		
	Verhaltensanalyse		
	Kontextabhängige Erkennung		
Vorhersagefähigkeiten	Vorhersage zukünftiger Risiken		
	Trendanalyse		
	Frühwarnsystem		
Integration	Integration von Bedrohungsdaten-Feeds		

	Integration von Sicherheitstools		
	Integration von Alarmsystemen		

3.3 Automatisierte Reaktion auf Vorfälle

Tipp: Eine automatisierte Reaktion auf Vorfälle ist entscheidend für die Aufrechterhaltung der Sicherheit in Cloud-Umgebungen. Konzentrieren Sie sich auf Lösungen, die flexible, konfigurierbare Reaktionsoptionen bieten und gleichzeitig eine angemessene menschliche Aufsicht für kritische Entscheidungen gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
KI-gesteuerte Antwort	Automatisierte Entscheidungsmöglichkeiten		
	Risikobasierte Priorisierung von Maßnahmen		
	Optimierung durch maschinelles Lernen		
Automatisierung von Arbeitsabläufen	Konfigurierbare Antwort-Workflows		
	Automatisierung von Genehmigungsverfahren		
	Eskalationsverfahren		
Verwaltung von Genehmigungen	Automatischer Widerruf von Genehmigungen		
	Vorübergehende Zugangsverwaltung		
	Zugangsverfahren für Notfälle		
Fähigkeiten zur Integration	Integration von Sicherheitstools		

	SIEM-Integration		
	Integration des Fahrscheinsystems		

3.4 Priorisierung von Alarmen und Risikobewertung

Tipp: Eine wirksame Priorisierung von Warnmeldungen ist für die Bewältigung der Vielzahl von Sicherheitsereignissen in Cloud-Umgebungen unerlässlich. Suchen Sie nach Lösungen, die mehrere Risikofaktoren mit maschinellem Lernen kombinieren, um eine genaue, kontextbezogene Risikobewertung zu ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Risiko-Scoring	KI-gestützte Risikobewertung		
	Dynamische Risikoberechnung		
	Berücksichtigung mehrerer Faktoren		
Management von Warnmeldungen	Risikobasierte Prioritätensetzung		
	Alert-Korrelation		
	Reduzierung von Falsch-Positiven		
Personalisierung	Benutzerdefinierte Risikometrien		
	Einstellbare Schwellenwerte		
	Organisationsspezifische Faktoren		
Tendenz	Historische Trendanalyse		
	Mustererkennung		

	Prädiktive Analytik		

3.5 Verwaltung des Datenschutzes

Tipp: Das Datenschutzmanagement erfordert ausgefeilte Klassifizierungs- und Schutzmechanismen in Cloud-Umgebungen. Bevorzugen Sie Lösungen, die eine automatische Erkennung sensibler Daten, eine KI-gestützte Klassifizierung und granulare Datenschutzkontrollen bieten und gleichzeitig die Einhaltung der einschlägigen Vorschriften gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Umgang mit sensiblen Daten	Sicheres Cloud-übergreifendes Informationsmanagement		
	Automatisierung der Datenklassifizierung		
	Implementierung der Datenschutzkontrolle		
AI-Klassifizierung	Automatisierte Datenklassifizierung		
	Mustererkennung für sensible Daten		
	Kontinuierliche Aktualisierung der Klassifikation		
Einhaltung des Datenschutzes	Automatisierte Überwachung der Einhaltung der Vorschriften		
	Datenschutz-Folgenabschätzungen		
	Verfolgung der gesetzlichen Anforderungen		
Zugriffsmuster	Analyse des Datenzugangs		
	Überwachung des Verwendungsmusters		

	Erkennung von Datenschutzverletzungen		

3.6 Sichtbarkeit und Analyse von Ansprüchen

Tipp: Umfassende Transparenz der Berechtigungen ist die Grundlage für ein effektives CIEM. Suchen Sie nach Lösungen, die tiefe Einblicke in Berechtigungsbeziehungen, Nutzungsmuster und potenzielle Risiken bieten und gleichzeitig intuitive Visualisierungstools für komplexe Berechtigungsstrukturen bereitstellen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Multi-Cloud-Sichtbarkeit	Zentralisierte Berechtigungsansicht		
	Plattformübergreifende Überwachung		
	Einheitliches Dashboard		
Musteranalyse	KI-gesteuerte Nutzungsanalyse		
	Erkennung von Verhaltensmustern		
	Erkennung von Anomalien		
Relationship Mapping	Verfolgung der Erlaubnisabhängigkeit		
	Visualisierung von Ressourcenbeziehungen		
	Analyse der Zugangswege		
Analytik	Visualisierung der Verwendungsmuster		
	Angabe der Risikostufe		
	Trendanalyse		

3.7 Durchsetzung und Einhaltung von Richtlinien

Tipp: Eine wirksame Durchsetzung von Richtlinien erfordert sowohl präventive als auch detektivische Kontrollen. Suchen Sie nach Lösungen, die KI-gesteuerte Richtlinienempfehlungen mit automatischen Durchsetzungsfunktionen kombinieren und gleichzeitig die Flexibilität für unternehmensspezifische Anforderungen wahren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Politikgestaltung	KI-generierte Empfehlungen		
	Vorlagenbasierte Richtlinienerstellung		
	Entwicklung maßgeschneiderter Strategien		
Automatisierte Updates	Nutzungsmuster-basierte Aktualisierungen		
	Integration von Compliance-Anforderungen		
	Dynamische Anpassung der Politik		
Zugangskontrolle	Feinkörnige Rechteverwaltung		
	Rollenbasierte Zugriffskontrolle		
	Just-in-time-Zugang		
Überwachung der Einhaltung	Kontinuierliche Einhaltung der Richtlinien		
	Erkennung von Verstößen		
	Automatisierte Abhilfemaßnahmen		

3.8 Kontinuierliche Überwachung und Risikobewertung

Tipp: Kontinuierliche Überwachung bietet Echtzeit-Einblicke in Ihre Sicherheitslage. Konzentrieren Sie sich auf Lösungen, die umfassende Überwachungsfunktionen mit KI-gesteuerter Risikobewertung bieten, um potenzielle Sicherheitsprobleme proaktiv zu identifizieren und zu priorisieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verfolgung in Echtzeit	Überwachung von Anspruchsänderungen		
	Aktivitätsprotokollierung		
	Warnmeldungen in Echtzeit		
Risikobewertung	KI-gesteuerte Risikobewertung		
	Ständige Aktualisierung der Bewertung		
	Kontextabhängige Analyse		
Dynamisches Scoring	Risikobewertung in Echtzeit		
	Multi-Faktor-Risikoberechnung		
	Trendanalyse		
Verhaltensanalytik	Überwachung des Nutzerverhaltens		
	Analyse der Ressourcennutzung		
	Erkennung von Anomalien		

3.9 Zugangsbescheinigung und Überprüfung

Tipp: Rationalisierte Zugriffszertifizierungsprozesse sind für die Aufrechterhaltung von Sicherheit und Compliance unerlässlich. Suchen Sie nach Lösungen, die Zertifizierungsworkflows automatisieren und gleichzeitig umfassende Prüfprotokolle und Funktionen zur Beweissammlung bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Zertifizierungs-Workflows	AI-gestützte Überprüfungsprozesse		
	Automatisierte Terminplanung		
	Verwaltung von Kampagnen		
Historische Analyse	Überprüfung des Zugangsmusters		
	Analyse der Nutzungstrends		
	Risikobasierte Zertifizierung		
Sammlung von Beweismitteln	Automatisierte Beweiserhebung		
	Pflege des Prüfpfads		
	Erstellung der Dokumentation		
Überprüfung Management	Aufgabe des Gutachters		
	Verfolgung der Fortschritte		
	Umgang mit Eskalationen		

3.10 Optimierung von Ansprüchen

Tipp: Eine wirksame Optimierung der Berechtigungen trägt dazu bei, Sicherheitsrisiken zu verringern und gleichzeitig die betriebliche Effizienz zu verbessern. Bevorzugen Sie Lösungen, die maschinelles Lernen nutzen, um Verbesserungsmöglichkeiten zu identifizieren und Optimierungsprozesse zu automatisieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
ML-Empfehlungen	Optimierungsvorschläge		

	Nutzungsbasierte Analyse		
	Risikobasierte Prioritätensetzung		
Überversorgung	Erkennung von überschüssigen Berechtigungen		
	Analyse der Verwendungslücke		
	Empfehlungen zur richtigen Dimensionierung		
Automatisierung	Automatisierte Optimierungsabläufe		
	Optimierung der Selbstbedienung		
	Stapelverarbeitungsfunktionen		
Analyse der Auswirkungen	Folgenabschätzung ändern		
	Risikobewertung		
	Analyse der Auswirkungen auf die Leistung		

3.11 Visuelle Darstellung

Tipp: Visuelle Analysen helfen den Beteiligten, komplexe Berechtigungsbeziehungen und Sicherheitsrisiken zu verstehen. Setzen Sie auf Lösungen, die interaktive, intuitive Visualisierungen mit Echtzeit-Updates und anpassbaren Ansichten bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Identitätsvisualisierung	KI-gestütztes Beziehungsmapping		
	Interaktive Visualisierungen		
	Hierarchische Ansichten		

Risiko-Visualisierung	Dynamische Risikoindikatoren		
	Visualisierung von Bedrohungen		
	Aufschlag-Display		
Dashboard-Anpassung	Benutzerspezifische Ansichten		
	Rollenbasierte Dashboards		
	Benutzerdefinierte Anzeige von Metriken		
Echtzeit-Analytik	Live-Daten-Updates		
	Trend-Visualisierung		
	Leistungsmetriken		

3.12 Anpassung und adaptive Politiken

Tipp: Flexible Anpassungsmöglichkeiten stellen sicher, dass die Lösung an die spezifischen Anforderungen Ihres Unternehmens angepasst werden kann. Suchen Sie nach Lösungen, die KI-gesteuerte Anpassung mit robusten Anpassungstools für Richtlinien, Workflows und Regeln kombinieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Anpassung von Richtlinien	KI-gestützte Politikgestaltung		
	Anpassung von Vorlagen		
	Organisationsspezifische Regeln		
Adaptives Lernen	ML-basierte Anpassung der Politik		
	Verhaltensbasierte Aktualisierungen		

	Dynamische Regelanpassung		
Workflow-Entwicklung	Erstellung benutzerdefinierter Arbeitsabläufe		
	Prozessautomatisierung		
	Flexibilität bei der Integration		
Verwaltung der Rahmenbedingungen	Anpassung des politischen Rahmens		
	Verwaltung der Regelhierarchie		
	Versionskontrolle		

3.13 Protokollierung und Berichterstattung

Tipp: Umfassende Protokollierungs- und Berichtsfunktionen sind für die Einhaltung von Vorschriften und die betriebliche Überwachung von entscheidender Bedeutung. Bevorzugen Sie Lösungen, die detaillierte Prüfprotokolle, automatische Berichterstellung und vorausschauende Analysen bieten und gleichzeitig historische Daten für Trendanalysen bereithalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Umfassende Protokollierung	Erstellung von Prüfprotokollen		
	Aktivitätsprotokollierung		
	Verfolgung von Änderungen		
Erstellung von Berichten	Automatisierte Berichte zur Einhaltung der Vorschriften		
	Erstellung benutzerdefinierter Berichte		

	Planmäßige Berichterstattung		
Einhaltung von Vorschriften	Compliance-spezifische Berichte		
	Unterstützende Prüfungsunterlagen		
	Sammlung von Beweismitteln		
Prädiktive Analytik	KI-gesteuerte Trendanalyse		
	Sicherheitsprognosen		
	Risikovorhersage		

4. Erforderliche Hauptmerkmale

4.1 Sichtbarkeit von Ansprüchen

- Vollständiger Überblick über alle Berechtigungen auf allen Cloud-Plattformen
- Verfolgung von Genehmigungen in Echtzeit
- Abbildung der Beziehungen zwischen Identitäten und Ressourcen
- Analyse der historischen Zugriffsmuster

4.2 Kontinuierliche Überwachung

- Aktivitätsverfolgung in Echtzeit
- Verhaltensanalyse
- Erkennung von Anomalien
- Überwachung des Verwendungsmusters

4.3 Durchsetzung der Politik

- Automatisierte Umsetzung von Richtlinien
- Regelbasierte Zugangskontrolle
- Erkennung von Richtlinienverstößen
- Durchsetzung der Vorschriften

4.4 Zugangsbescheinigung

- Automatisierte Überprüfungszyklen
- Sammlung von Beweismitteln
- Arbeitsabläufe bei der Zertifizierung
- Pflege des Prüfpfads

4.5 Risikobewertung

- Risikobewertung in Echtzeit
- Bewertung der Bedrohung
- Bewertung der Anfälligkeit
- Analyse der Auswirkungen

4.6 Berichterstattung über die Einhaltung der Vorschriften

- Automatisierte Berichterstellung
- Dashboard zur Einhaltung der Vorschriften
- Audit-Unterstützung
- Erstellung benutzerdefinierter Berichte

5. Erwarteter Nutzen

5.1 Erhöhte Sicherheit

- Reduzierte Angriffsfläche
- Verbesserte Erkennung von Bedrohungen
- Schnellere Reaktion auf Vorfälle
- Bessere Zugangskontrolle

5.2 Operative Effizienz

- Automatisierte Arbeitsabläufe
- Reduzierter manueller Aufwand
- Rationalisierte Prozesse

- Verbesserte Ressourcennutzung

5.3 Einhaltung von Vorschriften

- Automatisierte Überwachung der Einhaltung der Vorschriften
- Vereinfachte Rechnungsprüfung
- Geringeres Risiko der Einhaltung von Vorschriften
- Verbesserte Berichtsfunktionen

5.4 Verbesserte Sichtbarkeit

- Umfassende Einblicke in den Zugang
- Klare Erlaubnisbeziehungen
- Verbesserte Überwachungsmöglichkeiten
- Bessere Entscheidungshilfe

6. Technische Anforderungen

6.1 Skalierbarkeit

- Adaptive Skalierung je nach Unternehmensgröße
- Dynamische Ressourcenzuweisung
- AI-optimierte Leistung
- Unterstützung mehrerer Regionen
- Architektur für hohe Verfügbarkeit

6.2 Integrationsfähigkeiten

- Nahtlose Integration von Sicherheitstools
- Konnektivität des Identitätssystems
- KI-gesteuerte Datensynchronisierung
- API-Verfügbarkeit
- Unterstützung für benutzerdefinierte Integration

6.3 Datenverwaltung

- Sichere Datenverarbeitung
- Schutz der Privatsphäre
- Maßnahmen zur Datenspeicherung
- Sicherung und Wiederherstellung
- Verwaltung des Lebenszyklus von Daten

6.4 Unterstützung aufkommender Technologien

- Ausrichtung der Zero-Trust-Architektur
- Integration mit Cloud Security Posture Management (CSPM)
- KI-gestützte Analytik
- Fähigkeiten des maschinellen Lernens
- Anpassungsfähigkeit an künftige Technologien

7. Qualifikationen des Anbieters

1. Hintergrund des Unternehmens
    - Kompetenz in Sachen Cloud-Sicherheit
    - Erfahrung mit der CIEM-Implementierung
    - Kundenreferenzen und Fallstudien
    - Dokumentation zur finanziellen Stabilität
2. Unterstützungsdienste
    - Fähigkeiten zur technischen Unterstützung
    - Ausbildungsprogramme
    - Unterstützung bei der Umsetzung
    - Laufende Wartungsdienste
3. Konformität und Zertifizierungen
    - Einhaltung von Branchenstandards (ISO 27001, SOC 2)

- Unterstützung bei gesetzlichen Anforderungen (GDPR, HIPAA)
- Sicherheitszertifizierungen
- Audit-Fähigkeiten

8. Kriterien für die Bewertung

1. Vollständigkeit der Lösung (25%)
    - Abdeckung der funktionalen Anforderungen
    - Technische Fähigkeiten
    - AI/ML-Funktionen
    - Integrationsfähigkeit
2. Umsetzungskonzept (20%)
    - Methodik
    - Zeitleiste
    - Anforderungen an die Ressourcen
    - Ausbildungsplan
3. Kompetenz des Anbieters (20%)
    - Erfahrung mit Cloud-Sicherheit
    - Geschichte der CIEM-Implementierung
    - Kundenreferenzen
    - Unterstützungsmöglichkeiten
4. Innovation und Zukunftsfähigkeit (15%)
    - AI/ML-Fähigkeiten
    - Unterstützung neuer Technologien
    - Produkt-Fahrplan
    - F&E-Investitionen

5. Kostenstruktur (20%)
    - Gesamtbetriebskosten
    - Preismodell
    - Zusätzliche Kosten
    - ROI-Potenzial

9. Preisgestaltung und Lizenzierung

Die Anbieter müssen ausführliche Informationen zu folgenden Punkten liefern:

- Struktur der Preisgestaltung
- Modell der Lizenzvergabe
- Kosten der Durchführung
- Support- und Wartungsgebühren
- Ausbildungskosten
- Servicegebühren

10. Umsetzung und Integration

Erläutern Sie den Prozess für:

- Zeitplan für die Umsetzung
- Methodik der Integration
- Ansatz für die Datenmigration
- Verfahren zur Ersteinrichtung
- Ausbildungsprogramm
- Unterstützung nach der Implementierung

11. Leitlinien für die Einreichung

Die Vorschläge müssen Folgendes enthalten:

1. Zusammenfassung

2. Beschreibung der technischen Lösung
3. Ansatz für die Umsetzung
4. Zeitplan des Projekts
5. Details zur Preisgestaltung
6. Informationen zum Unternehmen
7. Referenzen
8. Beispielberichte und Screenshots
9. Dokumentation der AI/ML-Fähigkeiten
10. Spezifikationen für die Integration
11. Pläne für Support und Wartung
12. Details zum Schulungsprogramm

12. Zeitplan und Prozess

- RFP-Freigabedatum: [Datum]
- Einsendeschluss: [Datum]
- Fälligkeitsdatum des Vorschlags: [Datum]
- Präsentationen des Anbieters: [Datumsbereich]
- Datum der Auswahl: [Datum]
- Datum des Projektbeginns: [Datum]

13. Zu bewältigende Herausforderungen

1. Komplexität der Integration
    - Integration mit bestehenden Tools
    - Herausforderungen bei der Datenmigration
    - API-Kompatibilität
2. Benutzerakzeptanz

- Anforderungen an die Ausbildung
- Management von Veränderungen
- Intuitive Benutzeroberfläche

3. Kostenüberlegungen
    - ROI-Begründung
    - Anforderungen an die Ressourcen
    - Laufende Wartungskosten