#AD SEC

2020

Harden. Detect. Respond.

ALSID

#ADSEC

Active Directory est le vecteur privilégié par les cyber attaquants pour atteindre et voler les ressources les plus vitales des entreprises

Notre industrie considère, à tort, que les attaques sont couronnées de succès dès qu'une machine est compromise.

Pourtant, la route est longue entre la première machine et la cible finale et il n'est plus possible d'ignorer le seul vecteur permettant aux hackers de se déplacer ainsi dans l'infrastructure de leurs victimes : **Active Directory**.

95% — des entreprises du Fortune 1000 utilisent Active Directory

100M — de décisions de sécurité sont traitées chaque jour par de grandes infrastructures d'annuaire

85% — des administrateurs reconnaissent avoir du mal à totalement maitriser la sécurité de leur Active Directory

10% — du chiffre d'affaires est, en moyenne, englouti dans les remédiations post-incident

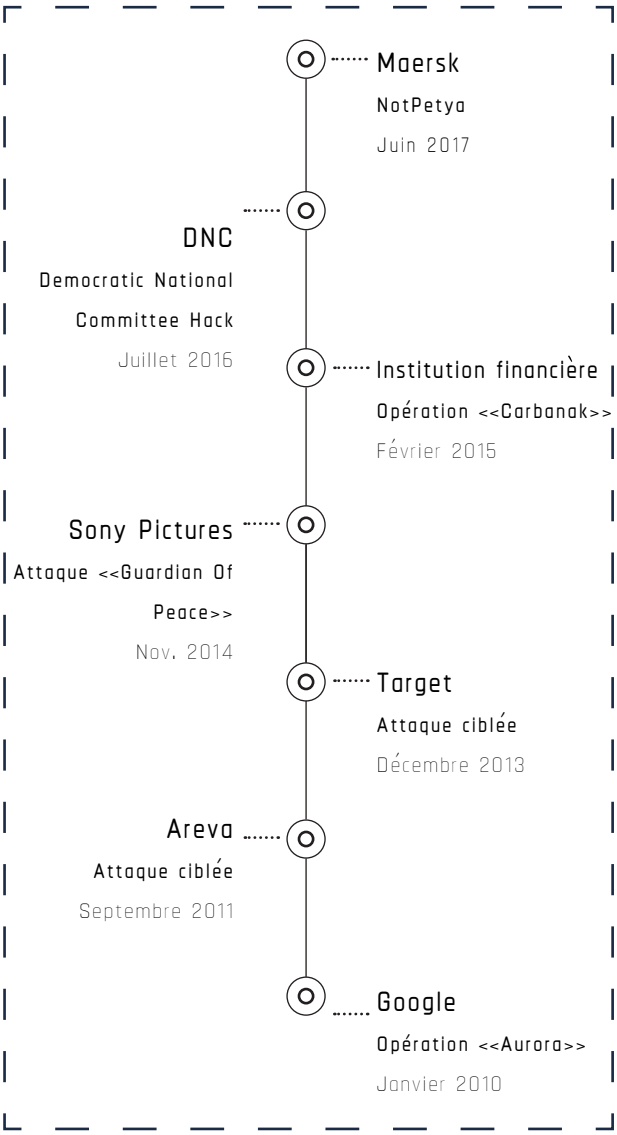
25 — Sur 25 grands groupes audités

95% — 95 % présentaient un AD vulnérable.

80% — présentaient des erreurs de configuration critiques

Pourquoi est-ce important ?

Les infrastructures Active Directory constituent le point central de toute la sécurité de votre entreprise. Informations d'authentification utilisateur, accès à la messagerie, documents liés au métier ou informations financières : tout est régi par Active Directory, qui demeure le maitre des clés des entreprises.



Pourquoi les solutions de défense actuelles sont inefficaces

- La plupart des outils de sécurité misent sur la détection des attaques, mais aucun d'entre eux ne cherche à augmenter la résilience interne de votre architecture AD, ni à prévenir les attaques elles-mêmes.
- L'infrastructure d'Active Directory est complexe et évolue rapidement. Avec des milliers de règles de sécurité simultanées, la moindre erreur de configuration apparemment minime peut, en quelques minutes, se traduire par une succession de vulnérabilités majeures.

ALSID réinvente la sécurité d'Active Directory

ALSID renforce votre infrastructure d'annuaire, enrichit vos capacités SOC avec la détection des menaces sur AD, et permet à vos équipes de répondre aux incidents et d'enquêter sur les menaces visant AD.

RECHERCHE/CORRECTION DES FAILLES EXISTANTES

Identifiez, cartographiez et évaluez immédiatement les vulnérabilités existantes.

Suivez nos recommandations correctives étape par étape et prévenez les attaques.

DÉTECTION DES CHEMINS D'ATTAQUE

Détectez instantanément les nouvelles faiblesses et erreurs de configuration.

Brisez les chemins d'attaque et maîtrisez votre exposition aux menaces.

IDENTIFICATION DES ATTAQUES EN TEMPS RÉEL

Obtenez des alertes en temps réel et des plan de remédiation concrets.

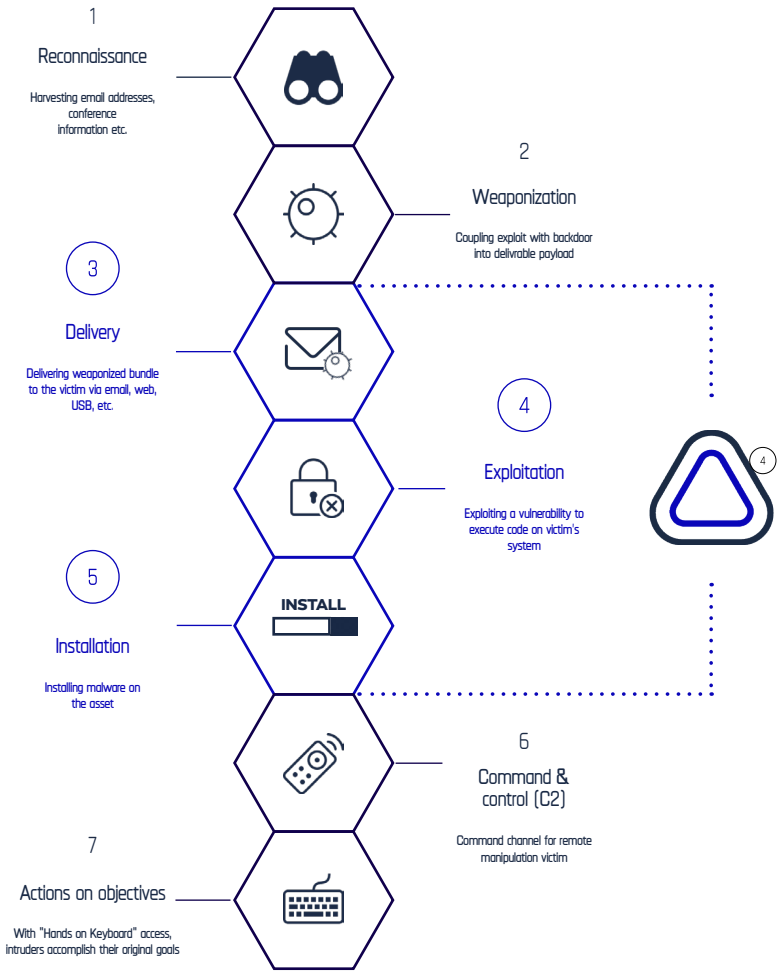
Visualisez les notifications et déclenchez les réponses dans votre environnement SIEM, SOAR ou SOC.

ENQUÊTE SUR LES INCIDENTS ET MENACES

Accédez à l'outil de suivi de sécurité le plus complet pour AD.

Recherchez et mettez en corrélation les modifications d'AD au niveau des objets et des attributs.

La place d'ALSID dans la cyber kill-chain



The Cyber Kill Chain® by Lockheed Martin

③ Delivery

1. **Prévention** - Alsid identifie les modes de diffusion exploitables et informe les équipes SOC en temps réel afin de déployer une solution préventive.
2. **Détection** - Alsid détecte en temps réel les attaques et fournit des plans de correction en temps réel.
3. **Répondre** - les alertes et indicateurs définis par Alsid permettent aux équipes d'intervention d'identifier les causes originelles et d'orienter les réponses et les procédures de renforcement

④ ⑤ Exploitation et installation

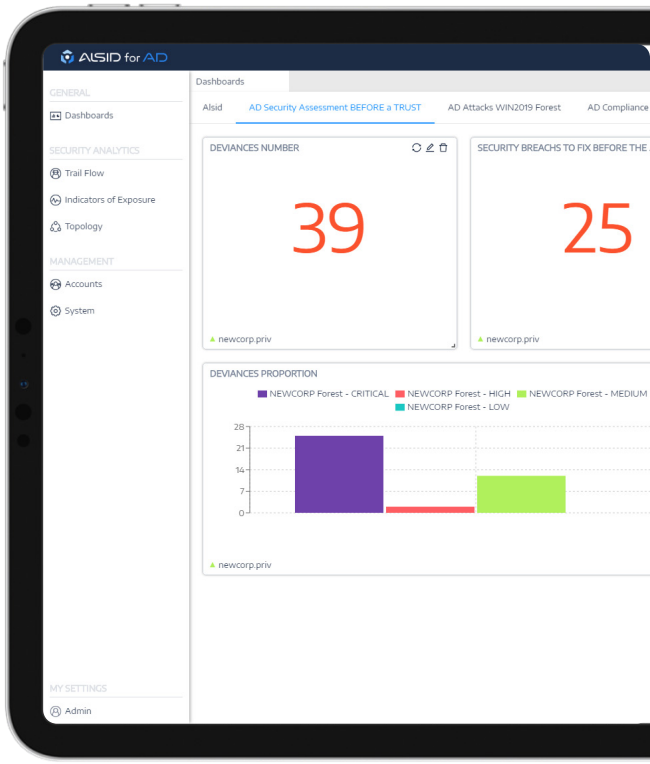
1. **Prévention** - qu'il s'agisse d'erreurs de configuration ou de failles logicielles, Alsid guide les équipes SOC tout au long du processus de renforcement d'Active Directory et de prévention des attaques.
2. **Détection** - grâce à la plus vaste surface de détection du marché, Alsid identifie les exploitations en cours et déclenche rapidement des mesures correctives.
3. **Réponse** - les recommandations détaillées d'Alsid guident les administrateurs d'AD durant le processus (sinon trop complexe) de gestion des objets compromis, des serveurs non conformes et du renforcement de l'infrastructure dans son ensemble.

ALSID

#ADSEC 2020

Plateforme intégrée

- Console d'administration agile de type tableau de bord.
- Plateforme centralisée permettant de gérer simultanément plusieurs infrastructures Active Directory.
- Mécanisme d'authentification sûr, combinant une architecture MFA et une base de données avec authentification isolée.
- Intégration aux processus de l'entreprise via les fonctions d'exportation intégrées vers Excel & JSON.



Nos clients parlent de nous

« Non seulement l'intégration d'Alsid a été réalisée en une journée, mais elle a également permis une surveillance efficace de la sécurité des infrastructures atomiques, sans incidence sur la charge de travail des équipes de sécurité. »

Thierry Auger
Lagardère Deputy CIO & CISO

« La solution d'Alsid nous a libérés des problèmes de sécurité d'Active Directory, pour nous permettre de nous recentrer sur la nouvelle intégration commerciale. »

Dominique Tessaro
VINCI Energies CIO

« Avoir une longueur d'avance sur les attaquants est essentiel pour garantir à nos clients une sécurité forte. La solution d'Alsid protège notre réseau contre les menaces internes grâce à une approche fluide et transparente. »

Eric Ho
HKBN Co-directeur & CIO

SAFRAN · Lagardère · UNIBAIL-RODAMCO-WESTFIELD · 香港寬頻 HONG KONG BROADBAND NETWORK · somfy · SANOFI · VINCI ENERGIES

Banking CyberSecurity Innovation Awards · black hat USA 2018 · NationalCouncilISACs · SINET

À propos d'Alsid

Alsid est un fournisseur de cybersécurité spécialisé dans la défense de ce qui est le dénominateur commun de la plupart des attaques contemporaines, à savoir : les infrastructures Active Directory (AD). Notre solution cloud de premier plan fournit à nos utilisateurs des recommandations détaillées et personnalisées qui renforcent leur environnement AD, un moteur de détection des attaques en temps réel, ainsi que des fonctionnalités permettant d'enquêter sur les violations d'AD lorsqu'elles sont à déplorer.

Alsid protège aujourd'hui plus de 6 millions d'utilisateurs dans le monde et aide de grandes entreprises telles que Sanofi, VINCI Energies ou Lagardère à se prémunir contre les attaques.

alsid.com · hello@alsid.com · @AlsidOfficial

book a demo

primo-infection is a lost battle

Lateral movement is the new front

ALSID