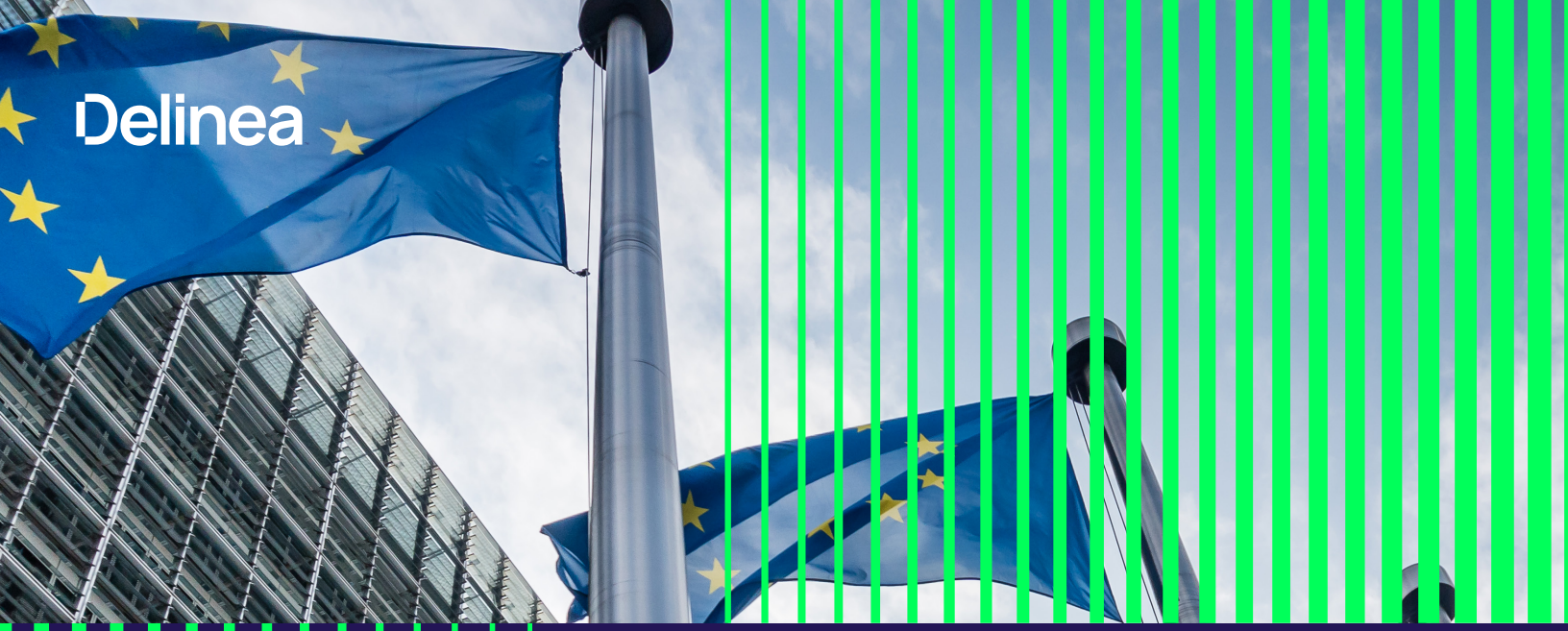
Delinea



Guide de la directive NIS2

À quoi s'attendre et comment se préparer ?

LIVRE BLANC

Synthèse

L'Union européenne (UE) a récemment publié une directive fondamentale visant à protéger des cybermenaces l'ensemble des secteurs majeurs de l'économie européenne. La *directive (UE) 2022/2555*, connue sous le nom de NIS2, comprend des mesures visant à assurer un niveau commun élevé de cybersécurité pour les réseaux et les systèmes d'information dans l'ensemble de l'UE.

La directive NIS2 énonce les conditions que doivent remplir les États membres et les entreprises dans le cadre de leurs stratégies de cybersécurité avant le 17 octobre 2024. Si l'on tient compte du temps nécessaire pour planifier, mettre en œuvre et tester de nouveaux outils, stratégies et procédures, il est important de s'y atteler dès maintenant.

Dans ce livre blanc, vous découvrirez le contexte, les changements et les objectifs de la directive NIS2 et ce que l'on peut en attendre en termes de surveillance. Vous verrez dans quelle mesure votre programme de cybersécurité actuel répond aux exigences de la directive NIS2 et vous découvrirez, le cas échéant, comment en combler les lacunes.

Contexte de la directive NIS

La directive NIS2 définit les conditions relatives à la communication entre les États membres de l'Union européenne, la gestion des risques et des incidents par les organismes de cybersécurité nationaux et l'adoption de stratégies par les entreprises de secteurs déterminés. Bien que la directive NIS2 soit essentiellement axée sur les moyennes et grandes entreprises, elle reconnaît également l'importance d'une cybersécurité renforcée pour les infrastructures et les services essentiels ayant un impact sur les TPE et les petites entreprises.

Officiellement adoptée par la Commission européenne en fin novembre 2022, la directive NIS2 est le prolongement d'une publication antérieure qui présentait certaines limites.

Pourquoi l'UE a-t-elle publié une deuxième version de la directive NIS ?

La première édition de la directive NIS, publiée en 2016, a permis d'améliorer la cyber-résilience globale au sein de l'UE. Elle a donné aux pays un cadre pour gérer les incidents de cybersécurité par l'intermédiaire d'une équipe chargée de répondre aux incidents de sécurité informatique (CSIRT) et d'une autorité compétente en matière de NIS. Elle a formé le Cooperation Group, une plateforme permettant aux États membres d'échanger des informations essentielles. Elle a également défini les opérateurs de services critiques, c'est-à-dire des entreprises essentielles à des secteurs tels que les services publics, les soins de santé, les transports et l'infrastructure numérique.

La directive NIS a servi de catalyseur efficace pour modifier l'approche directive de l'UE en matière de cybersécurité. Elle a également ouvert la voie à l'établissement de stratégies nationales pour la sécurité des réseaux et des systèmes d'information, ainsi que de mesures réglementaires couvrant les infrastructures essentielles.

Limites de la directive NIS

Cependant, la première édition de la directive NIS présentait plusieurs limites. Les pays de l'UE étaient responsables de la mise en œuvre de la directive NIS, ce qui a entraîné des disparités au niveau national, en particulier dans des domaines tels que la sécurité et le signalement des incidents, ainsi que la supervision et l'application. Il a été constaté un manque évident de discipline en ce qui concerne le signalement des incidents et l'application de sanctions.

La couverture des secteurs par la directive NIS était également trop limitée, et le champ d'application des opérateurs de services essentiels n'était pas clair.

Depuis l'annonce initiale de la directive NIS, la transformation numérique s'est accélérée dans toute l'Europe, les données et les communications traversant les frontières. Cela a élargi le paysage des cybermenaces et ouvert la voie à une augmentation du volume et de la sophistication des cyberincidents. Les États membres ont subi une intensification des cyberattaques pendant la pandémie de COVID-19, ce qui a mis en évidence la vulnérabilité des entreprises numériques ultra connectées.

L'un des principaux défis que la Commission européenne cherche à relever est l'interdépendance entre les États membres des secteurs tels que **l'énergie, les transports, l'infrastructure numérique, l'eau potable et les eaux usées, la santé, certains aspects de l'administration publique**, ainsi que **le secteur spacial**. Cela souligne l'importance de sécuriser ces entités, qu'elles soient publiques ou privées, car toute perturbation de ces services entraînera des conséquences transfrontalières.

Dans ce contexte, la Commission européenne a apporté plusieurs amendements à la deuxième version de la directive NIS.

Nouveautés dans la directive NIS2

Avec la publication de la directive NIS2, la Commission cherche à renforcer le signalement des incidents et la réponse à ces incidents, ainsi qu'à améliorer l'échange global d'informations entre les parties prenantes.

Nouvelle administration

La directive NIS2 crée de nouveaux organes chargés de gérer ces tâches et étend les responsabilités des organes existants.

EU-CyCLONe

La directive établit le réseau de coordination EU-CyCLONe (European Cyber Crises Liaison Organisation Network) pour la gestion de crise des incidents à grande échelle, que la Commission définit comme des incidents susceptibles de provoquer une grave perturbation opérationnelle des services et des pertes financières importantes ou d'affecter les personnes en causant des dommages matériels ou immatériels considérables.

Le réseau EU-CyCLONe coordonnera la gestion des incidents et des crises de cybersécurité à grande échelle afin de garantir l'échange d'informations entre les États membres et les autres institutions. Le réseau EU-CyCLONe participera également à l'évaluation des conséquences des incidents à grande échelle et proposera des mesures d'atténuation possibles.

Le Cooperation Group

Le Cooperation Group restera un organe global, composé de représentants des États membres, de la Commission et de l'Agence de l'Union européenne pour la cybersécurité (ENISA). Il supervisera et fournira des conseils sur la mise en œuvre de la directive NIS2. En cas de problèmes (incidents, communication et signalement), le Cooperation Group fournira des orientations stratégiques aux équipes nationales chargées de la réponse aux incidents de cybersécurité (réseau des CSIRT) et au réseau EU-CyCLONe. Bien que les responsabilités telles que le partage d'informations et l'échange de bonnes pratiques, la sensibilisation et la formation soient similaires à celles attribuées à l'ENISA, aux CSIRT ou au réseau EU-CyCLONe, le Cooperation Group aura un profil plus stratégique et de contrôle. En outre, il effectuera des évaluations des risques de sécurité des chaînes d'approvisionnement critiques, tâche importante du point de vue de la sécurité des infrastructures essentielles.

Nouveaux outils de partage d'informations

En améliorant l'échange d'informations, la directive NIS2 permettra aux praticiens de la cybersécurité de tirer des enseignements des incidents passés.

L'ENISA, secrétariat du réseau EU-CyCLONe, préparera une base de données des vulnérabilités dans laquelle les entreprises pourront enregistrer les incidents et divulguer des informations afin que d'autres puissent en tirer des enseignements.

L'ENISA coordonnera également les évaluations par les pairs des expériences, y compris la mise en œuvre des mesures ou les incidents transfrontaliers. En cas de succès, cela pourrait déboucher sur la création d'une base de données de pratiques d'excellence afin d'améliorer la compréhension des cyberincidents et des contrôles et pratiques en matière de cybersécurité chez les États membres.

Nouvelles obligations de signalement

Dans la directive NIS2, la Commission met davantage l'accent sur le signalement des incidents dès les premiers stades. Les entreprises doivent informer le réseau CSIRT ou un point de contact désigné dans un délai de **24 heures** à compter de la prise de connaissance d'un incident causé par des actes illégaux ou malveillants. Pour éviter la propagation de ces actes au sein des entreprises et des entités ultra connectées de l'UE, celles-ci doivent également signaler les incidents susceptibles d'avoir un impact transfrontalier.

Le rapport initial doit être suivi d'une notification dans un délai de **72 heures**, afin de mettre à jour les informations et d'évaluer la gravité de l'incident. Le processus doit se conclure par un rapport final au plus tard un mois après le premier signalement de l'incident. Il doit comporter une description détaillée de l'incident, y compris la cause probable, les mesures d'atténuation appliquées et tout impact transfrontalier.

Les institutions financières qui se conforment actuellement au Règlement (UE) 2022/2554 relatif à la gestion des risques liés aux TIC et au signalement des incidents doivent continuer à le faire et ne sont pas tenues d'appliquer les dispositions de la directive NIS2 relatives à la gestion des risques de cybersécurité et aux obligations de signalement, de supervision et d'application.

Nouveaux secteurs

Pour assurer la continuité des services et le bon fonctionnement de l'économie européenne, la directive NIS2 élargit la liste des secteurs critiques qui doivent être protégés des menaces pesant sur les réseaux et les systèmes d'information. Ainsi, de nouveaux secteurs tels que les eaux usées, l'espace et l'agroalimentaire sont désormais couverts par la législation.

Parmi les secteurs à forte criticité figurent les secteurs suivants :

1. **Énergie**
   - Électricité
   - Chauffage et climatisation urbains
   - Pétrole
   - Gaz
   - Hydrogène
2. **Transports**
   - Aériens
   - Ferroviaires
   - Maritimes
   - Terrestres
3. **Banques**
4. **Infrastructures des marchés financiers**
5. **Santé, y compris la fabrication de produits pharmaceutiques, dont les vaccins**
6. **Eau potable**
7. **Eaux usées**
8. **Infrastructures numériques**
   - Points d'échange Internet
   - Prestataires de services DNS
   - Registres de noms TLD
   - Prestataires de services informatiques dans le cloud
   - Prestataires de services de centre de données
   - Réseaux de diffusion de contenu
   - Prestataires de services de confiance
   - Prestataires de réseaux de communications électroniques publics
   - Services de communications électroniques accessibles au public
9. **Gestion des services TIC**
   - Prestataires de services gérés
   - Prestataires de services de sécurité gérés
10. **Administration publique**
11. **Espace**

Parmi les autres secteurs critiques figurent les services suivants :

1. **Services postaux et de messagerie**
2. **Gestion des déchets**
3. **Fabrication, production et distribution de produits chimiques**
4. **Production, transformation et distribution de denrées alimentaires**
5. **Fabrication**
   - Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro
   - Fabrication de produits informatiques, électroniques et optiques
   - Fabrication d'équipements électriques
   - Fabrication de machines et d'équipements
   - Fabrication de véhicules motorisés, de remorques et de semi-remorques
   - Fabrication d'autres équipements de transport
6. **Fournisseurs numériques**
   - Fournisseurs de places de marché en ligne
   - Fournisseurs de moteurs de recherche en ligne
   - Fournisseurs de plateformes de services de réseaux sociaux

Nouvelle classification des entités

Dans la version originale de la directive NIS, les entités étaient classées en tant qu'Opérateurs de services essentiels (OES) et Prestataires de services numériques (DSP). La directive NIS2 change cela en lançant la classification des entités comme « **essentielles** » ou « **importantes** », reflétant le degré de criticité de leurs services et leur taille. Lors de l'élaboration des mesures de cybersécurité, les États membres doivent tenir compte de l'exposition au risque des entités importantes et essentielles en termes d'impact social et économique d'une cyberattaque effective.

Nouvelles mesures d'application et amendes

Les entreprises qui tombent dans la catégorie des entités essentielles feront l'objet d'audits, d'inspections sur site et d'une supervision hors site. Elles devront fournir des stratégies de cybersécurité documentées, un accès aux données, documents et informations, ainsi que des preuves de la mise en œuvre desdites stratégies.

Les États membres devront veiller à ce que les autorités compétentes puissent exercer leurs pouvoirs d'exécution en émettant des avertissements, en adoptant des instructions, en désignant un agent de contrôle, en suspendant les certifications, etc. Si ces mesures n'aboutissent pas, l'organe d'autorité peut suspendre temporairement les responsabilités managériales des dirigeants, y compris des directeurs généraux et des représentants légaux.

Les entités importantes utilisent en grande partie les mêmes outils d'application que les entités essentielles. Il existe toutefois une approche plus souple en matière d'application. Les organes d'autorité émettront des recommandations quant à la manière de combler les lacunes en matière de conformité.

La directive NIS2 lance également une série d'amendes à imposer aux entités qui ne se conforment pas à la législation. L'amende maximale imposée aux entités essentielles est au minimum de **10 000 000 €** ou de **2 % du chiffre d'affaires annuel mondial total** de l'exercice financier précédent, le montant le plus élevé étant celui retenu. En ce qui concerne les entités importantes, la directive NIS2 demande aux États membres d'imposer une amende maximale au minimum de **7 000 000 €** ou de **1,4 % du chiffre d'affaires annuel mondial total** de l'exercice financier précédent, le montant le plus élevé étant celui retenu.

Nouveaux prestataires

La Commission établit également une ligne de communication avec les prestataires de services qui offrent des services étendus dans les États membres mais qui ne sont pas basés dans l'UE. Les prestataires qui utilisent une langue ou une monnaie locale pour vendre des produits ou des services, ou qui mentionnent des clients ou des utilisateurs dans l'Union européenne, devront désigner un représentant. L'ENISA créera et gérera le registre de ces prestataires.

Parmi les prestataires de services figurent les prestataires suivants :

- Prestataires de services DNS
- Registres de noms TLD
- Entités fournissant des services d'enregistrement de noms de domaine
- Prestataires de services informatiques dans le cloud
- Prestataires de services de centre de données
- Fournisseurs de réseaux de diffusion de contenu
- Prestataires de services gérés
- Prestataires de services de sécurité gérés
- Fournisseurs de places de marché en ligne, de moteurs de recherche ou de services de réseaux sociaux

Exigences en matière de cybersécurité

Les entreprises doivent mettre en place une stratégie active de cyberprotection qui comprend la prévention, la détection, la surveillance, l'analyse et l'atténuation.

Les entreprises essentielles et importantes sont tenues de gérer les risques pesant sur les réseaux et les systèmes d'information et de prévenir ou de minimiser l'impact des incidents.

Ces mesures incluent :

- Stratégies en matière d'analyse des risques et de sécurité des systèmes d'information
- Gestion des incidents
- Continuité des activités
- Sécurité de la chaîne d'approvisionnement
- Sécurité lors de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris la gestion et la divulgation des vulnérabilités
- Stratégies et procédures visant à évaluer l'efficacité des mesures de gestion des risques liés à la cybersécurité
- Pratiques de cyberhygiène et formation à la cybersécurité
- Chiffrement
- Sécurité des ressources humaines, stratégies de contrôle d'accès et gestion des ressources
- Recours à l'authentification multi-facteurs ou à des solutions d'authentification continue, aux communications vocales, vidéo et texte sécurisées, et à des systèmes de communication d'urgence sécurisés au sein de l'entité, le cas échéant

Exigences en matière de cyberhygiène

La directive NIS2 souligne l'importance de la cyberhygiène comme fondement de la protection de l'infrastructure réseau et des systèmes d'information, du matériel, des logiciels, de la sécurité des applications et des données personnelles et professionnelles. L'ENISA surveillera et analysera la mise en œuvre des stratégies de cyberhygiène par les pays de l'UE.

Les exigences sont les suivantes :

- Modifications des mots de passe
- Limitation des comptes d'accès au niveau administrateur
- Gestion des identités et des accès
- Mises à jour des logiciels et du matériel informatique
- Gestion des nouvelles installations
- Sauvegarde des données

Calendrier

D'ici le 17 juillet 2023

La Commission fournira des lignes directrices sur l'adoption de mesures de gestion des risques liés à la cybersécurité.

D'ici le 17 octobre 2024

Les pays de l'UE doivent adopter et publier les mesures nécessaires pour se conformer à la directive NIS2.

D'ici le 17 octobre 2024

La Commission adoptera également des lois d'exécution fixant les exigences techniques et méthodologiques des mesures concernant les prestataires de services DNS, les registres de noms TLD, les prestataires de services informatiques dans le cloud, les prestataires de services de centre de données, les fournisseurs de réseaux de diffusion de contenu, les prestataires de services gérés, les prestataires de services de sécurité gérés, les fournisseurs de places de marché en ligne, de moteurs de recherche et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

D'ici le 17 octobre 2024

Les pays de l'UE doivent adopter et publier les mesures nécessaires pour se conformer à la directive NIS2.

- Principes du Zero Trust
- Cadre proactif de préparation et de sûreté et de sécurité globales en cas d'incidents ou de cybermenaces
- Les entreprises doivent également mettre en place une stratégie de formation active afin de sensibiliser les employés à la sécurité.

Exigences supplémentaires pour les réseaux publics de communications électroniques

Outre les pratiques fondamentales de cyberhygiène susmentionnées, les fournisseurs de réseaux publics de communications électroniques doivent également utiliser le chiffrement de bout en bout et des concepts de sécurité axés sur les données tels que la cartographie, la segmentation, le balisage, des stratégies d'accès et la gestion des accès, ainsi que des décisions d'accès automatisées.

Adoption plus poussée de la technologie

La Commission européenne conseille aux entreprises d'adopter des systèmes d'IA et d'apprentissage automatique pour renforcer encore davantage les fonctionnalités de sécurité. Elle considère ces technologies comme des outils permettant d'améliorer la détection et la prévention des cyberattaques.

Comment se préparer à l'adoption de la directive NIS2

Au cours de ces deux dernières années, les pays européens ont constaté une augmentation exponentielle des attaques de rançongiciels et de logiciels malveillants. En l'absence de stratégie active et de mise en œuvre de stratégies de cybersécurité appropriées, les entreprises européennes opérant dans des secteurs critiques resteront vulnérables.

La directive NIS2 exige des entreprises qu'elles adoptent des stratégies de gestion des mots de passe, des identités et des accès, ainsi que de contrôle des applications. Ces stratégies peuvent être couvertes par les solutions modernes et complètes de gestion des accès à privilèges (PAM), qui peuvent vous aider à répondre dans une large mesure à la plupart des exigences à venir.

Gestion des mots de passe

La solution PAM proposée par Delinea effectue une rotation automatique des mots de passe en fonction d'un calendrier, en cas d'événement (tel que la vérification d'un mot de passe) ou à la demande, de sorte à bloquer toute personne ayant accès à des identifiants plus anciens. Elle garantit des mots de passe uniques dans tous les systèmes et promeut la qualité des mots de passe personnalisés.

Elle stocke également les mots de passe gérés en toute sécurité dans un coffre chiffré. Lorsqu'elle est utilisée pour contrôler l'accès à des serveurs reliés à des domaines Active Directory, la solution Delinea peut utiliser les stratégies de sécurité AD natives pour la gestion des informations d'identification.

Gestion des applications

Les solutions Privilege Manager et Server PAM de Delinea simplifient la gestion des applications en établissant des règles et des stratégies, ainsi qu'en offrant aux administrateurs un accès juste-à-temps. Elles proposent la génération de rapports, des fonctionnalités d'audit et l'enregistrement des sessions pour contrôler les activités des utilisateurs. Grâce à Privilege Manager, vous pouvez contrôler les applications connues à l'aide de listes d'autorisation et d'exclusion et analyser les applications inconnues dans un bac à sable.

Principes du Zero Trust

La solution PAM garantit que seuls les utilisateurs autorisés ont accès aux comptes à privilèges et aux données sensibles, tandis que la stratégie du Zero Trust exige l'authentification et l'agrément de tous les utilisateurs et périphériques avant qu'ils puissent accéder à toute ressource. La solution PAM permet de contrôler la création de nouveaux comptes à privilèges afin que les attaquants ne puissent pas se déplacer latéralement.

Stratégie du moindre privilège

Notre solution PAM applique le principe du moindre privilège, garantit des identifiants uniques et élimine les comptes à privilèges partagés, qui sont placés dans des coffres pour un accès exclusivement en cas d'urgence. L'octroi par défaut de droits minimaux aux utilisateurs évite de partager les informations d'identification.

Delinea vous permet de gérer facilement les stratégies d'accès pour tous les types de comptes à privilèges. Les utilisateurs peuvent demander des privilèges élevés instantanément (juste-à-temps) pour un accès granulaire et limité dans le temps aux serveurs, bases de données, applications et postes de travail.

L'élévation des privilèges permet aux utilisateurs d'exécuter des applications à privilèges telles que l'installation de logiciels ou la modification de la configuration, uniquement lorsque cela est nécessaire et approuvé.

Gestion des accès

L'authentification multi-facteurs (MFA) de Delinea fournit une confirmation supplémentaire qu'une personne est au clavier et qu'elle est le titulaire légitime des identifiants utilisés. Grâce à l'authentification MFA, même si un cybercriminel ou un initié malveillant parvenait à obtenir un mot de passe, il ne pourrait pas accéder aux ressources sensibles.

Pour faciliter les choses, lePAM prend en charge un grand nombre d'authentificateurs tiers et en intègre plusieurs.

Automatisation

La solution PAM de Delinea automatise le rôle des administrateurs IT en fournissant un contrôle et une gestion centralisés des accès à privilèges au sein de l'entreprise. Les administrateurs peuvent établir des stratégies et des règles d'accès et automatiser l'application desdites stratégies. Cela inclut la rotation automatique des mots de passe ou l'élévation des privilèges pour des applications et des commandes spécifiques. En outre, les administrateurs peuvent automatiser la génération de rapports, les fonctionnalités d'audit et l'enregistrement des sessions pour permettre aux administrateurs IT de suivre et de contrôler l'activité des utilisateurs. En automatisant ces tâches, Delinea permet aux administrateurs IT de se concentrer sur des tâches plus importantes et des initiatives stratégiques.

Delinea offre des capacités avancées d'apprentissage automatique pour analyser les activités des comptes à privilèges en temps réel, ce qui permet de détecter les anomalies et de fournir des alertes configurables avec un score de menace. Cette fonction permet d'identifier les problèmes potentiels et de mesurer la gravité d'une violation en analysant toutes les activités associées aux comptes à privilèges.

Prochaines étapes

- Discutez avec un expert de la façon dont notre solution PAM peut vous aider à vous conformer aux exigences de la directive NIS2.
- Commencez votre parcours PAM avec la version d'essai de Secret Server
- Modèle de réponse aux incidents de cybersécurité

Delinea

Defining the boundaries of access

Delinea est un fournisseur majeur de solutions de gestion des accès à privilèges (PAM) pour les entreprises modernes et hybrides. Delinea Platform étend en toute transparence les solutions PAM en fournissant des autorisations pour toutes les identités, en contrôlant l'accès à l'infrastructure cloud hybride la plus critique et aux données sensibles d'une entreprise pour aider à réduire les risques, à garantir la conformité et à simplifier la sécurité. Delinea supprime la complexité et définit les limites de l'accès pour des milliers de clients dans le monde. Nos clients vont des PME aux plus grandes institutions financières, agences de renseignement et sociétés spécialisées dans les infrastructures critiques du monde.

Découvrez les solutions de Delinea sur **delinea.com/fr/.**

© Delinea