Fiche technique

DORA : comment Specops vous aide à répondre aux exigences de conformité

Qu'est-ce que DORA ? Le Digital Operational Resilience Act (Règlement UE 2022/2554) est un cadre européen obligatoire en matière de cybersécurité.

Que couvre DORA ? DORA met l'accent sur la gestion des risques liés aux TIC (technologies de l'information et de la communication), la gestion des identités et des accès, la détection et le signalement des incidents, les tests de résilience opérationnelle, la gestion des risques liés aux tiers ainsi que le partage d'informations sur les cybermenaces..

Qui est concerné par DORA ? Cette réglementation concerne les banques, compagnies d'assurance, sociétés d'investissement, établissements de paiement et de monnaie électronique, prestataires de services sur crypto-actifs ainsi que les fournisseurs tiers critiques de services TIC opérant dans le secteur financier européen ou lui fournissant des services.

Existe-t-il des sanctions en cas de non-conformité ? Oui. Les entités financières s'exposent à des amendes pouvant atteindre 2 % de leur chiffre d'affaires annuel mondial total, ou jusqu'à 1 % de leur chiffre d'affaires quotidien mondial moyen. Les personnes responsables de manquements à laconformité s'exposent à des sanctions pouvant aller jusqu'à 1 million d'euros.

DORA est-il équivalent à NIS2 ? Non. La directive NIS2 s'applique de manière générale à l'ensemble des secteurs critiques, tandis que DORA est spécifiquement conçu pour les services financiers et prévaut sur NIS2 pour les entités financières concernées. Les deux réglementations poursuivent des objectifs communs en matière de cyberrésilience, mais DORA impose des exigences plus strictes et plus prescriptives au secteur financier.

Pourquoi choisir Specops pour DORA ?

Exigences DORA	Comment Specops facilite la mise en conformité
Visibilité des mots de passe ***DORA - Article 8 : Identification*** Les entités financières doivent identifier et évaluer les risques liés aux TIC, y compris les vulnérabilités associées aux identifiants utilisateurs et aux droits d'accès au sein de leur environnement informatique.	**Specops Password Auditor** (outil gratuit) Effectue une analyse en lecture seule de votre environnement AD afin d'identifier les mots de passe compromis, vides, obsolètes ou n'expirant jamais. Génère des rapports exportables pour les besoins de conformité et d'audit.
Identifiants compromis ***DORA - Article 9(4)(d) : Protection et prévention*** Les entités financières doivent mettre en œuvre des politiques et des procédures garantissant des mécanismes d'authentification robustes, notamment des contrôles permettant de s'assurer que les identifiants utilisés pour accéder aux systèmes TIC ne sont ni compromis ni faibles.	**Specops Password Policy avec Breached Password Protection** La plupart des outils bloquent uniquement les mots de passe compromis lors d'un changement ou d'une réinitialisation. Specops analyse en continu votre Active Directory et mpêche l'utilisation de mots de passe présents dans notre base de données en constante évolution, qui contient plus de 6 milliards de mots de passe compromis.

Exigence DORA	Comment Specops facilite la mise en conformité
Authentification multifactorielle (MFA) renforcée ***DORA - Article 9(4)(d) : Protection et prévention*** Les entités financières doivent mettre en œuvre des politiques et des procédures garantissant des mécanismes d'authentification robustes, notamment pour les accès distants au réseau, les accès à privilèges et l'accès aux systèmes supportant des fonctions critiques.	**Specops Secure Access** Ajoute une authentification multifacteur résistante au phishing pour les connexions Windows, RDP et VPN. Prend en charge le Single Sign-On (SSO) pour les applications SaaS via OIDC et SAML, et s'intègre aux plateformes SIEM, SOC et d'analyse de sécurité.
Vérification par le Service Desk ***DORA - Articles 9(4)(c) et 9(4)(d) : Protection et prévention*** Les contrôles des droits d'accès et l'authentification forte doivent également s'appliquer aux processus opérationnels, notamment au Service Desk, où une défaillance de la vérification d'identité constitue un risque TIC direct.	**Specops Secure Service Desk** Les agents vérifient l'identité de l'appelant via l'authentification multifactorielle (plus de 20 méthodes) avant toute action sur un compte. Chaque interaction est enregistrée dans un journal d'audit complet. S'intègre aux solutions ITSM ainsi qu'aux plateformes SIEM, SOC et d'analyse de sécurité.
Vérification d'identité à haut niveau d'assurance ***DORA – Articles 9(4)(c) et 9(4)(d) : Protection et prévention*** Les exigences en matière d'authentification forte s'appliquent également à la vérification d'identité permettant l'accès aux systèmes TIC, notamment dans le cadre d'opérations à haut risque telles que la récupération de compte ou la restauration d'accès privilégiés.	**Specops Verified ID** Vérifie les pièces d'identité officielles et réalise un contrôle biométrique de présence réelle afin de fournir le plus haut niveau d'assurance en matière de vérification d'identité.
Réinitialisation sécurisée des mots de passe ***DORA – Articles 9(4)(c) et 9(4)(d) : Protection et prévention*** Des contrôles d'accès et les exigences d'authentification forte doivent être appliqués tout au long du cycle de vie de l'identité, y compris lors de la réinitialisation des mots de passe, qui ne doit pas constituer un maillon plus faible que l'authentification principale.	**Specops uReset** Solution de réinitialisation de mot de passe en libre-service protégée par MFA. Les utilisateurs peuvent mettre à jour en toute sécurité leurs identifiants mis en cache localement, quel que soit leur emplacement, leur appareil ou leur navigateur, avec ou sans connexion VPN. S'intègre aux plateformes SIEM, SOC et d'analyse de sécurité.

Contactez votre interlocuteur Specops ou cliquez ici pour planifier un appel de cadrage.

Planifier un rendez-vous

SPECOPS
AN OUTPOST24 COMPANY