Communiqué de presse

Digora lance une offre de cyber sécurité en partenariat avec EBRC

***Strasbourg, le 22 juin 2018* – Digora, expert des infrastructures IT et des bases de données, et spécialiste des services managés pour les directions informatiques, annonce le lancement d'une offre de cyber sécurité développée avec son partenaire EBRC, acteur européen spécialiste de la gestion et de la protection de l'information et des infrastructures sensibles. Cette nouvelle offre est destinée à tester et protéger les systèmes d'information des entreprises.**

« *Pour Digora, expert des infrastructures IT et des bases de données depuis plus de 20 ans, la sécurité des données fait partie de nos préoccupations quotidiennes. Mais pour aller plus loin et aider nos clients à mieux identifier et maîtriser les risques de sécurité sur l'ensemble de leurs systèmes d'information, en tout indépendance, nous avons choisi de nous appuyer sur un des meilleurs spécialistes européens.* »

Didier Lavoine
Directeur Technique, Développement et Innovation du Groupe Digora

« *La prévention et la gestion des risques, l'assistance aux traitements d'incidents et la continuité d'activité sont inscrites dans les gènes d'EBRC. Notre expertise s'exprime dans une offre de services intégrée et certifiée (ISO 27001, ISO 20000, ISO22301, PCI DSS, Tier IV, solutions SIEM…) qui offre des garanties probantes à nos clients internationaux. Avec des centaines de tests d'intrusion réalisées à la fois sur nos infrastructures et pour nos clients, un pool de consultants experts, un SOC (Security Operations Centre) et un CERT (Cyber Emergency Response Team), nous plaçons la cyber sécurité au cœur du business.* »

Philippe Dann
Directeur de l'activité Conseil "CyberRésilience" de EBRC

Mesurer la sécurité d'une infrastructure

La nouvelle offre cyber sécurité de Digora sécurise les systèmes d'informations dans leur ensemble, de la base de données aux applications (API), en réalisant des tests d'intrusion et des scans de vulnérabilité. En simulant une attaque, Digora est ainsi capable de mesurer la sécurité d'une infrastructure, en détectant les failles latentes et en les exploitant. Les rapports techniques et managériaux remis en fin de mission permettent de mettre en place des solutions concrètes pour contrer ces menaces.

Les tests d'intrusion et scans de vulnérabilité sont réalisés par EBRC (European Business Reliance Centre), spécialiste européen de la gestion des applications informatiques et unique acteur au monde à opérer trois Datas Centres certifiés Tier IV - plus haut niveau de disponibilité, de sécurité et d'intégrité du marché.

L'offre cyber sécurité de Digora s'articule autour de trois modules de test et un module de recherche d'informations :

Scans de vulnérabilités depuis les réseaux internes : Ce module a pour objectif de tester les serveurs et machines connectés aux réseaux internes et d'identifier les vulnérabilités de ces services (configuration inadaptée, patches de sécurité manquants, etc.).

Test d'intrusion en boîte noire (Blackbox Pentest) : Le test d'intrusion en boîte noire est réalisé sans connaissance préalable du système d'information ou de son architecture. Il identifie les systèmes exposés à Internet, détecte les failles de sécurité et les degrés d'intrusion possibles en simulant une attaque réaliste.

Test d'intrusion en boîte grise (Greybox Pentest) : Le test d'intrusion en boîte grise est réalisé sur les applications web et les serveurs associés en se connectant au système d'information avec un compte utilisateur valide. Le testeur vérifie le fonctionnement de l'application notamment lors de l'authentification et de la connexion de session pour tenter de s'octroyer des privilèges d'accès ou d'accéder à des données dont l'accès est restreint. Des tests d'injection de paramètres permettent d'identifier les vulnérabilités telles que les injections XSS ou SQL.

Recherche d'informations : ce module d'investigation est intégré dans la phase initiale des tests d'intrusion en boîte noire et boîte grise. Il permet d'identifier les informations divulguées, volontairement ou non, comme : les adresses IP, les logins, mots de passe, numéros de téléphone, etc.

Tarifs au forfait

- Scans de vulnérabilité : à partir de 2 500,00 euros HT pour moins de 50 adresses IP.
- Test d'intrusion en boîte noire : à partir de 2 700,00 euros HT pour une URL.
- Test d'intrusion en boîte grise : à partir de 4 500,00 euros HT pour une URL.

En savoir plus sur l'offre Cyber Sécurité de Digora.

Contacts presse : AMALTHEA

Célia Ringeval – Tél. : 01 76 21 67 55 – Mail : cringeval@amalthea.fr
Laurent Meggs – Tél : 01 76 21 67 54 – Mail : lmeggs@amalthea.fr

À propos de Digora : @DigoraBlog

Acteur reconnu depuis plus de 20 ans, DIGORA est un expert des infrastructures IT et des bases de données tant pour leurs mises en œuvre, que leurs optimisations et leurs administrations au quotidien.

Digora propose aujourd'hui aux entreprises et organisations une gamme de services qui inclut les offres suivantes : Ingénierie & Conseil, Support Technologique, Maintien en Condition Opérationnelle, Courtage agile et évolutif (Cloud Broker), Sécurité et Gouvernance.

Créée en 1997 et ayant son siège à Strasbourg, Digora est un fournisseur d'Energie Numérique. Présente en France (Bordeaux, Lille, Lyon, Paris, Rennes, Strasbourg et Toulouse), au Luxembourg et au Maroc, le groupe Digora emploie plus de 130 collaborateurs pour un chiffre d'affaires de près de 33 millions d'euros.

Le capital de Digora est détenu majoritairement par ses dirigeants, et minoritairement par EBRC, acteur européen spécialiste de la gestion des applications informatiques critiques et de la sécurité informatique.

Digora compte 550 clients actifs, grands comptes et ETI de tous secteurs d'activités dont : BANDAI NAMCO, BNP Paribas, Compagnie des Alpes, le Conseil Régional d'Aquitaine, Engie, le Groupe ÏDKIDS, Lacoste, Ramsay - Générale de Santé, Maincare, Maisons du Monde, XPO, Poclain Hydraulics, Sanofi, Toyota, l'UGAP.

Digora en bref : Votre Transformation Numérique en toute sérénité.