Aufforderung zur Angebotsabgabe: Cloud Workload Protection Plattform

Inhaltsübersicht

1. Einleitung

Mit diesem Request for Proposal (RFP) wird eine Cloud Workload Protection Platform (CWPP) gesucht. CWPPs sind spezialisierte Sicherheitslösungen zum Schutz von Workloads - wie Anwendungen, Datenbanken und Dienste - in verschiedenen Cloud-Umgebungen, einschließlich öffentlicher, privater und hybrider Clouds. Diese Plattformen bieten umfassende Transparenz, Bedrohungserkennung und automatisierte Reaktionen, um die Integrität und Sicherheit von Cloud-basierten Operationen zu gewährleisten.

2. Wichtigste Vorteile

Die vorgeschlagene Lösung muss die folgenden Hauptvorteile bieten:

1. Erhöhte Sicherheitsvorkehrungen
    - Umfassender Schutz vor Bedrohungen
    - Proaktive Sicherheitsmaßnahmen
    - Erweiterte Bedrohungsdaten
2. Operative Effizienz
    - Rationalisierte Sicherheitsabläufe
    - Automatisierte Sicherheitsprozesse
    - Reduzierte manuelle Eingriffe
3. Skalierbarkeit
    - Unterstützung für wachsende Cloud-Umgebungen
    - Optimierung der Leistung
    - Verwaltung der Ressourcen
4. Sicherstellung der Einhaltung
    - Verwaltung der Einhaltung von Rechtsvorschriften
    - Automatisierte Überwachung der Einhaltung der Vorschriften
    - Compliance-Berichterstattung
5. Cloud-übergreifendes Management
    - Einheitliche Sicherheit über Cloud-Plattformen hinweg
    - Konsistente Durchsetzung von Richtlinien
    - Zentralisierte Verwaltung

3. Kernmerkmale

Die Anbieter müssen ihre Fähigkeiten in den folgenden Kernbereichen nachweisen:

1. Automatisierte Erkennung und Sichtbarkeit

- Entdeckung von Vermögenswerten in Echtzeit
- Umfassende Transparenz in allen Umgebungen
- Ressourcenkartierung

2. Erkennung von und Reaktion auf Bedrohungen
    - Erweiterte Erkennung von Bedrohungen
    - Automatisierte Antwortmöglichkeiten
    - Management von Zwischenfällen
3. Härtung der Arbeitslast
    - Verwaltung der Sicherheitskonfiguration
    - Management von Schwachstellen
    - Systemhärtung
4. Entdeckung von Vermögenswerten
    - Kontinuierliche Vermögensüberwachung
    - Klassifizierung der Vermögenswerte
    - Verwaltung der Bestände
5. Erkennung von Anomalien
    - Verhaltensanalyse
    - Mustererkennung
    - Erzeugung von Warnmeldungen
6. Datensicherheit
    - Datenschutz
    - Verwaltung der Verschlüsselung
    - Zugangskontrolle

7. Governance
    - Verwaltung der Politik
    - Überwachung der Einhaltung
    - Risikobewertung
8. Protokollierung und Berichterstattung
    - Umfassende Protokollierung
    - Benutzerdefinierte Berichte
    - Analytische Dashboards

4. Funktionale Anforderungen

4.1 Datenerhebung und -aggregation

Tipp: Eine effektive Datenerfassung und -aggregation bildet die Grundlage für Ihre CWPP-Lösung. Konzentrieren Sie sich auf umfassende Datenerfassungsfunktionen für alle Cloud-Umgebungen und berücksichtigen Sie dabei die Auswirkungen auf die Leistung und die Speicheranforderungen. Suchen Sie nach Lösungen, die große Datenmengen in Echtzeit verarbeiten können.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Datenerhebung und -aggregation	Sammlung bei mehreren Cloud-Anbietern (AWS, Azure, GCP)		
	Datenerfassung in Echtzeit von Cloud-Workloads		
	Erfassung und Aggregation von Protokollen		
	Sammlung von Leistungskennzahlen		
	Sammeln von Konfigurationsdaten		

	Überwachung des Netzwerkverkehrs		
	Datenerhebung auf API-Ebene		

4.2 Erkennung von Bedrohungen

Tipp: Erweiterte Funktionen zur Erkennung von Bedrohungen sollten mehrere Erkennungsmethoden kombinieren, um einen umfassenden Schutz zu bieten. Ziehen Sie Lösungen in Betracht, die sowohl traditionelle signaturbasierte Erkennung als auch moderne ML-gestützte Analysen nutzen, um Fehlalarme zu minimieren und gleichzeitig hohe Erkennungsraten zu erzielen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennung von Bedrohungen	Signaturbasierte Erkennung		
	Analyse des maschinellen Lernens		
	Verhaltensanalytik		
	Scannen auf Schwachstellen		
	Erkennung von Malware		
	Erkennung von Zero-Day-Bedrohungen		
	Erkennung fortgeschrittener anhaltender Bedrohungen (APT)		

4.3 Reaktion auf Vorfälle

Tipp: Automatisierte Reaktionsmöglichkeiten auf Vorfälle sind entscheidend für die Aufrechterhaltung der Sicherheit in Cloud-Umgebungen, in denen sich Bedrohungen schnell verbreiten können. Stellen Sie sicher, dass die Lösung sowohl automatische als auch manuelle Reaktionsmöglichkeiten mit klaren Workflows und Prüfprotokollen bietet.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen

Reaktion auf Vorfälle	Automatisierte Eindämmung von Bedrohungen		
	Fähigkeiten zur Systemisolierung		
	Mechanismen zur Sperrung des Verkehrs		
	Automatisierte Abhilfe-Workflows		
	Ausführung des Playbooks für Vorfälle		
	Manuelle Antwortmöglichkeiten		
	Instrumente für die Analyse nach einem Vorfall		

4.4 Priorisierung von Alarmen

Tipp: Eine wirksame Priorisierung von Warnmeldungen ist für die Verwaltung von Sicherheitsabläufen in großem Umfang unerlässlich. Suchen Sie nach Lösungen, die intelligente Algorithmen verwenden, um die Ermüdung durch Alarme zu verringern und gleichzeitig sicherzustellen, dass kritische Bedrohungen nicht unbemerkt bleiben.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Priorisierung von Warnungen	Risikobasierte Alarmeinstufung		
	Funktionen zur Korrelation von Warnmeldungen		
	Benutzerdefinierte Warnregeln		
	Optionen zur Unterdrückung von Alarmen		
	Automatisierte Alarmtriage		

	Anreicherung des Warnungskontexts		
	Historische Alarmanalyse		

4.5 Verwaltung der Einhaltung der Vorschriften

Tipp: Umfassende Compliance-Management-Funktionen sollten sowohl standardmäßige Regelwerke als auch individuelle Compliance-Richtlinien unterstützen. Ziehen Sie Lösungen in Betracht, die die Überwachung der Einhaltung von Vorschriften und die Berichterstattung automatisieren, um den manuellen Überwachungsaufwand zu verringern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Compliance Management	Durchsetzung der Industrievorschriften		
	Funktionen zur Überwachung von Richtlinien		
	Tools für die Compliance-Berichterstattung		
	Erstellung benutzerdefinierter Richtlinien		
	Automatisierte Konformitätsprüfungen		
	Warnungen vor Verstößen gegen die Vorschriften		
	Pflege des Prüfpfads		

4.6 Skalierbarkeit

Tipp: Skalierbarkeit ist für wachsende Cloud-Umgebungen entscheidend. Evaluieren Sie Lösungen anhand ihrer Fähigkeit, sowohl horizontal als auch vertikal zu skalieren und dabei die Leistung und Effektivität aller geschützten Workloads aufrechtzuerhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Skalierbarkeit	Unterstützung für wachsendes Arbeitsvolumen		
	Cloud-übergreifende Skalierungsmöglichkeiten		
	Funktionen zur Leistungsoptimierung		
	Effizienz der Ressourcennutzung		
	Automatische Skalierungsmechanismen		
	Lastausgleichsfunktionen		
	Unterstützung mehrerer Regionen		

4.7 Integration in bestehende Systeme

Tipp: Starke Integrationsfunktionen gewährleisten, dass Ihre CWPP-Lösung nahtlos mit Ihrer bestehenden Sicherheitsinfrastruktur zusammenarbeitet. Konzentrieren Sie sich auf Standard-API-Unterstützung und vorgefertigte Integrationen mit gängigen Sicherheitstools.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Integrationsfähigkeiten	API-Integration von Sicherheitstools		
	SIEM-Integration		
	Integration der SOAR-Plattform		
	Integration des Identitätsmanagements		
	Kundenspezifische API-Entwicklungsoptionen		
	Webhook-Unterstützung		

	Unterstützung von Drittanbieter-Plugins		

4.8 Verwaltung des Datenschutzes

Tipp: Die Datenschutzfunktionen sollten sowohl den gesetzlichen Anforderungen als auch den internen Sicherheitsrichtlinien entsprechen. Ziehen Sie Lösungen in Betracht, die eine granulare Kontrolle über die Handhabung sensibler Daten und starke Verschlüsselungsfunktionen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verwaltung des Datenschutzes	Umgang mit sensiblen Daten		
	Implementierung der Verschlüsselung		
	Merkmale der Zugangskontrolle		
	Funktionen zur Datenmaskierung		
	Durchsetzung der Datenschutzbestimmungen		
	Werkzeuge zur Datenklassifizierung		
	Berichterstattung zur Einhaltung des Datenschutzes		

4.9 KI-gesteuerte Fähigkeiten

Tipp: KI-Funktionen sollten sowohl den Sicherheitsbetrieb als auch die Erkennung von Bedrohungen verbessern. Achten Sie auf Lösungen, die praktische Anwendungen von KI/ML jenseits von Marketing-Schlagwörtern mit klaren Vorteilen für die Sicherheitsergebnisse demonstrieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
KI-gesteuerte Fähigkeiten	Überwachung der AI-Arbeitslastsicherheit		

	KI-generierte Sanierungsschritte		
	Optimierung der IAM-Richtlinien		
	KI-generierte Alarmbeschreibungen		
	Intelligente Erkennung von Anomalien		
	Erkennung von AI-Modellen/Paketen		
	KI-gestützte Angriffspfadanalyse		
	AI-Bestandsmanagement		
	AI-spezifische Laufzeitrichtlinien		

5. Anforderungen an die Integration

Die CWPP-Lösung muss integriert werden:

- Endpunkt-Erkennungs- und Reaktionssysteme (EDR)
- Software für die Sicherheit von Rechenzentren
- Cloud-Management-Plattformen
- Software zur Einhaltung von Vorschriften in der Cloud

6. Aufkommende Trends

Die Anbieter müssen ihre Vorgehensweise darlegen:

- Integration von KI und maschinellem Lernen für eine verbesserte Erkennung von und Reaktion auf Bedrohungen
- Shift-Left Sicherheitspraktiken
- Integration mit Cloud Security Posture Management (CSPM)

7. Umsetzung und Unterstützung

Die Anbieter müssen detaillierte Informationen zu folgenden Punkten liefern:

- Umsetzungsprozess und Zeitplan
- Schulung und Unterstützung bei der Einarbeitung
- Laufende technische Unterstützung und SLAs
- Regelmäßige Updates und Patch-Management

8. Einhaltung der Vorschriften und Zertifizierungen

Der Anbieter muss dies angeben:

- Einschlägige Branchenzertifizierungen (z. B. ISO 27001, SOC 2)
- Einhaltung von Datenschutzbestimmungen (z. B. GDPR, CCPA)

9. Preisgestaltung und Lizenzierungsmodell

Die Anbieter müssen Folgendes bereitstellen:

- Detaillierte Preisstruktur
- Lizenzierungsmodelle (pro Benutzer, pro Arbeitslast oder unternehmensweit)
- Zusätzliche Kosten für Premiumfunktionen oder Support

10. Fallstudien und Referenzen

Die Anbieter müssen folgende Angaben machen:

- Einschlägige Fallstudien, die den Erfolg der Umsetzung des CWPP belegen
- Referenzen von Kunden in ähnlichen Branchen oder mit vergleichbaren Cloud-Umgebungen

11. Kriterien für die Bewertung

Die Vorschläge werden nach folgenden Kriterien bewertet:

- Vollständigkeit der Merkmale
- Benutzerfreundlichkeit und Verwaltung
- Skalierbarkeit und Leistung
- Integrationsfähigkeit
- KI und maschinelles Lernen

- Preisgestaltung und Gesamtbetriebskosten
- Ruf des Anbieters und Qualität des Supports

Kontaktinformationen: security@company.com

12. Zeitleiste

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