NTLM Relay 2026 : Attaques, Outils et Contre-Mesures Active Directory

Les attaques NTLM Relay constituent en 2026 l'une des techniques les plus redoutables et les plus fréquemment exploitées lors des tests d'intrusion sur les environnements Active Directory d'entreprise. Le protocole d'authentification NTLM (NT LAN Manager), héritage des années 1990 encore omniprésent dans les parcs informatiques Windows, présente des failles architecturales fondamentales que les attaquants exploitent pour se déplacer latéralement à travers les réseaux, élever leurs privilèges et compromettre des contrôleurs de domaine en quelques minutes. Malgré des décennies d'alertes de la part de l'ANSSI, de Microsoft et du CISA, des milliers d'organisations continuent de fonctionner avec des configurations vulnérables au NTLM Relay attaque 2026. Cet article technique détaille le mécanisme précis des attaques NTLM Relay en 2026, les outils offensifs utilisés par les pentesters et les attaquants, les CVE actives, ainsi que les contre-mesures concrètes permettant de neutraliser cette menace persistante dans votre infrastructure Active Directory. Que vous soyez RSSI, administrateur système ou pentester, ce guide complet vous fournira les éléments techniques nécessaires pour évaluer votre exposition et durcir vos défenses.

Points essentiels à retenir

NTLM Relay exploite le mécanisme challenge-response de NTLM pour relayer une authentification légitime vers un autre service cible sans jamais connaître le hash

Responder + ntlmrelayx forment le duo offensif standard permettant d'obtenir des accès RCE, LDAP ou SMB en moins de 5 minutes sur un réseau non durci

L'activation du SMB Signing et la désactivation de NTLM v1 sont les contre-mesures les plus efficaces et déployables sans impact majeur

Les CVE-2019-1040, CVE-2021-36942 (PetitPotam) et CVE-2024-38124 illustrent la persistance de cette surface d'attaque malgré les correctifs successifs

L'ANSSI recommande une désactivation progressive de NTLM au profit de Kerberos et des mécanismes EPA (Extended Protection for Authentication)

Qu'est-ce que NTLM Relay et pourquoi est-ce toujours dangereux en 2026 ?

NTLM (NT LAN Manager) est un protocole d'authentification par défi-réponse développé par Microsoft dans les années 1990. Bien que Kerberos soit le protocole privilégié dans les domaines Active Directory modernes, NTLM reste activé par défaut sur tous les systèmes Windows et est utilisé dans de nombreux scénarios : accès par adresse IP directe, environnements de groupe de travail, ressources ne supportant pas Kerberos, authentification LDAP non-sécurisée, etc. Cette ubiquité en fait une cible de choix pour les attaquants dans tout audit de sécurité Active Directory.

Une attaque NTLM Relay ne consiste pas à casser le hachage NTLM d'un utilisateur (ce que fait le Pass-the-Hash), mais à intercepter un flux d'authentification NTLM en cours et à le retransmettre immédiatement à un service tiers, en se faisant passer pour le client légitime. La distinction est cruciale : l'attaquant n'a jamais besoin de connaître le mot de passe ni même le hash — il suffit d'intercepter la session d'authentification en temps réel et de la relayer avant qu'elle n'expire. Cette approche rend l'attaque particulièrement vicieuse car elle fonctionne même avec des mots de passe complexes et NTLMv2.

Histoire et évolution du protocole NTLM

LM (LAN Manager) fut introduit dans les années 1980, remplacé par NTLM v1 puis NTLM v2 dans Windows NT 4.0 SP4. Malgré l'introduction de Kerberos avec Windows 2000 et Active Directory, NTLM a survécu pour assurer la rétrocompatibilité. Aujourd'hui, NTLMv1 — la version la plus vulnérable — est encore activé dans de nombreuses organisations par crainte de

casser des applications legacy. NTLMv2, plus robuste, reste néanmoins vulnérable aux attaques de relay car il n'inclut aucune liaison au canal de transport (channel binding) par défaut.

L'évolution des attaques NTLM Relay a suivi un chemin remarquable depuis les premières démonstrations de SMB Relay dans les années 2000 par Josh Mazini et Luke Kenneth Casson Leighton. En 2001, le légendaire outil "SMBRelay" montrait déjà la faisabilité du relay. En 2015, Fox-IT publie ntlmrelayx. En 2017, Responder de Laurent Gaffié devient le standard. En 2019, CVE-2019-1040 permet de contourner les protections MIC (Message Integrity Code). En 2021, PetitPotam (CVE-2021-36942) exploite EfsRpcOpenFileRaw pour forcer des authentifications NTLM depuis le contrôleur de domaine lui-même, ouvrant la voie à une compromission totale sans aucune interaction utilisateur.

Différence entre NTLM Relay et Pass-the-Hash

Ces deux techniques sont souvent confondues mais fonctionnent différemment. Dans un Pass-the-Hash (PtH), l'attaquant possède déjà un hash NTLM volé (via Mimikatz, Secretsdump ou une autre technique d'extraction) et l'utilise directement pour s'authentifier. Dans un NTLM Relay, l'attaquant n'a pas le hash — il se positionne en man-in-the-middle entre une victime et un serveur, intercepte le flux d'authentification NTLM en cours et le relaie en temps réel vers un service tiers cible. Le relay est donc possible même avec NTLMv2, qui ne peut pas être utilisé directement dans un PtH. Pour aller plus loin sur le Pass-the-Hash, consultez notre article dédié : Pass-the-Hash : attaque NTLM Active Directory.

Comment fonctionne une attaque NTLM Relay : le mécanisme technique

Pour comprendre pourquoi NTLM Relay est si efficace, il faut d'abord comprendre le mécanisme NTLM en trois passes (three-way handshake). Ce protocole challenge-response ne lie pas l'authentification à une session réseau spécifique, ce qui crée la fenêtre d'opportunité pour le relay.

Le mécanisme challenge-response NTLM en détail

L'authentification NTLM se déroule en trois étapes distinctes :

NEGOTIATE (Type 1) : Le client envoie un message de négociation au serveur, indiquant les capacités NTLM supportées (NTLMv1, NTLMv2, etc.)

CHALLENGE (Type 2) : Le serveur répond avec un défi aléatoire de 8 octets (nonce) et ses propres capacités

AUTHENTICATE (Type 3) : Le client calcule une réponse au défi en utilisant son hash NTLM et renvoie le résultat avec son nom d'utilisateur et de domaine

Le serveur vérifie ensuite la réponse en interrogeant le contrôleur de domaine via Netlogon. La faille fondamentale : rien dans ce protocole ne lie cryptographiquement l'authentification au canal de transport (contrairement à Kerberos). L'attaquant peut donc intercepter le Type 1, le transmettre au service cible, récupérer le Type 2 du service cible, le renvoyer à la victime, puis relayer le Type 3 (la réponse signée avec le hash) directement au service cible. Le service cible authentifie alors l'attaquant en pensant dialoguer avec la victime légitime.

L'interception des authentifications réseau

Pour qu'un relay soit possible, l'attaquant doit d'abord intercepter une authentification NTLM. En réseau local, les protocoles de résolution de noms LLMNR (Link-Local Multicast Name Resolution) et NBT-NS (NetBIOS Name Service) permettent à n'importe quelle machine du sous-réseau de répondre aux requêtes de résolution pour des noms inexistants dans le DNS. C'est là qu'intervient Responder.

Lorsqu'une machine tente d'accéder à un partage réseau sur un serveur introuvable dans le DNS, Windows effectue successivement des requêtes DNS (qui échouent), LLMNR et NBT-NS sur le réseau local. Responder répond à ces requêtes en se faisant passer pour le serveur demandé, déclenchant ainsi une tentative d'authentification NTLM de la victime vers la machine de l'attaquant. D'autres méthodes de déclenchement incluent : les fichiers .scf ou .lnk malveillants dans des partages réseau, l'injection d'URL dans des e-mails, les requêtes WPAD malveillantes, et depuis 2021, les appels RPC forcés type PetitPotam ou Coercer qui permettent de déclencher une authentification depuis n'importe quel serveur Windows.

Le relai vers d'autres services

Une fois l'authentification NTLM interceptée, l'outil de relay la retransmet vers un service cible. Les services les plus prisés incluent SMB pour l'exécution de commandes si l'utilisateur est administrateur local, LDAP ou LDAPS pour la modification d'objets AD et l'ajout de droits DCSync, HTTP ou HTTPS pour l'accès à Exchange, SharePoint et ADCS (Active Directory Certificate Services), MSSQL pour l'exécution de requêtes ou l'activation de xp_cmdshell, et DCOM ou WMI pour l'exécution de code à distance. La règle d'or : on ne peut pas relayer une authentification vers le même hôte qui l'a générée (protection anti-reflexion implémentée par Microsoft). L'attaquant doit donc relayer vers un autre serveur que celui qui a initié l'authentification.

Outils offensifs NTLM Relay : l'arsenal du pentester en 2026

L'écosystème offensif autour de NTLM Relay s'est considérablement enrichi ces dernières années. Voici les outils incontournables utilisés lors des audits de sécurité Active Directory.

Responder : l'empoisonneur réseau multiprotocole

Responder, développé par Laurent Gaffié (SpiderLabs puis indépendant), est l'outil standard d'empoisonnement LLMNR/NBT-NS. Il répond aux requêtes de résolution de noms sur le réseau local pour forcer des authentifications NTLM vers l'attaquant. En mode capture (sans relay), il capture les hashes NTLMv2 pour les cracker offline. En mode relay, il est couplé à ntlmrelayx et se configure pour ne pas intercepter SMB et HTTP lui-même.

```
 # Mode capture simple
python3 Responder.py -I eth0 -rdwP

# Mode relay (désactiver SMB et HTTP pour laisser ntlmrelayx écouter)
python3 Responder.py -I eth0 -rdwP --disable-ess --lm
```

En 2026, Responder supporte également l'empoisonnement mDNS (Multicast DNS) et DHCP, élargissant considérablement sa surface d'interception. La configuration clé : dans Responder.conf, mettre SMB = Off et HTTP = Off lorsqu'on utilise ntlmrelayx simultanément, pour que les authentifications captées soient transmises au relay plutôt qu'absorbées localement par Responder.

ntlmrelayx : le couteau suisse du relay NTLM

Développé par Fox-IT et intégré dans la suite Impacket, ntlmrelayx est l'outil de relay le plus complet disponible. Il supporte de nombreux protocoles cibles et propose des actions post-exploitation automatisées qui peuvent mener à une compromission complète du domaine Active Directory.

```
 # Relay vers SMB sur toutes les machines du réseau (fichier targets.txt)
python3 ntlmrelayx.py -tf targets.txt -smb2support

# Relay vers LDAP pour dumper les informations AD
python3 ntlmrelayx.py -t ldap://DC01.domaine.local --dump-laps --dump-adcs

# Relay vers LDAP pour créer un compte avec droits DCSync
python3 ntlmrelayx.py -t ldap://DC01.domaine.local --escalate-user attacker

# Relay vers ADCS pour obtenir un certificat
python3 ntlmrelayx.py -t http://CA01.domaine.local/certsrv/certfnsh.asp \
  --adcs --template DomainController
```

Les fonctionnalités avancées de ntlmrelayx incluent : le shadow credentials attack (ajout de msDS-KeyCredentialLink via LDAP), la délégation contrainte basée sur les ressources (RBCD), et la manipulation d'ACL dans l'annuaire Active Directory. Ces actions post-relay peuvent mener à une compromission complète du domaine sans jamais avoir craqué un seul mot de passe ni déclenché la moindre alerte antivirus.

Impacket et l'écosystème complémentaire

Au-delà de ntlmrelayx, la suite Impacket propose des outils complémentaires pour les phases post-relay : secretsdump.py (extraction des hashes SAM et NTDS.dit), psexec.py (exécution distante via SMB), wmiexec.py et smbexec.py. En 2026, des outils comme Coercer (coercition

d'authentification via plus de 12 méthodes RPC) et DFSCoerce ont rejoint l'arsenal standard, permettant de forcer des authentifications NTLM depuis n'importe quel serveur Windows, y compris les contrôleurs de domaine, sans condition préalable d'accès particulier.

Scénarios d'attaque NTLM Relay avancés en 2026

Les attaques NTLM Relay ont évolué bien au-delà du simple SMB relay. Les scénarios modernes combinent plusieurs techniques pour atteindre une compromission totale du domaine. L'analyse des chemins d'attaque avec BloodHound permet d'identifier les cibles optimales pour ces relais avant même de lancer une quelconque exploitation.

LDAP Relay : la voie royale vers le Domain Admin

Le relay vers LDAP est particulièrement puissant car il permet de modifier les objets Active Directory sans nécessiter de droits administrateur locaux sur la cible SMB. Si l'attaquant relaie une authentification d'un utilisateur disposant de permissions LDAP suffisantes — membre des groupes Exchange Trusted Subsystem, comptes de service avec délégation, ou tout compte avec des droits GenericWrite sur le domaine — il peut accorder des droits DCSync à un compte contrôlé, ajouter des membres aux groupes Domain Admins ou Enterprise Admins, modifier les attributs msDS-KeyCredentialLink pour une attaque Shadow Credentials, ou configurer une délégation contrainte basée sur les ressources (RBCD) pour usurper n'importe quel utilisateur du domaine.

ADCS Relay : la bombe à retardement des certificats

Depuis la publication des scénarios d'escalade "ESC" dans la recherche "Certified Pre-Owned" de Will Schroeder et Lee Christensen en 2021, le relay vers Active Directory Certificate Services (ADCS) est devenu une technique de choix. En relayant l'authentification du contrôleur de domaine vers l'interface web des services de certificats, l'attaquant peut obtenir un certificat au nom du DC, puis l'utiliser pour s'authentifier en tant que celui-ci via PKINIT — menant

directement à un Golden Ticket ou à un DCSync complet. Cette chaîne d'exploitation PetitPotam + ADCS Relay a marqué un tournant dans la sécurité des PKI Active Directory.

CVE majeures exploitant NTLM Relay (2019-2026)

CVE	Nom	Année	Impact	CVSS
CVE-2019-1040	Drop the MIC	2019	Bypass du Message Integrity Code, relay NTLM vers LDAP depuis SMB	8.1
CVE-2019-1384	Ghost Potato	2019	Bypass anti-relay SMB, relay réflexif possible	8.0
CVE-2021-36942	PetitPotam	2021	Coercition NTLM depuis DC via MS-EFSRPC sans authentification	9.8
CVE-2022-26925	LSA Spoofing	2022	Coercition NTLM DC via LSARPC, contourne patch PetitPotam	8.1
CVE-2024-38124	Netlogon Relay	2024	Relay NTLM via Netlogon, élévation de privilèges domaine	9.0
CVE-2025-29810	LDAP Relay Bypass	2025	Contournement EPA sur LDAP, relay vers LDAPS possible	8.7

Ces CVE illustrent la persistance de la surface d'attaque NTLM. Malgré les correctifs successifs, de nouveaux vecteurs de coercition sont régulièrement découverts par la communauté de recherche en sécurité offensive. Pour rester informé, suivez les bulletins du CERT-FR de l'ANSSI et le Microsoft Security Response Center (MSRC).

Contre-mesures et durcissement Active Directory contre NTLM Relay

La bonne nouvelle est qu'il existe des contre-mesures efficaces pour neutraliser la quasi-totalité des vecteurs d'attaque NTLM Relay. Leur mise en œuvre demande un inventaire préalable des usages NTLM dans l'organisation, afin d'éviter de casser des applications legacy dépendantes de ce protocole. Un audit de santé Active Directory par script PowerShell peut révéler l'étendue réelle de l'utilisation de NTLM dans votre environnement avant tout changement de configuration.

1. Activer la signature SMB obligatoire (SMB Signing)

La contre-mesure la plus critique et la plus rapide à déployer : forcer la signature cryptographique des échanges SMB. Avec SMB Signing requis, l'attaquant ne peut pas relayer les authentifications SMB car le serveur cible exige que tous les paquets SMB soient signés avec une clé dérivée de la session — clé que l'attaquant positionné en man-in-the-middle ne possède pas.

```
 # Vérification de l'état actuel via PowerShell
Get-SmbServerConfiguration | Select RequireSecuritySignature, EnableSecuritySignature
Get-SmbClientConfiguration | Select RequireSecuritySignature

# Activation côté serveur
Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
Set-SmbClientConfiguration -RequireSecuritySignature $true -Force

# Via GPO (recommandé en production) :
# Computer Configuration > Windows Settings > Security Settings > Local Policies
# "Microsoft network server: Digitally sign communications (always)" = Enabled
# "Microsoft network client: Digitally sign communications (always)" = Enabled
```

Important : SMB Signing ne protège que contre le relay SMB vers SMB. Il ne bloque pas le relay SMB vers LDAP ou SMB vers HTTP. Des mesures complémentaires sont impérativement nécessaires pour une protection complète.

2. Activer l'Extended Protection for Authentication (EPA) sur LDAP et HTTP

EPA (Channel Binding) lie l'authentification NTLM au canal TLS sous-jacent. Cela rend le relay vers LDAPS ou HTTPS impossible car l'attaquant ne peut pas reproduire le channel binding token du canal TLS original. À activer sur les DCs (LDAP), IIS et Exchange (authentification Windows), et ADCS (interface certsrv). La valeur de registre LdapEnforceChannelBinding = 2 sur les DCs impose le channel binding pour toutes les connexions LDAP sécurisées.

3. Désactiver LLMNR et NBT-NS

Supprimer les vecteurs d'interception de Responder en désactivant les protocoles de résolution de noms non-DNS est une mesure à faible impact opérationnel et à haute valeur sécuritaire.

LLMNR se désactive via GPO (Turn off multicast name resolution = Enabled dans les paramètres DNS Client). NBT-NS se désactive via les options DHCP ou les paramètres d'interface réseau (NodeType = 2 dans le registre).

4. Désactiver ou restreindre NTLM avec des politiques granulaires

L'ANSSI recommande dans son guide de recommandations Active Directory une désactivation progressive de NTLM en quatre étapes : audit des usages via les Event ID 8001-8004, blocage de NTLMv1 via la GPO "Network security: LAN Manager authentication level = Send NTLMv2 response only", restriction par liste blanche des serveurs autorisés à recevoir du NTLM, puis désactivation totale après validation qu'aucune application n'utilise encore ce protocole.

5. Activer le filtrage des sessions RPC pour contrer la coercition

Pour bloquer PetitPotam et les variantes de coercition RPC, appliquez le patch Microsoft KB5005413, ajoutez des règles de filtrage RPC pour bloquer les UUID d'interface vulnérables sur les DC, et désactivez le service Windows Encrypting File System (EFS) si non utilisé dans votre environnement. Des outils comme RPCFirewall (open source) permettent un filtrage granulaire des appels RPC reçus par les contrôleurs de domaine.

Détection des attaques NTLM Relay : surveillance et réponse aux incidents

La détection efficace des attaques NTLM Relay nécessite une collecte de logs centralisée et des règles de corrélation adaptées. Voici les indicateurs clés à surveiller, utiles pour compléter votre surveillance Active Directory. Ces données doivent être remontées dans un SIEM pour corrélation en temps réel.

Événements Windows à surveiller

Event ID	Source	Signification	Gravité
4624	Security	Logon réussi — filtrer Type 3 (réseau) depuis hôtes inattendus	Moyenne
4625	Security	Échec d'authentification — bursts depuis une IP = relay raté	Haute
4648	Security	Logon avec credentials explicites — relay en cours	Haute
8001	NTLM	NTLM authentication succeeded (audit outgoing)	Info
8003	NTLM	NTLM authentication blocked	Haute
5145	Security	Accès partage réseau — IPC$ depuis IP inconnue via NTLM	Haute

Signaux réseau et règles de détection SIEM

Sur le plan réseau, les signatures caractéristiques d'un relay NTLM incluent des réponses LLMNR ou NBT-NS provenant d'une machine non-serveur DNS habituelle, des tentatives de connexion SMB vers de nombreuses cibles depuis une machine inhabituelle dans un court laps de temps, et des authentifications NTLM vers LDAP initiées depuis des postes de travail qui n'ont normalement pas à interroger directement LDAP. La corrélation de ces événements dans un SIEM avec les Event ID 4624 correspondants permet de détecter un relay NTLM abouti en quasi-temps réel. Les outils de détection spécialisés comme Microsoft Defender for Identity (anciennement Azure ATP) intègrent des règles de détection NTLM Relay par défaut, basées sur ces mêmes indicateurs comportementaux.

À RETENIR

À retenir : NTLM Relay 2026

NTLM Relay est distinct du Pass-the-Hash : le relay intercepte une session en temps réel sans jamais connaître le hash — donc NTLMv2 est vulnérable

Responder + ntlmrelayx : le duo standard permettant une compromission de domaine en moins de 10 minutes dans un réseau non-durci sans aucun bruit particulier

SMB Signing obligatoire : contre-mesure numero 1, déployable via GPO sans impact applicatif majeur sur les environnements modernes

EPA/Channel Binding : bloque le relay vers LDAPS et HTTPS, indispensable sur les DCs et ADCS pour protéger l'infrastructure d'identité

Désactiver LLMNR/NBT-NS : supprime le vecteur d'interception de Responder sans coût fonctionnel dans les environnements avec DNS correctement configuré

Audit NTLM avant désactivation : identifier les applications legacy via les Event ID 8001-8004 avant toute restriction pour éviter les pannes

PetitPotam et variantes RPC : patchez et filtrez les interfaces RPC vulnérables sur vos DCs pour bloquer la coercition d'authentification

Questions fréquentes sur NTLM Relay

Quelle est la différence fondamentale entre une attaque NTLM Relay et un Pass-the-Hash ?

La différence est fondamentale : dans un Pass-the-Hash, l'attaquant possède déjà le hash NTLM de l'utilisateur, obtenu via Mimikatz, secretsdump ou une autre technique d'extraction, et l'utilise directement pour s'authentifier en se faisant passer pour cet utilisateur. Dans un NTLM Relay, l'attaquant n'a jamais le hash — il se positionne en man-in-the-middle entre une victime et un serveur, intercepte le flux d'authentification NTLM en cours (les trois messages NTLM Type 1, 2 et 3) et le relaie en temps réel vers un service tiers cible. C'est pourquoi NTLM Relay fonctionne même avec NTLMv2, qui protège contre le crackage offline et le PtH direct, mais reste vulnérable au relay car il n'inclut pas de protection cryptographique contre la retransmission du défi-réponse à un service tiers non prévu.

Comment détecter une attaque NTLM Relay en temps réel sur mon réseau ?

La détection en temps réel repose sur plusieurs niveaux complémentaires. Au niveau réseau, surveillez les réponses LLMNR et NBT-NS anormales provenant d'une machine non-serveur DNS, et les connexions SMB en masse depuis une machine vers plusieurs cibles en quelques secondes. Au niveau Active Directory, les Event ID 4624 de type 3 (logon réseau NTLM) provenant d'adresses IP inattendues pour un compte donné sont un indicateur fort. Les modifications LDAP soudaines sur des attributs sensibles tels que msDS-KeyCredentialLink ou les membres d'un groupe privilégié, corrélées avec un logon NTLM depuis un poste inhabituel, constituent un signal de relay abouti. Un SIEM avec règles Sigma dédiées et des alertes sur les Event ID 8003 (NTLM bloqué) permettent une détection quasi-temps réel des tentatives de relay.

Est-il possible de réaliser un NTLM Relay même si Kerberos est activé dans le domaine ?

Absolument, et c'est un point de confusion fréquent même parmi les professionnels de la sécurité. Kerberos est le protocole d'authentification préféré dans Active Directory, mais NTLM reste activé par défaut comme protocole de fallback obligatoire. Dès lors qu'une machine client accède à une ressource par adresse IP plutôt que par nom DNS, qu'elle accède à un service ne supportant pas Kerberos, ou que le DC Kerberos est inaccessible, Windows bascule automatiquement vers NTLM sans avertissement. De plus, de nombreux protocoles et applications utilisent NTLM indépendamment de Kerberos. La désactivation complète de NTLM via les GPO de restriction est la seule solution définitive, mais elle nécessite un inventaire préalable rigoureux des usages pour éviter de casser des applications critiques métier.

Le déploiement de Windows 11 et Windows Server 2025 réduit-il significativement le risque NTLM Relay ?

Oui, significativement mais pas totalement. Windows 11 et Server 2025 désactivent par défaut NTLMv1 et implémentent des protections renforcées : SMB Signing activé par défaut côté client depuis Windows 11 22H2, EPA activé par défaut sur LDAP dans Server 2025. Cependant, tant que des systèmes legacy (Windows Server 2016, 2019, applications métier non mises à jour) cohabitent dans le parc, NTLM reste présent et attaquable. Une stratégie de sécurité complète doit combiner la mise à jour des OS, l'activation forcée du SMB Signing côté serveur via GPO,

l'EPA sur LDAP et HTTP, la restriction de NTLM, et la surveillance comportementale via un SIEM.