



Séverin DINGAORO

Je recherche un poste de : **Expert et Administrateur**

Splunk Core and Security + SOC Analyst

Disponible pour des missions de gestion, de configuration et d'optimisation de l'environnement Splunk : - Installation, configuration et maintenance des instances Splunk - Automatisation et amélioration continue des processus de collecte - Développement de Dashboards, rapports, alertes et KPIs de sécurité - Surveillance et analyse des données pour identifier les incidents système et cybersécurité, et y remédier.

INFORMATIONS

☎ 0753964679

✉ dingaoro@yahoo.fr

in www.linkedin.com/in/séverin-dingaoro-1a9b50102

SOFT SKILLS

- Communication
- Esprit d'équipe
- Proactivité

LOGICIELS

- Splunk Security
- Splunk ITSI
- Python + Bash

LANGUES

Anglais : C1 - Professionnel

INTÉRÊTS

- Cyber sécurité
- Machine Learning

EXPÉRIENCES PROFESSIONNELLES

2020 - 2025 | CONSULTANT INDÉPENDANT ADMIN SPLUNK BANQUE DE FRANCE

- Installation, configuration et maintenance des instances Splunk (Search Head, Indexer, Forwarder...)
- Administration et maintien en conditions opérationnelles de Splunk (Core, ES, ITSI...)
- Intégration et gestion du module Splunk ITSI : KPI, services, corrélation, tuning, alerting
- Automatisation et amélioration continue des processus de collecte (HF, HEC, Syslog.) et gestion des logs, des accès et qualité des données (CIM).
- Détection, analyse et investigation des incidents système et cybersécurité
- Développement de Dashboards, rapports et KPIs de sécurité et de supervision
- Collaboration avec les équipes SOC, CERT et de Supervision
- Documentation technique et formation des utilisateurs

2018 - 2020 | EXPERT SPLUNK ORANGE BUSINESS pour le compte de la Banque de France

- Installer Splunk Optimiser la configuration des index et sourcetypes pour améliorer la performance de recherche et la pertinence des résultats
- Intégration et gestion des logs, des accès et qualité des données
- Développement de Dashboards, des rapports/alertes et création des CS/NEAP (ITSI) pour la supervision KPIs de sécurité et de supervision
- Concevoir des tableaux de bord interactifs pour une visualisation claire des tendances et anomalies en temps réel
- Automatisation et amélioration continue des processus de collecte et de détection, des incidents optimisant l'efficacité opérationnelle et la réactivité
- Collaboration avec les équipes SOC, CERT et de Supervision (ITSI)
- Documentation technique et formation des utilisateurs

CERTIFICATIONS

<https://www.credly.com/users/dingaoro-severin/badges#credly>

- Splunk Enterprise Security Certified Admin
- Splunk Enterprise Certified Admin
- Certified Power User

2016 - 2017 | STAGE DE FIN D'ÉTUDES D'INGÉNIEURS : DATA SCIENTIST SPLUNK

BNP PARIBAS

- Développer des pipelines ETL robustes pour l'intégration et la transformation des données volumineuses
- Développer des solutions de Machine Learning (classification, clustering, prédiction) pour optimiser la prise de décision et automatiser les processus
- Optimiser les modèles de machine learning en ajustant hyperparamètres pour maximiser leur efficacité
- Concevoir des algorithmes d'optimisation pour améliorer la performance des modèles prédictifs
- Élaborer des stratégies de détection d'anomalies en temps réel pour anticiper les incidents critiques
- Créer des visualisations interactives pour faciliter la prise de décision basée sur les données
- Accompagnement technique des users Splunk

FORMATIONS

2015 - 2016 | MASTÈRE SPÉCIALISÉ (BAC+6) BIG DATA : ANALYSE, MANAGEMENT ET VALORISATION RESPONSABLE

INP ENSIMAG - GRENOBLE

2006 - 2007 | MASTER 2 (M2), ECONOMIE : AIDE À LA DÉCISION

UNIVERSITÉ CLAUDE BERNARD LYON 1

2004 - 2005 | MASTER 2 (M2), MATHÉMATIQUES APPLIQUÉES STATISTIQUES - INFORMATIQUE

UNIVERSITÉ CLAUDE BERNARD LYON 1