Purple Team 2026 : Exercices AD et Cloud — Méthodologie Complète

Points essentiels

- Le Purple Team fait collaborer Red et Blue Team en temps réel
- MITRE ATT&CK fournit le langage commun pour mesurer les gaps de détection
- Les scénarios ciblent Active Directory et les environnements cloud
- APT28, APT29, APT31 et APT41 visent particulièrement ETI et OIV françaises

À RETENIR

À retenir

Le Purple Team fait collaborer Red et Blue Team en temps réel

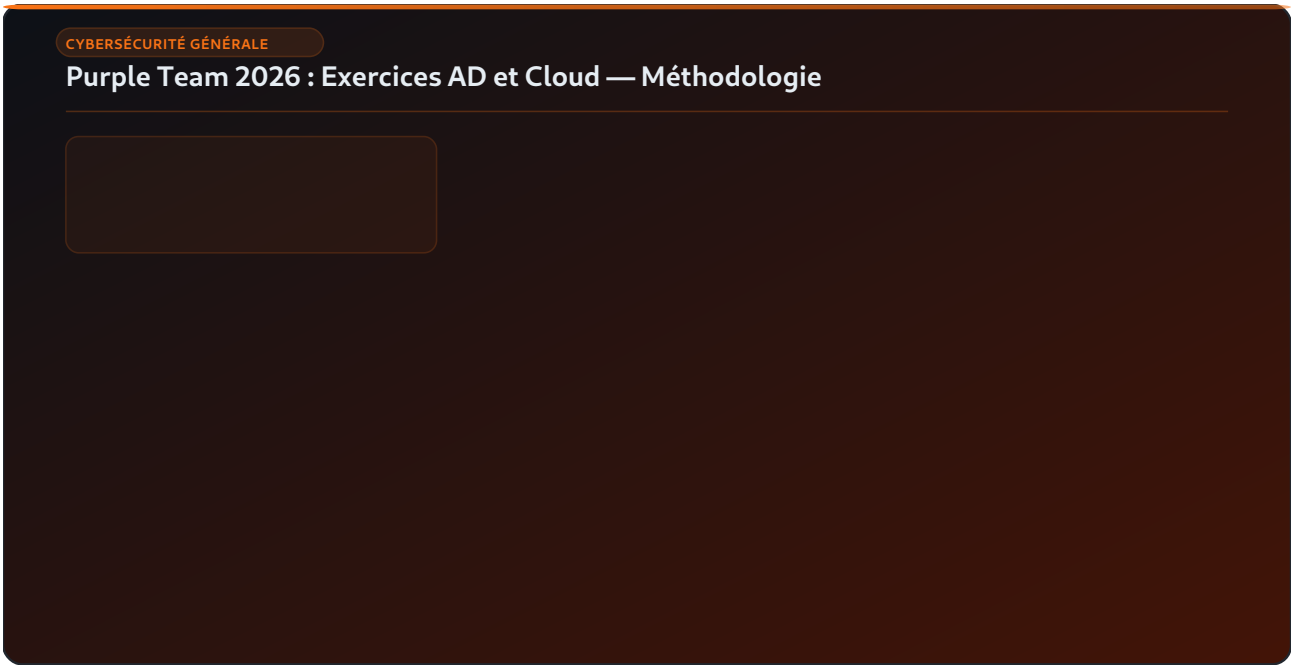
MITRE ATT&CK fournit le langage commun pour mesurer les gaps de détection

Les scénarios ciblent Active Directory et les environnements cloud

APT28, APT29, APT31 et APT41 visent particulièrement ETI et OIV françaises

Le Purple Team s'est imposé en 2026 comme l'approche la plus efficace pour renforcer concrètement la posture de sécurité des organisations françaises. Plutôt que d'opposer Red Team et Blue Team dans des exercices cloisonnés dont les rapports finissent trop souvent sans suite, il fait collaborer attaquants et défenseurs en temps réel : chaque technique jouée est immédiatement confrontée aux capacités de détection du SOC, puis les règles sont ajustées et rejouées jusqu'à validation. Cette boucle courte prend tout son sens sur les deux surfaces d'attaque les plus critiques aujourd'hui, l'Active Directory et les environnements cloud, où les chemins de compromission se croisent en permanence. Ce guide détaille une méthodologie complète de purple team exercises AD cloud : cadrage, matrice MITRE ATT&CK, scénarios d'escalade,

instrumentation des journaux et indicateurs de progression mesurables, applicables dès votre prochain exercice.



Le framework MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est la référence mondiale pour catégoriser les comportements des attaquants. **En 2026, ATT&CK Enterprise contient plus de 500 techniques et sous-techniques réparties sur 14 tactiques**, de la reconnaissance initiale (TA0043) à l'impact final (TA0040), en passant par l'accès initial, l'exécution, la persistance, l'élévation de privilèges, l'évasion de défense, l'accès aux credentials, la découverte, le mouvement latéral, la collection et l'exfiltration. Chaque technique est documentée avec ses procédures d'utilisation observées dans des campagnes réelles, les groupes APT qui l'emploient, les mitigations recommandées et les sources de données permettant de la détecter.

Pour un exercice Purple Team, ATT&CK joue deux rôles complémentaires. Côté Red Team, il guide la sélection des techniques à tester selon les TTP des groupes APT pertinents pour l'organisation — une ETI du secteur aérospatial français testera en priorité les techniques d'APT31 (groupe chinois ciblant l'industrie de défense), identifiées via le Navigator ATT&CK.

Côté Blue Team, il fournit le référentiel contre lequel mesurer la couverture de détection actuelle : pour chaque technique testée, le SOC peut-il alerter dans un délai acceptable ? Cette double utilisation fait d'ATT&CK le pivot méthodologique du Purple Team et la base de toute communication entre équipes offensives et défensives dans les organisations matures.

Atomic Red Team : automatiser les tests offensifs

Atomic Red Team est une bibliothèque open source maintenue par Red Canary, contenant plus de 1000 "atomics" — des tests unitaires de techniques ATT&CK, chacun consistant en un script d'exécution (PowerShell, Bash, Python) qui reproduit exactement une technique adversariale spécifique dans un environnement contrôlé. Par exemple, l'atomic T1003.001 (OS Credential Dumping : LSASS Memory) exécute `Invoke-Mimikatz` ou `procdump` sur le process LSASS et vérifie que les credentials sont extraits — ce qui déclenche (ou ne déclenche pas) une alerte dans l'EDR/SIEM. **L'intérêt d'Atomic Red Team pour les exercices Purple Team est de permettre des tests reproductibles et documentés, dont les résultats peuvent être comparés entre différentes sessions pour mesurer l'amélioration des capacités de détection dans le temps.**

> ⚡ **Retour terrain**
>
> Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

L'outil `Invoke-AtomicRedTeam` (module PowerShell) permet d'exécuter les atomics en ligne de commande avec logging automatique des résultats. Une session Purple Team typique commence par l'inventaire des techniques ATT&CK à tester (sélectionnées dans VECTR), l'exécution séquentielle des atomics correspondants, la vérification manuelle avec le Blue Team que les alertes attendues se sont bien déclenchées dans le SIEM, et la documentation des gaps découverts. Pour les équipes SOC n'ayant pas encore de Red Team interne, Atomic Red Team permet de démarrer des exercices Purple Team avec uniquement l'équipe bleue, car les atomics sont des scripts prêts à l'emploi ne nécessitant pas d'expertise offensive avancée.

VECTR : la plateforme de gestion des exercices Purple Team

VECTR (Vulnerability and Exploitation Correlation Tool for Red teams) est une plateforme web open source développée par SecurityRiskAdvisors qui centralise la planification, l'exécution et le reporting des exercices Purple Team. VECTR permet de créer des campagnes de test organisées par tactique ATT&CK, d'assigner des techniques aux opérateurs Red Team, d'enregistrer pour chaque test les résultats côté attaque (technique exécutée avec succès ?) et côté défense (alerte générée ? délai de détection ?), et de générer automatiquement des rapports de couverture ATT&CK. **La visualisation de couverture ATT&CK dans VECTR produit une heatmap ATT&CK Navigator montrant en rouge les techniques non détectées, en orange les techniques détectées tardivement, et en vert les techniques avec une détection rapide** — une visualisation immédiatement compréhensible par les RSSI et les directions pour piloter les investissements en capacités SOC.

VECTR s'installe en Docker (docker-compose up en 5 minutes) et s'intègre avec les SIEM les plus courants via des exports JSON/CSV compatibles avec Elastic, Splunk et Microsoft Sentinel. Pour les MSSP français proposant des services Purple Team à leurs clients ETI, VECTR permet de gérer plusieurs campagnes client en parallèle avec isolation des données, ce qui en fait la solution de référence pour les prestataires labellisés PRIS (Prestataire de Réponse aux Incidents de Sécurité) de l'ANSSI proposant des exercices Purple Team dans leur catalogue.

Scénario AD : Kerberoasting et détection

Le Kerberoasting est l'une des techniques d'escalade de privilèges Active Directory les plus couramment observées dans les compromissions réelles : un attaquant disposant d'un compte AD ordinaire demande des tickets de service Kerberos (TGS) pour des comptes de service ayant un SPN (Service Principal Name) enregistré, puis craque ces tickets hors ligne pour récupérer les mots de passe des comptes de service. L'efficacité du Kerberoasting tient à deux facteurs : la légitimité apparente de la requête TGS (tout utilisateur AD peut demander des tickets de service) et la fréquente utilisation de mots de passe faibles pour les comptes de service, qui n'ont souvent pas de politique d'expiration et utilisent des mots de passe définis manuellement par des administrateurs il y a plusieurs années.

Dans un exercice Purple Team, le scénario Kerberoasting se déroule ainsi : le Red Team exécute `Invoke-Kerberoast` (PowerShell/Impacket) depuis un compte utilisateur standard, récupère les hashes TGS-REP, et tente le cracking avec Hashcat. Parallèlement, le Blue Team surveille les Event ID 4769 (Kerberos Service Ticket Operations) avec un filtre sur les types de chiffrement RC4 (0x17) — une demande RC4 pour un compte de service ayant un SPN est un signal fort de Kerberoasting car les clients Windows modernes utilisent AES par défaut. **Une règle de détection Sigma efficace pour le Kerberoasting alerte sur plus de 5 demandes TGS de type RC4 en moins de 30 secondes depuis le même compte source**, ce qui exclut les comportements légitimes tout en capturant l'énumération massive caractéristique de l'outil automatisé.

Scénario AD : DCSync et protection des credentials

L'attaque DCSync exploite le protocole de réplication Active Directory pour extraire les hashes NTLM de tous les comptes du domaine, y compris KRBTGT, depuis un compte disposant des droits DS-Replication-Get-Changes et DS-Replication-Get-Changes-All. Ces droits sont normalement réservés aux contrôleurs de domaine eux-mêmes et à quelques comptes d'administration de réplication — mais dans les environnements mal configurés, ces droits sont

parfois accordés à des comptes de service ou d'administration dont la compromission permet à l'attaquant de passer directement à la compromission totale du domaine via la création d'un Golden Ticket.

Le scénario Purple Team DCSync teste : l'exécution de `lsadump::dcsync /domain:corp.fr /all` via Mimikatz depuis un compte compromis avec les droits de réplication, et la capacité du SIEM à détecter via l'Event ID 4662 (An operation was performed on an object) avec les GUID de propriété de réplication dans les attributs. **Microsoft Defender for Identity (MDI) offre une détection native du DCSync avec une alerte de sévérité haute**, mais nécessite un déploiement complet des sondes MDI sur tous les contrôleurs de domaine — un prérequis souvent incomplet dans les ETI qui n'ont déployé MDI que sur une partie de leur infrastructure DC. Le scénario Purple Team révèle précisément ces angles morts de déploiement.

Scénario AD : abus de GPO et persistance

Les objets de stratégie de groupe (GPO) Active Directory sont un vecteur de persistance et de mouvement latéral puissant : un attaquant contrôlant un compte avec des droits de modification sur une GPO liée à des OUs contenant des postes de travail ou des serveurs peut déployer des scripts malveillants exécutés au démarrage ou à l'ouverture de session de toutes les machines dans le périmètre de la GPO. La technique, référencée en ATT&CK sous T1484.001 (Domain Policy Modification : Group Policy Modification), est particulièrement dangereuse car elle permet de persister dans des centaines de machines simultanément avec des mécanismes de nettoyage difficiles.

Dans l'exercice Purple Team, le Red Team identifie d'abord les GPO modifiables par le compte compromis via `Get-GPPermission` (PowerShell) ou BloodHound, puis modifie une GPO de test pour ajouter un script de démarrage. La détection repose sur l'Event ID 5136 (A directory service object was modified) avec un filtre sur les objets GPO (objectClass=groupPolicyContainer) et l'Event ID 4657 (A registry value was modified) pour les modifications via RSAT. **SharpGPOAbuse est l'outil Red Team standard pour tester l'abus GPO dans les exercices Purple Team** — son utilisation dans un environnement de lab AD dupliqué (recommandé plutôt que l'AD de production) permet des tests sans risque d'impact sur les services.

BloodHound : cartographier les chemins d'attaque AD

BloodHound est l'outil de cartographie des relations Active Directory incontournable des exercices Purple Team. Il collecte via son ingesteur SharpHound (ou BloodHound.py pour une collecte sans agent) les relations entre utilisateurs, groupes, ordinateurs, GPO et droits ACL dans l'AD, puis les représente sous forme de graphe de relations où les nœuds sont les objets AD et les arêtes sont les chemins d'attaque. **La requête Cypher "Tous les chemins de Domain Users vers Domain Admins" révèle systématiquement des chemins d'escalade non documentés** dans 95% des environnements AD audités selon les statistiques de l'équipe BloodHound Enterprise — des chemins que les administrateurs ignorent souvent car ils résultent d'accumulations de droits accordés au fil des années pour des raisons opérationnelles.

Dans un exercice Purple Team, BloodHound sert à deux étapes : la phase de planification (identifier les chemins d'attaque les plus critiques à tester en priorité) et la phase de restitution (visualiser les remediation paths et l'impact des corrections appliquées sur la réduction de la surface d'attaque). Pour les RSSI des ETI françaises présentant les résultats Purple Team à leur direction, les graphes BloodHound montrant visuellement le chemin d'une attaque de l'utilisateur lambda au contrôleur de domaine en 3 sauts sont un outil de communication bien plus percutant que des tableaux de CVE.

Scénarios cloud : Azure AD / Entra ID

Les exercices Purple Team ne se limitent plus aux environnements on-premise : les scénarios cloud sont devenus incontournables en 2026, car la majorité des ETI françaises opèrent des environnements hybrides avec Azure AD / Entra ID comme plan de contrôle d'identité central. Les scénarios Purple Team Azure couvrent principalement trois vecteurs : l'abus de Service Principal et d'App Registrations (technique T1098.001), l'exploitation des Managed Identities mal configurées (T1552.005), et la compromission via Conditional Access bypass (T1556).

Le scénario Service Principal abus commence par l'énumération des applications Azure avec des secrets ou des certificats expirés ou trop permissifs via `az ad app list` et AzureHound (la

version Azure de BloodHound), puis tente d'obtenir un token OAuth avec les droits de l'application compromise. **L'outil ROADtools (Research Tool for Azure AD) permet d'analyser la configuration des objets Entra ID et d'identifier les relations de confiance dangereuses** entre applications, Service Principals et groupes, de façon similaire à ce que BloodHound fait pour l'AD on-premise. La détection repose sur les logs Azure AD Sign-in (Service Principal sign-ins) et les Audit Logs Entra ID, intégrés dans Microsoft Sentinel ou dans l'SIEM via le connecteur Azure Monitor.

Scénarios cloud : AWS IAM escalation

Les scénarios AWS Purple Team se concentrent sur l'escalade de privilèges IAM, décrite en détail dans l'article dédié de cette série. Dans un contexte Purple Team, les techniques les plus fréquemment testées sont : l'exploitation d'une fonction Lambda avec une politique IAM trop permissive pour assumer un rôle plus privilégié (T1098.003), la modification de policy inline via `iam:PutRolePolicy` ou `iam:AttachRolePolicy` pour s'attribuer des droits supplémentaires (T1098.001), et l'utilisation de `sts:AssumeRole` pour pivoter vers des rôles cross-account.

L'outil Pacu (framework de pentest AWS open source) contient des modules spécifiques pour tester chacune de ces techniques dans un compte AWS de staging. La détection via CloudTrail repose sur des alertes sur les événements `iam:CreatePolicy`, `iam:AttachRolePolicy`, `iam:PutRolePolicy` et `sts:AssumeRole` avec des sources IP inhabituelles ou des horaires atypiques. **AWS GuardDuty intègre nativement des détections IAM basées sur le machine learning, notamment la détection de "IAMUser/AnomalousBehavior" qui alerte quand un utilisateur IAM effectue des actions inhabituelles par rapport à son profil comportemental historique.**

Métriques Purple Team : MTTD, MTTR et couverture ATT&CK

Un exercice Purple Team sans métriques rigoureuses n'est qu'une démonstration technique sans valeur pour le pilotage de la sécurité. Les trois métriques clés à mesurer pour chaque technique testée sont : le *MTTD* (Mean Time To Detect, délai entre l'exécution de la technique et le déclenchement de l'alerte), le *MTTR* (Mean Time To Respond, délai entre l'alerte et la confirmation de l'investigation par l'analyste SOC), et le taux de couverture ATT&CK (pourcentage des techniques testées avec une alerte déclenchée dans les délais acceptables). Ces métriques permettent de calculer un "Purple Team Score" par tactique ATT&CK, identifiant précisément quelles phases de la kill chain sont bien couvertes (souvent : Initial Access et Execution) et lesquelles sont sous-détectées (souvent : Persistence, Defense Evasion, Lateral Movement).

Les objectifs typiques pour un SOC mature sont un MTTD inférieur à 15 minutes pour les techniques de sévérité haute et inférieur à 60 minutes pour les techniques de sévérité moyenne, et un MTTR inférieur à 2 heures. Pour un SOC en cours de maturation (niveau 2 selon la classification ANSSI), des objectifs intermédiaires de MTTD inférieur à 4 heures sont réalistes. La mesure de ces métriques avant et après chaque vague d'améliorations défensives démontre concrètement le retour sur investissement des exercices Purple Team, un argument précieux pour justifier le budget SOC auprès des directions d'ETI françaises qui perçoivent encore trop souvent la cybersécurité comme un centre de coût sans mesure de valeur claire.

Purple Team AD vs cloud : différences de méthodologie

Les exercices Purple Team on-premise AD et cloud présentent des différences méthodologiques importantes que les équipes doivent anticiper. En AD, les outils sont bien établis (BloodHound, Mimikatz, Impacket, CrackMapExec) et les sources de détection sont connues (Windows Event Log, Sysmon, MDI). En cloud, l'outillage évolue rapidement, les API de chaque provider ont des comportements spécifiques, et les logs de détection sont moins standardisés — CloudTrail AWS,

Activity Log Azure, Cloud Audit Logs GCP ont des structures et des délais d'ingestion différents qui compliquent la corrélation SIEM inter-cloud.

Une différence fondamentale est que les actions cloud génèrent des logs API centralisés et immuables (CloudTrail pour AWS, Activity Log pour Azure) que l'attaquant ne peut pas effacer depuis la console cloud — contrairement aux logs Windows qu'un attaquant avec des droits locaux peut tenter de vider. **Cette propriété des logs cloud rend la phase forensique post-incident plus fiable, mais nécessite que les équipes SOC configurent correctement la rétention et l'archivage de ces logs vers un SIEM** avant l'exercice — un prérequis souvent négligé qui se découvre pendant le Purple Team quand les analystes réalisent que les logs CloudTrail ne sont pas ingérés dans le SIEM depuis 30 jours.

CALDERA : simulation adversariale automatisée

CALDERA est un framework d'émulation adversariale open source développé par MITRE, permettant d'automatiser l'exécution de chaînes d'attaque ATT&CK complètes via un agent déployé sur les machines cibles. Contrairement à Atomic Red Team qui exécute des techniques isolées, CALDERA enchaîne des techniques selon des "adversary profiles" qui émulent le comportement complet d'un groupe APT spécifique — par exemple, un profil APT29 qui enchaîne spearphishing simulation → credential dumping → lateral movement via WMI → collection → exfiltration. Cette simulation de campagne complète teste non seulement la détection des techniques individuelles, mais aussi la capacité du SOC à corréler des alertes multiples pour reconstituer une kill chain complète.

CALDERA s'installe sur un serveur Linux avec pip et supporte des agents multi-plateformes (Windows, Linux, macOS). Pour les exercices Purple Team avancés incluant des scénarios de menace réalistes, CALDERA complète VECTR et Atomic Red Team en ajoutant la dimension temporelle et comportementale des campagnes APT réelles. L'intégration avec ATT&CK Navigator permet de visualiser en temps réel les techniques exécutées pendant la simulation et les alertes correspondantes générées dans le SIEM, créant une boucle de feedback immédiate pour les exercices Purple Team en mode "live replay".

Améliorer les règles de détection après Purple Team

La valeur principale d'un exercice Purple Team n'est pas la liste des techniques non détectées, mais les règles de détection créées ou améliorées en résultat. Pour chaque gap de détection découvert, le Blue Team doit développer une règle de détection spécifique (en Sigma pour la portabilité, puis compilée vers SPL/KQL/EQL selon le SIEM cible), la tester sur des données historiques pour valider qu'elle aurait alerté sur l'exercice réel, et l'ajouter au SIEM avec un seuil et une sévérité calibrés pour minimiser les faux positifs.

Le cycle vertueux du Purple Team est le suivant : exercice → découverte de gaps → développement de règles → re-test pour valider → exercice suivant avec des techniques plus avancées. **Une organisation qui pratique des exercices Purple Team trimestriels peut espérer couvrir 70% des techniques ATT&CK Enterprise pertinentes pour son secteur en 18 mois**, contre une couverture statique de 20-30% typique d'un SOC sans exercices actifs. Cette progression est documentée par VECTR et présentée sous forme de trending metrics au RSSI, démontrant la maturité croissante du SOC dans le temps.

Purple Team et conformité NIS 2 / ISO 27001

Les exercices Purple Team s'inscrivent directement dans les exigences de plusieurs référentiels réglementaires et normatifs auxquels les ETI françaises sont soumises. NIS 2 (article 21) exige des mesures de gestion des risques incluant des tests de sécurité réguliers et la capacité à évaluer l'efficacité des mesures de détection et de réponse. **La documentation VECTR des exercices Purple Team, avec les métriques MTTD/MTTR et les règles de détection déployées, constitue une preuve de conformité NIS 2 directement opposable à l'ANSSI lors d'un contrôle.** ISO 27001:2022 exige dans son annexe A le contrôle 5.36 (Conformity with policies, rules and standards for information security) et le contrôle 8.8 (Management of technical vulnerabilities), auxquels les exercices Purple Team répondent directement.

Pour les organisations cherchant à obtenir ou renouveler une certification ISO 27001, la présentation des résultats Purple Team lors de l'audit de certification (avec les preuves VECTR,

les règles Sigma déployées, et les métriques avant/après) est un élément distinctif qui démontre une approche proactive et mesurable de la gestion des risques de sécurité — bien au-delà de la simple documentation de politiques qui est le minimum requis par le standard.

Planifier son premier exercice Purple Team

Pour une ETI française sans Red Team interne, la mise en place d'un premier exercice Purple Team suit une progression en quatre étapes. Étape 1 : définir le scope et les scénarios (3-5 techniques ATT&CK prioritaires basées sur les groupes APT ciblant le secteur), en utilisant le Navigator ATT&CK filtré par les groupes pertinents. Étape 2 : préparer l'environnement (installer VECTR, configurer un lab AD de test séparé de la production, vérifier que les logs nécessaires sont collectés dans le SIEM). Étape 3 : exécuter l'exercice en binôme — un opérateur exécutant les atomics Atomic Red Team, un analyste SOC monitorant le SIEM en temps réel — en documentant chaque résultat dans VECTR. Étape 4 : développer les règles de détection manquantes et planifier un re-test dans 90 jours.

Le budget pour un premier exercice interne est minimal : Atomic Red Team, VECTR et BloodHound sont open source et gratuits. L'investissement principal est en temps humain (2-3 jours d'analyste SOC et 1-2 jours d'ingénieur sécurité) et en préparation de l'environnement de lab. Pour les ETI sans les ressources internes, des prestataires PRIS labellisés ANSSI proposent des exercices Purple Team packagés en 3-5 jours, incluant un lab AD cloud temporaire, la sélection des scénarios, l'animation de l'exercice et le rapport VECTR avec les recommandations de détection. Ces prestations, facturées entre 8 000 et 25 000 euros selon la complexité, offrent un retour sur investissement mesurable en termes d'amélioration de la couverture de détection et de réduction du MTTD.

Retour terrain : le DCSync que personne ne voyait

Lors d'un exercice Purple Team mené avec une ETI industrielle normande en novembre 2024, l'équipe a découvert une lacune de détection critique : l'attaque DCSync exécutée depuis un compte de service compromis n'alertait pas dans le SIEM, bien que Microsoft Defender for Identity soit déployé. L'investigation a révélé que MDI n'était installé que sur 4 des 7 contrôleurs de domaine du client — les 3 contrôleurs secondaires dans une filiale récemment acquise n'avaient jamais été couverts par MDI. L'attaquant aurait pu exécuter le DCSync en ciblant spécifiquement l'un de ces contrôleurs non monitorés, extrayant tous les hashes NTLM du domaine sans déclencher la moindre alerte. Sans l'exercice Purple Team, ce blind spot serait resté invisible. Le déploiement MDI sur les contrôleurs manquants, réalisé la semaine suivante, a pris 4 heures — mais n'aurait jamais été priorisé sans la découverte empirique de la lacune lors de l'exercice.

Questions fréquentes sur les exercices Purple Team

Quelle est la vraie différence entre un Red Team et un Purple Team ?

Un exercice Red Team traditionnel est cloisonné : le Red Team attaque sans informer le Blue Team, et les résultats sont partagés à la fin dans un rapport. Un exercice Purple Team est collaboratif : Red et Blue travaillent ensemble, le Blue Team sait quand le Red Team exécute une technique et peut observer en temps réel si l'alerte se déclenche. Le Purple Team est plus rapide pour améliorer les capacités de détection, car le feedback est immédiat et les règles sont créées pendant l'exercice. Le Red Team reste utile pour tester la réaction complète et non informée du SOC face à une attaque réelle.

À quelle fréquence pratiquer des exercices Purple Team ?

La fréquence minimale recommandée par l'ANSSI pour les entités NIS 2 est deux exercices par an. Pour un SOC en cours de maturation, des exercices trimestriels permettent une progression plus rapide de la couverture de détection. Chaque exercice doit couvrir 5-15 techniques ATT&CK nouvelles (non testées lors des exercices précédents) tout en re-testant les techniques des exercices antérieurs pour vérifier que les règles de détection déployées restent efficaces après les mises à jour de l'EDR et du SIEM.

Les outils Red Team utilisés en Purple Team sont-ils légaux ?

Oui, à condition que leur utilisation soit strictement limitée à des environnements de lab ou à des systèmes pour lesquels un mandat écrit d'autorisation de test a été signé par le responsable légal de l'organisation. En France, l'article 323-1 du Code Pénal (accès frauduleux à un système informatique) s'applique même aux tests internes sans mandat écrit. Tous les exercices Purple Team doivent être précédés d'une convention de test signée définissant le scope autorisé, les heures d'exécution, et les contacts d'escalade en cas d'impact non intentionnel sur la production.

Comparatif des outils Purple Team 2026

Outil	Usage principal	Licence	Intégration ATT&CK	Complexité déploiement
`Atomic Red Team`	Tests unitaires techniques ATT&CK	MIT (open source)	Native (mapping par technique)	Faible (scripts PS/ Bash)
`VECTR`	Gestion et reporting exercices	Freemium (Community free)	Native (heatmap Navigator)	Moyenne (Docker)
`BloodHound CE`	Cartographie relations AD/Azure	Apache 2.0 (open source)	Via requêtes Cypher	Moyenne (Docker+Neo4j)
`CALDERA`	Émulation campagnes APT complètes	Apache 2.0 (MITRE)	Native (profils adversaires)	Élevée (server+agents)
`Pacu`	Pentest AWS IAM et services	BSD (open source)	Partielle (modules ATT&CK)	Faible (pip install)
`ROADtools`	Énumération et analyse Entra ID	MIT (open source)	Indirecte (via résultats)	Faible (pip install)
`Stratus Red Team`	Attaques cloud AWS/ Azure/GCP	Apache 2.0 (DataDog)	Native (techniques cloud)	Faible (binaire Go)

Opinion : le cloisonnement Red/Blue coûte cher aux organisations françaises

La plupart des organisations françaises qui pratiquent encore des Red Team cloisonnés annuels dépensent entre 30 000 et 80 000 euros pour des rapports qui resteront dans un tiroir. Le modèle est fondamentalement cassé : le Red Team part pendant deux semaines, produit 150 pages de vulnérabilités, et le Blue Team qui reçoit le rapport n'a ni le temps ni les ressources pour en implémenter le dixième. Trois exercices Purple Team de deux jours chacun, pour un budget comparable, produisent systématiquement plus de valeur opérationnelle mesurable — des règles de détection déployées, des métriques MTTD améliorées, des blind spots comblés. L'industrie française de la sécurité commence à l'admettre, mais le modèle Red Team annuel reste dominant car il est plus facile à vendre et à budgéter. La transition vers le Purple Team continu est un changement culturel autant qu'un changement de méthode.

À RETENIR

Points clés à retenir

Le Purple Team combine Red et Blue en temps réel pour produire des améliorations de détection immédiatement opérationnelles

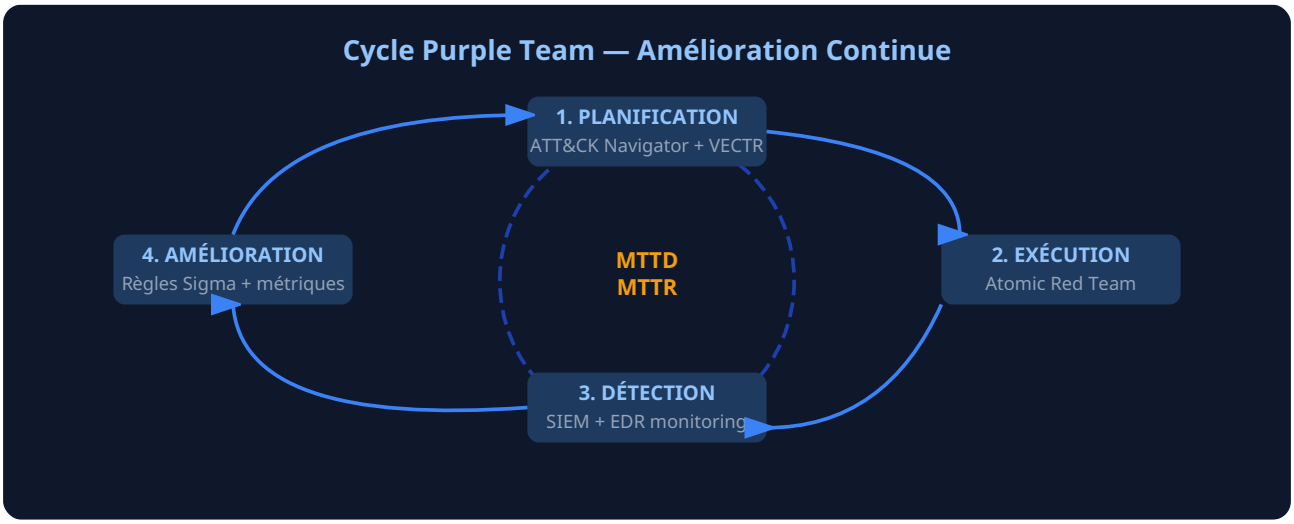
MITRE ATT&CK fournit le référentiel commun pour planifier les scénarios et mesurer la couverture de détection

Atomic Red Team + VECTR + BloodHound forment la stack open source minimale pour démarrer un programme Purple Team

MTTD et MTTR par tactique ATT&CK sont les métriques clés pour piloter la maturité SOC dans le temps

Les scénarios AD (Kerberoasting, DCSync, GPO abuse) et cloud (IAM escalation, Service Principal abuse) sont les plus critiques en 2026

NIS 2 et ISO 27001:2022 valorisent directement la documentation VECTR des exercices comme preuve de conformité



Ressources et formation Purple Team

Pour monter en compétence sur le Purple Team, plusieurs ressources de référence sont disponibles. **La certification PNPT (Practical Network Penetration Tester) de TCM Security intègre des modules Purple Team pratiques** directement applicables dans un contexte ETI. La formation "ATT&CK for Purple Teamers" de MITRE elle-même (disponible en ligne gratuitement) est le point de départ incontournable pour comprendre l'utilisation d'ATT&CK dans un contexte collaboratif. En France, le CLUSIF et Hexatrust proposent des groupes de travail Purple Team où les RSSI d'ETI françaises partagent leurs retours d'expérience — un réseau précieux pour éviter de réinventer la roue dans l'implémentation de son premier programme Purple Team.

Pour les équipes souhaitant approfondir la partie cloud, Stratus Red Team (DataDog) et Pacu (Rhino Security Labs) constituent les références open source pour les scénarios AWS et Azure. Les articles connexes de cette série — notamment celui sur l'escalade IAM cloud et celui sur le pentest Kubernetes — détaillent les techniques et détections spécifiques à chaque environnement. Pour l'Active Directory, le guide Purple Team AD et les ressources RBAC complètent cette vue d'ensemble méthodologique.

Intégration de la Threat Intelligence dans les scénarios Purple Team

Un exercice Purple Team générique testant des techniques ATT&CK aléatoires est moins efficace qu'un exercice calibré sur les TTP réelles des groupes APT qui ciblent effectivement le secteur de l'organisation. L'intégration de la Threat Intelligence dans la planification des scénarios Purple Team permet de simuler fidèlement le comportement des attaquants les plus probables et de prioriser les gaps de détection les plus dangereux. Pour une ETI française du secteur de l'énergie, les TTP d'APT28 (Russie, ciblage énergie et infrastructure critique) et de Volt Typhoon (Chine, ciblage infrastructure OT/ICS) sont plus pertinentes que les TTP génériques d'un groupe de cybercriminalité financière.

La mise en œuvre pratique consiste à utiliser le Navigator ATT&CK pour créer une heatmap des techniques utilisées par les groupes APT identifiés comme risque prioritaire (via les rapports ANSSI, les bulletins CERT-FR et les publications CTI de Sekoia.io ou Mandiant pour le contexte français), puis à sélectionner dans cette heatmap les techniques non détectées actuellement par le SOC pour les inclure dans l'exercice. **Cette approche "threat-informed defense", formalisée par le MITRE dans son cadre D3FEND, garantit que les ressources limitées des équipes SOC sont focalisées sur les techniques réellement utilisées par les attaquants pertinents**, plutôt que dispersées sur l'ensemble des 500+ techniques ATT&CK dont beaucoup ne sont jamais observées dans des attaques réelles contre des cibles françaises.

Purple Team pour tuner l'EDR : réduire les faux positifs

Un bénéfice souvent sous-estimé des exercices Purple Team est l'amélioration du tuning de l'EDR (Endpoint Detection and Response). Dans la plupart des SOC, l'EDR génère un volume de fausses alertes qui conduit les analystes à désactiver ou abaisser la priorité de certaines règles pour réduire le bruit — ce qui crée des blind spots non documentés. Le Purple Team, en exécutant des techniques ATT&CK connues et en observant les résultats dans l'EDR, permet d'identifier avec précision quelles règles EDR génèrent des faux positifs (et donc ont été incorrectement désactivées) et quelles techniques réelles ne déclenchent aucune alerte (gap de détection).

L'exercice Purple Team devient ainsi une session de tuning collaboratif : pour chaque technique testée, si l'EDR génère une alerte légitime sur l'atomic, la règle est confirmée comme fonctionnelle. Si l'EDR ne génère pas d'alerte, le Blue Team peut ajuster les paramètres de détection (agressivité du moteur comportemental, exclusions de processus, seuils d'alerting) immédiatement pendant l'exercice et retester la technique pour valider l'amélioration. Cette boucle de feedback immédiate, impossible dans un modèle Red Team cloisonné, justifie à elle seule le passage au Purple Team pour les organisations disposant d'un EDR mais se plaignant de son efficacité ou de son ratio signal/bruit. **Des sessions Purple Team de tuning EDR trimestrielles permettent d'atteindre des ratios de vrais positifs supérieurs à 85%**, contre des ratios typiques de 40-60% pour des EDR déployés sans exercices de validation réguliers.

Communiquer les résultats Purple Team à la direction

La communication des résultats d'un exercice Purple Team à des audiences non techniques — COMEX, conseil d'administration, DSI — est un exercice délicat qui conditionne l'obtention des budgets nécessaires aux améliorations identifiées. La clé est de traduire les métriques techniques (MTTD en secondes, couverture ATT&CK en pourcentage) en risques métier compréhensibles : "Si un attaquant compromise un compte utilisateur et tente d'extraire tous les mots de passe du domaine Active Directory, notre équipe SOC détecte cette activité en moyenne en 2h30 — or une extraction complète prend moins de 5 minutes. Cela signifie qu'un attaquant aurait le temps d'exfiltrer l'ensemble des credentials de nos 500 employés avant qu'une alerte soit levée."

Ce type de traduction concrète, ancrée dans les scénarios réels testés lors de l'exercice, est bien plus percutante que les slides ATT&CK heatmap que les RSSI présentent parfois à des directions qui n'ont aucun contexte pour les interpréter. VECTR génère des rapports exécutifs incluant des indicateurs de risque normalisés qui peuvent être adaptés pour une présentation direction. **La comparaison avant/après — "lors de notre exercice de janvier 2025, nous détections 35% des techniques testées ; après 6 mois d'améliorations, nous détectons maintenant 67%" — est l'argument le plus convaincant pour démontrer la valeur des investissements en capacités SOC** et obtenir les ressources pour continuer le programme Purple Team.

Purple Team avec un MSSP : bonnes pratiques contractuelles

Pour les ETI françaises externalisant leur SOC à un MSSP (Managed Security Service Provider), les exercices Purple Team présentent une dimension contractuelle spécifique : le MSSP est à la fois le Blue Team (qui doit détecter les techniques testées) et le prestataire évalué par l'exercice. Cette situation peut créer des résistances de la part du MSSP, qui voit dans le Purple Team un audit de sa propre performance plutôt qu'un outil d'amélioration collaborative. La rédaction du contrat MSSP doit anticiper ce point en incluant des clauses Purple Team explicites : droit du client à conduire ou faire conduire des exercices Purple Team, obligation du MSSP de participer

activement à la session de résultats, et SLA de correction des gaps de détection identifiés (règles Sigma déployées dans X semaines).

Les MSSP les plus matures, notamment ceux labellisés PRIS par l'ANSSI, proposent désormais des exercices Purple Team comme prestation incluse dans leurs contrats SOC-as-a-Service, reconnaissant que ces exercices améliorent leur propre niveau de service et réduisent les incidents non détectés qui pourraient engager leur responsabilité contractuelle. La sélection d'un MSSP qui accepte et encourage les exercices Purple Team est désormais un critère de qualification important pour les ETI françaises soumises à NIS 2, car elle garantit une posture de détection dynamique et mesurée plutôt qu'une couverture statique jamais challengée.

Scénarios de mouvement latéral : Pass-the-Hash et Over-Pass-the-Hash

Le mouvement latéral est la phase de l'attaque où la détection est le plus souvent défaillante dans les SOC français : les attaquants se déplacent entre machines en utilisant des credentials légitimes (volés via credential dumping) et des protocoles Windows natifs (SMB, WMI, RDP, WinRM), ce qui rend leur trafic quasiment identique à une activité administrative normale. Le Pass-the-Hash (PtH) exploite les hashes NTLM pour s'authentifier sans connaître le mot de passe en clair, tandis que le Over-Pass-the-Hash (OPtH) convertit un hash NTLM en ticket Kerberos TGT, permettant de s'authentifier via Kerberos avec un hash — une technique plus difficile à détecter car Kerberos est généralement moins surveillé que NTLM.

Dans le scénario Purple Team Pass-the-Hash, le Red Team exécute `sekurlsa::pth /user:admin /domain:corp.fr /ntlm:HASH` via Mimikatz pour ouvrir un shell sous l'identité de l'administrateur cible, puis utilise `psexec.py` (Impacket) pour se connecter à un serveur. La détection repose sur l'Event ID 4624 (Logon Success) avec un Logon Type 3 (Network) et un package d'authentification NtLmSsp depuis une source inhabituelle, combiné à l'Event ID 4776 (NTLM Authentication) en corrélation avec des connexions vers plusieurs machines en moins de 5 minutes. **Microsoft recommande la désactivation complète de l'authentification NTLM en faveur de Kerberos pour éliminer les vecteurs PtH**, mais cette migration reste complexe dans les environnements avec des applications legacy qui dépendent encore de NTLM — un état de fait dans la majorité des ETI françaises avec des systèmes hérités.

Scénarios de persistance : Golden Ticket et Silver Ticket

La persistance via Kerberos forged tickets est l'une des techniques les plus dangereuses d'un attaquant ayant compromis Active Directory : le Golden Ticket exploite le hash NTLM du compte KRBTGT (qui signe tous les TGT du domaine) pour créer un TGT arbitraire valide 10 ans pour n'importe quel compte du domaine. Une fois créé, ce ticket permet à l'attaquant de se réauthentifier au domaine indéfiniment, même si tous les mots de passe sont changés (car le ticket est auto-signé par la clé KRBTGT). Le Silver Ticket, moins puissant mais plus discret, forge un TGS pour un service spécifique en utilisant le hash NTLM du compte de service cible.

Le scénario Purple Team Golden Ticket teste la détection d'un ticket Kerberos présentant des anomalies de structure : durée de vie anormale (un TGT légitime dure 10 heures par défaut, pas 10 ans), absence de pre-authentication (flag PREAUTH non requis), ou utilisation d'un compte qui n'existe pas dans l'AD (technique de camouflage avancée). **Microsoft Defender for Identity détecte les Golden Tickets via la comparaison des caractéristiques des tickets présentés avec les politiques Kerberos du domaine**, mais cette détection peut être contournée par des attaquants sophistiqués qui configurent précisément les paramètres du Golden Ticket pour correspondre aux valeurs légitimes du domaine. La rotation du secret KRBTGT (deux fois, pour invalider tous les tickets existants) est la seule remédiation complète après une compromission Golden Ticket confirmée.

Les équipes SOC qui pratiquent le Purple Team de manière régulière développent une culture de remise en question de leurs hypothèses de détection, évitant le biais de confirmation qui consiste à supposer que parce qu'une règle est déployée dans le SIEM, elle détecte effectivement les attaques pour lesquelles elle a été conçue — une hypothèse rarement vérifiée dans les organisations sans programme de validation actif.

Conclusion

Ce sujet s'inscrit dans un contexte de menaces en constante évolution. La meilleure protection combine veille active, audits réguliers et sécurité by design. Pour approfondir ou évaluer votre exposition, consultez nos experts.

Vous souhaitez en savoir plus ou évaluer votre exposition ?

Contacter nos experts ou contactez-nous directement.