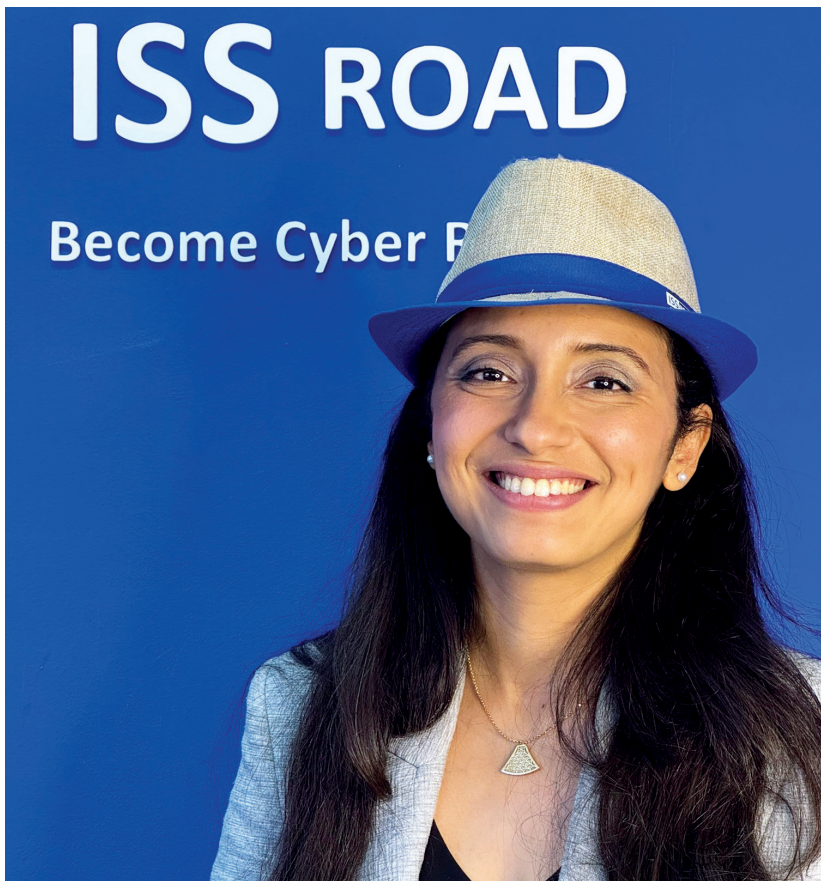
ISSROAD

«En matière de cybersécurité, chaque maillon compte»

Dans un contexte marqué par la montée des cybermenaces, ISSROAD ambitionne de démocratiser la cybersécurité auprès des PME marocaines.
La startup défend une approche globale qui combine formation, gouvernance IT et protection des données.
Entretien avec la fondatrice et CEO, Salwa Harif.

Propos recueillis par Ibtissam **Z.**



Finances News Hebdo : ***Pouvez-vous nous présenter ISSROAD et les solutions vous proposez ?***

Salwa Harif : 95% des cyberattaques exploitent une erreur humaine ou une faille connue. Et pourtant, des dizaines de dirigeants de PME marocaines pensent encore que l'antivirus suffit.
C'est en travaillant pendant plusieurs années avec des grands comptes, dans des environnements hautement sécurisés, que j'ai vu la différence flagrante entre les moyens déployés par les grandes structures… et la détresse des petites entreprises face à leur besoin en IT. J'ai vu, d'un côté, des équipes formées et outillées et, de l'autre côté, des patrons de PME qui galèrent avec un freelance, un technicien débordé, ou un cousin «bon en informatique».
La genèse d'ISSROAD part donc d'une indignation : pourquoi la sécurité, la méthode et la gouvernance IT seraient-elles un luxe réservé aux grands ?
ISSROAD s'est donc bâti sur l'idée que les grandes entreprises ne sont pas les seules à nécessiter une gouvernance de l'IT efficace, et qu'il est primordial pour les PME d'être correctement épaulées pour leur besoin en IT.
Les dirigeants de PME ne sont pas tous suffisamment à l'aise avec le numérique pour prendre des décisions éclairées. Quant aux techniciens en interne, lorsqu'ils existent, ils sont souvent isolés et/ou débordés.
C'est pour éviter cette vulnérabilité à la fois stratégique et opérationnelle qu'est née ISSROAD. Nous sommes un MSP (Managed Services Provider) nouvelle génération, avec un ADN cyber dès la conception. Cela veut dire que nos offres ne séparent pas l'IT de la cybersécurité. Du coup, chaque service que nous proposons, de la maintenance à la supervision en passant par le support utilisateur, est pensé pour sécuriser et responsabiliser.
Notre approche se distingue par trois piliers :
• 3 offres packagées adaptées à la maturité numérique des clients (de l'émergence à la conformité ISO/RGPD).
• Pas de cybersécurité possible sans formation et sensibilisation des agents.
• Suivis réguliers avec rapports, comités de pilotage, monitoring des vulnérabilités, et conseils stratégiques.
Aujourd'hui, ISSROAD veut devenir ce que le DSI externalisé devrait être, fiable et à l'écoute, au carrefour du technique et du stratégique. Car pour nous, la cybersécurité n'est pas une technologie, mais une base de développement tout comme une hygiène de vie au quotidien.

> **Le vrai enjeu aujourd'hui, c'est que l'écosystème du financement au Maroc n'est pas encore aligné avec les spécificités de la tech et de la cybersécurité.**

F.N.H. : ***Dans un contexte où le Maroc s'apprête à accueillir des événements majeurs comme la CAN 2025 et le Mondial 2030, quels sont les enjeux majeurs en matière de cybersécurité pour le Royaume ?***

S. H. : Un grand événement attire les foules… et les cyberattaques. La CAN 2025 et le Mondial 2030 placeront le Maroc sous les projecteurs du monde entier, avec une exposition numérique sans précédent. Cette visibilité accrue augmente mécaniquement les risques cyber, comme attaques par déni de service (DDoS), ransomwares, défigurations de sites officiels, fuites de données sensibles, ou encore campagnes de désinformation sur les réseaux sociaux. Ce n'est pas de la théorie. En effet, la France, en amont des JO 2024, a recensé plus de 140 cyber incidents majeurs en quelques semaines. Le Maroc ne doit pas attendre l'urgence pour agir. L'enjeu dépasse la simple protection technique. Il s'agit de garantir la continuité des services publics, la sécurité des données des citoyens, la fiabilité des infrastructures critiques (transport, télécoms, santé), mais aussi la confiance des partenaires économiques et institutionnels.
Cela exige une approche coordonnée avec un renforcement des capacités de détection, implication des acteurs publics et privés de la cybersécurité dans la chaîne de sécurité, exercices de simulation et gouvernance entre agences, ministères et acteurs privés. En matière de cybersécurité, chaque maillon compte. Le Maroc a aujourd'hui l'opportunité de faire de ces grands événements un catalyseur pour bâtir une résilience numérique durable et souveraine.

▶ 95% des cyberattaques exploitent une erreur humaine ou une faille connue.

F.N.H. : ***Le développement d'une offre locale solide en cybersécurité est essentiel pour la souveraineté numérique du pays. Comment percevez-vous l'évolution de l'écosystème entrepreneurial marocain dans ce domaine stratégique ?***

S. H. : On ne peut pas parler de souveraineté numérique si l'on ne crée pas les conditions de son exercice. Aujourd'hui, l'écosystème marocain de la cybersécurité est en pleine ébullition. Ainsi, des profils qualifiés émergent, des startups ambitieuses voient le jour, et l'intérêt pour la sécurité numérique se généralise. Mais cette dynamique masque une réalité plus contrastée.

L'offre locale reste très concentrée sur les services, avec peu de produits technologiques développés sur place. Selon Tracxn, à peine une dizaine d'acteurs marocains proposent aujourd'hui des solutions de cybersécurité innovantes, conçues et développées localement.

Le frein principal reste l'accès au marché. En effet, les grands donneurs d'ordre hésitent encore à faire confiance à des technologies locales, et les TPME n'ont pas les moyens d'y accéder. Résultat : beaucoup de startups n'ont d'autre choix que de lever des fonds à l'étranger, de viser directement l'export ou, dans le pire des cas, de disparaître.

D'ailleurs, nous lançons en septembre une solution d'automatisation de la formation et de la sensibilisation à la cybersécurité, pensée pour les TPME. Ce projet est développé en France, où nous avons trouvé un environnement propice à l'innovation et un marché réceptif. Nous espérons le réimporter au Maroc, mais cela illustre l'urgence de structurer un véritable écosystème national.

Le potentiel est là, à savoir les talents, les idées et les initiatives. Ce qui manque, c'est une vision commune, un environnement où l'on peut se faire confiance et unir nos forces, une stratégie claire et un cadre incitatif pour faire émerger des champions locaux.

F.N.H. : ***Quel rôle joue le financement dans le développement de votre activité et dans l'accompagnement des entreprises marocaines vers une meilleure cyber-résilience ?***

S. H. : Le financement est un levier stratégique pour passer de l'idée à l'impact. Dans un secteur comme la cybersécurité, l'innovation est coûteuse et les cycles de vente sont longs; l'accès à un financement adapté est une condition de survie.

Nous lançons en septembre une solution d'automatisation de la formation et de la sensibilisation à la cybersécurité, pensée pour les TPME.

Nous avons financé nos premières phases de développement sur fonds propres, avec une logique de croissance organique. Mais dès que l'on parle de solutions scalables, comme notre projet d'automatisation de la sensibilisation ou le service MSP nouvelle génération, le besoin de financement devient structurant.

Le vrai enjeu, aujourd'hui, c'est que l'écosystème du financement au Maroc n'est pas encore aligné avec les spécificités de la tech et de la cybersécurité. Les investisseurs privés restent prudents, faute de compréhension du marché. Les mécanismes publics de soutien à l'innovation sont trop généralistes, parfois trop complexes à mobiliser pour des startups en phase critique.

Côté entreprises marocaines, notamment les TPME, l'équation est inversée : elles ont besoin d'être protégées, mais manquent souvent de moyens pour investir dans leur sécurité numérique. C'est pourquoi nous plaidons pour des mécanismes de cofinancement public-privé, des incitations fiscales ou encore des programmes mutualisés sectoriels. La cyber-résilience n'est pas un coût, c'est une assurance pour la continuité économique.

F.N.H. : ***Quelles sont vos ambitions pour ISSROAD à moyen et long terme ? Quels leviers souhaitez-vous activer pour renforcer votre positionnement dans l'écosystème numérique ?***

S. H. : À moyen terme, notre ambition est de faire d'ISSROAD une référence nationale pour les TPME marocaines en matière d'infogérance et de cybersécurité. Nous voulons être identifiés non seulement comme un prestataire technique fiable, mais comme un véritable partenaire stratégique pour les dirigeants de PME. Cela passera par une couverture accrue du territoire, une montée en puissance de nos équipes, et le lancement progressif de plateformes technologiques innovantes, structurées autour des besoins et problématiques des TPME.

À long terme, nous souhaitons positionner ISSROAD comme une référence régionale en cybersécurité, mêlant expertise technique, formation, et conseil stratégique. Nous voulons faire partie des acteurs qui influencent la transformation numérique des PME dans les pays émergents. Pour atteindre ces objectifs, nous comptons activer plusieurs leviers stratégiques :

- Développement technologique et R&D : avec des outils intégrés et automatisés;
- Partenariats : avec des réseaux de TPME, des intégrateurs, des clusters régionaux;
- Communication ciblée : pour éduquer le marché, créer la confiance et affirmer notre positionnement;
- Montée en compétence interne: avec le recrutement progressif de profils clés, notamment en production, cybersécurité et relation client. ◆