Purple Team 2026 : Exercices AD et Cloud en Pratique

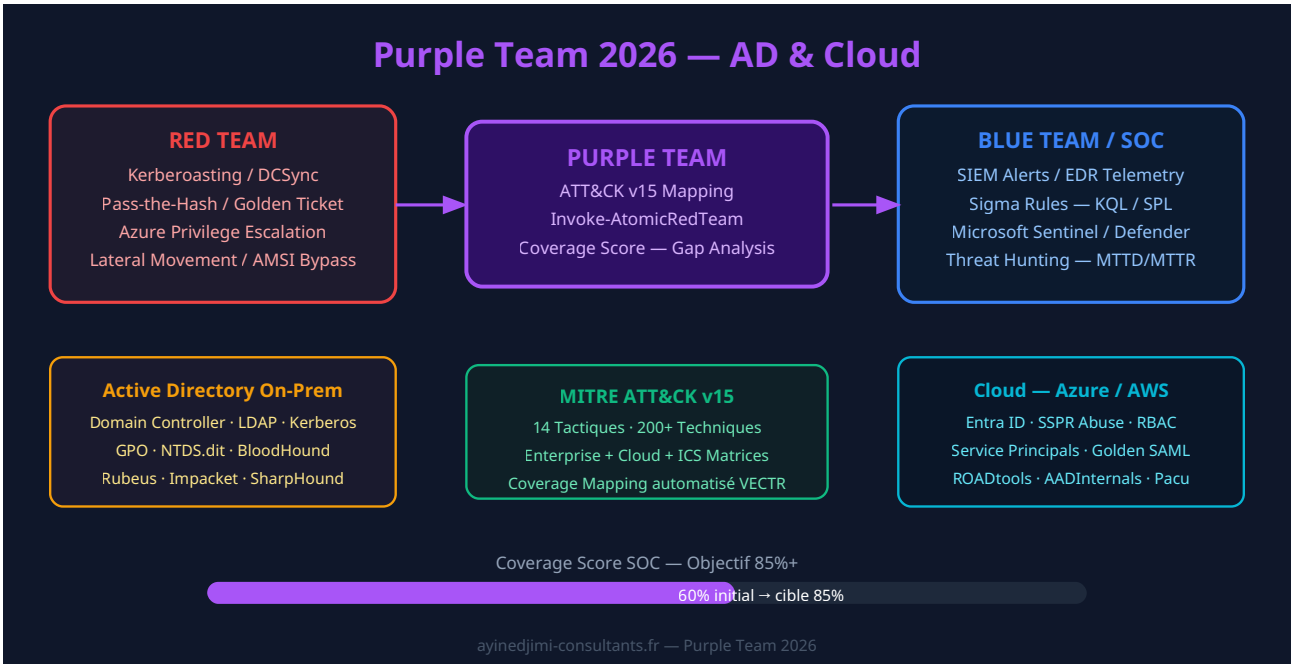
Maîtrisez les exercices purple team 2026 AD cloud : ATT&CK, Atomic Red Team, simulations hybrides Active Directory et Azure pour un SOC plus efficace.

Résumé exécutif

En 2026, les exercices **purple team** s'imposent comme la méthode la plus efficace pour tester et améliorer les capacités de détection d'un SOC face aux attaques hybrides Active Directory et cloud. Ce guide technique détaille les scénarios, outils et métriques indispensables pour organiser des exercices AD et cloud de niveau expert, en s'appuyant sur MITRE ATT&CK v15, Atomic Red Team et Invoke-AtomicRedTeam. Vous y trouverez une roadmap en quatre trimestres, un comparatif Red/Blue/Purple Team, des exemples de commandes, et les indicateurs de mesure d'efficacité attendus par les équipes SOC et les auditeurs NIS 2.

Le **purple team** représente l'évolution naturelle des tests d'intrusion classiques : au lieu d'opposer une équipe offensive (red team) à une équipe défensive (blue team) dans des silos distincts, le purple team les fait collaborer en temps réel pour maximiser l'apprentissage et la couverture de détection. Contrairement aux pentests classiques où le rapport final arrive des semaines après l'exercice, le purple team produit des améliorations de règles de détection immédiates, pendant l'exercice lui-même. En 2026, avec la généralisation des environnements hybrides Active Directory et Azure Entra ID, et la sophistication croissante des menaces ransomware et APT, les exercices purple team sont devenus un impératif stratégique pour toute

organisation voulant mesurer objectivement la maturité de son SOC. Ce guide vous explique comment concevoir, exécuter et mesurer des exercices purple team 2026 ciblant les infrastructures AD on-premises et cloud, en s'appuyant sur les frameworks MITRE ATT&CK, Atomic Red Team et Invoke-AtomicRedTeam pour des simulations reproductibles, documentées et alignées sur les menaces réelles observées en France et en Europe.



Architecture d'un exercice Purple Team 2026 : collaboration Red/Blue sur infrastructure AD et cloud, pilotée par MITRE ATT&CK v15 et Invoke-AtomicRedTeam

Qu'est-ce que le Purple Team en 2026 ?

Le *Purple Team* est une approche collaborative qui réunit les équipes offensives (red team) et défensives (blue team) dans un même exercice structuré, avec pour objectif principal d'améliorer la couverture de détection du SOC. Contrairement aux pentests adversariaux classiques, le purple team n'est pas une compétition : les deux équipes partagent ouvertement leurs actions, leurs outils et leurs observations pour produire des améliorations de règles de détection en temps réel, pendant l'exercice lui-même.

⚡ **Retour terrain**

Dans mes missions de red team, la phase de post-exploitation révèle systématiquement des données que le client pensait protégées. Le cas le plus fréquent : des fichiers Excel de comptabilité ou RH stockés sur des partages réseau accessibles à tous les utilisateurs du domaine, sans restriction. Sur les 30 dernières missions, 27 avaient des partages réseau avec des données sensibles accessibles à n'importe quel utilisateur authentifié. La sensibilité des données n'est pas corrélée à leur niveau de protection réel.

En 2026, la définition du purple team s'est enrichie de trois composantes majeures : l'intégration native des **environnements hybrides AD/cloud**, l'utilisation systématique du framework MITRE ATT&CK comme langage commun, et l'automatisation partielle via des outils comme Invoke-AtomicRedTeam. Cette évolution répond à la réalité des infrastructures modernes où la frontière entre Active Directory on-premises et Azure Entra ID est devenue poreuse, créant des chemins d'attaque multi-couches que seul le purple team permet d'appréhender de bout en bout.

Les exercices purple team 2026 se distinguent aussi par leur dimension métrique rigoureuse : chaque technique testée doit être associée à un **score de détection** (détectée / partiellement détectée / non détectée), et l'objectif chiffré est d'atteindre 75 à 85 % de couverture sur les techniques ATT&CK pertinentes pour l'organisation, contre une moyenne de départ souvent inférieure à 45 % pour les SOC non matures.

Anatomie d'un exercice Purple Team structuré

Un exercice purple team bien construit suit une méthodologie en quatre phases distinctes. La **phase de planification** définit le scope (AD uniquement, cloud uniquement, hybride), le threat model (quel groupe APT ou ransomware simuler ?), et les métriques de succès. Elle inclut la

sélection des 15 à 25 techniques ATT&CK à tester, choisies en fonction de la threat intelligence spécifique au secteur d'activité et des incidents passés de l'organisation.

La **phase d'exécution** alterne entre l'attaque d'une technique précise par la red team et l'observation collaborative des alertes générées dans le SIEM et l'EDR. La *gap analysis* est le cœur du purple team : pour chaque technique testée, l'équipe identifie si la détection existe, si elle est correctement tuned, et si elle déclenche la bonne playbook de réponse. Enfin, la **phase de remédiation immédiate** permet d'écrire ou d'ajuster les règles Sigma, KQL ou SPL pendant l'exercice, et de valider leur efficacité par un second passage de la technique offensive, confirmant que le gap est bien comblé.

> **Avertissement légal :** Les techniques offensives présentées dans cet article sont destinées exclusivement aux professionnels mandatés dans le cadre d'exercices purple team autorisés sur des infrastructures dont ils sont propriétaires ou pour lesquelles ils disposent d'une autorisation écrite explicite. Toute utilisation non autorisée est illégale et passible de poursuites en France sous les articles 323-1 et suivants du Code pénal.

Scénarios AD : attaques clés et règles de détection en 2026

L'**Active Directory** reste en 2026 la cible principale des attaquants dans les environnements enterprise. Notre guide complet du pentest Active Directory détaille les vecteurs d'attaque fondamentaux ; dans le contexte purple team, l'enjeu est de valider que chaque technique est effectivement détectée par le SOC en conditions réelles, avec les bons seuils d'alerte et les bonnes corrélations.

Les cinq techniques AD incontournables à tester lors d'un exercice purple team 2026 sont les suivantes. Le *Kerberoasting* (T1558.003) consiste à demander des tickets TGS pour des comptes avec SPN afin de les cracker offline — la détection repose sur l'Event ID 4769 avec EncryptionType 0x17 (RC4-HMAC). Le **DCSync** (T1003.006) simule la réplication AD pour extraire les hashes NTLM de tous les comptes du domaine, détectable via l'Event ID 4662 avec

les GUIDs de réplication 1131f6aa et 1131f6ad. Le **Pass-the-Hash** (T1550.002) utilise un hash NTLM capturé pour s'authentifier sans connaître le mot de passe clair, exploitant les protocoles NTLM et SMB.

Le *Lateral Movement via WMI et PSRemoting* (T1021.006) est particulièrement difficile à distinguer du trafic légitime dans les environnements où l'administration à distance est courante. Enfin, l'**AS-REP Roasting** (T1558.004) cible les comptes pour lesquels la pré-authentification Kerberos n'est pas requise — une mauvaise configuration fréquemment oubliée lors des durcissements AD. La détection repose sur l'Event ID 4768 avec PreAuthType égal à 0.

Environnement de lab Purple Team AD recommandé pour 2026

Pour reproduire ces scénarios dans un environnement contrôlé et légal, voici la configuration minimale validée :

- **DC Windows Server 2022** avec AD DS, niveau fonctionnel 2016 minimum, audit de sécurité avancé activé
- **2 workstations Windows 11** jointes au domaine pour simuler des utilisateurs standard et des comptes à privilèges
- **VM attaquant** : Kali Linux 2025.1 avec Impacket, BloodHound CE, Rubeus, Mimikatz et CrackMapExec
- **SIEM** : Splunk Free (500 MB/j) ou Elastic Security 8.x avec Windows Event Forwarding configuré vers un collecteur central
- **EDR** : Microsoft Defender for Endpoint (trial 90j) ou Elastic Agent avec les règles de détection communautaires
- **Purple Team Tooling** : Invoke-AtomicRedTeam et VECTR Community Edition pour le tracking des résultats

Purple Team Cloud : Azure, Entra ID et AWS en 2026

La dimension cloud du purple team 2026 est désormais incontournable. Les attaques hybrides AD/cloud — notamment via la synchronisation Azure AD Connect et ADFS — représentent le vecteur le plus exploité par les APT ciblant les entreprises françaises selon les rapports ANSSI 2025. L'objectif des exercices cloud est de tester la détection des techniques spécifiques aux environnements cloud, distinctes et complémentaires des techniques AD classiques.

Les scénarios Azure prioritaires en 2026 incluent l'**abus des Service Principals** (T1098.001) : création de credentials sur une application existante pour maintenir un accès persistant même après réinitialisation des mots de passe utilisateurs. L'**escalade de privilèges via rôles RBAC** Azure (T1078.004) exploite des configurations trop permissives sur les abonnements. Le *Golden SAML* (T1606.002) permet de forger des assertions SAML signées valides en compromettant la clé privée ADFS, offrant un accès persistant et furtif à tout service fédéré.

L'outil **AADInternals** (PowerShell) est la référence 2026 pour les exercices purple team Entra ID : il permet de simuler des techniques comme le Pass-the-PRT (Primary Refresh Token), l'abus de device enrollment et la compromission de comptes fedérés via Golden SAML. **ROADtools** complète cet arsenal avec l'énumération et l'analyse des configurations Entra ID pour identifier les chemins d'escalade. Pour les environnements AWS, les techniques d'abus de l'Instance Metadata Service (IMDS) et les escalades via politiques IAM trop permissives sont testées avec l'outil Pacu de Rhino Security Labs.

La détection côté cloud repose sur **Microsoft Sentinel** pour Azure, avec des règles d'analyse KQL couvrant les anomalies de Service Principal, les connexions depuis des localisations inhabituals et les modifications de rôles RBAC. Pour AWS, AWS CloudTrail et GuardDuty constituent le socle de détection à valider lors des exercices.

MITRE ATT&CK comme langage commun Red/Blue

Le framework MITRE ATT&CK est devenu en 2026 le standard universel pour structurer les exercices purple team. Sa version 15, publiée début 2026, couvre 14 tactiques, plus de 200 techniques et sous-techniques, avec des matrices dédiées Enterprise (Windows/Linux/macOS), Cloud (Azure/AWS/GCP/Microsoft 365) et ICS/OT.

L'apport fondamental d'ATT&CK dans un exercice purple team est de créer un **langage partagé** entre la red team qui exécute T1558.003 (Kerberoasting) et la blue team qui vérifie si l'alerte correspondante s'est déclenchée dans le SIEM. Cette référence commune élimine les ambiguïtés sémantiques et permet de produire des rapports exploitables par le management (coverage score par tactique) et les ingénieurs SOC (gap analysis par technique).

La matrice **ATT&CK for Cloud**, enrichie en 2026 avec des techniques spécifiques aux attaques sur Entra ID et les containers Kubernetes, est particulièrement pertinente pour les exercices purple team hybrides. Les données de **threat intelligence** disponibles sur la section Groups d'ATT&CK permettent de simuler précisément les TTPs d'acteurs comme APT29 (Midnight Blizzard), Scattered Spider ou des groupes ransomware actifs en France, rendant les exercices directement alignés sur les menaces réelles.

Atomic Red Team : framework de simulation standardisé

Le projet Atomic Red Team développé par Red Canary propose une bibliothèque de plus de 1 000 tests atomiques, chacun correspondant à une technique ATT&CK spécifique. Chaque atomic test est un script minimal (PowerShell, Bash, Python) qui exécute précisément la technique ciblée, avec la liste des prérequis, les commandes d'exécution et les commandes de nettoyage (cleanup), garantissant la reproductibilité et la réversibilité des tests.

L'outil d'orchestration **Invoke-AtomicRedTeam** (PowerShell) permet d'exécuter ces tests programmatiquement depuis une console d'attaquant, de les enchaîner pour simuler une kill chain complète, et de logger les résultats dans un format structuré. En 2026, Invoke-

AtomicRedTeam 2.x intègre nativement l'export vers des formats compatibles avec VECTR.io et Prelude Operator pour le tracking automatisé des résultats d'exercices purple team.

Exemple pratique : Kerberoasting avec Invoke-AtomicRedTeam

```
 # 1. Installation du module (environnement autorisé uniquement)
Install-Module -Name invoke-atomicredteam -Scope CurrentUser -Force
Import-Module invoke-atomicredteam

# 2. Vérifier les détails et prérequis pour T1558.003
Invoke-AtomicTest T1558.003 -ShowDetails
Invoke-AtomicTest T1558.003 -GetPrereqs

# 3. Exécution du test atomique Kerberoasting
Invoke-AtomicTest T1558.003

# 4. Nettoyage post-test
Invoke-AtomicTest T1558.003 -Cleanup

# 5. Enchaîner plusieurs techniques pour simuler une kill chain
$techniques = @("T1087.002","T1558.003","T1003.006","T1550.002")
foreach ($t in $techniques) {
    Invoke-AtomicTest $t
    Start-Sleep -Seconds 30  # laisser le temps au SOC de détecter
    Invoke-AtomicTest $t -Cleanup
}
```

Pendant cette exécution, la blue team observe en temps réel si les alertes correspondantes se déclenchent dans le SIEM (Event ID 4769 pour Kerberoasting, Event ID 4662 pour DCSync). Si aucune alerte n'est visible après 5 minutes, la règle de détection est manquante, désactivée ou mal configurée — un gap à documenter et corriger immédiatement.

Évasion EDR/XDR : dimension critique en 2026

Un exercice purple team 2026 qui n'intègre pas de techniques d'**évasion EDR** est incomplet. Les attaquants réels utilisent systématiquement des techniques d'obfuscation et de bypass pour

contourner les solutions de détection endpoints avant d'exécuter leurs payloads AD. Notre analyse approfondie des techniques d'évasion EDR/XDR détaille les méthodes les plus utilisées en 2026 avec leurs indicateurs de détection respectifs.

Dans un exercice purple team, on testera typiquement : le *process injection* (T1055) pour exécuter Mimikatz dans un processus légitime comme lsass.exe ou un processus signé Microsoft, le **AMSI bypass** (T1562.001) pour désactiver l'Antimalware Scan Interface avant l'exécution de scripts PowerShell offensifs, et les techniques de **living-off-the-land** (LOLBins T1218) qui abusent d'outils Windows légitimes comme certutil.exe, rundll32.exe ou mshta.exe pour éviter la détection par signature.

Notre article dédié au bypass EDR/XDR en 2026 pour red team couvre ces techniques en détail avec des indicateurs de détection précis. L'objectif dans un contexte purple team est de valider que le SOC détecte non seulement les comportements offensifs bruts, mais aussi leurs variantes obfusquées — car c'est précisément ainsi que les vrais acteurs APT opèrent en 2026.

Un aspect souvent négligé dans les exercices purple team est la persistance au niveau firmware. Les bootkits UEFI en 2026 représentent une catégorie de menaces que très peu de SOC savent détecter, et qu'un exercice purple team avancé devrait au moins cartographier en termes de gaps de visibilité, même si la simulation complète requiert un environnement physique dédié.

Les outils purple team open source de référence en 2026

L'écosystème des outils purple team a considérablement mûri en 2026. Trois catégories d'outils sont indispensables : les simulateurs d'attaque, les plateformes de tracking et les outils de visualisation des résultats. Voici les références open source actuelles pour chaque catégorie.

- **Invoke-AtomicRedTeam** : orchestrateur PowerShell de tests ATT&CK, plus de 1 000 tests atomiques couvrant Windows, Linux, macOS et cloud. Intégration native avec VECTR pour le reporting.

VECTR Community Edition : plateforme open source de tracking des exercices purple team. Permet de mapper les résultats sur la matrice ATT&CK, de calculer le coverage score et de générer des rapports d'exercice structurés.

Caldera (MITRE) : framework d'adversary emulation développé par le MITRE, avec des plugins pour automatiser des kill chains complètes basées sur les profils ATT&CK Groups. Particulièrement utile pour les exercices hybrides AD/cloud.

BloodHound Community Edition : cartographie des chemins d'attaque AD avec visualisation graphique. Indispensable en phase de planification pour identifier les techniques AD les plus critiques à tester en priorité.

Sigma Rule Repository : catalogue communautaire de règles de détection indépendantes du SIEM, convertibles en KQL, SPL ou Elasticsearch. Fournit un point de départ pour les règles à valider lors du purple team.

Comparatif Red Team, Blue Team et Purple Team en 2026

Comprendre les différences et complémentarités entre les trois approches est essentiel pour choisir l'exercice adapté à la maturité de votre organisation et à vos objectifs de sécurité en 2026. Les trois méthodes sont complémentaires et non substituables.

Critère	Red Team	Blue Team	Purple Team
Objectif principal	Compromettre l'organisation	Détecter et répondre	Améliorer la détection
Mode opératoire	Adversarial, furtif	Défensif, réactif	Collaboratif, transparent
Fréquence recommandée	1-2 fois par an	Continue (SOC 24/7)	Trimestrielle
Durée typique	2 à 6 semaines	Continue	2 à 5 jours
Livrables	Rapport de compromission	Métriques MTTR/ MTTD	Coverage score + règles Sigma
ROI mesurable	Difficile à quantifier	Partiel via KPIs SOC	Direct (% techniques détectées)
Prérequis maturité SOC	SOC opérationnel	Aucun	SIEM et EDR actifs et tuned
Conformité NIS 2	Partielle	Partielle	Forte (détection documentée)

Comment mesurer l'efficacité d'un exercice Purple Team ?

La mesure quantitative est l'une des grandes forces du purple team par rapport aux autres types d'exercices de sécurité. Le **coverage score** est la métrique principale : il exprime le pourcentage de techniques ATT&CK testées qui sont correctement détectées par le SOC avec une alerte de fidélité acceptable. Un score de départ typique pour une organisation sans programme purple team se situe entre 30 et 45 % — l'objectif après 12 mois de programme est d'atteindre 75 à 85 %.

Le *MTTD* (Mean Time To Detect) mesure combien de temps s'écoule entre l'exécution de la technique par la red team et la génération de l'alerte dans le SIEM. Le **MTTR** (Mean Time To Respond) mesure le temps entre l'alerte et la prise en charge effective par un analyste SOC. En 2026, les benchmarks industriels visent un MTTD inférieur à 5 minutes pour les techniques critiques AD (DCSync, Pass-the-Hash) et inférieur à 15 minutes pour les techniques cloud.

La **fidelity rate** (taux de fidélité des alertes) mesure la proportion d'alertes déclenchées qui correspondent effectivement à l'attaque simulée, en distinguant les vrais positifs des faux positifs générés par les règles trop sensibles. Un purple team qui améliore le coverage score mais génère un déluge de faux positifs épuise les analystes SOC et est contre-productif — la qualité des règles de détection est aussi importante que leur quantité. L'objectif est d'atteindre un taux de faux positifs inférieur à 15 % pour les alertes de sévérité haute.

Pourquoi le Purple Team est-il indispensable en 2026 ?

Trois tendances majeures de 2026 rendent le purple team incontournable pour toute organisation ayant un SOC opérationnel. Premièrement, la **généralisation des environnements hybrides AD/cloud** crée des chemins d'attaque complexes traversant plusieurs couches technologiques que ni la red team classique ni le SOC traditionnel ne peuvent appréhender seuls. Les exercices purple team hybrides sont le seul moyen de valider la détection de ces chemins de bout en bout, de l'initial access cloud jusqu'à la compromission du Domain Controller on-premises.

Deuxièmement, la **pression réglementaire NIS 2** (entrée en vigueur effective en France en 2025-2026) impose aux entités essentielles et importantes de démontrer leur capacité de détection et de réponse aux incidents. Un programme de purple team avec des métriques documentées — coverage score, MTTD/MTTR, gap analysis — constitue une preuve convaincante de maturité SOC pour les auditeurs et l'ANSSI lors des contrôles de conformité.

Troisièmement, la **sophistication croissante des menaces** a atteint un niveau tel que les tests ponctuels annuels ne suffisent plus. Les groupes ransomware actifs en France évoluent leurs TTPs sur des cycles mensuels, adoptant rapidement les nouvelles techniques de bypass EDR et d'exploitation cloud. Seul un programme purple team trimestriel permet de maintenir un coverage score élevé face à ces menaces en constante évolution, en testant les techniques nouvellement documentées dans les mises à jour ATT&CK dès leur publication.

Roadmap pour lancer un programme Purple Team en 2026

Voici une roadmap opérationnelle structurée en quatre trimestres pour les organisations souhaitant démarrer un programme purple team en 2026, partant d'un SOC avec SIEM et EDR déployés mais sans exercice purple team antérieur :

T1 — Foundation (mois 1-3) : Déployer Invoke-AtomicRedTeam et VECTR Community Edition. Cartographier les 20 techniques ATT&CK les plus pertinentes pour votre threat model sectoriel. Réaliser un premier exercice de baseline sur 10 techniques AD fondamentales pour établir le coverage score initial. Documenter les gaps prioritaires.

T2 — AD Coverage (mois 4-6) : Atteindre 70 % de coverage sur les 15 techniques AD critiques (Kerberoasting, DCSync, Pass-the-Hash, Lateral Movement WMI, BloodHound path exploitation). Écrire et valider les règles Sigma correspondantes. Former les analystes SOC aux playbooks de réponse associées.

T3 — Cloud Extension (mois 7-9) : Étendre le scope aux 15 techniques cloud Azure/AWS prioritaires. Tester les scénarios hybrides AD/cloud (Azure AD Connect abuse, Golden SAML, Service Principal credential add). Objectif : 65 % de coverage cloud. Intégrer Microsoft Sentinel ou Elastic Cloud dans le workflow de détection.

T4 — Automation et Continuous (mois 10-12) : Automatiser les 30 tests atomiques récurrents via scripts planifiés. Intégrer les résultats dans des dashboards SOC temps réel. Atteindre 80 %+ de coverage global AD et cloud combinés. Établir un cycle trimestriel pérenne avec rapport de couverture pour le RSSI et la direction.

À RETENIR

À retenir

Le **Purple Team 2026** combine red team et blue team en temps réel pour maximiser le coverage de détection SOC face aux attaques hybrides AD et cloud.

MITRE ATT&CK v15 est le langage commun indispensable : 14 tactiques, 200+ techniques, matrices Enterprise et Cloud. Référence sur attack.mitre.org.

Invoke-AtomicRedTeam permet d'automatiser l'exécution de tests standardisés reproductibles sur 1 000+ techniques ATT&CK depuis une console PowerShell.

Les exercices **hybrides AD/cloud** sont prioritaires en 2026 : Azure AD Connect, ADFS/Golden SAML et Service Principal abuse sont les vecteurs les plus exploités.

Le **coverage score cible** est de 75-85 % des techniques pertinentes après 12 mois de programme, avec un MTTD inférieur à 5 minutes sur les techniques critiques.

La conformité **NIS 2 et ANSSI** valorise un programme purple team documenté avec métriques comme preuve de maturité SOC lors des audits de contrôle.

FAQ — Purple Team 2026 AD et Cloud

Quelle est la différence concrète entre un exercice Purple Team et un pentest classique ?

Un pentest classique est un exercice adversarial où la red team tente de compromettre l'organisation de manière furtive, sans coordination avec la blue team, livrant un rapport de vulnérabilités plusieurs semaines après l'exercice. Le **purple team** est à l'opposé collaboratif et en temps réel : la red team exécute une technique spécifique de manière transparente, la blue team observe les alertes générées et ajuste ses règles de détection immédiatement. L'objectif n'est pas de "gagner" mais d'améliorer ensemble le coverage de détection. En 2026, les deux approches sont complémentaires et non substituables : le pentest et la red team mesurent la résistance globale de l'organisation à un adversaire déterminé, le purple team optimise les capacités de détection technique par technique. La fréquence recommandée pour une organisation mature est d'une red team annuelle complétée par quatre exercices purple team trimestriels ciblés sur les techniques les plus récentes.

Comment choisir les techniques ATT&CK à prioriser dans un exercice Purple Team 2026 ?

La sélection des techniques ATT&CK prioritaires doit se baser sur trois critères combinés et pondérés en fonction du contexte organisationnel. D'abord, la **threat intelligence sectorielle** : les techniques utilisées par les groupes APT et ransomware ciblant votre industrie sont disponibles sur les profils ATT&CK Groups de attack.mitre.org. Ensuite, les **angles morts identifiés** lors d'audits précédents ou d'incidents de sécurité passés de l'organisation — ce sont les gaps les plus critiques à combler en priorité. Enfin, les techniques à **fort impact business** doivent toujours figurer dans le top 10 : DCSync, Golden Ticket, Golden SAML et Azure Global Admin escalation constituent le socle minimum non négociable. En pratique, un premier exercice de deux jours peut couvrir 15 à 20 techniques soigneusement sélectionnées, ce qui est significativement plus efficace qu'un exercice exhaustif non structuré dilué sur trop de techniques.

Pourquoi les programmes Purple Team échouent-ils fréquemment en entreprise ?

Les facteurs d'échec des programmes purple team en entreprise sont bien documentés et évitables. Le premier facteur est le **manque de sponsorship managérial** : sans un RSSI ou DSI activement engagé, les recommandations post-exercice ne sont jamais implémentées et le programme s'essoufle après le premier exercice. Le deuxième est l'absence de SIEM et d'EDR correctement configurés et actifs — un purple team sur un SOC aveugle ne produit aucune valeur mesurable. Le troisième est un **scope trop ambitieux** pour le premier exercice : vouloir tout couvrir dès le départ mène à un exercice superficiel sans impact réel sur les règles de détection. Le quatrième facteur est la non-intégration dans le cycle de vie de la sécurité : le purple team doit être un programme récurrent et trimestriel, pas un exercice one-shot dont les résultats sont oubliés. Enfin, négliger la dimension **cloud et hybride AD** en se concentrant uniquement sur l'AD on-premises produit une image incomplète et trompeuse de la posture de sécurité réelle en 2026.

Quels outils open source sont recommandés pour débuter un programme Purple Team AD en 2026 ?

Pour un premier programme purple team AD avec un budget maîtrisé, la stack open source suivante est validée par la communauté en 2026. Côté offensif : **BloodHound Community Edition** avec SharpHound pour cartographier les chemins d'attaque AD, **Rubeus** pour les attaques Kerberos (Kerberoasting, AS-REP Roasting, Pass-the-Ticket), **Impacket** en Python pour DCSync, Pass-the-Hash et SMB relay, et Invoke-AtomicRedTeam pour orchestrer les tests ATT&CK de manière standardisée et reproductible. Côté défensif : **Velociraptor** pour la collecte de télémétrie et le threat hunting ad hoc, **Elastic SIEM 8.x** ou Wazuh pour la corrélation des événements Windows, et le catalogue **Sigma Community Rules** comme base de règles de détection de départ couvrant les techniques AD les plus communes. Pour le mapping et le reporting, **VECTR Community Edition** permet de tracker les résultats par technique ATT&CK et de générer automatiquement des rapports de coverage score exploitables par la direction et les équipes techniques.

Conclusion

Le purple team s'est imposé en 2026 comme l'approche la plus efficace et la plus mesurable pour améliorer la maturité défensive des organisations face aux menaces hybrides Active Directory et cloud. En combinant la rigueur méthodologique du framework MITRE ATT&CK, l'automatisation via Invoke-AtomicRedTeam, et la collaboration en temps réel entre équipes offensive et défensive, un programme purple team bien conduit transforme significativement les capacités de détection d'un SOC en 12 mois, avec un coverage score documenté et des métriques MTTD/MTTR améliorées de façon démontrable.

Les organisations qui n'ont pas encore démarré un programme purple team prennent un retard structurel face à des menaces qui évoluent plus vite que les cycles traditionnels d'audit annuel. Les pressions réglementaires NIS 2 et les recommandations de l'ANSSI rendent par ailleurs ce type d'exercice de plus en plus incontournable pour démontrer une maturité SOC crédible auprès

des auditeurs et des partenaires. La question n'est plus "faut-il faire du purple team ?" mais "comment structurer son programme pour obtenir le meilleur ROI en 2026 ?"