Aufforderung zur Angebotsabgabe: Cloud-native Anwendungsschutz-Plattform (CNAPP)

Inhaltsübersicht

1. Überblick

Wir suchen Angebote für eine umfassende Cloud-Native Application Protection Platform (CNAPP) zum Schutz unserer Cloud-nativen Anwendungen während ihres gesamten Lebenszyklus. Die Lösung sollte integrierte Sicherheitsfunktionen bieten, die umfassende Transparenz, konsistente Richtliniendurchsetzung und robusten Schutz in unseren verschiedenen Cloud-Umgebungen ermöglichen.

2. Schlüsselkomponenten

Die vorgeschlagene Lösung muss die folgenden Schlüsselkomponenten enthalten:

2.1. Cloud Security Posture Management (CSPM)

2.2. Cloud Workload Protection Platform (CWPP)

2.3. Cloud Infrastructure Entitlement Management (CIEM)

2.4. DevSecOps-Integration

2.5. Laufzeitschutz

3. Funktionale Anforderungen

3.1. Einheitliche Sichtbarkeit

Tipp: Eine robuste, einheitliche Sichtbarkeitslösung ist entscheidend für eine umfassende Sicherheitsüberwachung. Suchen Sie nach Lösungen, die Echtzeit-Überwachungsfunktionen bieten und Daten aus verschiedenen Quellen in eine einzige, kohärente Ansicht integrieren können. Achten Sie auf die Tiefe der Sichtbarkeit über verschiedene Cloud-Dienste hinweg und auf die Möglichkeit, die Ansichten an die Bedürfnisse der verschiedenen Interessengruppen anzupassen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Einheitliche Sichtbarkeit	Zentraler Überblick über die Sicherheit aller Cloud-Ressourcen und -Services		
	Sichtbarkeit von Konfigurationen		
	Sichtbarkeit der Vermögenswerte		
	Sichtbarkeit von Berechtigungen		
	Sichtbarkeit des Codes		
	Sichtbarkeit der Arbeitslasten		

3.2. Automatisierte Einhaltung

Tipp: Automatisierte Compliance-Funktionen sollten die manuelle Überwachung reduzieren und gleichzeitig die kontinuierliche Einhaltung von Vorschriften gewährleisten. Evaluieren Sie Lösungen auf der Grundlage ihrer Fähigkeit, Compliance-Verstöße über mehrere rechtliche Rahmenbedingungen hinweg automatisch zu erkennen, zu melden und zu beheben.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Automatisierte Einhaltung	Kontinuierliche Bewertung der Einhaltung von Industriestandards		

	Kontinuierliche Durchsetzung der Einhaltung von Industriestandards		
	Optimierte Einhaltung gesetzlicher Vorschriften durch Überwachung		
	Optimierte Einhaltung gesetzlicher Vorschriften durch Berichterstattung		

3.3. Erkennung von und Reaktion auf Bedrohungen

Tipp: Erweiterte Funktionen zur Erkennung von und Reaktion auf Bedrohungen sollten sowohl traditionelle als auch KI-gestützte Methoden nutzen. Suchen Sie nach Lösungen, die Bedrohungen in Echtzeit erkennen und umsetzbare Reaktionsempfehlungen geben können.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennung von und Reaktion auf Bedrohungen	Echtzeit-Identifizierung von Bedrohungen über den gesamten Lebenszyklus von Anwendungen		
	Echtzeit-Abwehr von Bedrohungen über den gesamten Lebenszyklus von Anwendungen		
	KI-gestützte Erkennung von Bedrohungen durch fortschrittliche Analysen		
	KI-gestützte Erkennung von Bedrohungen durch prädiktive Analyse		
	Implementierung von Smart Cloud Detection & Response (CDR)		
	Erkennung von Bedrohungen in Echtzeit mit Absichtsanalyse		

3.4. Verwaltung der Politik

Tipp: Eine effektive Richtlinienverwaltung erfordert sowohl Konsistenz als auch Intelligenz. Bewerten Sie Lösungen auf der Grundlage ihrer Fähigkeit, einheitliche Sicherheitsrichtlinien in verschiedenen Umgebungen aufrechtzuerhalten und gleichzeitig KI zur Optimierung und Anpassung von Richtlinien auf der Grundlage neuer Bedrohungen und Unternehmensanforderungen zu nutzen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verwaltung der Politik	Konsistente Definition von Sicherheitsrichtlinien in verschiedenen Umgebungen		
	Konsistente Durchsetzung von Sicherheitsrichtlinien in verschiedenen Umgebungen		
	KI-gestützte Funktionen für die Richtlinienverwaltung		
	Intelligente politische Empfehlungen		

3.5. Skalierbarkeit

Tipp: Skalierbarkeit ist für wachsende Unternehmen unerlässlich. Suchen Sie nach Lösungen, die nahtlos mit Ihrer Infrastruktur skalieren können und dabei die Leistung aufrechterhalten. Achten Sie auf horizontale und vertikale Skalierungsmöglichkeiten sowie auf die Fähigkeit, plötzliche Lastspitzen zu bewältigen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Skalierbarkeit	Fähigkeit zur Anpassung an dynamische Cloud-Umgebungen		
	Unterstützung für wachsende Arbeitsbelastungen		
	Leistungserhaltung im großen Maßstab		

3.6. Integrationsfähigkeiten

Tipp: Integrationsfähigkeiten sind entscheidend für die Schaffung eines kohärenten Sicherheitsökosystems. Bewerten Sie die Lösungen nach ihrer Fähigkeit, sich in Ihre bestehende Toolchain zu integrieren, und nach der Einfachheit der Implementierung neuer Integrationen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Integrationsfähigkeiten	Nahtlose Integration mit bestehenden Entwicklungswerkzeugen		
	Nahtlose Integration mit Sicherheitstools		
	Nahtlose Integration mit Cloud-Management-Tools		
	Einfache Integration in SecOps-Ökosysteme für Echtzeit-Warnungen		

3.7. Multi-Cloud-Sicherheitsabdeckung

Tipp: Umfassende Multi-Cloud-Sicherheit ist in den vielfältigen Cloud-Umgebungen von heute unerlässlich. Suchen Sie nach Lösungen, die konsistente Sicherheitskontrollen für alle wichtigen Cloud-Anbieter bieten und gleichzeitig die anbieterspezifischen Nuancen berücksichtigen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Multi-Cloud-Sicherheitsabdeckung	Sichtbarkeit über IaaS-Umgebungen hinweg		
	Sichtbarkeit über PaaS-Umgebungen hinweg		
	Sichtbarkeit über serverlose Umgebungen hinweg		
	Unterstützung für AWS		
	Unterstützung für Azure		

	Unterstützung für Google Cloud		

3.8. Scannen der Infrastruktur als Code (IaC)

Tipp: IaC-Scanfunktionen sollten Sicherheitsprobleme frühzeitig im Entwicklungszyklus erkennen. Suchen Sie nach Lösungen, die sich in Ihren Entwicklungs-Workflow integrieren lassen und umsetzbare Anleitungen zur Behebung bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Scannen der Infrastruktur als Code	Erkennung von Sicherheitsschwachstellen im Infrastrukturcode vor der Bereitstellung		
	Unterstützung für mehrere IaC-Frameworks		
	Validierung vor dem Einsatz		
	Durchsetzung bewährter Sicherheitsverfahren		

3.9. Scannen von Containern und Kubernetes

Tipp: Die Containersicherheit erfordert ein umfassendes Scannen während des gesamten Container-Lebenszyklus. Bewerten Sie Lösungen anhand ihrer Fähigkeit, Container-Images zu scannen, Laufzeitschwachstellen zu erkennen und Kubernetes-spezifische Sicherheitskontrollen bereitzustellen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Scannen von Containern und Kubernetes	Identifizierung von Schwachstellen in containerisierten Anwendungen		
	Überwachung der Containersicherheit zur Laufzeit		

	Bewertung der Sicherheit von Kubernetes-Clustern		
	Scannen von Containerbildern		

3.10. Datenschutz

Tipp: Datenschutzfunktionen sollten ruhende und bewegte Daten abdecken. Suchen Sie nach Lösungen, die umfassende Datensicherheitskontrollen bieten, einschließlich Klassifizierung, Verschlüsselung und Zugriffsüberwachung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Datenschutz	Überwachung von Daten auf mögliche Exfiltration		
	Fähigkeiten zur Datenklassifizierung		
	Möglichkeiten der Datenprüfung		
	Verhinderung der Datenexfiltration		

3.11. Risikopriorisierung

Tipp: Eine effektive Risikopriorisierung hilft, die Sicherheitsmaßnahmen auf die wichtigsten Bedrohungen zu konzentrieren. Suchen Sie nach Lösungen, die KI nutzen, um Risiken im Kontext Ihrer Umgebung und der geschäftlichen Auswirkungen zu analysieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Priorisierung von Risiken	KI-gestützte Analyse von Risiken		
	KI-gestützte Priorisierung von Risiken		
	Korrelation der Schwachstellen		
	Kontextanalyse über den gesamten Lebenszyklus der Entwicklung		

	Abbildung der Beziehungen über den gesamten Entwicklungslebenszyklus		

3.12. KI-gestützte Sicherheit für KI-Apps im Unternehmen

Tipp: Die Sicherheit von KI-Anwendungen erfordert spezielle Funktionen. Suchen Sie nach Lösungen, die KI/ML-Workload-Muster verstehen und vor KI-spezifischen Bedrohungen schützen können.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI App Sicherheit	Sicherheitsposition für GenAI-Anwendungen		
	Schutz vor Bedrohungen für GenAI-Anwendungen		
	Verwaltung der KI-Sicherheitslage (AI-SPM)		
	Funktionen zur Erkennung von AI-Workloads		
	Sicherheitsfunktionen für AI-Workloads		

3.13. GenAI-gesteuerte Sanierung

Tipp: GenAI-Abhilfemaßnahmen sollten umsetzbare, kontextabhängige Lösungen bieten. Bewerten Sie die Qualität und Praktikabilität von KI-generierten Abhilfevorschlägen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
GenAI-gesteuerte Remediation	Kontextabhängige Abhilfevorschläge mit generativer KI		
	Erstellung von Konsolenrichtlinien		
	Erzeugung von CLI-Befehlen		
	Generierung von Codeschnipseln		

3.14. KI-gestützte Einstufung und Priorisierung von Alarmen

Tipp: Das Alarmmanagement sollte das Rauschen effektiv reduzieren und gleichzeitig sicherstellen, dass kritische Probleme angegangen werden. Suchen Sie nach Lösungen, die KI nutzen, um Alarme intelligent zu kategorisieren und zu priorisieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Einstufung und Priorisierung von Warnmeldungen	AI/ML-Modelle für die Alarmanalyse		
	AI/ML-Modelle für die Kategorisierung von Warnmeldungen		
	AI/ML-Modelle für die Priorisierung von Warnmeldungen		
	Funktionen zur Verringerung der Ermüdung durch Alarme		

3.15. Kontextuelle Anreicherung mit KI

Tipp: Die kontextuelle Anreicherung sollte aussagekräftige Erkenntnisse für eine bessere Entscheidungsfindung liefern. Suchen Sie nach Lösungen, die mehrere Datenquellen intelligent kombinieren können, um einen reichhaltigeren Kontext zu liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Kontextuelle Anreicherung	KI-gesteuerte Anreicherung von Alarmdaten		
	Unterstützung einer fundierten Entscheidungsfindung		
	Integration der Analyse der geschäftlichen Auswirkungen		

	Verbesserung der Priorisierungsprozesse		

3.16. Adaptives KI-Lernen

Tipp: Adaptive Lernfähigkeiten gewährleisten eine kontinuierliche Verbesserung der Sicherheitsmaßnahmen. Suchen Sie nach Lösungen, die von Ihrer Umgebung lernen und sich an neue Bedrohungen anpassen können.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Adaptives KI-Lernen	Kontinuierliche Verbesserung der KI-Empfehlungen		
	Implementierung von Feedback-Schleifen		
	KNAPP-übergreifendes kontextuelles Lernen		
	Schnelle Integration der neuen Sicherheitsabdeckung		

3.17. Abfrage des Sicherheitsgraphen

Tipp: Abfragefunktionen für Sicherheitsgraphen sollten leistungsstarke und dennoch benutzerfreundliche Analysetools bieten. Suchen Sie nach Lösungen, die sowohl visuelle als auch programmatische Schnittstellen für die Analyse von Sicherheitsdaten bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Abfrage des Sicherheitsgraphen	Umfassende Suche bei allen Cloud-Anbietern		
	Tools zur Visualisierung von Sicherheitsdaten		
	Erstellung von Sicherheitsrichtlinien aus dem Query Builder		

	Funktionen zur Verwaltung von Sicherheitsrichtlinien		

4. Technische Anforderungen

4.1. Plattform-Architektur

- Cloud-natives Design
- Microservices-Architektur
- Skalierbare Infrastruktur
- Hohe Verfügbarkeit

4.2. Integrationsfähigkeiten

- API-zentrierter Entwurf
- Integration von DevOps-Werkzeugen
- SIEM-Integration
- Unterstützung für benutzerdefinierte Integration

4.3. Leistungsstandards

- Verarbeitung in Echtzeit
- Minimale Latenzzeit
- Skalierbare Leistung
- Optimierung der Ressourcen

4.4. KI und maschinelles Lernen

- Erweiterte ML-Modelle
- Analyse in Echtzeit
- Prädiktive Fähigkeiten
- Kontinuierliches Lernen

5. Zusätzliche Anforderungen

5.1. Benutzeroberfläche

- Intuitive webbasierte Schnittstelle
- Anpassbare Dashboards
- Rollenbasierte Zugriffskontrolle
- Mobile Zugänglichkeit

5.2. Bereitstellungsoptionen

- SaaS-Bereitstellung
- Hybride Bereitstellungsoptionen
- Unterstützung mehrerer Regionen
- Wiederherstellung im Katastrophenfall

5.3. Unterstützung und Ausbildung

- 24/7 technische Unterstützung
- Umfassende Dokumentation
- Ressourcen für die Ausbildung
- Professionelle Dienstleistungen

5.4. Leistung und Skalierbarkeit

- Unterstützung auf Unternehmensebene
- Leistungsgarantien
- Metriken zur Skalierbarkeit
- Unterkunft mit Wachstum

6. Kriterien für die Bewertung der Anbieter

Kriterium	Gewicht	Beschreibung
Vollständigkeit der CNAPP-Lösung	20%	Umfassende Abdeckung der erforderlichen Funktionalität

AI/ML-Fähigkeiten	15%	Stärke der KI- und maschinellen Lernfunktionen
Multi-Cloud-Unterstützung	15%	Abdeckung und Integration über Cloud-Anbieter hinweg
Skalierbarkeit	10%	Leistung im Unternehmensmaßstab
Benutzererfahrung	10%	Benutzerfreundlichkeit und Zugänglichkeit der Schnittstelle
Analytik	10%	Funktionen für Berichte und Einblicke
Einhaltung der Vorschriften	10%	Regulatorische Abdeckung und Zertifizierungen
Unterstützung	5%	Technische Unterstützung und professionelle Dienstleistungen
Kosten	5%	Gesamtbetriebskosten

7. Anforderungen an die Einreichung

7.1. Technischer Vorschlag

- Detaillierte Lösungsarchitektur
- Matrix der Merkmalsabdeckung
- Integrationsfähigkeit
- AI/ML-Fähigkeiten
- Sicherheitskontrollen

7.2. Durchführungsplan

- Methodik des Einsatzes
- Zeitleiste
- Anforderungen an die Ressourcen
- Risikominderung

7.3. Struktur der Preisgestaltung

- Modell der Lizenzvergabe
- Kosten der Durchführung
- Kosten der Unterstützung
- Ausbildungskosten

7.4. Unternehmensinformationen

- Erleben Sie
- Fallstudien
- Referenzen
- Fahrplan für Innovation

7.5. Unterstützung Details

- SLA-Bedingungen
- Unterstützungsebenen
- Ausbildungsansatz
- Professionelle Dienstleistungen

8. Zeitleiste

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

Kontaktinformationen:

Bitte senden Sie Vorschläge und Fragen an: [Name der Kontaktperson] [E-Mail-Adresse] [Telefonnummer]