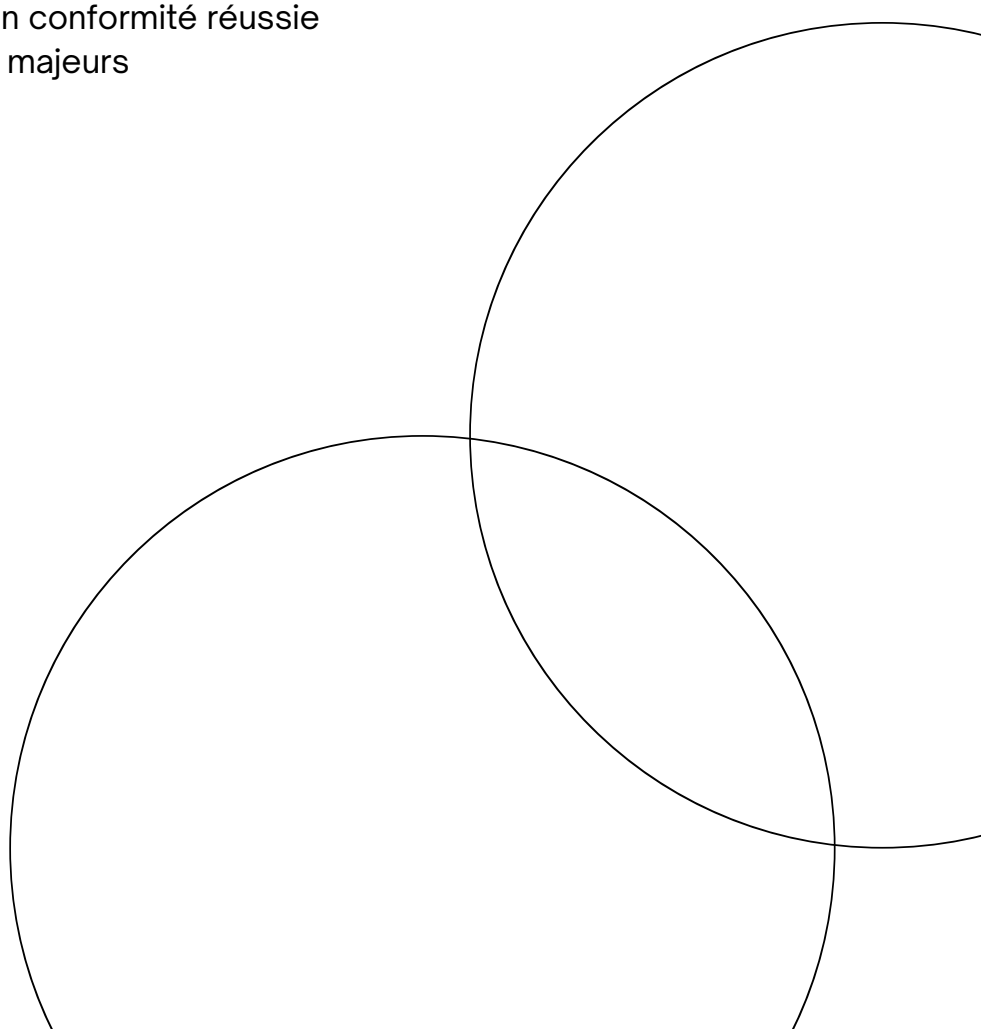
NIS 2 : mode d'emploi pour une conformité assurée

squad

Sommaire



Edito

Le constat est sans appel. Près d'une entreprise sur deux (47 %) a subi au moins une cyberattaque réussie en 2024. Une tendance à la hausse qui ne risque pas de s'inverser, l'Hexagone ayant enregistré +40 % d'atteintes numériques en 5 ans !

Désormais, dans un contexte de fortes tensions géopolitiques, plus aucun secteur, ni organisme n'est épargné. Les grandes entreprises ne sont plus les seules visées, bien au contraire. Parmi les raisons : l'émergence de l'IA générative facilitant notamment les campagnes de phishing. Or, malgré l'explosion des usages d'intelligence artificielle, seules 22 % des entreprises ont mis en place des mesures de cybersécurité adaptées.

Résultat, les plus petites entreprises comme les collectivités, disposant souvent de moins de ressources, ouvrent la porte de leurs systèmes d'information aux failles de sécurité et par la même occasion aux cybercriminels. Quant aux grandes entreprises, moins agiles, elles sont peut-être plus avancées dans leur transformation mais elles doivent souvent composer avec des infrastructures obsolètes et des métiers peu enclins au changement.

En réponse, l'Union européenne a alors décidé d'étendre sa directive NIS 1 (Network and Information Security – ou en français, sécurité des réseaux et des systèmes d'information) pour couvrir un champ beaucoup plus large de domaines et d'entités. Officiellement entrée en vigueur en Europe le 17 octobre 2024, elle devrait être adoptée par la France courant 2025 avec quelques ajustements.

Une adaptation à laquelle participe Yoann Moreau, Head of Cybersecurity Audit & Advisory chez SQUAD. En tant qu'interlocuteur privilégié de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'autorité en charge de la transposition NIS 2 pour la France, Yoann Moreau a participé à de nombreuses tables rondes afin de formaliser la transposition française de la règlementation européenne. Une proximité et une expertise qui rendent les équipes Squad particulièrement au fait des différentes mesures devant être déclinées par l'ensemble de l'écosystème concerné par cette directive, et en ce sens, font d'elles les plus à même de vous accompagner dans votre projet de mise en conformité.

Il n'est pas trop tard ! Pour vous accompagner dans votre démarche, nos experts partagent leur retour d'expérience et leurs bonnes pratiques.
Bonne lecture !

PREMIÈRE PARTIE

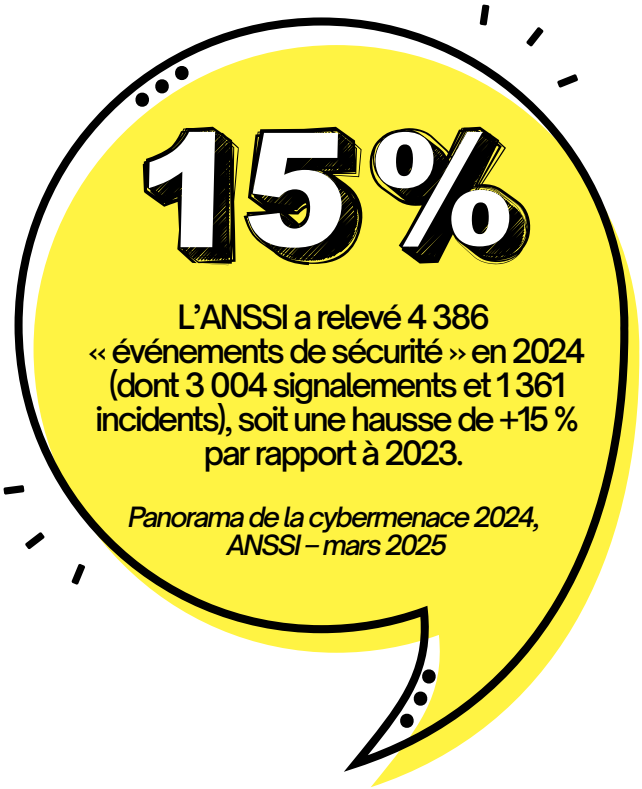
NIS 2 : décryptage et enjeux

La directive NIS 2 répond à l'augmentation de la menace cyber en Europe. Publiée au Journal Officiel de l'Union européenne en décembre 2022 et entrée en vigueur dans plusieurs pays européens le 17 octobre 2024, elle marque une évolution notable dans la protection des réseaux et des systèmes servant à fournir des services essentiels dans les secteurs clés.

De NIS 1 à NIS 2 : genèse et évolution

Adoptée en juillet 2016, NIS 1 permettait d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne (UE). Alors pourquoi NIS 2 ? Comme indiqué sur le site officiel[1] :

« L'enjeu de NIS 2 est de mieux protéger les réseaux et les systèmes d'information servant à fournir des services essentiels dans les secteurs clés de nos sociétés. Alors que la première directive NIS visait à protéger les acteurs économiques majeurs de l'UE, cette nouvelle directive élargit le champ des entités et secteurs concernés et introduit des exigences plus adaptées, notamment au regard du renforcement de la menace cyber. Elle prévoit un socle de mesures juridiques, techniques et organisationnelles que les futures entités régulées devront mettre en œuvre, en fonction du risque existant, afin d'élever leur niveau général de cybersécurité et d'accroître leur résilience opérationnelle.»



Qu'est-ce qui change entre NIS 1 et NIS 2 ?

Les évolutions les plus notables concernent principalement :

- Le périmètre d'application de la directive, considérablement élargi à d'autres secteurs et organismes (collectivités territoriales, administrations publiques, moyennes entreprises et grandes entreprises) ;
- La sévérité des sanctions imposées en cas de non-conformité ;
- Et la définition d'exigences plus exigeantes en matière de cybersécurité pour mieux répondre aux menaces toujours plus nombreuses et sophistiquées.

« Avant 2016, chaque pays européen gérait la cybersécurité à son échelle nationale. NIS 1 avait pour ambition de mieux coordonner la gestion des risques, de fournir des guidelines claires et précises pour toutes les organisations, qu'elles soient transnationales ou non, et d'homogénéiser les pratiques en matière de cybersécurité. Son objectif était d'homogénéiser le niveau de maturité cyber dans l'ensemble des pays européens. Mais la directive n'allait pas assez loin et de plus en plus d'entreprises non initialement ciblées en tant qu'opérateurs de services essentiels ont été touchées par des cyberattaques. D'où la nécessité d'étendre le périmètre des secteurs et des entreprises concernées. NIS 2 permet ainsi de multiplier le nombre d'organisations ciblées par dix, passant de 15 000 entreprises européennes concernées par NIS 1 à 160 000. »

Yoann Moreau,
Head of Cybersecurity Audit & Advisory, SQUAD

Qui est concerné ?

Nouveaux secteurs, abaissement de la taille des entreprises concernées à 50 salariés, la directive NIS 2 augmente considérablement le nombre d'acteurs désormais sommés par l'obligation de répondre à des exigences de sécurisation de leurs systèmes d'information.

Les entités directement impliquées par NIS 2 se répartissent en deux catégories :

- 10 secteurs dits essentiels ;
- Et 8 secteurs dits importants.

Chacun de ces secteurs doit répondre à un certain nombre d'obligations au regard de son niveau de criticité.

Secteurs hautement critiques	Autres secteurs critiques
Administrations publiques	Fabrication, production et distribution de produits chimiques
Eau potable	Fournisseurs numériques
Eaux usées	Gestion des déchets
Énergies	Industrie manufacturière

Secteurs hautement critiques	Autres secteurs critiques
Espace	Production, transformation et distribution de denrées alimentaires
Gestion des services Technologies de l'Information et de la Communication (interentreprises)	Recherche
Infrastructures des marchés financiers	Services postaux et d'expédition
Infrastructures numériques	
Santé	
Secteur bancaire	
Transports	

Désormais, les organisations sont réparties en deux catégories selon leur degré de criticité, leur taille et leur chiffre d'affaires :

- **Les Entités Essentielles (EE)**, déjà concernées par NIS 1, avec un minimum de 250 collaborateurs et un chiffre d'affaires supérieur à 50 M€ ou un bilan annuel d'au moins 43 millions d'euros ;
- **Et les Entités Importantes (EI)**, pour les organisations nouvellement intégrées au périmètre NIS 2, soit un minimum de 50 collaborateurs et un chiffre d'affaires ou un bilan annuel de 10 M€.

« Les mesures de sécurité les plus complexes à implémenter et imposées par NIS 2 sont désormais d'applications obligatoires pour les Entités Essentielles, là où les entités dites importantes bénéficient d'une certaine souplesse. Plus précisément, l'ANSSI a traduit l'intégralité des mesures présentes au niveau de l'article 21 européen[1] en 20 objectifs de sécurité avec un mécanisme de proportionnalité. En somme, les Entités Importantes doivent mettre en place un certain nombre de mesures parmi les 20 proposées pour assurer leur résilience et leur robustesse face aux cyberattaques, alors que les Entités Essentielles, qui disposent de moyens et de capacités supplémentaires, vont devoir appliquer la totalité. En revanche, il est un point sur lequel toutes les entités, quelles qu'elles soient, doivent se conformer : c'est la sécurisation de leur supply chain. »

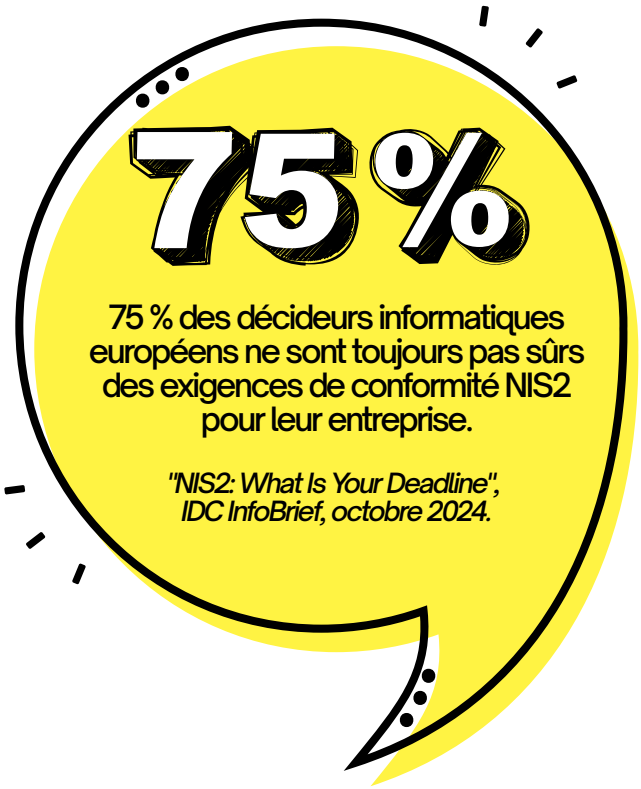
Yoann Moreau,
Head of Cybersecurity Audit & Advisory, SQUAD

Quelles obligations pour les entreprises ?

1. LE PARTAGE D'INFORMATIONS

Les entités incluses dans le périmètre NIS 2 sont dans l'obligation de fournir un certain nombre d'informations à l'autorité nationale définie, soit l'ANSSI pour la France, et de les mettre à jour. Elles doivent par conséquent stocker et archiver leurs rapports d'audit notamment pour être en mesure de les présenter en cas de contrôle ou d'incident. Ces informations peuvent alors servir de preuve de conformité ou témoigner de la remédiation de la vulnérabilité.

La sensibilisation et la formation des collaborateurs sont également des prérequis comme le stipule l'article 20 de la directive européenne :
« Les États membres veillent à ce que les membres des organes de direction des Entités Essentielles et importantes soient tenus de suivre une formation, et encouragent les Entités Essentielles et importantes à proposer régulièrement une formation similaire à leurs employés, afin qu'ils acquièrent des connaissances et des compétences suffisantes pour leur permettre d'identifier les risques et d'évaluer les pratiques de gestion des risques liés à la cybersécurité et leur impact sur les services fournis par l'entité. »



2. LA GESTION DES RISQUES CYBER

La gestion des risques est l'élément central de la directive NIS 2. Les entités sont ainsi dans l'obligation de mettre en place des mesures à la fois juridiques, techniques et organisationnelles pour sécuriser leurs réseaux et leurs systèmes d'information.
Selon l'article 21 : « Les États membres veillent à ce que les Entités Essentielles et importantes prennent des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui pèsent sur la sécurité des réseaux et des systèmes d'information que ces entités utilisent pour leurs activités ou pour la fourniture de leurs services, et pour prévenir ou réduire au minimum l'impact des incidents sur les destinataires de leurs services et sur d'autres services. »

Plus précisément, les organismes doivent adopter des mesures proportionnelles aux risques encourus, au regard de leur taille, de leur degré d'exposition aux risques lié à leurs activités, du risque de gravité et de la probabilité d'occurrence d'incidents, incluant l'impact sociétal et économique que ceux-ci pourraient avoir. Ces mesures peuvent prendre la forme de procédures de gestion des incidents, du renforcement de la sécurité tout au long de la chaîne d'approvisionnement, ou de dispositifs de contrôle d'accès et de chiffrement.

3. LA DÉCLARATION D'INCIDENTS

En cas d'incident de sécurité, l'entité est tenue de remonter l'information à l'autorité nationale de référence au plus tard 24 heures après avoir eu connaissance du cyber-incident. Elle doit également préciser son impact, et fournir au plus tard 72 heures après un rapport complet des actions mises en place et un état des lieux précis de l'évolution de la situation. Ce document initial doit être suivi un mois après l'incident d'un rapport final attestant du plan de reprise d'activité (PRA) mis en œuvre.
Selon l'article 23, « un incident est considéré comme significatif si :
(a) il a causé ou est susceptible de causer une grave perturbation opérationnelle des services ou une perte financière pour l'entité concernée ;
(b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels ou immatériels considérables. »
En conséquence, à travers ces obligations, l'Union européenne exige des entités d'atteindre un haut niveau de maturité à quatre niveaux :

- La gouvernance de l'entreprise ;
- La protection des systèmes ;
- La cybersécurité ;
- Et la résilience.

« La résilience au sens NIS2 peut se traduire par l'assurance que toutes les interconnexions vis-à-vis de la supply chain soient suffisamment sécurisées/robustes et que la sensibilisation des collaborateurs et des tierces parties est bien réalisée. L'idée ici est donc de couvrir toute la chaîne de production, y compris les fournisseurs, pour éviter d'atteindre un service essentiel via un tiers. Le 2e vecteur différenciant de NIS 2 porte sur la gestion de crise et plus précisément la préparation à la gestion de crise, jusque-là absente de la plupart des règlementations. NIS 2 fait en sorte que cet élément redevienne central. Le but n'est pas de savoir si les entreprises vont être attaquées, mais de préparer leur capacité de gérer une cyberattaque quand elle arrivera. Tous ces points – défense, préparation à la gestion de crise, conception de fiches réflexes, résilience et robustesse des systèmes vis-à-vis de cyberattaques – sont extrêmement importants à mettre en place. »

Yoann Moreau,
Head of Cybersecurity Audit & Advisory, SQUAD

Les sanctions en cas de non conformité.

Comme pour le règlement général sur la protection des données (RGPD), NIS 2 intègre aussi, en cas de non-conformité, des pénalités de plusieurs types.

Les pénalités non financières

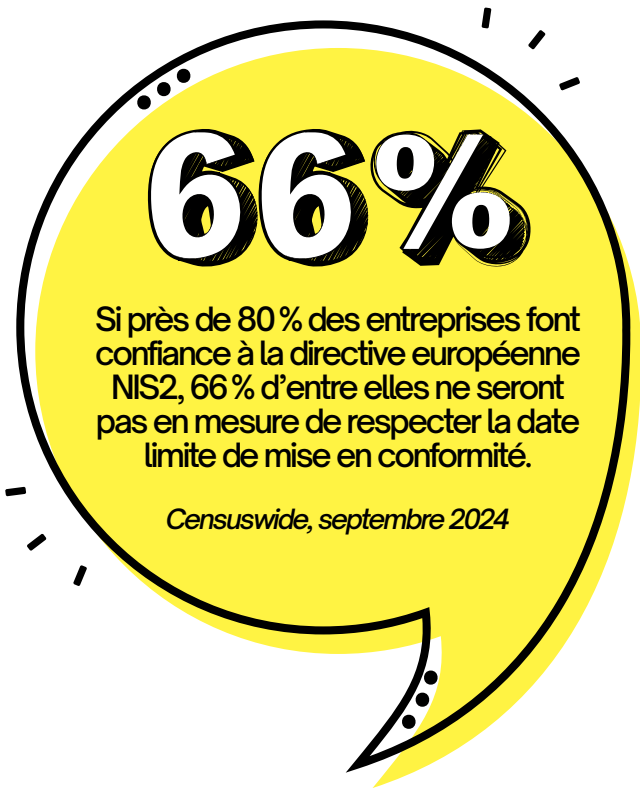
Il est possible d'un point de vue juridique d'imposer à l'entreprise la mise en conformité immédiate de certains systèmes sous un mois. Si celle-ci refuse de coopérer, un message sera envoyé à l'ensemble de ses clients pour les prévenir de sa non-conformité à NIS 2 et que, par conséquent, l'entreprise est à risque.

Cette mesure s'accompagne d'une publication au Journal Officiel pouvant engendrer un fort impact négatif sur l'image de marque des entreprises CAC40. Il sera alors impossible de travailler avec ces entreprises.

Les sanctions visant le PDG de l'entreprise

Tout directeur doit s'assurer qu'un chantier de mise en conformité des systèmes dont il a la responsabilité a été lancé.

Dans le cas inverse, la personne ne pourra plus exercer de fonction de direction dans toute entreprise européenne pendant 2 à 5 ans, l'entreprise qui l'embauche pourrait elle aussi être sanctionnée. Le fait désormais de toucher à la personne physique et pas que morale opère un changement majeur par rapport aux autres directives européennes.



Les pénalités financières

- Pour les Entreprises Essentielles, l'amende minimale est 10 M€ ou 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.
- Pour les Entreprises Importantes, le système est identique mais avec un palier moindre : l'amende est au minimum de 7 M€ ou équivalent à 1% du chiffre d'affaires si celui-ci dépasse 7 M€.

« Les entreprises non conformes risquent fort de perdre des parts de marché, voire de disparaître au vu de la sévérité des mesures. Mais, à l'inverse, pour les entreprises qui seront en conformité, NIS 2 s'impose comme un moteur de compétitivité majeur. Les entreprises françaises ont donc à peu près deux ans pour se mettre en conformité car l'ANSSI s'est engagée pendant cette période à ne pas sanctionner les entreprises dites essentielles ou importantes au titre de NIS2 pour leur laisser le temps de mettre en place les mesures nécessaires. Mais attention car cet engagement ne s'applique qu'au niveau national. Les entreprises transnationales peuvent potentiellement être auditées au sein de l'Union européenne d'ici fin 2025. Elles ne sont donc pas à l'abri d'une sanction. »

Yoann Moreau,
Head of Cybersecurity Audit & Advisory, SQUAD

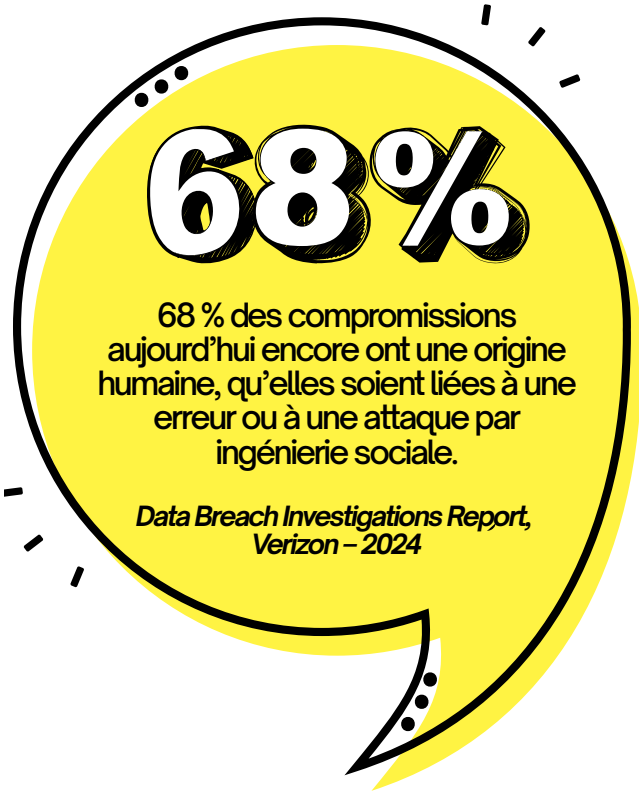
DEUXIÈME PARTIE

Comment s’y conformer ?

NIS 2 entraîne un véritable changement de paradigme. Pourquoi ?
Parce que c’est désormais à la société de fournir les preuves de sa conformité et non aux auditeurs de les rechercher. Par conséquent, les entreprises doivent disposer à tout moment de l’ensemble des preuves pour pouvoir prouver leur conformité totale avec l’ensemble des mesures qui les concernent et, par extension, une conformité globale à l'objectif de sécurité.

Les principaux défis des entreprises

Dans ce contexte, les entreprises font face à de nombreux défis pour répondre aux obligations induites par la directive NIS 2. Pour rappel, elles vont devoir établir un état des lieux du niveau de sécurité de leurs systèmes d'information et réseaux, et mettre en place des mesures concrètes pour assurer leur conformité sur les plans technologique, organisationnel et juridique.



1. LE PARTAGE D'INFORMATIONS

L'entreprise doit documenter précisément les mesures qu'elle a prises afin d'assurer la conformité de ses systèmes, et en informer l'ANSSI en cas de contrôle ou de demande de preuve lors d'un incident cyber.

Cette documentation n'est pas exhaustive mais doit inclure a minima l'ensemble des éléments cités dans le paragraphe précédent, c'est-à-dire les contrats établis avec des tiers intervenant le long de la supply chain (fournisseurs, sous-traitants, partenaires, etc.), le rapport d'audit interne, le plan de reprise d'activité (PRA), la liste des formations et des certifications des équipes IT en charge de la sécurité, etc.

2. LA GESTION DES RISQUES CYBER

Une gestion efficace des risques cyber implique la mise en œuvre d'un certain nombre de mesures de sécurité selon l'infrastructure en place. Mais cette gestion ne s'effectue pas que sur le seul plan technique, et ne s'arrête pas aux seuls systèmes et réseaux de l'entité. Elle intègre en effet une analyse des risques au niveau de l'écosystème complet de l'entreprise, incluant notamment les fournisseurs et les sous-traitants dont les systèmes peuvent être en interaction avec ceux de l'entreprise.

C’est ici aussi que les campagnes de sensibilisation et les programmes de formation des collaborateurs prennent toute leur importance, la plupart des risques cyber ayant une origine humaine. Les tests de vulnérabilité et le plan de reprise d’activité (PRA), comprenant un environnement de secours et une sauvegarde opérationnelle, constituent eux aussi des prérequis.

3. LA DÉCLARATION D’INCIDENTS

Les Entités Essentielles et les Entités Importantes ont désormais l’obligation d’alerter l’autorité de contrôle en cas de détection d’une attaque ou d’une faille de sécurité. C’est pourquoi, elles doivent anticiper en établissant un plan de gestion des incidents capable d'identifier les incidents de sécurité, d'y remédier et d'y répondre rapidement.
Un plan de gestion des incidents doit donc intégrer les éléments nécessaires pour permettre à l’entreprise d’identifier l’incident ; de le classifier ; de recueillir les preuves et d’enquêter ; d’analyser les causes ; de résoudre l'incident et de s’assurer de sa résolution ; et de clôturer l’incident.

« Il est tout à fait possible de quantifier l'impact d’une cyberattaque : nombre de clients et de collaborateurs touchés, effets sur l’expérience utilisateur en cas de panne, perte de chiffre d'affaires, etc. Il existe de nombreuses façons de mesurer les risques. C’est là que la pénalité financière associée à NIS 2 peut être un levier pour clarifier le business case de la cybersécurité et convaincre plus facilement les décideurs au plus haut niveau.
Mais ce qui est encore plus essentiel, c’est que NIS 2 introduit une approche plus pragmatique, indispensable aujourd’hui. Nous ne sommes plus simplement dans une logique d’audit et de gestion des risques potentiels, mais bien dans une dynamique visant à mesurer l’efficacité réelle de la sécurité, en évaluant la capacité d’une organisation à répondre rapidement à une vulnérabilité.
NIS 2 va également favoriser une nécessaire standardisation des pratiques en France. Cette directive peut – et doit – devenir un catalyseur pour l’adoption des technologies modernes. Pourtant, beaucoup d’organisations restent cloisonnées, ce qui freine leur mise en conformité. Si certaines technologies peuvent être déployées sans une réorganisation complète, une nouvelle gouvernance est souvent nécessaire. En conséquence, les projets de transformation se font progressivement. »

Erwan Bornier,
CTO, WIZ

Que dit la directive NIS ?

L’article 21 de la directive (EU) 2022/2555 du parlement européen et du conseil du 14 décembre 2022 récapitule les mesures de gestion des risques liés à la cybersécurité que doivent adopter les entreprises dans le cadre de NIS 2. Ces mesures entendent proposer une approche multirisque en vue de protéger les réseaux et les systèmes d'information ainsi que l'environnement physique de ces systèmes contre les incidents.

En ce sens, elles doivent au minimum inclure les dix éléments suivants :

- Des politiques en matière d'analyse des risques et de sécurité des systèmes d'information ;
- Le traitement des incidents ;
- La continuité des activités, notamment la gestion des sauvegardes et la reprise après sinistre, ainsi que la gestion des crises ;
- La sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité des relations entre chaque entité et ses fournisseurs directs ou ses prestataires de services ;
- La sécurité dans l'acquisition, le développement et la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
- Les politiques et procédures permettant d'évaluer l'efficacité des mesures de gestion des risques liés à la cybersécurité ;
- Les pratiques de base en matière de cyber-hygiène et la formation à la cybersécurité ;
- Des politiques et des procédures concernant l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
- La sécurité des ressources humaines, les politiques de contrôle d'accès et la gestion des actifs ;
- L'utilisation de solutions d'authentification multifactorielle ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes de communication d'urgence sécurisés au sein de l'entité, le cas échéant.

« La gestion des risques est essentielle pour toute organisation d'infrastructure critique. Identifier les risques et y répondre de manière efficace permet de réduire considérablement les chances qu'une attaque réussisse. Cependant, il est tout aussi important de limiter l'impact d'une attaque en la maîtrisant dès les premiers signes. Cette approche, nous la constatons chaque jour, sur le terrain, auprès de nos clients à travers l'Europe, dans des secteurs tels que l'énergie, la santé ou la logistique – des domaines dont la nature même les rend particulièrement sensibles.

Pour protéger leurs actifs les plus essentiels, la majorité de nos clients met en place des mesures de contrôle rigoureuses sur les accès aux ressources et aux personnes. Cela leur permet de maintenir la continuité de leurs opérations, même en cas d'incident majeur.

En France, il convient de rappeler que le pays a été pionnier en matière de sécurité des infrastructures critiques avec la directive NIS, directement inspirée de la Loi de Programmation Militaire (LPM). Ce cadre législatif impose aux Opérateurs d'Importance Vitale (OIV) des mesures de sécurité strictes et a contribué à définir une approche claire pour protéger les infrastructures critiques contre les cybermenaces. Grâce à cette expérience, la mise en conformité en France est relativement bien encadrée. Cependant, de nombreuses organisations devront probablement investir davantage dans la gestion des incidents pour renforcer leur résilience face aux risques actuels. »

Trevor Dearing,
Director of Critical Infrastructure Solutions, ILLUMIO

Autant de mesures qui dépendent principalement de la maturité de l'entreprise vis-à-vis des enjeux de protection des données, de l'état d'avancée de sa transformation numérique et de l'obsolescence de ses infrastructures technologiques.

Or, sur ce point, on observe des disparités certaines entre les entreprises « digital natives », plus agiles et qui, par essence, reposent sur les dernières technologies, et les grandes entreprises du CAC 40 par exemple qui, certes disposent de plus de moyens, mais dont la hiérarchie, plus lourde, peut ralentir la transformation. Quant aux PME et ETI, désormais elles aussi concernées par NIS 2, si leur organisation plus souple favorise des prises de décision plus rapides, elles peuvent en revanche manque de moyens financiers pour déployer les technologies adaptées et appliquer certaines mesures.

20%

20 % des entreprises de la région EMEA considèrent le budget comme un obstacle majeur à leur mise en conformité avec NIS 2. Résultat, 95 % puisent dans d'autres budgets.

Censuswide , octobre 2024

« Il faut bien garder à l'esprit que ce n'est pas tout le périmètre IT qui est soumis à cette réglementation NIS 2, mais uniquement ce qu'on appelle les systèmes d'information essentiels. C'est-à-dire ceux qui vont être en communication directe avec une chaîne d'assemblage par exemple. Pourquoi ? Parce que, potentiellement, un sous-traitant va fournir de la data au niveau de cette chaîne d'assemblage. Résultat, le système d'information de ce sous-traitant va lui aussi être considéré comme un système d'information essentiel. On parle de système d'information réglementé ou SIR. En revanche, l'ensemble des systèmes de l'entreprise ne sont pas nécessairement concernés réduisant très fortement le périmètre concerné. »

Xavier Gruau,
CTO, SQUAD

Technologies et stratégies : comment traduire les exigences en actions concrètes ?

Quelles technologies sont conformes avec la règlementation ? Cette question, toutes les entités concernées se la posent. C'est pourquoi il est important pour les EE et EI de s'appuyer sur une liste déjà établie de solutions conformes et donc de privilégier les solutions certifiées / qualifiées car elles ont déjà été éprouvées. En cas de contrôle par l'autorité nationale, elles pourront alors plus facilement prouver leur conformité.

L'ANSSI et le BSI *(Bundesamt für Sicherheit in der Informationstechnik, équivalent de l'ANSSI pour l'Allemagne)* poussent à l'utilisation de produits qualifiés ou certifiés. Il n'y a aucune obligation, mais dans le cas contraire, ce sont les équipes qui risquent d'être auditées et devront fournir les éléments de preuve de conformité à l'ensemble des mesures.

Toutefois, il existe une zone de flou autour de certains points pour lesquels aucune technologie n'est certifiée. NIS 2 ne fait aucune différence entre les éditeurs. C'est donc aux éditeurs de justifier leurs caractéristiques techniques en termes de robustesse. Ensuite, il appartient à chaque entité de vérifier quel périmètre de sécurité est couvert par la solution déployée.

Chez Squad, nous avons donc tenté d'établir une correspondance entre les points de sécurité et les technologies.

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 1 : **Recensement des SI**	Les entités doivent réaliser et maintenir à jour une liste de l'ensemble de leurs activités et services ainsi que des systèmes d'information permettant de les opérer. En outre, sur la base d'une analyse de risques, les entités sont tenus de justifier la non-application de certains objectifs de sécurité ainsi que la déclinaison des mesures de sécurité qu'elles comptent implémenter.	Toutes les entités EI et EE	Asset Discovery / IT Asset Management / CMDB enrichie	Forescout
			CAASM (Cyber Asset Attack Surface Management)	
			GRC / Risk Management	Forescout
Objectif de sécurité 2 : **Mise en oeuvre d'un cadre de gouvernance de la sécurité numérique**	Les entités doivent définir un cadre de gouvernance de la sécurité numérique placé sous la responsabilité du directeur de l'entité. A ce titre, il est nécessaire pour les entités concernées de formaliser une PSSI et des politiques de sécurité adéquates.	Toutes les entités EI et EE (sauf la désignation d'un RSSI pour les EI)	GRC / Risk Management	
			Gestion documentaire / PSSI / Politiques de sécurité	
			Automatisation de la conformité et des audits	
Objectif de sécurité 3 : **Maîtrise de l'écosystème**	Les entités réalisent et maintiennent à jour une liste des prestataires et fournisseurs informatiques intervenant dans la réalisation de leurs activités ou dans la fourniture de leurs services et avec lesquels il existe une relation contractuelle ainsi que le périmètre et la nature de la prestation ou du service fourni.	Toutes les entités EI et EE	Third-Party Risk Management / TPRM	
			GRC / Gestion des fournisseurs	
			Contract Management / Suivi des prestataires	

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 4 : **Prise en compte de la sécurité numérique dans la gestion des ressources humaines**	Les entités prennent en compte la sécurité numérique dans la gestion de leurs ressources humaines en sensibilisant leurs utilisateurs, en particulier les dirigeants de l'entité, et en formant à la sécurité numérique les personnes occupant des fonctions à responsabilités dans le domaine du numérique.	Toutes les entités EI et EE	Sensibilisation et formation à la cybersécurité	
			LMS / Plateformes de formation	
			Simulations de phishing / tests de vigilance	
Objectif de sécurité 5 : **Maîtrise des SI**	Les entités disposent d'au moins une cartographie de leurs systèmes d'information suffisamment détaillée pour faciliter le MCO/MCS et la réactivité des entités en cas d'incident de sécurité. Une politique de MCO/MCS doit d'ailleurs être rédigé à cet effet.	Uniquement les EE	Cartographie des systèmes d'information	Extrahop Forescout WIZ
			IT Asset Management / CMDB	Forescout
			MCO/MCS / gestion de la configuration et des correctifs	
Objectif de sécurité 6 : **Maîtrise des accès physiques aux locaux**	Les entités mettent en place des mécanismes de contrôle d'accès et de gestion des droits d'accès ainsi que des processus de gestion des visiteurs afin de s'assurer que seules les personnes autorisées ont accès aux locaux sensibles.	Surtout les EE sauf pour la gestion des locaux techniques (où les EI sont concernés)	Contrôle d'accès physique	
			Gestion des identités physiques (PIAM)	
			Gestion des visiteurs	Forescout

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 7 : **Sécurisation de l'architecture des SI**	Les entités identifient les besoins d'exposition et d'interconnexion de leurs activités et services fournis à des systèmes d'information tiers. Ces entités filtrent les communications entrantes et sortantes de leurs systèmes d'information, en particulier les flux dont l'origine, le transit ou la destination est un système d'information tiers. Les entités essentielles, elles, doivent cloisonner leurs systèmes d'information en zones de sécurité cohérentes et contrôler les points d'entrée et de sortie des systèmes d'information pour les utilisateurs, les prestataires et les fournisseurs.	Surtout les EE	Pare-feu nouvelle génération (NGFW)	
			Zoning réseau / Micro-segmentation	Extrahop Forescout Illumio
			NAC (Network Access Control)	Forescout
			CASB / Contrôle des connexions cloud	
			Reverse proxy / Contrôle des accès distants	
Objectif de sécurité 8 : **Sécurisation des accès distants aux SI**	Les entités mettent en place 1. Des mécanismes d'identification et d'authentification des personnes 2. Des mécanismes de sécurisation du canal de communication, des points d'entrée et de sortie et des accès à leurs systèmes d'information depuis des systèmes d'information tiers (ex : internet)	Toutes les entités	IAM / Gestion des identités et des accès	Extrahop
			MFA / Authentification multifacteur	
			VPN / accès distant sécurisé	
			ZTNA / Zero Trust Network Access	
			SASE / Sécurisation du canal réseau	

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 9 : **Protection des SI contre les codes malveillants**	Les entités mettent en œuvre des mécanismes de protection contre les codes malveillants sur les ressources de leurs systèmes d'informations.	Toutes les entités	EPP / Protection des postes de travail	WIZ
			EDR / Détection et réponse sur les endpoints	
			XDR / Détection étendue multi-sources	Forescout
Objectif de sécurité 10 : **Gestion des identités et des accès des utilisateurs aux SI**	Les entités mettent en œuvre : 1. Des mécanismes d'identification et d'authentification des utilisateurs et des processus automatiques de leurs systèmes d'information ; 2. De processus de gestion des droits permettant notamment l'attribution des droits d'accès aux ressources en fonction du besoin opérationnels des utilisateurs	Toutes les entités	IAM / Gestion des identités et des accès	
			IGA / Gestion des identités et des droits	
			PAM / Gestion des accès à privilèges	
			MFA / Authentification multifacteur	
Objectif de sécurité 11 : **Maîtrise de l'administration des SI**	Les entités ou toute personne qu'elles ont mandatée pour réaliser les activités d'administration, disposent de comptes d'administrations exclusivement dédiés à cet usage et utilisés par les seules personnes autorisées. Les entités s'assurent de la sécurisation de l'administration de leurs annuaires en s'appuyant sur l'état de l'art en la matière (incluant la mise en place de bastion pour les EE)	Surtout les EE	PAM / Gestion des accès à privilèges	
			Bastion d'administration / Jump server	
			Sécurisation des annuaires (AD)	

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 12 : **Identification et réaction aux incidents de sécurité**	Les entités mettent en œuvre une organisation, des processus et des outils adaptés pour se préparer et réagir à des événements de sécurité susceptibles d'impacter la réalisation de leurs activités ou la fourniture de leurs services.	Uniquement les EE	SIEM / Supervision et corrélation des événements	Extrahop
			SOAR / Automatisation de la réponse	
			XDR / Détection et réponse étendues	Extrahop
			Threat Intelligence / renseignement sur les menaces	
Objectif de sécurité 13 : **Continuité et reprise d'activité**	Les entités mettent en œuvre des mécanismes de sauvegarde et de restauration opérationnels et les testent au minimum une fois par an. Les entités essentielles définissent et maintiennent à jour des plans de continuité et de reprise d'activité adaptés aux besoins de leurs activités et de la fourniture de leurs services.	Toutes les entités (seuls les EE doivent définir des PCA/PRA)	Sauvegarde et restauration	
			PRA / PCA (plans de reprise et de continuité d'activité)	
			Orchestration de la continuité d'activité	
			Gestion de crise cyber / Orchestration de réponse	
Objectif de sécurité 14 : **Réaction aux crises d'origine cyber**	Les entités mettent en œuvre une organisation, des processus et des outils adaptés pour se préparer et réagir à des crises d'origine cyber.	Toutes les entités	Plateformes de simulation de crise / entraînement	
			Notification et communication de crise	

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 15 : **Exercices, tests et entraînements**	Les entités réalisent des exercices, tests et entraînements à intervalles réguliers pour vérifier l'efficacité de leur organisation, leurs processus, leurs outils et leur préparation pour faire face aux incidents de sécurité et aux crises d'origine cyber.	Uniquement les EE (sauf pour la sensibilisation où les EI sont concernés)	Plateformes de cyber range / Entraînement technique	
			Simulation d'incidents et de crises	
			Gestion et orchestration des exercices de crise	
Objectif de sécurité 16 : **Mise en oeuvre d'une approche par les risques**	Les entités mettent en oeuvre une approche par les risques placée sous la responsabilité du dirigeant exécutif et leur permettant : 1. de prendre connaissance et de suivre l'évolution des risques pesant sur leurs systèmes d'information ; 2. de définir et suivre la mise en œuvre des mesures de sécurité pour maîtriser ces risques ; 3. d'accepter les risques résiduels. Ici il est attendu pour les EE de réaliser et de mettre à jour les analyses de risques de chaque SI	Uniquement les EE	GRC / Gestion des risques et conformité	WIZ
			Analyse de risques cybersécurité	
			Cartographie des risques et plans de traitement	
Objectif de sécurité 17 : **Audit de la sécurité des SI**	Les entités auditent à intervalles planifiés leurs systèmes d'information.	Uniquement les EE	Outils d'audit de sécurité des SI	
			Gestion des audits / GRC	
			Conformité et audit cloud / SaaS	WIZ

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 18 : **Sécurisation de la configuration des ressources des SI**	Les entités s'assurent que l'ensemble des configurations de leurs équipements sont suffisamment durcis d'un point de vue configuration.	Uniquement les EE	CSPM / Durcissement des configurations cloud	WIZ
			SCAP / Audit de configuration	
			Gestion de la conformité de configuration	Forescout
			Benchmark de durcissement (référentiels)	
Objectif de sécurité 19 : **Administration des SI depuis des ressources dédiées**	Les entités mettent en place pour l'administration de leurs systèmes d'information : 1° des postes d'administrations maîtrisées par l'entité ou toute personne qu'elle a mandatée pour réaliser cette activité et qui sont conformes aux recommandations de l'autorité nationale de sécurité des systèmes d'information ; 2° une sécurisation et un cloisonnement des flux dédiés à cette activité, qui s'appuient sur les recommandations de l'autorité nationale de sécurité des systèmes d'information.	Uniquement les EE	Postes d'administration sécurisés / Durcis	
			Bastion d'administration / Jump server	
			Cloisonnement et filtrage des flux d'administration	Forescout Illumio
			Supervision et traçabilité des sessions d'administration	

Objectifs de Sécurité	Descriptif	Périmètre d'application de la directive	Type de technologies	Nos Partenaires dans ce guide
Objectif de sécurité 20 : **Supervision de la sécurité des SI**	Les entités essentielles : 1 : s'assurent que les équipes en charge de l'activité de supervision de sécurité dimensionnent et opèrent le système d'information supportant l'activité de supervision de sécurité en adéquation avec leur capacité opérationnelle, afin de prendre en compte les journaux et les évènements de sécurité, sans retard injustifié et au maximum sous 24h ouvrés. 2 : élaborent et mettent en œuvre une démarche d'amélioration continue de leur activité de supervision de sécurité, afin d'améliorer la couverture des scénarios de menaces identifiés à l'occasion de l'analyse de risque prévue à l'[objectif de sécurité 16] du présent décret, et l'efficacité de la supervision de sécurité ; 3° s'assurent que les événements de sécurité et les journaux sont conservés pour une durée d'au moins trois mois sans préjudice d'autres obligations légales et réglementaires.	Uniquement les EE	SIEM / Supervision centralisée des événements	Extrahop
			SOC / Supervision externalisée ou internalisée	
			Journalisation et conservation des logs	
			Amélioration continue de la détection	
			Orchestration et réponse automatisée (SOAR)	

« J'encourage toujours les entreprises à privilégier les solutions, si elles existent, qui sont qualifiées ou certifiées pour un point de vue sécurité. Côté implémentation, il est important que les solutions soient facilement déployables et sécurisées.
En revanche, s'il n'existe pas de solution ou que le catalogue de l'ANSSI n'en propose pas, elles doivent alors se faire accompagner par des équipes d'experts capables de résoudre leurs problèmes de déploiement. Il faut juste s'assurer que la solution retenue réponde bien au besoin de sécurité imposé par NIS 2.

Les solutions certifiées garantissent simplement de suivre les bonnes guidelines. Mais si on a la capacité de justifier que l'outil en place a le bon rôle et que l'on a bien implémenté les bonnes configurations, il n'est alors pas impératif de changer de solution si, entretemps, une technologie a obtenu une certification.»

Xavier Gruau,
CTO, SQUAD

TROISIÈME PARTIE

Retours d’expérience

Nos experts partenaires témoignent et nous partagent leurs visions sur ce sujet stratégique.

Hassan El Karhani,
Field Technology Officer, Forescout Technologies Inc.

Acteur mondial de la cybersécurité, Forescout Technologies aide les organisations à identifier en continu, à protéger et à garantir la conformité de l'ensemble des actifs cyber gérés et non gérés – IT, IoT, IoMT et OT.

Notre plateforme permet ainsi aux organisations d'identifier chaque actif cyber, de recueillir des informations contextuelles étendues à leur sujet, et d'assurer une mise à jour précise de la base de données de gestion des configurations (CMDB), ceci constituant une étape clé du processus de conformité. Comment ? Grâce à notre approche Zero Trust qui permet de segmenter les réseaux, en priorisant les dispositifs à risque et les actions d'atténuation comme mesures proactives, et à notre technologie agnostique vis-à-vis des fournisseurs qui permet d'assurer une interopérabilité optimale. Objectif : faciliter la détection des menaces et la réponse aux incidents, en garantissant un contrôle et une gouvernance sur l'ensemble des actifs cyber.

Nous accompagnons ainsi les organisations dans leur mise en conformité avec NIS 2 - un point essentiel - car de nombreuses entreprises réalisent seulement maintenant l'ampleur des exigences imposées par la directive, d'autant plus qu'elle couvre désormais un éventail plus large de secteurs. Une confusion courante consiste à voir NIS 2 comme une simple liste de contrôle IT, alors qu'elle englobe aussi les systèmes IoT et OT.

Les entreprises sont donc confrontées à plusieurs défis. D'abord, elles doivent déployer une visibilité complète sur leurs actifs afin de pouvoir gérer les dispositifs à risque. Ensuite, elles doivent se protéger contre les cybermenaces, tout en maîtrisant l'impact des incidents sur les environnements IT et OT.

Souvent, les organisations doivent faire face à des réseaux fragmentés, des outils dispersés, des systèmes OT obsolètes et des ressources de sécurité limitées, rendant la mise en conformité particulièrement complexe. Bien que la prise de conscience progresse, un grand nombre d'entreprises en France peinent à unifier leurs mesures de sécurité IT et OT, tout en maintenant une surveillance en temps réel.
C'est pourquoi nous avons défini des étapes clés pour les aider à se préparer à NIS 2, en mettant l'accent sur la gestion des risques et la réponse aux incidents tout en garantissant l'interopérabilité entre IT et OT. En parallèle, l'automatisation des rapports de conformité permet de réduire les risques de sanctions.

Concrètement, voici les cinq axes majeurs que nous avons identifiés pour la mise en conformité avec NIS 2 :

1. **La gestion des risques** : notre plateforme permet aux RSSI d'obtenir une visibilité complète sur les actifs IT, OT et IoT/IoMT, qu'ils soient gérés ou non, et de réduire le risque d'attaques potentielles.
2. **La gestion des incidents** : en accélérant la détection des menaces et la réponse aux incidents de cybersécurité grâce à une automatisation avancée, les organisations respectent les exigences de NIS2 en matière de signalement rapide et précis.
3. **Les tests de résilience opérationnelle** : la surveillance continue des actifs, la détection des menaces et les capacités de réponse de la plateforme répondent aux exigences de résilience opérationnelle de NIS2.
4. **La gestion des risques liés aux tiers** : Forescout aide les organisations à améliorer leur visibilité sur leurs fournisseurs TIC tiers, leur permettant ainsi de gérer et de sécuriser ces contributeurs critiques aux services numériques.
5. **Le partage d'informations** via un signalement sécurisé des incidents et des événements, ainsi qu'un partage sécurisé des journaux et des données d'audit avec les parties prenantes. Les organisations bénéficient également des renseignements sur les menaces fournis par Vedere Labs, intégrés à la plateforme et partagés avec la communauté élargie de la cybersécurité.

NIS 2 incite les organisations à adopter une gestion continue des risques et une détection / réponse en temps réel, transformant ainsi la cybersécurité d'un projet ponctuel à un enjeu stratégique permanent. L'extension des exigences réglementaires aux systèmes OT et IoT pousse les entreprises à développer une visibilité totale et à mettre en place des systèmes de réponse rapide pour se conformer aux normes toujours plus strictes.

Notre objectif est de créer un point de visibilité unique pour les actifs, les risques et les menaces, en appliquant des contrôles et en orchestrant des actions automatisées pour que les organisations puissent rapidement contenir et atténuer leurs risques les plus critiques. L'intégration transparente de notre solution avec différentes infrastructures permet aux entreprises de répondre aux exigences réglementaires tout en restant prêtes à faire face aux cybermenaces émergentes.

Cependant, la technologie seule ne suffit pas pour garantir la conformité. L'accompagnement humain est crucial. C'est là d'ailleurs qu'intervient notre partenariat avec Squad. Celui-ci repose sur un échange mutuellement bénéfique d'expertises complémentaires : Squad apporte son savoir-faire en matière de conseil stratégique pour la conformité NIS 2, tandis que Forescout fournit une plateforme technologique permettant une gestion continue des actifs, l'évaluation des risques, la détection des menaces et l'application automatisée des politiques. Ensemble, nous aidons les entreprises à mettre en place des systèmes de cybersécurité durables et à répondre aux exigences de sécurité et de conformité en constante évolution.

Trevor Dearing,
Director of Critical Infrastructure Solutions, Illumio

Illumio se positionne comme le leader de la segmentation Zero Trust. Cette approche repose sur la micro-segmentation en appliquant les principes Zero Trust, avec l'avantage clé de pouvoir contenir une attaque et prévenir sa propagation latérale. Ainsi, Illumio permet de réduire l'impact d'une cyberattaque et d'améliorer la cyber-résilience des entreprises. Contrairement à d'autres solutions qui se concentrent principalement sur la réduction des risques d'une attaque réussie, Illumio reconnaît que cette prévention ne peut jamais être absolue.

La directive NIS 2 s'inscrit parfaitement dans ce contexte, puisqu'elle vise à renforcer la résilience des organisations dans les secteurs des infrastructures critiques. Son objectif est d'améliorer la réponse aux incidents pour éviter qu'une menace ne dégénère en catastrophe.
En ce sens, NIS 2 met l'accent sur la résilience, la gouvernance et l'atténuation proactive des menaces. C'est précisément là que la segmentation Zero Trust joue un rôle crucial pour améliorer la cyber-résilience à travers plusieurs étapes clés :

1. **Identification des risques** : repérer les vulnérabilités comme les ports ouverts à haut risque, les systèmes non corrigés, ou les connexions à des IP malveillantes.
2. **Atténuation des risques** : éliminer ces vulnérabilités et établir des barrières pour contenir une attaque, par exemple en séparant les environnements IT et OT.
3. **Atténuation de l'impact** : isoler dynamiquement les ressources infectées pour les séparer du reste de l'infrastructure.

NIS 2 a donc pour objectif de réduire les incohérences en matière de résilience et de renforcer la prise de conscience collective des risques. Toutefois, la directive s'appuie surtout sur des exigences déjà existantes et cherche à harmoniser les réponses, plutôt qu'à introduire de nouveaux contrôles. Son changement majeur réside dans l'élargissement considérable des secteurs et des organisations concernés, notamment les PME, qui devront probablement relever le défi de trouver les ressources nécessaires pour se concentrer sur la conformité.

Ainsi, toutes les entreprises n'en sont pas au même stade de préparation. Celles ayant déjà adopté NIS 1 sont généralement prêtes pour NIS 2, puisque la plupart des ajustements concernent principalement l'harmonisation entre les États.

En revanche, les entreprises découvrant NIS 2 se retrouvent dans deux situations : celles ayant une bonne hygiène cyber trouvent souvent le processus relativement simple, tandis que celles sans politique de cybersécurité risquent de rencontrer des difficultés. Le principal défi reste sans doute le manque de ressources pour se consacrer pleinement à la conformité. Heureusement, la plupart des pays ont fixé la date limite de conformité à 2030, offrant ainsi un délai supplémentaire pour les entreprises.

Il reste à déterminer comment chaque État transposera la directive et quelles seront les modalités de certification. Le principal défi résidera probablement dans la protection des équipements anciens. Bien que de nombreux contrôles de sécurité soient déjà en place, plusieurs organisations devront probablement investir davantage dans les domaines suivants :

- Analyse des risques : identification des zones de risque pouvant mener à une compromission ;
- Gestion des incidents : confinement des attaques et mise en quarantaine des ressources infectées ;
- Continuité des activités : réduction de l'impact d'une attaque ;
- Sécurité de la chaîne d'approvisionnement : contrôle de l'accès aux ressources par des tiers ;
- Gestion des vulnérabilités : désactivation des services à haut risque et des systèmes non corrigés.

Aussi, bien que les transpositions nationales de NIS 2 puissent varier, la solution Illumio répond de manière efficace à la majorité des exigences, notamment en matière de gestion des risques et d'amélioration de la cyber-résilience.

L'étape la plus importante consiste à comprendre les risques au sein de l'organisation, ce qui implique notamment de :

- Comprendre et cartographier tous les flux de trafic dans l'organisation ;
- Identifier et fermer les services à haut risque inutiles ;
- Atténuer les vulnérabilités ;
- Et segmenter et séparer les environnements pour empêcher la propagation d'une attaque.

Malgré les défis liés à la mise en conformité, NIS 2 est une initiative positive car elle favorise une meilleure prise en compte de la résilience et de la continuité des opérations. À terme, les révisions futures de la directive devraient s'inspirer de DORA, avec des exigences plus précises et harmonisées au niveau européen.

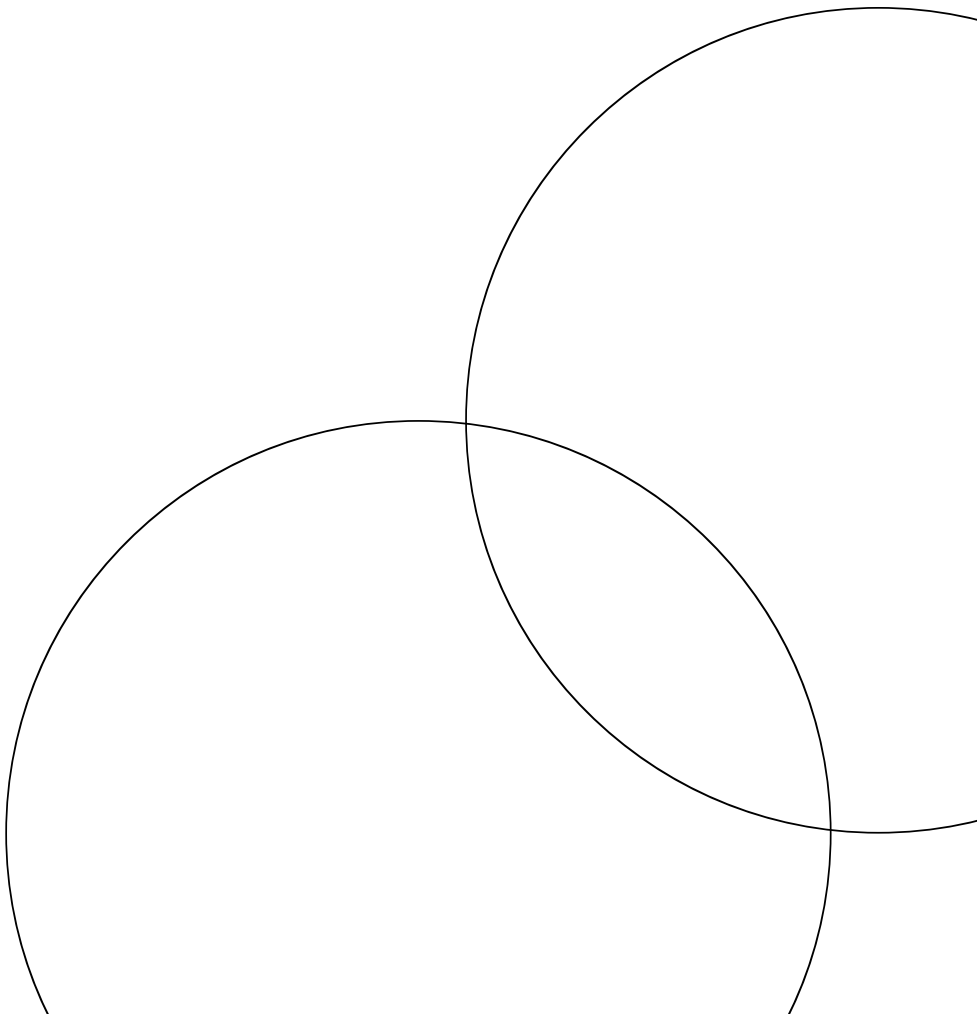
Pour les entreprises, il est crucial d'adopter une approche fondée sur les risques, en identifiant les éléments essentiels pour garantir la continuité des activités et en construisant la conformité autour de ces priorités.

Dans cette démarche, 2 erreurs sont aisément commises :

- La 1ère, c'est de tenter d'appliquer toutes les exigences à la lettre - ce qui peut se révéler coûteux et inefficace.
- La seconde, c'est de négliger l'importance de travailler aux côtés d'experts, car la mise en conformité avec NIS 2 peut être complexe selon le niveau de maturité de l'entreprise.

C'est d'ailleurs pourquoi nous collaborons avec Squad qui, en tant que ZTS Select Partner - l'un des niveaux de partenariat technique les plus avancés du programme Illumio - aide les organisations à développer leur stratégie Zero Trust et à se conformer aux régulations telles que NIS 2.

En conclusion, une approche stratégique, axée sur les risques et soutenue par des experts est essentielle pour naviguer efficacement dans les exigences de NIS 2, tout en renforçant la résilience et la sécurité à long terme des entreprises face aux défis du numérique.



Erwan Bornier,
Chief Technology Officer, WIZ

Créé en 2020, WIZ a pour mission de sécuriser tout ce que les clients construisent et déploient dans le cloud.

Au quotidien, WIZ sécurise à la fois l'infrastructure cloud elle-même, l'environnement cloud et les services qui en découlent, et offre la capacité d'adresser les menaces en temps réel grâce à une vue complète de la chaîne digitale et de sa sécurisation.
Lorsqu'on parle de sécurisation dans le cadre de NIS 2, il y a deux concepts clés à retenir : contextualisation et démocratisation.

La contextualisation d'abord. Aujourd'hui, les entreprises utilisent le plus souvent un grand nombre de solutions différentes qui répondent toutes à un besoin précis de sécurisation : les données, l'exposition sur internet, la gestion des vulnérabilités, etc. Chacune de ces solutions remonte des alertes et il devient alors difficile pour les équipes de sécurité de savoir lesquelles traiter en priorité. L'approche de WIZ consiste à ingérer toutes ces alertes, à les corréler et à identifier ce que l'on appelle des "combinaisons toxiques". Par exemple, une alerte classique sur une vulnérabilité dans une application exposée sur Internet, accédant à des données sensibles, doit être traitée en priorité en raison de la nature de cette combinaison.

Le pilier n°2, c'est la démocratisation, c'est dire que la sécurité est la responsabilité de tous. La complexité croissante des environnements cloud et des applications rend difficile pour les équipes de sécurité de gérer l'ensemble des risques. Aujourd'hui, il est possible de déployer une application en quelques secondes, la rendant immédiatement vulnérable sur le web. C'est pourquoi nous avons conçu une plateforme unifiée avec une expérience utilisateur simple, permettant aux développeurs de visualiser en temps réel la vulnérabilité de leurs applications et de prioriser les actions de remédiation. En fournissant le bon contexte et les bonnes informations, nous permettons aux développeurs de prendre des décisions éclairées et d'assumer la responsabilité de la sécurité de leurs applications.

NIS2 élève le niveau d'exigence au sein des entreprises dans un contexte de forte complexité liée au cloud et même au multicloud. En ce sens, l'approche multifournisseur est essentielle dans la mise en conformité avec NIS 2, car elle permet une intégration transparente avec de multiples plateformes comme Azure, Amazon, Google et Alibaba. Or les entreprises ne comprennent pas toujours quelle est leur responsabilité vis-à-vis du service qu'elles consomment.

La gestion des risques liés aux infrastructures externalisées est un enjeu critique. L'aspect multicloud permet par conséquent aux entreprises de bénéficier d'une visibilité complète et immédiate sur l'ensemble de leurs actifs cloud, indépendamment du nombre de fournisseurs ou de la complexité des infrastructures impliquées.

De la même manière, cette stratégie aide à standardiser les processus de sécurité à travers différents fournisseurs, en simplifiant la gestion des vulnérabilités et des politiques de sécurité, ce qui est crucial pour les entreprises opérant dans un environnement cloud complexe.

Les entreprises doivent donc adopter une approche plus cohérente, ce qui implique un tournant technologique dans leurs solutions et leurs processus. La clé de leur conformité réside dans une vue exhaustive et en temps réel de l'ensemble de leurs actifs cloud : machines virtuelles, conteneurs, composants réseaux, bases de données, etc. Par exemple, pour chaque machine virtuelle, il est essentiel de connaître la version du système d'exploitation ou du framework utilisé pour l'application. Cette double vue – globale et granulaire – est indispensable pour obtenir une visibilité complète et répondre aux exigences de gestion des actifs stipulées par NIS 2.

Pour accélérer les remédiations et éviter les pénalités, nous avons automatisé la détection et la réponse aux incidents grâce à un "security graph" qui visualise les liens entre tous les objets et les règles de contrôle prédéfinies dans notre plateforme. Par exemple, dès qu'une application exposée sur Internet manipule des données sensibles avec une vulnérabilité, une alerte de sécurité élevée se déclenche. Certaines règles, appliquées de manière continue, couvrent déjà une partie des exigences de NIS 2. De plus, des rapports d'audit peuvent être générés et archivés ou partagés avec des tiers, et un tableau de bord permet de monitorer l'ensemble des données en temps réel. La plateforme fournit également des remédiations automatisées.

Avec cette approche, NIS 2 ne doit pas être perçu comme un frein à l'innovation, mais comme un levier pour améliorer la posture de sécurité et accélérer l'adoption du cloud, et par extension, la capacité d'innovation des entreprises. Ce que nous observons dans les appels d'offres auxquels nous répondons confirme cette tendance : les entreprises, quelle que soit leur taille, prennent désormais pleinement conscience de l'importance de la conformité à NIS 2, bien que nous soyons encore au début de cette transition.

Mohammad Kaouk,

EMEA Sales Engineering Director, Extrahop

ExtraHop offre une solution de détection et de réponse aux menaces pour les réseaux natifs du cloud, apportant une visibilité complète sur l'environnement numérique des entreprises. Notre approche repose sur l'exploitation de l'intelligence réseau en temps réel, permettant ainsi de fournir une analyse approfondie du trafic réseau. Cela permet aux organisations de détecter, enquêter et répondre aux menaces de manière rapide et efficace - ce qui est essentiel pour répondre aux exigences de NIS 2 !

Bien que NIS 2 concerne spécifiquement les infrastructures critiques, nous avons choisi de concentrer nos efforts sur la sécurisation des environnements IT, IoT, K8s et des applications modernes qui soutiennent ces fonctions critiques. Si NIS 2 est une étape cruciale dans le renforcement de la sécurité des réseaux à travers l'Europe, de nombreuses entreprises prennent seulement conscience de l'étendue complète de leurs obligations.

Les entreprises se retrouvent confrontées à plusieurs défis majeurs, à commencer par la mise en œuvre des mesures de sécurité requises, surtout dans des environnements IT complexes. En France, l'accent est mis sur la sécurité nationale, ce qui pousse les organisations à se conformer aux réglementations, mais elles rencontrent encore des difficultés pratiques concernant la sécurisation de leurs actifs IT et IoT.
C'est pourquoi nos solutions intègrent les exigences liées à NIS 2. Notre plateforme aide les organisations à identifier, protéger et sécuriser les actifs IT et IoT. Les objectifs sont multiples :

- Maintenir une vue d'ensemble des actifs pertinents grâce à la détection automatisée et continue des appareils, à la surveillance et à l'analyse comportementale en temps réel.
- Mettre en place des processus de gestion des risques et d'atténuation des menaces pesant sur les services critiques grâce à une visibilité totale sur le trafic réseau et sur les détails des équipements. Par exemple : si un équipement est un serveur HTTP ou SSL.
- Identifier les menaces en temps réel grâce à des règles et à des détections basées sur le comportement, soutenues par des analyses avancées.
- Enquêter rapidement sur les incidents de sécurité et respecter les obligations de reporting grâce à 90 jours d'enregistrements de transactions et à des flux d'enquête rationalisés permettant d'obtenir des preuves médico-légales en quelques clics, et non en quelques jours.

Cette vue unifiée du réseau est cruciale pour la mise en conformité, car elle simplifie la gestion de la sécurité et facilite la détection des anomalies dans des environnements complexes et multifournisseurs. De plus, les données réseau détaillées et les journaux d'activité permettent de générer des rapports d'audit et de preuves de conformité à NIS 2. Cette approche rationalisée aide les entreprises à se concentrer sur ce qui est essentiel : sécuriser leurs actifs IT et IoT.

L'un de nos principaux différenciateurs réside dans notre approche agnostique des fournisseurs. Cela nous permet de fournir une visibilité complète et une analyse du trafic réseau, quel que soit l'infrastructure sous-jacente ou le fournisseur de services. En conséquence, les organisations bénéficient d'une interopérabilité optimale et peuvent appliquer la cybersécurité de manière homogène, sans être limitées à un seul écosystème fournisseur.

Cependant, des erreurs d'interprétation de NIS 2 sont encore courantes et peuvent compromettre la conformité. Une erreur fréquente est de considérer NIS 2 uniquement comme un exercice de conformité IT. Il est essentiel de comprendre que NIS 2 touche l'ensemble de l'organisation, pas uniquement le département IT. La conformité exige une approche holistique qui inclut la gouvernance, la gestion des risques et la réponse aux incidents.

De plus, la surveillance continue et la détection des menaces sont des aspects souvent négligés. La conformité ne doit pas être perçue comme un projet ponctuel, mais comme un processus continu de gestion et de réaction face aux risques.
Enfin, NIS 2 présente encore des zones d'ombre, notamment sur la définition exacte des entités « essentielles » et « importantes ». Une clarification des exigences spécifiques à chaque secteur serait bénéfique pour les entreprises.

En attendant, ExtraHop s'engage à aider les organisations à naviguer dans ce paysage complexe de cybersécurité et à relever les défis posés par NIS 2 et au-delà.
Notre partenariat avec Squad est un atout précieux dans cette démarche. Grâce à leur compréhension approfondie du marché local, en particulier en France, Squad aide nos clients à interpréter et appliquer les exigences de NIS 2 dans leur contexte spécifique. Ce partenariat permet de traduire les capacités techniques d'ExtraHop en actions concrètes et adaptées aux besoins réels des entreprises.

En combinant notre expertise technique et la connaissance locale de Squad, nous offrons une solution puissante pour atteindre la conformité NIS 2 et renforcer la cybersécurité globale des entreprises.

QUATRIÈME PARTIE

Les bonnes pratiques NIS 2

Les entités françaises vont dès 2025 devoir se conformer à la directive NIS 2. Une mise en conformité qui peut s’avérer complexe. Par où commencer ? Quelle solution choisir ? Quels points sécuriser en priorité ? Autant de questions qui peuvent freiner l’entité et lui faire risquer des pénalités.

Étapes clés pour une mise en conformité réussie

Quelle est la roadmap idéale pour se mettre en conformité avec NIS 2 ? Si tout dépend bien évidemment de l'entité, il existe néanmoins quelques étapes importantes pour bien se préparer.

ÉTAPE 1 : DÉTERMINER ET ENREGISTRER VOTRE STATUT

Avant toute chose, il importe pour l'entreprise de déterminer si elle est concernée par NIS 2. Si oui, il est alors nécessaire de vérifier si elle est classée comme entité essentielle ou importante. Une étape d'autant plus cruciale qu'elle dictera les obligations spécifiques à NIS 2 auxquelles l'entité sera soumise. Une fois le statut établi, il est alors temps de procéder à l'enregistrement proactif auprès des autorités compétentes du pays pour officialiser son statut et comprendre les exigences réglementaires précises. Attention, cette étape n'est pas si simple que l'on croit car il existe des zones d'ombre quant à la définition du statut.

ÉTAPE 2 : CARTOGRAPHIER ET ÉVALUER LES RISQUES

Pour réaliser une cartographie détaillée du système d'information, il est nécessaire d'identifier les actifs numériques critiques, les données sensibles et les connexions tierces. Ensuite, il est essentiel de détecter les risques en examinant les failles potentielles du système et les impacts possibles d'un incident. Cette évaluation participe à prioriser les actions de protection et de remédiation.

ÉTAPE 3 : STRUCTURER LA GOUVERNANCE DE CYBERSÉCURITÉ

Une fois la cartographie des risques établie, l'entreprise doit mettre en place une gouvernance forte en définissant clairement les rôles et les responsabilités au sein de l'organisation. Cette gouvernance s'avère indispensable pour mettre en place une politique de sécurité robuste, organiser le reporting et structurer les processus décisionnels à travers des comités de pilotage dédiés. En ce sens, elle est gage d'une gestion efficace de la sécurité.

ÉTAPE 4 : RENFORCER LES MESURES DE SÉCURITÉ

Maintenant, l'équipe Sécurité a toutes les cartes en main pour implémenter des solutions de cybersécurité avancées, incluant notamment une authentification forte, la protection des accès distants, la supervision continue des systèmes et le chiffrement des données. Ces mesures techniques sont essentielles pour sécuriser les infrastructures contre les menaces.

ÉTAPE 5 : ADOPTER UNE GESTION PROACTIVE DES INCIDENTS

Il s'agit de développer des procédures pour une notification rapide des incidents et la gestion des crises. En complément, il est recommandé de mettre en place une cellule de crise et des canaux de communication clairs pour une réponse rapide et efficace en cas de cyberattaque.

ÉTAPE 6 : DÉPLOYER UNE SENSIBILISATION ET UNE FORMATION CONTINUES

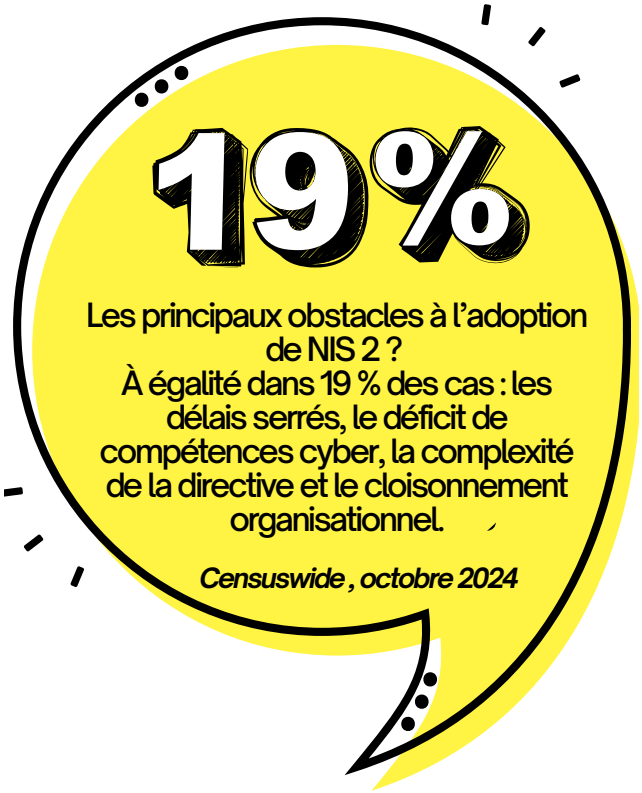
La sensibilisation à la cybersécurité doit être une priorité pour tous les employés. C'est pourquoi il est indispensable d'organiser des formations régulières et des exercices pratiques pour maintenir un niveau élevé de préparation face aux nouvelles menaces.

ÉTAPE 7 : SÉCURISER LA CHAÎNE D'APPROVISIONNEMENT

Cette sécurisation se construit autour de trois principes clés : évaluer le niveau de cybersécurité des fournisseurs et des partenaires ; intégrer des exigences strictes de cybersécurité dans les contrats ; et effectuer un suivi régulier pour minimiser les risques liés à la chaîne d'approvisionnement.

ÉTAPE 8 : AUDITER ET CONTRÔLER RÉGULIÈREMENT

Ajuster continuellement sa stratégie de sécurité implique de mettre en place des indicateurs de performance, réaliser des audits périodiques et rester informé des changements dans les exigences réglementaires.



ÉTAPE 9 : MAINTENIR DES PREUVES DE CONFORMITÉ

Parmi ses obligations, l'entité se doit notamment de documenter de manière rigoureuse toutes ses procédures, de préparer ses rapports réglementaires et de maintenir un registre des incidents pour répondre aux exigences de contrôle et d'audit.

ÉTAPE 10 : ÊTRE ACCOMPAGNÉ PAR DES EXPERTS

Implémentation de nouvelles technologies au sein d'infrastructures parfois obsolètes, interaction avec l'écosystème global de l'entreprise, mise en œuvre d'une gouvernance appropriée, prise en compte des évolutions règlementaires, etc. Autant de points qu'il faut prendre en compte ! Or, l'entreprise ne dispose pas toujours des ressources et des compétences nécessaires en interne. L'accompagnement par un expert externe tout au long du projet et par la suite est alors un gage de conformité.

« À terme, la directive générera une plus grande attention portée à la sécurité proactive et à la résilience, une harmonisation des règlementations en matière de cybersécurité à l'échelle européenne, et une amélioration de la collaboration d'informations entre les organisations, les groupes industriels et les organismes de réglementation pour lutter efficacement contre les cybermenaces. Mon conseil aux RSSI, responsables informatiques et équipes de sécurité qui débutent leur parcours NIS 2 ? Tout d'abord, donnez la priorité à la visibilité en investissant dans des solutions qui offrent une visibilité complète sur les environnements informatiques et IoT. C'est la base d'une détection efficace des menaces et d'une réponse aux incidents. Ensuite, il importe de se concentrer sur l'automatisation : automatisez les processus de sécurité dans la mesure du possible pour améliorer l'efficacité et réduire la charge des équipes de sécurité. Il est aussi essentiel de se préparer à la réponse aux incidents en élaborant et en testant des plans de réponse aux incidents pour vous assurer d'être prêt en cas de violation de la sécurité. Enfin, la communication et la collaboration sont essentielles pour garantir une approche unifiée de la conformité NIS 2, notamment entre l'informatique, la sécurité et les unités commerciales. »

Mohammad Kaouk,
EMEA Sales Engineering Director, EXTRAHOP

Bonnes pratiques VS risques majeurs

Tout au long de leur roadmap de mise en conformité, les entreprises risquent de se retrouver confrontées à de nombreux obstacles. Et ce pour plusieurs raisons.

- **La première repose sur le manque de documentation et de gouvernance récurrent observé au sein des organisations.** Les sociétés savent souvent bien implémenter la sécurité mais pas la documenter. Or l'insuffisance de documentation sur les procédures de sécurité et les analyses de risques peut créer une vulnérabilité significative, surtout lors du départ des employés clés.

Un autre écueil peut être lié au fait que de nombreuses entreprises adoptent une approche réactive plutôt que proactive, qui consiste à attendre que des incidents se produisent avant d'agir. Ce positionnement est souvent le résultat d'une visibilité insuffisante de l'activité du réseau et d'une politique qui consiste à s'appuyer uniquement sur la sécurité du périmètre. Considérer NIS 2 comme un simple exercice de conformité IT est une erreur. Il faut au contraire adopter une approche holistique impliquant la gouvernance, la gestion des risques et la réponse aux incidents.

- **La surveillance continue et la détection des menaces sont elles aussi souvent négligées.** La conformité ne doit pas être vue comme un événement ponctuel mais bien comme un processus continu.
- **De la même manière, les entreprises rencontrent de nombreux défis liés à la gestion des permissions et des privilèges**, à commencer par les problèmes de gestion des permissions, notamment dans les environnements cloud. Leur complexité requiert une surveillance et une gestion rigoureuses pour éviter les abus ou les accès non autorisés.

À l'inverse, les bonnes pratiques permettent d'éviter ces risques et les erreurs qui en découlent, et facilitent ainsi la mise en conformité NIS 2. Ces méthodes, lorsqu'elles sont intégrées de manière cohérente et stratégique dans les opérations d'une entreprise, renforcent la conformité à NIS 2 tout en améliorant la posture de sécurité globale de l'organisation.

1. ÉVALUER SA MATURITÉ EN AMONT

Une évaluation approfondie de la maturité en cybersécurité permet aux organisations de comprendre leur état actuel de préparation face aux exigences de NIS 2. Cette évaluation devrait inclure une analyse détaillée des systèmes en place, des politiques de sécurité, et de l'efficacité des contrôles existants. Cela aide à identifier les domaines dans lesquels l'organisation excelle et ceux où elle nécessite un renforcement, permettant ainsi une allocation ciblée des ressources pour les améliorations les plus critiques. Les organisations doivent en parallèle se tenir informées des mises à jour réglementaires, participer à des forums sectoriels, et s'engager auprès des pairs de l'industrie et des organismes de réglementation pour rester informées. Elles devraient également procéder à des audits internes réguliers afin d'évaluer leur niveau de conformité et d'identifier les points à améliorer.

2. AUTOMATISER LES RAPPORTS DE CONFORMITÉ

L'automatisation des rapports de conformité est essentielle pour maintenir une visibilité constante sur la posture de sécurité et simplifier le processus de démonstration de la conformité à NIS 2. En intégrant des systèmes qui génèrent automatiquement des tableaux de bord et des rapports, les organisations peuvent facilement surveiller leur état de conformité en temps réel et répondre rapidement aux éventuelles défaillances ou lacunes. À la clé : la capacité à réduire la charge de travail manuelle et permettre aux équipes de se concentrer sur des tâches plus stratégiques.

3. DÉPLOYER L'AUTHENTIFICATION MULTIFACTEUR

L'authentification multifacteur ajoute une couche supplémentaire de protection en requérant plusieurs formes de vérification de l'identité avant d'accorder l'accès à un système ou à des données. Elle s’avère particulièrement importante dans la protection contre les tentatives de phishing, les attaques de force brute, et autres stratégies d'exploitation des identifiants de connexion. Pour les entités, elle offre donc la possibilité de réduire significativement les risques de compromission. L'authentification multifacteur doit être envisagée non seulement pour l'accès aux systèmes d’information internes mais aussi pour tous les services cloud, les systèmes de gestion de bases de données, et les infrastructures critiques.

4. CYBERVIGILANCE DES EMPLOYÉS

Le risque n°1 dans les entreprises, ce sont les hommes. C'est pourquoi la formation et la sensibilisation continues des collaborateurs aux enjeux de cybersécurité recouvrent des enjeux critiques. Les programmes de formation doivent inclure des simulations d'attaques de phishing, l'enseignement des meilleures pratiques de sécurité et des mises à jour régulières sur les nouvelles menaces. Il est également recommandé de personnaliser les campagnes de sensibilisation selon le niveau de risque associé à chaque collaborateur : positionnement dans l'entreprise, accès systèmes dont il dispose, comportement face à une cybermenace, etc.

5. MAINTIEN DES CONDITIONS DE SÉCURITÉ

Le maintien en conditions de sécurité représente souvent la tâche la plus complexe pour les entreprises. Si elles mettent systématiquement leurs systèmes à jour avant un audit, la plupart ne font aucune mise à jour entre deux. D'où la nécessité pour elles de s'appuyer sur des outils d'automatisation et de s'équiper de systèmes d'alertes. Les organisations peuvent y remédier en mettant en œuvre des politiques de mise à jour régulières et automatisées qui incluent non seulement les systèmes informatiques mais aussi les logiciels et applications. En complément, l'utilisation d'outils de gestion des correctifs qui automatisent le processus de mise à jour permet aussi de s'assurer de la protection continue des systèmes avec les derniers correctifs de sécurité disponibles.
Et si ces pratiques restent trop compliquées ou longues à appliquer en interne, il reste toujours la possibilité de se faire accompagner par une société d'expertise dotée d'une vision 360 de la sécurité et de NIS 2 pour être sûre de n'oublier aucun point.

« Les pires pratiques surviennent souvent lorsque les organisations s'appuient sur des inventaires statiques, des processus manuels ou des outils de sécurité étroitement ciblés qui ne prennent pas en compte les risques en temps réel. Un autre aspect négligé est la responsabilité de la chaîne d'approvisionnement – certaines entreprises supposent que les fournisseurs supportent tout le fardeau de la conformité, mais en pratique, NIS 2 exige une responsabilité collective. Il existe également des zones d'ombre qui nécessitent une plus grande clarté réglementaire, notamment en ce qui concerne les délais de mise en œuvre et les attentes des fournisseurs de services plus petits mais néanmoins essentiels. C'est pourquoi mon conseil aux RSSI et aux responsables informatiques est de partir du principe que les obligations liées au NIS 2 vont évoluer. Commencez par une approche continue basée sur le risque : maintenez une visibilité dynamique des actifs à travers l'IT, l'OT et l'IoT ; mettez en œuvre la segmentation automatisée et l'application des politiques en fonction du risque ou de la menace détectée ; et préparez-vous à pivoter rapidement lorsque de nouvelles orientations apparaissent. Surtout, traitez NIS 2 comme une stratégie de sécurité continue plutôt que comme un projet ponctuel, en construisant une base qui évolue avec les exigences futures. »

Hassan El Karhani
Field Technology Officer, FORESCOUT Technologies INC.

Conclusion

En France, plusieurs milliers d'entités, qu'elles soient classées « Essentielles » ou « Importantes », se verront dans l'obligation de se conformer à NIS 2 dès 2025, là où elles n'étaient que quelques centaines à être couvertes par NIS 1. Selon l'étude d'impact de la directive NIS 2, 15 000 entités dans 18 secteurs d'activités, contre 500 dans 6 secteurs pour NIS 1, entrent directement dans le champ d'application de cette directive. Une nécessité face aux cyberattaques dont sont victimes les organismes : 90 % des entreprises de la région EMEA ont ainsi été confrontées à des incidents de cybersécurité que la conformité à la directive NIS2 aurait pu prévenir.

Pour autant, elles sont peu nombreuses à répondre aux exigences de la directive. Opacité de certaines obligations, manque de ressources, problème de budget, frein au changement… Les raisons sont multiples et les pénalités lourdes. Des sanctions qui, néanmoins, peuvent s'avérer tellement dissuasives qu'elles poussent à accélérer la mise en conformité et, in fine, la transformation des entreprises. En ce sens, NIS 2 tend à s'imposer dans les années à venir comme un moteur d'innovation !

Tel est l'objectif réel derrière la directive : uniformiser la maturité des entreprises en matière de pratiques de cybersécurité dans toute l'Europe. Par conséquent, dans quelques années, la cybersécurité sera davantage intégrée à l'ensemble des activités de l'entreprise, plaçant l'automatisation et l'apprentissage automatique au centre des enjeux de sécurité.

Néanmoins, la gestion des risques ne peut se faire sous le seul angle technique, et implique le plus souvent d'engager une transformation organisationnelle pour mettre en place une nouvelle gouvernance.

Soit un grand nombre de chantiers à lancer, parfois en simultané. Résultat, les entreprises peuvent rencontrer un certain nombre de difficultés d'implémentation ou même humaines. NIS 2 implique une vision 360 de la sécurité et une approche holistique, nécessitant un grand nombre d'expertises. C'est pourquoi les organisations qui décideront de mener ces transformations en interne s'exposeront davantage aux risques de pénalités financières du fait d'une conformité partielle ou d'erreurs d'interprétation de la règlementation.

En tant que délégataire au niveau des autorités nationales, et prestataire qualifié PASSI et en cours de qualification PACS, Squad est en contact direct avec les responsables français de la directive NIS 2, par le biais de sa maison-mère, Groupe SQUAD. Nos équipes échangent ainsi régulièrement avec l'ANSSI et partagent leurs retours d'expérience issus du terrain. Objectif : rendre les différentes réglementations en cours de révision ou à venir les plus pragmatiques possibles vis-à-vis des contextes et des enjeux de la société.

Un positionnement hybride, entre les autorités de régulation et les entreprises, qui renforce notre expertise et notre capacité de conseil.

« Chez Squad, nous accompagnons déjà de nombreuses sociétés du CAC 40 et du SBF 120 sur leur mise en conformité nous octroyant une vision large de leurs besoins et des points de complexité. Notre positionnement multi-éditeur nous permet d'enrichir tout l'écosystème de l'entreprise et de nous assurer que les technologies déployées sont les plus sécurisées possibles et répondent aux exigences NIS 2. En parallèle, nous alertons les autorités sur les éventuels blocages que rencontrent les organisations afin d'en tenir compte dans la directive », explique Xavier Gruau, CTO.

C'est là que se trouve la valeur ajoutée de l'expert qui va vous accompagner. Grâce à cette relation privilégiée, Squad est l'une des sociétés les plus à même de pouvoir vous conseiller au mieux sur votre mise en conformité et de vous assurer une conformité dès le premier essai.

A propos du Groupe Squad

Le Groupe Squad est un acteur majeur de la cybersécurité.
Avec 1000 collaborateurs et près de 125 Millions d'Euros de chiffre d'affaires, le Groupe Squad fait partie des premières forces cyber de France.

Depuis 2024, Squad a initié une stratégie de croissance forte, en intégrant Newlode (intégrateur cybersécurité) et Scassi (expert des systèmes critiques & embarqués) dans ses effectifs.
Ensemble, les 3 sociétés créent le Groupe Squad et proposent une offre autour de quatre grands métiers : l'audit, le conseil & l'expertise, l'intégration, et les services managés (MSSP).

Au quotidien, les experts du Groupe mènent des audits approfondis pour identifier les vulnérabilités et mesurer le niveau de résilience des systèmes. Ils conseillent et accompagnent les enjeux de transformation de nos clients. Ils renforcent leur posture cyber en concevant, intégrant et déployant des solutions de sécurité adaptées aux environnements IT comme OT. Enfin, ils assurent la supervision continue, la détection proactive et la réponse aux incidents de sécurité, au plus près des opérations. En tant que MSSP de confiance, le Groupe Squad garantit une proximité opérationnelle 24/7 pour une cybersécurité robuste et évolutive.

Réunis par la passion de leur métier, les experts du Groupe Squad poursuivent l'ambition de devenir l'acteur de référence en cybersécurité préféré et reconnu à la fois pour son expertise et sa réactivité auprès des grands comptes et pour sa capacité à attirer, développer et fidéliser les meilleurs talents dans un environnement convivial, inspirant et innovant.

Pour en savoir + : www.squadgroup.com

WWW.SQUADGROUP.COM

En collaboration avec les experts

EXTRAHOP™

FORESCOUT®

illumio

WIZ