Audit Active Directory : PingCastle, BloodHound et remédiation

Auditez votre Active Directory avec PingCastle et BloodHound : installation, lecture des rapports, 20 points critiques et plan de remédiation complet.

L'Active Directory reste, en 2025-2026, le vecteur d'attaque privilégié dans plus de 90 % des incidents de ransomware et d'espionnage industriel affectant les entreprises françaises et européennes. Selon les derniers rapports de l'ANSSI et de Microsoft, la quasi-totalité des compromissions majeures analysées impliquent une élévation de privilèges dans l'annuaire Windows avant l'exfiltration de données ou le déploiement de charge malveillante. Pourtant, la majorité des organisations n'auditent leur AD que de façon ponctuelle, souvent trop tard, après un incident. Conduire un audit Active Directory structuré, régulier et documenté avec des outils comme PingCastle, BloodHound ou SharpHound n'est plus une option réservée aux grandes ESN : c'est une nécessité pour tout système d'information critique. Ce guide vous accompagne pas à pas, de l'installation des outils jusqu'à la priorisation des findings et la construction d'un plan de remédiation efficace, en couvrant les 20 points critiques que tout auditeur doit vérifier.

À RETENIR

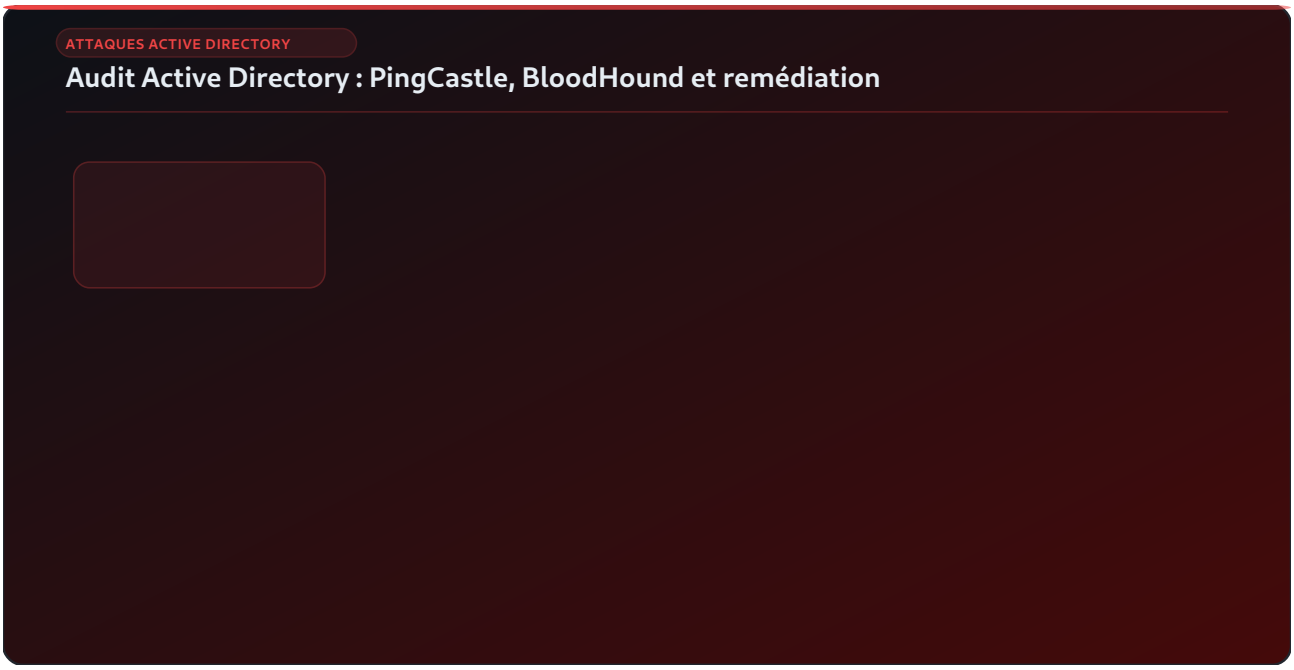
À retenir :

PingCastle génère un score de risque global et catégorise les anomalies AD en quelques minutes sans agent.

BloodHound/SharpHound visualise les chemins d'attaque vers les Domain Admins grâce à des graphes et requêtes Cypher.

Les 20 points critiques incluent Kerberoasting, AS-REP Roasting, délégation non contrainte, AdminSDHolder, LAPS et tiering.

Un plan de remédiation efficace distingue les quick wins (moins de 2 jours) des projets structurels (plusieurs mois).



Les statistiques 2025-2026 sont sans appel : selon le rapport M-Trends 2025 de Mandiant, le temps médian avant détection d'une compromission AD est de 16 jours. Durant cette fenêtre, un attaquant peut cartographier l'ensemble du domaine, identifier les comptes privilégiés, et préparer une attaque de type DCSync ou Golden Ticket en toute discrétion. L'ANSSI recense chaque année des dizaines d'incidents où l'AD constituait le pivot central de l'attaque, permettant aux acteurs malveillants de rebondir latéralement vers des systèmes industriels, des sauvegardes ou des environnements cloud hybrides.

Un audit AD régulier — idéalement trimestriel pour les environnements sensibles, semestriel au minimum — permet de détecter la dérive de configuration : un compte de service créé en urgence avec des privilèges excessifs, une GPO mal configurée qui ouvre un vecteur d'escalade, ou un groupe imbriqué qui accorde silencieusement des droits Domain Admin à des utilisateurs non autorisés. La dette technique s'accumule rapidement dans les annuaires qui ont traversé des migrations, des fusions-acquisitions ou des projets d'intégration cloud.

L'audit AD s'inscrit également dans les exigences réglementaires : NIS 2 impose une gestion des risques et une supervision des accès privilégiés, ISO 27001 requiert la revue périodique des

droits d'accès (contrôle A.9.2.5), et le référentiel PGSSI-S du ministère de la Santé mentionne explicitement la sécurisation de l'annuaire. Documenter vos audits constitue une preuve de conformité opposable en cas de contrôle ou d'incident.

PingCastle : installation, exécution et lecture du rapport

PingCastle est un outil gratuit (licence professionnelle disponible) développé par Netwrix, qui évalue le niveau de risque d'un domaine Active Directory en quelques minutes sans installation d'agent. Il collecte des informations via LDAP et les protocoles natifs Windows depuis n'importe quel poste joint au domaine.

> ⚡ **Retour terrain**
>
> J'utilise BloodHound systématiquement en début de mission AD. Pour un groupe de distribution retail, la cartographie a révélé un chemin de 4 sauts depuis un compte utilisateur standard vers Domain Admin — via un GPO modifiable par le compte, appliqué à une OU contenant un admin, avec une ACL WriteOwner sur un groupe privilégié. Aucun des quatre liens n'était visible sans la vue graphique. La correction a pris 2 heures une fois le chemin identifié.

Installation et exécution de PingCastle

PingCastle se télécharge depuis pingcastle.com sous forme d'un exécutable portable. Aucune installation n'est requise. Exécutez-le depuis un compte utilisateur standard (les droits admin ne sont pas nécessaires pour un audit de base) :

```
 # Téléchargement et exécution (depuis un poste Windows joint au domaine)
PingCastle.exe --healthcheck --server domain.local

# Mode interactif (menu guidé)
PingCastle.exe

# Audit multi-domaines avec trust mapping
PingCastle.exe --healthcheck --server . --explore-trust
```

PingCastle génère un rapport HTML autonome (PingCastle_HealthCheck_DOMAIN_YYYYMMDD.html) et un fichier XML exploitable pour l'intégration dans un tableau de bord. L'exécution complète prend entre 2 et 15 minutes selon la taille du domaine.

Lecture du rapport et score de risque

Le rapport PingCastle présente un score global de 0 à 100 (100 = risque maximal) décomposé en quatre catégories :

StaleObjects : comptes inactifs, machines obsolètes, mots de passe jamais changés

Trusts : relations d'approbation, SID filtering désactivé, trusts transitifs non justifiés

Anomalies : délégations Kerberos, AdminSDHolder, schéma AD étendu

PrivilegedAccounts : membres de groupes sensibles, comptes de service avec privilèges excessifs

Chaque finding est documenté avec son niveau de risque (critical, high, medium, informational), une explication technique et une recommandation de remédiation. Portez une attention particulière aux findings marqués "critical" : ils représentent des vecteurs d'escalade exploitables immédiatement par un attaquant disposant d'un accès utilisateur standard.

BloodHound et SharpHound : graphes et chemins d'attaque

BloodHound est un outil d'analyse des relations dans l'Active Directory qui utilise la théorie des graphes pour identifier les chemins d'attaque vers les comptes et groupes privilégiés. Développé initialement par SpecterOps (voir github.com/BloodHoundAD/BloodHound), il est devenu un standard de l'audit AD offensif et défensif. BloodHound CE (Community Edition) est la version open source maintenue activement.

Collecte des données avec SharpHound

SharpHound est le collecteur de données pour BloodHound. Il s'exécute depuis un poste Windows joint au domaine et collecte les ACL, les appartenances aux groupes, les sessions actives, et les objets GPO via LDAP et SMB :

```
 # Collecte complète (recommandée pour un audit)
SharpHound.exe -c All --zipfilename bloodhound_audit.zip

# Collecte sans sessions (plus discret, moins de bruit réseau)
SharpHound.exe -c DCOnly,ACL,ObjectProps,Container,GPOLocalGroup

# Collecte depuis un contexte non joint (avec credentials)
SharpHound.exe -c All -d domain.local --ldapusername auditeur --ldappassword P@ssw0rd
```

La collecte génère un fichier ZIP contenant des fichiers JSON que vous importez dans l'interface BloodHound. Pour les environnements sensibles, préférez une collecte DCOnly qui n'établit pas de connexions SMB vers toutes les machines.

Requêtes Cypher critiques dans BloodHound

Une fois les données importées, ces requêtes Cypher révèlent les chemins d'attaque les plus critiques :

```
 # Trouver les chemins les plus courts vers Domain Admins depuis tous les users
MATCH p=shortestPath((u:User)-[*1..]->(g:Group {name:"DOMAIN ADMINS@DOMAIN.LOCAL"}))
WHERE NOT u=g RETURN p

# Kerberoastable users avec admin local
MATCH (u:User {hasspn:true})-[:AdminTo]->(c:Computer) RETURN u.name, c.name

# Délégations non contraintes (hors DCs)
MATCH (c:Computer {unconstraineddelegation:true}) WHERE c.name <> "DC01.DOMAIN.LOCAL" RETURN c.na

# ACL dangereuses : qui peut modifier les Domain Admins ?
MATCH p=(u)-[:GenericAll|GenericWrite|WriteOwner|WriteDacl]->(g:Group {name:"DOMAIN ADMINS@DOMAIN

# Utilisateurs avec DCSync rights
MATCH (u)-[:DCSync|GetChangesAll]->(d:Domain) RETURN u.name
```

Ces requêtes constituent le cœur de l'analyse BloodHound. Le chemin le plus court vers Domain Admins depuis un utilisateur standard représente la profondeur de compromission maximale qu'un attaquant peut atteindre sans exploiter de vulnérabilité logicielle.

PowerView et AD Explorer : requêtes manuelles complémentaires

PowerView (inclus dans PowerSploit) offre des cmdlets PowerShell pour interroger l'AD de façon granulaire. Combiné à BloodHound, il permet de vérifier manuellement les findings et d'explorer des vecteurs spécifiques :

```
 # Comptes avec SPN (Kerberoastable)
Get-DomainUser -SPN | Select-Object samaccountname, serviceprincipalname

# AS-REP Roastable (ne nécessitent pas de pré-authentification Kerberos)
Get-DomainUser -UACFilter DONT_REQ_PREAUTH | Select-Object samaccountname

# Machines avec délégation non contrainte
Get-DomainComputer -UnconstrainedDelegation | Select-Object dnshostname, useraccountcontrol

# ACL sur AdminSDHolder
Get-ObjectAcl -ADSprefix "CN=AdminSDHolder,CN=System" -ResolveGUIDs |
  Where-Object {$_.ActiveDirectoryRights -match "GenericAll|WriteProperty|WriteDacl"}

# GPO appliquées à une OU sensible
Get-DomainGPO -ComputerIdentity DC01 | Select-Object displayname, gpcfilesyspath
```

SysInternals AD Explorer complète l'analyse en offrant une vue graphique de la structure LDAP, utile pour examiner les attributs spécifiques des objets suspects et naviguer dans les ACL sans avoir à écrire des requêtes LDAP.

Outils complémentaires : Purple Knight et ORADAD

Purple Knight, développé par Semperis, est un outil gratuit qui évalue la posture de sécurité AD selon plus de 100 indicateurs de compromission (IoC) et indicateurs d'exposition (IoE). Contrairement à PingCastle qui se concentre sur la configuration, Purple Knight recherche aussi les traces d'activité suspecte passée : modifications d'objets critiques, resets de mot de passe AdminSDHolder, altérations de ACL sur les GPO sensibles.

ORADAD (Outil de Récolte et d'Analyse de Données Active Directory) est un projet de l'ANSSI qui automatise la collecte de données AD et produit des rapports conformes aux bonnes pratiques françaises. Il est particulièrement adapté aux audits commandés dans un contexte réglementaire ou pour les organismes de l'État.

Les 20 points critiques de l'audit Active Directory

Ces 20 points constituent le référentiel minimal de tout audit AD sérieux. Classés par ordre de criticité décroissante :

Points critiques niveaux 1-5 (remédiation immédiate)

1. Kerberoasting : Identifiez tous les comptes avec un SPN (Get-DomainUser -SPN). Les comptes de service avec des mots de passe faibles ou anciens sont directement exploitables. Voir notre article sur Kerberoasting : attaque et défense.

2. AS-REP Roasting : Les comptes avec DONT_REQ_PREAUTH permettent de récupérer un hash crackable hors-ligne sans aucune interaction avec la cible. Ce flag ne doit jamais être activé sauf cas exceptionnels documentés.

3. DCSync rights : Vérifiez qui dispose des droits DS-Replication-Get-Changes-All sur le domaine. Seuls les Domain Controllers et quelques outils légitimes (Azure AD Connect, Quest Recovery Manager) devraient avoir ces droits. Référez-vous à notre guide sur l'attaque DCSync.

4. Délégation non contrainte (Unconstrained Delegation) : Toute machine ou compte avec ce flag peut être utilisé pour capturer des tickets Kerberos TGT d'autres utilisateurs. Seuls les Domain Controllers sont légitimement concernés.

5. AdminSDHolder et SDProp : Vérifiez les ACL sur l'objet AdminSDHolder (CN=AdminSDHolder,CN=System). Toute entrée non standard est répliquée toutes les heures sur tous les comptes protégés du domaine (Domain Admins, Enterprise Admins, etc.).

Points critiques niveaux 6-10

6. LAPS (Local Administrator Password Solution) : Vérifiez si LAPS est déployé sur l'ensemble des postes de travail et serveurs. L'absence de LAPS permet le mouvement latéral via pass-the-hash avec un mot de passe administrateur local partagé.

7. Tiering Active Directory : Le modèle de tier 0/1/2 de Microsoft doit isoler les comptes Domain Admin (T0) des postes de travail (T2). Un administrateur qui se connecte depuis un poste de travail expose ses credentials Kerberos.

8. GPO dangereuses : Auditez les GPO qui déploient des scripts, modifient les droits locaux, ou contiennent des credentials en clair dans SYSVOL (cpassword dans les préférences GPO — vulnérabilité MS14-025).

9. ACL abusables : GenericAll, GenericWrite, WriteOwner, WriteDacl sur des objets critiques (Domain Admins, GPO, OU contenant des DCs) permettent une escalade discrète. BloodHound cartographie ces relations automatiquement.

10. Comptes de service avec privilèges excessifs : Les comptes de service membres de Domain Admins ou disposant de droits administrateurs locaux sur de nombreuses machines constituent des cibles privilégiées pour le Kerberoasting.

Points critiques niveaux 11-20

11. Mots de passe anciens : Identifiez les comptes dont le mot de passe n'a pas changé depuis plus de 365 jours, en particulier les comptes de service et les comptes admin.

12. Comptes inactifs : Les comptes utilisateurs et machines inactifs depuis plus de 90 jours représentent une surface d'attaque inutile et doivent être désactivés ou supprimés.

13. Constrained Delegation mal configurée : La délégation contrainte (S4U2Proxy) peut être détournée si elle est configurée sur un compte compromis pour usurper l'identité d'utilisateurs vers des services sensibles.

14. SID History abusable : La présence de SID provenant d'autres domaines dans l'attribut SIDHistory peut accorder des privilèges involontaires, notamment après des migrations.

15. Trusts mal sécurisés : Les relations d'approbation sans SID Filtering activé permettent à un attaquant qui contrôle un domaine de confiance d'escalader vers le domaine parent.

16. Print Spooler activé sur les DCs : Le service Spooler sur les Domain Controllers est exploitable via SpoolSample pour capturer des tickets Kerberos (attaque Printer Bug).

17. NTLM activé sans restriction : L'absence de restriction NTLM facilite les attaques de type NTLM Relay. Consultez notre guide sur NTLM Relay LDAP et RBCD.

18. Accès SYSVOL en écriture : Vérifiez que seuls les Domain Controllers ont accès en écriture à SYSVOL. Des ACL incorrectes peuvent permettre l'injection de scripts malveillants dans les GPO.

19. Comptes membres de groupes Built-in sensibles : Account Operators, Server Operators, Backup Operators, et Print Operators disposent de droits qui peuvent être détournés pour une élévation de privilèges indirecte.

20. Audit et journalisation insuffisants : Vérifiez que les politiques d'audit (Logon Events, Object Access, Privilege Use) sont activées et que les logs sont centralisés dans un SIEM. Sans logs, la détection est impossible.

Priorisation des findings : critique, élevé, moyen, faible

La priorisation des findings repose sur deux axes : la probabilité d'exploitation (liée à la facilité d'accès et aux outils disponibles) et l'impact potentiel (étendue des droits obtenus). Cette matrice guide la construction du plan de remédiation :

Critique : Exploitation triviale, impact Domain Admin ou exfiltration de données. Exemples : DCSync rights non justifiés, délégation non contrainte sur des serveurs critiques, cpassword en clair dans SYSVOL, chemin BloodHound vers Domain Admin en moins de 3 sauts. Remédiation sous 48h.

Élevé : Exploitation requiert quelques étapes mais reste accessible avec des outils publics. Exemples : comptes Kerberoastable avec mots de passe faibles, AS-REP Roastable, ACL GenericAll sur des GPO sensibles, LAPS absent sur les serveurs. Remédiation sous 2 semaines.

Moyen : Exploitation nécessite des conditions particulières ou un accès réseau spécifique. Exemples : NTLM non restreint, Printer Bug activé sur les DCs, SID History suspecte, tiering non appliqué. Remédiation sous 1 mois.

Faible : Amélioration de la posture sans risque immédiat. Exemples : comptes inactifs, mots de passe anciens sur des comptes non privilégiés, documentation manquante. Remédiation selon calendrier de maintenance.

Plan de remédiation : quick wins et projets structurels

La remédiation AD se structure en deux horizons temporels qu'il faut mener en parallèle :

Quick wins (moins de 2 jours par action)

Ces actions à fort impact et faible effort constituent les priorités absolues :

Révoquer les droits DCSync non justifiés et vérifier les membres de Domain Admins

Supprimer les cpassword des préférences GPO (script PowerShell ou Get-GPPPassword)

Désactiver la délégation non contrainte sur les comptes et machines non-DC

Corriger les ACL AdminSDHolder non standard

Désactiver les comptes inactifs depuis plus de 90 jours (après validation métier)

Activer la politique d'audit avancée sur les Domain Controllers

Désactiver le service Spooler sur les Domain Controllers

Projets structurels (semaines à mois)

Ces projets nécessitent une planification et un accompagnement du changement :

Déploiement LAPS v2 (Windows LAPS intégré à Windows Server 2022/2019) : inventaire, GPO, monitoring

Tiering AD : conception du modèle T0/T1/T2, création des silos d'authentification, migration des comptes

PAM (Privileged Access Management) : déploiement d'une solution Just-in-Time (CyberArk, BeyondTrust, ou solution open source)

Revue et nettoyage des SPN : audit des comptes de service, rotation des mots de passe, migration vers gMSA

Restriction NTLM : audit des dépendances applicatives, déploiement progressif des restrictions via GPO

Outillage continu : alertes SIEM et surveillance AD

L'audit ponctuel ne suffit pas : la dérive de configuration est un processus continu. La surveillance permanente repose sur plusieurs niveaux :

Microsoft Defender for Identity (MDI) : anciennement Azure ATP, MDI analyse les flux Kerberos et LDAP en temps réel et détecte les patterns d'attaque (Kerberoasting, DCSync, Golden Ticket, Pass-the-Hash). C'est la solution de référence pour les environnements hybrides Azure AD.

Wazuh SIEM : pour les environnements on-premises, Wazuh offre des règles de détection préconfigurées pour les événements AD critiques (4768, 4769, 4771, 4776). Voir notre guide sur BloodHound, SharpHound et BloodyAD.

Alertes Event ID critiques à surveiller :

```
 # Event IDs Windows critiques pour la surveillance AD
4625 - Echec de connexion (brute force)
4648 - Connexion avec credentials explicites (pass-the-hash)
4672 - Privilèges spéciaux assignés (connexion admin)
4728/4732/4756 - Ajout dans groupes sensibles
4769 - Demande de ticket Kerberos service (Kerberoasting si RC4)
4771 - Echec pré-authentification Kerberos (AS-REP Roasting)
5136 - Modification objet AD (ACL, groupes critiques)
4662 - Opération réplication répertoire (DCSync)
```

La mise en place d'alertes temps réel sur ces événements, corrélées avec des seuils de volume et des listes blanches des comptes légitimes, permet de détecter une attaque en cours en quelques minutes plutôt qu'en plusieurs jours.

FAQ — Questions fréquentes sur l'audit Active Directory

Quelle est la différence entre PingCastle et BloodHound pour un audit AD ?

PingCastle évalue la configuration globale du domaine et génère un score de risque avec des recommandations de remédiation : c'est l'outil de référence pour un état des lieux rapide et un reporting direction. BloodHound analyse les relations entre objets AD (groupes, comptes, machines, GPO) pour identifier les chemins d'attaque concrets vers les comptes privilégiés : c'est l'outil indispensable pour comprendre "comment un attaquant avec un compte standard peut devenir Domain Admin". Les deux outils sont complémentaires et doivent être utilisés ensemble dans tout audit sérieux.

Faut-il des droits Domain Admin pour exécuter un audit Active Directory ?

Non, et c'est d'ailleurs une bonne pratique de ne pas utiliser de compte privilégié pour la collecte, afin de simuler le niveau d'accès d'un attaquant interne. PingCastle fonctionne avec un compte utilisateur standard pour la majorité de ses checks. SharpHound nécessite un accès LDAP standard. PowerView et la plupart des requêtes d'audit fonctionnent également avec un utilisateur du domaine. Certains checks spécifiques (lecture des ACL système, accès SYSVOL étendu) peuvent nécessiter des droits supplémentaires, mais jamais Domain Admin complet pour une collecte de données.

À quelle fréquence doit-on réaliser un audit Active Directory complet ?

La fréquence recommandée dépend de la criticité de l'environnement : trimestrielle pour les secteurs régulés (santé, finances, OIV/OSE), semestrielle pour les ETI standard, et annuelle au minimum pour toute organisation. Cette fréquence doit être complétée par une surveillance continue (SIEM, MDI) et des audits ponctuels après tout changement majeur : migration, fusion-acquisition, incident de sécurité, ou déploiement d'un nouveau système connecté à l'AD. Le score PingCastle peut être intégré dans un tableau de bord mensuel pour suivre l'évolution de la posture de sécurité.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité.

