N°238 — Juillet-Août 2025

www.linformaticien.com

L'INFORMATICIEN

DevOps
Les nouveautés RHEL 10

Cloud
Snowflake Summit

Hardware
PCIe 7

Logiciel
Attention : IA Washing !

2025

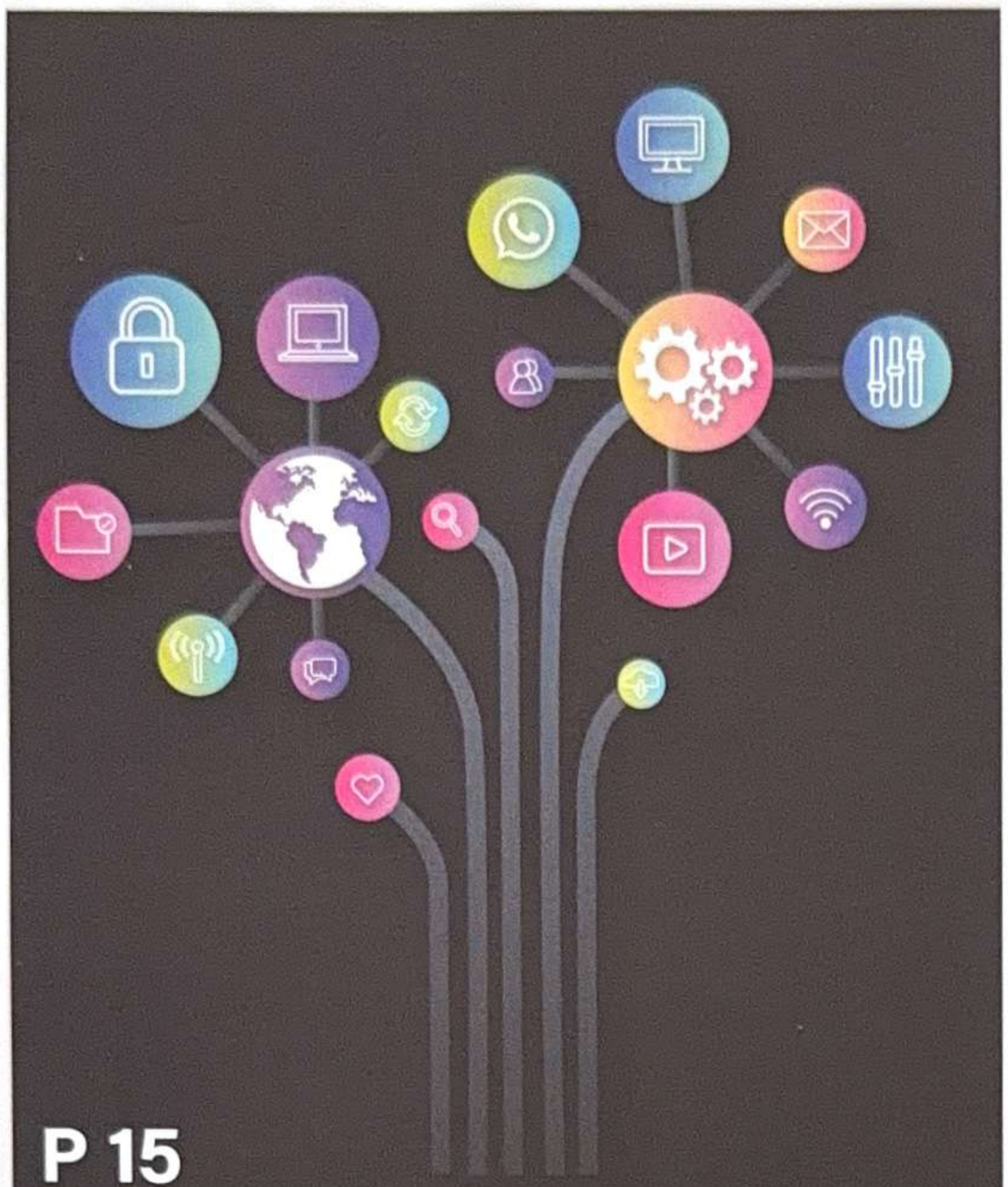
Top Tech

Les entreprises en action !

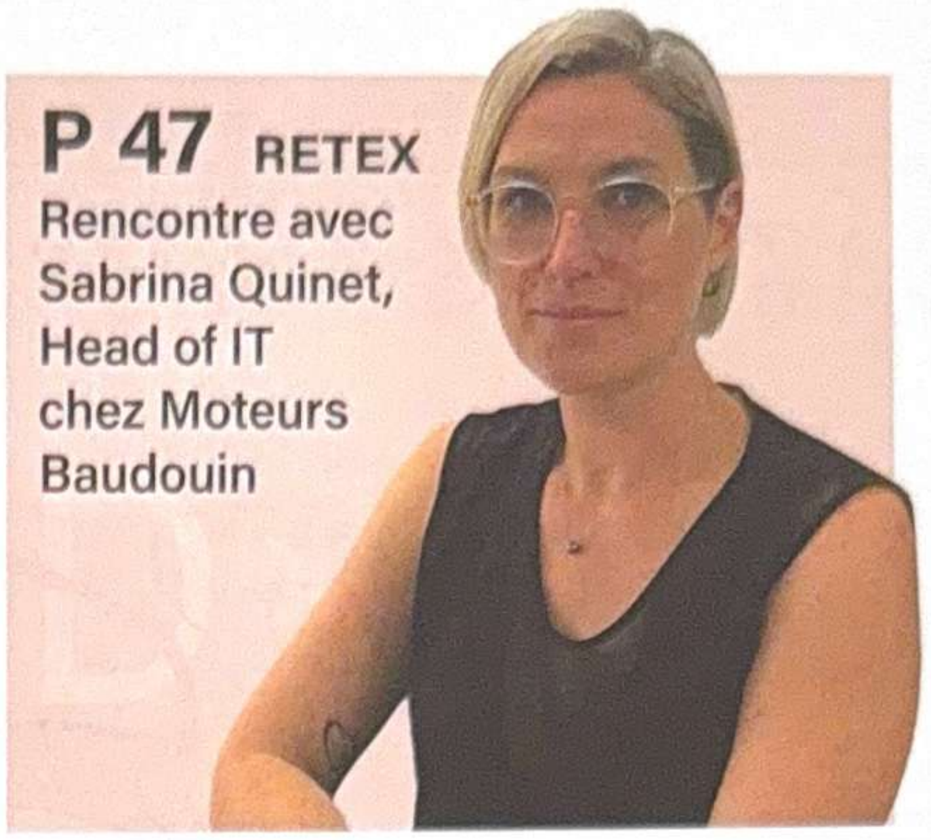
ESN
Infosys fait vibrer Roland-Garros

Retex
« En dépit du fait d'être bien protégé et vigilant, nous cherchons à préparer la société dans l'éventualité d'une attaque »
Sabrina Quinet, Head of IT chez Moteurs Baudouin

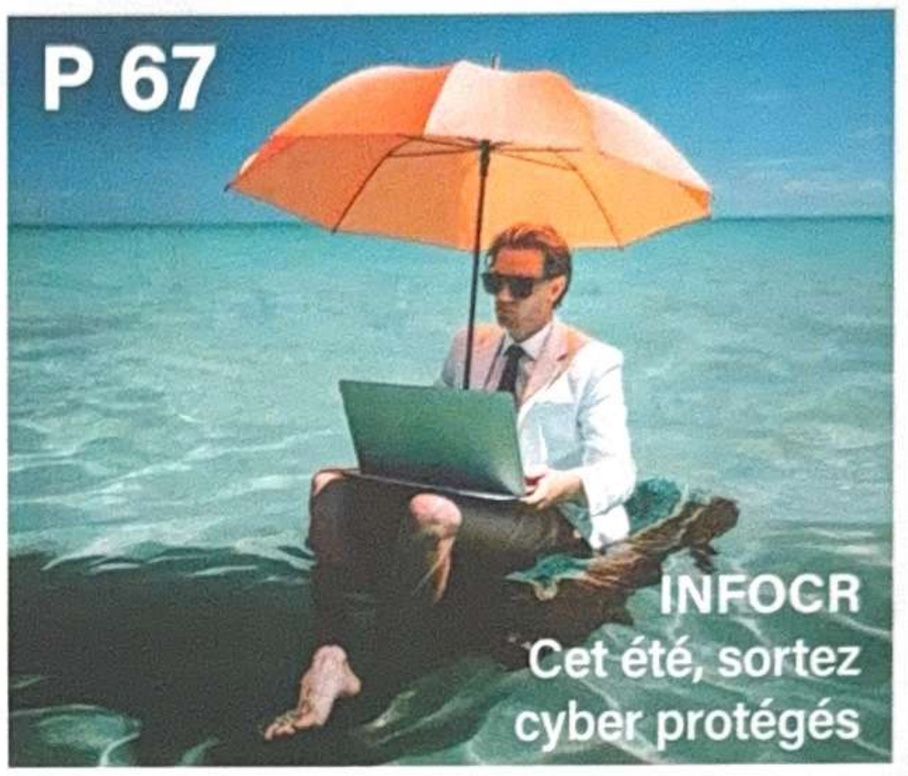
L 14614 - 238 - F: 8,50 € - RD



P 15
DOSSIER TOP TECH 2025
Les entreprises en action



P 47 RETEX
Rencontre avec Sabrina Quinet, Head of IT chez Moteurs Baudouin



P 67
INFOCR
Cet été, sortez cyber protégés

Sensibilisation

La DSI de Moteurs Baudouin accélère sur la résilience

Sabrina Quinet, Head of IT chez Moteurs Baudouin, basée à Cassis, anticipe la perte de fonctions critiques et fait évoluer la sensibilisation des équipes aux défis de la cyber-résilience.

L'Informaticien : Quelle est la genèse de votre entreprise et votre rôle dans l'organisation ?
Sabrina Quinet : Fondée en 1918, Baudouin est une entreprise française spécialisée dans la conception et la fabrication de moteurs marins diesel, qui a diversifié son expertise, grâce au rachat en 2009 par la société chinoise Weichai Power. Aujourd'hui, avec un rayonnement dans plus de 100 pays, nous proposons des solutions énergétiques complètes, tant pour les besoins principaux que pour les systèmes de secours alimentant notamment hôpitaux, stades ou datacenters. Forte de 220 salariés, l'entreprise est notamment dotée d'un centre de Recherche et Développement et d'une usine à Cassis. En tant que Head of IT, je pilote une équipe de sept personnes avec un rôle centralisateur et temporisateur visant à réussir davantage de projets avec un vrai retour sur investissement, des projets utilisés au quotidien, car plus réfléchis, mûris au sein d'ateliers avec les experts et dotés d'une gouvernance.

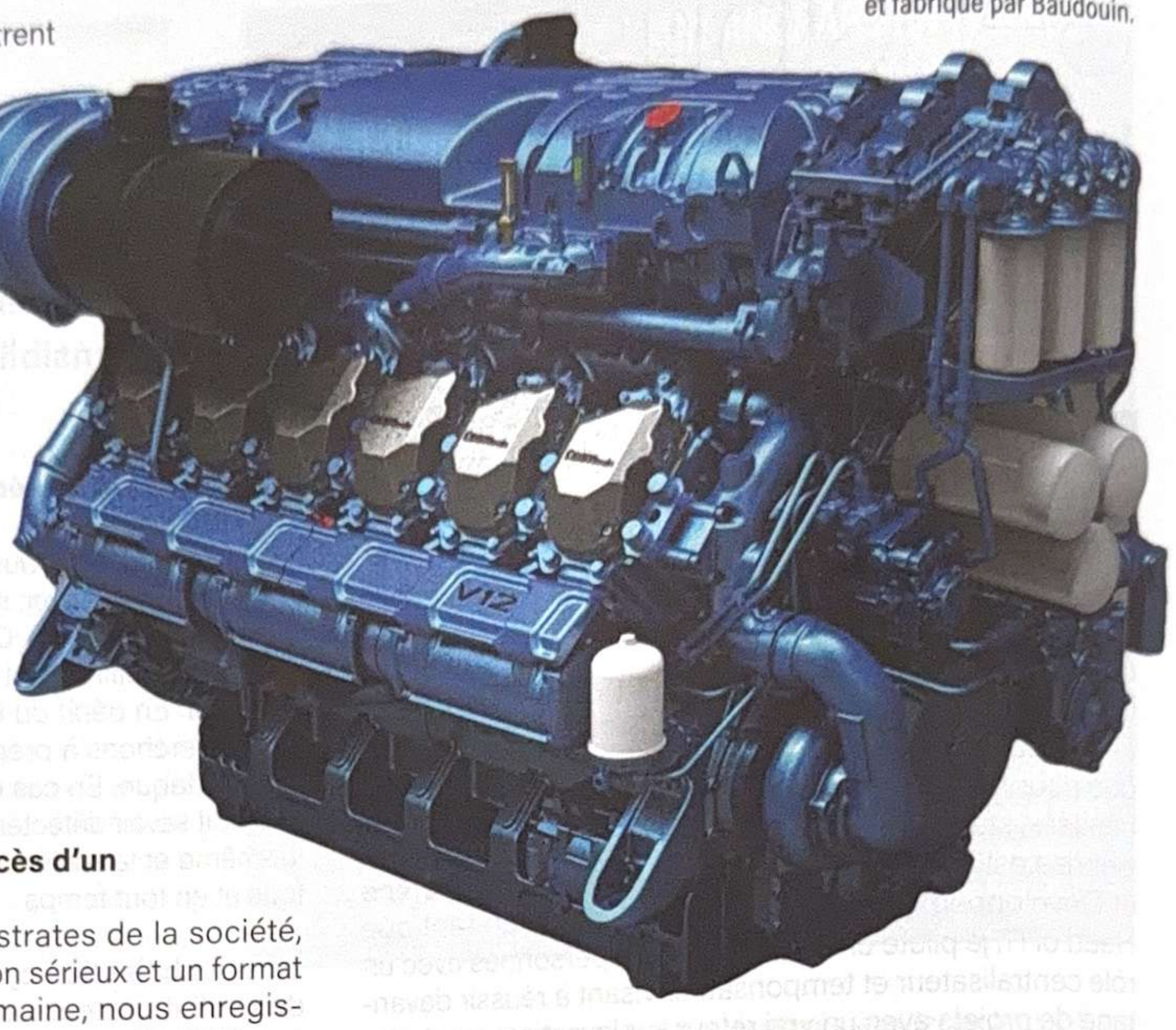
Quelles priorités recensez-vous en termes de cybersécurité ? De nouveaux risques ont-ils été identifiés par les métiers ou le Comex ?
Le fil rouge de la DSI, concernant les enjeux cyber, consiste à protéger l'ensemble de la supply chain, les moyens informatiques de la société et ceux de ses sous-traitants interconnectés. Une fois le moteur fourni, chaque client est fidélisé au travers de services de maintenance, de renouvellement d'équipements et de pièces détachées. Une chaîne d'acteurs de toutes tailles intervient dans nos activités, des fournisseurs aux clients. Nous évaluons les risques en fonction de la typologie de nos partenaires. Ce contact pérenne exige une cyber-vigilance constante, particulièrement en matière d'infrastructure IT, de réseau, et de protection des postes de travail des utilisateurs.

Quels aspects de sécurité renforcez-vous à présent ?
Ces derniers mois, nous avons mis l'accent sur la sécurité de l'infrastructure avec notre partenaire Customer Business Management (CBM). Ce projet étant opérationnel, nous engageons maintenant la cyber-résilience, déjà présentée en CoDir. En dépit du fait d'être bien protégé et vigilant, nous cherchons à préparer la société dans l'éventualité d'une attaque. En cas de crise cyber, chaque collaborateur doit savoir détecter, informer et comment se protéger lui-même et la société. La cybersécurité reste l'affaire de tous et en tout temps.

La sensibilisation cyber des collaborateurs progresse-t-elle ?
Sur ce point, nous avions une solution existante traditionnelle qui devenait obsolète.

Sabrina Quinet, Head of IT chez Moteurs Baudouin

Un type de moteur marine conçu et fabriqué par Baudouin.



Les résultats d'analyse 2024 montrent un intérêt décroissant pour les formations et une augmentation du taux de clics imprudents. Quelques chiffres nous ont alertés en particulier : 61% d'échec aux simulations de phishing et un taux de clic moyen de 24%, avec un pic à 40% sur des sujets de messages plus personnels.

Après un benchmark des solutions existant sur le marché et plusieurs PoC, nous avons finalement préféré une solution pré-configurée, montrant un engagement dans le renouvellement des cours et des contenus.

Comment évaluez-vous le succès d'un chatbot de cyber-training ?
L'outil doit parler à toutes les strates de la société, sans cajoler le salarié, avec un ton sérieux et un format ludique. Déployé il y a une semaine, nous enregistrons un taux de participation aux cours de 53%, un taux de clic de 10% sur les premières simulations et un taux de signalement de 36%. C'est un lancement prometteur.

Quelles fonctionnalités font la différence ?
La solution que nous avons choisie est intégrée à notre chat de communication interne et propose des formats courts de 3 à 5 minutes. Le chatbot sollicite, relance, et fait valider les connaissances à l'aide de quizz. Il permet de comparer sa progression à celle des collègues ; l'utilisateur suit sa propre progression et celle de ses collaborateurs sur son tableau de bord. Cela nous permet de récompenser ceux qui jouent le jeu, d'effectuer un suivi fin sur ceux qui ont plus de difficultés, et d'impliquer facilement la RH ou le management dans l'avancée de chaque équipe. Une nouvelle fonctionnalité de bannières intelligentes, boostées à l'IA, sécurise les boîtes mail en proposant une première détection de risques.

Quels enseignements tirez-vous des projets cyber menés depuis quatre ans ?
La sensibilisation est un sujet certes présent mais vite oublié. Notre mission est d'animer ce sujet en fil rouge avec les équipes, en présentiel ou à distance, de montrer des exemples dans notre industrie, de nous projeter sur les conséquences potentielles d'un arrêt de production ou d'une fuite de données.

En cyber-sécurité comme dans tout projet, il est important de s'assurer que la population cible adhère au changement et que les solutions appuient la volonté d'innovation de l'entreprise.

Comment faire progresser la cyber résilience de son organisation ?
En travaillant sur la gestion de crise avec les départements, la cyber-résilience va progresser. Il s'agit de bien identifier les risques, la perte de fonctions critiques et comment assurer la continuité de service, la protection de nos partenaires et notre image de marque.

Les défis de la résilience sont nombreux avec des budgets en tension et des solutions du marché déjà nombreuses. Les critères de sélection doivent être bien déterminés, les benchmarks et PoC s'avèrent particulièrement utiles. En termes de sensibilisation, il faut reconquérir l'intérêt des employés, améliorer le taux de participation et de réussite des formations pour gagner en résilience.

L'intelligence artificielle exige-t-elle de nouvelles précautions ?
Bien sûr. L'IA est aujourd'hui un sujet phare. Elle met à portée de tous un réel accélérateur de business, comme a pu l'être l'automatisation par processus robotisés il y a quelques années.

Nous devons prendre en compte ces évolutions et ajuster les règles de sécurité, le cloisonnement des données, et le durcissement des droits d'accès. Nous constatons une réelle envie en interne d'explorer l'IA, qu'elle soit générative ou non et un début d'utilisation globalisée. Nous étudions en ce moment les cas d'usage pertinents et travaillons à mettre en place une vraie gouvernance. □

Propos recueillis par Olivier Bouzereau