Commvault

livre électronique

LA CRISE DES IDENTITÉS NON HUMAINES:

COMBLER L'ANGLE MORT DE LA PROTECTION MODERNE DES DONNÉES ET DE LA CYBERRÉSILIENCE

EXÉCUTIF RÉSUMÉ

À l'ère de l'automatisation pilotée par l'IA, le périmètre traditionnel s'est effondré, laissant l'identité comme ultime point de contrôle. Si la sécurité des entreprises a consacré des décennies à renforcer l'authentification humaine, une explosion silencieuse des identités non humaines (INH) – comptes de service, clés API, jetons OAuth et agents d'IA – a créé une surface d'attaque massive et non maîtrisée.

Ces identités sont désormais 144 fois plus nombreuses que les identités humaines, et pourtant, elles sont rarement gérées avec la même rigueur. Cet ebook explique comment les adversaires modernes exploitent cette « dette d'identité » pour assurer leur persistance et pourquoi les organisations doivent adopter une architecture de type Tier 0 axée sur la récupération afin de garantir la résilience des identités

1 Rapport sur les risques liés aux identités non humaines et aux secrets, premier semestre 2025, Entrée

SECTION 1: DÉFINITION DE LA SURFACE D'ATTAQUE DES MACHINES

La portée des identités non humaines (NHI) dépasse largement le cadre des logiciels natifs du cloud ; elles constituent l'élément de liaison essentiel pour le système physique et...

L'infrastructure médicale est essentielle au fonctionnement de la société moderne. Dans ces environnements critiques, un dispositif médical autonome (DMA) désigne tout appareil ou « objet » doté d'identifiants, capable d'exécuter des actions et de transférer des données de manière autonome.

Il est essentiel de reconnaître que le « point aveugle » des identités non humaines inclut désormais les actifs matériels qui interagissent directement avec le monde physique. Lorsque ces identités sont surprivilégiées ou insuffisamment encadrées, le risque encouru ne se limite pas à la perte de données, mais également des dommages physiques et des risques pour la sécurité humaine.

FINANCIER INFRASTRUCTURE

Les guichets automatiques modernes fonctionnent comme des identités non humaines sophistiquées qui s'authentifient auprès des systèmes bancaires centraux via des comptes de service et des clés API pour autoriser la distribution de liquidités et traiter des informations personnelles sensibles.

FABRICATION & INDUSTRIEL IOT

Dans les usines intelligentes, les automates programmables et les bras robotisés agissent comme des identités de charge de travail au sein des pipelines d'automatisation de type DevOps. Une faille à ce niveau permet à un attaquant de manipuler l'intégrité du système, en modifiant les paramètres de production physiques sans déclencher d'alerte humaine.

AGENT IA DANS LES SYSTÈMES PHYSIQUES

Lorsqu'une IA agentielle est déployée pour gérer des scripts de construction ou des réseaux électriques, ces agents s'authentifient avant d'agir. Une manipulation malveillante par injection d’invites (prompt injection) pourrait inciter un agent à exfiltrer des schémas de site sensibles ou à perturber les services publics.

BIOTECH ET L' IOT MÉDICAL :

Dispositifs hospitaliers

Les appareils d'imagerie et les pompes à perfusion fonctionnent comme des identités non humaines qui héritent de l'accès aux dossiers médicaux électroniques, souvent grâce à des jetons à longue durée de vie rarement renouvelés.

Dispositifs implantables

Les stimulateurs cardiaques et les pompes à insuline connectés représentent le maillon le plus sensible du plan d’identité. Ces dispositifs s'authentifient auprès des réseaux de soins pour transmettre leurs données de télémétrie. Si cette sécurité est compromise, la décision qui en découle est un ajustement médical vital.

La résilience de l'identité pour ces appareils nécessite une architecture axée sur la récupération, où l'organisation doit être en mesure d'auditer et d'annuler les élévations de privilèges non autorisées en temps réel afin de vérifier que vos « identités » physiques et médicales restent dans un état de confiance.

LES CHIFFRES CLÉS

L'ampleur de l'écosystème des identités non humaines est stupéfiante et croît à un rythme [4] à [10] fois plus rapide que celui des comptes humains.[2]

DÉFAUT DE GOUVERNANCE

Moins de

25%

certaines organisations ont des politiques formelles concernant la création ou la suppression de ces identités.[3]

PRIVILÈGE EXCESSIF

97%

Les agents des NHI possèdent des autorisations qui vont bien au-delà de ce qui est requis pour leur rôle fonctionnel.[4]

VULNÉRABILITÉ

Seulement

12%

de nombreuses organisations se disent très confiantes dans leur capacité à prévenir une attaque ciblant ces identités de machines.[5]

2. Alliance CyberRisk
3. État des lieux de l'identité non humaine et de la sécurité de l'IAAlliance pour la sécurité du cloud
4. État des identités non humaines et des secrets en cybersécurité en 2025, Entrée
5. État des lieux de l'identité non humaine et de la sécurité de l'IAAlliance pour la sécurité du cloud

SECTION 2 : ÉTUDE DE CAS SUR LA GUERRE MODERNE – LE MODÈLE SLH ET SHINYHUNTERS

Des adversaires comme le supergroupe de cybercriminels Scattered LAPSUS$ Hunters (SLH) – qui comprend des acteurs notoires comme ShinyHunters et Scattered Spider – ont été les pionniers d'un changement mortel en matière de méthodologie d'attaque. Leurs tactiques illustrent pourquoi les NHI sont plus précieuses stratégiquement que les qualifications humaines.

LE PIPELINE INDUSTRIALISÉ DE VISHING

SLH a industrialisé le phishing vocal**(Vishing),** un vecteur qui a connu une augmentation de 449% en 2025.6

01 RECRUTEMENT ET INCITATION

Il a été observé que le groupe offrait des incitations financières de 500 à 1 000 dollars par appel pour recruter des talents spécialisés, cherchant spécifiquement des femmes pour mener des attaques de vishing.7 Cette tactique est conçue pour augmenter le taux de réussite de l'usurpation d'identité auprès du support informatique en contournant les profils traditionnels d'« attaquants » que le personnel peut être formé à identifier.

02 L'ENTRÉE

Utilisant des scripts pré-écrits, ces recrues se font passer pour des employés afin de convaincre les services d'assistance informatique d'effectuer des réinitialisations de mots de passe ou d'authentification multifacteurs (MFA).

03 03LE PIVOT VERS LES INH

Une fois l'accès initial obtenu, les attaquants se déplacent latéralement vers les environnements virtualisés et cloud. Ils maintiennent souvent leur présence en migrant du compte humain vers des couches automatisées, par exemple en volant des jetons OAuth ou en créant de nouveaux comptes de service d'administration.

04 LA PERSISTANCE

Contrairement aux mots de passe humains, ces identités de machine sont rarement renouvelées et souvent invisibles pour les systèmes de surveillance traditionnels. Cela permet à l'attaquant de conserver un accès longtemps après la résolution du problème affectant l'utilisateur humain.

6 Rapport sur les tendances des menaces de phishing en 2025, vol. 6, KnowBe4

7 Les actualités des hackers

SECTION 3: LES VULNÉRABILITÉS ⚠ CRITIQUES DES INH

Les NHI contournent les trois piliers traditionnels de la sécurité : l'authentification multifacteur des utilisateurs, la détection des endpoint et le filtrage des courriels.

ABUS D'OAUTH

Les attaquants incitent les utilisateurs à approuver des applications via un écran de consentement, leur accordant ainsi un accès délégué à leurs boîtes mail et à leurs données. Cette activité se confond avec le trafic API légitime et persiste même après une réinitialisation de mot de passe, ce qui complique sa détection et son enregistrement en tant que menace justifiant une intervention.

COMPTES DE SERVICE FANTÔMES

Dans les grandes entreprises, des milliers de comptes de service non documentés fonctionnent avec des privilèges d'administrateur et restent souvent actifs longtemps après la fin de leur projet initial. Ce manque de rigueur constitue un point critique qui doit être traité de manière efficace et efficiente.

VOL DE TOKENS ET DE CLÉS

Les clés API à longue durée de vie intégrées dans des fichiers de configuration statiques ou des pipelines DevOps ne tiennent pas compte du contexte de l'appareil ou de la géolocalisation, ce qui permet un accès large et automatisé sans déclencher d'alerte de connexion utilisateur.

SECTION 4: UN CADRE POUR LA RÉSILIENCE IDENTITAIRE

Les organisations doivent faire évoluer leurs processus pour traiter les identités non humaines (NHI) comme des actifs de niveau 0, équivalents en termes de risque,

aux administrateurs de domaine ou aux plans de contrôle cloud.

PROTOCOLES DE CRÉATION PRIVILÉGIÉS

La création d'une application ou d'un compte de service OAuth devrait nécessiter une approbation administrative et générer des données de télémétrie de sécurité de haut niveau.

CORRÉLATION ENTRE HUMAINS ET INH

La plupart des violations pourraient être stoppées rapidement en corrélant les signaux croisés entre domaines, comme une interaction avec un service d'assistance suivie immédiatement d'une réinitialisation de l'authentification multifacteur ou de la création d'un nouveau jeton.

ÉLIMINATION DES SECRETS STATIQUES

Les secrets statiques représentent un risque inacceptable. Ils doivent être remplacés par des jetons à durée de vie limitée et une rotation automatique.

ARCHITECTURE DE LA RÉCUPÉRATION

Puisqu'une prévention à 100 % est impossible, les organisations doivent être capables de détecter, de contenir et de rétablir rapidement l'environnement d'identité dans un état de confiance.

SECTION 5:
COMMVAULT IDENTITÉ RÉSILIENCE

La résilience des identités de Commvault permet de fournir la visibilité et les capacités de récupération nécessaires pour protéger les environnements d'identité complexes à l'échelle de l'entreprise.

RÉCUPÉRATION RAPIDE D'IDENTITÉ

Offre des fonctionnalités de récupération automatisées allant des attributs et objets AD individuels à la restauration complète de la forêt. La récupération d'une forêt AD étant l'un des processus les plus complexes et sujets aux erreurs en informatique, elle implique DNS, SYSVOL, les rôles FSMO, les catalogues globaux,

Pour la gestion des relations de confiance, de la réplication et du séquençage de la récupération sur plusieurs domaines, la solution est conçue pour automatiser et orchestrer ces étapes grâce à des flux de travail guidés et des manuels d'exécution.

Cela aide les organisations à rétablir rapidement l'environnement d'identité dans un état fiable et approuvé, minimiser les temps d'arrêt et de réduire le risque d'erreur humaine ; et rétablir les fondements d'authentification et d'autorisation dont dépend le reste de l'organisation.

ÉVALUATION DES VULNÉRABILITÉS D'IDENTITÉ

Évalue l'environnement Active Directory (AD) en matière de sécurité

L'évaluation identifie les faiblesses qui augmentent la probabilité ou l'impact d'une compromission. Elle met en évidence les privilèges excessifs et les comptes disposant de trop d'autorisations, l'utilisation de protocoles obsolètes et non sécurisés tels que NTLMv1, SMBv1 et LDAP non signé, des paramètres d'authentification faibles, l'absence de contrôles de sécurité et une dérive de configuration à risque.

Ce rapport met également en lumière des problèmes tels que la délégation non encadrée, les comptes privilégiés obsolètes, les politiques de mots de passe et Kerberos faibles, les relations de confiance non sécurisées et le manque de protection des actifs de niveau 0. Il en résulte une cartographie priorisée des risques liés à l'identité, permettant aux organisations de réduire le périmètre d'impact et de renforcer leur résilience en amont.

Un attaquant peut transformer Active Directory en une plateforme persistante de compromission et de déplacement latéral.

AUDIT ET RESTAURATION EN TEMPS RÉEL

Ce service surveille en continu Active Directory à l'aide des données de synchronisation d'annuaires et des journaux d'événements Windows afin de détecter les modifications suspectes ou non autorisées dès leur apparition. Il suit les activités telles que l'élévation de privilèges, l'ajout à des groupes privilégiés, les modifications des GPO, la modification des comptes de niveau 0, les changements de stratégie d'authentification, la création d'utilisateurs non autorisés et les tentatives d'affaiblissement des paramètres de sécurité.

Chaque événement est intégré à une chronologie permettant aux administrateurs de distinguer rapidement les tâches administratives courantes des premières étapes d'une usurpation d'identité. En cas de modification malveillante ou accidentelle, la plateforme permet une restauration instantanée (rollback), en un seul clic, de l'état antérieur de confiance.

Commvault

livre électronique

Apprenez-en davantage sur la résilience identitaire

commvault.com | 888.746.3849 | talktous@commvault.com