# Aufforderung zur Angebotsabgabe: Plattformlösung für erweiterte Erkennung und Reaktion (XDR)

## Inhaltsübersicht



## 1. Einleitung und Hintergrund

bittet um Vorschläge für eine umfassende Extended Detection and Response (XDR)-Plattform zur Verbesserung unserer Cybersicherheitsinfrastruktur. Diese Ausschreibung umreißt unsere Anforderungen an eine fortschrittliche Sicherheitslösung, die mehrere Sicherheitsprodukte in ein kohärentes System integriert und verbesserte Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen in unserem gesamten Technologiebereich bietet.

### Derzeitige Sicherheitsposition

- Wir wollen ein einheitliches Konzept für die Sicherheitsüberwachung und -reaktion umsetzen.
- Die Lösung muss Daten aus verschiedenen Quellen sammeln und korrelieren, darunter Endgeräte, Netzwerke, Cloud-Workloads, E-Mail-Systeme und Server.

- Die Integration in bestehende Sicherheitstools und -infrastrukturen ist unerlässlich.

### Ziele des Projekts

Die Hauptziele der Implementierung einer XDR-Plattform sind:

- Verbesserung der Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen im gesamten Technologiebereich des Unternehmens
- Konsolidierung der Sicherheitstools und Verbesserung der betrieblichen Effizienz
- Stärkung unserer allgemeinen Sicherheitslage durch fortschrittliche Analysen und Automatisierung
- Gewährleistung der Einhaltung der einschlägigen Vorschriften und Datenschutzstandards

## 2. Umfang der Arbeit

Der ausgewählte Anbieter wird für folgende Aufgaben verantwortlich sein:

### Umsetzung und Integration

1. Bereitstellung einer umfassenden XDR-Plattform
2. Integration in bestehende Sicherheitsinfrastrukturen und -werkzeuge
3. Konfiguration der Datenerfassung aus mehreren Quellen:
    - Endpunkte
    - Netzwerke
    - Cloud-Workloads
    - E-Mail-Systeme
    - Server

### Kernfunktionalität

1. Datenerfassung und -integration
    - Nahtlose Zusammenführung von Daten aus mehreren Quellen
    - Integration mit bestehenden Sicherheitswerkzeugen

- Datenverarbeitung und -korrelation in Echtzeit

2. Erkennung von und Reaktion auf Bedrohungen
    - Erweiterte Analysen für eine umfassende Identifizierung von Bedrohungen
    - Automatisierte Antwortmöglichkeiten
    - Domänenübergreifende Bedrohungsanalyse
3. Überwachung und Sichtbarkeit
    - Verbesserte Transparenz über alle Sicherheitsebenen hinweg
    - Umfassende Überwachungsmöglichkeiten
    - Funktionen zur Bedrohungssuche in Echtzeit

## 3. Technische Anforderungen

1. Plattform-Architektur
    - Cloud-native Architektur
    - Skalierbare Bereitstellungsoptionen
    - Hochverfügbarkeitsdesign
    - Lastausgleichsfunktionen
    - Unterstützung bei der Wiederherstellung im Katastrophenfall
2. Leistungsanforderungen
    - Datenverarbeitung in Echtzeit
    - Minimale Latenzzeit bei der Erkennung von Bedrohungen
    - Effiziente Ressourcennutzung
    - Skalierbare Speicherlösung
    - Hochgeschwindigkeits-Suchfunktionen
3. Sicherheitsanforderungen

- Ende-zu-Ende-Verschlüsselung
- Rollenbasierte Zugriffskontrolle
- Multi-Faktor-Authentifizierung
- Audit-Protokollierung
- Sichere API-Endpunkte

4. Anforderungen an die Integration
    - Standard-API-Unterstützung
    - Unterstützung gemeinsamer Datenformate
    - Integration von Drittanbieter-Tools
    - Individuelle Integrationsmöglichkeiten
    - Webhook-Unterstützung

## 4. Funktionale Anforderungen

### 1. Datenerhebung und -integration

***Tipp: Die Grundlage einer effektiven XDR-Plattform liegt in ihrer Fähigkeit, Daten aus verschiedenen Quellen zu sammeln und zusammenzuführen. Konzentrieren Sie sich darauf, sowohl die Breite der unterstützten Datenquellen als auch die Tiefe der Integrationsmöglichkeiten zu bewerten. Berücksichtigen Sie die Kompatibilität mit der vorhandenen Infrastruktur und den künftigen Bedarf an Skalierbarkeit.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Sammlung von Datenquellen | Sammlung von Endpunkten | | |
| | Sammlung bei den Netzen | | |
| | Sammlung von Cloud-Workloads | | |

| | | | |
|---|---|---|---|
| | Sammlung aus E-Mail-Systemen | | |
| | Abholung von Servern | | |
| Integrationsfähigkeiten | Integration mit bestehendem SIEM | | |
| | Integration mit Firewall-Systemen | | |
| | Integration mit EDR-Lösungen | | |
| | Integration mit Identitätsmanagementsystemen | | |
| Datenverarbeitung | Datenerfassung in Echtzeit | | |
| | Normalisierung der Daten | | |
| | Anreicherung der Daten | | |

## 2. Einheitliche Erkennung von Bedrohungen

***Tipp: Ein robustes System zur Erkennung von Bedrohungen sollte umfassende Transparenz bieten und gleichzeitig die Zahl der Fehlalarme minimieren. Prüfen Sie die Fähigkeit der Lösung, Bedrohungen über verschiedene Sicherheitsebenen hinweg zu korrelieren, und ihre Effektivität bei der Erkennung komplexer Angriffsmuster.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Sichtbarkeit der Bedrohung | Stapelübergreifende Überwachung von Bedrohungen | | |
| | Erkennung von Bedrohungen in Echtzeit | | |
| | Historische Bedrohungsanalyse | | |
| Analyse-Fähigkeiten | Datenkorrelation zwischen verschiedenen Quellen | | |

| | | | |
|---|---|---|---|
| | Verhaltensanalyse | | |
| | Mustererkennung | | |
| | Erkennung von Anomalien | | |

### 3. Automatisierte Antwortmöglichkeiten

***Tipp: Achten Sie sowohl auf die Automatisierungsfunktionen als auch auf die Flexibilität bei der Anpassung der Reaktionsmaßnahmen. Achten Sie auf Lösungen, die ein Gleichgewicht zwischen automatisierten Antworten und menschlicher Aufsicht herstellen und klare Prüfprotokolle aller durchgeführten Aktionen bieten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| AI/ML-Integration | Auf maschinellem Lernen basierende Antwort | | |
| | Automatisierte Klassifizierung von Bedrohungen | | |
| | Dynamische Anpassung der Reaktion | | |
| Orchestrierung von Antworten | Schichtübergreifende Reaktionsmaßnahmen | | |
| | Anpassbare Antwort-Playbooks | | |
| | Validierung der Antwortaktion | | |
| | Rollback-Funktionen | | |

### 4. Bessere Sichtbarkeit

***Tipp: Die Lösung sollte bei Bedarf sowohl einen umfassenden Überblick als auch granulare Details bieten. Konzentrieren Sie sich auf die Bewertung der Transparenz über verschiedene Umgebungen hinweg und die Möglichkeit, schnell zwischen übergeordneten und detaillierten Ansichten zu wechseln.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Mehrschichtige Sichtbarkeit | Sichtbarkeit der Endpunkte | | |
| | Sichtbarkeit des Netzes | | |
| | Sichtbarkeit der Cloud-Umgebung | | |
| Monitoring-Fähigkeiten | Überwachung in Echtzeit | | |
| | Analyse historischer Daten | | |
| | Entdeckung von Vermögenswerten | | |
| Jagd auf Bedrohungen | Benutzerdefinierte Abfragefunktionen | | |
| | Arbeitsabläufe bei der Bedrohungsjagd | | |
| | Ermittlungsinstrumente | | |

## 5. Alarmmanagement und Triage

***Tipp: Ein effizientes Alarmmanagement ist entscheidend für die Produktivität des SOC. Bewerten Sie die Fähigkeit der Lösung, die Ermüdung durch Alarme zu verringern und gleichzeitig sicherzustellen, dass kritische Bedrohungen nicht übersehen werden. Berücksichtigen Sie sowohl automatische als auch manuelle Triage-Funktionen.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Warnung Konsolidierung | Bündelung von Warnmeldungen aus mehreren Quellen | | |
| | Alert-Deduplizierung | | |
| | Alert-Korrelation | | |

| | | | |
|---|---|---|---|
| Falsch-Positiv-Reduzierung | Auf maschinellem Lernen basierende Filterung | | |
| | Benutzerdefinierte Filterregeln | | |
| | Validierung von Warnmeldungen | | |
| Prioritätsmanagement | Automatisierte Priorisierung | | |
| | Benutzerdefinierte Prioritätsregeln | | |
| | Risikobasiertes Scoring | | |

### 6. Domänenübergreifende Bedrohungsanalyse

***Tipp: Eine effektive bereichsübergreifende Analyse erfordert sowohl Tiefe als auch Breite des Einblicks. Suchen Sie nach Lösungen, die nicht nur Daten bereichsübergreifend sammeln, sondern diese auch sinnvoll korrelieren und analysieren können, um verwertbare Erkenntnisse und klare Angriffsdarstellungen zu liefern.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Kontext der Bedrohung | Domänenübergreifende Telemetrie-Korrelation | | |
| | Visualisierung der Angriffskette | | |
| | Attribution von Bedrohungsakteuren | | |
| Analyse der Auswirkungen | Folgenabschätzung für Gastgeber | | |
| | Analyse der Auswirkungen auf das Netz | | |
| | Bewertung der Auswirkungen auf das Geschäft | | |

| | | | |
|---|---|---|---|
| Analyse der Grundursache | Erste Identifizierung von Angriffsvektoren | | |
| | Abbildung der Ausbreitungswege | | |
| | Analyse der beitragenden Faktoren | | |
| Erstellung der Zeitleiste | Sequenzierung von Ereignissen | | |
| | Zeitliche Korrelation | | |
| | Integration des historischen Kontextes | | |

## 7. Skalierbarkeit

***Tipp: Berücksichtigen Sie nicht nur den aktuellen Bedarf, sondern auch künftiges Wachstum. Die Lösung sollte wachsende Datenmengen, neue Sicherheitstools und eine wachsende Infrastruktur ohne signifikante Leistungseinbußen oder Architekturänderungen bewältigen können.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Organisatorisches Wachstum | Unterstützung für die Erhöhung der Endpunktanzahl | | |
| | Flexibles Lizenzierungsmodell | | |
| | Unterstützung für mehrere Standorte | | |
| Verwaltung des Datenvolumens | Skalierbare Datenspeicherung | | |
| | Maßnahmen zur Datenspeicherung | | |
| | Optimierung der Leistung | | |
| Anpassungsfähigkeit der Infrastruktur | Skalierbarkeit der Cloud | | |

| | | | |
|---|---|---|---|
| | Vor-Ort-Erweiterungsmöglichkeit | | |
| | Unterstützung für den hybriden Einsatz | | |

## 8. Benutzeroberfläche und Berichterstattung

***Tipp: Die Benutzeroberfläche sollte ein ausgewogenes Verhältnis zwischen Leistungsfähigkeit und Benutzerfreundlichkeit aufweisen und sowohl schnelle Einblicke für junge Analysten als auch tiefgreifende Untersuchungsmöglichkeiten für fortgeschrittene Benutzer bieten. Die Berichterstattung sollte sowohl umfassend als auch anpassbar sein.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Schnittstellengestaltung | Intuitive Navigation | | |
| | Rollenbasierte Ansichten | | |
| | Anpassbare Dashboards | | |
| Untersuchungstools | Interaktive Bedrohungsjagd | | |
| | Visuelle Link-Analyse | | |
| | Erweiterte Suchfunktionen | | |
| Berichtsfunktionen | Vorgefertigte Berichtsvorlagen | | |
| | Erstellung benutzerdefinierter Berichte | | |
| | Planmäßige Berichterstattung | | |
| | Ausführliche Zusammenfassungen | | |
| | Technische Detailberichte | | |

## 9. Integration von Bedrohungsdaten

***Tipp: Achten Sie sowohl auf die Qualität der integrierten Bedrohungsdaten als auch auf die Fähigkeit der Plattform, diese effektiv zu nutzen. Achten Sie darauf, wie gut die Lösung externe Informationen mit internem Kontext kombinieren kann.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Intelligenz-Quellen | Integration kommerzieller Futtermittel | | |
| | Open-Source-Intelligenz | | |
| | Branchenspezifische Informationen | | |
| Nachrichtenmanagement | Verwaltung von Indikatoren | | |
| | Kuratierung von Informationen | | |
| | Erstellung benutzerdefinierter Informationen | | |
| Operative Integration | Korrelation in Echtzeit | | |
| | Automatisierte Anreicherung | | |
| | Rückwirkende Jagd | | |

## 10. Compliance und Datenschutz

***Tipp: Stellen Sie sicher, dass die Lösung nicht nur zur Einhaltung der Vorschriften beiträgt, sondern auch den Nachweis der Einhaltung erbringt. Berücksichtigen Sie sowohl aktuelle gesetzliche Anforderungen als auch potenzielle zukünftige Verpflichtungen.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Datenverarbeitung | Konforme Datenerhebung | | |
| | Unterstützung der Datenhoheit | | |

| | | | |
|---|---|---|---|
| | Funktionen zur Datenmaskierung | | |
| Einhaltung von Vorschriften | Einhaltung der GDPR | | |
| | Einhaltung des HIPAA | | |
| | PCI DSS-Konformität | | |
| Datenschutz-Kontrollen | Zugangskontrollen | | |
| | Anonymisierung von Daten | | |
| | Verwaltung der Einverständniserklärung | | |
| Audit-Unterstützung | Compliance-Berichterstattung | | |
| | Prüfpfade | | |
| | Sammlung von Beweismitteln | | |

## 11. Unterstützung von API und Integration

***Tipp: APIs sollten gut dokumentiert und sicher sein und sowohl grundlegende Integrationsanforderungen als auch erweiterte Automatisierungsszenarien unterstützen. Achten Sie auf die Vollständigkeit der API-Oberfläche und die Qualität der Entwicklerunterstützung.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| API-Fähigkeiten | RESTful API-Unterstützung | | |
| | Datenzugang in Echtzeit | | |
| | Unterstützung von Massenoperationen | | |
| Integrationsmerkmale | Entwicklung kundenspezifischer Integration | | |

| | | | |
|---|---|---|---|
| | Vorgefertigte Integrationen | | |
| | Webhook-Unterstützung | | |
| Unterstützung der Entwicklung | API-Dokumentation | | |
| | Tools für Entwickler | | |
| | Verfügbarkeit von Beispielcode | | |
| Sicherheitskontrollen | API-Authentifizierung | | |
| | Ratenbegrenzung | | |
| | Zugangsprotokollierung | | |

## 12. Echtzeit-Überwachung und -Warnung

***Tipp: Echtzeit-Funktionen sollten ein ausgewogenes Verhältnis zwischen Geschwindigkeit und Genauigkeit bieten. Berücksichtigen Sie sowohl die Aktualität der Warnungen als auch die Fähigkeit des Systems, die Leistung unter Bedingungen mit hohem Aufkommen aufrechtzuerhalten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Monitoring-Fähigkeiten | Datenverarbeitung in Echtzeit | | |
| | Kontinuierliche Vermögensüberwachung | | |
| | Überwachung der Leistung | | |
| Management von Warnmeldungen | Generierung von Warnmeldungen in Echtzeit | | |
| | Alarm-Routing | | |
| | Regeln zur Unterdrückung von Alarmen | | |

| | | | |
|---|---|---|---|
| System Status | Überwachung der Gesundheit | | |
| | Überwachung der Kapazität | | |
| | Latenzverfolgung | | |
| Benachrichtigungssysteme | Mehrere Benachrichtigungskanäle | | |
| | Anpassbare Benachrichtigungen | | |
| | Eskalations-Workflows | | |

### 13. KI-gestützte Funktionen

***Tipp: KI-Funktionen sollten die menschliche Analyse nicht ersetzen, sondern ergänzen. Suchen Sie nach Lösungen, die erklärbare KI-Entscheidungen bieten und eine menschliche Kontrolle ermöglichen, während sie gleichzeitig Routineaufgaben automatisieren und erweiterte Analysefunktionen bereitstellen.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Fallanalyse | Erstellung von AI-Fallzusammenfassungen | | |
| | Korrelation von Ereignissen und Entitäten | | |
| | Empfehlungen für die nächsten Schritte | | |
| Befehlsanalyse | Entschleierung über die Befehlszeile | | |
| | Absichtsanalyse | | |
| | Bewertung der Auswirkungen auf die Sicherheit | | |

| | | | |
|---|---|---|---|
| Suchfunktionen | Abfragen in natürlicher Sprache | | |
| | Optimierung der Suche im Datensee | | |
| | Kontextabhängige Ergebnisse | | |
| MITRE ATT&CK-Integration | Automatische TTP-Zuordnung | | |
| | Taktische Klassifizierung | | |
| | Identifizierung der Technik | | |
| Erweiterte AI-Modelle | Integration von Cyber-trainierten Modellen | | |
| | Erkennung von Angriffsmustern | | |
| | Verhaltensanalyse | | |
| Intelligente Bedrohung | ML-verstärkte Erkennung | | |
| | Automatisierte Korrelation von Bedrohungen | | |
| | Intelligenz-Updates in Echtzeit | | |
| Antwort Automatisierung | KI-gestützte Playbooks | | |
| | Szenariobasierte Antwort | | |
| | Automatisierte Orchestrierung | | |
| Prädiktive Analytik | Vorhersage von Angriffstendenzen | | |
| | Vorhersage der Anfälligkeit | | |
| | Risikobewertung | | |

| | | | |
|---|---|---|---|
| SOC-Automatisierung | Automatisierung von Arbeitsabläufen | | |
| | Optimierung der Ressourcen | | |
| | Priorisierung der Aufgaben | | |
| Adaptives Lernen | Kontinuierliches Modelltraining | | |
| | Lernen von Endpunktdaten | | |
| | Dynamische Verbesserung der Sicherheit | | |
| Analyse in Echtzeit | KI-gesteuerte Datenaggregation | | |
| | Korrelation der Telemetrie | | |
| | Gewinnung von Erkenntnissen in Echtzeit | | |

## 5. Qualifikationen des Anbieters

### Erforderliche Qualifikationen

1. Mindestens 5 Jahre Erfahrung mit XDR oder verwandten Sicherheitslösungen
2. Nachgewiesene Erfolgsbilanz erfolgreicher Unternehmensimplementierungen
3. Starke Marktpräsenz im Bereich Cybersicherheit
4. Fester Kundenstamm mit nachprüfbaren Referenzen
5. Engagiertes Support- und Wartungsteam
6. Klarer Fahrplan für die Produktentwicklung
7. Finanzielle Stabilität und Nachhaltigkeit

### Bevorzugte Qualifikationen

1. Anerkennung der Branche durch Analysten (Gartner, Forrester)
2. Erfahrung in ähnlichen vertikalen Branchen
3. Lokale Präsenz der Unterstützung

4. Aktives Forschungs- und Entwicklungsprogramm

5. Etabliertes Partner-Ökosystem

## 6. Kriterien für die Bewertung

Die Vorschläge werden auf der Grundlage der folgenden Kriterien bewertet:

| Kriterium | Gewicht |
|---|---|
| Technisches Leistungsvermögen | 30% |
| Integrationsfähigkeiten | 20% |
| AI/ML-Fähigkeiten | 15% |
| Benutzerfreundlichkeit | 10% |
| Kosten | 10% |
| Erfahrung des Anbieters | 10% |
| Unterstützung und Wartung | 5% |

## 7. Einreichungsrichtlinien

Die Anbieter müssen einreichen:

1. Detaillierter technischer Vorschlag

2. Methodik der Umsetzung

3. Zeitplan des Projekts

4. Struktur der Preisgestaltung

5. Profil des Unternehmens

6. Kundenreferenzen

7. Support- und Wartungspläne

8. Details zum Schulungsprogramm

## 8. Zeitleiste

| Meilenstein | Datum |
|---|---|
| RFP-Freigabe | |
| Fragen Abgabetermin | |
| Fälligkeitsdatum des Vorschlags | |
| Präsentationen von Anbietern | |
| Auswahlentscheidung | |
| Projekt-Auftakt | |

## 9. Kontaktinformationen

Für Fragen und die Einreichung von Vorschlägen: