Demande de proposition : Solution logicielle de détection et de réponse dans le nuage (CDR)

Table des matières

1. Introduction et contexte
2. Objectifs du projet
3. Champ d'application
4. Exigences techniques
5. Exigences fonctionnelles
6. Qualifications des fournisseurs
7. Critères d'évaluation
8. Lignes directrices pour la soumission
9. Chronologie

1. Introduction et contexte

Notre organisation recherche des propositions pour une solution logicielle complète de détection et de réponse dans le nuage (CDR) afin d'améliorer notre infrastructure de sécurité dans le nuage. Cet appel d'offres décrit les exigences d'un système robuste fournissant une surveillance continue, une détection des menaces et des capacités de réponse automatisée dans des environnements multi-cloud.

2. Objectifs du projet

1. Mettre en œuvre une surveillance et une réponse complètes en matière de sécurité de l'informatique en nuage :
 - Capacités de détection et de réponse aux menaces en temps réel
 - Surveillance continue des environnements en nuage
 - Audit automatisé et gestion de la conformité

- Visibilité accrue sur l'infrastructure multi-cloud
2. Renforcer la posture de sécurité par :
 - Détection avancée des menaces à l'aide de l'IA et de l'apprentissage automatique
 - Réponse automatisée aux menaces identifiées
 - Évaluation et atténuation proactives des risques
 - Gestion et application complètes des politiques
 3. Assurer la conformité réglementaire par :
 - Contrôle de conformité et rapports automatisés
 - Mise en œuvre de politiques dans les ressources en nuage
 - Rationalisation des processus d'audit
 - Suivi en temps réel de l'état de conformité
 4. Améliorer l'efficacité opérationnelle grâce à :
 - Intégration avec les outils et processus de sécurité existants
 - Capacités de réponse automatisée
 - Collaboration simplifiée entre les équipes de sécurité et de développement
 - Réduction de la fatigue liée aux alertes grâce à une hiérarchisation intelligente des alertes

3. L'étendue des travaux

Le fournisseur sélectionné sera responsable de

1. Mise en œuvre de la solution CDR :
 - Déploiement dans tous les environnements en nuage
 - Intégration avec les outils de sécurité existants
 - Configuration de la surveillance et de l'alerte

- Mise en place de capacités de réponse automatisée
2. Collecte et analyse des données :
 - Mise en œuvre de la collecte de données à partir de toutes les sources en nuage
 - Configuration des outils d'analyse et des algorithmes
 - Mise en place de rapports et de tableaux de bord
 - Intégration avec les systèmes d'enregistrement existants
 3. Gestion des politiques et de la conformité :
 - Mise en œuvre des cadres de conformité
 - Configuration de l'application de la politique
 - Mise en place d'un audit automatisé
 - Intégration avec les outils de conformité existants
 4. Formation et transfert de connaissances :
 - Formation des administrateurs à la gestion du système
 - Formation de l'équipe de sécurité à la réponse aux menaces
 - Documentation des processus et des procédures
 - Assistance permanente et conseils en matière de maintenance

4. Exigences techniques

1. Intégration dans le nuage :
 - Prise en charge des principaux fournisseurs de services en nuage (AWS, Azure, GCP)
 - Capacités de surveillance sans agent
 - Intégration basée sur l'API
 - Console de gestion multi-cloud

2. Détection des menaces :

- Détection basée sur l'IA et l'apprentissage automatique
- Détection basée sur la signature
- Analyse comportementale
- Détection des anomalies
- Analyse du comportement des utilisateurs et des entités

3. Automatisation des réponses :

- Manuels de réponse automatisée aux menaces
- Actions de réponse personnalisables
- Intégration avec les outils de sécurité existants
- Capacités de remédiation automatisée

4. Gestion de la conformité :

- Cadres de conformité préétablis
- Création de politiques personnalisées
- Contrôle automatisé de la conformité
- Création d'une piste d'audit

5. Rapports et analyses :

- Tableaux de bord en temps réel
- Rapports personnalisables
- Intégration des renseignements sur les menaces
- Analyse de l'évaluation des risques

5. Exigences fonctionnelles

1. Collecte et agrégation des données

Conseil : La collecte de données complètes est fondamentale pour l'efficacité du PCEM. Concentrez-vous sur l'évaluation de l'étendue des sources de données, de la profondeur des informations collectées et de l'efficacité des méthodes d'agrégation. Considérez à la fois les capacités en temps réel et la conservation des données historiques pour garantir une visibilité complète de votre environnement en nuage.

Exigence	Sous-exigence	O/N	Notes
Sources de données	Intégration des logs dans le nuage		
	Surveillance du trafic sur le réseau		
	Suivi de l'activité des points finaux		
	Intégration de sources personnalisées		
	Traitement des données	Traitement en temps réel	
	Analyse des données historiques		
	Normalisation des données		
	Extraction des métadonnées		
Intégration	Compatibilité API		
	Support multiplateforme		

2. Détection des menaces avancées

Conseil : la détection des menaces modernes nécessite un mélange sophistiqué de méthodes traditionnelles et de méthodes alimentées par l'IA. Évaluez la capacité de la solution à détecter les menaces connues tout en s'adaptant aux nouveaux modèles d'attaque.

Exigence	Sous-exigence	O/N	Notes
Méthodes de détection	Détection basée sur la signature		

	Algorithmes d'apprentissage automatique		
	Analyse comportementale		
	Détection des anomalies		
Types de menaces	Menaces de type "jour zéro		
	Menaces persistantes avancées		
	Menaces d'initiés		
	Attaques spécifiques à l'informatique en nuage		
Intelligence	Intégration des flux de menaces		
	Création de règles personnalisées		

3. Réponse aux incidents

Conseil : une réponse efficace aux incidents équilibre l'automatisation et la supervision humaine. Concentrez-vous sur des manuels de réponse personnalisables qui s'alignent sur vos procédures de sécurité.

Exigence	Sous-exigence	O/N	Notes
Automatisation	Capacités d'isolation du système		
	Blocage du trafic		
	Collecte de preuves		
	Mesures d'assainissement		
Gestion des réponses	Personnalisation du playbook		
	Traitement prioritaire		
	Procédures d'escalade		
	Capacité de retour en arrière		

Intégration	Intégration des outils de sécurité		
	Automatisation des flux de travail		

4. Priorité aux alertes

Conseil : une gestion efficace des alertes est essentielle pour réduire le bruit et s'assurer que les menaces critiques reçoivent une attention immédiate. Concentrez-vous sur les capacités de hiérarchisation intelligente et sur l'intégration avec les flux de travail existants.

Exigence	Sous-exigence	O/N	Notes
Moteur de hiérarchisation	Priorités basées sur l'IA		
	Notation basée sur le risque		
	Prise en compte du contexte		
	Règles de priorité personnalisées		
Gestion des alertes	Réduction des faux positifs		
	Corrélation des alertes		
	Suppression des alertes		
	Triage automatisé		
Intégration du flux de travail	Intégration du système de billetterie		
	Règles de notification des équipes		

5. Gestion de la conformité

Conseil : La gestion de la conformité nécessite à la fois un contrôle proactif et une mise en œuvre automatisée. Recherchez des solutions qui s'adaptent à l'évolution des exigences réglementaires et qui fournissent des pistes d'audit complètes.

Exigence	Sous-exigence	O/N	Notes

Cadre politique	Modèles de normes réglementaires		
	Création de politiques personnalisées		
	Application de la politique		
	Gestion des exceptions		
Contrôle	Contrôles de conformité en temps réel		
	Évaluation de la configuration		
	Suivi des changements		
	Détection des infractions		
Rapports	Tableaux de bord de conformité		
	Création d'une piste d'audit		

6. L'évolutivité

Conseil : l'évolutivité doit tenir compte à la fois de la croissance horizontale et de la complexité verticale. Évaluez la capacité de la solution à maintenir les performances au fur et à mesure que votre environnement se développe, tout en prenant en charge de nouvelles fonctionnalités et exigences.

Exigence	Sous-exigence	O/N	Notes
Mise à l'échelle des performances	Capacité de manutention des charges		
	Optimisation des ressources		
	Prise en charge multi-cloud		
	Traitement distribué		
Architecture	Conception modulaire		
	Haute disponibilité		

	Reprise après sinistre		
	Répartition géographique		
Gestion	Administration centralisée		
	Support multi-locataires		

7. Intégration aux systèmes existants

Conseil : les capacités d'intégration doivent aller au-delà de la connectivité API de base et inclure l'automatisation des flux de travail et la synchronisation des données. Tenez compte des besoins d'intégration actuels et futurs.

Exigence	Sous-exigence	O/N	Notes
Outils de sécurité	Intégration SIEM		
	Intégration SOAR		
	Intégration EDR/XDR		
	Intégration IAM		
Outils de développement	Intégration du pipeline CI/CD		
	Soutien aux outils DevOps		
	Sécurité des conteneurs		
	API des fournisseurs d'informatique en nuage		
Échange de données	Synchronisation bidirectionnelle		
	Intégrations personnalisées		

8. Gestion de la confidentialité des données

Conseil : Les caractéristiques de confidentialité des données doivent tenir compte à la fois de la conformité réglementaire et des exigences de sécurité

de l'organisation. Tenez compte des réglementations régionales et des exigences propres à votre secteur d'activité.

Exigence	Sous-exigence	O/N	Notes
Protection des données	Capacités de cryptage		
	Contrôles d'accès		
	Masquage des données		
	Politiques de conservation		
Contrôles de la vie privée	Contrôle des données géographiques		
	Application de la politique de protection de la vie privée		
	Gestion des consentements		
	Minimisation des données		
Conformité	Soutien à la réglementation en matière de protection de la vie privée		
	Capacités d'audit		

9. Chasse automatisée aux menaces

Conseil : La chasse automatisée aux menaces doit combiner des capacités de recherche proactive et une reconnaissance intelligente des schémas.

Recherchez des solutions qui font évoluer en permanence leurs stratégies de recherche en fonction des nouvelles informations sur les menaces.

Exigence	Sous-exigence	O/N	Notes
Opérations de chasse	Balayage continu		
	Détection des COI		

	Correspondance des modèles		
	Analyse comportementale		
Intégration de l'IA	Modèles d'apprentissage automatique		
	Reconnaissance des formes		
	Détection des anomalies		
	Chasse prédictive		
Rapports	Résultats de la chasse		
	Mises à jour des renseignements sur les menaces		

10. Analyse du comportement des utilisateurs et des entités (UEBA)

Conseil : les fonctionnalités de l'UEBA doivent permettre une surveillance complète du comportement de base et une détection précise des anomalies. Il convient de prendre en compte les exigences en matière de surveillance des entités des utilisateurs et des systèmes.

Exigence	Sous-exigence	O/N	Notes
Comportement Référence	Profilage de l'activité des utilisateurs		
	Suivi du comportement des entités		
	Apprentissage par patrons		
	Adaptation de base		
Détection	Identification des anomalies		
	Evaluation des risques		
	Génération d'alertes		
	Analyse du contexte		

Réponse	Actions automatisées		
	Aide à l'enquête		

11. Traitement du langage naturel (NLP)

Conseil : les capacités NLP devraient permettre d'améliorer le traitement des renseignements sur les menaces et l'accessibilité des informations de sécurité. Envisagez des applications pratiques dans vos opérations de sécurité.

Exigence	Sous-exigence	O/N	Notes
Analyse de texte	Traitement des flux de menaces		
	Analyse contextuelle		
	Extraction d'entités		
	Cartographie des relations		
	Traitement du renseignement	Corrélation multi-sources	
	Notation de la pertinence		
	Catégorisation automatisée		
	Évaluation des priorités		
Génération de sorties	Résumés des renseignements		
	Des informations exploitables		

12. Visualisation améliorée par l'IA

Conseil : Les fonctions de visualisation doivent fournir des informations claires et exploitables tout en restant faciles à utiliser. Privilégiez les fonctionnalités qui permettent de mieux comprendre les scénarios de sécurité complexes.

Exigence	Sous-exigence	O/N	Notes

Conception du tableau de bord	Affichages interactifs		
	Vues personnalisables		
	Mises à jour en temps réel		
	Capacités d'exploration		
Visualisation des menaces	Cartographie des attaques		
	Visualisation des risques		
	Analyse des tendances		
	Analyse d'impact		
Rapports	Création de rapports personnalisés		
	Génération automatisée		

13. Suggestions de remédiation automatisée

Conseil : Les capacités de remédiation doivent fournir des recommandations contextuelles tout en maintenant des contrôles de sécurité appropriés.

Pensez à l'équilibre entre l'automatisation et la supervision humaine.

Exigence	Sous-exigence	O/N	Notes
Moteur de recommandation	Analyse du contexte		
	Évaluation des priorités		
	Évaluation de l'impact		
	Prise en charge des règles personnalisées		
Gestion des actions	Exécution automatisée		
	Flux de travail d'approbation		
	Capacités de retour en arrière		

	Vérification des actions		
Documentation	Modifier la journalisation		
	Suivi des résultats		

14. Apprentissage et amélioration continus

Conseil : le système doit présenter des mécanismes clairs permettant d'intégrer de nouveaux renseignements sur les menaces et de tirer des enseignements des incidents passés. Envisager la validation et la mesure des améliorations.

Exigence	Sous-exigence	O/N	Notes
Processus d'apprentissage	Boucle de rétroaction des incidents		
	Reconnaissance des formes		
	Mises à jour du modèle		
	Optimisation des performances		
Validation	Mesure de la précision		
	Suivi des faux positifs		
	Mesures d'efficacité		
	Vérification de l'amélioration		
Rapports	Analyse des performances		
	Analyse des tendances		

15. Évaluation prédictive des risques

Conseil : Les capacités prédictives doivent fournir des informations exploitables basées sur des données historiques et des renseignements sur les menaces actuelles. Concentrez-vous sur la valeur pratique et la précision des prédictions.

Exigence	Sous-exigence	O/N	Notes
Analyse des risques	Analyse historique		
	Identification des tendances		
	Corrélation des menaces		
	Prévision d'impact		
	Modélisation des menaces futures		
Prévisions	Cartographie de la trajectoire du risque		
	Prévision de la vulnérabilité		
	Simulation d'attaque		
Atténuation	Planification proactive		
	Allocation des ressources		

6. Qualifications des fournisseurs

1. Informations sur l'entreprise :

- Des années d'expérience en matière de sécurité informatique
- Expertise technique en matière de solutions CDR
- Références clients
- Informations sur la stabilité financière

2. Informations sur le produit :

- Feuille de route du produit
- Méthodologie de développement
- Fréquence de mise à jour
- Capacités de soutien

3. Capacités de service :

- Méthodologie de mise en œuvre
- Programmes de formation
- Services d'appui
- Offres de services professionnels

7. Critères d'évaluation

1. Capacité technique (30%) :

- Complétude des caractéristiques
- Architecture technique
- Capacités d'intégration
- Évolutivité

2. Capacité fonctionnelle (25%) :

- Capacités de surveillance
- Automatisation des réponses
- Gestion des politiques
- Rapports et analyses

3. Qualification des fournisseurs (20 %) :

- Expérience
- Références
- Capacités de soutien
- Stabilité financière

4. Approche de la mise en œuvre (15 %) :

- Méthodologie
- Chronologie
- Besoins en ressources

- Gestion des risques

5. Coût (10%) :

- Frais de licence
- Coûts de mise en œuvre
- Coûts d'entretien courants
- Coûts de formation

8. Lignes directrices pour la soumission

Les vendeurs doivent soumettre :

1. Proposition technique :

- Description de la solution
- Architecture technique
- Approche de la mise en œuvre
- Calendrier du projet

2. Proposition commerciale :

- Structure des prix
- Modèle de licence
- Coûts de mise en œuvre
- Coûts de soutien

3. Informations sur l'entreprise :

- Profil de l'entreprise
- Références clients
- Informations financières
- Qualifications de l'équipe

9. Calendrier

- Date de publication de l'appel d'offres : [Date]
- Date limite pour les questions : [Date]
- Date d'échéance de la proposition : [Date]
- Présentations des fournisseurs : [Fourchette de dates]
- Date de sélection : [Date]
- Date de début du projet : [Date]

10. Informations sur les contacts

Veillez soumettre vos propositions et vos questions à [Nom du contact] [Adresse électronique] [Numéro de téléphone]