SAFEO NEWS

La Newsletter de SAFEO - Janvier 2026

SAFEO RENFORCE SON OFFRE SOUVERAINE EN DEVOILANT SAFEO OPEN CLOUD !

SAFEO OPEN CLOUD

EDITORIAL

Depuis 2023, le paysage de la Virtualisation de plateformes informatiques a été bouleversé, avec notamment des hausses de prix drastiques et un modèle d'abonnement contraignant qui forcent les organisations à repenser leur infrastructure IT. À cela s'ajoute un environnement géopolitique instable, où le choix d'hébergeurs grand public américains interroge : soumission aux lois d'extraterritorialité US comme le Patriot Act (2001) et le CLOUD Act (2018), risques de blocage de données et absence de réciprocité. Les entreprises françaises et européennes recherchent désormais des solutions souveraines et sécurisées, libérées des dépendances étrangères.

C'est dans ce contexte que SAFEO dévoile son offre Open Cloud, une solution d'hébergement professionnel flexible et souveraine, 100% opérée en France. Elle s'appuie sur des technologies Open Source stables, reconnues et accessibles, et repose sur des compétences en conseil, installation et maintenance entièrement maîtrisées par SAFEO.

SAFEO Open Cloud, qui s'inscrit pleinement dans la proposition de valeur de SAFEO, hébergeur souverain et infogéreur de confiance, garantit aux entreprises la maîtrise, la sécurité et la confidentialité de leurs applications et de leurs données, tout en assurant simplicité, transparence et accompagnement de proximité.

L'INTERVIEW

Je parlerai d'abord de Sensibilisation. Mon objectif est d'aider les collaborateurs de SAFEO à faire face aux cybermenaces à travers des mises en situation concrètes, comme les « P'tits Dej Sécu » ou les campagnes de phishing fictives !

Paul-Antoine Keib, Stagiaire Réseau et Sécurité Informatique chez SAFEO **PAGE 2**

LA DATE

SAFEO vous souhaite une Bonne Année 2026 !

BONNES PRATIQUES METIERS

La Gouvernance de la Sécurité

PAGE 2

L'interview

Paul-Antoine Keib, Stagiaire Réseau et Sécurité Informatique chez SAFEO

Quelle est votre fonction et périmètre d'actions ? Stagiaire actuellement au sein du Service Sécurité de l'Information (SSI) de SAFEO, ma mission principale consiste à sensibiliser les collaborateurs aux bonnes pratiques en cybersécurité. Concrètement, je prépare et j'anime les « P'tits Dej Sécu », des ateliers mensuels de formation à la cybersécurité. J'interviens aussi dans la mise en place de campagnes de phishing fictives, envoyées en interne, qui servent à tester et renforcer la vigilance des équipes.

En 3 mots, comment définissez-vous votre activité ? Je parlerai d'abord de **Sensibilisation**. Mon objectif est d'aider les collaborateurs de SAFEO à faire face aux cybermenaces à travers des mises en situation concrètes, comme les « P'tits Dej Sécu » ou les campagnes de phishing fictives, afin qu'ils adoptent les bons réflexes. Je dois aussi faire preuve de **Pédagogie** et savoir vulgariser des notions complexes de cybersécurité pour les rendre accessibles aussi bien aux profils techniques qu'aux équipes commerciales ou administratives. Durant les « P'tits Dej Sécu », un quiz en fin de session rend la formation plus ludique et permet de mieux mémoriser les messages clés partagés pendant l'atelier. Enfin, j'évoquerai la **Créativité** de mes activités, en participant notamment à l'élaboration de campagnes de phishing de plus en plus élaborées, en restant en veille sur l'évolution rapide des menaces afin d'actualiser les supports des « P'tits Dej Sécu » et d'adapter les scénarios de phishing au contexte du moment. Ce travail fait aussi appel à une certaine dimension psychologique : se mettre à la place d'un collaborateur technique, commercial, d'un manager ou d'un membre du back-office, comprendre ses habitudes professionnelles afin de concevoir des scénarios assez réalistes pour susciter le clic… tout en gardant l'objectif final de sensibilisation !

Comment vous voyez-vous évoluer ? En stage chez SAFEO pour quelques mois, je suis actuellement en 4e année d'école d'ingénieur généraliste. Cette expérience professionnelle oriente ma réflexion sur les spécialisations que je pourrai choisir en 5e année à la rentrée prochaine. Une première voie est celle de la Cybersécurité, domaine dans lequel j'ai déjà pu développer des compétences opérationnelles, notamment en découvrant et en travaillant autour de l'offre SAFEO Cyber. Une seconde voie porte sur l'Energie & Ville du futur, un sujet en lien avec les engagements de SAFEO en matière de sobriété énergétique : l'entreprise a par exemple choisi, en octobre dernier, d'implanter une partie de ses infrastructures à Rennes chez Nation Data Center, reconnu pour ses centres de données performants et durables.

BONNES PRATIQUES MÉTIERS

La Gouvernance de la Sécurité

Chez SAFEO, la cybersécurité n'est pas essentiellement qu'une question technologique, c'est avant tout un pilotage stratégique partagé. Les défis numériques sont transformés en décisions collaboratives, impliquant Direction, RSSI et Responsable Métiers pour que sécurité informatique ne riment pas avec contrainte business.

Les Bonnes Pratiques mises en œuvre par SAFEO dans la gouvernance de la sécurité se caractérisent en une supervision globale. Elles créent un cadre clair pour la gestion des incidents et la remontée des alertes afin de contenir leurs impacts via une réaction rapide et coordonnée. Elles capitalisent sur l'expérience pour consolider le Système de Management de la Sécurité de l'Information (SMSI), permettent d'optimiser la posture sécurité globale et d'entretenir une culture de la confiance. Plus concrètement, tout événement comme une défaillance serveur, une interruption système, une anomalie réseau ou application, … déclenche un signalement immédiat au responsable concerné, une qualification selon son importance et son urgence, et une réponse appropriée pour limiter les effets, préserver les preuves et activer la cellule de crise si nécessaire. Une enquête diagnostique l'origine, oriente la remédiation, puis un bilan final analyse la cause originelle pour alimenter l'amélioration continue.

Certifié ISO27001 et HDS, SAFEO protège ainsi toutes les données de ses clients (quotidiennes, métiers, sensibles) grâce à une gouvernance proactive de la sécurité et une gestion réactive des incidents. Il en résulte des bénéfices pour les entreprises en garantissant leur continuité d'activité et en renforçant leur résilience face aux cybermenaces !