cpl.thalesgroup.com

THALES
Building a future we can all trust

Solutions Thales pour la prévention des attaques de ransomware

Correspondance des solutions Thales par rapport au cadre de cybersécurité du NIST et conseils de prévention contre les ransomware

Les attaques de ransomware sont un problème depuis plusieurs années, mais dernièrement, leurs conséquences sont bien plus désastreuses car les cybercriminels n'épargnent personne, des infrastructures essentielles aux hôpitaux et aux commerçants, exigeant des dizaines de millions de dollars en rançon. Aujourd'hui, alors que ces attaques sont l'un des sujets de conversation des sommets majeurs réunissant les chefs d'État du monde entier, les agences gouvernementales font preuve de proactivité en éduquant les entreprises et les organisations et en leur donnant les ressources nécessaires pour les aider à se protéger.

Conseils du NIST pour empêcher les attaques de ransomware

Sous l'égide du National Institute of Standards and Technology (NIST), le National Cybersecurity Center of Excellence (NCCoE) a publié des conseils sur l'identification et la protection des ressources contre les ransomware. Le document Cybersecurity Special Publication (SP) 1800-25 décrit les étapes à suivre pour bénéficier d'une stratégie de protection des ressources exhaustive. Il explique également qu'il n'existe pas de remède miracle contre la menace des ransomware.

Solutions Thales pour la prévention des ransomware

Les solutions de sécurité des données et de gestion des accès de Thales fournissent quelques-uns des composants les plus essentiels proposés par le cadre de cybersécurité du NIST afin de protéger les organisations contre les ransomware. Grâce à la gamme de produits de pointe de Thales, les organisations peuvent :

- Découvrir les données sensibles et les classer en fonction du risque
- Mettre en place un contrôle de gestion des identités et des accès robuste
- Protéger et contrôler les données sensibles au repos et en transit par le biais du chiffrement et de la tokénisation
- Surveiller la sécurité des données, pour une correction intelligente des anomalies

Vous trouverez ci-dessous une description de la correspondance de nos solutions par rapport au cadre de cybersécurité du NIST :

Correspondance des solutions Thales par rapport au cadre de cybersécurité du NIST et conseils de prévention contre les ransomware

Catégorie	Exigence	Solutions Thales
IDENTIFIER **Évaluation des risques (ID.RA)**	ID.RA-1 : les vulnérabilités des ressources sont identifiées et documentées.	**CipherTrust Data Discovery and Classification** localise les données sensibles réglementées, qu'elles soient structurées ou non structurées, dans le cloud, les Big Data et les magasins de données traditionnels. Un écran unique permet de comprendre les données sensibles et leurs vulnérabilités, de prendre de meilleures décisions concernant le comblement des failles de sécurité et la correction des violations de conformité, la hiérarchisation des mesures correctives et la protection de votre transformation cloud et du partage des données tierces.
PROTÉGER **Contrôle des accès (PR.AC)**	PR.AC-1 : les identités et les identifiants sont émis, gérés, vérifiés, révoqués et contrôlés pour les appareils, les utilisateurs et les processus autorisés. PR.AC-3 : l'accès à distance est géré. PR.AC-4 : la gestion des permissions et des autorisations d'accès intègre les principes de moindre privilège et de séparation des devoirs.	**SafeNet Trusted Access fournit une gestion des accès centralisée** qui permet aux organisations de mettre en place des politiques d'authentification cohérentes sur les différentes plateformes en automatisant et en simplifiant le déploiement et la gestion d'un ensemble de tokens distribués tout en protégeant une vaste gamme de ressources, sur site, dans le cloud ou virtualisées. **SafeNet Trusted Access fournit également une authentification multifacteur commerciale prête à l'emploi** avec l'éventail de méthodes d'authentification et de facteurs de forme le plus vaste. Ainsi, ses clients peuvent traiter de nombreux cas d'utilisation, niveaux d'assurance et vecteurs de menace grâce à des politiques unifiées et centralisées, gérées à partir d'un back-end d'authentification unique délivré dans le cloud ou sur site. **CipherTrust Transparent Encryption fournit des contrôles d'accès granulaires** aux données essentielles à vos activités, définit qui a accès à des fichiers/dossiers protégés spécifiques et quelles opérations peuvent être effectuées. • Empêcher les utilisateurs administratifs d'exploiter leurs privilèges d'accès en lecture aux fichiers ou aux bases de données sensibles. • Mettre en place des politiques de contrôle d'accès strictes autour des archives de sauvegarde, et chiffrer les sauvegardes pour prévenir l'exfiltration des données. • Mettre en place une séparation des devoirs de sorte que les utilisateurs de base de données peuvent obtenir un accès en lecture/écriture, tandis que le logiciel de sauvegarde n'a qu'un accès en écriture à la même base de données.

Catégorie	Exigence	Solutions Thales
PROTÉGER **Sécurité des donnée (PR.DS)**	PR.DS-1 : les données au repos sont protégées.	**CipherTrust Data Security Platform** unifie la découverte des données, la classification, la protection des données avec des contrôles d'accès granulaires inégalés et une gestion centralisée des clés, le tout sur une seule plateforme. Ceci permet une réduction des ressources dédiées aux opérations de sécurité des données, des contrôles de conformité omniprésents et une diminution des risques dans votre entreprise. • **CipherTrust Transparent Encryption** chiffre les données au repos, contrôle l'accès des utilisateurs privilégiés et se charge de la création de journaux de vérification de l'accès aux données détaillés sans devoir apporter des modifications aux applications existantes. Les organisations informatiques peuvent ainsi configurer des mesures pour empêcher le chiffrement de vos données les plus sensibles par des processus malveillants ou empêcher les utilisateurs non autorisés d'exposition des données sensibles via l'exfiltration. Ce qui protège ainsi les organisations contre les attaques de ransomware. Des agents protègent les données dans les fichiers, les volumes et les bases de données sur les serveurs physiques et virtuels Windows, AIX et Linux, dans les environnements de cloud et Big Data. • **CipherTrust Application Data Protection** fournit des fonctions de chiffrement telles que des services de gestion de clés, de signature, de hachage et de chiffrement accessibles par le biais d'API, afin que les développeurs puissent facilement sécuriser les données au niveau du serveur de l'application ou du nœud des Big Data. • CipherTrust Tokenization **est disponible avec et sans coffre et peut aider à réduire le coût et la complexité de la mise en conformité avec les mandats de sécurité des données tels que PCI-DSS.** • **Les solutions CipherTrust Database Protection** intègrent le chiffrement des données pour les champs sensibles dans les bases de données grâce à la gestion de clé centralisée et sécurisée sans avoir besoin de modifier les applications de bases de données. Les solutions CipherTrust Database Protection prennent en charge Oracle, Microsoft SQL Server ainsi que les bases de données IBM DB2 et Teradata. • **CipherTrust Manager est le point de gestion central pour la plateforme**. Il permet aux organisations de gérer les clés de chiffrement, de mettre en place des contrôles d'accès granulaires et de configurer les politiques de sécurité de manière centralisée. De plus, il gère le cycle de vie des clés, dont la génération, la rotation, la destruction, l'importation et l'exportation, met en place des contrôles d'accès aux clés et aux politiques axés sur les rôles, améliore la robustesse des audits et des rapports et offre des API REST conviviales pour les développeurs. Il est disponible aux formats physiques et virtuels conformes FIPS 140-2, jusqu'au niveau 3. **Les modules de sécurité matériels Luna** génèrent, stockent, protègent et gèrent les clés de chiffrement utilisées pour protéger les données sensibles et les applications essentielles. Les HSM Luna offrent le plus de certifications dans l'industrie, y compris CC (Critères Communs), FIPS 140-2 niveau 3, ITI et bien plus encore. Bénéficiez d'une infrastructure des plus fiables, soutenue par une base HSM cryptographique reconnue à l'international. Les HSM Luna de Thales fournissent une racine de confiance pour les technologies existantes et émergentes, y compris l'infrastructure de clé publique (PKI), et stockent les clés en sécurité pour la signature de code, afin de maintenir l'intégrité du code. Thales offre également une solution de signature de code d'entreprise personnalisée imbriquée sur les HSM Luna, les conteneurs et les API REST, disponible sur site, en tant que service HSM cloud et dans les environnements hybrides. **Data Protection On Demand** est une plateforme basée sur le cloud offrant toute une gamme de HSM cloud et de services de gestion de clés essentiels, accessibles via une simple marketplace en ligne.

Catégorie	Exigence	Solutions Thales
PROTÉGER la sécurité des données (PR.DS)	PR.DS-2 : les données en transit sont protégées.	**Les dispositifs de chiffrement à haut débit Thales** offrent la solution certifiée et éprouvée idéale pour la sécurité des données en transit des entreprises et des organisations gouvernementales, y compris les diffusions vocales et vidéo avec contraintes de temps : • La série de dispositifs de chiffrement réseau CN sont des appliances réseau matérielles qui fournissent un chiffrement réseau indépendant des couches (couches 2, 3 et 4) pour les données en transit. Ces dispositifs de chiffrement matériels sont certifiés FIPS 140-2 niveau 3, CC (Critères Communs) et OTAN. Ils figurent également sur la liste des produits approuvés DoDIN. • La série CV est une appliance virtuelle renforcée qui fournit un chiffrement robuste pour les données en transit sur les liaisons WAN et SD-WAN avec porteur à haut débit, grâce à la fonction VNF (fonctions réseau virtualisées).
RÉPONSE (RS) Mesures correctives (RS-MI)	RS.MI-3 : les vulnérabilités qui viennent d'être identifiées sont corrigées ou documentées en tant que risques acceptés.	**CipherTrust Intelligent Remediation** intègre la découverte des données sensibles basées sur les risques avec le chiffrement transparent des données basé sur les politiques afin de corriger les risques d'exposition de données automatiquement. Il aide les organisations à visualiser les risques d'entreprise et à automatiser les actions correctives pour offrir une protection contre les attaques de ransomware. **SafeNet Trusted Access** permet aux organisations de réagir et de réduire le risque d'attaque de ransomware en fournissant une piste de vérification immédiate et actualisée contenant tous les événements d'accès à tous les systèmes. Des rapports automatisés étendus documentent tous les aspects de l'application des accès et de l'authentification. De plus, le service diffuse automatiquement les journaux aux systèmes SIEM.

Un ensemble complet de solutions pour satisfaire aux exigences du cadre de cybersécurité du NIST

Alors que les solutions Thales fournissent quelques-unes des fonctionnalités les plus importantes du cadre de cybersécurité du NIST, aucune entreprise ne peut proposer à elle seule un ensemble complet de solutions qui respectent toutes ses exigences. C'est pourquoi Thales a plus de 400 partenaires, parmi les fournisseurs de technologie les plus influents dans le monde, afin de fournir aux clients un ensemble complet de solutions et d'intégrations qui satisfont aux exigences du cadre de cybersécurité du NIST. Veuillez nous contacter pour en savoir plus sur les solutions que nous proposons pour vous aider à empêcher les attaques de ransomware, ainsi que les programmes malveillants destructeurs, les menaces intérieures et autres menaces persistantes avancées.

À propos de Thales

Thales est un leader mondial dans la sécurité des données, approuvé par les gouvernements et les entreprises les plus éminentes du monde entier pour les aider à protéger leurs données les plus sensibles. Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.