Aufforderung zur Angebotsabgabe: Application Security Posture Management (ASPM) Software-Lösung

Inhaltsübersicht

1. Einleitung und Hintergrund

1.1 Überblick über die Organisation

[Geben Sie folgende Informationen über Ihre Organisation an:]

- Kurze Beschreibung Ihrer Firma/Organisation

- Industriesektor und spezifische regulatorische Anforderungen
- Größe der Organisation und Umfang der IT-Infrastruktur
- Geografische Präsenz und Standorte

1.2 Aktuelles Umfeld

- Beschreibung der bestehenden Sicherheitsinfrastruktur
- Anzahl und Arten von Endpunkten
- Aktuelle Herausforderungen und Problembereiche
- Integrationspunkte und Abhängigkeiten
- Aktuelle Sicherheitslage

1.3 Projektkontext

- Wirtschaftliche Triebkräfte für diese Initiative
- Strategische Ziele
- Wichtige Interessengruppen
- Kritische Erfolgsfaktoren
- Projektbeschränkungen und Annahmen

2. Projektziele

2.1 Primäre Zielsetzungen

- Verbessertes Management der Sicherheitslage
- Verbesserte Erkennung von und Reaktion auf Bedrohungen
- Rationalisierte Sicherheitsabläufe
- Einhaltung der Vorschriften
- Kostenoptimierung

2.2 Spezifische Ziele

- [Auflistung spezifischer, messbarer Ziele]
- [Einschließlich zeitlich festgelegter Ziele]

- [Detaillierte Ziele in Bezug auf die Einhaltung der Vorschriften]
- [Angabe der operativen Effizienzziele]

2.3 Erfolgskriterien

- Leistungsmetriken
- Metriken zur Sicherheit
- Operative Metriken
- Metriken zum Geschäftswert
- ROI-Erwartungen

3. Umfang der Arbeit

3.1 Komponenten der Lösung

- Implementierung einer Sicherheitsplattform
- Integration in bestehende Systeme
- Anforderungen an die Datenmigration
- Ausbildung und Wissenstransfer
- Anforderungen an die Dokumentation

3.2 Phasen der Umsetzung

1. Entdeckung und Planung
    - Validierung der Anforderungen
    - Architekturentwurf
    - Planung der Durchführung
2. Entwurf und Konfiguration
    - Konfiguration des Systems
    - Entwicklung der Politik
    - Gestaltung der Integration

3. Pilot-Einsatz
    - Begrenzter Einsatz
    - Prüfung und Validierung
    - Benutzerakzeptanztests
4. Vollständige Markteinführung
    - Einsatz in der Produktion
    - Benutzerschulung
    - Überprüfung des Systems
5. Nach der Einführung
    - Übergang unterstützen
    - Leistungsüberwachung
    - Optimierung

3.3 Liefergegenstände

- Software und Lizenzen
- Implementierung von Dienstleistungen
- Dokumentation
- Schulungsunterlagen
- Unterstützungsdienste

4. Technische Anforderungen

4.1 Plattform-Architektur

- Anforderungen an die Skalierbarkeit
- Hochverfügbarkeitsdesign
- Leistungsspezifikationen
- Anforderungen an die Infrastruktur

- Fähigkeiten zur Datenverwaltung

4.2 Sicherheitsmerkmale

4.2.1 Zentrale Sicherheitsfunktionen

- Endpunktschutz
- Sicherheit der Anwendung
- Sicherheit im Netz
- Sicherheit in der Cloud
- Sicherheit der Daten

4.2.2 Erweiterte Sicherheitsfunktionen

- Integration von Bedrohungsdaten
- Verhaltensanalyse
- Zero-Day-Schutz
- Automatisierte Antwortmöglichkeiten
- Forensik und Ermittlungsinstrumente

4.3 KI- und maschinelle Lernfähigkeiten

- Prädiktive Sicherheitsanalytik
- Automatisierte Erkennung von Bedrohungen
- Intelligente Antwortautomatisierung
- Mustererkennung
- Erkennung von Anomalien

4.4 Verwaltung und Kontrolle

- Zentralisierte Verwaltungskonsole
- Verwaltung der Politik
- Konfigurationsmanagement
- Vermögensverwaltung

- Fernverwaltungsfunktionen

5. Funktionale Anforderungen

5.1 Erkennung und Inventarisierung von Anwendungen

Die Erkennung von Anwendungen und die Bestandsverwaltung bilden die Grundlage für Ihre Sicherheitslage. Ein robustes Erkennungssystem stellt sicher, dass keine Anwendung oder Anlage unüberwacht bleibt, während eine umfassende Bestandsverwaltung einen klaren Überblick über Ihre gesamte Anwendungslandschaft bietet.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Entdeckung von Vermögenswerten	Automatische Anwendungserkennung		
	Kartierung der Infrastruktur		
	Erkennung von Cloud-Ressourcen		
	Scannen von Containerregistern		
	Zuordnung von Dienstabhängigkeiten		
Vermögensverwaltung	Kategorisierung von Anwendungen		
	Versionsverfolgung		
	Kartierung der Umwelt		
	Lebenszyklus-Management		
	Konfigurationsmanagement		

5.2 Bewertung der Sicherheit

Die Fähigkeiten zur Sicherheitsbewertung bestimmen, wie effektiv Ihr Unternehmen potenzielle Schwachstellen erkennen und bewerten kann. Ein

umfassender Bewertungsansatz, der mehrere Testmethoden kombiniert, gewährleistet eine gründliche Abdeckung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Scannen auf Schwachstellen	Automatisierte Sicherheitsüberprüfung		
	Benutzerdefinierte Scan-Konfigurationen		
	Zeitplanungsfunktionen		
	Verwaltung der Ergebnisse		
	Verwaltung der Scan-Richtlinien		
Sicherheitsprüfung	SAST-Integration		
	DAST-Fähigkeiten		
	IAST-Unterstützung		
	API-Sicherheitstests		
	Prüfung der Sicherheit mobiler Anwendungen		

5.3 Risikomanagement

Ein effektives Risikomanagement kombiniert eine robuste Schwachstellenerkennung mit ausgefeilten Analysen, um Sicherheitsprobleme zu priorisieren und anzugehen. So wird sichergestellt, dass Ressourcen effizient zugewiesen werden und sich die Sicherheitsmaßnahmen auf kritische Bedrohungen konzentrieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Schwachstellen-Management	Erkennung und Klassifizierung		
	Priorisierung der Risiken		

	Verfolgung und Lebenszyklusmanagement		
	Behandlung von Fehlalarmen		
	Arbeitsablauf bei der Sanierung		
Risiko-Analytik	Risikobewertungssysteme		
	Trendanalyse		
	Metriken und KPIs		
	Historische Analyse		
	Prädiktive Analytik		

5.4 Verwaltung von Richtlinien

Die Richtlinienverwaltung sorgt für konsistente Sicherheitspraktiken bei gleichzeitiger Einhaltung der einschlägigen Normen. Starke Richtlinienkontrollen in Kombination mit automatisierten Konformitätsprüfungen schaffen einen robusten Rahmen für die Sicherheitsverwaltung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Politische Verwaltung	Erstellung und Verwaltung von Richtlinien		
	Vorlagenbibliothek		
	Versionskontrolle		
	Behandlung von Ausnahmen		
	Durchsetzung der Politik		
Compliance Management	Abbildung des Rahmens		

	Automatisierte Überprüfung der Einhaltung der Vorschriften		
	Sammlung von Beweismitteln		
	Möglichkeiten der Berichterstattung		
	Audit-Unterstützung		

5.5 KI- und maschinelle Lernfähigkeiten

KI- und ML-Funktionen ermöglichen eine fortschrittliche Erkennung von Bedrohungen, automatische Reaktionen und intelligente Entscheidungshilfen. Diese Technologien verbessern die Sicherheitsabläufe durch vorausschauende Analysen und Automatisierung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Vorhersage der Bedrohung	ML-basierte Erkennung von Bedrohungen		
	Mustererkennung		
	Verhaltensanalyse		
	Modelle zur Risikovorhersage		
	Systeme zur Aufdeckung von Anomalien		
	Analyse historischer Daten		
	Prädiktive Schwachstellenbewertung		
	Vorhersage der Angriffsfläche		
Intelligente Analyse	Kontextabhängige Sicherheitsanalyse		

	Automatisierte Folgenabschätzung		
	Intelligente Korrelations-Engines		
	Dynamische Risikoeinstufung		
	Adaptive Lernsysteme		
Intelligente Sanierungsmaßnahmen	Automatisierte Korrekturvorschläge		
	Kontextabhängige Prioritätensetzung		
	Intelligentes Workflow-Routing		
	Automatisierung der Wirkungsanalyse		
	Aus Sanierungsmustern lernen		
	Vorschläge zur Korrektur des Codes		
	Empfehlungen für bewährte Verfahren		
	Analyse der Erfolgsmuster		
Automatisierte Prüfung	KI-gesteuerte Testerstellung		
	Intelligente Optimierung der Abdeckung		
	Zuweisung von Ressourcen		
	Analyse der Ergebnisse		

	Progressives Lernen		
	Adaptive Prüfstrategien		
	Priorisierung von Testfällen		
	Automatisierte Validierung		

5.6 Natürliche Sprachverarbeitung und autonome Operationen

NLP und autonome Operationen ermöglichen intelligente Systeminteraktion und selbstoptimierende Sicherheitskontrollen. Diese Funktionen rationalisieren den Betrieb und verbessern die Systemeffizienz im Laufe der Zeit.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Dokumentation Analyse	Analyse der Sicherheitsanforderungen		
	Auslegung der Politik		
	Bearbeitung von Compliance-Dokumenten		
	Intelligente Dokumentationserstellung		
	Kontextabhängige Suche		
	Semantische Analyse		
	Extraktion von Wissen		
	Automatisierte Kategorisierung		
Intelligente Interaktion	Abfragen in natürlicher Sprache		
	Kontextabhängige Antworten		
	Intelligente Filterung		

	Semantische Suche		
	Optimierung von Abfragen		
	Absichtserkennung		
	Automatisierte Aktualisierungen der Wissensdatenbank		
	Generierung von Antworten		
Selbstlernende Systeme	Dynamische Regelanpassung		
	Automatisierte Verfeinerung der Richtlinien		
	Selbstoptimierende Steuerung		
	Kontinuierliche Verbesserung		
	Mustererkennung		
	Verhaltensanalyse		
	Erkennung von Anomalien		
	Anpassungsfähige Antworten		
Workflow-Intelligenz	Intelligente Weiterleitung von Aufgaben		
	Vorrangige Optimierung		
	Zuweisung von Ressourcen		
	Prozessautomatisierung		
	Aus Mustern lernen		
	Optimierung der Effizienz		
	Automatisierte Orchestrierung		

	Unterstützung der Entscheidung		

5.7 Berichterstattung und Analyse

Umfassende Berichts- und Analysefunktionen liefern verwertbare Erkenntnisse und ermöglichen eine datengestützte Entscheidungsfindung. Diese Tools unterstützen sowohl das operative Management als auch die strategische Planung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erstellung von Berichten	Anpassbare Vorlagen		
	Planmäßige Berichterstattung		
	Interaktive Dashboards		
	Exportmöglichkeiten		
	Visualisierung von Daten		
Analytische Merkmale	Trendanalyse		
	Leistungsmetriken		
	Benutzerdefinierte Analysen		
	Benchmarking		
	Prädiktive Analyse		

6. Operative Anforderungen

6.1 Leistungsanforderungen

- Angaben zur Reaktionszeit
- Anforderungen an den Durchsatz
- Metriken zur Skalierbarkeit
- Nutzung der Ressourcen
- Kapazitätsplanung

6.2 Verfügbarkeit und Verlässlichkeit

- Anforderungen an die Betriebszeit
- Failover-Fähigkeiten
- Sicherung und Wiederherstellung
- Wiederherstellung im Katastrophenfall
- Geschäftskontinuität

6.3 Bereitstellungsoptionen

- Einsatz in der Cloud
- Vor-Ort-Installation
- Hybride Konfigurationen
- Multi-Cloud-Unterstützung
- Container-Einsatz

7. Anforderungen an die Integration

7.1 Erforderliche Integrationen

- SIEM-Systeme
- ITSM-Werkzeuge
- Verzeichnisdienste
- Cloud-Plattformen
- Entwicklungswerkzeuge

7.2 API und Interoperabilität

- API-Spezifikationen
- Integrationsprotokolle
- Formate für den Datenaustausch
- Authentifizierungsmethoden
- Individuelle Integrationsmöglichkeiten

8. Sicherheits- und Compliance-Anforderungen

8.1 Sicherheitsstandards

- Industrie-Zertifizierungen
- Sicherheitsprotokolle
- Rahmen für die Einhaltung der Vorschriften
- Anforderungen an den Datenschutz
- Datenschutz-Standards

8.2 Anforderungen an die Einhaltung

- Einhaltung von Vorschriften
- Industrienormen
- Interne Politikbereiche
- Audit-Anforderungen
- Anforderungen an die Berichterstattung

9. Anforderungen an Support und Service

9.1 Unterstützungsdienste

- Supportstufen und SLAs
- Management von Zwischenfällen
- Management von Problemen
- Eskalationsverfahren
- Zugang zur Wissensdatenbank

9.2 Freiberufliche Dienstleistungen

- Implementierung von Dienstleistungen
- Ausbildungsprogramme
- Beratungsdienste
- Anpassungsdienste

- Verwaltete Dienste

10. Qualifikationen des Anbieters

10.1 Unternehmensprofil

- Geschichte des Unternehmens
- Finanzielle Stabilität
- Marktpräsenz
- Kundenstamm
- Anerkennung durch die Industrie

10.2 Erfahrung und Fachwissen

- Ähnliche Implementierungen
- Fachwissen über die Industrie
- Technische Fähigkeiten
- Unterstützung der Infrastruktur
- Erfolgsbilanz der Innovation

11. Kriterien für die Bewertung

11.1 Technische Bewertung (40%)

- Vollständigkeit der Merkmale
- Technische Architektur
- Leistungsfähigkeiten
- Integrationsfähigkeit
- Sicherheitsmerkmale

11.2 Funktionale Bewertung (25%)

- Benutzererfahrung
- Möglichkeiten der Verwaltung
- Berichterstattung und Analyse

- Merkmale der Automatisierung
- Anpassungsmöglichkeiten

11.3 Bewertung des Anbieters (20%)

- Stabilität des Unternehmens
- Marktstellung
- Referenzprüfungen
- Fähigkeit zur Unterstützung
- Innovationspotenzial

11.4 Kommerzielle Bewertung (15%)

- Gesamtbetriebskosten
- Preismodell
- Zahlungsbedingungen
- Vertragsbedingungen
- Gutes Preis-Leistungs-Verhältnis

12. Leitlinien für die Einreichung

12.1 Format des Vorschlags

1. Zusammenfassung
2. Firmenprofil
3. Technische Antwort
4. Ansatz für die Umsetzung
5. Details zur Preisgestaltung
6. Referenzen
7. Unterstützende Dokumentation

12.2 Antwortanforderungen

- Punkt für Punkt Antwort auf die Anforderungen

- Belege und Dokumentation
- Kundenreferenzen
- Beispiele für Leistungen
- Profile der Projektteams

13. Zeitplan und Prozess

13.1 Wichtige Daten

- RFP Freigabe: [Datum]
- Einsendeschluss: [Datum]
- Antwort auf Fragen: [Datum]
- Fälligkeitsdatum des Vorschlags: [Datum]
- Präsentationen des Anbieters: [Datumsbereich]
- Auswahlentscheidung: [Datum]
- Projektbeginn: [Datum]

13.2 Auswahlverfahren

1. Bewertung des Vorschlags
2. Auswahl für die Auswahlliste
3. Präsentationen von Anbietern
4. Referenzkontrollen
5. Endgültige Auswahl

14. Kommerzielle Bedingungen

14.1 Preisstruktur

- Lizenzkosten
- Kosten der Durchführung
- Kosten der Unterstützung

- Ausbildungskosten
- Zusätzliche Dienstleistungen

14.2 Zahlungsbedingungen

- Zahlungsplan
- Meilensteinzahlungen
- Wiederkehrende Kosten
- Zusätzliche Gebühren
- Bedingungen und Konditionen

15. Kontaktinformationen

15.1 Hauptansprechpartner

[Name] [Titel] [E-Mail] [Telefon]

15.2 Anweisungen zur Einreichung

[Spezifische Einreichungsanforderungen und -kanäle angeben]