Aufforderung zur Angebotsabgabe: SSPM-Lösungen (SaaS Security Posture Management)

Inhaltsübersicht

1. Einleitung

SaaS Security Posture Management (SSPM) ist eine wichtige Lösung für Unternehmen, die sich bei ihren kritischen Operationen auf Cloud-Plattformen verlassen. Die SSPM-Software schützt Cloud-Anwendungen kontinuierlich, indem sie Schwachstellen erkennt, die Einhaltung von Vorschriften gewährleistet und das Risiko von Datendiebstahl mindert.

Mit dieser Ausschreibung sollen Angebote für eine SSPM-Lösung eingeholt werden, die einen umfassenden Schutz für die SaaS-Umgebung unserer Organisation bietet, einschließlich Zugangskontrolle, Datensicherheit, Überwachung der Einhaltung von Vorschriften und Risikobewertung.

2. Projektziele

Die Lösung muss Folgendes bieten:

- Umfassender Schutz für die SaaS-Umgebung des Unternehmens

- Robuste Zugangskontrolle und Datensicherheitsmaßnahmen
- Kontinuierliche Überwachung der Einhaltung der Vorschriften und Berichterstattung
- Integrierte Fähigkeiten zur Risikobewertung
- Nahtlose Integration in die bestehende Infrastruktur
- Skalierbarkeit zur Unterstützung des Unternehmenswachstums

3. Geltungsbereich

Der Geltungsbereich erstreckt sich auf Folgendes:

- Implementierung einer umfassenden SSPM-Lösung
- Integration in die bestehende Sicherheitsinfrastruktur
- Konfiguration und Einsatz
- Personalschulung und Wissenstransfer
- Laufende Unterstützung und Wartung
- Regelmäßige Updates und Patch-Management

4. Funktionale Anforderungen

4.1 Erkennung und Inventarisierung von SaaS-Anwendungen

Tipp: Unverzichtbare Grundlage für SSPM, das eine automatisierte, kontinuierliche Erkennung und umfassende Transparenz aller SaaS-Anwendungen erfordert, um Schatten-IT wirksam zu verhindern und die Sicherheitskontrolle aufrechtzuerhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Auffinden und Katalogisieren	Automatische Erkennung aller SaaS-Anwendungen		
	Katalogisierung und Bestandsaktualisierung in Echtzeit		

	Umfassende Transparenz zur Vermeidung von Schatten-IT		
	Klassifizierung und Einstufung von Vermögenswerten		
Inventarverwaltung	Verfolgung und Analyse der Anwendungsnutzung		
	Überwachung der Lizenznutzung		
	Konfigurationsmanagement		
	Verfolgung der Versionskontrolle		

4.2 Kontinuierliche Überwachung und Berichterstattung

Tipp: Entscheidend für die Aufrechterhaltung des Sicherheitsbewusstseins in Echtzeit durch aktive Überwachung, sofortige Erkennung von Bedrohungen und umfassende Berichtsfunktionen, die verwertbare Erkenntnisse liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Überwachung in Echtzeit	Erkennung von Sicherheitsproblemen und Warnmeldungen		
	Kontinuierliches Scannen der Umgebung		
	Leistungsüberwachung		
	Verfolgung von Konfigurationsänderungen		
Berichterstattungsfähigkeiten	Berichterstattung über die Erkennung von Anomalien		
	Anpassbare Berichterstellung		

	Stakeholder-spezifische Dashboards		
	Trendanalyse und Metriken		

4.3 Überwachung der Benutzeraktivitäten

Tipp: Die Überwachung des Nutzerverhaltens bildet den Eckpfeiler der Sicherheitsintelligenz und ermöglicht die schnelle Erkennung verdächtiger Aktivitäten und potenzieller Sicherheitsverletzungen durch Musteranalyse.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennung von Verhaltensweisen	Überwachung verdächtiger Aktivitäten in Echtzeit		
	Analyse der Benutzerzugriffsmuster		
	Festlegung von Verhaltensbasisszenarien		
	Erkennung von Anomalien		
Reaktion der Sicherheit	Rasche Identifizierung von Verstößen		
	Automatische Erzeugung von Warnmeldungen		
	Arbeitsablauf bei der Reaktion auf Vorfälle		
	Prüfpfade für Benutzeraktivitäten		

4.4 Kontrollen zur Verhinderung von Datenverlusten (DLP)

Tipp: DLP-Kontrollen müssen einen umfassenden Schutz vor versehentlichen und böswilligen Datenlecks bieten und gleichzeitig die Unternehmensproduktivität durch intelligente Richtliniendurchsetzung aufrechterhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Umsetzung der Politik	Erstellung und Verwaltung von DLP-Richtlinien		
	Identifizierung sensibler Daten		
	Automatisierung der Durchsetzung von Richtlinien		
	Erstellung benutzerdefinierter Regeln		
Datenschutz	Verhinderung ungewollter Leckagen		
	Verhinderung bösartiger Lecks		
	Klassifizierung der Daten		
	Inhaltskontrolle		

4.5 Überwachung der Einhaltung

Tipp: Die automatisierte Überwachung der Einhaltung von Vorschriften sollte die Einhaltung der gesetzlichen Bestimmungen kontinuierlich verfolgen und gleichzeitig einen klaren Überblick über den Status der Einhaltung und den Bedarf an Abhilfemaßnahmen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verfolgung der Einhaltung	Kontinuierliche Überwachung der Körperhaltung		
	Einhaltung der Industrievorschriften		
	Dashboard zum Stand der Einhaltung		
	Analyse der Lücken		
Regulatorisches Management	Rahmenspezifische Kontrollen		

	Automatisierte Compliance-Berichterstattung		
	Durchsetzung der Politik		
	Pflege des Prüfpfads		

4.6 Passwort- und Zugangsverwaltung

Tipp: Starke Kennwortrichtlinien und die Zugriffsverwaltung sollten ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit herstellen, um einen soliden Schutz vor unbefugtem Zugriff zu gewährleisten und gleichzeitig die Produktivität der Benutzer zu erhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Passwortschutz	Erkennung schwacher Passwörter		
	Analyse der Passwortstärke		
	Durchsetzung der Passwortaktualisierung		
	Einhaltung von Passwortrichtlinien		
Durchsetzung der Politik	Umsetzung strenger Passwortrichtlinien		
	Verwaltung des Ablaufs von Passwörtern		
	Durchsetzung des Passwortverlaufs		
	Regeln für die Passwortkomplexität		

4.7 Risikobewertung und -sanierung

Tipp: Risikobewertungssysteme sollten durch eine genaue Bewertung des Schweregrads und klare Abhilfemaßnahmen verwertbare Erkenntnisse liefern,

damit sich Unternehmen zuerst auf die kritischsten Sicherheitsprobleme konzentrieren können.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Risikobewertung	Analyse des Schweregrads von Sicherheitsrisiken		
	Risikobewertung in Echtzeit		
	Bewertung der Anfälligkeit		
	Priorisierung von Bedrohungen		
Sanierung	Automatisierte Anleitung zur Abhilfe		
	Priorisierung der Maßnahmen		
	Verwaltung des Sanierungs-Workflows		
	Überprüfung der Sanierung		

4.8 Integrationsfähigkeiten

Tipp: Die Integrationsfunktionen sollten eine nahtlose Verbindung mit der bestehenden Sicherheitsinfrastruktur ermöglichen und gleichzeitig so flexibel sein, dass sie an neue Anwendungen und sich verändernde Sicherheitsanforderungen angepasst werden können.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
SaaS-Integration	Nahtlose Anwendungsintegration		
	API-basierte Konnektivität		
	Unterstützung für benutzerdefinierte Integration		
	Datensynchronisierung in Echtzeit		

Anpassungsfähigkeit	Unterstützung neuer Anwendungen		
	Skalierbarkeit der Integration		
	Plattformübergreifende Kompatibilität		
	Überwachung der Integration		

4.9 Zugangskontrolle durch Dritte

Tipp: Die Verwaltung des Zugriffs von Drittanbietern erfordert eine granulare Kontrolle und kontinuierliche Überwachung, um Sicherheitsrisiken zu minimieren und gleichzeitig notwendige Geschäftsbeziehungen aufrechtzuerhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Zugang Sichtbarkeit	Anwendungsüberwachung durch Dritte		
	Verfolgung der Zugangsberechtigung		
	Analyse der Nutzung		
	Risikobewertung		
Zugangsverwaltung	Verwaltung von Genehmigungen		
	Funktionen zum Entzug des Zugangs		
	Automatisierung der Zugangsprüfung		
	Lebenszyklusmanagement für den Anbieterzugang		

4.10 Sicherheitsinspektionen

Tipp: Umfassende Sicherheitsinspektionen sollten alle Aspekte der Sicherheitslage abdecken und gleichzeitig die Einhaltung der einschlägigen Vorschriften und Industrienormen gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Zugangskontrolle	Überprüfung der Zugangspolitik		
	Erlaubnisprüfung		
	Rollenbasierte Zugriffsüberprüfung		
	Überprüfung der Authentifizierung		
Datenschutz	DLP-Prüfung		
	Antiviren-Scannen		
	Überprüfung der Verschlüsselung		
	Einhaltung der Datenverarbeitung		

4.11 Automatisierte Abhilfemaßnahmen

Tipp: Automatisierte Abhilfemaßnahmen sollten manuelle Eingriffe auf ein Minimum reduzieren und gleichzeitig Genauigkeit und klare Prüfprotokolle aller automatisierten Aktionen gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Automatisierung	Beseitigung von Fehlkonfigurationen		
	Durchsetzung der Politik		
	Bereitstellung von Sicherheitspatches		
	Standardisierung der Konfiguration		

Management von Warnmeldungen	Erzeugung von Warnmeldungen löschen		
	Reduzierung von Falsch-Positiven		
	Priorisierung von Warnungen		
	Verfolgung von Sanierungsmaßnahmen		

4.12 Skalierbarkeit

Tipp: Skalierbarkeitsfunktionen sollten eine konsistente Leistung und Sicherheit gewährleisten, wenn das Unternehmen wächst, und eine erhöhte Last ohne Beeinträchtigung der Effektivität bewältigen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Unterstützung des Wachstums	Erweiterung der Anwendungsbasis		
	Verwaltung des Benutzervolumens		
	Wartung der Leistung		
	Optimierung der Ressourcen		
Umwelt Anpassung	Skalierung der Cloud-Umgebung		
	Flexibilität der Infrastruktur		
	Lastausgleich		
	Kapazitätsplanung		

4.13 API-Sicherheit

Tipp: Die API-Sicherheit muss eine sichere Datenübertragung gewährleisten und gleichzeitig eine umfassende Überwachung und Kontrolle über alle API-Interaktionen sicherstellen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Zugangskontrolle	Überwachung des API-Zugangs		
	Durchsetzung der Authentifizierung		
	Verwaltung von Berechtigungen		
	Ratenbegrenzung		
Datensicherheit	Durchsetzung der Politik zur gemeinsamen Nutzung von Daten		
	Verschlüsselung des Verkehrs		
	Validierung der Daten		
	Sicherheitstests		

4.14 Maschinelles Lernen und KI-Integration

Tipp: KI-/ML-Funktionen sollten die Erkennung und Abwehr von Bedrohungen verbessern und gleichzeitig durch erweiterte Analysen und Mustererkennung verwertbare Erkenntnisse liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennung von Bedrohungen	ML-gestützte Erkennung		
	Mustererkennung		
	Verhaltensanalyse		
	Prädiktive Analytik		
Prävention	Identifizierung neu auftretender Bedrohungen		
	Automatisierte Antwort		
	Risikovorhersage		

	Kontinuierliches Lernen		

4.15 Automatisierung der Einhaltung von Vorschriften

Tipp: Die Automatisierung der Einhaltung von Vorschriften sollte die Einhaltung mehrerer gesetzlicher Vorschriften optimieren und gleichzeitig für eine genaue Dokumentation und einen Nachweis der Einhaltung sorgen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Berichterstattung	Automatisierte Compliance-Berichterstattung		
	Rahmenspezifische Vorlagen		
	Erstellung benutzerdefinierter Berichte		
	Sammlung von Beweismitteln		
Standard-Management	Vorkonfigurierte Compliance-Einstellungen		
	Behebung von Lücken		
	Kontrolle des Mappings		
	Überwachung der Einhaltung		

4.16 KI-gestützte Risikobewertung

Tipp: Eine KI-gesteuerte Risikobewertung sollte tiefe Einblicke in die Sicherheitslage bieten und gleichzeitig genau sein und klare Anleitungen für Abhilfemaßnahmen liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Risikoanalyse	Risikobewertung von Drittanbieter-Apps		
	Bewertung von Browser-Erweiterungen		

	Automatisierung der Risikobewertung		
	Priorisierung von Bedrohungen		
Bewertung Berichterstattung	Automatisierte Risikoberichte		
	Analyse der Einhaltung von Sicherheitsvorschriften		
	Risikotrends		
	Empfehlungen zur Abhilfe		

4.17 Verwaltung von KI-Sicherheitsvorkehrungen

Tipp: AI-SPM sollte umfassende Transparenz und Schutz für KI-Ressourcen bieten und gleichzeitig detaillierte Bestands- und Sicherheitskontrollen ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI-Sichtbarkeit	Verfolgung des Einsatzes von Modellen		
	Projektüberwachung		
	Erkennung von Risiken		
	Zugangskontrolle		
Vermögensverwaltung	AI-Bestandspflege		
	Stücklistenverwaltung		
	Verfolgung der Konfiguration		
	Bewertung der Sicherheit		

4.18 KI-Modell Sicherheit

Tipp: Die Sicherheit von KI-Modellen sollte einen umfassenden Schutz von Modellkonfigurationen und -daten gewährleisten und gleichzeitig strenge Zugriffskontrollen und Überwachungen vorsehen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Konfiguration Sicherheit	Implementierung der Netzsicherheit		
	Maßnahmen zum Schutz der Daten		
	Verwaltung der Zugangskontrolle		
	Audit der Modellkonfiguration		
Überwachung	Überwachung der Zugangstasten		
	Erkennung sensibler Daten		
	Verfolgung der Nutzung		
	Sicherheitswarnungen		

4.19 GenAI App Management

Tipp: Das GenAI-Anwendungsmanagement sollte Kontrolle und Sicherheit auf Unternehmensniveau bieten und gleichzeitig die Flexibilität für die legitime geschäftliche Nutzung erhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Kontoführung	Konfiguration des Unternehmenskontos		
	Benutzerzugangskontrolle		
	Leitung der Gruppe		
	Durchsetzung der Politik		

Sicherheitskontrollen	Verwaltung von Authentifizierungsrichtlinien		
	MFA-Implementierung		
	Überwachung der Nutzung		
	Zugang zu Bewertungen		

4.20 Benutzerdefiniertes GPT und Plugin-Verwaltung

Tipp: Die benutzerdefinierte GPT-Verwaltung sollte eine sichere Erstellung und Bereitstellung ermöglichen und gleichzeitig eine strenge Kontrolle über die Integration von Drittanbietern und den Zugriff auf den Marktplatz gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
GPT-Verwaltung	Unterstützung für die Erstellung benutzerdefinierter GPTs		
	Plugin-Verwaltung		
	Versionskontrolle		
	Sicherheitsprüfung		
Zugangskontrolle	Marktplatz-Zugangsverwaltung		
	Plugin-Autorisierung		
	Nutzungsbeschränkungen		
	Durchsetzung der Politik		

5. Zusätzliche Überlegungen

5.1 Integration in die bestehende Infrastruktur

- Beschreibung der Integrationsmethoden
- Unterstützte Plattformen und Systeme
- API-Dokumentation

- Zeitplan für die Integration

5.2 Benutzererfahrung und Benutzerfreundlichkeit

- Schnittstellengestaltung
- Anforderungen an die Ausbildung
- Administrative Kontrollen
- Optimierung des Benutzer-Workflows

5.3 Skalierbarkeit und Leistung

- Unterkunft mit Wachstum
- Leistungsmetriken
- Anforderungen an die Ressourcen
- Kapazitätsplanung

5.4 Unterstützung und Wartung

- Optionen zur Unterstützung
- Reaktionszeiten
- Häufigkeit der Aktualisierung
- Wartungsfenster

5.5 Preismodell

- Lizenzstruktur
- Kosten der Durchführung
- Laufende Wartungsgebühren
- Zusätzliche Kosten für Dienstleistungen

5.6 Einhaltung von Vorschriften und Zertifizierungen

- Industrie-Zertifizierungen
- Rahmen für die Einhaltung der Vorschriften
- Audit-Unterstützung

- Regulatorische Anforderungen

5.7 Berichterstattung und Analyse

- Standardberichte
- Benutzerdefinierte Berichte
- Analytische Fähigkeiten
- Anpassung des Dashboards

5.8 Privatsphäre und Datenschutz

- Verfahren zur Datenverarbeitung
- Datenschutz-Kontrollen
- Aufenthaltsort der Daten
- Verschlüsselungsmethoden

6. Kriterien für die Bewertung

Die Vorschläge werden nach folgenden Kriterien bewertet:

1. Vollständigkeit der Lösung
2. Integrationsfähigkeit
3. Kompatibilität des Systems
4. Benutzerfreundlichkeit
5. Anforderungen an die Ausbildung
6. Metriken zur Skalierbarkeit
7. Leistungsmaßstäbe
8. Unterstützungsangebote
9. Gesamtbetriebskosten
10. Erfahrung des Anbieters
11. Ansehen auf dem Markt

7. Anweisungen zur Einreichung

Die Anbieter müssen Folgendes bereitstellen:

1. Detaillierte Beschreibung der Lösung
2. Technische Daten
3. Durchführungsplan
4. Ausbildungsansatz
5. Details zur Unterstützung
6. Struktur der Preisgestaltung
7. Profil des Unternehmens
8. Kundenreferenzen
9. Beispielhafte Dokumentation
10. Zeitplan des Projekts

8. Zeitleiste

- RFP-Freigabedatum:
- Frist für Anfragen:
- Fälligkeitsdatum des Vorschlags:
- Präsentationen von Anbietern:
- Endgültige Auswahl:
- Projekt Kickoff:

9. Kontaktinformationen

Bei Fragen zu dieser Ausschreibung wenden Sie sich bitte an:

Ende des RFP-Dokuments