Cyberdefense

Construire une architecture de cybersécurité fiable pour se mettre en conformité avec la directive NIS 2

Sécurisez votre avenir numérique

Table des matières

01 Tout savoir sur NIS2

Qu'est-ce que NIS 2 ?

La directive NIS 2 (Network and Information Systems Directive 2) est une réglementation de l'Union européenne visant à renforcer la cybersécurité des infrastructures critiques et des services essentiels des entreprises et organisations.

Dans les 3 ans en moyenne, à compter du vote du projet de loi ou du règlement d'exécution européen. NIS 2 élève le niveau d'exigence en matière de cybersécurité dans toute l'UE, obligeant les organisations à mettre en place des cadres de sécurité robustes, à réaliser des audits réguliers et à engager la responsabilité de la direction.

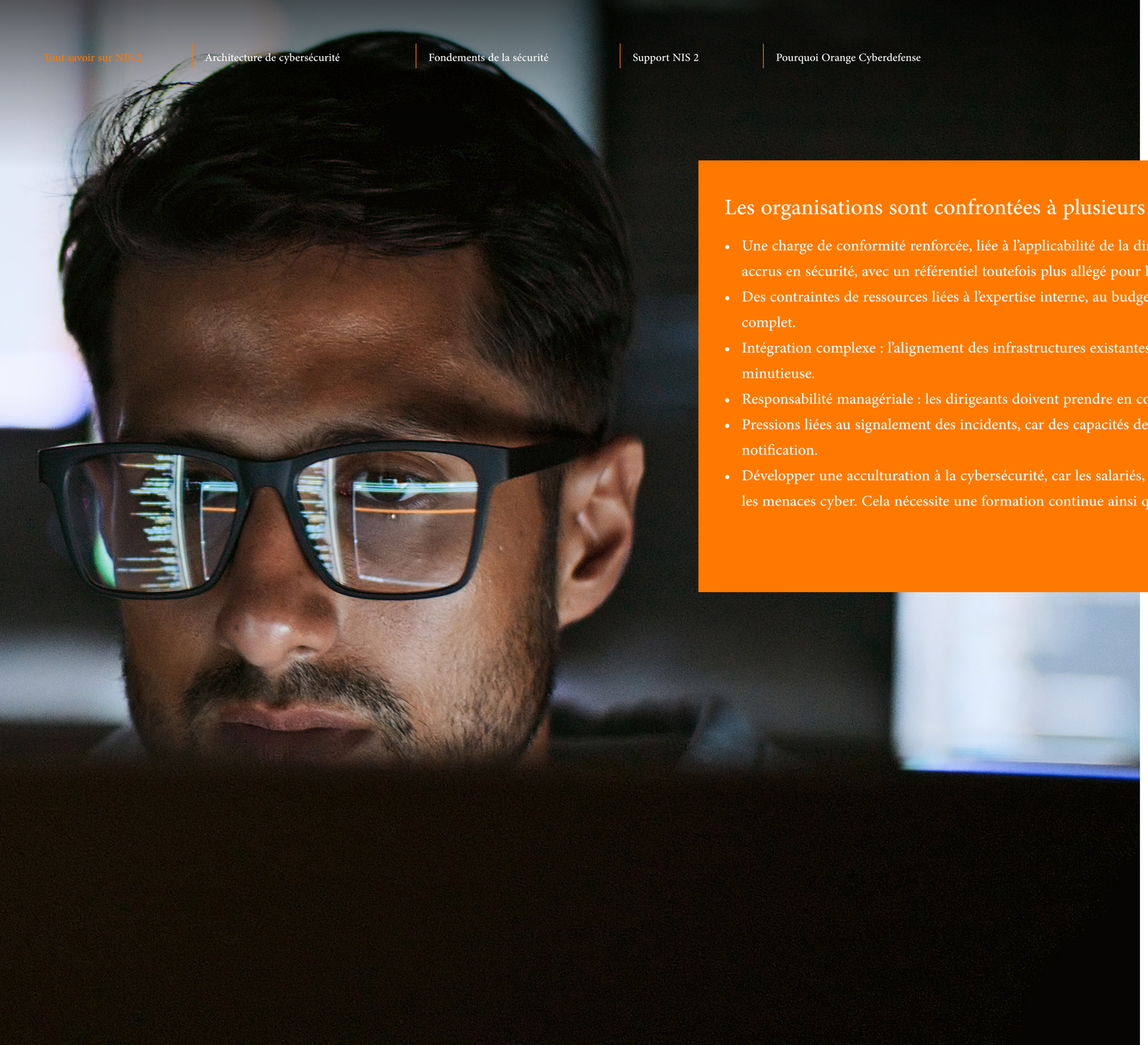
La directive distingue deux catégories d'organisations : Entités Essentielles (EE) et Entités Importantes (EI), selon leur niveau de criticité et les exigences associées.
Vérifiez si votre organisation est concernée ou non sur le site de l'ANSSI :

Elle élargit également le champ d'application de NIS en :

- couvrant davantage de secteurs et reposant sur des critères communs d'applicabilité
- imposant des mesures de sécurité plus strictes, et
- introduisant des sanctions plus sévères en cas de non-conformité.

Comment NIS 2 impacte-t-elle les entreprises ?

- NIS 2 exige des organisations qu'elles mettent en place un cadre documenté de gestion des risques liés aux TIC.
- Parmi les mesures de sécurité clés figurent la segmentation des réseaux, la gestion des identités et des accès, ainsi que les plans de réponse aux incidents.
- S'aligner sur les prérequis de la Directive permettra aux entreprises et organisations de renforcer leur cybersécurité, de garantir la conformité et de contribuer à la protection des données ainsi qu'à la lutte contre des menaces cyber en constante évolution.



Les organisations sont confrontées à plusieurs défis majeurs :

- Une charge de conformité renforcée, liée à l'applicabilité de la directive sur l'ensemble du SI et à l'adoption de règles plus strictes, exigeant des investissements accrus en sécurité, avec un référentiel toutefois plus allégé pour les entités importantes (EI) que pour les entités essentielles (EE).
- Des contraintes de ressources liées à l'expertise interne, au budget ou au personnel nécessaire pour mettre en place et maintenir un cadre de cybersécurité complet.
- Intégration complexe : l'alignement des infrastructures existantes avec les exigences de NIS 2 nécessite souvent des mises à niveau et une planification minutieuse.
- Responsabilité managériale : les dirigeants doivent prendre en compte la cybersécurité et conduire les évolutions culturelles et opérationnelles nécessaires.
- Pressions liées au signalement des incidents, car des capacités de détection et de réponse rapides sont nécessaires pour respecter des obligations strictes de notification.
- Développer une acculturation à la cybersécurité, car les salariés, à tous les niveaux de l'entreprise, doivent être sensibilisés, préparés et capables d'identifier les menaces cyber. Cela nécessite une formation continue ainsi que des exercices de sécurité réguliers.

Les organisations ont besoin d'une approche proactive, qui inclut :

- L' évaluation de leur posture de sécurité actuelle ainsi que l'identification des failles,
- La construction d'une stratégie et feuille de route de cyber-résilience et
- Le soutien de partenaires experts en sécurité pour s'assurer d'être en conformité et de protéger les assets critiques.

02 Architecture de cybersécurité

Plus que jamais, être en conformité cyber est essentiel pour protéger votre entreprise.

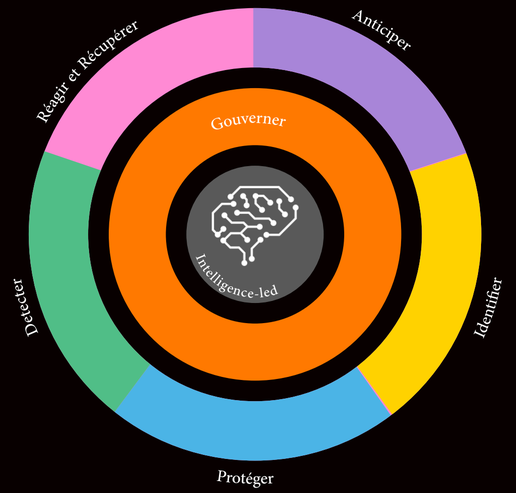
Avec Orange Cyberdefense, la conformité NIS 2 n'est qu'un point de départ — notre expertise de sécurité de bout en bout renforce l'ensemble de votre stratégie de cybersécurité et vous accompagne tout au long du cycle de vie des menaces.

L'expertise d'Orange Cyberdefense vous offre une approche sur tout le cycle de la menace

02 Architecture de cybersécurité

Architecture de cybersécurité pour NIS 2

Panorama des menaces
- Gestion des vulnérabilités
- Conseil en matière de menaces



Renseignement sur les menaces
Surveillance de la cybercriminalité

Priorités business

Risque lié à la sécurité de l'information

Exigences de conformité et contractuelles

Gouvernance de la cybersécurité – Gestion des risques, audits et évaluations, planification et hiérarchisation, indicateurs de performance (KPIs)

Gestion des actifs | Gestion des identités | Gestion de la chaîne d'approvisionnement | Sensibilisation et formation | Politiques et directives de sécurité

Data Gouvernance | Architecture continue Secure by Design et Secure by Default, intégrant une approche Zero Trust

Identification des actifs et des vulnérabilités, tests d'intrusion et évaluations techniques

Opérations de sécurité et gestion de la posture de sécurité (surveiller et atténuer les risques techniques grâce à une approche et une conception Zero Trust)

Utilisateur & Appareil
Accès sécurisé

- Système d'identité
- Messagerie
- Collaboration

Internet

Sécurité de l'utilisateur et de l'identité | Sécurité des appareils | Logiciels en tant que service (SaaS) | Sécurité Internet / Web | Applications privées

Secure Service Edge (SSE)

EDGE/LAN and SD-WAN Network Security

Production
Application
Information

Business SaaS Applications

Applications à accès public | Développement logiciel sécurisé | Sécurité des données, de l'IA et de l'intégration

Applicationsà accès privé | Sécurité du cloud et des infrastructures | Sécurité des technologies opérationnelles

Comptes privilégiés + identités non humaines | Sécurité du réseau

Visibilité et analyses – Datalake

Logs (SIEM) | Endpoint (EDR) | Network data (NDR) | Identité data | Cloud data | Archive logging

Fonctionnalité unifiée de détection et de réponse managée (XDR)

Automatisation et orchestration de la sécurité (SOAR) | Détection, chasse et réponse 24/7 (Analystes)

Récupération, Sauvegarde, Restauration

Plans de réponse aux incidents
Plans de continuité d'activité (BCP)
Plans de reprise après sinistre (DR)

Analyse forensique, reporting et coordination

Réponse et reprise après incident (CIRT)

02 Architecture de cybersécurité

Orientation d'une architecture

Une stratégie de cybersécurité bien structurée repose sur une approche holistique qui équilibre les priorités business, la gestion des risques et la conformité.
Les organisations peuvent bâtir un cadre de cybersécurité résilient, évolutif et conforme en intégrant ces éléments dans leurs décisions d'architecture de sécurité.
Il est également essentiel d'inclure une analyse du paysage des menaces et des vulnérabilités émergentes afin de s'assurer d'anticiper les menaces pertinentes.

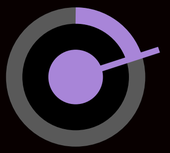
Vue d'ensemble d'une architecture cyber

Panorama des menaces
- Analyse des vulnérabilités
- Alerte sur les menaces

Enjeux business

Risque lié à la sécurité de l'information

Enjeux de conformité et contractuels

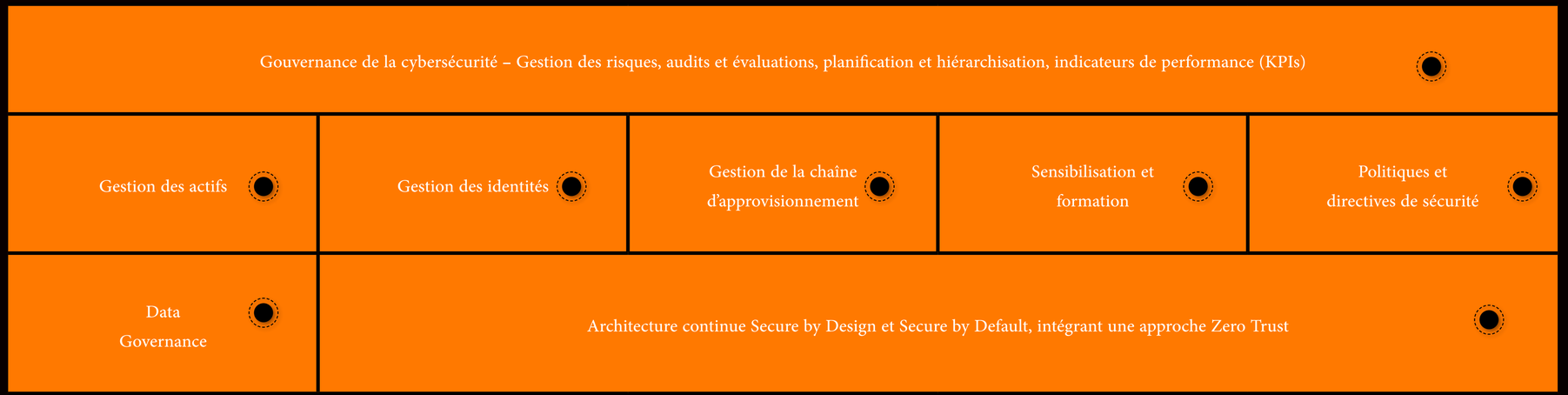


02 Architecture de cybersécurité

Intégrer la gouvernance dans l'architecture de cybersécurité

La gouvernance définit la manière dont les décisions de sécurité sont prises, mises en œuvre, surveillées et mesurées.
Elle garantit l'alignement avec les objectifs business, les exigences réglementaires et les menaces émergentes.
Elle intègre la gestion des risques, la protection des actifs, la gouvernance des identités et la sécurité des tiers dans les opérations quotidiennes, afin de favoriser une atténuation proactive des risques.

Elle contribue également à intégrer la sécurité dès la conception, à instaurer une culture du "security first" et à garantir une réponse aux incidents rapide et efficace.



02 Architecture de cybersécurité

Identifier

Il est également important d'évaluer techniquement votre posture de sécurité actuelle afin d'identifier les écarts et d'ajuster les contrôles de sécurité en conséquence.

Cette évaluation peut être réalisée de manière continue ou périodique, et couvrir de nombreux domaines, comme illustré ici.

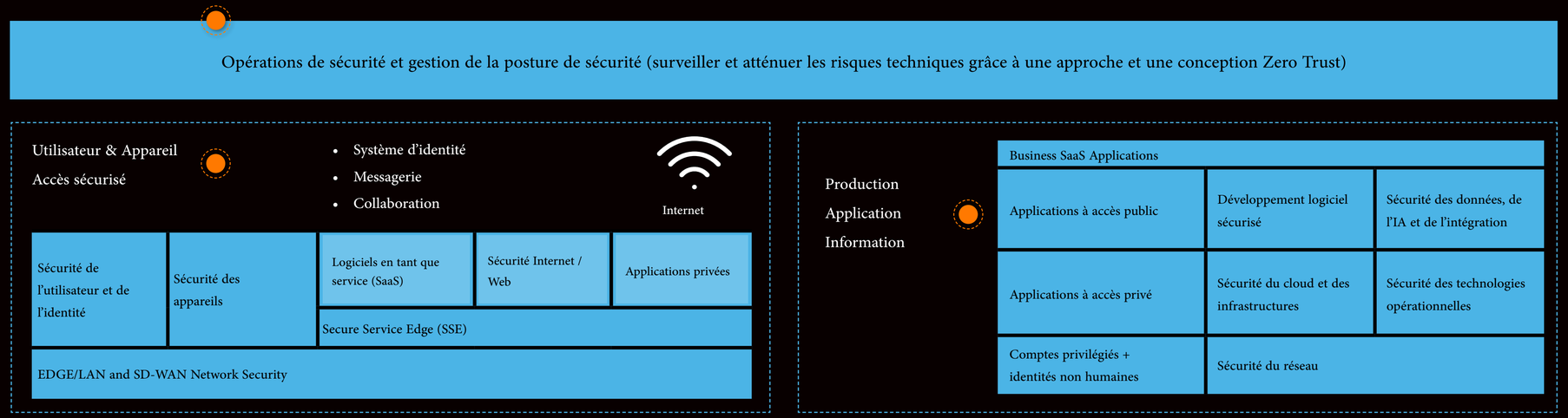
Lorsqu'elle est intégrée à l'architecture de sécurité, la veille sur les menaces fournit aux organisations des informations exploitables sur les menaces potentielles.

- Identification des actifs et des vulnérabilités
- Évaluations techniques
- Tests d'intrusion

02 Architecture de cybersécurité

Protection des opérations et de la posture de sécurité

Le maintien d'une posture de sécurité solide nécessite une surveillance, une adaptation et une amélioration continues, assurées par des professionnels de la sécurité qualifiés.
En identifiant et en traitant proactivement les vulnérabilités, les organisations peuvent garantir une protection robuste sur l'ensemble des domaines de sécurité.



02 Architecture de cybersécurité

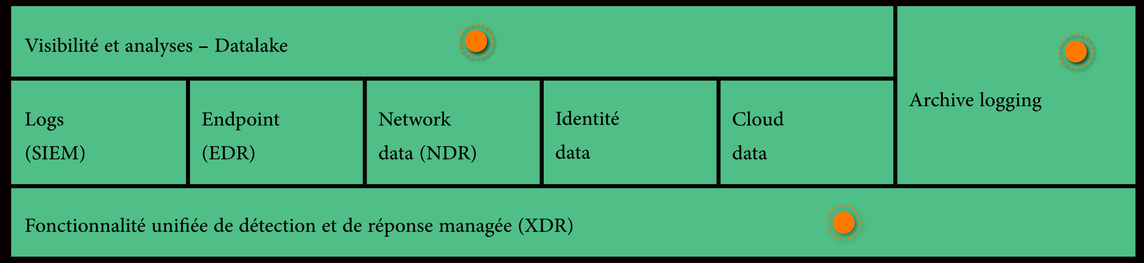
Capacités de détection

Des violations peuvent néanmoins survenir en raison de facteurs tels que des vulnérabilités zero-day, des erreurs humaines, des menaces internes ou d'autres risques imprévisibles.
Les capacités de détection sont essentielles pour identifier rapidement, réagir et gérer tout incident de sécurité potentiel.

En intégrant les données provenant de diverses sources — Endpoint Detection and Response, Network Detection and Response, systèmes d'identité, API cloud et journaux archivés, les organisations peuvent élaborer une stratégie de détection complète.

Cette approche permet aux équipes de sécurité de repérer les menaces précocement, d'agir rapidement et de minimiser l'impact de toute violation avant qu'elle ne s'aggrave.

Renseignement sur les menaces
Surveillance de la cybercriminalité



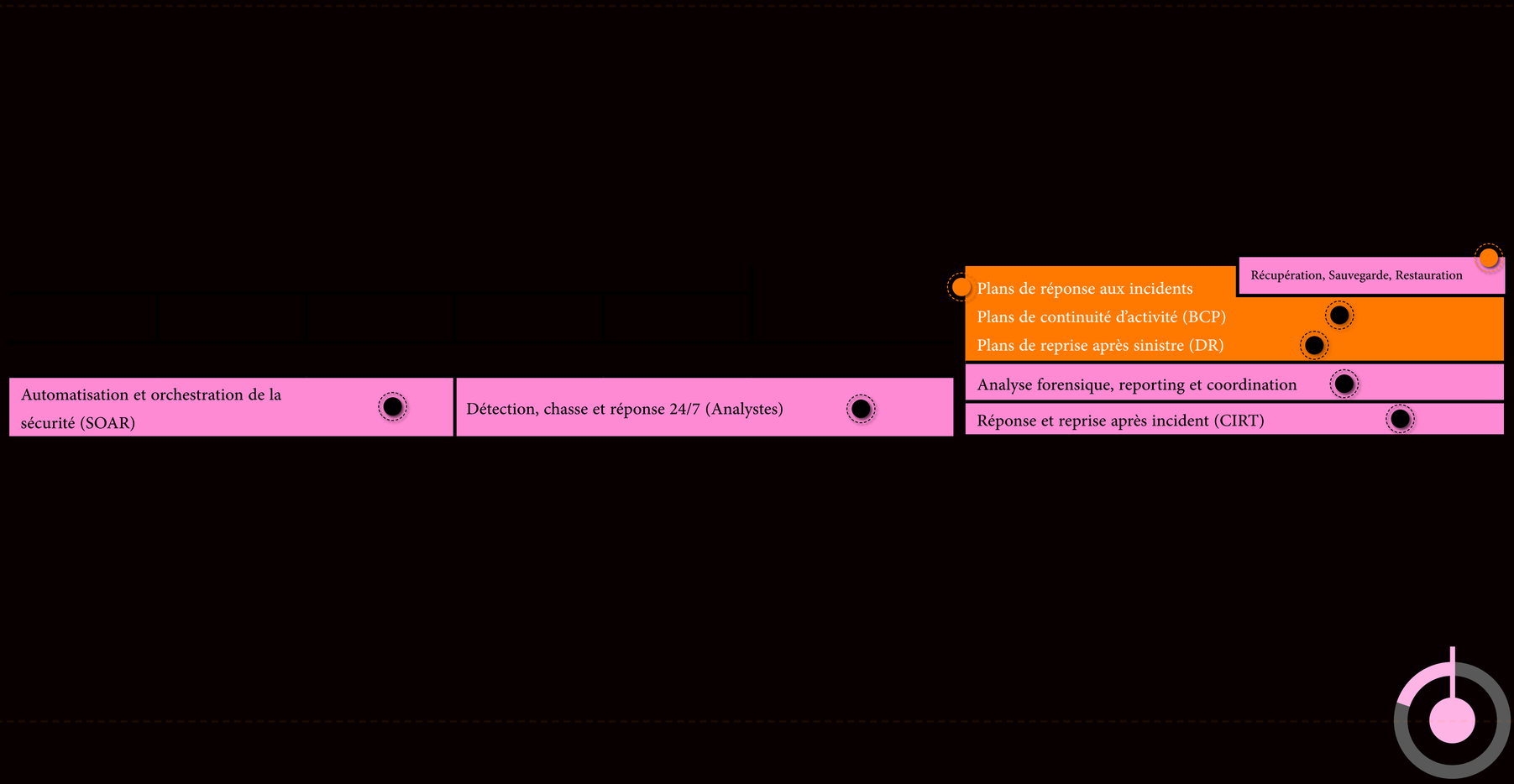
02 Architecture de cybersécurité

Réponse aux incidents

Si les capacités de détection sont essentielles pour identifier les menaces, la réponse aux incidents l'est tout autant. Les organisations doivent être prêtes à agir rapidement et efficacement lorsqu'une violation survient, afin de limiter les dégâts et d'assurer une reprise rapide.

L'architecture de réponse aux incidents doit être complète et holistique, couvrant l'ensemble des actions nécessaires en cas de violation de sécurité — de la détection jusqu'à la reprise. En intégrant l'automatisation, la surveillance continue, des capacités d'analyse forensique avancées, la planification de la continuité d'activité et des mesures de reprise efficaces, les organisations peuvent s'assurer d'être prêtes à faire face à tout défi en matière de cybersécurité.

Ce processus continu et circulaire renforce la posture de sécurité tout en accélérant la réponse et en améliorant l'agilité.



03 Fondements de la sécurité

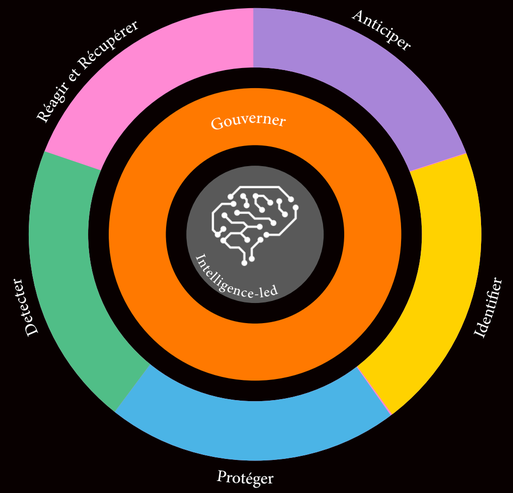
Bonnes pratiques d'hygiène cyber pour NIS 2

Les pratiques de sécurité essentielles, appelées facteurs d'hygiène cyber, constituent les fondations d'un environnement sécurisé.
Chaque organisation doit les mettre en œuvre pour protéger son infrastructure contre les menaces.
Elles garantissent la résilience, la conformité et la réduction des risques.

03 Fondements de la sécurité

Cybersécurité NIS 2 : bonnes pratiques d'hygiène cyber

Panorama des menaces
- Gestion des vulnérabilités
- Conseil en matière de menaces



Renseignement sur les menaces
Surveillance de la cybercriminalité

Priorités business

Risque lié à la sécurité de l'information

Exigences de conformité et contractuelles

Gouvernance de la cybersécurité – Gestion des risques, audits et évaluations, planification et hiérarchisation, indicateurs de performance (KPIs)

Gestion des actifs | Gestion des identités | Gestion de la chaîne d'approvisionnement | Sensibilisation et formation | Politiques et directives de sécurité

Data Gouvernance | Architecture continue Secure by Design et Secure by Default, intégrant une approche Zero Trust

Identification des actifs et des vulnérabilités, tests d'intrusion et évaluations techniques

Opérations de sécurité et gestion de la posture de sécurité (surveiller et atténuer les risques techniques grâce à une approche et une conception Zero Trust)

Utilisateur & Appareil
Accès sécurisé

- Système d'identité
- Messagerie
- Collaboration

Internet

Sécurité de l'utilisateur et de l'identité | Sécurité des appareils | Logiciels en tant que service (SaaS) | Sécurité Internet / Web | Applications privées

Secure Service Edge (SSE)

EDGE/LAN and SD-WAN Network Security

Production
Application
Information

Business SaaS Applications		
Applications à accès public	Développement logiciel sécurisé	Sécurité des données, de l'IA et de l'intégration
Applicationsà accès privé	Sécurité du cloud et des infrastructures	Sécurité des technologies opérationnelles
Comptes privilégiés + identités non humaines	Sécurité du réseau	

Visibilité et analyses – Datalake

Logs (SIEM) | Endpoint (EDR) | Network data (NDR) | Identité data | Cloud data

Archive logging

Fonctionnalité unifiée de détection et de réponse managée (XDR)

Automatisation et orchestration de la sécurité (SOAR) | Détection, chasse et réponse 24/7 (Analystes)

Récupération, Sauvegarde, Restauration

Plans de réponse aux incidents
Plans de continuité d'activité (BCP)
Plans de reprise après sinistre (DR)

Analyse forensique, reporting et coordination

Réponse et reprise après incident (CIRT)

03 Fondements de la sécurité

La directive Cybersécurité NIS 2 constitue également une référence en matière de mesures minimales de cybersécurité que les entreprises doivent déployer.

Ces mesures clés incluent :

01

Gestion des risques :
Seules les entités essentielles (EE) doivent mettre en place des mesures pour réduire les risques cyber, notamment la gestion des incidents, le renforcement de la sécurité de la chaîne d'approvisionnement, l'amélioration de la sécurité des réseaux, un meilleur contrôle des accès et le chiffrement.

02

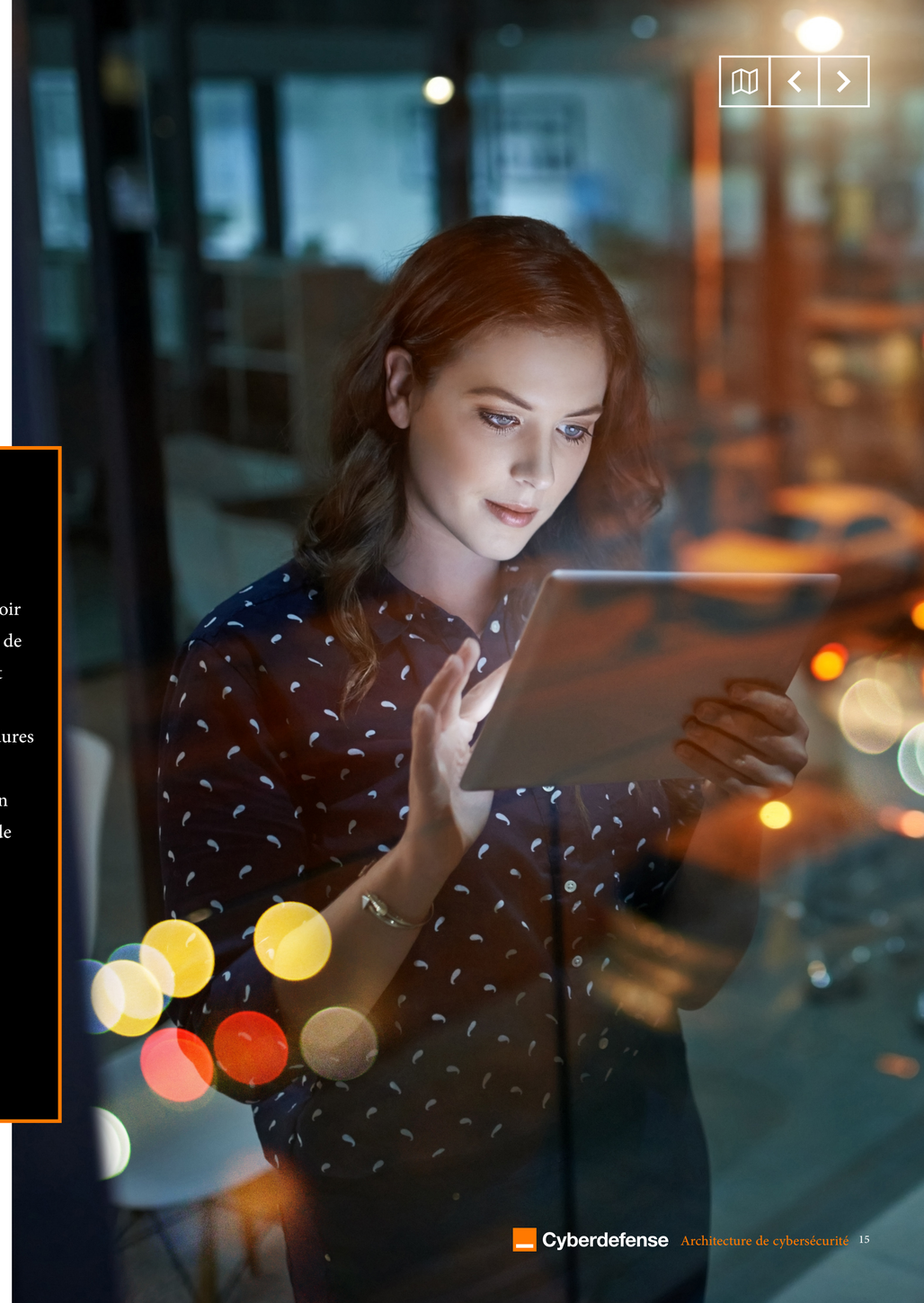
Responsabilité de l'entreprise :
NIS2 impose aux dirigeants de superviser, valider et suivre une formation sur les mesures de cybersécurité mises en place au sein de leur organisation, ainsi que de gérer les risques cyber.
En cas de manquement, des sanctions peuvent s'appliquer à la direction, incluant la responsabilité personnelle et des interdictions temporaires d'exercer des fonctions de gestion.

03

Obligations de signalement :
Les entités essentielles et importantes doivent disposer de processus permettant de signaler rapidement tout incident de sécurité ayant un impact significatif sur la fourniture de leurs services ou sur leurs utilisateurs.
NIS2 définit des délais précis de notification, notamment un "early warning" dans les 24 heures.

04

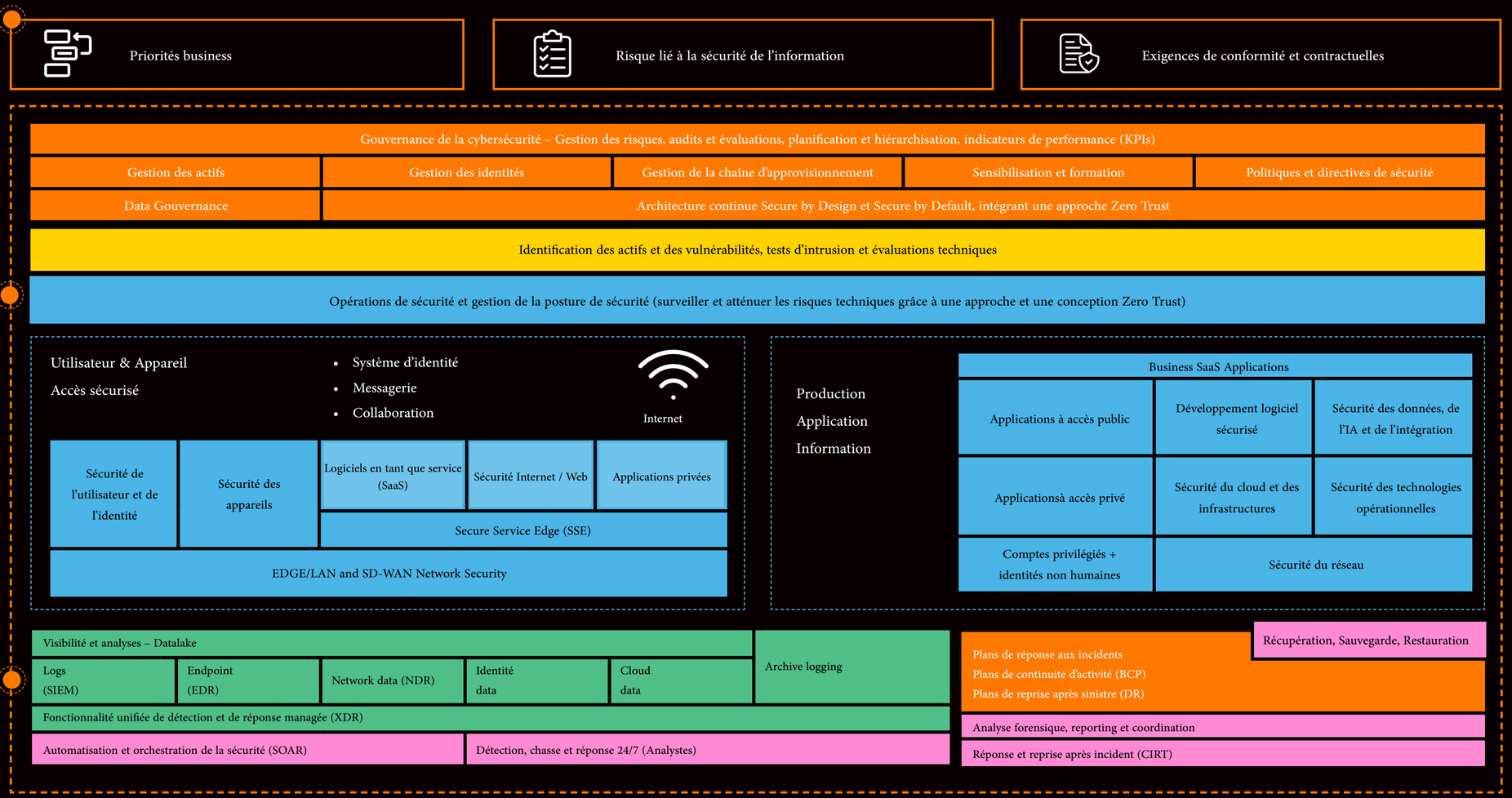
Continuité d'activité :
Les organisations doivent prévoir comment assurer la continuité de leurs activités en cas d'incident cyber majeur.
Ce plan doit inclure les procédures de reprise des systèmes, les mesures d'urgence et la mise en place d'une cellule de gestion de crise.



03 Fondements de la sécurité

Mesures minimales de sécurité exigées par NIS 2

NIS2 exige que toutes les entités essentielles et importantes mettent en place un ensemble minimal de mesures techniques, opérationnelles et organisationnelles afin de gérer les risques cyber et d'assurer la continuité d'activité.
Ces mesures ne sont pas ponctuelles : elles doivent être continues, proportionnées et fondées sur l'évaluation des risques.



03 Fondements de la sécurité

Mesures de sécurité minimales :

NIS 2 impose aux entités essentielles et importantes de mettre en œuvre des mesures de sécurité de base pour faire face aux principales formes de menaces cyber probables. Ces mesures visent à renforcer et à harmoniser les pratiques de cybersécurité entre les États membres de l'Union européenne, en corrigeant les limites de la première directive NIS.

Celles-ci incluent :

- Évaluations des risques et politiques de sécurité pour les systèmes d'information
- Politiques et procédures d'évaluation de l'efficacité des mesures de sécurité
- Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
- Un plan de gestion des incidents de sécurité
- Sécurité liée à l'acquisition, au développement et à l'exploitation des systèmes
- Formation en cybersécurité et bonnes pratiques d'hygiène informatique
- Procédures de sécurité pour les employés ayant accès à des données sensibles ou importantes
- Une vue d'ensemble de tous les actifs concernés et la garantie qu'ils sont correctement utilisés et gérés
- Un plan de gestion des opérations pendant et après un incident de sécurité
- L'utilisation de l'authentification multifacteur, de solutions d'authentification continue, du chiffrement des communications vocales, vidéo et textuelles, ainsi que du chiffrement des communications internes d'urgence, lorsque cela est approprié.
- Sécurité des chaînes d'approvisionnement et des relations entre l'entreprise et ses fournisseurs directs

04 Support NIS 2

L'architecture de cybersécurité d'Orange Cyberdefense au service de la directive NIS 2

Nous pouvons aligner nos offres sur une architecture de cybersécurité complète afin de répondre à l'ensemble des exigences clés de la directive NIS 2.

Services de conseil en gouvernance, gestion des risques et conformité (GRC)

- Évaluer la posture de sécurité actuelle et identifier les écarts de conformité avec NIS 2.
- Cela implique de réaliser des évaluations des risques, de mettre en œuvre des politiques de sécurité et de garantir la protection des actifs critiques.
- Les experts GRC apportent des conseils stratégiques et un soutien technique pour aider à naviguer dans un environnement réglementaire complexe et maintenir la conformité.

Services de sécurité managés (MSS)

- Assurer la surveillance et la protection continues des environnements informatiques.
- Cela inclut la détection et la réponse managées aux menaces (Managed Threat Detection and Response), qui offrent des capacités de surveillance et de réponse aux incidents 24/7 pour détecter et atténuer les menaces potentielles.
- Le service Incident Response Retainer garantit le déploiement rapide d'équipes d'experts pour gérer et résoudre efficacement les incidents cyber.

Services d'Ethical Hacking et de tests d'intrusion

- Identifier les vulnérabilités à travers les systèmes et les réseaux.
  En simulant de véritables cyberattaques, nos experts en Ethical Hacking révèlent les faiblesses et fournissent des recommandations concrètes pour renforcer les mesures de sécurité.
- Cela prépare proactivement les organisations à se défendre contre les menaces potentielles et à se conformer aux exigences de NIS 2.

Sécurité de l'IA

- Nous vous aidons à intégrer l'intelligence artificielle de manière pertinente, cas d'usage par cas d'usage, au sein de votre cadre NIS 2. L'objectif est de renforcer les mesures de cybersécurité à l'échelle de l'ensemble de l'architecture.
- Nos solutions pilotées par l'IA offrent une détection avancée des menaces, une surveillance en temps réel et des mécanismes de défense proactifs, garantissant la conformité aux normes de sécurité strictes de NIS 2.

Programmes de formation et de sensibilisation

- S'assurer que les employés appliquent les meilleures pratiques de cybersécurité et comprennent leur rôle dans le maintien d'un environnement sécurisé.
- Des sessions de formation régulières et des pratiques d'hygiène cyber permettent aux organisations de garder une longueur d'avance sur les menaces émergentes et de maintenir leur conformité à NIS 2.

04 Support NIS 2

Sécurité de l'IA

L'IA se déploie partout, mais la sécurité ne s'y adapte pas toujours.
Avec les plateformes SaaS sous licence des grands fournisseurs comme Microsoft, Google ou AWS, une grande partie de la sécurité est prise en charge par ces derniers, mais vous restez toujours responsable des risques liés à la gouvernance des données et aux accès.
Si vous exécutez vous-même les applications d'IA, vous devez alors prendre en compte l'ensemble des risques associés

Gouvernance de l'IA

- Assurez-vous de connaître la sensibilité des données accessibles par l'IA.
- Appliquez les contrôles appropriés.
- Limitez l'impact de l'IA.

- Les risques liés à l'usage de l'IA incluent les attaques par contournement, les prompt injections, la divulgation de données sensibles, le vol de modèle et les scénarios de déni de service.
- Les risques liés au développement de l'IA concernent l'empoisonnement des données, les vulnérabilités de la chaîne d'approvisionnement et les fuites d'informations sensibles.
- Les risques de sécurité à l'exécution de l'IA incluent la sécurisation de l'infrastructure sur laquelle elle fonctionne, l'empoisonnement ou le vol de modèle, ainsi que les attaques par injection.

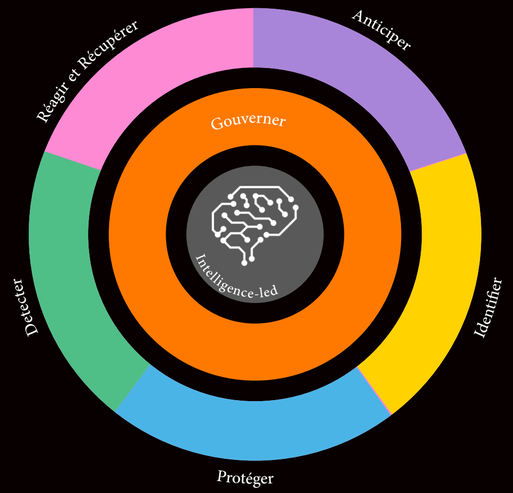
Pour contrer ces risques, les organisations doivent appliquer des pratiques de développement sécurisé de l'IA, mettre en place des mécanismes de supervision, valider les résultats et garantir la transparence ainsi que l'explicabilité de l'IA.

04 Support NIS 2

Cybersécurité : aperçu des services et des domaines

NIS 2

Panorama des menaces
- Gestion des vulnérabilités
- Conseil en matière de menaces



Renseignement sur les menaces
Surveillance de la cybercriminalité

Priorités business

Risque lié à la sécurité de l'information

Exigences de conformité et contractuelles

Gouvernance de la cybersécurité – Gestion des risques, audits et évaluations, planification et hiérarchisation, indicateurs de performance (KPIs)

Gestion des actifs | Gestion des identités | Gestion de la chaîne d'approvisionnement | Sensibilisation et formation | Politiques et directives de sécurité

Data Gouvernance | Architecture continue Secure by Design et Secure by Default, intégrant une approche Zero Trust

Identification des actifs et des vulnérabilités, tests d'intrusion et évaluations techniques

Opérations de sécurité et gestion de la posture de sécurité (surveiller et atténuer les risques techniques grâce à une approche et une conception Zero Trust)

Utilisateur & Appareil
Accès sécurisé

- Système d'identité
- Messagerie
- Collaboration

Internet

Sécurité de l'utilisateur et de l'identité | Sécurité des appareils | Logiciels en tant que service (SaaS) | Sécurité Internet / Web | Applications privées

Secure Service Edge (SSE)

EDGE/LAN and SD-WAN Network Security

Production
Application
Information

Business SaaS Applications

Applications à accès public	Développement logiciel sécurisé	Sécurité des données, de l'IA et de l'intégration
Applicationsà accès privé	Sécurité du cloud et des infrastructures	Sécurité des technologies opérationnelles
Comptes privilégiés + identités non humaines	Sécurité du réseau	

Visibilité et analyses – Datalake

Logs (SIEM) | Endpoint (EDR) | Network data (NDR) | Identité data | Cloud data

Archive logging

Fonctionnalité unifiée de détection et de réponse managée (XDR)

Automatisation et orchestration de la sécurité (SOAR) | Détection, chasse et réponse 24/7 (Analystes)

Récupération, Sauvegarde, Restauration

Plans de réponse aux incidents
Plans de continuité d'activité (BCP)
Plans de reprise après sinistre (DR)

Analyse forensique, reporting et coordination

Réponse et reprise après incident (CIRT)

04 Support NIS 2

Actions clés pour un environnement OT sécurisé et conforme

Les technologies opérationnelles (OT) sont un élément essentiel de la directive NIS2, car elles garantissent l'intégration fluide et le bon fonctionnement des systèmes industriels, indispensables au maintien de l'efficacité et de la sécurité des opérations.

Avec la bonne stratégie, la conformité NIS 2 représente une opportunité de pérenniser vos systèmes OT.
L'adoption d'une approche proactive garantit une sécurité renforcée, une réduction des risques et une résilience durable de l'environnement OT.

Comprendre et cartographier votre environnement OT

- Réaliser une évaluation exploratoire pour identifier les risques cyber.
- Cartographier les actifs critiques, les vulnérabilités et les interdépendances.

Déployer des mesures de cybersécurité robustes

- Segmenter les réseaux pour isoler les environnements IT et OT.
- Appliquer l'authentification multifacteur pour les accès à distance.
- Déployer la détection d'intrusion en temps réel et la surveillance continue.

Élaborer une stratégie de réponse aux incidents résiliente

- Définir des protocoles clairs pour les menaces propres à l'OT.
- Garantir une détection, un confinement et une reprise rapides.
- Organiser des formations et des exercices de simulation réguliers.

Sécuriser votre chaîne d'approvisionnement

- Évaluer la posture de sécurité et les risques des tiers.
- Intégrer les exigences de conformité NIS 2 dans les contrats.
- Surveiller en continu les vulnérabilités des fournisseurs.

Aligner la gouvernance sur les exigences de conformité

- Nommer un responsable dédié à la conformité NIS 2.

Maintenir des politiques de sécurité et une documentation complètes

- Garantir le signalement rapide des incidents dans un délai de 24 heures, comme l'exige la réglementation.

Mettre en place une surveillance continue et renforcer la résilience

- Mettre en œuvre la détection des anomalies en temps réel sur l'ensemble des systèmes OT.
- Mettre régulièrement à jour et corriger les vulnérabilités logicielles.
- Favoriser une culture de la cybersécurité grâce à des formations continues.

05 Pourquoi Orange Cyberdefence

Pourquoi Orange Cyberdefense

- Présence locale et portée mondiale : assurez la conformité avec les réglementations régionales tout en bénéficiant d'une expertise mondiale
- Solutions évolutives et fiables : adaptez-vous aux exigences réglementaires en constante évolution grâce à des services de sécurité éprouvés et évolutifs
- Approche holistique : abordez la conformité en intégrant les personnes, les processus et la technologie au sein de votre stratégie de sécurité
- Sécurité fondée sur l'intelligence : respectez proactivement les normes de conformité grâce aux informations issues de plus de 500 sources de renseignement sur les menaces
- Opérations résilientes : plusieurs centres de prestation de services de sécurité à travers le monde garantissent une surveillance et une réponse continues, soutenant ainsi le respect des obligations réglementaires
- Excellence certifiée : les certifications ISO 27001, SOC 2 et CREST s'alignent sur les cadres de conformité les plus reconnus du secteur
- Un partenariat tourné vers l'avenir : anticipez les évolutions réglementaires avec un MSSP de confiance, reconnu à l'échelle mondiale

Prêt à naviguer dans la conformité NIS 2 et à vous préparer pour l'avenir ?

Assurer la conformité à NIS2 et sécuriser les infrastructures critiques peut représenter un défi complexe, surtout face à l'évolution constante des menaces cyber et au renforcement des exigences réglementaires.
Orange Cyberdefense met à votre disposition les compétences, les technologies et l'accompagnement stratégique nécessaires pour bâtir une entreprise résiliente et agile, conforme aux exigences d'aujourd'hui et prête à relever les défis de demain.

Contactez-nous dès aujourd'hui pour découvrir comment nous pouvons vous aider à naviguer dans la conformité NIS2 et à renforcer votre posture de cybersécurité.


orange
Cyberdefense