European Bank
for Reconstruction and Development

EBRD

Soutien aux fournisseurs de services de cybersécurité au Maroc

Dans le paysage numérique en évolution rapide d'aujourd'hui, les entreprises et les particuliers du monde entier font face à une gamme de risques de cybersécurité évolutifs. Cela est particulièrement critique au Maroc, un pays avec une longue histoire de cyberattaques, où les PME représentent plus de 90 % de l'économie. La capacité des entreprises, en particulier des PME, à répondre à ces menaces dépend en grande partie de la disponibilité de services de cybersécurité de qualité sur le marché local.

Ainsi, la Banque Européenne pour la Reconstruction et le Développement (BERD) dirige un projet visant à contribuer a l'amélioration du paysage de la cybersécurité au Maroc, en développant et en codifiant des normes pour les services de cybersécurité clés. Développé en collaboration avec CREST, une organisation internationale à but non lucratif et leader mondial dans la certification des normes des fournisseurs de services de cybersécurité, ce projet est conçu pour aider les fournisseurs de cybersécurité des PME au Maroc en les évaluant par rapport aux meilleures pratiques internationales et en leur offrant un soutien pour s'améliorer, contribuant ainsi à leur compétitivité et à leur capacité dans quatre disciplines cruciales de l'industrie :

- Tests de pénétration : Le but des exigences d'accréditation des tests de pénétration est d'établir un cadre clair et structuré que les organisations doivent suivre pour obtenir l'accréditation en matière de tests de pénétration. Ces exigences garantissent que les entreprises démontrent une qualité, une sécurité et un professionnalisme constants dans leurs services de tests de pénétration.
- Centre des opérations de sécurité (SOC) en tant que service : Les exigences d'accréditation des réponses aux incidents de CREST fournissent un cadre structuré et rigoureux que les organisations doivent suivre pour obtenir l'accréditation dans le domaine de la réponse aux incidents. Ces exigences sont conçues pour garantir que les organisations démontrent systématiquement des niveaux élevés d'expertise, de professionnalisme et de respect des meilleures pratiques dans la gestion des incidents cybernétiques.
- Réponse aux incidents : Les exigences d'accréditation des réponses aux incidents de CREST définissent un cadre structuré et rigoureux que les organisations doivent suivre pour obtenir l'accréditation dans le domaine de la réponse aux incidents. Ces exigences sont conçues pour garantir que les organisations démontrent systématiquement des niveaux élevés d'expertise, de professionnalisme et de respect des meilleures pratiques dans la gestion des incidents cybernétiques.
- Architecture de sécurité : L'accréditation de l'architecture de sécurité décrit une approche globale pour développer une architecture de sécurité pour un client. Cette norme garantit que tous les aspects du processus d'évaluation - des exigences commerciales de haut niveau aux plans de mise en œuvre détaillés et à la gestion opérationnelle - sont soigneusement planifiés, exécutés et rapportés.

Pour chacune de ces quatre disciplines, les fournisseurs de cybersécurité marocains peuvent remplir une auto-évaluation gratuite et pratique via un portail en ligne. Les réponses à chaque évaluation seront validées par CREST, y compris des questions de suivi pour garantir la fidélité. Les entreprises participantes peuvent ensuite recevoir soit la certification CREST Pathway Plus - une certification internationale démontrant leur compétence - soit une analyse des lacunes, décrivant clairement les étapes qu'elles doivent suivre pour être prêtes à recevoir la certification.

En s'appuyant sur les lacunes identifiées, les fournisseurs de services participants peuvent également devenir candidats à un programme pilote d'assistance technique ultérieur, pour les aider à combler les lacunes identifiées avec les outils, la main-d'œuvre et les processus appropriés. Ainsi, ce projet représente une première étape essentielle dans la culture, la mesure et l'amélioration des capacités

des fournisseurs de cybersécurité, garantissant qu'ils peuvent protéger efficacement les entreprises au Maroc et dans le monde contre les menaces cybernétiques.

Quelles sont les étapes suivantes si ma candidature est retenue ?

- Si votre candidature est retenue, CREST contactera progressivement les entreprises sélectionnées et enverra directement aux entreprises un formulaire d'auto-évaluation.
- CREST créera un compte pour l'entreprise.
- L'entreprise sera invitée à effectuer une auto-évaluation via la plateforme de CREST.
- Toutes les entreprises ayant réussi l'auto-évaluation recevront un rapport détaillé d'analyse des écarts, fournissant des informations claires sur leur maturité actuelle en cybersécurité, leurs points forts et les domaines nécessitant des améliorations.
- Les entreprises éligibles nécessitant un développement supplémentaire auront, à un stade ultérieur, l'opportunité de travailler en étroite collaboration avec l'équipe de financement et de développement des PME de la BERD pour recevoir un soutien consultatif personnalisé identifié dans l'analyse des écarts.
- Les entreprises démontrant une maturité suffisante peuvent obtenir un accès entièrement financé au statut Pathway+ de CREST. Cette reconnaissance permet à votre organisation de mettre en avant ses progrès vers l'accréditation CREST en utilisant le logo Pathway+ pendant un an.
  Plus d'informations sur l'adhésion complète et l'accréditation peuvent être trouvées ici.