Demande de proposition : Plateforme de protection des applications cloud-natives (CNAPP)

Table des matières

1. Vue d'ensemble

Nous recherchons des propositions pour une plateforme complète de protection des applications cloud-natives (CNAPP) afin de protéger nos applications cloud-natives tout au long de leur cycle de vie. La solution doit fournir des fonctions de sécurité intégrées, offrant une visibilité complète, une application cohérente des politiques et une protection solide dans nos divers environnements en nuage.

2. Composants clés

La solution proposée doit comprendre les éléments clés suivants :

2.1. Gestion de la sécurité dans l'informatique dématérialisée (CSPM)

2.2. Plate-forme de protection de la charge de travail dans le nuage (CWPP)

2.3. Gestion des droits sur l'infrastructure en nuage (CIEM)

2.4. Intégration DevSecOps

2.5. Protection en cours d'exécution

3. Exigences fonctionnelles

3.1. Visibilité unifiée

Conseil : Une solution robuste de visibilité unifiée est essentielle pour maintenir une surveillance complète de la sécurité. Recherchez des solutions qui offrent des capacités de surveillance en temps réel et qui peuvent intégrer des données provenant de sources multiples dans une vue unique et cohérente. Prenez en compte la profondeur de la visibilité sur les différents services cloud et la possibilité de personnaliser les vues en fonction des besoins des différentes parties prenantes.

Exigence	Sous-exigence	O/N	Notes
Visibilité unifiée	Vue centralisée de la sécurité de toutes les ressources et de tous les services en nuage		
	Visibilité des configurations		
	Visibilité des actifs		
	Visibilité sur les autorisations		
	Visibilité sur le code		
	Visibilité des charges de travail		

3.2. Conformité automatisée

Conseil : Les fonctions automatisées de mise en conformité devraient réduire la surveillance manuelle tout en garantissant le respect continu des réglementations. Évaluez les solutions en fonction de leur capacité à détecter, signaler et corriger automatiquement les violations de la conformité dans plusieurs cadres réglementaires.

Exigence	Sous-exigence	O/N	Notes
Conformité automatisée	Évaluation continue de la conformité aux normes de l'industrie		
	Application continue de la conformité aux normes de l'industrie		

	Rationalisation du respect des exigences réglementaires grâce à la surveillance		
	Rationalisation du respect des exigences réglementaires grâce à l'établissement de rapports		

3.3. Détection des menaces et réaction

Conseil : Les capacités de détection et de réponse aux menaces avancées doivent s'appuyer à la fois sur des méthodes traditionnelles et sur des méthodes améliorées par l'IA. Recherchez des solutions capables de détecter les menaces en temps réel et de fournir des recommandations de réponse exploitables.

Exigence	Sous-exigence	O/N	Notes
Détection des menaces et réaction	Identification en temps réel des menaces tout au long du cycle de vie des applications		
	Atténuation en temps réel des menaces tout au long du cycle de vie des applications		
	Détection des menaces améliorée par l'IA grâce à l'analyse avancée		
	Détection des menaces améliorée par l'IA grâce à l'analyse prédictive		
	Mise en œuvre d'un système intelligent de détection et de réponse dans le nuage (CDR)		
	Détection des menaces en temps réel avec analyse des intentions		

3.4. Gestion des politiques

Conseil : une gestion efficace des politiques exige à la fois de la cohérence et de l'intelligence. Évaluez les solutions en fonction de leur capacité à maintenir des politiques de sécurité uniformes dans divers environnements tout en exploitant l'IA pour optimiser et adapter les politiques en fonction des menaces émergentes et des besoins de l'organisation.

Exigence	Sous-exigence	O/N	Notes
Gestion des politiques	Définition cohérente des politiques de sécurité dans tous les environnements		
	Application cohérente des politiques de sécurité dans tous les environnements		
	Capacités de gestion des politiques renforcées par l'IA		
	Des recommandations politiques intelligentes		

3.5. L'évolutivité

Conseil : l'évolutivité est essentielle pour les entreprises en pleine croissance. Recherchez des solutions capables d'évoluer de manière transparente avec votre infrastructure tout en maintenant les performances. Prenez en compte les capacités d'évolution horizontale et verticale, ainsi que la capacité à gérer les pics soudains de la charge de travail.

Exigence	Sous-exigence	O/N	Notes
Évolutivité	Capacité à s'adapter à des environnements dynamiques en nuage		
	Prise en charge des charges de travail croissantes		
	Maintien des performances à grande échelle		

3.6. Capacités d'intégration

Conseil : les capacités d'intégration sont essentielles pour créer un écosystème de sécurité cohérent. Évaluez les solutions en fonction de leur capacité à s'intégrer à votre chaîne d'outils existante et de la facilité à mettre en œuvre de nouvelles intégrations.

Exigence	Sous-exigence	O/N	Notes
Capacités d'intégration	Intégration transparente avec les outils de développement existants		

	Intégration transparente avec les outils de sécurité		
	Intégration transparente avec les outils de gestion de l'informatique en nuage		
	Intégration facile avec les écosystèmes SecOps pour des alertes en temps réel		

3.7. Couverture de sécurité multi-cloud

Conseil : Une sécurité multi-cloud complète est essentielle dans les divers environnements cloud d'aujourd'hui. Recherchez des solutions qui offrent des contrôles de sécurité cohérents pour tous les principaux fournisseurs de cloud, tout en tenant compte des nuances propres à chacun d'entre eux.

Exigence	Sous-exigence	O/N	Notes
Couverture de sécurité multi-cloud	Visibilité sur les environnements IaaS		
	Visibilité des environnements PaaS		
	Visibilité sur les environnements sans serveur		
	Support pour AWS		
	Support pour Azure		
	Prise en charge de Google Cloud		

3.8. Analyse de l'infrastructure en tant que code (IaC)

Conseil : les capacités d'analyse de l'IaC doivent permettre de détecter les problèmes de sécurité dès le début du cycle de développement. Recherchez des solutions qui s'intègrent à votre flux de travail de développement et fournissent des conseils de remédiation exploitables.

Exigence	Sous-exigence	O/N	Notes

Analyse de l'infrastructure en tant que code	Détection des failles de sécurité dans le code de l'infrastructure avant son déploiement		
	Prise en charge de plusieurs cadres IaC		
	Validation avant déploiement		
	Application des meilleures pratiques en matière de sécurité		

3.9. Analyse des conteneurs et de Kubernetes

Conseil : La sécurité des conteneurs nécessite une analyse complète tout au long du cycle de vie des conteneurs. Évaluez les solutions en fonction de leur capacité à analyser les images de conteneurs , à détecter les vulnérabilités d'exécution et à fournir des contrôles de sécurité spécifiques à Kubernetes.

Exigence	Sous-exigence	O/N	Notes
Analyse des conteneurs et de Kubernetes	Identification des vulnérabilités dans les applications conteneurisées		
	Contrôle de la sécurité des conteneurs en cours d'exécution		
	Évaluation de la sécurité des clusters Kubernetes		
	Numérisation de l'image du conteneur		

3.10. Protection des données

Conseil : Les capacités de protection des données doivent couvrir les données au repos et en mouvement. Recherchez des solutions qui offrent des contrôles complets de la sécurité des données, y compris la classification, le cryptage et la surveillance de l'accès.

Exigence	Sous-exigence	O/N	Notes
Protection des données	Surveillance des données en vue d'une éventuelle exfiltration		

	Capacités de classification des données		
	Capacités d'inspection des données		
	Prévention de l'exfiltration des données		

3.11. Hiérarchisation des risques

Conseil : une hiérarchisation efficace des risques permet de concentrer les efforts de sécurité sur les menaces les plus critiques. Recherchez des solutions qui utilisent l'IA pour analyser les risques dans le contexte de votre environnement et de l'impact sur votre activité.

Exigence	Sous-exigence	O/N	Notes
Hiérarchisation des risques	Analyse des risques par l'IA		
	Hiérarchisation des risques par l'IA		
	Corrélation des vulnérabilités		
	Analyse du contexte tout au long du cycle de développement		
	Cartographie des relations tout au long du cycle de développement		

3.12. Sécurité renforcée par l'IA pour les applications d'entreprise basées sur l'IA

Conseil : la sécurité des applications d'IA nécessite des capacités spécialisées. Recherchez des solutions qui comprennent les modèles de charge de travail de l'IA/ML et peuvent protéger contre les menaces spécifiques à l'IA.

Exigence	Sous-exigence	O/N	Notes
Sécurité des applications d'IA	Posture de sécurité pour les applications de la GenAI		
	Protection contre les menaces pour les applications GenAI		

	Gestion de la posture de sécurité par l'IA (AI-SPM)		
	Capacités de découverte de la charge de travail par l'IA		
	Capacités de sécurité de la charge de travail de l'IA		

3.13. Remédiation pilotée par la GenAI

Conseil : la remédiation par l'IA générique doit fournir des solutions exploitables et adaptées au contexte. Évaluez la qualité et la praticité des suggestions de remédiation générées par l'IA.

Exigence	Sous-exigence	O/N	Notes
Remédiation basée sur la GenAI	Suggestions de remédiation en fonction du contexte à l'aide de l'IA générative		
	Génération de lignes directrices pour la console		
	Génération de commandes CLI		
	Génération d'extraits de code		

3.14. Triage et hiérarchisation des alertes par l'IA

Conseil : La gestion des alertes doit permettre de réduire efficacement le bruit tout en garantissant que les problèmes critiques sont traités. Recherchez des solutions qui utilisent l'IA pour classer et hiérarchiser intelligemment les alertes.

Exigence	Sous-exigence	O/N	Notes
Triage et hiérarchisation des alertes	Modèles IA/ML pour l'analyse des alertes		
	Modèles IA/ML pour la catégorisation des alertes		

	Modèles IA/ML pour la hiérarchisation des alertes		
	Capacités de réduction de la fatigue des alertes		

3.15. Enrichissement contextuel avec l'IA

Conseil : L'enrichissement contextuel doit permettre d'obtenir des informations significatives pour une meilleure prise de décision. Recherchez des solutions capables de combiner intelligemment plusieurs sources de données pour fournir un contexte plus riche.

Exigence	Sous-exigence	O/N	Notes
Enrichissement contextuel	Enrichissement des données d'alerte par l'IA		
	Aide à la prise de décision éclairée		
	Intégration de l'analyse d'impact sur l'entreprise		
	Amélioration des processus de hiérarchisation		

3.16. Apprentissage adaptatif de l'IA

Conseil : Les capacités d'apprentissage adaptatif garantissent une amélioration continue des mesures de sécurité. Recherchez des solutions capables d'apprendre de votre environnement et de s'adapter aux nouvelles menaces.

Exigence	Sous-exigence	O/N	Notes
Apprentissage adaptatif de l'IA	Amélioration continue des recommandations de l'IA		
	Mise en œuvre des boucles de rétroaction		
	Apprentissage contextuel trans-CNAPP		

	Intégration rapide d'une nouvelle couverture de sécurité		

3.17. Requête sur le graphe de sécurité

Conseil : les capacités d'interrogation des graphes de sécurité doivent fournir des outils d'analyse puissants et conviviaux. Recherchez des solutions qui offrent des interfaces visuelles et programmatiques pour l'analyse des données de sécurité.

Exigence	Sous-exigence	O/N	Notes
Requête sur le graphe de sécurité	Recherche complète parmi les fournisseurs de services en nuage		
	Outils de visualisation des données de sécurité		
	Création d'une politique de sécurité à partir d'un générateur de requêtes		
	Capacités de gestion de la politique de sécurité		

4. Exigences techniques

4.1. Architecture de la plate-forme

- Conception orientée vers l'informatique en nuage
- Architecture microservices
- Infrastructure évolutive
- Haute disponibilité

4.2. Capacités d'intégration

- Une conception fondée sur l'API
- Intégration des outils DevOps
- Intégration SIEM
- Soutien à l'intégration personnalisée

4.3. Normes de performance

- Traitement en temps réel
- Latence minimale
- Performances évolutives
- Optimisation des ressources

4.4. IA et apprentissage automatique

- Modèles ML avancés
- Analyse en temps réel
- Capacités prédictives
- Apprentissage continu

5. Exigences supplémentaires

5.1. Interface utilisateur

- Interface web intuitive
- Tableaux de bord personnalisables
- Contrôle d'accès basé sur les rôles
- Accessibilité mobile

5.2. Options de déploiement

- Déploiement SaaS
- Options de déploiement hybride
- Prise en charge multirégionale
- Reprise après sinistre

5.3. Soutien et formation

- Assistance technique 24 heures sur 24, 7 jours sur 7
- Documentation complète

- Ressources de formation
- Services professionnels

5.4. Performance et évolutivité

- Soutien à l'échelle de l'entreprise
- Garanties de performance
- Mesures d'évolutivité
- Logement de croissance

6. Critères d'évaluation des fournisseurs

Critère	Poids	Description
Complétude de la solution CNAPP	20%	Couverture complète des fonctionnalités requises
Capacités en matière d'IA/ML	15%	Force des fonctions d'IA et d'apprentissage automatique
Support multi-cloud	15%	Couverture et intégration des fournisseurs de services en nuage
Évolutivité	10%	Performance à l'échelle de l'entreprise
Expérience des utilisateurs	10%	Convivialité et accessibilité de l'interface
Analyse	10%	Capacités de reporting et d'analyse
Conformité	10%	Couverture réglementaire et certifications
Soutien	5%	Assistance technique et services professionnels
Coût	5%	Coût total de possession

7. Exigences en matière de soumission

7.1. Proposition technique

- Architecture détaillée de la solution

- Matrice de couverture des caractéristiques
- Capacités d'intégration
- Capacités en matière d'IA/ML
- Contrôles de sécurité

7.2. Plan de mise en œuvre

- Méthodologie de déploiement
- Chronologie
- Besoins en ressources
- Atténuation des risques

7.3. Structure des prix

- Modèle de licence
- Coûts de mise en œuvre
- Coûts de soutien
- Coûts de formation

7.4. Informations sur les entreprises

- Expérience
- Études de cas
- Références
- Feuille de route pour l'innovation

7.5. Détails du support

- Conditions de l'ANS
- Niveaux de soutien
- Approche de la formation

- Services professionnels

8. 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]

Informations de contact :

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