Livre blanc

Directive NIS2 :

Sensibiliser votre comité de direction pour assurer la conformité

Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

Table des matières

NIS & NIS2, quelles différences ?

	NIS	NIS2
	**CHAMP D'APPLICATION**	
	Liste limitée d'opérateurs de services essentiels (OSE) et de fournisseurs de services numériques pertinents (OIV). Les OIV comprennent : les transports, les banques, les marchés financiers, l'eau potable, les infrastructures numériques, l'énergie, la santé.	L'éventail des secteurs est élargi aux services postaux/messagerie, industrie manufacturière, gestion des eaux usées, administration publique, espace, recherche, services numériques, production/distribution de denrées alimentaires, fournisseurs de communications électroniques, produits chimiques selon la taille des entités réglementées.
	**REPORTING / SÉCURITÉ**	
	Des exigences floues pour les OSE et les OIV concernant l'application de mesures de sécurité « appropriées » et le signalement des incidents qui ont un « impact significatif » sur la continuité des activités. Obligation d'informer l'autorité de régulation dans les 72 heures.	10 mesures de sécurité de base obligatoires (voir ci-dessous). Obligation d'informer l'autorité de régulation « sans retard injustifié » ou dans les 24 heures suivant un incident, et de déposer un rapport officiel dans les 72 heures. Les organisations ont également des obligations d'audit.
	**MISE EN APPLICATION**	
	Les États membres sont autorisés à fixer leur propre seuil pour les sanctions financières.	Règles de mise en application harmonisées. Des amendes pour les entités essentielles allant jusqu'à 10 M€ ou 2 % du CA annuel mondial*. Amendes pour les entités importantes pouvant aller jusqu'à 7 M€ ou 1,4 % du CA annuel mondial*. * Le montant le plus élevé est retenu
	**RESPONSABILITÉ DE LA DIRECTION**	
	Les cadres supérieurs ne sont pas tenus directement responsables des incidents.	Les cadres supérieurs peuvent être tenus personnellement responsables du non-respect de la législation en cas de négligence grave.

Introduction

Selon la Commission européenne, le coût annuel de la cybercriminalité pour l'économie mondiale était estimé à 5 500 milliards d'euros fin 2020. Il est prévu que ce montant double d'ici 2025.

Si cette sommes représentait un PIB, il s'agirait de la troisième économie mondiale derrière les États-Unis et la Chine. Les fournisseurs d'Infrastructures Nationales Critiques (CNI, Critical National Infrastructure), ainsi que leurs partenaires et fournisseurs, sont la cible d'un grand nombre d'attaques. En réponse à ces menaces et aux menaces croissantes de certains États, la Commission européenne a introduit une nouvelle version de sa directive européenne sur **la sécurité des réseaux et de l'information**, aussi appelée **NIS2** (ou SRI en français).

Les États membres ont jusqu'au 17 octobre 2024 pour transposer les exigences de la directive NIS2 dans leur législation nationale. Comme il s'agit d'une directive de l'UE (plutôt que d'un règlement), les pays interpréteront les règles de manière légèrement différente les uns des autres. Cela signifie que les organisations devront attendre que les versions de la directive NIS2 transposées localement soient publiées pour avoir une vision claire de leurs exigences et de leur calendrier de mise en conformité. Cependant, vous pouvez dès aujourd'hui vous préparer à l'entrée en vigueur des nouvelles règles.

Phil MUNCASTER

La directive NIS2 a pour objectif d'améliorer la cyber-résilience d'organisations assurant des fonctions essentielles ou importantes en Europe. Elle vise à réduire les incohérences dans la gestion des risques cyber et à encourager le partage d'informations entre les autorités compétentes. De plus, elle établit des règles claires pour la réponse aux incidents en cas de crise de grande ampleur.

Le coût d'une seule atteinte à la sécurité des données est estimé en moyenne à 4,1 millions d'euros, un record absolu. Ce chiffre peut toutefois être multiplié en cas d'attaque sérieuse par un ransomware qui interromprait également la disponibilité de services essentiels. La société de conseil européenne Sopra Steria a admis qu'une attaque de ransomware en 2020 avait pu lui coûter jusqu'à 50 millions d'euros.

Être conforme à NIS2 ne sert pas seulement à réduire les risques sur les finances et la réputation d'une organisation. Pour les membres des comités de direction, la raison est également plus pressante, car ils peuvent désormais être tenus personnellement responsables de la non-conformité s'il s'avère qu'une négligence grave est à l'origine d'un incident.

Ce sont là des raisons impérieuses pour lesquelles les RSSI devraient promouvoir la conformité à NIS2 auprès de leur comité de direction. Mais plutôt que d'envisager le processus comme un moyen d'atténuer les risques, ils peuvent également présenter des arguments convaincants en faveur de la conformité en tant que catalyseur de l'activité. En considérant les défis représentés par la directive comme une opportunité, les organisations peuvent mettre en place les bons éléments pour réussir leur transformation numérique et assurer une croissance durable.

Ce livre blanc décrit ce que les RSSI et les comités de direction doivent faire pour y parvenir.

En se conformant à NIS2, les membres des comités de direction peuvent non seulement éviter d'être tenus personnellement responsables en cas de négligence grave à l'origine d'un incident, mais également saisir l'opportunité offerte par la directive pour réussir la transformation numérique de leur organisation et assurer sa croissance durable.

Quelles sont les nouveautés de NIS2 ?

La directive NIS2 comprend plusieurs changements clés par rapport à la directive d'origine. Les principaux changements sont les suivants :

UN CHAMP D'APPLICATION PLUS ÉTENDU

La directive NIS2 s'appliquera aux organisations des secteurs considérés comme fournisseurs de services « essentiels » ou « importants ». Le premier groupe comprend de grands opérateurs de secteurs hautement critiques tels que l'énergie, la banque et la santé, ainsi que quelques cas particuliers. Cette dernière catégorie comprend les grands opérateurs d'autres secteurs critiques, tels que les fournisseurs de services numériques et les fabricants, ainsi que les opérateurs de taille moyenne.

DES AMENDES PLUS ÉLEVÉES

Les régulateurs pourront infliger aux organisations des amendes allant jusqu'à 2 % de leur chiffre d'affaires annuel, ou 10 millions d'euros en cas de manquement grave. Certaines sanctions peuvent être également imposées de manière continue.

DES EXIGENCES MINIMALES DE SÉCURITÉ

La directive NIS2 introduit un ensemble de mesures de base que toutes les organisations doivent respecter. Ce sont :

- Analyse des risques et politiques de sécurité de l'information
- Prévention, détection et réponse aux incidents
- Continuité des activités et gestion des crises, avec reprise après sinistre
- Sécurité des chaînes d'approvisionnement
- Protection de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, avec gestion des vulnérabilités
- Test et audit des mesures de gestion des risques cyber
- Cyber-hygiène de base, avec formation à la cybersécurité
- Politiques et procédures relatives à l'utilisation de la cryptographie et du chiffrement
- Sécurité des ressources humaines, avec politiques de contrôle des accès et gestion des actifs
- Authentification multifacteur ou authentification continue ; communications vocales, vidéo et texte sécurisées ; et systèmes de communication d'urgence sécurisés

SÉCURITÉ DES CHAÎNES D'APPROVISIONNEMENT

Les organisations doivent évaluer et gérer les risques liés aux tiers en utilisant des « mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées ». Cela doit commencer par une évaluation coordonnée des risques.

RESPONSABILITÉ DE LA DIRECTION

Les cadres supérieurs seront directement responsables de la sécurité au sein de leur organisation. Les PDG ou les représentants légaux peuvent faire l'objet d'une interdiction temporaire d'exercer en cas de négligence entraînant une atteinte grave à la sécurité. Ils doivent recevoir une formation à la cybersécurité et procéder à des évaluations régulières des risques.

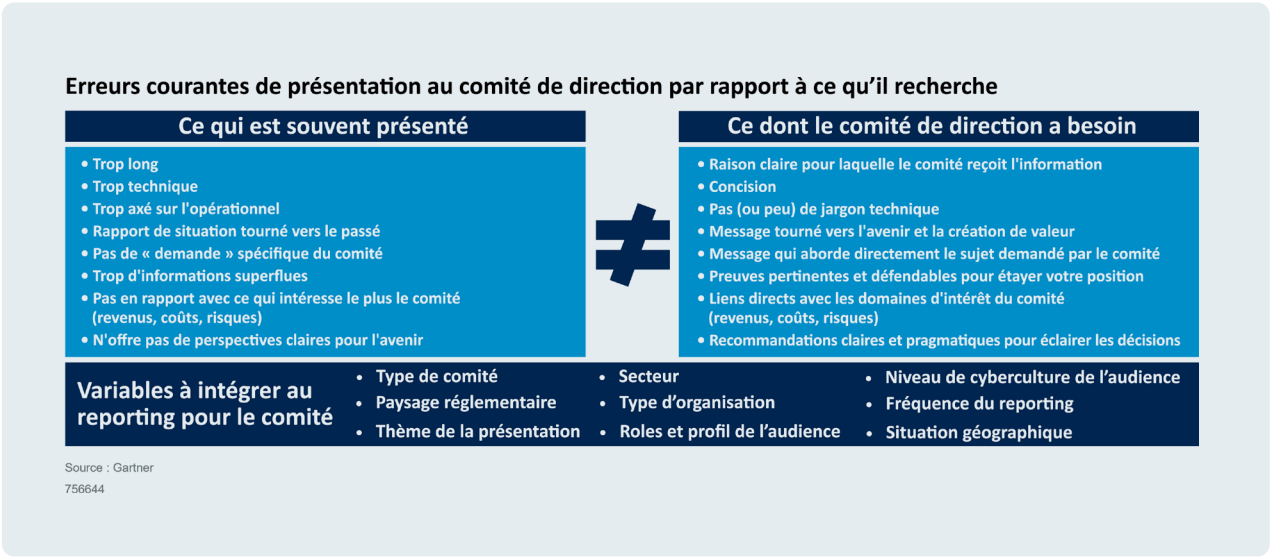
Aborder NIS2 en comité de direction

Les membres des comités de direction sont de plus en plus conscients de l'importance de la cybersécurité pour la réussite de leur organisation. Une étude du Forum économique mondial (FEM) réalisée en 2023 affirme que « l'instabilité géopolitique mondiale a contribué à combler l'écart de perception entre les responsables métiers et informatiques sur l'importance de la gestion des risques cyber. »

En dépit de ces progrès, certaines mentalités héritées du passé perdurent, notamment de considérer que tout ce qui touche au domaine du « cyber » relève purement des opérations informatiques plutôt que d'être une fonction métier stratégique. Une enquête de PwC réalisée en 2023 note que seulement deux cinquièmes (41 %) des cadres supérieurs estiment que leur comité de direction comprend « très bien » les risques liés à la sécurité. Une autre étude révèle que seulement 5 % des membres des comités de direction européens ont une expérience en matière de cybersécurité.

Les défis des RSSI seront d'autant plus importants qu'ils essaieront de faire comprendre aux chefs d'entreprise l'importance de la conformité à NIS2. Gartner® a identifié 8 « erreurs courantes de présentation au comité de direction » :

Figure 1 : Les erreurs les plus courantes en matière de présentation au comité de direction et ce qu'il recherche



Source : *Gartner®*, *Fondations pour les RSSI : Liste de ressources complète pour présenter la cybersécurité au comité de direction*, publication initiale le 8 août 2022. Mise à jour le 26 septembre 2023. GARTNER est une marque commerciale déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays, et est utilisée ici avec autorisation. Tous droits réservés.

Pour veiller à ce que les comités de direction reçoivent le bon message, les RSSI devraient :

UTILISER LE BON LANGAGE ET RESTER BREFS

La première étape vers une harmonisation des départements métiers et de l'informatique sur la conformité à NIS2 consiste à adopter un langage commun compréhensible. Cela signifie qu'il faut parler le langage du risque métier plutôt que de détails technologiques complexes. Les RSSI devraient abandonner le jargon technique et utiliser un langage simple, clair et accessible. Des anecdotes provenant de l'organisation ou de concurrents peuvent également aider à faire passer un message. Expliquer avec des exemples concrets ce qui est arrivé à une entreprise lorsqu'elle n'a pas respecté les règles de cybersécurité est un moyen efficace d'influencer l'opinion du comité de direction.

Quel que soit le contenu, les RSSI devraient également être conscients que leur audience aura une durée d'attention limitée. Cela signifie qu'ils devraient se concentrer sur les points essentiels, limiter le nombre de diapositives, et veiller à ce que la présentation soit brève et attrayante.

SE PRÉPARER À FAIRE PLUS AVEC MOINS

Les RSSI devraient s'attendre à ce que les comités de direction leur demandent de se conformer à NIS2 avec leur budget actuel. Ceux qui auront préparé à l'avance un rapport soulignant les réductions et les coupes possibles dans leur budget gagneront plus facilement l'adhésion de leur directeur financier et de leur comité de direction.

RENDRE LA DISCUSSION PERTINENTE POUR LEUR AUDIENCE

La pertinence est essentielle. Il ne s'agit pas seulement de présenter des indicateurs et de parler des risques métiers que les membres du comité de direction comprendront, mais également de les sensibiliser à l'impact potentiel d'une non-conformité sur leur responsabilité personnelle. Cela devrait être relativement simple étant donné les nouvelles obligations prévues par la directive NIS2 pour les des cadres supérieurs.

Les RSSI doivent également expliquer l'impact potentiel du non-respect des exigences de la

Les amendes pour les entités essentielles s'élèvent à

10 M€

ou 2 %
du CA annuel mondial.

Les amendes pour les entités importantes s'élèvent à

7 M€

ou 1,4 % au moins
du CA annuel mondial.

Le montant le plus élevé est retenu.

directive NIS2, en termes de dommages sur les finances et la réputation qui pourraient découler de graves atteintes à la sécurité. Il peut s'agir :

- De conséquences des atteintes à la sécurité, notamment des amendes réglementaires et des frais de justice
- D'exigences en matière d'audit et de preuve de conformité, qui pourraient donner lieu à des amendes de la part des autorités de surveillance si les exigences ne sont pas respectées
- De perte d'activité, y compris une interruption immédiate, la perte de clients et l'impossibilité d'en acquérir de nouveaux

Dans le cadre de cette discussion, il peut également être utile d'articuler la manière dont les régulateurs mettront en œuvre la nouvelle directive. Pour les deux types d'entités, les autorités auront le pouvoir de procéder à des inspections sur site et à une supervision à distance après les faits, ainsi qu'à des audits de sécurité ad hoc, à des analyses de sécurité et des demandes d'accès aux données. Ces dernières peuvent inclure des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats d'audits de sécurité réalisés par des tiers.

ARGUMENTER EN FAVEUR DE LA CONFORMITÉ

Les RSSI n'ont pas besoin de structurer la conformité à NIS2 en termes d'évitement des risques. Elle peut également fournir de robustes avantages pour l'organisation. Plus précisément, la conformité à NIS2 peut contribuer à :

- Réduire les coûts d'exploitation en éliminant ou en minimisant les temps d'arrêt, les amendes et les autres coûts énumérés ci-dessus.
- Augmenter le chiffre d'affaires en aidant l'organisation à se différencier et attirer les clients pour qui la sécurité et la confidentialité sont prioritaires. Environ 87 % des consommateurs déclarent qu'ils feront leurs achats ailleurs s'ils ne sont pas convaincus qu'une entreprise traite leurs données de manière responsable. Les certifications volontaires telles que la certification ENISA de l'UE ou les certifications et les rapports d'audit pertinents pour des secteurs spécifiques constituent un important facteur de différenciation concurrentielle.
- Se différencier et attirer des partenaires commerciaux qui accordent la priorité à la sécurité. La plupart des organisations auxquelles vous fournissez des produits ou avec lesquelles vous faites des affaires exigeront une conformité à NIS2 ; vous devriez donc être en mesure d'y répondre. Vous devriez également l'exiger de vos fournisseurs.
- Renforcer l'efficacité interne en améliorant les processus et en réduisant les erreurs.
- Alimenter la croissance par l'innovation en fournissant une base stable et sécurisée pour la transformation numérique.

PRÉSENTER SA CONFORMITÉ COMME UNE OPPORTUNITÉ

La conformité à NIS2 n'est pas simplement quelque chose qu'il est bon d'avoir. C'est la loi. Il est donc conseillé aux membres des comités de direction de se tenir informés de la transposition de la directive NIS2 au niveau national, lorsqu'elle entrera en vigueur aux alentours d'octobre 2024. Ils pourront alors évaluer plus clairement leur degré de conformité et les investissements encore nécessaires pour .

Les RSSI devraient saisir l'occasion qui leur est offerte de veiller à ce que le comité de direction investisse davantage dans la sécurité. Ce pourrait être par exemple le moment de promouvoir la nécessité d'un programme de bonnes pratiques Zero Trust pluriannuel.

62 %

des opérateurs de services et des fournisseurs de services numériques dans l'UE estiment que la directive NIS a eu un impact positif sur la détection des menaces.

Source : *ENISA, Investissements pour NIS, novembre 2022*.

21 %

ou 1/5

confirment cet impact sur la capacité à se remettre rapidement d'un incident.

Source : *ENISA, Investissements pour NIS, novembre 2022*.

Comme toujours, des indicateurs peuvent aider à formuler les arguments. Selon l'ENISA, l'agence de sécurité de l'UE, 62 % des opérateurs de services essentiels et des fournisseurs de services numériques de la région estiment que la mise en œuvre de la première directive NIS a eu un impact direct et positif sur la détection des menaces. Et un cinquième (21 %) confirme cet impact sur la capacité à se remettre rapidement d'un incident.

Anatomie d'un programme de conformité à NIS2

Une fois que le comité de direction a accepté de financer un programme de conformité à NIS2, les étapes de préparation du projet peuvent commencer. La première consiste à déterminer si l'organisation est une entité essentielle ou importante. Cela déterminera les règles à suivre et les sanctions potentielles en cas de non-respect.

Considérez ensuite les démarches suivantes :

1. **Déterminez le champs d'application :** Quels sont les services réglementés ? Comment l'organisation peut-elle les encadrer en termes d'actifs, d'unités organisationnelles, de sites et de réseaux ?
2. **Effectuez une analyse des écarts :** Pour évaluer la posture de sécurité existante, et mettre en évidence des domaines de non-conformité à NIS2 et d'autres vulnérabilités. Elle devrait permettre de formuler des recommandations concrètes pour améliorer les contrôles de sécurité, la gouvernance et d'autres domaines essentiels.
3. **Planifiez le programme de conformité :** Il devrait comprendre une formation et une sensibilisation du personnel et de la direction, conformément aux nouvelles exigences de NIS2.
4. **Envisagez la possibilité de bénéficier d'une aide de l'État :** Pour aider à financer les efforts de mise en conformité à NIS2. La Commission européenne a mis de côté une importante enveloppe financière pour aider spécifiquement les PME.
5. **Mettez le projet en œuvre.**
6. **Effectuez des examens / audits préliminaires :** Pour vérifier l'état de la conformité.
7. **Faites des ajustements et revenez au point 3 jusqu'à ce que l'organisation soit conforme.**

Concepts à garder à l'esprit

Des dizaines de milliers d'organisations à travers l'UE entreront dans le champ d'application de la nouvelle directive NIS2. Certaines seront en mesure de gérer la conformité en interne. Toutefois, de nombreuses petites entreprises devront faire appel à une expertise externe, et éventuellement à un financement, pour les aider à accélérer leur parcours avant l'échéance d'octobre 2024.

Tout au long de ce processus, les RSSI devraient garder à l'esprit trois concepts clés : la communication, la sensibilisation et la résilience collective. La communication avec la direction, et sa sensibilisation, sont essentielles pour garantir le financement nécessaire et veiller à ce que les cadres supérieurs disposent des niveaux de connaissance et d'engagement adéquats pour prendre des décisions clés en matière de gestion des risques. Il s'agit avant tout de mettre en place une défense collective robuste à l'échelle européenne contre les cybermenaces.

Conclusion : Il est temps de passer à l'action

Selon l'enquête du FEM, la plupart des responsables métiers et de la cybersécurité affirment que les tensions géopolitiques sont « modérément » (93 %) ou « très probablement » (86 %) susceptibles d'entraîner un cyberévènement catastrophique au cours des deux prochaines années. Les enjeux ne pourraient être plus élevés. C'est pourquoi la directive NIS2 a été conçue, non seulement pour améliorer la cyber-résilience dans l'ensemble de l'Union, mais également pour en faire un enjeu des comités de direction des fournisseurs de services les plus importants. Si, comme l'affirme l'ancienne patronne d'IBM Ginni Rometty, les PDG d'aujourd'hui doivent également être des directeurs du risque de leur organisation, et les questions liées à l'informatique doivent être au cœur de toutes les orientations futures. Pourtant, la plupart (72 %) sont encore mal à l'aise quant aux décisions à prendre en matière de sécurité. Cela doit changer, et la directive NIS2 permettra ce changement.

Une grande responsabilité repose cependant sur les épaules des RSSI. Ce sont eux qui doivent convaincre le comité de direction et le PDG de l'importance de la conformité à NIS2, non seulement pour éviter les risques métiers, mais également pour permettre à l'organisation de se développer et de mener à bien sa transformation numérique. C'est donc à eux qu'il incombe d'orienter l'organisations vers la conformité, y compris par la formation et la sensibilisation des cadres supérieurs. Ce ne sera pas facile, mais les RSSI capables de relever ces défis verront leur rôle et leurs perspectives de carrière s'améliorer.

L'effort nécessaire dépendra de la maturité de la posture et des processus de sécurité existants de l'organisation, ainsi que du niveau d'engagement de la direction générale. Mais comme pour tout programme de conformité, la directive NIS2 est un parcours continu et non une destination. La seule certitude est qu'il doit commencer maintenant.

MINIMISER SA SURFACE D'ATTAQUE ET OPTIMISER SA CONFORMITÉ À NIS2

Gestion des vulnérabilités et des correctifs
Votre organisation peut bénéficier d'une couche de sécurité supplémentaire grâce au suivi actif des vulnérabilités des systèmes d'exploitation et des applications les plus répandues, ainsi qu'à l'application automatisée de correctifs sur l'ensemble des endpoints gérés par ESET PROTECT.

Détection et réponse étendues (XDR)
ESET Inspect, notre solution d'XDR, offre aux gestionnaires de risques et au personnel chargé de répondre aux incidents une visibilité exceptionnelle sur les menaces. Elle leur permet d'effectuer une analyse rapide et approfondie des causes profondes, et de répondre immédiatement aux incidents.

ESET Endpoint Encryption
Il fournit une fonctionnalité simple et puissante de chiffrement des données, pour améliorer considérablement la sécurité des données de votre entreprise et la conformité aux réglementations.

Détection et réponse managées
ESET MDR et ESET Detection & Response Ultimate sont des services de gestion des menaces 24/7, utilisant l'IA et l'expertise humaine pour fournir une protection de haut niveau contre les ransomwares, sans nécessiter de spécialistes sécurité en interne.

ESET Threat Intelligence (ETI)
La Threat Intelligence des experts d'ESET de renommée mondiale fournit des informations et des rapports approfondis sur les menaces. Bénéficiez d'une perspective unique sur le paysage des menaces et améliorez votre posture de cybersécurité.

ESET PROTECT Platform
Une plateforme de cybersécurité unifiée qui intègre de puissantes fonctionnalités de prévention, de détection et de réponse aux atteintes à la sécurité, complétées par les services professionnels et managés d'ESET.

Une protection complète avec un service MDR 24/7
Découvrez **ESET PROTECT MDR**

EN SAVOIR PLUS

Défense proactive.
Nous minimisons la surface d'attaque.

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre **approche préventive reposant sur l'IA et l'expertise humaine**.

Bénéficiez d'une protection de haut niveau grâce à notre **Threat Intelligence** interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des **chercheurs reconnus**.

ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

Digital Security
Progress. Protected.

+ 30
années d'expertise

+ 1 Mrd
d'internautes protégés

+ 400 k
entreprises clientes

195
pays et territoires

13
centres de recherche

protégé par ESET depuis 2016
plus de 32 000 endpoints

partenaire FAI depuis 2008
2 millions d'utilisateurs

protégé par ESET depuis 2016
plus de 4 000 boîtes mail

protégé par ESET depuis 2017
plus de 9 000 endpoints

Plus de 30 ans d'innovation

1er éditeur Européen de solutions de sécurité

Focus continu sur la technologie

Croissance continue depuis sa création

Digital Security
Progress. Protected.

Eversheds Sutherland est un cabinet international d'avocats et de notaires qui compte 74 bureaux dans 35 pays et emploie plus de 3 000 juristes. Grâce à notre caractère international, nous sommes en mesure de fournir des conseils transfrontaliers comme personne d'autre. Eversheds Sutherland possède 44 succursales en Europe.

Février 2024