Demande de proposition: Solution logicielle de gestion de la posture de sécurité des applications (ASPM)

Table des matières

1. Introduction et contexte
2. Objectifs du projet
3. Champ d'application
4. Exigences techniques
5. Exigences fonctionnelles
6. Exigences opérationnelles
7. Exigences d'intégration
8. Exigences en matière de sécurité et de conformité
9. Exigences en matière de soutien et de service
10. Qualifications des fournisseurs
11. Critères d'évaluation
12. Lignes directrices pour la soumission
13. Calendrier et procédure
14. Conditions commerciales
15. Informations sur le contact

1. Introduction et contexte

1.1 Vue d'ensemble de l'organisation

[Fournissez les informations suivantes sur votre organisation :]

- Brève description de votre entreprise/organisation
- Secteur d'activité et toute exigence réglementaire spécifique

- Taille de l'organisation et de l'infrastructure informatique
- Présence géographique et implantations

1.2 Environnement actuel

- Description de l'infrastructure de sécurité existante
- Nombre et types de points d'aboutissement
- Défis et difficultés actuels
- Points d'intégration et dépendances
- Position actuelle en matière de sécurité

1.3 Contexte du projet

- Les moteurs de cette initiative
- Objectifs stratégiques
- Principales parties prenantes
- Facteurs critiques de succès
- Contraintes et hypothèses du projet

2. Objectifs du projet

2.1 Objectifs principaux

- Gestion améliorée de la posture de sécurité
- Amélioration de la détection et de la réponse aux menaces
- Rationalisation des opérations de sécurité
- Respect de la conformité
- Optimisation des coûts

2.2 Objectifs spécifiques

- [Énumérer des objectifs spécifiques et mesurables]
- [Inclure des objectifs assortis d'un calendrier]
- [Détailler les objectifs liés à la conformité]

- [Préciser les objectifs d'efficacité opérationnelle]

2.3 Critères de réussite

- Mesures de performance
- Mesures de sécurité
- Mesures opérationnelles
- Mesures de la valeur commerciale
- Attentes en matière de retour sur investissement

3. L'étendue des travaux

3.1 Composants de la solution

- Mise en œuvre de la plate-forme de sécurité
- Intégration avec les systèmes existants
- Exigences en matière de migration des données
- Formation et transfert de connaissances
- Exigences en matière de documentation

3.2 Phases de mise en œuvre

1. Découverte et planification
  - Validation des exigences
  - Conception de l'architecture
  - Planification de la mise en œuvre
2. Conception et configuration
  - Configuration du système
  - Développement de la politique
  - Conception de l'intégration
3. Déploiement pilote

- Déploiement limité
  - Essais et validation
  - Tests d'acceptation par l'utilisateur
4. Déploiement complet
- Déploiement de la production
  - Formation des utilisateurs
  - Vérification du système
5. Après la mise en œuvre
- Soutenir la transition
  - Contrôle des performances
  - Optimisation

3.3 Résultats attendus

- Logiciels et licences
- Services de mise en œuvre
- Documentation
- Matériel de formation
- Services d'appui

4. Exigences techniques

4.1 Architecture de la plate-forme

- Exigences en matière d'évolutivité
- Conception à haute disponibilité
- Spécifications de performance
- Exigences en matière d'infrastructure
- Capacités de gestion des données

4.2 Caractéristiques de sécurité

4.2.1 Capacités de sécurité de base

- Protection des points finaux
- Sécurité des applications
- Sécurité des réseaux
- Sécurité de l'informatique en nuage
- Sécurité des données

4.2.2 Fonctions de sécurité avancées

- Intégration des renseignements sur les menaces
- Analyse comportementale
- Protection contre les attaques de type "zero-day"
- Capacités de réponse automatisée
- Outils de criminalistique et d'investigation

4.3 Capacités d'IA et d'apprentissage automatique

- Analyse prédictive de la sécurité
- Détection automatisée des menaces
- Automatisation des réponses intelligentes
- Reconnaissance des formes
- Détection des anomalies

4.4 Gestion et contrôle

- Console de gestion centralisée
- Gestion des politiques
- Gestion de la configuration
- Gestion des actifs
- Capacités de gestion à distance

5. Exigences fonctionnelles

5.1 Découverte et inventaire des applications

La découverte des applications et la gestion de l'inventaire constituent la base de votre posture de sécurité. Un système de découverte robuste garantit qu'aucune application ou actif ne reste sans surveillance, tandis qu'une gestion complète de l'inventaire offre une visibilité claire sur l'ensemble de votre paysage applicatif.

Exigence	Sous-exigence	O/N	Notes
Découverte d'actifs	Découverte automatique des applications		
	Cartographie des infrastructures		
	Découverte des ressources en nuage		
	Analyse du registre des conteneurs		
	Cartographie de la dépendance des services		
Gestion des actifs	Catégorisation des applications		
	Suivi des versions		
	Cartographie de l'environnement		
	Gestion du cycle de vie		
	Gestion de la configuration		

5.2 Évaluation de la sécurité

Les capacités d'évaluation de la sécurité déterminent l'efficacité avec laquelle votre organisation peut identifier et évaluer les vulnérabilités potentielles. Une approche d'évaluation complète combinant plusieurs méthodologies de test garantit une couverture complète.

Exigence	Sous-exigence	O/N	Notes

Analyse de la vulnérabilité	Analyse automatisée de la sécurité		
	Configurations de balayage personnalisées		
	Capacités de programmation		
	Gestion des résultats		
	Gestion de la politique d'analyse		
Tests de sécurité	Intégration de SAST		
	Capacités DAST		
	Soutien de l'IAST		
	Tests de sécurité de l'API		
	Tests de sécurité des applications mobiles		

5.3 Gestion des risques

Une gestion efficace des risques associe une détection robuste des vulnérabilités à des analyses sophistiquées afin de hiérarchiser et de traiter les problèmes de sécurité. Cela permet d'allouer efficacement les ressources et de concentrer les efforts de sécurité sur les menaces critiques.

Exigence	Sous-exigence	O/N	Notes
Gestion de la vulnérabilité	Détection et classification		
	Hiérarchisation des risques		
	Suivi et gestion du cycle de vie		
	Traitement des faux positifs		
	Flux de travail de l'assainissement		

Analyse des risques	Systèmes d'évaluation des risques		
	Analyse des tendances		
	Mesures et indicateurs clés de performance		
	Analyse historique		
	Analyse prédictive		

5.4 Gestion des politiques

La gestion des politiques garantit des pratiques de sécurité cohérentes tout en maintenant la conformité avec les normes pertinentes. Des contrôles stricts de la politique combinés à une vérification automatisée de la conformité créent un cadre solide de gouvernance de la sécurité.

Exigence	Sous-exigence	O/N	Notes
Administration des politiques	Création et gestion de politiques		
	Bibliothèque de modèles		
	Contrôle des versions		
	Gestion des exceptions		
	Application de la politique		
	Gestion de la conformité	Cartographie du cadre	
Contrôle de conformité automatisé			
Collecte de preuves			
Capacités d'établissement de rapports			
Soutien à l'audit			

5.5 Capacités d'IA et d'apprentissage automatique

Les capacités d'IA et de ML permettent une détection avancée des menaces, une réponse automatisée et une aide à la décision intelligente. Ces technologies améliorent les opérations de sécurité grâce à l'analyse prédictive et à l'automatisation.

Exigence	Sous-exigence	O/N	Notes
Prévision des menaces	Détection des menaces basée sur la ML		
	Reconnaissance des formes		
	Analyse comportementale		
	Modèles de prédiction des risques		
	Systèmes de détection d'anomalies		
	Analyse des données historiques		
	Évaluation prédictive de la vulnérabilité		
	Prédiction de la surface d'attaque		
Analyse intelligente	Analyse de la sécurité en fonction du contexte		
	Analyse d'impact automatisée		
	Moteurs de corrélation intelligents		
	Évaluation dynamique des risques		
	Systèmes d'apprentissage adaptatifs		
Remédiation intelligente	Suggestions de corrections automatisées		
	Priorité au contexte		
	Acheminement intelligent du flux de travail		
	Automatisation de l'analyse d'impact		

	Tirer les leçons des modèles de remédiation		
	Propositions de correction du code		
	Recommandations de bonnes pratiques		
	Analyse des modèles de réussite		
Tests automatisés	Génération de tests pilotée par l'IA		
	Optimisation intelligente de la couverture		
	Allocation des ressources		
	Analyse des résultats		
	Apprentissage progressif		
	Stratégies d'essai adaptatives		
	Hierarchisation des cas de test		
	Validation automatisée		

5.6 Traitement du langage naturel et opérations autonomes

Le NLP et les opérations autonomes permettent une interaction intelligente des systèmes et des contrôles de sécurité auto-optimisés. Ces capacités permettent de rationaliser les opérations et d'améliorer l'efficacité du système au fil du temps.

Exigence	Sous-exigence	O/N	Notes
Analyse de la documentation	Analyse des besoins en matière de sécurité		
	Interprétation de la politique		
	Traitement des documents de conformité		
	Génération de documentation intelligente		

	Recherche contextuelle		
	Analyse sémantique		
	Extraction de connaissances		
	Catégorisation automatisée		
Interaction intelligente	Requêtes en langage naturel		
	Des réponses adaptées au contexte		
	Filtrage intelligent		
	Recherche sémantique		
	Optimisation des requêtes		
	Reconnaissance des intentions		
	Mises à jour automatisées de la base de connaissances		
	Génération de réponses		
Systemes d'auto-apprentissage	Adaptation dynamique des règles		
	Raffinement automatisé de la politique		
	Contrôles auto-optimisants		
	Amélioration continue		
	Reconnaissance des formes		
	Analyse comportementale		
	Détection des anomalies		
	Réponses adaptatives		

Intelligence du flux de travail	Routage intelligent des tâches		
	Optimisation des priorités		
	Allocation des ressources		
	Automatisation des processus		
	Apprendre à partir de modèles		
	Optimisation de l'efficacité		
	Orchestration automatisée		
	Aide à la décision		

5.7 Rapports et analyses

Des capacités complètes de reporting et d'analyse fournissent des informations exploitables et permettent une prise de décision fondée sur les données. Ces outils soutiennent à la fois la gestion opérationnelle et la planification stratégique.

Exigence	Sous-exigence	O/N	Notes
Génération de rapports	Modèles personnalisables		
	Rapports programmés		
	Tableaux de bord interactifs		
	Capacités d'exportation		
	Visualisation des données		
	Caractéristiques analytiques	Analyse des tendances	
Mesures de performance			
Analyse personnalisée			

	Analyse comparative		
	Analyse prédictive		

6. Exigences opérationnelles

6.1 Exigences de performance

- Spécifications du temps de réponse
- Exigences en matière de débit
- Mesures d'évolutivité
- Utilisation des ressources
- Planification des capacités

6.2 Disponibilité et fiabilité

- Exigences en matière de disponibilité
- Capacités de basculement
- Sauvegarde et récupération
- Reprise après sinistre
- Continuité des activités

6.3 Options de déploiement

- Déploiement dans le nuage
- Installation sur site
- Configurations hybrides
- Prise en charge multi-cloud
- Déploiement de conteneurs

7. Exigences en matière d'intégration

7.1 Intégrations requises

- Systèmes SIEM

- Outils ITSM
- Services d'annuaire
- Plateformes en nuage
- Outils de développement

7.2 API et interopérabilité

- Spécifications de l'API
- Protocoles d'intégration
- Formats d'échange de données
- Méthodes d'authentification
- Capacités d'intégration personnalisées

8. Exigences en matière de sécurité et de conformité

8.1 Normes de sécurité

- Certifications industrielles
- Protocoles de sécurité
- Cadres de conformité
- Exigences en matière de protection des données
- Normes de protection de la vie privée

8.2 Exigences de conformité

- Conformité réglementaire
- Normes industrielles
- Politiques internes
- Exigences en matière d'audit
- Exigences en matière de rapports

9. Exigences en matière de soutien et de service

9.1 Services d'appui

- Niveaux d'assistance et accords de niveau de service
- Gestion des incidents
- Gestion des problèmes
- Procédures d'escalade
- Accès à la base de connaissances

9.2 Services professionnels

- Services de mise en œuvre
- Programmes de formation
- Services de conseil
- Services de personnalisation
- Services gérés

10. Qualifications des fournisseurs

10.1 Profil de l'entreprise

- Historique de l'entreprise
- Stabilité financière
- Présence sur le marché
- Base de clientèle
- Reconnaissance du secteur

10.2 Expérience et expertise

- Mises en œuvre similaires
- Expertise sectorielle
- Capacités techniques
- Infrastructure de soutien
- Expérience en matière d'innovation

11. Critères d'évaluation

11.1 Évaluation technique (40%)

- Complétude des caractéristiques
- Architecture technique
- Capacités de performance
- Capacités d'intégration
- Caractéristiques de sécurité

11.2 Évaluation fonctionnelle (25 %)

- Expérience de l'utilisateur
- Capacités d'administration
- Rapports et analyses
- Fonctions d'automatisation
- Options de personnalisation

11.3 Évaluation des fournisseurs (20 %)

- Stabilité de l'entreprise
- Position sur le marché
- Contrôle des références
- Capacité de soutien
- Potentiel d'innovation

11.4 Évaluation commerciale (15 %)

- Coût total de possession
- Modèle de tarification
- Conditions de paiement
- Conditions du contrat
- Rapport qualité-prix

12. Lignes directrices en matière de soumission

12.1 Format de la proposition

1. Résumé
2. Profil de l'entreprise
3. Réponse technique
4. Approche de la mise en œuvre
5. Détails des prix
6. Références
7. Documentation à l'appui

12.2 Exigences de réponse

- Réponse point par point aux exigences
- Preuves et documentation à l'appui
- Références clients
- Exemples de produits à fournir
- Profils des équipes de projet

13. Calendrier et processus

13.1 Dates clés

- Publication de l'appel d'offres : [Date]
- Date limite pour les questions : [Date]
- Réponse aux questions : [Date]
- Date d'échéance de la proposition : [Date]
- Présentations des fournisseurs : [Fourchette de dates]
- Décision de sélection : [Date]
- Début du projet : [Date]

13.2 Processus de sélection

1. Évaluation de la proposition
2. Sélection de la liste restreinte
3. Présentations des fournisseurs
4. Contrôles de référence
5. Sélection finale

14. Conditions commerciales

14.1 Structure des prix

- Frais de licence
- Coûts de mise en œuvre
- Coûts de soutien
- Coûts de formation
- Services complémentaires

14.2 Conditions de paiement

- Calendrier de paiement
- Paiements d'étape
- Coûts récurrents
- Frais supplémentaires
- Conditions d'utilisation

15. Informations sur les contacts

15.1 Contact principal

[Nom] [Titre] [Courriel] [Téléphone]

15.2 Instructions de soumission

[Détaillez les exigences et les canaux de soumission spécifiques]