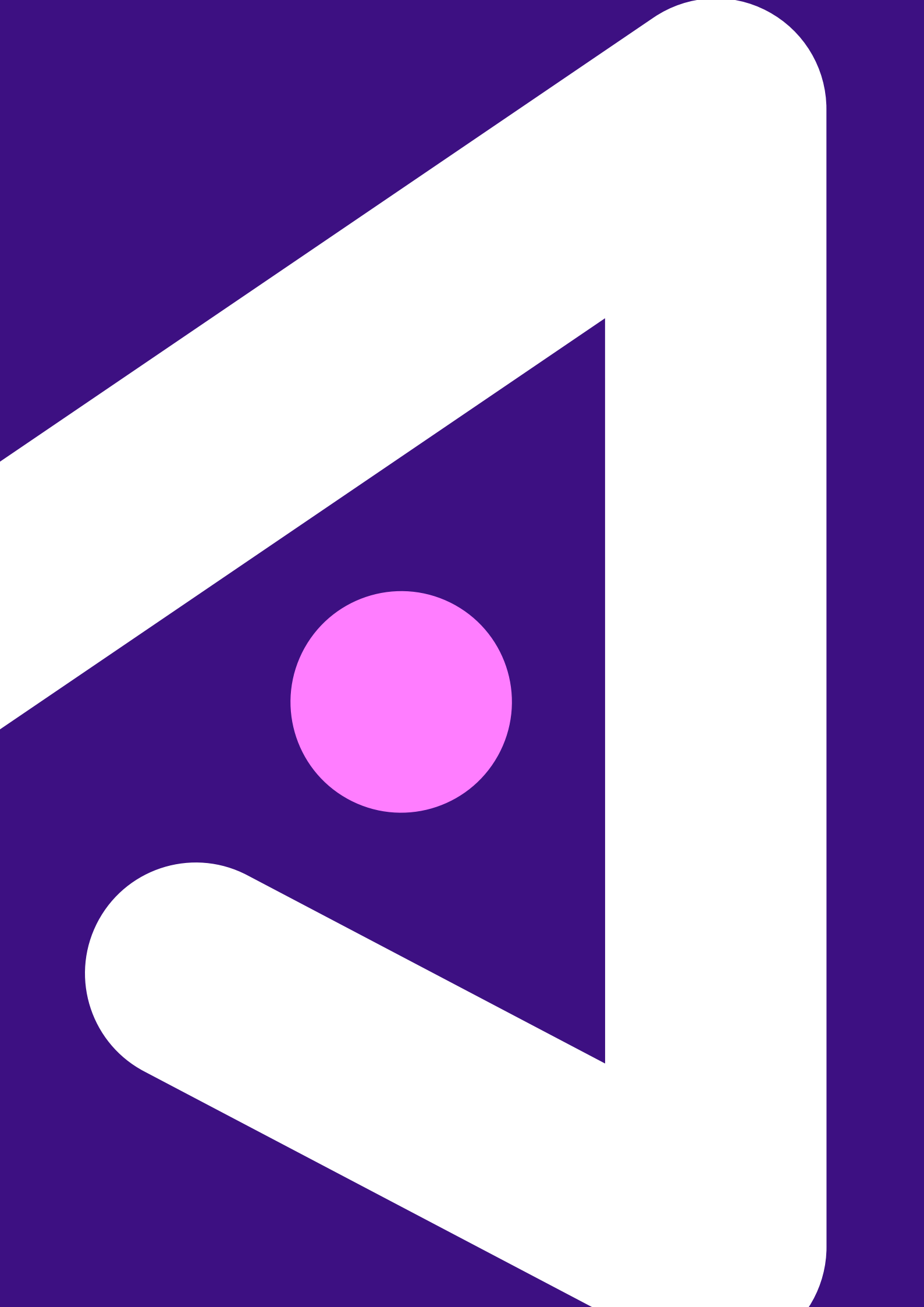
NIS2 et l'avenir de la sûreté des infrastructures critiques avec ALCEA.

Votre infrastructure critique mérite une protection sur tous les fronts. NIS2 n'est pas simplement une directive ; c'est une feuille de route pour garantir la résilience face à la montée des menaces. Cet eBook vous guidera dans la sécurisation de vos opérations en toute confiance.



dans cet eBook, vous découvrirez...

le défi croissant de la sûreté dans un monde en constante mutation.

Les infrastructures critiques d'aujourd'hui font face à des défis sans précédent. Les systèmes cyber et physiques sont plus interconnectés que jamais, créant des vulnérabilités qu'on ne peut plus ignorer. Que vous opériez dans les télécommunications, l'énergie, les transports ou tout autre secteur critique, rester sécurisé implique d'adopter une approche globale couvrant tous les aspects de votre activité.

NIS2 ne se limite pas à la conformité, c'est une préparation à l'avenir. La directive reconnaît la nature complexe et hybride des menaces modernes et met l'accent sur une protection proactive. ALCEA est là pour vous aider à comprendre et à vous adapter.

À retenir

La sécurisation de votre infrastructure critique commence par une compréhension claire du paysage des menaces en constante évolution et l'adoption d'un état d'esprit intégré et proactif.


Dispositivi
DBP.BPLE0922

NIS2 : un pont entre la sécurité physique et numérique.

Conçue pour renforcer la résilience numérique et physique, NIS2 établit de nouvelles normes de sécurité à travers l'Union européenne pour les services essentiels, en élargissant sa portée à de nombreux secteurs. Elle met l'accent sur des protocoles de sécurité robustes, une déclaration rapide des incidents, et une responsabilité accrue à tous les niveaux de l'organisation. Pour votre organisation, cela signifie réévaluer vos pratiques actuelles et adopter une stratégie de sécurité globale.

Aperçu rapide :

- Portée élargie : davantage de secteurs sont désormais couverts par NIS2.
- Déclaration plus stricte : la déclaration rapide des incidents n'est plus optionnelle.
- Normes renforcées : attendez-vous à des évaluations de risques rigoureuses et à des plans de mitigation.
- Calendrier de mise en œuvre : Les États membres de l'UE sont en train de transposer NIS2 dans leur législation nationale ; les exigences et délais peuvent varier selon les pays.

Pourquoi c'est important

NIS2 vise à combler les lacunes en matière de sécurité et à renforcer la résilience à tous les niveaux. La conformité devient un levier d'autonomisation, garantissant que les organisations ne se contentent pas de survivre, mais prospèrent dans un environnement imprévisible.

les nouvelles normes de NIS2 : ce que vous devez savoir.

NIS2 introduit des changements majeurs qui impactent les organisations comme la vôtre. Ces évolutions corrigent des vulnérabilités ignorées par NIS1 et établissent des exigences plus strictes pour sécuriser les opérations.

Modifications clés :

- Sécurité de la chaîne d’approvisionnement : vous êtes désormais responsable de l’évaluation des pratiques de sécurité de vos fournisseurs et partenaires.
- Déclaration des incidents : les incidents doivent être signalés aux autorités compétentes dans un délai de 24 heures.
- Couverture élargie : des secteurs comme l’administration publique et la santé sont désormais inclus.
- Sanctions possibles : le non-respect peut entraîner de lourdes conséquences — jusqu’à 10 millions d’euros ou 2 % du chiffre d’affaires annuel mondial pour les entités essentielles, et 7 millions d’euros ou 1,4 % pour les entités importantes, selon le montant le plus élevé.

Pourquoi c’est important

Avec ces exigences renforcées, les organisations peuvent mieux se défendre contre des menaces sophistiquées. Une approche intégrée garantit la continuité des opérations et renforce la confiance des parties prenantes.

Comparaison entre NIS1 et NIS2

Élément	NIS1	NIS2
Scope	OES et DSP	Entités essentielles et importantes
Déclaration des incidents	Volontaire	Obligatoire
Gestion des risques	Pas un objectif principal	Est un objectif principal
Coopération et coordination	Partage d'informations via le CSIRT national et l'ENISA	Partage d'informations via le CSIRT national et le Groupe de coopération
Application et sanctions	Pas de délais ni de sanctions spécifiés	Délais spécifiés avec sanctions définies par les États membres

3. Évaluer votre posture de sûreté actuelle

votre organisation est-elle prête ? réalisez une analyse des écarts de conformité.

Réaliser une analyse complète des écarts vous aidera à identifier les domaines nécessitant une attention particulière. Commencez par cette liste de vérification :

Checklist :

- Avez-vous évalué vos risques en cybersécurité au cours des six derniers mois ?
- Vos mesures de sécurité physique et numérique sont-elles intégrées ?
- Disposez-vous d'un plan clair de réponse aux incidents ?
- Votre équipe est-elle formée pour gérer des menaces hybrides ?

En évaluant votre niveau de préparation, vous identifierez les lacunes et pourrez établir une feuille de route vers la conformité. Pour aller plus loin, vous pouvez consulter la page officielle de la campagne de sensibilisation de l'ENISA, qui propose des conseils et des ressources adaptés à la directive NIS2:
ENISA – Network and Information Systems Awareness.

une approche unifiée : sécurité physique et cybersécurité en harmonie.

Imaginez ce scénario : un système de contrôle d'accès compromis dans un centre de données ouvre la voie à une cyberattaque plus vaste. Dans ce cas, un accès physique non autorisé permet l'infection par un ransomware qui chiffre des données opérationnelles sensibles, paralysant ainsi les activités de l'entreprise. La faille de sécurité ne s'arrête pas au numérique : les vulnérabilités physiques offrent un accès direct aux attaquants, amplifiant l'impact.

Étude de cas

Une entreprise de transport a subi une double violation : d'abord, un point d'accès physique dans un hub de transport a été compromis, permettant à des individus non autorisés d'entrer dans des zones restreintes. Cette brèche a permis à des cybercriminels d'installer un malware, déclenchant ensuite une attaque par ransomware sur les systèmes critiques de l'entreprise. Les opérations ont été interrompues et les chaînes d'approvisionnement perturbées pendant plusieurs jours. L'intégration des systèmes de sécurité — en combinant contrôle d'accès physique et cybersécurité — a permis d'éviter une escalade supplémentaire. Elle a accéléré la reprise en contenant la brèche à sa source et a renforcé la résilience globale.

Les solutions d'ALCEA visent à prévenir ce type de scénario grâce à une approche intégrée et proactive, garantissant que les couches de sécurité physique et numérique soient parfaitement alignées et renforcées.

que signifie réellement une sûreté totale, et pourquoi est-ce important pour vous ?

Aujourd’hui, la sûreté ne se limite plus aux serrures, caméras ou identifiants. Il s’agit de la manière dont tous les éléments fonctionnent ensemble, entre les départements, les technologies et les sites. À mesure que les menaces évoluent, notre manière de protéger les opérations doit également évoluer.

La réalité ? Une seule faille peut compromettre l’ensemble de votre infrastructure. C’est pourquoi un assemblage de systèmes déconnectés ne suffit plus. Ce qu’il vous faut, c’est une approche connectée, complète, simple à gérer, évolutive et conçue pour s’adapter.

C’est cela, une solution globale. Et c’est là qu’ALCEA peut vous aider.

Nos Solutions Globales regroupent le contrôle d’accès, la gestion des clés et des visiteurs, la détection d’intrusion, la vidéosurveillance et les services, le tout sous une seule plateforme. Vous bénéficiez de clarté, de contrôle et de confiance, avec une couverture complète de chaque couche de votre sûreté. Que vous débutiez avec NIS2 ou que vous renforciez un système existant, nous sommes là pour vous accompagner à chaque étape.

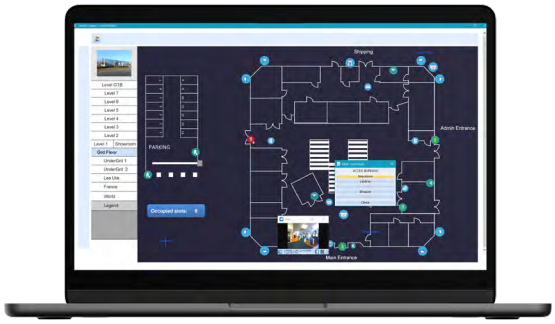
Contactez-nous pour découvrir comment nous pouvons vous aider

Solutions Globales ALCEA – Conçues pour les environnements critiques

Nous combinons des technologies éprouvées et des outils issus d'ALCEA et d'autres fabricants de premier plan pour vous offrir un portefeuille complet et flexible, capable de répondre aux exigences des opérations critiques d'aujourd'hui.

ALWIN

Votre plateforme de sûreté centrale pour la gestion en temps réel des accès, de la vidéo et des intégrations. Flexible, fiable et conçue pour répondre aux besoins des infrastructures critiques.



ALWIN CIPE

Un portefeuille numérique évolutif pour une protection de haut niveau. Gérez les clés, les serrures et les droits d'accès à distance. Compatible avec BEAT, CLIQ et les systèmes mécaniques. Assure une efficacité opérationnelle et une visibilité complète de la situation.

CLIQ

Accès intelligent basé sur des clés électroniques. Aucun câblage nécessaire. Définissez les autorisations, suivez les usages et gardez le contrôle — même dans les zones éloignées ou difficiles d'accès.

ABLOY BEAT

Utilisez votre téléphone comme clé. ABLOY BEAT offre un accès mobile sécurisé, chiffré et sans clé à vos installations — simple à utiliser, facile à gérer.

conçu avec NIS2 à l'esprit.

Chaque composant de notre solution répond aux exigences clés de la directive NIS2 :

- Gestion robuste des identités et des accès
- Journaux d'audit traçables et historique des activités
- Architecture évolutive pour s'adapter aux risques croissants
- Compatibilité entre systèmes et fournisseurs

6. Étapes pratiques vers la conformité : Une feuille de route pour les organisations

votre parcours vers la conformité NIS2 : étape par étape.

Atteindre la conformité NIS2 ne consiste pas à cocher des cases, mais à construire une résilience à long terme. Pour la plupart des organisations, cela implique des améliorations au niveau des personnes, des processus et des technologies. Cela demande du temps, de la coordination et du leadership. Mais vous n'avez pas à tout faire d'un coup, ni à le faire seul.

La conformité n'est pas un projet ponctuel. NIS2 exige des organisations qu'elles s'améliorent en continu. Cela signifie des audits réguliers, des mises à jour des systèmes, la formation du personnel et la révision des politiques à mesure que votre environnement évolue.

Voici une feuille de route générale pour bien démarrer.

Étape 1

Comprendre vos risques

Commencez par une évaluation détaillée des risques, à la fois cyber et physiques. Cartographiez vos actifs critiques, identifiez les points vulnérables et comprenez comment un incident potentiel pourrait affecter vos opérations. C'est la base de tout le reste.

Étape 2

Définir vos priorités

Tous les systèmes ne présentent pas le même niveau de risque. Concentrez-vous d'abord sur les domaines qui soutiennent les services essentiels, protègent les données sensibles ou ont un impact sur la sécurité et la conformité. Alignez vos équipes internes autour d'un plan d'action clair.

Étape 3

Intégration des systèmes

Examinez comment vos outils de sécurité physique et numérique fonctionnent ensemble. Les lacunes proviennent souvent d'un manque d'intégration entre le contrôle d'accès, les alarmes, la vidéosurveillance, les systèmes d'identité et la cybersécurité. L'intégration améliore la visibilité et accélère les temps de réponse.

en savoir plus

Parce que c'est la responsabilité de tous

Étape 4

Préparez-vous à l'imprévu

Des incidents surviendront, ce qui compte, c'est votre capacité à y répondre. Élaborez ou révisez votre plan de réponse aux incidents. Définissez les rôles, les circuits de remontée d'information et les procédures d'escalade. Testez régulièrement votre dispositif.

Étape 5

Évoluez en continu

Une fois votre procédure en place, il faudra la revoir de façon régulière, procéder à des exercices de gestion de crise et déterminer des KPIs. La traçabilité de vos vulnérabilités et de vos actions devra être archivée et rendue disponible pour des audits.

7. Devenir partenaire d'ALCEA

votre allié stratégique pour la conformité NIS2.

Répondre aux exigences de NIS2 ne se résume pas à adopter de nouveaux outils, il s'agit d'un changement durable. C'est pourquoi avoir le bon partenaire à vos côtés fait toute la différence.

Chez ALCEA, nous accompagnons les infrastructures critiques et leurs prestataires avec des solutions de sûreté intégrées et une expertise sectorielle. Du contrôle d'accès aux journaux d'audit, nous savons comment vous aider à renforcer votre environnement conformément aux attentes de NIS2, et à rester résilient dans la durée.

La sûreté n'est pas un projet ponctuel. C'est un processus. Et nous sommes là pour vous accompagner, étape par étape.

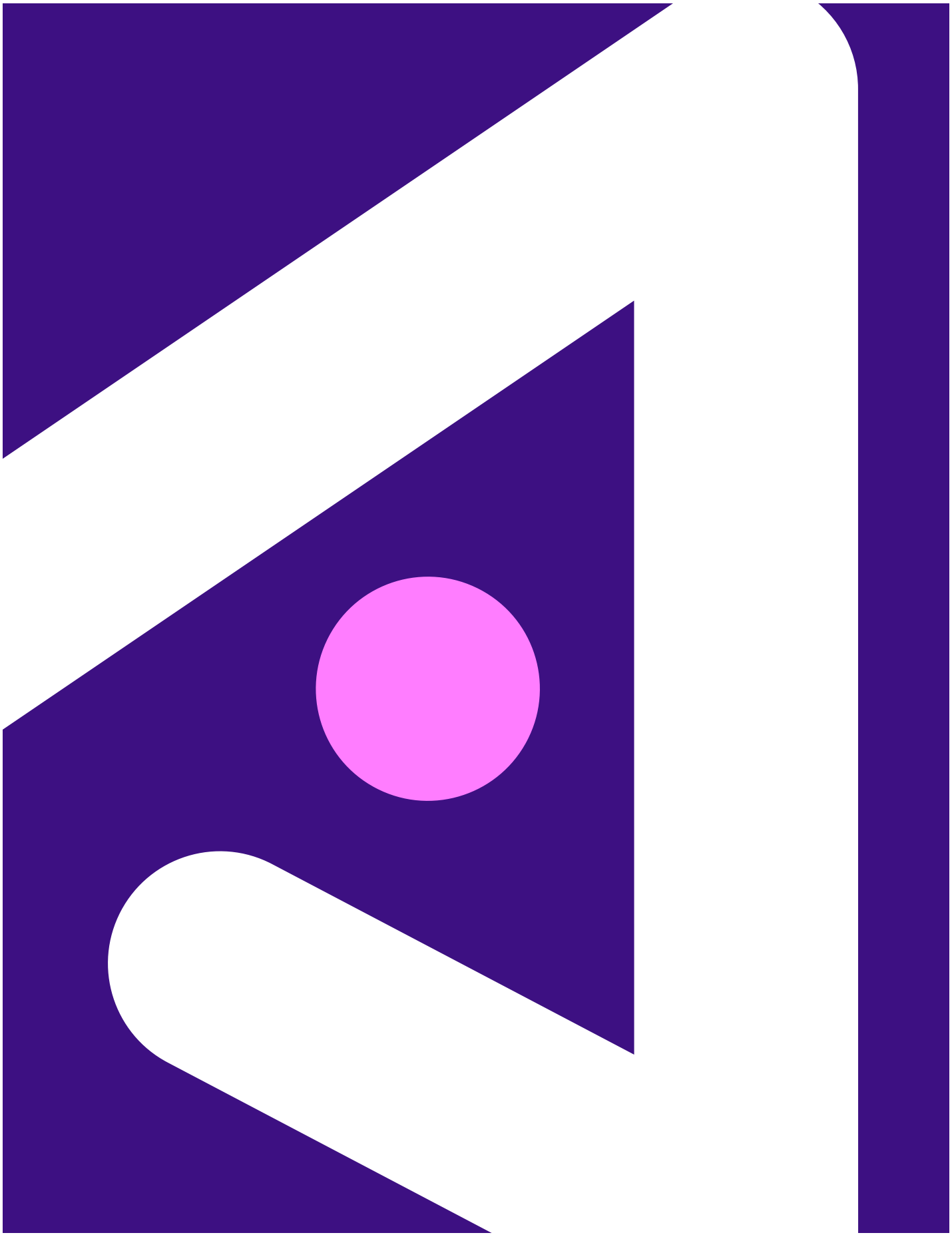
Prêt à renforcer votre sûreté ?

L'avenir de la sûreté des infrastructures est proactif, connecté et conçu pour durer. Que vous cherchiez à améliorer vos systèmes actuels ou à comprendre ce que NIS2 implique pour vos opérations, notre équipe est là pour vous soutenir.

Assurons ensemble la continuité de vos infrastructures critiques.

Contactez-nous

Visitez alceaglobal.com/fr



ALCEA specializes in protecting critical infrastructure globally, including energy, water, telecom, transportation, mining, oil, and gas. We provide comprehensive security solutions tailored to your unique needs, from access control and intrusion detection to key and video management. Our experienced specialists deliver customized, digitalized solutions that enhance efficiency, ensure compliance, and offer peace of mind.

alceaglobal.com

NIS2 et l'avenir de la sûreté des infrastructures critiques avec ALCEA | 09/2025