Demande de proposition : Solution de surveillance et d'analyse de la sécurité dans l'informatique en nuage

Table des matières

1. Introduction et contexte

L'organisation a besoin d'une solution complète de surveillance et d'analyse de la sécurité dans le nuage pour améliorer l'infrastructure de cybersécurité. Le présent appel d'offres décrit les exigences relatives à un système robuste assurant une surveillance continue, la détection des menaces et l'analyse complète des événements de sécurité dans les environnements en nuage.

1.1 Vue d'ensemble de l'organisation

- Infrastructure multi-cloud utilisant les services AWS, Azure et GCP
- Architecture hybride en nuage avec des centres de données sur site
- Opérations mondiales dans plusieurs régions géographiques
- Exigences en matière de déploiement à l'échelle de l'entreprise

- Besoins critiques en matière de protection des données

1.2 Situation actuelle en matière de sécurité

- Outils SIEM et de gestion des journaux existants
- Systèmes de surveillance de la sécurité des réseaux
- Plateformes de protection des points finaux
- Outils de sécurité natifs de l'informatique en nuage
- Défis actuels en matière d'intégration

1.3 Objectifs du projet

- Améliorer la visibilité de l'infrastructure en nuage et des événements liés à la sécurité
- Améliorer les capacités de détection et de réponse aux menaces dans tous les environnements
- Assurer la conformité avec les réglementations et les normes du secteur
- Optimiser les opérations de sécurité grâce à des analyses avancées
- Mettre en œuvre l'automatisation de la sécurité pilotée par l'IA
- Mettre en place une surveillance complète de la sécurité

2. Objectifs du projet

2.1 Objectifs de sécurité fondamentaux

- Mettre en place une surveillance complète de la sécurité du cloud dans tous les environnements
- Mettre en place des capacités de détection et de réaction aux menaces en temps réel
- Améliorer les fonctions de contrôle de la conformité et d'établissement de rapports
- Améliorer les enquêtes sur les incidents de sécurité et la criminalistique
- Déployer des analyses de sécurité avancées

- Permettre une réponse automatisée aux menaces

2.2 Objectifs de l'analyse et du renseignement

- Déployer des analyses avancées pour la corrélation des événements de sécurité
- Mettre en œuvre la détection et l'analyse des menaces alimentées par l'IA
- Mettre en place des capacités de sécurité prédictive
- Permettre une réponse automatisée aux incidents de sécurité
- Développer l'intégration des renseignements sur les menaces
- Créer des informations exploitables sur la sécurité

2.3 Objectifs opérationnels

- Rationaliser les opérations de sécurité grâce à l'automatisation
- Réduire la fatigue liée aux alertes grâce à une hiérarchisation intelligente des alertes
- Améliorer l'efficacité des enquêtes de sécurité
- Mettre en place des capacités de chasse aux menaces proactives
- Améliorer les flux de réponse aux incidents
- Optimiser l'utilisation des ressources

3. Champ d'application des travaux

3.1 Services de mise en œuvre

- Évaluation complète de l'environnement et analyse des lacunes
- Conception et documentation de l'architecture de la solution
- Intégration avec les outils et plateformes de sécurité existants
- Procédures d'essai et de validation des systèmes
- Déploiement et optimisation de la production
- Transfert de connaissances et formation

3.2 Mise en œuvre de la fonctionnalité de base

- Systèmes de collecte et d'agrégation de données
- Cadres de surveillance de la sécurité
- Systèmes de gestion des alertes
- Flux de travail pour la réponse aux incidents
- Outils de contrôle de conformité
- Plateformes de reporting et d'analyse

3.3 Mise en œuvre de l'analyse avancée

- Déploiement de modèles d'IA et d'apprentissage automatique
- Capacités d'analyse prédictive
- Systèmes de réponse automatisés
- Intégration des renseignements sur les menaces
- Mise en œuvre de l'analyse comportementale
- Développement d'analyses personnalisées

4. Exigences techniques

4.1 Collecte et intégration des données

- Capacités d'ingestion de données multi-cloud pour AWS, Azure et GCP
- Agrégation et normalisation des journaux en temps réel
- Cadre d'intégration API complet
- Capacités de traitement des données en temps réel
- Prise en charge des sources de données personnalisées
- Solutions de stockage de données évolutives

4.2 Contrôle de la sécurité

- Surveillance continue de la posture de sécurité
- Analyse du trafic réseau en temps réel

- Analyse avancée du comportement des utilisateurs et des entités
- Contrôle de la configuration et de la conformité de l'informatique en nuage
- Recherche d'actifs et suivi des stocks
- Surveillance et évaluation de la vulnérabilité

4.3 Détection des menaces

- Détection basée sur une signature multicouche
- Analyse comportementale avancée
- Détection des menaces basée sur l'apprentissage automatique
- Identification des menaces de type "zero-day
- Surveillance des menaces d'initiés
- Création de règles de détection personnalisées

5. Exigences fonctionnelles

5.1 Fonctionnalités de base

5.1.1 Collecte et agrégation des données

La collecte et l'agrégation efficaces des données constituent la base de la surveillance de la sécurité de l'informatique en nuage. L'accent doit être mis sur une couverture complète de tous les actifs du cloud et sur la capacité à normaliser les données provenant de diverses sources en vue d'une analyse unifiée.

Exigence	Sous-exigence	O/N	Notes
Sources de collecte de données	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		

	Prise en charge de l'intégration de sources de données personnalisées		
Visibilité	Fournir une visibilité complète de l'environnement en nuage		
	Mettre en place des capacités de surveillance en temps réel		
	Soutenir l'analyse des données historiques		
Traitement des données	Normalisation des données en temps réel		
	Permettre le filtrage et la classification des données		
	Fournir des capacités d'enrichissement des données		

5.1.2 Détection des menaces

Une détection efficace des menaces nécessite une approche multicouche combinant la détection basée sur les signatures, l'analyse comportementale et l'apprentissage automatique.

Exigence	Sous-exigence	O/N	Notes
Méthodes de détection	Mise en œuvre d'une détection basée sur les signatures		
	Utiliser des algorithmes d'apprentissage automatique		
	Permettre l'analyse comportementale		
	Prise en charge de règles de détection personnalisées		
Couverture des menaces	Identifier les menaces connues		
	Détecter les menaces de type "zero-day		

	Surveiller les menaces internes		
	Traquer les menaces persistantes avancées		
Mise en œuvre	Soutenir une approche de détection à multiples facettes		
	Mettre en place des capacités de chasse aux menaces		
	Assurer l'intégration des renseignements sur les menaces		

5.1.3 Réponse aux incidents

La rapidité et l'efficacité de la réponse aux incidents ont un impact direct sur votre niveau de sécurité. Concentrez-vous sur les capacités d'automatisation tout en maintenant une surveillance humaine pour les décisions critiques.

Exigence	Sous-exigence	O/N	Notes
Actions de réponse	Activer l'isolation du système		
	Soutien au blocage du trafic		
	Permettre l'ouverture d'une enquête		
	Fournir des options de réponse automatisées		
	Permettre la remédiation du système à distance		
Cahiers de lecture	Prise en charge des carnets de commande de réponses personnalisées		
	Permettre l'automatisation des flux de travail		
	Fournir des capacités de test des playbooks		
Documentation	Suivre le cycle de vie des incidents		
	Maintenir les pistes d'audit des réponses		

	Générer des rapports d'incidents		

5.1.4 Priorité aux alertes

La hiérarchisation intelligente des alertes est essentielle pour gérer efficacement les opérations de sécurité et réduire la fatigue liée aux alertes.

Exigence	Sous-exigence	O/N	Notes
Système de priorisation	Mise en œuvre d'une priorisation basée sur la criticité		
	Tenir compte de la valeur des actifs dans l'établissement des priorités		
	Inclure le contexte de la menace dans l'évaluation		
	Prise en charge des règles de priorisation personnalisées		
Gestion des alertes	Filtrage intelligent des alertes		
	Permettre l'acheminement et l'escalade des alertes		
	Corrélation des alertes		
	Autoriser les catégories d'alertes personnalisées		

5.1.5 Gestion de la conformité

Des capacités complètes de gestion de la conformité sont essentielles pour maintenir le respect des réglementations et des normes de sécurité dans les environnements en nuage.

Exigence	Sous-exigence	O/N	Notes
Gestion des politiques	Appliquer les politiques de conformité		
	Prise en charge de plusieurs cadres de conformité		

	Permettre la création de politiques personnalisées		
	Fournir des capacités de test des politiques		
Contrôle	Mettre en place un contrôle continu de la conformité		
	Suivi des violations de la politique		
	Générer des alertes de conformité		
	Soutenir les évaluations automatisées		
Rapports	Créer des rapports de conformité automatisés		
	Maintenir des pistes d'audit détaillées		
	Prise en charge de la génération de rapports personnalisés		
	Activer les rapports planifiés		

5.1.6 Évolutivité

Les solutions de sécurité en nuage doivent s'adapter efficacement à la croissance de l'entreprise tout en maintenant les performances et la fiabilité dans toutes les régions et tous les environnements.

Exigence	Sous-exigence	O/N	Notes
Mise à l'échelle de l'infrastructure	Prise en charge de la mise à l'échelle horizontale		
	Activer la mise à l'échelle verticale		
	Traiter des volumes de données accrus		
	Soutien au déploiement multirégional		
Performance	Maintien de la vitesse de traitement sous charge		

	Soutenir le traitement distribué		
	Activer l'équilibrage de la charge		
Soutien à la croissance	S'adapter à la croissance de l'organisation		
	Modèle de licence d'échelle		
	Soutenir l'intégration des nouvelles technologies		

5.1.7 Capacités d'intégration

L'intégration transparente avec l'infrastructure et les outils de sécurité existants est essentielle pour maintenir l'efficacité opérationnelle et une couverture de sécurité complète.

Exigence	Sous-exigence	O/N	Notes
Intégration des outils de sécurité	Connexion avec les systèmes SIEM		
	Intégration avec les plateformes EDR		
	Soutenir l'intégration SOAR		
	Permettre l'intégration de la gestion des identités		
Intégration du développement	Soutenir l'intégration du pipeline CI/CD		
	Permettre les flux de travail DevSecOps		
	Fournir des interfaces d'automatisation		
Support API	Proposer des API REST complètes		
	Prise en charge des implémentations de webhook		

	Permettre le développement d'une intégration personnalisée		

5.1.8 Gestion de la confidentialité des données

Une gestion robuste de la confidentialité des données est essentielle pour protéger les informations sensibles et maintenir la conformité réglementaire dans les environnements en nuage.

Exigence	Sous-exigence	O/N	Notes
Protection des données	Mettre en œuvre le cryptage des données au repos		
	Activer le cryptage en transit		
	Prise en charge du masquage des données		
	Permettre l'anonymisation des données		
Classification	Soutenir la classification automatisée des données		
	Activer les règles de classification personnalisées		
	Fournir des rapports de classification		
Contrôle d'accès	Mettre en place un contrôle d'accès basé sur les rôles		
	Activer le contrôle d'accès basé sur les attributs		
	Soutenir le principe du moindre privilège		
	Suivre les activités d'accès aux données		

5.2 Capacités alimentées par l'IA

5.2.1 Assistants d'IA générative

Les assistants IA devraient améliorer les opérations de sécurité grâce à l'interaction avec le langage naturel et à l'automatisation intelligente, tout en maintenant la précision et la pertinence.

Exigence	Sous-exigence	O/N	Notes
Traitement des langues	Traiter les requêtes en langage naturel		
	Soutenir des réponses adaptées au contexte		
	Activer la prise en charge multilingue		
Tâches de sécurité	Automatiser les opérations de routine		
	Générer des informations sur la sécurité		
	Fournir des conseils en matière de remédiation		
Intégration	Soutenir l'intégration du flux de travail		
	Activer l'automatisation personnalisée		
	Maintenir des pistes d'audit		

5.2.2 Intégration des renseignements sur les menaces

L'intégration des renseignements sur les menaces doit permettre d'obtenir des informations exploitables tout en mettant automatiquement en corrélation des données provenant de sources multiples afin d'améliorer la détection des menaces et les capacités de réaction.

Exigence	Sous-exigence	O/N	Notes
Analyse du renseignement	Traiter des flux de menaces multiples		
	Corréler les indicateurs de menace		
	Générer des profils d'acteurs		

	Fournir une évaluation d'impact		
Automatisation	Permettre l'ingestion automatisée des aliments		
	Soutenir la création d'informations personnalisées		
	Mise à jour automatique des règles de détection		
Intégration	Se connecter à des plateformes externes		
	Prise en charge des formats STIX/TAXII		
	Mettre en place des capacités de partage des menaces		

5.2.3 Analyse du code

L'analyse de code alimentée par l'IA devrait fournir des capacités d'évaluation de la sécurité complètes tout en minimisant les faux positifs et en offrant des conseils de remédiation clairs.

Exigence	Sous-exigence	O/N	Notes
Caractéristiques de l'analyse	Effectuer une analyse statique du code		
	Permettre l'analyse dynamique du code		
	Prise en charge de plusieurs langues		
	Identifier les failles de sécurité		
Automatisation	Automatiser la programmation des analyses		
	Permettre l'intégration CI/CD		
	Générer des étapes de remédiation		
Rapports	Fournir des conclusions détaillées		

	Suivre les tendances en matière de vulnérabilité		
	Prise en charge des rapports personnalisés		

5.2.4 Détection et réponse intelligentes dans le nuage (CDR)

Les capacités CDR devraient tirer parti de l'IA pour la détection précoce des menaces, tout en permettant des actions de réponse automatisées et en fournissant une visualisation claire de la chaîne d'attaque.

Exigence	Sous-exigence	O/N	Notes
Capacités de détection	Détection précoce des attaques		
	Contrôler les services en nuage		
	Identifier les schémas d'attaque		
	Suivi des mouvements latéraux		
Éléments de réponse	Automatiser la réponse initiale		
	Prise en charge des playbooks personnalisés		
	Permettre l'endiguement de l'incident		
Analyse	Corrélation des événements de sécurité		
	Visualisation des attaques		
	Produire une analyse d'impact		

5.2.5 Sécurité adaptative

Les cadres de sécurité adaptatifs doivent évoluer en permanence pour faire face aux nouvelles menaces tout en ajustant automatiquement les contrôles de sécurité sur la base d'une évaluation des risques en temps réel.

Exigence	Sous-exigence	O/N	Notes

Cadre adaptatif	Mettre en place des contrôles dynamiques		
	Permettre un suivi en temps réel		
	Soutenir l'adaptation des politiques		
	Fournir un ajustement basé sur le risque		
Capacités d'apprentissage	Activer la reconnaissance des formes		
	Soutenir l'apprentissage du comportement		
	Mise à jour des bases de sécurité		
Automatisation	Adapter les règles de sécurité		
	Modifier les contrôles d'accès		
	Mise à jour des critères de détection		

5.2.6 Analyse prédictive

Les capacités d'analyse prédictive devraient exploiter les données historiques et les informations actuelles sur les menaces pour prévoir les incidents de sécurité potentiels et permettre une atténuation proactive.

Exigence	Sous-exigence	O/N	Notes
Prévisions	Prévoir les incidents de sécurité		
	Identifier les menaces potentielles		
	Calculer les scores de risque		
	Tendances des attaques de projets		
Analyse	Traiter les données historiques		
	Analyser les modèles de menace		
	Évaluer les facteurs de risque		

Rapports	Générer des rapports de prévision		
	Fournir une analyse des tendances		
	Créer des évaluations de risques		

5.2.7 Opérations de sécurité automatisées

L'automatisation de la sécurité devrait rationaliser les opérations tout en maintenant la transparence et en permettant un contrôle humain des décisions critiques.

Exigence	Sous-exigence	O/N	Notes
Automatisation des tâches	Automatiser les tâches de routine		
	Gérer les alertes de sécurité		
	Gérer la réponse aux incidents		
	Gestion de la vulnérabilité des processus		
Gestion du flux de travail	Créer des flux de travail automatisés		
	Activer l'automatisation personnalisée		
	Soutenir la surveillance humaine		
Rapports	Suivi des actions automatisées		
	Tenir à jour les journaux d'audit		
	Produire des rapports d'efficacité		

5.2.8 Contrôle d'accès intelligent

Les systèmes de contrôle d'accès devraient tirer parti de l'IA pour prendre des décisions dynamiques tout en maintenant l'équilibre entre sécurité et convivialité.

Exigence	Sous-exigence	O/N	Notes

Analyse du comportement	Contrôler les activités des utilisateurs		
	Suivre les schémas d'accès		
	Détecter les anomalies		
	Profil du comportement de l'utilisateur		
Gestion de l'accès	Définir des autorisations dynamiques		
	Mettre en place un accès basé sur le risque		
	Permettre un accès juste à temps		
Protection de l'environnement	Empêcher les accès non autorisés		
	Bloquer les activités suspectes		
	Appliquer les politiques d'accès		

5.2.9 Prévention de la perte de données renforcée par l'IA

Les capacités de DLP devraient utiliser l'IA pour identifier et protéger avec précision les données sensibles tout en minimisant les interruptions d'activité.

Exigence	Sous-exigence	O/N	Notes
Détection des données	Identifier les données sensibles		
	Classer les types d'informations		
	Contrôler le mouvement des données		
	Suivi de l'utilisation des données		
La prévention	Bloquer le partage non autorisé		
	Chiffrer les données sensibles		
	Appliquer les politiques DLP		

Gestion	Créer des règles personnalisées		
	Générer des rapports DLP		
	Suivi des violations de la politique		

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

L'AI-SPM devrait fournir une visibilité complète sur la sécurité des services d'IA tout en permettant une remédiation automatisée des problèmes identifiés.

Exigence	Sous-exigence	O/N	Notes
Sécurité des services d'IA	Surveiller les charges de travail d'IA		
	Évaluer la sécurité du programme d'éducation et de formation tout au long de la vie		
	Suivi de l'accès au modèle d'IA		
	Évaluer l'utilisation des données d'IA		
Gestion	Automatiser les contrôles de sécurité		
	Activer les actions de remédiation		
	Maintenir les lignes de base en matière de sécurité		
Rapports	Générer des rapports sur la posture		
	Suivi des mesures de sécurité		
	Documenter l'état de conformité		

5.2.11 Sécurité SaaS alimentée par la GenAI

La sécurité SaaS devrait tirer parti de l'IA générative pour améliorer la protection tout en maintenant une visibilité et un contrôle complets.

Exigence	Sous-exigence	O/N	Notes

Protection du SaaS	Surveiller les applications SaaS		
	Contrôler l'accès aux données		
	Protéger les informations sensibles		
	Suivre les activités des utilisateurs		
Intégration	Soutenir les fonctions de la CASB		
	Activer l'intégration DLP		
	Assurer la sécurité de l'API		
Gestion	Générer des informations sur la sécurité		
	Automatiser l'application des politiques		
	Créer des rapports de conformité		

6. Qualifications des fournisseurs

6.1 Informations sur l'entreprise

- Au moins 5 ans d'expérience dans le domaine de la sécurité de l'informatique dématérialisée
- Expérience confirmée dans le domaine des solutions de sécurité pour les entreprises
- Une stabilité financière et une croissance solides
- Certifications et partenariats avec l'industrie
- Capacités de soutien au niveau mondial

6.2 Expertise technique

- Une expertise approfondie en matière de sécurité dans l'informatique dématérialisée
- Capacités d'analyse et d'IA avancées
- Expérience d'intégration avec les principales plates-formes

- Capacités de développement et de personnalisation
- Recherche en matière de sécurité et capacités de renseignement sur les menaces

6.3 Capacités de soutien

- Assistance technique 24/7/365
- Multiples canaux d'assistance
- Des programmes de formation complets
- Disponibilité des services professionnels
- Mises à jour et améliorations régulières des produits

7. Critères d'évaluation

7.1 Mérite technique (40%)

- Complétude de la solution
- Innovation technique
- Capacités en matière d'IA/ML
- Capacités d'intégration
- Évolutivité et performance
- Efficacité de la sécurité

7.2 Capacités fonctionnelles (30%)

- Caractéristiques de sécurité essentielles
- Analyse avancée
- Capacités d'automatisation
- Rapports et visibilité
- Expérience de l'utilisateur
- Options de personnalisation

7.3 Qualifications des fournisseurs (20%)

- Expérience de l'entreprise
- Expertise technique
- Références clients
- Infrastructure de soutien
- Feuille de route pour l'innovation
- Position sur le marché

7.4 Coût (10%)

- Prix de la solution
- Coûts de mise en œuvre
- Maintenance continue
- Frais de formation
- Services complémentaires
- Coût total de possession

8. Exigences en matière de soumission

Les vendeurs doivent soumettre :

1. Description détaillée de la solution technique
2. Méthodologie de mise en œuvre et d'intégration
3. Calendrier du projet avec les principales étapes
4. Structure tarifaire complète
5. Qualifications et expérience de l'entreprise
6. Au moins trois références d'entreprises
7. Plans d'assistance et de maintenance
8. Approche de la formation et du transfert de connaissances
9. Exemples de rapports et de documentation

10. Feuille de route des produits et plans de développement futurs

9. Calendrier

- Communiqué de presse :
- Questions à poser :
- Date limite de dépôt des propositions :
- Période d'évaluation :
- Présentations des fournisseurs :
- Sélection des fournisseurs :
- Début du projet :
- Phase de mise en œuvre 1 :
- Phase de mise en œuvre 2 :
- Achèvement du projet :

Soumettre toutes les propositions à

Contact technique :

Contact pour les achats :