Trellix

PRÉSENTATION DE SOLUTION

Directive NIS2

Comment Trellix peut renforcer la cyberrésilience et assurer la conformité des entreprises, tous secteurs confondus

Qu'est-ce que la directive NIS2 ?

La deuxième version de la directive sur la sécurité des réseaux et des systèmes d'information (NIS2) est une réglementation européenne visant à renforcer la cybersécurité et la résilience à l'échelle de l'UE. Il ne s'agit pas d'un cadre de contrôles de sécurité spécifiques, mais d'une approche mandatée de gestion continue des risques destinée à améliorer constamment la maturité de la cybersécurité, la gestion des incidents et le partage d'informations dans les entreprises d'infrastructures critiques et les États membres.

Qui est concerné par la directive NIS2 ?

Les organisations concernées par la directive NIS2 sont nombreuses et comprennent les entités fournissant des services essentiels (énergie, transports, services bancaires, santé, eau, etc.), les fournisseurs de services numériques et les administrations publiques. NIS2 s'applique également aux entités fournissant des services importants, par exemple les services postaux et de courrier, la gestion des déchets, l'industrie chimique, les fournisseurs de services TIC, l'agroalimentaire et certains types de fabricants. Pour obtenir la liste complète des organisations concernées, veuillez vous reporter au texte intégral de la directive NIS2.

Pourquoi adopter Trellix pour la mise en conformité avec NIS2 ?

Trellix vous aide à répondre plus rapidement aux exigences de la directive NIS2. Trellix Helix Connect unifie la visibilité sur les menaces au sein de votre environnement grâce à une détection plus avancée des menaces qui peuvent échapper aux outils individuels. Trellix Helix Connect intègre des données issues des contrôles de sécurité Trellix et de plus de 500 sources tierces utilisant des analyses prédéfinies pour créer des détections multivectorielles et multisources, ainsi qu'une automatisation optimisée par l'IA en vue de réduire les délais de réponse aux incidents. Trellix Security Platform, notre plate-forme riche en fonctionnalités et optimisée par l'IA générative, fournit les contrôles de sécurité avancés requis pour améliorer les pratiques de cybersécurité au niveau des endpoints, des serveurs, des réseaux, des données, du cloud et des terminaux mobiles. Reposant sur plus d'une décennie de modélisation IA et 25 ans d'expérience dans les analyses et l'apprentissage automatique, les fonctionnalités d'IA générative de Trellix Wise réduisent la désensibilisation aux alertes et identifient les menaces furtives. Trellix Consulting Services peut évaluer votre programme de sécurité actuel au regard des normes internationales et européennes, en vous fournissant des évaluations du niveau de préparation et une Threat Intelligence pour l'analyse continue des risques.

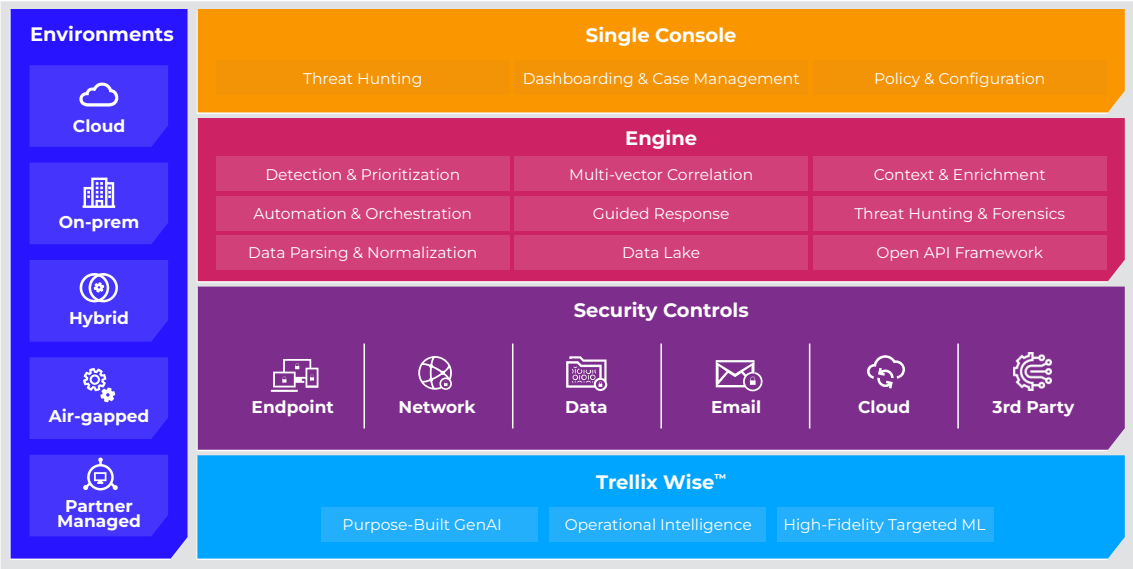

Figure 1. Trellix Security Platform

Les exigences de conformité spécifiques peuvent varier en fonction des directives de mise en œuvre des États membres, mais la résilience et la réduction des cyberrisques restent le fil conducteur pour la mise en conformité avec NIS2. Vous trouverez ci-dessous les cinq principales façons dont Trellix, en collaboration avec nos solutions partenaires, peut vous aider à répondre aux exigences de la directive NIS2 et à gérer le risque de menaces émergentes.

Identifiez les risques auxquels vous êtes exposé grâce aux services d'évaluation Trellix

La directive NIS2 exige que les organisations effectuent des évaluations des risques et adoptent des normes internationales ou européennes telles que l'ISO 27001 ou le cadre de cybersécurité du NIST afin de gérer les cyberrisques en continu. La date limite de mise en conformité approche à grands pas. Il est important d'évaluer votre programme actuel au regard de l'une de ces normes et votre niveau de préparation dans les domaines à haut risque potentiels. D'après notre expérience et la Threat Intelligence de Trellix, nous vous recommandons de vous concentrer sur ces cinq évaluations fondamentales.

Solution Trellix	Description de la solution	Articles NIS2 associés
Évaluation de cybersécurité	Évaluation de la maturité au regard des normes internationales et établissement de politiques de sécurité des informations	20.2, 21.1, 21.2a
Intelligence as a Service	Identification des menaces ciblées qui mettent en péril votre entreprise	20.2, 21.1, 21.2a
Évaluation du niveau de préparation face aux ransomwares	Exercices de simulation personnalisés permettant d'évaluer votre exposition aux ransomwares	20.2, 21.1,21.2a, 21.2c, 21.2f
Évaluation du niveau de préparation des SOC	Développement d'un programme de réponse aux incidents, évaluation et conception de fonctionnalités XDR, et support de réponse aux incidents d'urgence en cas de crise	20.2, 21.2a, 21.2b, 21.2f
Évaluation des applications web	Évaluation des processus DevSecOps et des applications externes	20.2, 21.2a, 21.2f

Pour profiter des services d'évaluation Trellix, contactez votre responsable de compte ou rendez-vous sur cette page.

Renforcez votre résilience face aux ransomwares

Notre récent Rapport sur le paysage des cybermenaces décrit l'escalade des attaques de ransomwares, avec de nouvelles menaces exerçant un impact croissant. Les ransomwares représentent une menace majeure pour les entités fournissant des services essentiels régis par la directive NIS2. Des attaques de grande envergure affectent les secteurs de l'énergie et des transports ainsi que les administrations publiques, entraînant une perturbation des services essentiels. Les organisations doivent ériger des défenses robustes pour prévenir, détecter et neutraliser rapidement les attaques de ransomwares. En plus des évaluations du niveau de préparation face aux ransomwares de Trellix, nous vous recommandons de tirer parti des solutions Trellix suivantes pour combler les failles dans la protection antimalware et réduire le risque de ransomwares qui pourraient affecter votre activité.

Solution Trellix	Description de la solution	Articles NIS2 associés
Trellix Endpoint Security	Protection avancée contre les ransomwares sur les systèmes des utilisateurs finaux, les serveurs et les terminaux mobiles	21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j
Trellix IVX for Collaboration Applications	Prévention et détection de la distribution de ransomwares via des attaques de phishing et des applications de collaboration	21.2g, 21.2j
Trellix File Protect	Identification des ransomwares dissimulés dans le stockage et les applications métier personnalisées	21.2c, 21.2g
Trellix Network Security	Prévention et détection des mouvements latéraux et des techniques de distribution ultérieure de ransomwares	21.2e, 21.2b
Trellix Helix Connect	Unification des signaux de plusieurs outils afin d'identifier les menaces de ransomwares qui peuvent échapper aux outils individuels	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j

Pour en savoir plus sur la façon dont Trellix peut protéger votre entreprise contre les ransomwares, consultez notre site web sur la détection et la réponse aux ransomwares ici.

Accélérez la détection et la réponse aux menaces des SecOps

L'un des principaux objectifs de la directive NIS2 est d'améliorer la détection et la réponse aux incidents dans toute l'entreprise. De nombreux fournisseurs de services essentiels se heurtent probablement à des obstacles au niveau des SOC, tels qu'un manque de visibilité, une pénurie de talents et un manque d'automatisation. Nos évaluations des SOC et de la réponse aux incidents mettent en lumière ces lacunes et vous aident à élaborer un plan d'action pour corriger et affiner le programme. Sur le plan technologique, Trellix Helix Connect réduit la charge de travail des analystes et le délai moyen de résolution grâce à une plate-forme de sécurité ouverte qui intègre les données issues des capteurs Trellix et de plus de 500 intégrations. Nous enrichissons les données grâce à une Threat Intelligence intégrée et à une automatisation optimisée par l'IA, ce qui nous permet d'assurer une détection et une réponse rapides sur les réseaux IT, OT et cloud. En plus de Trellix Helix Connect et des évaluations des SOC, nous vous recommandons les solutions Trellix suivantes qui offrent une visibilité et une détection des menaces avancées à l'échelle de l'entreprise.

Solution Trellix	Description de la solution	Articles NIS2 associés
Trellix EDR et Trellix Endpoint Forensics	Visibilité étendue sur les endpoints, détection des activités malveillantes et investigations numériques pour la réponse aux incidents	21.2b, 21.2g
Trellix NDR et Trellix Network Forensics	Capture complète de paquets réseau et détection des activités réseau malveillantes	21.2e, 21.2b
Trellix IVX for Enterprise Applications	Analyse antimalware cloud hautement évolutive	21.2b, 21.2g
Trellix Helix Connect	Fonctionnalités XDR avec Threat Intelligence, IA et analyses intégrées pour réduire les délais moyens de détection et de réponse	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j
Semperis (partenaire)	Protection des services d'annuaire et intégration avec Helix Connect pour profiter des fonctionnalités de détection et de réponse pour la protection de l'identité	21.2g, 21.2i

Protégez vos réseaux et systèmes OT

De nombreuses entités fournissant des services essentiels régis par la direction NIS2 exécutent des systèmes et réseaux OT. Ces systèmes OT sont cruciaux pour la résilience des entreprises et sont souvent la cible des cybercriminels. L'environnement OT est exposé à un risque accru, car les contrôles de sécurité sont souvent insuffisants pour prévenir les menaces avancées à ce niveau. En outre, la surveillance de la sécurité OT est généralement assurée par des opérateurs inexpérimentés, qui ne sont pas en relation avec les équipes de sécurité IT. Trellix Security Platform, notre plate-forme optimisée par l'IA générative, contribue à sécuriser vos systèmes OT critiques. Trellix Endpoint Security propose des contrôles de base et avancés pour les systèmes OT et est certifié par tous les principaux fabricants de systèmes de contrôle et d'acquisition de données (SCADA, Supervisory Control and Data Acquisition). Cependant, la sécurité des endpoints n'offre pas à elle seule une protection suffisante. Il est primordial de disposer d'une visibilité sur les ressources pour identifier les vulnérabilités, de contrôles de sécurité aux limites du réseau et d'une surveillance pour détecter les comportements anormaux. En plus de Trellix Endpoint Security, nous vous recommandons de tirer parti des solutions Trellix suivantes pour combler les failles dans la protection antimalware, fournir une visibilité sur des ressources SCADA spécifiques et détecter les menaces potentielles.

Solution Trellix	Description de la solution	Articles NIS2 associés
Trellix Endpoint Security	Protection avancée contre les ransomwares sur les systèmes des utilisateurs finaux, les serveurs et les terminaux mobiles	21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j
Trellix Embedded Security	Protection avancée contre les ransomwares sur les terminaux des utilisateurs finaux et les serveurs dans les environnements OT	21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j
Trellix Network Detection and Response Security	Détection des activités réseau malveillantes entre les réseaux IT et OT	21.2e, 21.2b
Nozomi Networks (partenaire) Tenable (partenaire)	Découverte d'informations sur les ressources SCADA et les vulnérabilités associées, intégration avec les fonctionnalités XDR pour la détection et la réponse aux menaces	21.2e, 21.2b
Trellix Helix Connect	Mise en corrélation des données provenant de multiples sources, y compris les équipements OT et IoT, pour dresser un tableau complet d'une menace	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j

Pour découvrir comment Trellix peut protéger vos systèmes OT, consultez cette étude de cas.

Réduisez le risque de compromission de données

La protection des données sensibles et propriétaires devient de plus en plus complexe. Pour commencer, les données sont partout : applications client, stockage cloud, bases de données et terminaux personnels. Ensuite, il existe un risque de compromission par des menaces externes et internes. En effet, selon le rapport *Data Breach Investigations 2024* de Verizon, 68 % des compromissions sont dues à des risques internes. Les groupes APT externes ont recours à l'IA pour générer des exploits plus rapidement, ce qui peut exposer vos données client et données d'entreprise sensibles à des menaces au travers d'applications vulnérables. La directive NIS2 prévoyant des délais de déclaration serrés en cas de compromission de données, le moment est venu de se concentrer sur l'amélioration de votre programme de sécurité des données. Trellix Consulting Services peut booster votre programme de sécurité des données en alignant vos priorités en matière de sécurité des informations métier sur le contrôle de la protection. Ensuite, Trellix DLP Discover analysera votre réseau et vos référentiels tels que SharePoint, améliorant ainsi la visibilité et la classification. Cette approche vous aidera à vous lancer, mais pour adopter une couverture de protection complète, nous vous recommandons d'implémenter les contrôles Trellix Data Security suivants afin de réduire le risque de compromission de données sur les terminaux et dans le cloud.

Solution Trellix	Description de la solution	Articles NIS2 associés
Trellix Endpoint Data Protection and Discovery	Découverte, classification et protection des données sur les endpoints	21.2h, 21.2i
Trellix Network Data Protection and Discovery	Découverte, classification et protection des données sur le réseau	21.2i
Trellix Database Security	Surveillance et contrôle de l'accès aux informations sensibles dans les bases de données d'application	21.2i
Trellix Helix Connect	Fonctionnalités XDR permettant d'améliorer la détection et la réponse pour la protection des données	21.2d, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j
Skyhigh Security (partenaire)	Surveillance et contrôle de l'accès aux informations sensibles dans les applications cloud	21.2d, 21.2i, 21.2j

Pour en savoir plus sur Trellix et la directive NIS2, regardez notre webinar Achieving NIS2 Compliance with Trellix ou planifiez un atelier avec vos représentants Trellix.