Objet

Data Scientist (F/H)

Date

09.01.2025

idruide est un acteur majeur de la gestion de la mobilité numérique et un éditeur de solutions reconnu et certifié dans le domaine du MDM/UEM. Ā destination des entreprises, des collectivités et des gouvernements, nos solutions répondent aux défis de la souveraineté numérique ; de déploiement, de sécurité et de maintenance des parcs d'appareils mobiles.

Forte de deux entités et d'une trentaine de collaborateurs, notre entreprise connaît une croissance soutenue, portée par une équipe jeune, dynamique et passionnée.

Chez idruide, nous avons à cœur d'innover et de maintenir un haut niveau d'exigence dans nos solutions, tout en assurant un climat de confiance et de bien-être pour nos collaborateurs. Notre ambition est de faire du MDM/UEM le socle des projets de cybersécurité des SI.

Missions principales

Dans le cadre de l'évolution de nos solutions et de notre volonté de créer de la valeur à partir des données collectées, nous recherchons un·e Data Scientist qui sera chargé·e de :

- Comprendre, exploiter et valoriser les données issues de nos parcs d'appareils mobiles (MDM/UEM) afin de renforcer la sécurité, la conformité et l'optimisation du parc.
- Mettre en place et optimiser des pipelines AI/ML en collaboration avec l'équipe technique (techniciens, architectes, CTO) et contribuer aux projets visant à faire de la solution MDM/UEM un élément central de la cybersécurité des SI.
- Construire des modèles de machine learning (supervisé, non supervisé, prédictif, temps réel, etc.) et assurer leur industrialisation pour améliorer la gestion du parc et détecter d'éventuelles menaces ou anomalies.

Vous deviendrez la référence Data Science au sein de l'entreprise pour transformer nos données en insights et solutions à forte valeur ajoutée, notamment dans la mise en œuvre d'analyses de sécurité avancées (ex. détection d'intrusions, maintenance prédictive, veille d'anomalies…).

Profil

Formation & expérience

- Diplôme d'ingénieur, Master ou équivalent en Data Science, Statistiques, Mathématiques, Cybersécurité ou un domaine similaire.
- Expérience significative (stages, alternances, postes précédents) en Data Science, idéalement dans la conception de modèles ML et la mise en place de pipelines (incluant des problématiques de sécurité ou de SI critiques).

Compétences techniques

- Maîtrise de Python (pandas, NumPy, scikit-learn, TensorFlow, PyTorch…) ou d'un autre langage adapté aux tâches d'IA/ML.
- Aisance avec les outils d'IA open source et capacité à travailler sur des environnements MLOps (CI/CD, conteneurisation, etc.).
- Connaissance des bases de données (SQL, NoSQL) et des bonnes pratiques pour la préparation et la structuration des données.
- Familiarité avec la démarche Data as a Product : cycle de vie des données, conception de produits data, exploitation et valorisation.

- Capacité à mettre en place des flux de données temps réel (ex. Apache Flink) pour l'analyse de la sécurité et la détection d'incidents.
- Compréhension des principes de sécurité mobile (MDM/UEM) : politiques d'accès, chiffrement, authentification, surveillance des terminaux, etc.
- Connaissance ou sensibilité aux problématiques de cybersécurité et de sécurité des SI (MTD, XDR/eDR, SIEM, SOAR).

Qualités humaines
- Esprit d'analyse et rigueur méthodologique.
- Capacité à vulgariser et à communiquer clairement auprès d'équipes techniques et non techniques.
- Curiosité et goût pour l'innovation, notamment pour les sujets de cybersécurité.
- Autonomie, sens de l'initiative et excellent relationnel.

Responsabilitées

Analyse et compréhension des données
- Cartographier et comprendre les différents flux de données collectées via le MDM/UEM (logs, métadonnées, indicateurs d'usage, événements de sécurité, etc.).
- Effectuer un data cleaning et une analyse exploratoire pour identifier les patterns, les anomalies et les tendances (y compris en matière de sécurité).

Développement de modèles AI/ML
- Proposer, concevoir et entraîner des modèles de machine learning adaptés aux problématiques de gestion de flotte, de détection d'intrusions, de maintenance prédictive, etc.
- Travailler avec l'équipe technique pour définir les architectures de données nécessaires (data lakes, bases de données, plateformes de calcul, intégration avec SIEM…).

Mise en place de pipelines
- Mettre en place des pipelines AI/ML robustes et évolutifs, en s'appuyant sur l'infrastructure existante ou en la co-construisant avec l'équipe en place (MDM/UEM, outils de cybersécurité…).
- Assurer l'industrialisation (MLOps) et le déploiement des modèles, y compris le suivi de leurs performances et la mise à jour continue.

Analyse en temps réel et automatisation

- Intégrer et exploiter des flux de données temps réel (par exemple via Apache Flink) pour détecter rapidement des comportements suspects ou des failles de sécurité.
- Participer à l'automatisation de la réponse aux incidents (isolation d'un terminal compromis, déclenchement d'alertes, etc.).

Collaboration et veille

- Collaborer étroitement avec le CTO, les techniciens et les architectes pour aligner les développements Data Science aux objectifs métiers, techniques et de sécurité.
- Réaliser une veille technologique (nouvelles méthodes d'analyse, frameworks ML/AI open source, solutions de visualisation…) et être force de proposition pour améliorer nos processus.
- Participer à la démarche "Data as a Product" pour faire des données un véritable atout stratégique et proposer des évolutions produits centrées sur la sécurité et la conformité.

Transversalité, cybersécurité et communication

- Contribuer à la définition et à l'implémentation des politiques de cybersécurité sur les terminaux (chiffrement, authentification forte, règles de sécurité…) en synergie avec l'équipe MDM/UEM.
- Communiquer de manière pédagogique les résultats d'analyse et les recommandations auprès des équipes internes et des clients.
- Participer à la définition des bonnes pratiques en matière de gouvernance des données, de cybersécurité et de conformité (RGPD, ISO 27001, NIS2…).

Ce que nous offrons

Ambiance startup : Environnement jeune, dynamique et novateur en plein cœur de Monaco.
Cadre de travail agréable : Bureaux proches des commerces, snacks et café à volonté.
Perspectives d'évolution : Vous serez le pilier de la Data Science et participerez à la structuration d'une équipe Data axée sur la mobilité et la cybersécurité.
Avantages : Mutuelle d'entreprise, projets R&D stimulants, opportunités de monter en compétences sur des technologies de pointe et d'avoir un réel impact sur la sécurité des SI. Aménagement du temps de travail et télétravail

Candidature et rémunération

Prise de poste : immédiate à Monaco

Rémunération : selon profil

Type d'emploi : temps plein (39h)

Période d’essai : 3 mois

Envoyez votre curriculum vitæ, portfolio et une lettre de motivation à recrutement@idruide.com