



BONNES PRATIQUES METIERS

**SAFEO Cyber : Endpoint
Detection & Response
(EDR)**

Page 2

LE ZOOM

**Les rencontres SAFEO
e-Santé à l'Université
Paris Saclay**

EDITORIAL

Depuis janvier 2024, SAFEO e-Santé, la filiale Santé du Groupe SAFEO, participe activement aux séminaires scientifiques mensuels organisés à l'Université Paris-Saclay. Ce sont des opportunités importantes pour les étudiants, chercheurs et ingénieurs qui leur permettent d'échanger sur leurs expériences et innovations.

Les projets présentés lors de ces séminaires mensuels s'appuient largement sur des outils numériques, nécessitant souvent des ressources informatiques hébergées, surtout pour les données de santé. Par exemple, le 16 mai, une présentation sur l'imagerie multimodale a mis en lumière les besoins considérables en puissance de calcul et en stockage pour ce type de technologie avancée. Un autre projet notable le 17 octobre, "Advanced nanoparticles for drug delivery", a soulevé la question de l'hébergement sécurisé de données sensibles et confidentielles.

Face à ces enjeux, les infrastructures de SAFEO jouent un rôle clé en permettant à diverses entités de collaborer efficacement sur des projets impliquant des données sensibles, tout en garantissant leur sécurité et leur confidentialité.

LE NOMBRE

R25

**Stand R25 de SAFEO au
salon Cloud Expo Europe
Paris les 27 et 28
novembre 2024**



L'INTERVIEW



Trois minutes avec ...

Bruno Rignon

Page 2

LA PHRASE

« Plus globalement, je compte sur les applications IA pour appuyer cette progression, en leur déléguant certaines tâches de moindres valeurs ajoutées ! »

Bruno Rignon,
Administrateur Systèmes
& Réseaux chez SAFEO



Groupe
safeo

Newsletter Novembre 2024



L'INTERVIEW

Trois minutes avec ...

Bruno Rignon, Administrateur
Systèmes & Réseaux chez SAFE0

Quelle est votre fonction et périmètre d'actions au sein de SAFE0 ? Je suis Administrateur Systèmes & Réseaux, avec une spécialisation orientée systèmes Linux. Mon périmètre d'actions consiste à optimiser les performances des infrastructures informatiques hébergées de nos clients et à répondre à leurs différentes problématiques.

En 3 mots, parlez-nous de votre activité ? Dans mon activité, il faut faire preuve de **Polyvalence Technique**. Pour dire simplement les choses, mes activités quotidiennes résident en ce que les Systèmes d'Information de SAFE0, et donc de nos clients, fonctionnent bien. Pour se faire, des actions en mode projet sont à mener quand il s'agit par exemple d'améliorer les performances et la fiabilité des infrastructures en datacenter ou de délivrer les prestations systèmes et réseaux commandées par les clients. Des démarches correctives sont aussi à prendre en compte quand un ticket client est émis ou qu'une alerte de fonctionnement se déclenche. A ce propos, l'**Esprit d'Equipe** chez SAFE0 est remarquable. La gestion des tickets clients, tant pour les demandes de services que pour les traitements d'incidents, illustre bien la forte collaboration qui règne dans le service Exploitation. La première personne disponible et qui estime posséder les compétences s'occupe du traitement du ticket, ce qui garantit fluidité et rapidité dans la réponse aux clients. Enfin je souhaiterais évoquer la **Bienveillance** de la direction qui s'implique fortement dans nos activités quotidiennes et qui sait nous épauler quand nécessaire.

Comment voyez-vous évoluer votre métier ? Dans le cadre de SAFE0, je souhaite monter en compétences sur les différents environnements technologiques sur lesquels je travaille. Plus globalement, je compte sur les applications IA pour appuyer cette progression, en leur déléguant certaines tâches de moindres valeurs ajoutées.

BONNES PRATIQUES METIERS

SAFE0 Cyber : Endpoint Detection & Response (EDR)

Parmi les propositions de valeur proposées par SAFE0 et mises en œuvre au sein de ces propres infrastructures informatiques, SAFE0 CYBER EDR (EDR pour Endpoint Detection and Response) est une offre de nouvelle génération.

Notre solution de cybersécurité repose sur deux piliers essentiels : la détection des menaces et la réponse immédiate. Elle se distingue par sa capacité à alerter contre les cyberattaques en effectuant une analyse comportementale et en détectant les activités suspectes directement sur les terminaux (endpoints) d'un Système d'Information, tels que les ordinateurs, les serveurs et les mobiles. La détection s'appuie sur une surveillance continue et des analyses avancées des endpoints du réseau. Elle permet d'identifier rapidement toute activité anormale ou potentiellement malveillante. La réponse, quant à elle, se caractérise par sa rapidité et son efficacité, permettant d'intervenir immédiatement pour bloquer les attaques et limiter leur impact avant qu'elles ne se propagent ou ne causent des dommages significatifs.

Ces deux aspects fondamentaux, parties intégrantes des Bonnes Pratiques Métiers des équipes de SAFE0, leur permettent d'identifier rapidement les menaces potentielles et d'y réagir de manière proactive et appropriée.