Demande de proposition : Solution logicielle de gestion de la posture de sécurité en nuage (CSPM)

Table des matières

1. Introduction

1.1 Objectif

Le présent appel d'offres vise à obtenir des propositions pour une solution de gestion de la sécurité de l'informatique en nuage (CSPM) afin d'améliorer la sécurité de l'informatique en nuage de notre organisation, de garantir la conformité et de gérer les risques dans l'ensemble de nos environnements en nuage.

1.2 Contexte

Le logiciel CSPM est conçu pour surveiller, détecter et répondre en permanence aux risques de sécurité et aux problèmes de conformité dans les infrastructures en nuage, y compris les environnements IaaS, PaaS et SaaS.

2. Exigences de la solution

2.1 Fonctionnalité de base

2.1.1 Contrôle continu

- Surveillance en temps réel des ressources en nuage
- Détection des mauvaises configurations et des vulnérabilités

2.1.2 Remédiation automatisée

- Correction automatique des problèmes identifiés
- Réduction des erreurs humaines dans la gestion de la sécurité

2.1.3 Gestion de la conformité

- Contrôle de l'état de conformité
- Génération de rapports de conformité
- Aide au respect des normes et réglementations du secteur

2.1.4 Évaluation des risques

- Évaluation et hiérarchisation des risques de sécurité
- Se concentrer sur les menaces à fort impact

2.1.5 Capacités d'intégration

- Intégration transparente avec les outils de sécurité existants
- Compatibilité avec diverses plates-formes en nuage

2.2 Exigences fonctionnelles

2.2.1 Collecte et agrégation des données

Conseil : Un système de collecte de données robuste constitue la base d'une GRC efficace. Tenez compte du volume, de la variété et de la rapidité des sources de données que votre organisation doit surveiller, et assurez-vous que la solution peut répondre à vos besoins actuels et prévus en matière d'ingestion de données tout en maintenant les performances.

Sous-exigence	O/N	Notes

Recueillir des données à partir des journaux de l'informatique en nuage		
Recueillir des données sur le trafic réseau		
Recueillir des données sur l'activité des points d'extrémité		
Fournir une visibilité complète de l'environnement en nuage		

2.2.2 Détection des menaces

Conseil : les méthodes de détection multiples fonctionnant de concert offrent la couverture la plus complète des menaces. Évaluez la manière dont chaque méthode de détection complète les autres et tenez compte des taux de faux positifs en même temps que de l'efficacité de la détection.

Sous-exigence	O/N	Notes
Utiliser la détection basée sur les signatures		
Utiliser des algorithmes d'apprentissage automatique		
Utiliser l'analyse comportementale		
Identifier les menaces potentielles en temps réel		

2.2.3 Capacités de réponse aux incidents

Conseil : la rapidité et l'efficacité de la réponse aux incidents ont un impact direct sur l'endiguement des incidents de sécurité. Recherchez des capacités d'automatisation qui peuvent réduire les temps de réponse tout en maintenant une supervision humaine appropriée pour les décisions critiques.

Sous-exigence	O/N	Notes
Permettre l'isolement des systèmes affectés		
Permettre le blocage du trafic malveillant		
Faciliter l'ouverture d'enquêtes		
Soutenir la gestion des enquêtes		

2.2.4 Gestion des alertes

Conseil : La fatigue des alertes peut avoir un impact significatif sur l'efficacité de l'équipe de sécurité. Privilégiez les solutions qui offrent une corrélation et une hiérarchisation intelligentes des alertes afin de garantir que les alertes critiques reçoivent l'attention nécessaire tout en réduisant le bruit des faux positifs.

Sous-exigence	O/N	Notes
Hiérarchiser les alertes en fonction de leur criticité		
Hiérarchiser les alertes en fonction de leur impact potentiel		
Mise en œuvre d'un traitement intelligent des alertes		
Réduire la fatigue liée à l'alerte		

2.2.5 Évolutivité et adaptabilité

Conseil : Les environnements en nuage peuvent se développer rapidement et changer fréquemment. Assurez-vous que la solution peut évoluer horizontalement et verticalement pour faire face à la croissance tout en maintenant les performances, et s'adapter aux nouveaux services et modèles architecturaux de l'informatique en nuage.

Sous-exigence	O/N	Notes
Évoluer pour s'adapter aux organisations de toutes tailles		
S'adapter à des environnements complexes en nuage		
Prise en charge de l'allocation dynamique des ressources		
Gérer efficacement les pics de charge		

2.2.6 Gestion de la confidentialité des données

Conseil : Les exigences en matière de confidentialité des données varient selon les secteurs et les régions. Vérifiez que la solution prend en charge vos exigences de conformité spécifiques et fournit des contrôles granulaires pour

l'accès, le stockage et la transmission des données dans différents environnements en nuage.

Sous-exigence	O/N	Notes
Gérer en toute sécurité les informations sensibles		
Mettre en œuvre des mesures robustes de protection des données		
Prise en charge des déploiements multi-cloud		
Fournir des pistes d'audit pour l'accès aux données		

2.3 Fonctionnalités alimentées par l'IA

2.3.1 Gestion de la posture de sécurité par l'IA (AI-SPM)

Conseil : La gestion de la posture de sécurité de l'IA nécessite une visibilité spécialisée sur les charges de travail et l'infrastructure de l'IA/ML. Assurez-vous que la solution comprend les défis de sécurité uniques des systèmes d'IA et peut fournir des informations significatives sur l'état de sécurité de votre pile d'IA.

Sous-exigence	O/N	Notes
Fournir une visibilité sur la sécurité des services GenAI		
Proposer un inventaire de la pile d'IA (modèles, données, infrastructure)		
Identifier les vulnérabilités spécifiques à l'IA		
Cartographier les voies d'attaque potentielles dans les environnements d'IA		

2.3.2 Amélioration de la détection grâce à l'IA et à l'apprentissage automatique

Conseil : La détection assistée par l'IA doit compléter les méthodes traditionnelles tout en minimisant les faux positifs. Recherchez des solutions qui présentent des avantages évidents en termes de précision et de rapidité de détection par rapport aux approches conventionnelles.

Sous-exigence	O/N	Notes
Utiliser des algorithmes avancés pour la détection de modèles		
Utiliser des algorithmes avancés pour la détection des anomalies		
Détection en temps réel des menaces complexes		

2.3.3 Hiérarchisation des risques par l'IA

Conseil : une hiérarchisation efficace des risques est cruciale pour l'affectation des ressources. Le système d'IA doit fournir une justification claire de ses évaluations de risques et permettre une personnalisation en fonction de la tolérance au risque spécifique de votre organisation.

Sous-exigence	O/N	Notes
Analyser le rayon d'explosion des biens à risque		
Découvrir efficacement les risques complexes		
Hiérarchiser les risques identifiés		

2.3.4 Analyse prédictive

Conseil : Les capacités prédictives doivent fournir des informations exploitables plutôt que de simples possibilités théoriques. Privilégiez les solutions qui ont fait leurs preuves en matière de prédictions précises et de recommandations claires en matière d'atténuation des risques.

Sous-exigence	O/N	Notes
Anticiper les vulnérabilités potentielles avant leur exploitation		
Permettre des stratégies proactives de gestion des risques		

2.3.5 Copilote IA pour la GPSC

Conseil : Les assistants d'IA doivent améliorer l'efficacité de l'opérateur sans remplacer le jugement humain. Évaluez dans quelle mesure le copilote s'intègre dans les flux de travail existants et s'il fournit des explications claires sur ses recommandations.

Sous-exigence	O/N	Notes
Permettre des requêtes en langage naturel pour l'interaction avec le système		
Fournir des informations rapides sur le niveau de sécurité		
Proposer des recommandations de remédiation		
Proposer des flux de travail optimaux		

2.3.6 Contrôle automatisé de la conformité grâce à l'IA

Conseil : Le contrôle de la conformité piloté par l'IA doit s'adapter aux changements réglementaires tout en conservant sa précision. Vérifiez la capacité de la solution à interpréter les nouvelles exigences de conformité et à les traduire en contrôles exploitables.

Sous-exigence	O/N	Notes
S'adapter aux changements réglementaires avec une intervention humaine minimale		
Surveillance en temps réel d'un large éventail de réglementations		
Générer des rapports de conformité		

2.3.7 Prévision des menaces par l'IA

Conseil : la prévision des menaces doit combiner les renseignements sur les menaces globales et le contexte local. Recherchez des solutions capables de démontrer l'exactitude de leurs prévisions et de les justifier clairement.

Sous-exigence	O/N	Notes
Utiliser l'apprentissage automatique pour améliorer les capacités prédictives		
Permettre une prévision précise des menaces		
Détection des anomalies		

2.3.8 Sécurité des applications d'IA générative

Conseil : la sécurité de l'IA générative nécessite une compréhension spécialisée des vulnérabilités des modèles d'IA et des risques liés à la chaîne d'approvisionnement. Assurez-vous que la solution peut surveiller et protéger efficacement les modèles d'IA et leur infrastructure de soutien.

Sous-exigence	O/N	Notes
Découvrir et évaluer les risques de sécurité dans les applications d'IA générative		
Identifier les vulnérabilités dans les dépendances de la bibliothèque d'IA		
Analyser le code source pour détecter les mauvaises configurations de l'infrastructure en tant que code		

3. Exigences techniques

3.1 Compatibilité des plateformes d'informatique dématérialisée

- Prise en charge des principaux fournisseurs de services en nuage (AWS, Azure, Google Cloud)
- Prise en charge des environnements multi-cloud et cloud hybride
- Intégration basée sur l'API avec les outils de sécurité existants
- Prise en charge des systèmes courants de gestion des informations et des événements de sécurité (SIEM)

3.2 Capacités d'intégration

- Intégration basée sur l'API avec les outils de sécurité existants
- Prise en charge des systèmes courants de gestion des informations et des événements de sécurité (SIEM)

3.3 Évolutivité

- Capacité à gérer des déploiements à grande échelle dans le nuage
- Optimisation des performances pour le traitement de gros volumes de données

3.4 Gestion des données

- Stockage et traitement sécurisés des données
- Capacités de conservation et d'archivage des données

4. Rapports et analyses

4.1 Tableaux de bord et visualisation

- Tableaux de bord personnalisables pour différents rôles d'utilisateurs
- Visualisation en temps réel de la posture de sécurité

4.2 Capacités d'établissement de rapports

- Génération de rapports automatisés à des fins de conformité et d'audit
- Modèles de rapports personnalisables

5. Soutien et maintenance

5.1 Assistance technique

- Assistance disponible 24 heures sur 24 et 7 jours sur 7
- Plusieurs canaux d'assistance (téléphone, e-mail, chat)

5.2 Mises à jour et mises à niveau

- Mises à jour régulières des logiciels et correctifs de sécurité
- Voie de mise à niveau claire pour les versions futures

6. Formation et documentation

6.1 Formation des utilisateurs

- Programme de formation complet pour les administrateurs et les utilisateurs finaux
- Options de formation en ligne et en personne

6.2 Documentation

- Manuels d'utilisation et d'administration détaillés
- Mises à jour régulières de la documentation

7. Prix et licences

7.1 Modèle de tarification

- Explication claire de la structure tarifaire (par utilisateur, par actif, etc.)
- Remises sur volume ou avantages liés à un engagement à long terme

7.2 Conditions d'octroi des licences

- Flexibilité des options de licence
- Toute restriction ou limitation d'utilisation

8. Informations sur le fournisseur

8.1 Profil de l'entreprise

- Bref historique et historique de l'entreprise
- Stabilité financière et position sur le marché

8.2 Références

- Fournir au moins trois références d'organisations de taille similaire
- Des études de cas démontrant des mises en œuvre réussies

9. Critères d'évaluation

Les propositions seront évaluées sur la base des éléments suivants

- Exhaustivité de la solution par rapport aux exigences énoncées
- Fonctionnalités innovantes, en particulier les fonctionnalités basées sur l'IA
- Facilité d'utilisation et d'intégration
- Évolutivité et performance
- Prix et coût total de possession
- Réputation du fournisseur et capacités d'assistance

10. Instructions relatives à la soumission

Les propositions doivent comprendre

- Réponse détaillée à toutes les exigences
- Plan de mise en œuvre et calendrier
- Informations sur les prix

- Informations et références sur l'entreprise
- Exemples de rapports et de documentation