Aufforderung zur Angebotsabgabe: Cloud Detection and Response (CDR) Software-Lösung

Inhaltsübersicht

1. Einleitung und Hintergrund

Unsere Organisation bittet um Angebote für eine umfassende Cloud Detection and Response (CDR)-Softwarelösung zur Verbesserung unserer Cloud-Sicherheitsinfrastruktur. Diese Ausschreibung umreißt die Anforderungen an ein robustes System, das kontinuierliche Überwachung, Bedrohungserkennung und automatisierte Reaktionsmöglichkeiten in Multi-Cloud-Umgebungen bietet.

2. Projektziele

1. Implementierung einer umfassenden Cloud-Sicherheitsüberwachung und -Reaktion:
    - Erkennung von und Reaktion auf Bedrohungen in Echtzeit
    - Kontinuierliche Überwachung von Cloud-Umgebungen
    - Automatisiertes Auditing und Compliance-Management

- Verbesserte Transparenz in einer Multi-Cloud-Infrastruktur

2. Verbesserung der Sicherheitslage durch:
    - Erweiterte Erkennung von Bedrohungen durch KI und maschinelles Lernen
    - Automatisierte Reaktion auf erkannte Bedrohungen
    - Proaktive Risikobewertung und -minderung
    - Umfassende Verwaltung und Durchsetzung von Richtlinien
3. Sicherstellung der Einhaltung von Vorschriften durch:
    - Automatisierte Überwachung der Einhaltung von Vorschriften und Berichterstattung
    - Durchsetzung von Richtlinien über Cloud-Ressourcen hinweg
    - Rationalisierte Prüfungsverfahren
    - Verfolgung des Konformitätsstatus in Echtzeit
4. Verbesserung der betrieblichen Effizienz durch:
    - Integration in bestehende Sicherheitstools und -prozesse
    - Automatisierte Antwortmöglichkeiten
    - Optimierte Zusammenarbeit zwischen Sicherheits- und Entwicklungsteams
    - Geringere Ermüdung durch intelligente Priorisierung von Alarmen

3. Umfang der Arbeit

Der ausgewählte Anbieter wird für folgende Aufgaben verantwortlich sein:

1. Implementierung der CDR-Lösung:
    - Einsatz in allen Cloud-Umgebungen
    - Integration mit bestehenden Sicherheitswerkzeugen
    - Konfiguration von Überwachung und Alarmierung

- Einrichtung von automatischen Antwortmöglichkeiten

2. Datenerhebung und -analyse:
    - Implementierung der Datenerfassung aus allen Cloud-Quellen
    - Konfiguration von Analysewerkzeugen und Algorithmen
    - Einrichtung von Berichten und Dashboards
    - Integration in bestehende Protokollierungssysteme
3. Richtlinien- und Compliance-Management:
    - Umsetzung von Compliance-Rahmenwerken
    - Konfiguration der Richtliniendurchsetzung
    - Einrichtung einer automatisierten Rechnungsprüfung
    - Integration mit bestehenden Compliance-Tools
4. Ausbildung und Wissenstransfer:
    - Schulung von Administratoren für die Systemverwaltung
    - Schulung des Sicherheitsteams zur Reaktion auf Bedrohungen
    - Dokumentation von Prozessen und Verfahren
    - Laufende Unterstützung und Anleitung zur Wartung

4. Technische Anforderungen

1. Cloud-Integration:
    - Unterstützung für die wichtigsten Cloud-Anbieter (AWS, Azure, GCP)
    - Agentenlose Überwachungsfunktionen
    - API-basierte Integration
    - Multi-Cloud-Verwaltungskonsole
2. Erkennung von Bedrohungen:
    - KI und auf maschinellem Lernen basierende Erkennung

- Signaturbasierte Erkennung
- Verhaltensanalyse
- Erkennung von Anomalien
- Analyse des Benutzer- und Entitätsverhaltens

3. Antwort Automatisierung:
    - Automatisierte Playbooks zur Reaktion auf Bedrohungen
    - Anpassbare Antwortaktionen
    - Integration mit bestehenden Sicherheitswerkzeugen
    - Automatisierte Abhilfemöglichkeiten
4. Management der Einhaltung von Vorschriften:
    - Vorgefertigte Rahmenwerke für die Einhaltung von Vorschriften
    - Erstellung benutzerdefinierter Richtlinien
    - Automatisierte Überwachung der Einhaltung der Vorschriften
    - Erstellung von Prüfpfaden
5. Berichte und Analysen:
    - Dashboards in Echtzeit
    - Anpassbare Berichte
    - Integration von Bedrohungsdaten
    - Analytische Risikobewertung

5. Funktionale Anforderungen

1. Datenerhebung und Aggregation

Tipp: Eine umfassende Datenerfassung ist für die Wirksamkeit der CDR von grundlegender Bedeutung. Konzentrieren Sie sich auf die Bewertung der Breite der Datenquellen, der Tiefe der erfassten Informationen und der Effizienz der Aggregationsmethoden. Berücksichtigen Sie sowohl Echtzeit-

Funktionen als auch die Speicherung historischer Daten, um einen vollständigen Überblick über Ihre Cloud-Umgebung zu gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Datenquellen	Integration von Cloud-Protokollen		
	Überwachung des Netzwerkverkehrs		
	Verfolgung von Endpunktaktivitäten		
	Integration benutzerdefinierter Quellen		
Datenverarbeitung	Verarbeitung in Echtzeit		
	Analyse historischer Daten		
	Normalisierung der Daten		
	Extraktion von Metadaten		
Integration	API-Kompatibilität		
	Plattformübergreifende Unterstützung		

2. Erweiterte Erkennung von Bedrohungen

Tipp: Moderne Bedrohungserkennung erfordert eine ausgeklügelte Mischung aus traditionellen und KI-gestützten Methoden. Bewerten Sie die Fähigkeit der Lösung, bekannte Bedrohungen zu erkennen und sich gleichzeitig an neue Angriffsmuster anzupassen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennungsmethoden	Signaturbasierte Erkennung		
	Algorithmen für maschinelles Lernen		

	Verhaltensanalyse		
	Erkennung von Anomalien		
Arten von Bedrohungen	Zero-Day-Bedrohungen		
	Fortgeschrittene hartnäckige Bedrohungen		
	Insider-Bedrohungen		
	Cloud-spezifische Angriffe		
Geheimdienst	Integration von Bedrohungsdaten		
	Erstellung benutzerdefinierter Regeln		

3. Reaktion auf Vorfälle

Tipp: Bei einer effektiven Reaktion auf Vorfälle muss ein Gleichgewicht zwischen Automatisierung und menschlicher Aufsicht bestehen. Konzentrieren Sie sich auf anpassbare Reaktionspläne, die mit Ihren Sicherheitsverfahren übereinstimmen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Automatisierung	Fähigkeiten zur Systemisolierung		
	Verkehrsbehinderung		
	Sammlung von Beweismitteln		
	Abhilfemaßnahmen		
Antwort-Management	Spielbuch-Anpassung		
	Prioritätsbasierte Bearbeitung		

	Eskalationsverfahren		
	Aktion Rollback-Fähigkeit		
Integration	Integration von Sicherheitstools		
	Automatisierung von Arbeitsabläufen		

4. Priorisierung von Warnungen

Tipp: Ein effektives Alarmmanagement ist entscheidend, um das Rauschen zu reduzieren und sicherzustellen, dass kritische Bedrohungen sofortige Aufmerksamkeit erhalten. Konzentrieren Sie sich auf intelligente Priorisierungsfunktionen und die Integration in bestehende Arbeitsabläufe.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Priorisierungsmaschine	KI-gesteuerte Prioritätensetzung		
	Risikobasiertes Scoring		
	Bewusstsein für den Kontext		
	Benutzerdefinierte Priorisierungsregeln		
Management von Warnmeldungen	Reduzierung von Falsch-Positiven		
	Alert-Korrelation		
	Unterdrückung von Alarmen		
	Automatisierte Triage		
Integration von Arbeitsabläufen	Integration des Fahrscheinsystems		

	Regeln für Mannschaftsmeldungen		

5. Compliance Management

Tipp: Das Compliance-Management erfordert sowohl eine proaktive Überwachung als auch eine automatische Durchsetzung. Suchen Sie nach Lösungen, die sich an sich ändernde gesetzliche Anforderungen anpassen und umfassende Prüfprotokolle liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Politischer Rahmen	Regulatorische Standardvorlagen		
	Erstellung benutzerdefinierter Richtlinien		
	Durchsetzung der Politik		
	Verwaltung von Ausnahmen		
Überwachung	Konformitätsprüfungen in Echtzeit		
	Bewertung der Konfiguration		
	Verfolgung von Änderungen		
	Erkennung von Verstößen		
Berichterstattung	Dashboards zur Einhaltung der Vorschriften		
	Erstellung von Prüfprotokollen		

6. Skalierbarkeit

Tipp: Die Skalierbarkeit sollte sowohl das horizontale Wachstum als auch die vertikale Komplexität berücksichtigen. Bewerten Sie die Fähigkeit der Lösung, die Leistung aufrechtzuerhalten, wenn Ihre Umgebung wächst, und gleichzeitig neue Funktionen und Anforderungen zu unterstützen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Leistungsskalierung	Fähigkeit zur Lastaufnahme		
	Optimierung der Ressourcen		
	Multi-Cloud-Unterstützung		
	Verteilte Verarbeitung		
Architektur	Modularer Aufbau		
	Hohe Verfügbarkeit		
	Wiederherstellung im Katastrophenfall		
	Geografische Verteilung		
Verwaltung	Zentralisierte Verwaltung		
	Unterstützung von mehreren Mandanten		

7. Integration in bestehende Systeme

Tipp: Die Integrationsfunktionen sollten über die grundlegende API-Konnektivität hinausgehen und auch die Automatisierung von Arbeitsabläufen und die Datensynchronisierung umfassen. Berücksichtigen Sie sowohl den aktuellen als auch den zukünftigen Integrationsbedarf.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Sicherheits-Tools	SIEM-Integration		
	SOAR-Integration		
	EDR/XDR-Integration		
	IAM-Integration		

Entwicklungswerkzeuge	Integration von CI/CD-Pipelines		
	DevOps-Tools unterstützen		
	Sicherheit der Container		
	APIs von Cloud-Anbietern		
Datenaustausch	Bi-direktionale Synchronisation		
	Benutzerdefinierte Integrationen		

8. Verwaltung des Datenschutzes

Tipp: Datenschutzfunktionen sollten sowohl die Einhaltung gesetzlicher Vorschriften als auch organisatorische Sicherheitsanforderungen berücksichtigen. Berücksichtigen Sie regionale Vorschriften und branchenspezifische Anforderungen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Datenschutz	Verschlüsselungsfunktionen		
	Zugangskontrollen		
	Maskierung von Daten		
	Aufbewahrungsrichtlinien		
Datenschutz-Kontrollen	Kontrolle geografischer Daten		
	Durchsetzung der Datenschutzbestimmungen		
	Verwaltung der Einverständniserklärung		
	Minimierung der Datenmenge		

Einhaltung der Vorschriften	Unterstützung der Datenschutzbestimmungen		
	Audit-Fähigkeiten		

9. Automatisierte Bedrohungsjagd

Tipp: Die automatisierte Bedrohungsjagd sollte proaktive Suchfunktionen mit intelligenter Mustererkennung kombinieren. Suchen Sie nach Lösungen, die ihre Suchstrategien auf der Grundlage neuer Bedrohungsdaten kontinuierlich weiterentwickeln.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Jagdbetrieb	Kontinuierliches Scannen		
	IOC-Erkennung		
	Abgleich von Mustern		
	Verhaltensanalyse		
KI-Integration	Modelle für maschinelles Lernen		
	Mustererkennung		
	Erkennung von Anomalien		
	Prädiktive Jagd		
Berichterstattung	Ergebnisse der Jagd		
	Aktualisierungen der Bedrohungsdaten		

10. Analyse des Nutzer- und Entitätsverhaltens (UEBA)

Tipp: UEBA-Funktionen sollten eine umfassende Überwachung des Grundverhaltens und eine genaue Erkennung von Anomalien ermöglichen. Berücksichtigen Sie sowohl die Anforderungen an die Benutzer- als auch an die Systementitätsüberwachung.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Verhalten Baseline	Erstellung von Nutzeraktivitätsprofilen		
	Verfolgung des Verhaltens von Entitäten		
	Lernen von Mustern		
	Grundlegende Anpassung		
Erkennung	Identifizierung von Anomalien		
	Risiko-Scoring		
	Erzeugung von Warnmeldungen		
	Analyse des Kontextes		
Antwort	Automatisierte Aktionen		
	Unterstützung bei Ermittlungen		

11. Natürliche Sprachverarbeitung (NLP)

Tipp: NLP-Funktionen sollten die Verarbeitung von Bedrohungsdaten und die Zugänglichkeit von Sicherheitsinformationen verbessern. Erwägen Sie praktische Anwendungen für Ihre Sicherheitsmaßnahmen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Textanalyse	Verarbeitung von Bedrohungsdaten		
	Kontextuelle Analyse		
	Extraktion von Entitäten		
	Kartierung von Beziehungen		
Intelligente Verarbeitung	Multi-Source-Korrelation		

	Relevanz-Scoring		
	Automatisierte Kategorisierung		
	Vorrangige Bewertung		
Erzeugung von Output	Geheimdienstliche Zusammenfassungen		
	Umsetzbare Erkenntnisse		

12. KI-unterstützte Visualisierung

Tipp: Die Visualisierungsfunktionen sollten klare, umsetzbare Erkenntnisse liefern und gleichzeitig benutzerfreundlich sein. Konzentrieren Sie sich auf Funktionen, die das Verständnis für komplexe Sicherheitsszenarien verbessern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Dashboard-Design	Interaktive Anzeigen		
	Anpassbare Ansichten		
	Aktualisierungen in Echtzeit		
	Drill-down-Fähigkeiten		
Visualisierung von Bedrohungen	Angriffszuordnung		
	Risiko-Visualisierung		
	Trendanalyse		
	Folgenabschätzung		
Berichterstattung	Erstellung benutzerdefinierter Berichte		
	Automatisierte Erzeugung		

13. Automatisierte Vorschläge zur Behebung von Mängeln

Tipp: Abhilfemaßnahmen sollten kontextabhängige Empfehlungen liefern und gleichzeitig angemessene Sicherheitskontrollen gewährleisten. Achten Sie auf ein ausgewogenes Verhältnis zwischen Automatisierung und menschlicher Aufsicht.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Empfehlungsmaschine	Analyse des Kontextes		
	Vorrangige Bewertung		
	Bewertung der Auswirkungen		
	Unterstützung benutzerdefinierter Regeln		
Aktionsmanagement	Automatisierte Ausführung		
	Genehmigungs-Workflows		
	Rollback-Funktionen		
	Überprüfung der Maßnahmen		
Dokumentation	Protokollierung ändern		
	Verfolgung der Ergebnisse		

14. Kontinuierliches Lernen und Verbesserung

Tipp: Das System sollte klare Mechanismen für die Einbeziehung neuer Bedrohungsdaten und das Lernen aus vergangenen Vorfällen aufweisen. Erwägen Sie die Validierung und Messung von Verbesserungen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Lernprozess	Rückkopplungsschleife bei Vorfällen		
	Mustererkennung		
	Modell-Updates		

	Optimierung der Leistung		
Validierung	Genauigkeitsmessung		
	Falsches positives Tracking		
	Metriken zur Effektivität		
	Überprüfung der Verbesserung		
Berichterstattung	Leistungsanalytik		
	Trendanalyse		

15. Prädiktive Risikobewertung

Tipp: Vorhersagefunktionen sollten umsetzbare Erkenntnisse auf der Grundlage historischer Daten und aktueller Bedrohungsdaten liefern. Konzentrieren Sie sich auf den praktischen Wert und die Genauigkeit der Vorhersagen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Risikoanalyse	Historische Analyse		
	Identifizierung von Trends		
	Korrelation der Bedrohungen		
	Vorhersage der Auswirkungen		
Vorhersage	Modellierung künftiger Bedrohungen		
	Kartierung des Risikoverlaufs		
	Vorhersage der Anfälligkeit		
	Angriffssimulation		
Milderung	Proaktive Planung		
	Zuweisung von Ressourcen		

6. Qualifikationen des Anbieters

1. Informationen zum Unternehmen:
    - Jahrelange Erfahrung im Bereich Cloud-Sicherheit
    - Technisches Fachwissen über CDR-Lösungen
    - Kundenreferenzen
    - Informationen zur finanziellen Stabilität
2. Informationen zum Produkt:
    - Produkt-Fahrplan
    - Entwicklungsmethodik
    - Häufigkeit der Aktualisierung
    - Unterstützungsmöglichkeiten
3. Service-Fähigkeiten:
    - Methodik der Umsetzung
    - Ausbildungsprogramme
    - Unterstützungsdienste
    - Angebote für professionelle Dienstleistungen

7. Kriterien für die Bewertung

1. Technische Fähigkeiten (30%):
    - Vollständigkeit der Merkmale
    - Technische Architektur
    - Integrationsfähigkeit
    - Skalierbarkeit
2. Funktionale Fähigkeit (25%):
    - Überwachungsmöglichkeiten

- Antwort Automatisierung
- Verwaltung der Politik
- Berichterstattung und Analyse

3. Qualifizierung der Anbieter (20%):
    - Erleben Sie
    - Referenzen
    - Unterstützungsmöglichkeiten
    - Finanzielle Stabilität
4. Umsetzungskonzept (15%):
    - Methodik
    - Zeitleiste
    - Anforderungen an die Ressourcen
    - Risikomanagement
5. Kosten (10%):
    - Lizenzkosten
    - Kosten der Durchführung
    - Laufende Wartungskosten
    - Ausbildungskosten

8. Einreichungsrichtlinien

Die Anbieter müssen einreichen:

1. Technischer Vorschlag:
    - Beschreibung der Lösung
    - Technische Architektur
    - Ansatz für die Umsetzung

- Zeitplan des Projekts

2. Kommerzieller Vorschlag:
    - Struktur der Preisgestaltung
    - Lizenzmodell
    - Kosten der Durchführung
    - Kosten der Unterstützung
3. Informationen zum Unternehmen:
    - Profil des Unternehmens
    - Kundenreferenzen
    - Finanzielle Informationen
    - Team-Qualifikationen

9. Zeitleiste

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

10. Kontaktinformationen

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