Demande de proposition : Solution de sécurité API

Table des matières

1. Introduction et vue d'ensemble
2. Exigences techniques
3. Exigences fonctionnelles
4. Infrastructure de l'IA et de l'apprentissage automatique
5. Exigences opérationnelles
6. Conformité et gouvernance
7. Évaluation des fournisseurs
8. Considérations relatives à la mise en œuvre
9. Analyse du retour sur investissement
10. La protection de l'avenir
11. Lignes directrices et critères d'évaluation de l'appel d'offres
12. Exigences en matière de soumission
13. Calendrier et procédure

1. Introduction et vue d'ensemble

1.1 Objectif

[Nom de l'organisation] lance un appel d'offres pour une solution complète de sécurité des API afin de protéger notre infrastructure API, d'assurer la conformité et de maintenir l'intégrité de nos services numériques. Comme les organisations s'appuient de plus en plus sur les API pour la transformation numérique, cette solution servira de composant d'infrastructure critique pour assurer l'intégrité, la confidentialité et la disponibilité de nos services.

1.2 Champ d'application

Le champ d'application du présent appel d'offres est le suivant :

- Protection de l'infrastructure API
- Surveillance de la sécurité et détection des menaces
- Mise en œuvre de la conformité et de la gouvernance
- Optimisation des performances
- Gestion des risques
- Fonctions de sécurité pilotées par l'IA

2. Exigences techniques

2.1 Exigences en matière d'infrastructure

Spécifications du matériel

- Configuration du serveur :
  - CPU : Processeurs multicœurs
  - RAM : 16 Go minimum recommandés
  - Stockage : SSD avec IOPS élevé
  - Réseau : Connectivité Gigabit
- Exigences en matière de stockage :
  - Capacité de stockage des grumes
  - Stockage de sauvegarde
  - Stockage de données analytiques
- Exigences du réseau :
  - Spécifications de la bande passante
  - Exigences en matière de latence
  - Configurations de l'équilibreur de charge
- Infrastructure de sauvegarde :
  - Systèmes redondants

- Capacités de basculement
- Reprise après sinistre

Dépendances logicielles

- Compatibilité avec les systèmes d'exploitation :
  - Distributions Linux
  - Versions du serveur Windows
  - Plateformes de conteneurs
- Exigences en matière de base de données :
  - Bases de données SQL
  - Bases de données NoSQL
  - Bases de données chronologiques
- Environnements d'exécution :
  - Exécution Java
  - Cadre .NET
  - Environnement Python
- Logiciels tiers :
  - Serveurs web
  - Serveurs de cache
  - Files d'attente de messages

2.2 Intégration de la passerelle API

- Prise en charge du protocole :
  - Gestion de l'API REST
  - Traitement SOAP
  - Intégration GraphQL

  - Prise en charge de WebSocket
  - Capacités gRPC
  - Protocoles personnalisés
- Caractéristiques de la passerelle :
  - Gestion du trafic
    - Limitation du taux
    - Gestion des quotas
    - Mise en forme du trafic
  - Équilibrage de la charge
    - Options de l'algorithme
    - Contrôle sanitaire
    - Gestion du basculement
  - Contrôle des versions
    - Version de l'API
    - Rétrocompatibilité
    - Acheminement des versions

3. Exigences fonctionnelles

3.1 Gestion du cycle de vie des API

Conseil : La gestion du cycle de vie des API constitue la base de votre stratégie de sécurité des API. Un système robuste de gestion du cycle de vie garantit des contrôles de sécurité cohérents du développement au retrait, tout en maintenant la visibilité et le contrôle sur toutes les versions et dépendances de l'API.

Exigence	Sous-exigence	O/N	Notes

Conception et développement de l'API	Validation des spécifications		
	Application des lignes directrices en matière de design		
	Intégration du contrôle de version		
	Génération de documents		
	Cadres de test		
	Outils de développement		
Catalogage API	Inventaire central		
	Gestion des métadonnées		
	Suivi des versions		
	Cartographie des dépendances		
	Analyse de l'utilisation		
	Mesures de performance		

3.2 Opérations de sécurité

Conseil : les capacités d'opérations de sécurité doivent fournir une protection en temps réel tout en maintenant l'efficacité opérationnelle. Recherchez des solutions qui équilibrent les réponses automatisées et les capacités de supervision humaine.

Exigence	Sous-exigence	O/N	Notes
Prévention des menaces	Détection des attaques		
	Blocage automatisé		
	Filtrage IP		
	Géo-blocage		

	Limitation du taux		
	Protection DDoS		
Surveillance de la sécurité	Tableaux de bord en temps réel		
	Enregistrement des événements		
	Détection des anomalies		
	Analyse du comportement		
	Reconnaissance des formes		
	Suivi des mesures		

3.3 Fonctions de sécurité alimentées par l'IA

Conseil : Les fonctions de sécurité alimentées par l'IA doivent améliorer, et non remplacer, les contrôles de sécurité traditionnels. Concentrez-vous sur les solutions qui démontrent des améliorations concrètes de la sécurité grâce à l'IA/ML, en accordant une attention particulière aux taux de faux positifs.

Exigence	Sous-exigence	O/N	Notes
Détection intelligente des menaces	Prévision d'une attaque de type "zero-day		
	Détection d'anomalies basée sur la ML		
	Analyse du comportement		
	Suivi de l'évolution des schémas d'attaque		
	Simulation de scénarios de risque		
	Analyse de la chaîne d'exploitation		
Réponse automatisée en matière de sécurité	Classification des attaques en temps réel		

	Mécanismes de défense dynamiques		
	Triage automatisé des incidents		
	Règles de blocage intelligentes		
	Capacités d'autoréparation		
	Confinement autonome des menaces		
Analyse intelligente de l'API	Traitement en langage naturel de la documentation de l'API		
	Analyse et validation automatiques des schémas		
	Inspection sémantique de la charge utile		
	Analyse de la chaîne d'appels API		
	Inférence de la logique d'entreprise		
	Détection des similitudes entre les API		

3.4 Gestion améliorée par l'IA

Conseil : Les fonctions de gestion améliorées par l'IA doivent démontrer des améliorations mesurables de l'efficacité opérationnelle. Privilégiez les solutions qui proposent des décisions d'IA explicables et qui maintiennent une supervision humaine.

Exigence	Sous-exigence	O/N	Notes
Opérations automatisées	Allocation dynamique des ressources		
	Auto-réglage des performances		
	Stratégies de mise en cache intelligentes		
	Prévision de la charge		

	Version automatique de l'API		
	Optimisation de l'exécution		
Aide au développement	Analyse de la qualité du code		
	Analyse des failles de sécurité		
	Examens automatisés du code		
	Application des bonnes pratiques		
	Suggestions d'optimisation du code		
	Détection de la dette technique		

3.5 Fonctions de conformité et de gouvernance de l'IA

Conseil : évaluez les fonctions de conformité et de gouvernance en fonction de leur capacité à maintenir la responsabilité tout en automatisant les tâches de routine. Assurez des pistes d'audit claires pour les décisions basées sur l'IA.

Exigence	Sous-exigence	O/N	Notes
Conformité automatisée	Contrôle de conformité en temps réel		
	Détection des violations de la politique		
	Cartographie des exigences réglementaires		
	Génération automatisée de rapports		
	Analyse de la piste d'audit		
	Évaluation de l'impact sur la vie privée		
Éthique et équité	Détection des biais dans les décisions de sécurité		
	Contrôle de l'équité		
	Explicabilité de la décision		

	Responsabilité algorithmique		
	Modèle de gouvernance		
	Validation de l'utilisation éthique		

3.6 Fonctions de sécurité avancées

Conseil : Les fonctions de sécurité avancées doivent fournir une protection sophistiquée tout en restant gérables et efficaces. Recherchez des solutions qui offrent des capacités de pointe sans introduire de complexité inutile.

Exigence	Sous-exigence	O/N	Notes
Authentification intelligente	Intégration de systèmes biométriques		
	Contrôle continu de l'authentification		
	Évaluation fondée sur les risques		
	Détection avancée de la fraude		
	Analyse du comportement en séance		
	Protection des données d'identification		
Interface de sécurité intelligente	Requêtes de sécurité en langage naturel		
	Enquête interactive sur les menaces		
	Commandes de sécurité à commande vocale		
	Recommandations contextuelles en matière de sécurité		
	Rapports de sécurité automatisés		
	Interactions avec la base de connaissances		

3.7 Validation de la sécurité

Conseil : les processus de validation de la sécurité doivent fournir une assurance continue de l'efficacité des contrôles. Privilégiez les solutions offrant des capacités de tests automatisés tout en conservant une certaine flexibilité.

Exigence	Sous-exigence	O/N	Notes
Capacités d'évaluation	Évaluations automatisées de la posture de sécurité		
	Scénarios d'attaque simulés		
	Surveillance continue des contrôles		
	Intégration avec les scanners de vulnérabilité		
Gestion de la validation	Validation de la configuration de sécurité		
	Tests de détection et de réaction		
	Mise à jour régulière des critères de validation		
	Rapport sur les résultats		
Caractéristiques d'intégration	Intégration de la gestion du changement		
	Intégration d'essais par des tiers		

3.8 Rapports d'incidents

Conseil : les fonctionnalités de rapport d'incident doivent offrir une visibilité complète tout en permettant une action rapide. Recherchez des solutions offrant des rapports personnalisables avec des fonctions de génération automatique.

Exigence	Sous-exigence	O/N	Notes
Génération de rapports	Modèles de rapports personnalisables		

	Tableaux de bord de la sécurité en temps réel		
	Analyse des tendances		
	Rapport d'évaluation de la vulnérabilité		
Rapport de conformité	Rapports spécifiques à la conformité		
	Rapports sur l'inventaire des actifs		
	Rapports d'activité des utilisateurs		
	Documentation sur les violations de la politique		
Caractéristiques de la gestion	Génération automatisée de rapports		
	Options d'exportation multiformat		

3.9 Gestion des actifs

Conseil : Les fonctionnalités de gestion des actifs doivent offrir une visibilité et un contrôle complets sur votre infrastructure API. Privilégiez les solutions offrant une découverte automatisée et une gestion complète du cycle de vie.

Exigence	Sous-exigence	O/N	Notes
Découverte et inventaire	Découverte et inventaire automatisés		
	Collecte d'informations détaillées sur les actifs		
	Surveillance de l'état en temps réel		
	Suivi des licences de logiciels		
Caractéristiques de la gestion	Intégration de la gestion de l'identité		
	Capacités de regroupement des actifs		

	Système d'alerte automatisé		
	Gestion du cycle de vie des actifs		
Capacités d'intégration	Rapports d'inventaire		
	Intégration ITSM		
	Suivi mobile/à distance des actifs		

3.10 Isolation du système

Conseil : les capacités d'isolation des systèmes doivent permettre de réagir rapidement aux menaces tout en maintenant la continuité de l'activité. Privilégiez les solutions qui offrent un contrôle granulaire et des déclencheurs d'isolation automatisés avec des voies de restauration claires.

Exigence	Sous-exigence	O/N	Notes
Contrôles d'isolement	Isolation rapide des points d'accès compromis		
	Désactivation d'une application ou d'un service à distance		
	Isolement automatique en fonction des violations de la politique		
	Contrôle granulaire de l'accès au réseau		
Caractéristiques de la gestion	Des canaux de communication sécurisés		
	Procédures de restauration		
	Enregistrement des événements d'isolation		
	Flux de travail pour la réponse aux incidents		
Gestion des utilisateurs	Système de notification aux utilisateurs		

	Options de restauration en libre-service		

4. Infrastructure de l'IA et de l'apprentissage automatique

4.1 Infrastructure du modèle

- Ressources informatiques :
  - Exigences en matière de GPU/TPU
  - Spécifications de la mémoire
  - Exigences en matière de stockage
  - Largeur de bande du réseau
  - Capacité de traitement
  - Capacités de mise à l'échelle
- Déploiement du modèle :
  - Modèle d'infrastructure de desserte
  - Gestion des versions
  - Capacité de test A/B
  - Mécanismes de retour en arrière
  - Contrôle des performances
  - Optimisation des ressources

4.2 Gestion des données

- Données de formation :
  - Systèmes de stockage de données
  - Prétraitement des données
  - Ingénierie des fonctionnalités
  - Validation des données
  - Assurance qualité

  - Contrôle des versions
- Données opérationnelles :
  - Traitement en temps réel
  - Pipelines de données
  - Traitement des flux
  - Conservation des données
  - Systèmes d'archivage
  - Procédures de récupération

4.3 Opérations d'IA

- Gestion des modèles :
  - Contrôle des versions
  - Contrôle des performances
  - Déclencheurs de réentraînement
  - Détection de la dérive
  - Gestion des données
  - Outils de validation
- Gouvernance de l'IA :
  - Audit des décisions
  - Détection de biais
  - Explicabilité
  - Respect de l'éthique
  - Transparence
  - Mesures de performance

5. Exigences opérationnelles

5.1 Options de déploiement

- Sur place
- Basé sur l'informatique en nuage
- Hybride
- Multirégion
- Haute disponibilité

5.2 Exigences de performance

- Disponibilité :
  - Systèmes de basculement
  - Redondance
  - Reprise après sinistre
  - Systèmes de sauvegarde
  - Répartition géographique
  - Équilibrage de la charge
- Mesures :
  - Temps de réponse
  - Débit
  - Limites de latence
  - Taux d'erreur
  - Utilisation des ressources
  - Respect des accords de niveau de service

6. Conformité et gouvernance

6.1 Normes

- PCI DSS

- GDPR
- HIPAA
- SOC 2
- ISO 27001
- Exigences spécifiques à l'industrie

6.2 Rapports

- Incidents de sécurité
- État de conformité
- Pistes d'audit
- Évaluation des risques
- Analyse des tendances
- Résumés exécutifs

7. Évaluation des fournisseurs

7.1 Qualifications

- Histoire de l'entreprise
- Position sur le marché
- Références
- Reconnaissance
- Situation financière
- Une présence mondiale

7.2 Soutien

- Couverture 24/7
- Assistance à la mise en œuvre
- Programmes de formation

- Documentation
- Services professionnels
- Conditions de l'ANS

8. Considérations relatives à la mise en œuvre

8.1 Calendrier

- Phases du projet
- Les étapes de la migration
- Périodes d'essai
- Calendrier des formations
- Planification de la mise en service
- Soutien après le lancement

8.2 Ressources

- Besoins en personnel
- Soutien aux fournisseurs
- Besoins en infrastructures
- Exigences en matière de formation
- Plans de maintenance
- Opérations en cours

9. Analyse du retour sur investissement

9.1 Avantages

- Amélioration de la sécurité
- Économies de mise en conformité
- Efficacité opérationnelle
- Vitesse de développement

- Réduction des risques
- Gains de performance

9.2 Coûts

- Investissement initial
- Dépenses opérationnelles
- Coûts de formation
- Frais de maintenance
- Coûts de mise à niveau
- Dépenses de soutien

10. La protection de l'avenir

10.1 Feuille de route technologique

- Progrès de l'IA
- Confiance zéro
- Native de l'informatique en nuage
- Sécurité des conteneurs
- Sécurité sans serveur
- Menaces émergentes

10.2 Extensibilité

- Personnalisation de l'API
- Systèmes de plugins
- Règles personnalisées
- Options d'intégration
- Capacités d'automatisation
- Voies d'extensibilité

11. Lignes directrices et critères d'évaluation de l'appel d'offres

11.1 Critères d'évaluation

Les propositions seront évaluées sur la base des éléments suivants

1. Complétude de la solution technique (25%)
2. Capacités et innovation en matière d'IA/ML (20 %)
3. Approche de la mise en œuvre et du soutien (15 %)
4. Expertise et stabilité du fournisseur (15 %)
5. Coût total de possession (15%)
6. Références clients et antécédents (10 %)

11.2 Questions clés

- Évaluation technique
- Vérification de l'intégration
- Validation des performances
- Preuve de conformité
- Détails de l'aide
- Clarté des prix

12. Exigences en matière de soumission

Les vendeurs doivent soumettre :

1. Proposition technique détaillée répondant à toutes les exigences
2. Méthodologie et calendrier de mise en œuvre
3. Structure tarifaire complète
    - Frais de licence
    - Coûts de mise en œuvre
    - Coûts de formation

- Coûts de soutien

4. Accords de niveau de service
5. Plans d'assistance et de maintenance
6. Qualifications et structure de l'équipe
7. Au moins trois références de clients
8. Feuille de route du produit
9. Exemples de rapports et de documentation
10. Certifications de conformité
11. États financiers
12. Certificats d'assurance

13. Calendrier et processus

- Date de publication de l'appel d'offres : [Date]
- Date limite pour les questions des fournisseurs : [Date]
- Réponses aux questions : [Date]
- Date d'échéance de la proposition : [Date]
- Présentations des fournisseurs : [Fourchette de dates]
- Décision de sélection : [Date]
- Négociation du contrat : [Période]
- Lancement du projet : [Date]

Informations sur le contact

Adresser toutes les propositions et demandes de renseignements à [Nom du contact] [Titre] [Adresse électronique] [Numéro de téléphone] [Nom de l'organisation] [Adresse]

Les vendeurs doivent accuser réception du présent appel d'offres et indiquer leur intention de soumettre une proposition au plus tard le [Date] par courrier électronique au contact ci-dessus.