Demande de proposition : Plateforme de protection de la charge de travail en nuage

Table des matières

1. Introduction

Le présent appel d'offres porte sur une plateforme de protection des charges de travail en nuage (CWPP). Les CWPP sont des solutions de sécurité spécialisées conçues pour protéger les charges de travail - telles que les applications, les bases de données et les services - dans divers environnements en nuage, y compris les nuages publics, privés et hybrides. Ces plateformes offrent une visibilité complète, une détection des menaces et des réponses automatisées pour garantir l'intégrité et la sécurité des opérations basées sur le cloud.

2. Principaux avantages

La solution proposée doit offrir les avantages clés suivants :

1. Posture de sécurité renforcée
    - Protection complète contre les menaces
    - Mesures de sécurité proactives
    - Renseignements sur les menaces avancées
2. Efficacité opérationnelle
    - Rationalisation des opérations de sécurité
    - Processus de sécurité automatisés
    - Réduction des interventions manuelles
3. Évolutivité
    - Prise en charge des environnements en nuage en pleine croissance
    - Optimisation des performances
    - Gestion des ressources
4. Assurance de la conformité
    - Gestion de la conformité réglementaire
    - Contrôle automatisé de la conformité
    - Rapport de conformité
5. Gestion inter-cloud
    - Sécurité unifiée sur les plates-formes en nuage
    - Application cohérente de la politique
    - Gestion centralisée

3. Caractéristiques principales

Les fournisseurs doivent démontrer leurs capacités dans les domaines essentiels suivants :

1. Découverte et visibilité automatisées

- Recherche d'actifs en temps réel
- Visibilité complète sur l'ensemble des environnements
- Cartographie des ressources

2. Détection des menaces et réaction
    - Détection avancée des menaces
    - Capacités de réponse automatisée
    - Gestion des incidents
3. Durcissement de la charge de travail
    - Gestion de la configuration de la sécurité
    - Gestion de la vulnérabilité
    - Durcissement du système
4. Découverte d'actifs
    - Surveillance continue des actifs
    - Classification des actifs
    - Gestion des stocks
5. Détection des anomalies
    - Analyse comportementale
    - Reconnaissance des formes
    - Génération d'alertes
6. Sécurité des données
    - Protection des données
    - Gestion du chiffrement
    - Contrôle d'accès

7. Gouvernance
    - Gestion des politiques
    - Contrôle de conformité
    - Évaluation des risques
8. Journalisation et rapports
    - Enregistrement complet
    - Rapports personnalisés
    - Tableaux de bord analytiques

4. Exigences fonctionnelles

4.1 Collecte et agrégation des données

Conseil : une collecte et une agrégation efficaces des données constituent la base de votre solution CWPP. Concentrez-vous sur des capacités complètes de collecte de données dans tous les environnements en nuage, tout en tenant compte de l'impact sur les performances et des exigences en matière de stockage. Recherchez des solutions capables de traiter de gros volumes de données en temps réel.

Exigence	Sous-exigence	O/N	Notes
Collecte et agrégation des données	Collecte auprès de plusieurs fournisseurs de services en nuage (AWS, Azure, GCP)		
	Collecte de données en temps réel à partir de charges de travail en nuage		
	Collecte et agrégation de données		
	Collecte d'indicateurs de performance		
	Collecte des données de configuration		
	Surveillance du trafic sur le réseau		
	Collecte de données au niveau de l'API		

4.2 Détection des menaces

Conseil : Les capacités de détection des menaces avancées doivent combiner plusieurs méthodes de détection afin de fournir une protection complète. Envisagez des solutions qui exploitent à la fois la détection traditionnelle basée sur les signatures et l'analyse moderne basée sur le ML afin de minimiser les faux positifs tout en maintenant des taux de détection élevés.

Exigence	Sous-exigence	O/N	Notes
Détection des menaces	Détection basée sur la signature		
	Analyse de l'apprentissage automatique		
	Analyse comportementale		
	Analyse de la vulnérabilité		
	Détection des logiciels malveillants		
	Détection des menaces de type "jour zéro		
	Détection des menaces persistantes avancées (APT)		

4.3 Réponse aux incidents

Conseil : Les capacités de réponse automatisée aux incidents sont essentielles pour maintenir la sécurité dans les environnements en nuage où les menaces peuvent se propager rapidement. Assurez-vous que la solution offre des options de réponse automatisées et manuelles avec des flux de travail et des pistes d'audit clairs.

Exigence	Sous-exigence	O/N	Notes
Réponse aux incidents	Confinement automatisé des menaces		
	Capacités d'isolation du système		
	Mécanismes de blocage du trafic		

	Flux de travail automatisés pour la remédiation		
	Exécution de la procédure en cas d'incident		
	Options de réponse manuelle		
	Outils d'analyse post-incident		

4.4 Priorité aux alertes

Conseil : une hiérarchisation efficace des alertes est essentielle pour gérer les opérations de sécurité à grande échelle. Recherchez des solutions qui utilisent des algorithmes intelligents pour réduire la fatigue des alertes tout en veillant à ce que les menaces critiques ne passent pas inaperçues.

Exigence	Sous-exigence	O/N	Notes
Priorité aux alertes	Classement des alertes en fonction du risque		
	Capacités de corrélation des alertes		
	Règles d'alerte personnalisées		
	Options de suppression des alertes		
	Triage automatisé des alertes		
	Enrichissement du contexte d'alerte		
	Analyse historique des alertes		

4.5 Gestion de la conformité

Conseil : Les fonctions complètes de gestion de la conformité doivent prendre en charge à la fois les cadres réglementaires standard et les politiques de conformité personnalisées. Envisagez des solutions qui automatisent le contrôle de la conformité et l'établissement de rapports afin de réduire les exigences en matière de contrôle manuel.

Exigence	Sous-exigence	O/N	Notes

Gestion de la conformité	Application de la réglementation de l'industrie		
	Capacités de suivi des politiques		
	Outils de rapport de conformité		
	Création de politiques personnalisées		
	Contrôles de conformité automatisés		
	Alertes de violation de la conformité		
	Maintenance de la piste d'audit		

4.6 Évolutivité

Conseil : l'évolutivité est essentielle pour les environnements en nuage qui se développent. Évaluez les solutions en fonction de leur capacité à évoluer horizontalement et verticalement tout en maintenant les performances et l'efficacité de toutes les charges de travail protégées.

Exigence	Sous-exigence	O/N	Notes
Évolutivité	Prise en charge d'une charge de travail croissante		
	Capacités de mise à l'échelle inter-cloud		
	Fonctions d'optimisation des performances		
	Efficacité de l'utilisation des ressources		
	Mécanismes de mise à l'échelle automatique		
	Capacités d'équilibrage de la charge		
	Prise en charge multirégionale		

4.7 Intégration aux systèmes existants

Conseil : des capacités d'intégration solides garantissent que votre solution CWPP fonctionne de manière transparente avec votre infrastructure de

sécurité existante. Concentrez-vous sur la prise en charge des API standard et sur les intégrations prédéfinies avec les outils de sécurité courants.

Exigence	Sous-exigence	O/N	Notes
Capacités d'intégration	Intégration de l'API de l'outil de sécurité		
	Intégration SIEM		
	Intégration de la plate-forme SOAR		
	Intégration de la gestion de l'identité		
	Options de développement d'API personnalisées		
	Prise en charge des webhooks		
	Prise en charge de plugins tiers		

4.8 Gestion de la confidentialité des données

Conseil : Les fonctions de confidentialité des données doivent répondre à la fois aux exigences réglementaires et aux politiques de sécurité internes. Envisagez des solutions qui offrent un contrôle granulaire sur le traitement des données sensibles et des capacités de cryptage solides.

Exigence	Sous-exigence	O/N	Notes
Gestion de la confidentialité des données	Traitement des données sensibles		
	Mise en œuvre du cryptage		
	Fonctions de contrôle d'accès		
	Capacités de masquage des données		
	Application de la politique de protection de la vie privée		

	Outils de classification des données		
	Rapport sur le respect de la vie privée		

4.9 Capacités basées sur l'IA

Conseil : Les capacités d'IA devraient améliorer à la fois les opérations de sécurité et la détection des menaces. Recherchez des solutions qui démontrent des applications pratiques de l'IA/ML au-delà des mots à la mode du marketing, avec des avantages clairs pour les résultats de sécurité.

Exigence	Sous-exigence	O/N	Notes
Capacités basées sur l'IA	Surveillance de la sécurité de la charge de travail par l'IA		
	Étapes de remédiation générées par l'IA		
	Optimisation des politiques IAM		
	Descriptions d'alertes générées par l'IA		
	Détection intelligente des anomalies		
	Détection de modèles et de paquets par l'IA		
	Analyse de la trajectoire de l'attaque améliorée par l'IA		
	Gestion des stocks par l'IA		
	Politiques d'exécution spécifiques à l'IA		

5. Exigences en matière d'intégration

La solution CWPP doit s'intégrer avec :

- Systèmes de détection et de réponse des points finaux (EDR)
- Logiciel de sécurité des centres de données
- Plateformes de gestion de l'informatique en nuage
- Logiciel de conformité en nuage

6. Tendances émergentes

Les fournisseurs doivent préciser leur approche en matière de :

- Intégration de l'IA et de l'apprentissage automatique pour améliorer la détection et la réponse aux menaces.
- Shift-Left Pratiques de sécurité
- Intégration avec le Cloud Security Posture Management (CSPM)

7. Mise en œuvre et soutien

Les vendeurs doivent fournir des informations détaillées sur

- Processus et calendrier de mise en œuvre
- Formation et soutien à l'intégration
- Assistance technique permanente et accords de niveau de service
- Mises à jour régulières et gestion des correctifs

8. Conformité et certifications

Les vendeurs doivent préciser :

- Certifications sectorielles pertinentes (par exemple, ISO 27001, SOC 2)
- Conformité avec les réglementations en matière de protection des données (par exemple, GDPR, CCPA)

9. Modèle de tarification et de licence

Les vendeurs doivent fournir :

- Structure tarifaire détaillée
- Modèles de licence (par utilisateur, par charge de travail ou à l'échelle de l'entreprise)
- Coûts supplémentaires pour les fonctions premium ou l'assistance

10. Études de cas et références

Les vendeurs doivent inclure

- Études de cas pertinentes démontrant la réussite de la mise en œuvre du PPECF

- Références de clients dans des secteurs d'activité similaires ou avec des environnements "cloud" comparables

11. Critères d'évaluation

Les propositions seront évaluées sur la base des éléments suivants

- Complétude des caractéristiques
- Facilité d'utilisation et de gestion
- Évolutivité et performance
- Capacités d'intégration
- Capacités en matière d'IA et d'apprentissage automatique
- Prix et coût total de possession
- Réputation du fournisseur et qualité de l'assistance

Informations de contact : security@company.com

12. 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]