AKKA

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Attestation de conformité à la Directive sur la sécurité des réseaux et des systèmes d'information 2 (NIS2)

Introduction

La Directive (UE) 2022/2555 — Directive sur la sécurité des réseaux et des systèmes d'information 2 (NIS2) — est la principale législation de l'Union européenne en matière de cybersécurité pour les entités essentielles et importantes opérant dans l'UE. Elle abroge et renforce substantiellement la Directive NIS initiale (2016/1148), en élargissant considérablement son champ d'application, en relevant les exigences en matière de sécurité et en resserrant les obligations de notification des incidents. Les États membres devaient transposer NIS2 en droit national au plus tard le 17 octobre 2024.

NIS2 s'applique aux organisations opérant dans des secteurs désignés comme essentiels ou importants, ainsi qu'aux fournisseurs d'infrastructures et de services numériques — notamment les fournisseurs de services d'informatique en nuage, les prestataires de services gérés et les fournisseurs de places de marché en ligne, de moteurs de recherche et de plateformes de réseaux sociaux — qui opèrent dans l'UE ou y fournissent des services. Akka, en tant que fournisseur d'une plateforme SaaS de microservices réactifs et de systèmes distribués au service de clients entreprises dans l'UE, s'aligne sur les obligations applicables aux fournisseurs de services numériques et aux prestataires de services gérés au titre de NIS2.

La présente attestation confirme l'alignement d'Akka avec les exigences de sécurité et de gouvernance de NIS2 à la date indiquée ci-dessous. Le Système de Management de la Sécurité de l'Information (SMSI) d'Akka, aligné sur la norme ISO 27001, et son attestation SOC 2 Type II fournissent l'infrastructure de gouvernance sous-tendant cette posture de conformité.

AKKA

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Périmètre

La présente attestation couvre les pratiques de gestion des risques de cybersécurité, de notification des incidents et de sécurité de la chaîne d'approvisionnement d'Akka Technologies, Inc. (« Akka ») telles qu'elles se rapportent à NIS2. Les systèmes et activités entrant dans le périmètre comprennent :

Réseaux et systèmes d'information : la plateforme SaaS d'Akka, l'infrastructure cloud sous-jacente, les systèmes informatiques internes de l'entreprise et les environnements de développement.

Gestion des incidents : détection, analyse, confinement et notification des incidents de cybersécurité affectant les services d'Akka.

Sécurité de la chaîne d'approvisionnement : évaluation et gestion des fournisseurs tiers et sous-traitants ayant accès aux systèmes d'Akka ou aux données des clients.

Continuité des activités : capacités de sauvegarde, de reprise après sinistre et de résilience pour la plateforme et les opérations d'Akka.

Situation de conformité

Akka maintient 17 contrôles spécifiquement mappés à NIS2 au sein de son Système de Management de la Sécurité de l'Information (SMSI). Les 17 contrôles sont au statut Mis en œuvre. La répartition des risques au sein du dispositif de contrôle est la suivante :

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

- 5 contrôles cotés Risque faible
- 12 contrôles cotés Risque moyen
- 0 contrôle coté Risque élevé

La conformité globale à NIS2 est évaluée comme Conforme. Les cotations de risque moyen reflètent la complexité inhérente à l'exploitation d'une plateforme SaaS distribuée sur une infrastructure multi-cloud, et Akka a mis en œuvre des contrôles compensatoires et de détection dans chaque cas. Le SMSI d'Akka est aligné sur la norme ISO/IEC 27001 et s'appuie sur une attestation SOC 2 Type II délivrée par un auditeur indépendant, fournissant une assurance externe sur l'efficacité des contrôles de sécurité d'Akka.

Principaux contrôles mis en œuvre

Gestion des risques de cybersécurité

Akka exploite un programme formel et documenté de gestion des risques liés à la sécurité de l'information, aligné sur les principes de la norme ISO/IEC 27001. Les risques pesant sur les réseaux et les systèmes d'information sont identifiés, évalués et traités au moyen d'un registre des risques structuré. Des propriétaires de risques sont désignés pour chaque risque identifié, les plans de traitement font l'objet d'un suivi jusqu'à leur clôture, et la posture de risque globale est examinée au moins annuellement par la direction générale. Des évaluations des risques sont déclenchées par des modifications substantielles apportées aux systèmes, services ou au paysage des menaces, en complément du cycle d'examen planifié.

Détection des incidents et réponse aux incidents

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Akka maintient un plan de réponse aux incidents documenté couvrant l'intégralité du cycle de vie d'un incident de sécurité : détection, triage, confinement, éradication, rétablissement et examen post-incident. Une supervision de la sécurité est mise en œuvre sur l'ensemble de l'infrastructure d'Akka pour détecter les activités anormales, les tentatives d'accès non autorisé et les indicateurs de compromission. Les incidents sont classés par niveau de gravité, et les voies d'escalade sont clairement définies. En cas d'incident significatif affectant les services d'Akka ou les données des clients, Akka est en mesure de notifier les clients concernés et les autorités compétentes compétentes conformément aux délais de notification prévus par NIS2 : alerte précoce dans les 24 heures, notification initiale dans les 72 heures et rapport final dans le délai d'un mois.

Sécurité de la chaîne d'approvisionnement

Akka applique un programme structuré de gestion des risques fournisseurs à l'ensemble des prestataires tiers et sous-traitants. Préalablement à leur intégration, les fournisseurs font l'objet d'une évaluation de leur posture de sécurité, et des exigences contractuelles en matière de sécurité sont imposées dans tous les contrats fournisseurs. Les sous-traitants traitant des données clients sont tenus de démontrer des niveaux de sécurité équivalents et font l'objet d'examens périodiques. Akka tient un registre actualisé des sous-traitants et communique les modifications aux clients préalablement à leur prise d'effet. Les dépendances critiques dans la chaîne d'approvisionnement d'Akka sont identifiées et soumises à une surveillance renforcée.

Continuité des activités et résilience

Akka maintient des plans documentés de continuité des activités et de reprise après sinistre couvrant sa plateforme SaaS et ses systèmes internes critiques. Des sauvegardes régulières sont effectuées, testées et stockées avec un isolement approprié pour se protéger contre les attaques par rançongiciel et autres attaques destructrices. Les objectifs de délai de reprise et de point de reprise sont définis pour les services critiques, et les procédures de rétablissement sont testées via des exercices de simulation sur table et des guides opérationnels. La résilience de l'infrastructure est assurée par des déploiements multi-zones de disponibilité sur les fournisseurs d'infrastructure cloud d'Akka.

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Contrôle des accès et cryptographie

L'accès aux systèmes et à la plateforme d'Akka est contrôlé selon le principe du moindre privilège. L'authentification multifacteur est imposée pour l'accès aux systèmes critiques et aux interfaces d'administration. Les accès privilégiés sont limités dans le temps, audités et soumis à une surveillance renforcée. Akka applique le chiffrement aux données en transit et au repos en utilisant des algorithmes cryptographiques actuels conformes aux standards de l'industrie. Des procédures de gestion des clés cryptographiques encadrent la génération, le stockage, la rotation et la révocation des clés.

Gestion des vulnérabilités et correctifs

Akka exploite un programme documenté de gestion des vulnérabilités couvrant sa plateforme SaaS, l'infrastructure sous-jacente et les logiciels développés en interne. Des analyses de vulnérabilités sont effectuées régulièrement, et les vulnérabilités identifiées sont triées et corrigées conformément à des délais définis en fonction de leur niveau de gravité. Akka maintient une politique de divulgation responsable permettant aux chercheurs externes de signaler les vulnérabilités potentielles. Les correctifs critiques et de haute gravité sont appliqués selon un calendrier accéléré, avec des procédures de modification d'urgence disponibles pour les menaces de type zero-day.

Politiques de sécurité et gouvernance

Le cadre de gouvernance de la sécurité de l'information d'Akka comprend un ensemble de politiques couvrant l'utilisation acceptable, le contrôle des accès, la gestion des incidents, la continuité des activités, la sécurité des fournisseurs, la cryptographie et la gestion des vulnérabilités. Ces politiques sont examinées et mises à jour au moins annuellement, approuvées par la direction générale et communiquées à l'ensemble du personnel concerné. Une formation de sensibilisation à la sécurité est dispensée à l'ensemble du personnel lors de

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

l'intégration et de manière récurrente chaque année, avec une formation spécifique au rôle pour le personnel occupant des postes sensibles en matière de sécurité.

Éléments probants à l'appui

Les éléments probants suivants viennent à l'appui de la présente attestation :

- SMSI aligné sur la norme ISO 27001 avec registre des risques complet, plans de traitement et programme d'examen par la direction
- Rapport d'attestation SOC 2 Type II délivré par un auditeur indépendant (disponible sous accord de confidentialité sur demande)
- Plan de réponse aux incidents documenté avec délais de notification alignés sur NIS2
- Programme d'évaluation de la sécurité des fournisseurs et registre des sous-traitants
- Plans de continuité des activités et de reprise après sinistre avec procédures de rétablissement testées
- Programme de gestion des vulnérabilités avec indicateurs de remédiation suivis
- Politiques de sécurité examinées et approuvées par la direction générale dans les douze derniers mois
- Formation annuelle de sensibilisation à la sécurité avec suivi des taux d'achèvement pour l'ensemble du personnel

Conclusion

Akka Technologies, Inc. atteste qu'à la date du présent document, ses pratiques de sécurité des réseaux et des systèmes d'information sont alignées sur les exigences de la Directive (UE) 2022/2555 (Directive NIS2). Les 17 contrôles NIS2 du SMSI d'Akka sont intégralement

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

mis en œuvre, les niveaux de risque sont Faibles ou Moyens, et aucune lacune de contrôle à Risque élevé n'existe.

Akka opère en tant que prestataire SaaS sur le marché de l'UE et prend au sérieux ses obligations au titre de NIS2, maintenant les capacités de gouvernance, techniques et opérationnelles requises pour protéger sa plateforme et ses clients contre les menaces de cybersécurité. La présente attestation est réexaminée annuellement ou lors de modifications substantielles de la posture de sécurité d'Akka ou du cadre réglementaire applicable. Elle est disponible sur demande auprès des clients, prospects et autorités compétentes.

Michael Nash

Directeur de la Sécurité des Systèmes d'Information (CISO)

Akka Technologies, Inc.

michael.nash@akka.io

Date : 20 avril 2026