Aufforderung zur Angebotsabgabe: Cloud Security Posture Management (CSPM) Software-Lösung

Inhaltsübersicht

1. Einleitung

1.1 Zweck

Mit dieser Ausschreibung sollen Angebote für eine Cloud Security Posture Management (CSPM)-Lösung eingeholt werden, um die Cloud-Sicherheitslage unserer Organisation zu verbessern, die Einhaltung von Vorschriften zu gewährleisten und Risiken in unseren Cloud-Umgebungen zu verwalten.

1.2 Hintergrund

Die CSPM-Software wurde entwickelt, um Sicherheitsrisiken und Compliance-Probleme in Cloud-Infrastrukturen, einschließlich IaaS-, PaaS- und SaaS-Umgebungen, kontinuierlich zu überwachen, zu erkennen und darauf zu reagieren.

2. Anforderungen an die Lösung

2.1 Kernfunktionalität

2.1.1 Kontinuierliche Überwachung

- Überwachung von Cloud-Ressourcen in Echtzeit
- Erkennung von Fehlkonfigurationen und Schwachstellen

2.1.2 Automatisierte Abhilfemaßnahmen

- Automatische Korrektur von erkannten Problemen
- Verringerung menschlicher Fehler beim Sicherheitsmanagement

2.1.3 Verwaltung der Einhaltung der Vorschriften

- Überwachung des Stands der Einhaltung der Vorschriften
- Erstellung von Compliance-Berichten
- Unterstützung bei der Einhaltung von Industrienormen und -vorschriften

2.1.4 Risikobewertung

- Bewertung und Priorisierung von Sicherheitsrisiken
- Konzentration auf hochwirksame Bedrohungen

2.1.5 Integrationsfähigkeiten

- Nahtlose Integration in vorhandene Sicherheitstools
- Kompatibilität mit verschiedenen Cloud-Plattformen

2.2 Funktionale Anforderungen

2.2.1 Datenerfassung und -aggregation

Tipp: Ein robustes Datenerfassungssystem bildet die Grundlage für ein effektives CSPM. Berücksichtigen Sie das Volumen, die Vielfalt und die Geschwindigkeit der Datenquellen, die Ihr Unternehmen überwachen muss, und stellen Sie sicher, dass die Lösung Ihre aktuellen und geplanten Dateneingabeanforderungen bei gleichbleibender Leistung bewältigen kann.

Teilanforderung	JA/NEIN	Anmerkungen

Sammeln von Daten aus Cloud-Protokollen		
Sammeln von Daten aus dem Netzwerkverkehr		
Sammeln von Daten aus Endpunktaktivitäten		
Umfassende Transparenz der Cloud-Umgebung		

2.2.2 Erkennung von Bedrohungen

Tipp: Mehrere Erkennungsmethoden, die zusammenarbeiten, bieten die umfassendste Bedrohungsabdeckung. Bewerten Sie, wie jede Erkennungsmethode die anderen ergänzt, und berücksichtigen Sie neben der Erkennungseffizienz auch die Falsch-Positiv-Raten.

Teilanforderung	JA/NEIN	Anmerkungen
Nutzung der signaturbasierten Erkennung		
Nutzung von Algorithmen für maschinelles Lernen		
Verhaltensanalyse anwenden		
Identifizierung potenzieller Bedrohungen in Echtzeit		

2.2.3 Möglichkeiten der Reaktion auf Zwischenfälle

Tipp: Die Geschwindigkeit und Effektivität der Reaktion auf Vorfälle wirkt sich direkt auf die Eindämmung von Sicherheitsvorfällen aus. Achten Sie auf Automatisierungsfunktionen, die die Reaktionszeiten verkürzen und gleichzeitig eine angemessene menschliche Kontrolle für kritische Entscheidungen gewährleisten.

Teilanforderung	JA/NEIN	Anmerkungen
Isolierung der betroffenen Systeme ermöglichen		
Blockieren von bösartigem Datenverkehr zulassen		
Erleichterung der Einleitung von Untersuchungen		
Unterstützung der Verwaltung von Untersuchungen		

2.2.4 Verwaltung von Warnmeldungen

Tipp: Alarmmüdigkeit kann die Effektivität des Sicherheitsteams erheblich beeinträchtigen. Konzentrieren Sie sich auf Lösungen, die eine intelligente Korrelation und Priorisierung von Alarmen bieten, um sicherzustellen, dass kritische Alarme angemessene Aufmerksamkeit erhalten und gleichzeitig das Rauschen von Fehlalarmen reduziert wird.

Teilanforderung	JA/NEIN	Anmerkungen
Priorisierung von Alarmen auf der Grundlage ihrer Kritikalität		
Priorisierung von Alarmen auf der Grundlage möglicher Auswirkungen		
Implementierung einer intelligenten Alarmverarbeitung		
Verringerung der Ermüdung		

2.2.5 Skalierbarkeit und Anpassungsfähigkeit

Tipp: Cloud-Umgebungen können schnell wachsen und sich häufig ändern. Stellen Sie sicher, dass die Lösung horizontal und vertikal skaliert werden kann, um das Wachstum bei gleichbleibender Leistung zu bewältigen und sich an neue Cloud-Services und Architekturmuster anzupassen.

Teilanforderung	JA/NEIN	Anmerkungen
Skalierbarkeit für Organisationen jeder Größe		
Anpassung an komplexe Cloud-Umgebungen		
Unterstützung der dynamischen Ressourcenzuweisung		
Spitzenlasten effizient bewältigen		

2.2.6 Verwaltung des Datenschutzes

Tipp: Die Anforderungen an den Datenschutz variieren je nach Branche und Region. Vergewissern Sie sich, dass die Lösung Ihre spezifischen Compliance-Anforderungen unterstützt und granulare Kontrollen für Datenzugriff, -speicherung und -übertragung in verschiedenen Cloud-Umgebungen bietet.

Teilanforderung	JA/NEIN	Anmerkungen
Sichere Verwaltung sensibler Informationen		
Umsetzung solider Datenschutzmaßnahmen		
Unterstützung von Multi-Cloud-Bereitstellungen		
Bereitstellung von Prüfpfaden für den Datenzugriff		

2.3 KI-gestützte Funktionen

2.3.1 AI Security Posture Management (AI-SPM)

Tipp: Die Verwaltung der KI-Sicherheitslage erfordert einen speziellen Einblick in die KI/ML-Workloads und -Infrastruktur. Stellen Sie sicher, dass die Lösung die einzigartigen Sicherheitsherausforderungen von KI-Systemen versteht und aussagekräftige Einblicke in den Sicherheitsstatus Ihres KI-Stacks bieten kann.

Teilanforderung	JA/NEIN	Anmerkungen
Einblick in die Sicherheit der GenAI-Dienste gewähren		
Angebot einer Bestandsaufnahme des AI-Stacks (Modelle, Daten, Infrastruktur)		
Identifizierung AI-spezifischer Schwachstellen		
Abbildung potenzieller Angriffswege in AI-Umgebungen		

2.3.2 Verbesserte Erkennung mit KI und maschinellem Lernen

Tipp: KI-gestützte Erkennung sollte herkömmliche Methoden ergänzen und gleichzeitig die Zahl der Fehlalarme minimieren. Achten Sie auf Lösungen, die im Vergleich zu konventionellen Ansätzen deutliche Vorteile bei der Erkennungsgenauigkeit und -geschwindigkeit aufweisen.

Teilanforderung	JA/NEIN	Anmerkungen
Verwendung fortschrittlicher Algorithmen zur Mustererkennung		

Nutzung fortschrittlicher Algorithmen zur Erkennung von Anomalien		
Ermöglicht die Erkennung komplexer Bedrohungen in Echtzeit		

2.3.3 KI-gestützte Risikopriorisierung

Tipp: Eine wirksame Risikopriorisierung ist für die Ressourcenzuweisung entscheidend. Das KI-System sollte eine klare Begründung für seine Risikobewertungen liefern und eine Anpassung an die spezifische Risikotoleranz Ihres Unternehmens ermöglichen.

Teilanforderung	JA/NEIN	Anmerkungen
Analyse des Explosionsradius von gefährdeten Anlagen		
Komplexe Risiken effizient aufdecken		
Priorisierung der identifizierten Risiken		

2.3.4 Prädiktive Analytik

Tipp: Vorhersagefunktionen sollten umsetzbare Erkenntnisse liefern und nicht nur theoretische Möglichkeiten. Konzentrieren Sie sich auf Lösungen, die nachweislich genaue Vorhersagen mit klaren Empfehlungen zur Schadensbegrenzung liefern.

Teilanforderung	JA/NEIN	Anmerkungen
Antizipieren Sie potenzielle Schwachstellen, bevor sie ausgenutzt werden		
Ermöglichung proaktiver Risikomanagementstrategien		

2.3.5 AI Copilot für CSPM

Tipp: KI-Assistenten sollten die Effizienz des Bedieners steigern, ohne das menschliche Urteilsvermögen zu ersetzen. Beurteilen Sie, wie gut sich der Copilot in bestehende Arbeitsabläufe integrieren lässt und ob er klare Erklärungen für seine Empfehlungen liefert.

Teilanforderung	JA/NEIN	Anmerkungen
Ermöglicht Abfragen in natürlicher Sprache für die Systeminteraktion		
Schnelle Einblicke in die Sicherheitslage gewähren		
Empfehlungen für Abhilfemaßnahmen anbieten		
Optimale Arbeitsabläufe vorschlagen		

2.3.6 Automatisierte Compliance-Überwachung mit KI

Tipp: KI-gesteuerte Compliance-Überwachung sollte sich an regulatorische Änderungen anpassen und dabei genau bleiben. Überprüfen Sie die Fähigkeit der Lösung, neue Compliance-Anforderungen zu interpretieren und in umsetzbare Kontrollen zu übersetzen.

Teilanforderung	JA/NEIN	Anmerkungen
Anpassung an regulatorische Änderungen mit minimalem menschlichen Eingriff		
Echtzeitüberwachung für eine Vielzahl von Vorschriften		
Erstellung von Berichten über die Einhaltung der Vorschriften		

2.3.7 KI-gestützte Vorhersage von Bedrohungen

Tipp: Die Vorhersage von Bedrohungen sollte globale Bedrohungsdaten mit lokalem Kontext kombinieren. Suchen Sie nach Lösungen, die die Genauigkeit ihrer Vorhersagen nachweisen und ihre Prognosen klar begründen können.

Teilanforderung	JA/NEIN	Anmerkungen
Nutzung des maschinellen Lernens für verbesserte Vorhersagefähigkeiten		
Ermöglicht genaue Bedrohungsprognosen		
Anomalie-Erkennung durchführen		

2.3.8 Sicherheit generativer KI-Anwendungen

Tipp: Generative KI-Sicherheit erfordert ein spezielles Verständnis der Schwachstellen von KI-Modellen und der Risiken in der Lieferkette. Stellen Sie sicher, dass die Lösung sowohl die KI-Modelle als auch die sie unterstützende Infrastruktur effektiv überwachen und schützen kann.

Teilanforderung	JA/NEIN	Anmerkungen
Entdeckung und Bewertung von Sicherheitsrisiken in generativen KI-Anwendungen		
Identifizierung von Schwachstellen in den Abhängigkeiten von KI-Bibliotheken		
Scannen des Quellcodes auf Fehlkonfigurationen der Infrastruktur als Code		

3. Technische Anforderungen

3.1 Kompatibilität von Cloud-Plattformen

- Unterstützung für die wichtigsten Cloud-Anbieter (AWS, Azure, Google Cloud)
- Unterstützung von Multi-Cloud- und Hybrid-Cloud-Umgebungen
- API-basierte Integration in bestehende Sicherheitstools
- Unterstützung für gängige SIEM-Systeme (Security Information and Event Management)

3.2 Integrationsfähigkeiten

- API-basierte Integration in bestehende Sicherheitstools
- Unterstützung für gängige SIEM-Systeme (Security Information and Event Management)

3.3 Skalierbarkeit

- Fähigkeit zur Durchführung umfangreicher Cloud-Bereitstellungen
- Leistungsoptimierung für die Verarbeitung großer Datenmengen

3.4 Datenverwaltung

- Sichere Datenspeicherung und -verarbeitung

- Funktionen zur Datenaufbewahrung und -archivierung

4. Berichterstattung und Analyse

4.1 Dashboards und Visualisierung

- Anpassbare Dashboards für verschiedene Benutzerrollen
- Visualisierung der Sicherheitslage in Echtzeit

4.2 Möglichkeiten der Berichterstattung

- Automatische Berichterstellung für Compliance- und Prüfungszwecke
- Anpassbare Berichtsvorlagen

5. Unterstützung und Wartung

5.1 Technische Unterstützung

- 24/7-Support-Verfügbarkeit
- Mehrere Supportkanäle (Telefon, E-Mail, Chat)

5.2 Aktualisierungen und Upgrades

- Regelmäßige Software-Updates und Sicherheits-Patches
- Klarer Upgrade-Pfad für zukünftige Versionen

6. Ausbildung und Dokumentation

6.1 Benutzerschulung

- Umfassendes Schulungsprogramm für Administratoren und Endbenutzer
- Online- und persönliche Schulungsoptionen

6.2 Dokumentation

- Ausführliche Benutzerhandbücher und Verwaltungsleitfäden
- Regelmäßige Aktualisierung der Dokumentation

7. Preisgestaltung und Lizenzierung

7.1 Preismodell

- Klare Erläuterung der Preisstruktur (pro Benutzer, pro Anlage, usw.)
- Etwaige Mengenrabatte oder Vorteile bei langfristigen Verpflichtungen

7.2 Bedingungen für die Lizenzierung

- Flexibilität bei den Lizenzierungsoptionen
- Etwaige Einschränkungen oder Begrenzungen der Nutzung

8. Informationen zum Anbieter

8.1 Unternehmensprofil

- Kurze Geschichte und Hintergrund des Unternehmens
- Finanzielle Stabilität und Marktposition

8.2 Referenzen

- Nennen Sie mindestens drei Referenzen von Organisationen ähnlicher Größe
- Fallstudien, die erfolgreiche Implementierungen zeigen

9. Kriterien für die Bewertung

Die Vorschläge werden nach folgenden Kriterien bewertet:

- Vollständigkeit der Lösung bei der Erfüllung der angegebenen Anforderungen
- Innovative Funktionen, insbesondere KI-gestützte Funktionen
- Benutzerfreundlichkeit und Integration
- Skalierbarkeit und Leistung
- Preisgestaltung und Gesamtbetriebskosten
- Ruf des Anbieters und Supportmöglichkeiten

10. Anweisungen zur Einreichung

Die Vorschläge müssen Folgendes enthalten:

- Detaillierte Antwort auf alle Anforderungen
- Umsetzungsplan und Zeitplan
- Informationen zur Preisgestaltung
- Unternehmensinformationen und Referenzen
- Musterberichte und Dokumentation