Demande de proposition: Solutions de gestion de la posture de sécurité SaaS (SSPM)

Table des matières

1. Introduction

SaaS Security Posture Management (SSPM) est une solution essentielle pour les organisations qui dépendent de plateformes en nuage pour leurs opérations critiques. Le logiciel SSPM protège en permanence les applications en nuage en détectant les vulnérabilités, en garantissant la conformité et en atténuant les risques de vol de données.

Cet appel d'offres vise à obtenir des propositions pour une solution SSPM qui assurera une protection complète de l'environnement SaaS de notre organisation, y compris le contrôle d'accès, la sécurité des données, la surveillance de la conformité et l'évaluation des risques.

2. Objectifs du projet

La solution doit fournir :

- Protection complète de l'environnement SaaS de l'entreprise
- Des mesures robustes de contrôle d'accès et de sécurité des données

- Contrôle continu de la conformité et établissement de rapports
- Capacités intégrées d'évaluation des risques
- Intégration transparente avec l'infrastructure existante
- Évolutivité pour soutenir la croissance de l'organisation

3. Champ d'application

Le champ d'application englobe

- Mise en œuvre d'une solution SSPM complète
- Intégration à l'infrastructure de sécurité existante
- Configuration et déploiement
- Formation du personnel et transfert de connaissances
- Soutien et maintenance continus
- Mises à jour régulières et gestion des correctifs

4. Exigences fonctionnelles

4.1 Découverte et inventaire des applications SaaS

Conseil : Base essentielle pour le SSPM qui nécessite une découverte automatisée et continue ainsi qu'une visibilité complète de toutes les applications SaaS afin de prévenir efficacement l'informatique parallèle et de maintenir le contrôle de la sécurité.

Exigence	Sous-exigence	O/N	Notes
Découverte et catalogage	Découverte automatique de toutes les applications SaaS		
	Catalogage et mise à jour des stocks en temps réel		
	Visibilité complète pour la prévention de l'informatique parallèle		
	Classification et catégorisation des actifs		

Gestion des stocks	Suivi et analyse de l'utilisation des applications		
	Contrôle de l'utilisation des licences		
	Gestion de la configuration		
	Suivi du contrôle des versions		

4.2 Surveillance continue et rapports

Conseil : Indispensable pour maintenir une sensibilisation à la sécurité en temps réel grâce à une surveillance active, une détection immédiate des menaces et des capacités de reporting complètes qui permettent d'obtenir des informations exploitables.

Exigence	Sous-exigence	O/N	Notes
Contrôle en temps réel	Détection des problèmes de sécurité et alertes		
	Analyse continue de l'environnement		
	Contrôle des performances		
	Suivi des changements de configuration		
Capacités d'établissement de rapports	Rapports sur la détection des anomalies		
	Génération de rapports personnalisables		
	Tableaux de bord spécifiques aux parties prenantes		
	Analyse des tendances et mesures		

4.3 Contrôle de l'activité des utilisateurs

Conseil : la surveillance du comportement des utilisateurs est la pierre angulaire de la veille de sécurité, car elle permet de détecter rapidement les

activités suspectes et les failles de sécurité potentielles grâce à l'analyse des schémas.

Exigence	Sous-exigence	O/N	Notes
Détection des comportements	Surveillance des activités suspectes en temps réel		
	Analyse des schémas d'accès des utilisateurs		
	Établissement d'une base comportementale		
	Détection des anomalies		
Réponse en matière de sécurité	Identification rapide des violations		
	Génération automatisée d'alertes		
	Flux de travail de la réponse aux incidents		
	Pistes d'audit de l'activité de l'utilisateur		

4.4 Contrôles de prévention des pertes de données (DLP)

Conseil : Les contrôles DLP doivent fournir une protection complète contre les fuites de données accidentelles et malveillantes tout en maintenant la productivité de l'entreprise grâce à une application intelligente des règles.

Exigence	Sous-exigence	O/N	Notes
Mise en œuvre de la politique	Création et gestion de politiques DLP		
	Identification des données sensibles		
	Automatisation de l'application des politiques		
	Création de règles personnalisées		

Protection des données	Prévention des fuites accidentelles		
	Prévention des fuites malveillantes		
	Classification des données		
	Contrôle du contenu		

4.5 Contrôle de conformité

Conseil : Le contrôle automatisé de la conformité doit permettre de suivre en permanence le respect des exigences réglementaires tout en offrant une visibilité claire sur l'état de la conformité et les besoins de remédiation.

Exigence	Sous-exigence	O/N	Notes
Suivi de la conformité	Surveillance continue de la posture		
	Adhésion à la réglementation de l'industrie		
	Tableau de bord de l'état de conformité		
	Analyse des lacunes		
Gestion de la réglementation	Contrôles spécifiques au cadre		
	Rapports de conformité automatisés		
	Application de la politique		
	Maintenance de la piste d'audit		

4.6 Gestion des mots de passe et des accès

Conseil : des politiques de mots de passe et de gestion des accès solides doivent permettre d'équilibrer la sécurité et la convivialité, en assurant une protection solide contre les accès non autorisés tout en préservant la productivité des utilisateurs.

Exigence	Sous-exigence	O/N	Notes

Protection par mot de passe	Détection des mots de passe faibles		
	Analyse de la force du mot de passe		
	Application de la mise à jour du mot de passe		
	Conformité de la politique en matière de mots de passe		
Application de la politique	Mise en œuvre d'une politique de mots de passe forts		
	Gestion de l'expiration des mots de passe		
	Application de l'historique des mots de passe		
	Règles de complexité des mots de passe		

4.7 Évaluation des risques et remédiation

Conseil : Les systèmes d'évaluation des risques doivent fournir des informations exploitables grâce à une évaluation précise de la gravité et à des voies de remédiation claires, ce qui permet aux organisations de se concentrer d'abord sur les problèmes de sécurité les plus critiques.

Exigence	Sous-exigence	O/N	Notes
Évaluation des risques	Analyse de la gravité des risques de sécurité		
	Évaluation des risques en temps réel		
	Évaluation de la vulnérabilité		
	Hiérarchisation des menaces		
Remédiation	Conseils automatisés en matière de remédiation		
	Priorité à l'action		

	Gestion du flux de travail de l'assainissement		
	Vérification de l'assainissement		

4.8 Capacités d'intégration

Conseil : les capacités d'intégration doivent permettre une connexion transparente avec l'infrastructure de sécurité existante tout en restant suffisamment souples pour s'adapter aux nouvelles applications et à l'évolution des besoins en matière de sécurité.

Exigence	Sous-exigence	O/N	Notes
Intégration SaaS	Intégration transparente des applications		
	Connectivité basée sur l'API		
	Soutien à l'intégration personnalisée		
	Synchronisation des données en temps réel		
Adaptabilité	Nouveau support d'application		
	Évolutivité de l'intégration		
	Compatibilité multiplateforme		
	Contrôle de l'intégration		

4.9 Contrôle d'accès par des tiers

Conseil : la gestion des accès des tiers nécessite un contrôle granulaire et une surveillance continue afin de minimiser les risques de sécurité tout en maintenant les relations commerciales nécessaires.

Exigence	Sous-exigence	O/N	Notes
Accès Visibilité	Surveillance des applications par des tiers		
	Suivi des autorisations d'accès		
	Analyse de l'utilisation		

	Évaluation des risques		
Gestion de l'accès	Gestion des autorisations		
	Capacités de révocation d'accès		
	Automatisation de l'examen de l'accès		
	Gestion du cycle de vie de l'accès des fournisseurs		

4.10 Inspections de sécurité

Conseil : Les inspections de sécurité complètes doivent couvrir tous les aspects de la posture de sécurité tout en garantissant la conformité avec les réglementations et les normes industrielles pertinentes.

Exigence	Sous-exigence	O/N	Notes
Contrôle d'accès	Inspection de la politique d'accès		
	Audit des autorisations		
	Examen de l'accès en fonction des rôles		
	Vérification de l'authentification		
Protection des données	Inspection DLP		
	Analyse antivirus		
	Vérification du cryptage		
	Conformité du traitement des données		

4.11 Remédiation automatisée

Conseil : La remédiation automatisée doit minimiser les interventions manuelles tout en garantissant la précision et en maintenant des pistes d'audit claires de toutes les actions automatisées entreprises.

Exigence	Sous-exigence	O/N	Notes

Automatisation	Remédiation aux erreurs de configuration		
	Application de la politique		
	Déploiement de correctifs de sécurité		
	Normalisation de la configuration		
Gestion des alertes	Génération d'alertes claires		
	Réduction des faux positifs		
	Priorité aux alertes		
	Suivi de l'assainissement		

4.12 Évolutivité

Conseil : les fonctions d'évolutivité doivent garantir des performances et une sécurité constantes au fur et à mesure de la croissance de l'organisation, en gérant l'augmentation de la charge sans compromettre l'efficacité.

Exigence	Sous-exigence	O/N	Notes
Soutien à la croissance	Élargissement de la base d'applications		
	Gestion du volume des utilisateurs		
	Maintien des performances		
	Optimisation des ressources		
Adaptation à l'environnement	Mise à l'échelle de l'environnement en nuage		
	Flexibilité de l'infrastructure		
	Équilibrage de la charge		
	Planification des capacités		

4.13 Sécurité de l'API

Conseil : La sécurité de l'API doit garantir une transmission sécurisée des données tout en assurant une surveillance et un contrôle complets de toutes les interactions de l'API.

Exigence	Sous-exigence	O/N	Notes
Contrôle d'accès	Surveillance de l'accès à l'API		
	Application de l'authentification		
	Gestion des autorisations		
	Limitation du taux		
Sécurité des données	Application de la politique de partage des données		
	Cryptage du trafic		
	Validation des données		
	Tests de sécurité		

4.14 Intégration de l'apprentissage automatique et de l'IA

Conseil : Les capacités d'IA/ML devraient améliorer la détection et la prévention des menaces tout en fournissant des informations exploitables grâce à des analyses avancées et à la reconnaissance des formes.

Exigence	Sous-exigence	O/N	Notes
Détection des menaces	Détection par ML		
	Reconnaissance des formes		
	Analyse comportementale		
	Analyse prédictive		
La prévention	Identification des menaces émergentes		
	Réponse automatisée		

	Prévision des risques		
	Apprentissage continu		

4.15 Automatisation de la conformité

Conseil : L'automatisation de la conformité doit permettre de rationaliser l'adhésion à de multiples cadres réglementaires tout en conservant une documentation précise et des preuves de conformité.

Exigence	Sous-exigence	O/N	Notes
Rapports	Rapports de conformité automatisés		
	Modèles spécifiques au cadre		
	Génération de rapports personnalisés		
	Collecte de preuves		
Gestion des normes	Paramètres de conformité préconfigurés		
	Remédiation aux lacunes		
	Cartographie de contrôle		
	Contrôle de conformité		

4.16 Évaluation des risques pilotée par l'IA

Conseil : L'évaluation des risques pilotée par l'IA devrait fournir des informations approfondies sur la posture de sécurité tout en maintenant la précision et en fournissant des conseils clairs en matière de remédiation.

Exigence	Sous-exigence	O/N	Notes
Analyse des risques	Évaluation des risques liés aux applications par des tiers		
	Évaluation des extensions de navigateur		
	Automatisation de l'évaluation des risques		

	Hiérarchisation des menaces		
Rapport d'évaluation	Rapports automatisés sur les risques		
	Analyse de la conformité de la sécurité		
	Tendance des risques		
	Recommandations de remédiation		

4.17 Gestion de la posture de sécurité de l'IA

Conseil : L'AI-SPM doit fournir une visibilité et une protection complètes des actifs de l'IA tout en maintenant un inventaire détaillé et des contrôles de sécurité.

Exigence	Sous-exigence	O/N	Notes
Visibilité de l'IA	Suivi du déploiement du modèle		
	Suivi du projet		
	Détection des risques		
	Contrôle d'accès		
Gestion des actifs	Maintenance des stocks d'IA		
	Gestion des nomenclatures		
	Suivi de la configuration		
	Évaluation de la sécurité		

4.18 Sécurité du modèle d'IA

Conseil : La sécurité des modèles d'IA doit assurer une protection complète des configurations et des données des modèles tout en maintenant des contrôles d'accès et une surveillance stricts.

Exigence	Sous-exigence	O/N	Notes

Sécurité de la configuration	Mise en œuvre de la sécurité des réseaux		
	Mesures de protection des données		
	Gestion du contrôle d'accès		
	Audit de la configuration du modèle		
Contrôle	Contrôle des clés d'accès		
	Détection des données sensibles		
	Suivi de l'utilisation		
	Alertes de sécurité		

4.19 GenAI App Management

Conseil : la gestion des applications GenAI doit fournir un contrôle et une sécurité de niveau entreprise tout en conservant la flexibilité nécessaire à un usage professionnel légitime.

Exigence	Sous-exigence	O/N	Notes
Gestion des comptes	Configuration du compte d'entreprise		
	Contrôle d'accès des utilisateurs		
	Gestion du groupe		
	Application de la politique		
Contrôles de sécurité	Gestion de la politique d'authentification		
	Mise en œuvre de l'AMF		
	Contrôle de l'utilisation		
	Examens d'accès		

4.20 Gestion personnalisée du GPT et des plugins

Conseil : La gestion personnalisée des TPG doit permettre une création et un déploiement sécurisés tout en maintenant un contrôle strict sur les intégrations de tiers et l'accès à la place de marché.

Exigence	Sous-exigence	O/N	Notes
Gestion des TPG	Prise en charge de la création de GPT personnalisés		
	Gestion des plugins		
	Contrôle des versions		
	Validation de la sécurité		
Contrôle d'accès	Gestion de l'accès au marché		
	Autorisation du plugin		
	Restrictions d'utilisation		
	Application de la politique		

5. Autres considérations

5.1 Intégration à l'infrastructure existante

- Description des méthodes d'intégration
- Plates-formes et systèmes pris en charge
- Documentation de l'API
- Calendrier d'intégration

5.2 Expérience de l'utilisateur et facilité d'utilisation

- Conception de l'interface
- Exigences en matière de formation
- Contrôles administratifs
- Optimisation du flux de travail de l'utilisateur

5.3 Évolutivité et performances

- Logement de croissance
- Mesures de performance
- Besoins en ressources
- Planification des capacités

5.4 Soutien et maintenance

- Options de soutien
- Temps de réponse
- Fréquence de mise à jour
- Fenêtres de maintenance

5.5 Modèle de tarification

- Structure de la licence
- Coûts de mise en œuvre
- Frais d'entretien courants
- Coûts supplémentaires des services

5.6 Conformité et certifications

- Certifications industrielles
- Cadres de conformité
- Soutien à l'audit
- Exigences réglementaires

5.7 Rapports et analyses

- Rapports standards
- Rapports personnalisés
- Capacités d'analyse
- Personnalisation du tableau de bord

5.8 Confidentialité et protection des données

- Procédures de traitement des données
- Contrôle de la vie privée
- Résidence des données
- Méthodes de cryptage

6. Critères d'évaluation

Les propositions seront évaluées sur la base des éléments suivants

1. Complétude de la solution
2. Capacités d'intégration
3. Compatibilité des systèmes
4. Facilité d'utilisation
5. Exigences en matière de formation
6. Mesures d'évolutivité
7. Critères de performance
8. Offres de soutien
9. Coût total de possession
10. Expérience des fournisseurs
11. Réputation sur le marché

7. Instructions relatives à la soumission

Les vendeurs doivent fournir :

1. Description détaillée de la solution
2. Spécifications techniques
3. Plan de mise en œuvre
4. Approche de la formation
5. Détails de l'aide

6. Structure des prix
7. Profil de l'entreprise
8. Références clients
9. Exemple de documentation
10. Calendrier du projet

8. Calendrier

- Date de publication de l'appel d'offres :
- Date limite pour les questions :
- Date d'échéance de la proposition :
- Présentations des fournisseurs :
- Sélection finale :
- Coup d'envoi du projet :

9. Informations sur les contacts

Pour toute question concernant cet appel d'offres, veuillez contacter

Fin du document d'appel d'offres