Demande de proposition : Solution de plateforme de détection et de réponse étendue (XDR)

Table des matières

1. Introduction et contexte

lance un appel d'offres pour une plateforme complète de détection et de réponse étendues (XDR) afin d'améliorer son infrastructure de cybersécurité. Cet appel d'offres décrit nos besoins en matière de solution de sécurité avancée qui intègre plusieurs produits de sécurité dans un système cohésif, offrant des capacités améliorées de détection des menaces et de réponse sur l'ensemble de notre pile technologique.

Position actuelle en matière de sécurité

- Nous cherchons à mettre en œuvre une approche unifiée de la surveillance de la sécurité et de la réaction.
- La solution doit collecter et mettre en corrélation des données provenant de diverses sources, notamment des terminaux, des réseaux, des charges de travail en nuage, des systèmes de messagerie et des serveurs

- L'intégration avec les outils et l'infrastructure de sécurité existants est essentielle

Objectifs du projet

Les principaux objectifs de la mise en œuvre d'une plateforme XDR sont les suivants :

- Améliorer les capacités de détection et de réponse aux menaces dans l'ensemble des technologies de l'organisation.
- Consolider les outils de sécurité et améliorer l'efficacité opérationnelle
- Renforcer notre position globale en matière de sécurité grâce à des analyses avancées et à l'automatisation
- Veiller au respect des réglementations et des normes en matière de protection de la vie privée

2. L'étendue des travaux

Le fournisseur sélectionné sera responsable de

Mise en œuvre et intégration

1. Déploiement d'une plateforme XDR complète
2. Intégration avec l'infrastructure et les outils de sécurité existants
3. Configuration de la collecte de données provenant de sources multiples :
    - Points finaux
    - Réseaux
    - Charges de travail en nuage
    - Systèmes de courrier électronique
    - Serveurs

Fonctionnalité de base

1. Collecte et intégration des données
    - Agrégation transparente de données provenant de sources multiples
    - Intégration avec les outils de sécurité existants

- Traitement et corrélation des données en temps réel

2. Détection des menaces et réaction
    - Analyse avancée pour une identification complète des menaces
    - Capacités de réponse automatisée
    - Analyse des menaces inter-domaines
3. Suivi et visibilité
    - Visibilité accrue à travers les couches de sécurité
    - Capacités de surveillance complètes
    - Fonctions de chasse aux menaces en temps réel

3. Exigences techniques

1. Architecture de la plate-forme
    - Architecture native en nuage
    - Options de déploiement évolutives
    - Conception à haute disponibilité
    - Capacités d'équilibrage de la charge
    - Soutien à la reprise après sinistre
2. Exigences de performance
    - Traitement des données en temps réel
    - Temps de latence minimal dans la détection des menaces
    - Utilisation efficace des ressources
    - Solution de stockage évolutive
    - Capacités de recherche à grande vitesse
3. Exigences en matière de sécurité
    - Cryptage de bout en bout

- Contrôle d'accès basé sur les rôles
- Authentification multifactorielle
- Journalisation des audits
- Points d'extrémité d'API sécurisés

4. Exigences d'intégration
    - Support API standard
    - Prise en charge de formats de données communs
    - Intégration d'outils tiers
    - Capacités d'intégration personnalisées
    - Prise en charge des webhooks

4. Exigences fonctionnelles

1. Collecte et intégration des données

Conseil : le fondement d'une plateforme XDR efficace réside dans sa capacité à rassembler et à unifier des données provenant de sources diverses. Concentrez-vous sur l'évaluation de l'étendue des sources de données prises en charge et de la profondeur des capacités d'intégration. Tenez compte de la compatibilité de l'infrastructure existante et des besoins futurs en matière d'évolutivité.

Exigence	Sous-exigence	O/N	Notes
Source des données Collecte	Collecte à partir des points d'extrémité		
	Collecte auprès des réseaux		
	Collecte des charges de travail en nuage		
	Collecte à partir de systèmes de courrier électronique		
	Collecte auprès des serveurs		

Capacités d'intégration	Intégration avec le SIEM existant		
	Intégration avec les systèmes de pare-feu		
	Intégration avec les solutions EDR		
	Intégration avec les systèmes de gestion de l'identité		
Traitement des données	Ingestion de données en temps réel		
	Normalisation des données		
	Enrichissement des données		

2. Détection unifiée des menaces

Conseil : Un système de détection des menaces robuste doit offrir une visibilité complète tout en minimisant les faux positifs. Évaluez la capacité de la solution à corréler les menaces entre les différentes couches de sécurité et son efficacité à identifier des schémas d'attaque sophistiqués.

Exigence	Sous-exigence	O/N	Notes
Visibilité des menaces	Surveillance des menaces à travers la pile		
	Détection des menaces en temps réel		
	Analyse historique des menaces		
Capacités d'analyse	Corrélation des données entre les sources		
	Analyse comportementale		
	Reconnaissance des formes		
	Détection des anomalies		

3. Capacités de réponse automatisée

Conseil : Tenez compte à la fois des capacités d'automatisation et de la possibilité de personnaliser les actions de réponse. Recherchez des solutions

qui équilibrent les réponses automatisées et la supervision humaine et qui fournissent des pistes d'audit claires de toutes les actions entreprises.

Exigence	Sous-exigence	O/N	Notes
Intégration de l'IA/ML	Réponse basée sur l'apprentissage automatique		
	Classification automatisée des menaces		
	Adaptation dynamique de la réponse		
Orchestration des réponses	Actions de réponse à plusieurs niveaux		
	Cahiers de réponses personnalisables		
	Validation de l'action de réponse		
	Capacités de retour en arrière		

4. Visibilité accrue

Conseil : la solution doit offrir à la fois une vue d'ensemble et des détails granulaires en cas de besoin. Concentrez-vous sur l'évaluation de la profondeur de la visibilité dans les différents environnements et sur la capacité à pivoter rapidement entre les vues de haut niveau et les vues détaillées.

Exigence	Sous-exigence	O/N	Notes
Visibilité multicouche	Visibilité des points d'accès		
	Visibilité du réseau		
	Visibilité de l'environnement en nuage		
Capacités de surveillance	Contrôle en temps réel		
	Analyse des données historiques		
	Découverte des actifs		

Chasse aux menaces	Possibilités d'interrogation personnalisées		
	Flux de travail pour la chasse aux menaces		
	Outils d'enquête		

5. Gestion des alertes et triage

Conseil : une gestion efficace des alertes est cruciale pour la productivité du SOC. Évaluez la capacité de la solution à réduire la fatigue liée aux alertes tout en veillant à ce que les menaces critiques ne soient pas manquées. Prenez en compte les capacités de triage automatisées et manuelles.

Exigence	Sous-exigence	O/N	Notes
Consolidation des alertes	Agrégation d'alertes multi-sources		
	Déduplication des alertes		
	Corrélation des alertes		
Réduction des faux positifs	Filtrage basé sur l'apprentissage automatique		
	Règles de filtrage personnalisées		
	Validation des alertes		
Gestion des priorités	Hiérarchisation automatisée des priorités		
	Règles de priorité personnalisées		
	Notation basée sur le risque		

6. Analyse des menaces inter-domaines

Conseil : une analyse inter-domaines efficace nécessite une visibilité à la fois profonde et étendue. Recherchez des solutions capables non seulement de collecter des données dans plusieurs domaines, mais aussi de les corréler et de les analyser de manière significative afin de fournir des informations exploitables et des récits d'attaque clairs.

Exigence	Sous-exigence	O/N	Notes
Contexte de la menace	Corrélation de la télémétrie inter-domaine		
	Visualisation de la chaîne d'attaque		
	Attribution des acteurs de la menace		
Analyse d'impact	Évaluation de l'impact de l'accueil		
	Analyse de l'impact sur le réseau		
	Évaluation de l'impact sur les entreprises		
Analyse des causes profondes	Identification du vecteur d'attaque initial		
	Cartographie du chemin de propagation		
	Analyse des facteurs contributifs		
Création d'un calendrier	Séquencement des événements		
	Corrélation temporelle		
	Intégration du contexte historique		

7. L'évolutivité

Conseil : Tenez compte non seulement des besoins actuels, mais aussi de la croissance future. La solution doit pouvoir gérer des volumes de données croissants, de nouveaux outils de sécurité et une infrastructure en expansion sans dégradation significative des performances ni modification de l'architecture.

Exigence	Sous-exigence	O/N	Notes
Croissance organisationnelle	Prise en charge de l'augmentation du nombre de points d'extrémité		

	Modèle de licence flexible		
	Soutien multisite		
Gestion du volume de données	Stockage évolutif des données		
	Politiques de conservation des données		
	Optimisation des performances		
Adaptabilité des infrastructures	Évolutivité de l'informatique en nuage		
	Capacité d'extension sur site		
	Soutien au déploiement hybride		

8. Interface utilisateur et rapports

Conseil : l'interface doit concilier puissance et convivialité, permettant à la fois aux analystes débutants d'obtenir des informations rapides et aux utilisateurs expérimentés de mener des recherches approfondies. Les rapports doivent être à la fois complets et personnalisables.

Exigence	Sous-exigence	O/N	Notes
Conception de l'interface	Navigation intuitive		
	Vues basées sur les rôles		
	Tableaux de bord personnalisables		
Outils d'enquête	Chasse interactive aux menaces		
	Analyse visuelle des liens		
	Capacités de recherche avancées		
Caractéristiques des rapports	Modèles de rapports prédéfinis		
	Création de rapports personnalisés		

	Rapports programmés		
	Résumés exécutifs		
	Rapports techniques détaillés		

9. Intégration du renseignement sur les menaces

Conseil : Concentrez-vous sur la qualité des renseignements intégrés sur les menaces et sur la capacité de la plateforme à les rendre opérationnels de manière efficace. Examinez la capacité de la solution à combiner les renseignements externes avec le contexte interne.

Exigence	Sous-exigence	O/N	Notes
Sources de renseignements	Intégration des aliments pour animaux dans le commerce		
	Renseignements en libre accès		
	Renseignements spécifiques à l'industrie		
Gestion du renseignement	Gestion des indicateurs		
	La curation de l'information		
	Création de renseignements personnalisés		
Intégration opérationnelle	Corrélation en temps réel		
	Enrichissement automatisé		
	Chasse rétroactive		

10. Conformité et confidentialité des données

Conseil : assurez-vous que la solution permet non seulement de maintenir la conformité, mais aussi d'en fournir la preuve. Tenez compte à la fois des exigences réglementaires actuelles et des obligations futures potentielles.

Exigence	Sous-exigence	O/N	Notes
Traitement des données	Collecte de données conforme		
	Soutien à la souveraineté des données		
	Capacités de masquage des données		
Conformité réglementaire	Conformité au GDPR		
	Conformité HIPAA		
	Conformité à la norme PCI DSS		
Contrôles de la vie privée	Contrôles d'accès		
	Anonymisation des données		
	Gestion des consentements		
Soutien à l'audit	Rapport de conformité		
	Pistes d'audit		
	Collecte de preuves		

11. Soutien à l'API et à l'intégration

Conseil : Les API doivent être bien documentées, sécurisées et prendre en charge à la fois les besoins d'intégration de base et les scénarios d'automatisation avancés. Tenez compte de l'exhaustivité de la surface de l'API et de la qualité de l'assistance aux développeurs.

Exigence	Sous-exigence	O/N	Notes
Capacités de l'API	Prise en charge de l'API RESTful		
	Accès aux données en temps réel		
	Soutien aux opérations en vrac		

Caractéristiques d'intégration	Développement d'une intégration personnalisée		
	Intégrations prédéfinies		
	Prise en charge des webhooks		
Soutien au développement	Documentation de l'API		
	Outils du développeur		
	Disponibilité d'un exemple de code		
Contrôles de sécurité	Authentification de l'API		
	Limitation du taux		
	Enregistrement des accès		

12. Surveillance et alerte en temps réel

Conseil : Les capacités en temps réel doivent concilier rapidité et précision. Il faut tenir compte à la fois de la rapidité des alertes et de la capacité du système à maintenir ses performances dans des conditions de volume élevé.

Exigence	Sous-exigence	O/N	Notes
Capacités de surveillance	Traitement des données en temps réel		
	Surveillance continue des actifs		
	Contrôle des performances		
Gestion des alertes	Génération d'alertes en temps réel		
	Acheminement des alertes		
	Règles de suppression des alertes		
État du système	Surveillance de la santé		
	Suivi des capacités		

	Suivi des temps de latence		
Systèmes de notification	Multiples canaux de notification		
	Notifications personnalisables		
	Flux de travail d'escalade		

13. Fonctionnalités alimentées par l'IA

Conseil : Les capacités de l'IA doivent améliorer et non remplacer l'analyse humaine. Recherchez des solutions qui permettent d'expliquer les décisions de l'IA et d'assurer une supervision humaine tout en automatisant les tâches de routine et en fournissant des capacités d'analyse avancées.

Exigence	Sous-exigence	O/N	Notes
Analyse de cas	Génération d'un résumé de cas d'IA		
	Corrélation entre les événements et les entités		
	Recommandations pour les prochaines étapes		
Analyse du commandement	Désobfuscation de la ligne de commande		
	Analyse des intentions		
	Évaluation de l'impact sur la sécurité		
Capacités de recherche	Interrogation en langage naturel		
	Optimisation de la recherche dans le lac de données		
	Des résultats adaptés au contexte		
Intégration de MITRE ATT&CK	Cartographie automatique des TTP		

	Classification des tactiques		
	Identification de la technique		
Modèles d'IA avancés	Intégration de modèles cyber-entraînés		
	Reconnaissance des schémas d'attaque		
	Analyse comportementale		
Renseignements sur les menaces	Détection améliorée par ML		
	Corrélation automatisée des menaces		
	Mises à jour des renseignements en temps réel		
Automatisation des réponses	Manuels de jeu alimentés par l'IA		
	Réponse basée sur un scénario		
	Orchestration automatisée		
Analyse prédictive	Prévision des tendances en matière d'attaques		
	Prévision de la vulnérabilité		
	Évaluation des risques		
Automatisation du SOC	Automatisation des flux de travail		
	Optimisation des ressources		
	Hiérarchisation des tâches		
Apprentissage adaptatif	Formation continue du modèle		
	Apprentissage des données d'extrémité		
	Amélioration dynamique de la sécurité		

Analyse en temps réel	Agrégation de données pilotée par l'IA		
	Corrélation télémétrique		
	Génération d'informations en temps réel		

5. Qualifications des fournisseurs

Qualifications requises

1. Au moins 5 ans d'expérience dans le domaine de XDR ou des solutions de sécurité connexes
2. Expérience confirmée dans la mise en œuvre réussie de projets d'entreprise
3. Forte présence sur le marché de la cybersécurité
4. Base de clientèle établie avec des références vérifiables
5. Équipe d'assistance et de maintenance dédiée
6. Une feuille de route claire pour le développement des produits
7. Stabilité et viabilité financières

Qualifications souhaitées

1. Reconnaissance du secteur par les analystes (Gartner, Forrester)
2. Expérience dans des secteurs verticaux similaires
3. Présence d'un soutien local
4. Programme actif de recherche et développement
5. Un écosystème de partenaires bien établi

6. Critères d'évaluation

Les propositions seront évaluées sur la base des critères suivants :

Critère	Poids
Capacité technique	30%
Capacités d'intégration	20%

Capacités en matière d'IA/ML	15%
Facilité d'utilisation	10%
Coût	10%
Expérience des fournisseurs	10%
Soutien et maintenance	5%

7. Lignes directrices pour la soumission

Les vendeurs doivent soumettre :

1. Proposition technique détaillée
2. Méthodologie de mise en œuvre
3. Calendrier du projet
4. Structure des prix
5. Profil de l'entreprise
6. Références clients
7. Plans d'assistance et de maintenance
8. Détails du programme de formation

8. Calendrier

Jalon	Date
Publication de l'appel d'offres	
Date limite pour les questions	
Date d'échéance de la proposition	
Présentations des fournisseurs	
Décision de sélection	
Coup d'envoi du projet	

9. Informations sur les contacts

Pour toute question ou soumission de proposition :