AYI NEDJIMI Consultants

Purple Team : Collaboration entre SOC et Red Team Guide

Catégorie : SOC et Detection Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide Purple Team en 2026 : méthodologie de collaboration entre SOC et Red Team, exercices de validation des détections et amélioration continue de.

Résumé exécutif

Ce guide détaille la méthodologie Purple Team en 2026 : principes fondamentaux de collaboration transparente entre équipes offensives et défensives, planification et exécution d'exercices structurés autour du framework MITRE ATT&CK, validation des détections SIEM et EDR en conditions réalistes, et amélioration continue et mesurable de la posture de sécurité du SOC. Contrairement au Red Team classique où l'attaquant opère en secret et livre un rapport final, le Purple Team maximise l'apprentissage mutuel en testant les détections en temps réel et en corrigeant immédiatement les lacunes identifiées. Nous couvrons les quatre phases d'un exercice réussi (cadrage, préparation, exécution, capitalisation), les techniques prioritaires à tester, les outils d'émulation d'adversaire comme Atomic Red Team et Caldera, et les métriques pour démontrer le ROI du programme Purple Team à votre direction.

L'approche **Purple Team** représente une évolution majeure dans la manière dont les organisations évaluent et améliorent leurs capacités de détection et de réponse. Contrairement au modèle traditionnel où la Red Team attaque en secret et la Blue Team défend à l'aveugle, le Purple Team instaure une **collaboration structurée** entre les deux équipes pour maximiser l'apprentissage mutuel et l'amélioration concrète des détections. En 2026, cette approche est devenue indispensable face à la réalité suivante : la majorité des SOC ne testent jamais réellement leurs règles de détection contre des attaques réalistes, fonctionnant avec une confiance aveugle dans des détections qui n'ont jamais été validées en conditions opérationnelles. Un exercice Purple Team typique révèle que 30 à 50% des règles SIEM censées détecter une technique d'attaque spécifique échouent réellement face à une exécution réaliste de cette technique. Les raisons sont multiples : sources de données manquantes, seuils mal calibrés, variations de la technique non couvertes par la règle, ou simplement une logique de détection erronée qui n'a jamais été testée. Ce guide vous fournit une méthodologie complète pour planifier, exécuter et capitaliser sur les exercices Purple Team afin de transformer votre SOC d'un dispositif théorique en une machine de détection dont l'efficacité est prouvée et continuellement améliorée par la confrontation avec des attaques réalistes.

Retour d'expérience : Un programme Purple Team trimestriel sur 12 mois pour un SOC financier a révélé que sur 45 techniques ATT&CK testées, seulement 62% étaient détectées lors du premier exercice. Après 4 cycles d'exercices et d'améliorations, le taux de détection est monté à 89%. Les améliorations les plus significatives ont concerné la détection du mouvement latéral (de 40% à 85%) et l'escalade de privilèges (de 55% à 92%), grâce à l'ajout de sources de données Sysmon et au tuning des règles basé sur les observations des exercices.

Principes fondamentaux du Purple Team

Le Purple Team repose sur plusieurs **principes fondamentaux** qui le distinguent des tests de pénétration classiques et des exercices Red Team traditionnels. Le premier principe est la *transparence opérationnelle* : contrairement au Red Team où les attaquants opèrent en secret, le Purple Team est un exercice collaboratif où les deux équipes partagent les informations en temps réel. La Red Team annonce les techniques qu'elle va exécuter, les exécute, et la Blue Team vérifie immédiatement si la détection a fonctionné. Si elle n'a pas fonctionné, les deux équipes analysent ensemble pourquoi et développent ou corrigent la détection sur place. Le deuxième principe est l'**orientation résultats** : l'objectif n'est pas de prouver que l'attaquant peut compromettre l'entreprise (c'est presque toujours le cas) mais d'améliorer concrètement les capacités de détection. Chaque technique testée doit se terminer par une détection validée ou un plan d'action documenté pour combler la lacune identifiée.

Le troisième principe est la **structuration ATT&CK** : les exercices sont organisés autour du framework MITRE ATT&CK qui fournit le vocabulaire commun et la matrice de couverture. Chaque technique testée est mappée à son identifiant ATT&CK, permettant de maintenir une vue précise de la couverture de détection validée. Le quatrième principe est l'**itération continue** : le Purple Team n'est pas un événement ponctuel mais un programme régulier (idéalement trimestriel) qui couvre progressivement l'ensemble des techniques pertinentes pour le profil de menace de l'organisation. Le cinquième principe est la **documentation exhaustive** : chaque exercice produit un rapport détaillé documentant les techniques testées, les résultats de détection, les lacunes identifiées et les actions correctives mises en œuvre. Pour comprendre les techniques offensives que le Purple Team doit tester, consultez nos articles sur les attaques Golden Ticket et le DCSync.

Comment planifier un exercice Purple Team ?

La planification d'un exercice Purple Team suit un processus structuré en **quatre phases**. La **phase 1 (Cadrage)** définit les objectifs, le périmètre et les techniques à tester. Identifiez les threat actors les plus pertinents pour votre secteur via les rapports CTI et sélectionnez 10 à 15 techniques ATT&CK de leur arsenal. Priorisez les techniques que votre SOC prétend détecter mais qui n'ont jamais été validées. Définissez les systèmes cibles (qui doivent être représentatifs de la production), les créneaux horaires et les conditions de test (heures ouvrées vs hors heures, avec ou sans préavis aux analystes L1). La **phase 2 (Préparation)** est critique. L'équipe offensive prépare les outils et les procédures d'exécution pour chaque technique, en s'assurant qu'ils sont réalistes mais contrôlés (pas de destruction de données, pas de déni de service). L'équipe défensive prépare les dashboards de monitoring, vérifie que les sources de données sont opérationnelles et documente les détections attendues pour chaque technique.

La **phase 3 (Exécution)** est le cœur de l'exercice. Pour chaque technique, le processus est le suivant : l'opérateur Red Team annonce la technique, l'exécute sur le système cible, et marque le timestamp. L'équipe Blue Team vérifie dans le SIEM et les outils de détection si une alerte a été générée. Si oui, on valide la détection et on documente les détails (temps de détection, qualité de l'alerte, informations contextuelles). Si non, les deux équipes analysent ensemble la cause de l'échec : source de données manquante, règle absente, règle mal configurée, ou technique

exécutée d'une manière non couverte par la règle. L'équipe développe ou corrige la détection en temps réel quand c'est possible. La **phase 4 (Capitalisation)** produit le rapport d'exercice, met à jour la matrice de couverture ATT&CK et crée les tickets d'amélioration pour les détections qui n'ont pas pu être corrigées pendant l'exercice. Utilisez des outils d'émulation comme **Atomic Red Team** ou **Caldera** pour standardiser l'exécution des techniques. Le standard Sigma facilite l'écriture rapide de nouvelles règles pendant l'exercice. Consultez notre article sur l'évasion EDR/XDR pour des techniques avancées à inclure dans vos exercices.

Phase	Durée	Activités clés	Livrables
Cadrage	1-2 semaines	Sélection techniques, périmètre, planning	Plan d'exercice, matrice techniques
Préparation	1-2 semaines	Outils, procédures, vérification sources	Playbooks d'exécution, checklists
Exécution	2-5 jours	Tests techniques, validation détections	Résultats bruts, corrections en direct
Capitalisation	1 semaine	Rapport, mise à jour couverture, actions	Rapport final, plan d'amélioration

Pourquoi le Purple Team est-il supérieur au Red Team classique ?

Le Red Team classique et le Purple Team ont des **objectifs complémentaires mais distincts**. Le Red Team classique simule une attaque réaliste en conditions d'opacité pour évaluer la posture de sécurité globale de l'organisation. Son principal livrable est un rapport qui démontre ce qu'un attaquant motivé peut accomplir. Le problème est que ce rapport arrive souvent après coup : l'attaque est terminée, et le SOC n'a appris que de manière passive, en lisant un rapport plutôt qu'en améliorant ses détections en temps réel. Le Purple Team maximise l'**apprentissage et l'amélioration concrète** en transformant chaque échec de détection en une opportunité d'amélioration immédiate. Là où le Red Team produit une liste de vulnérabilités et de lacunes, le Purple Team produit des détections nouvelles ou corrigées et validées. Le ROI du Purple Team est directement mesurable : augmentation du pourcentage de techniques ATT&CK détectées, réduction du MTTD pour les techniques testées, et diminution des angles morts de détection.

L'approche Purple Team présente aussi des **bénéfices humains** significatifs. Elle favorise la compréhension mutuelle entre les équipes offensives et défensives, réduit les tensions qui existent parfois entre Red et Blue Teams, et développe les compétences des analystes SOC qui voient concrètement comment les techniques d'attaque se manifestent dans les logs et les alertes. Les analystes qui ont participé à des exercices Purple Team sont significativement plus efficaces dans le triage et l'investigation des incidents réels car ils reconnaissent les patterns qu'ils ont observés pendant les exercices. Pour les techniques d'attaque Active Directory à tester en Purple Team, consultez nos articles sur le Kerberos et les attaques ADCS. Les retours d'expérience de l'ANSSI confirment l'efficacité de cette approche collaborative.

Mon avis : Si vous ne devez investir que dans un seul type d'exercice de sécurité, choisissez le Purple Team plutôt que le pentest ou le Red Team classique. Le Purple Team produit un ROI immédiat et mesurable sous forme de détections améliorées, là où le pentest produit un rapport qui finit souvent dans un tiroir. Le seul prérequis est un niveau de maturité minimal du SOC : il faut au moins avoir un SIEM opérationnel avec des règles de détection en place pour que le Purple Team ait quelque chose à tester et à améliorer.

Quelles techniques prioriser pour les premiers exercices ?

Les premiers exercices Purple Team doivent cibler les **techniques les plus fréquemment utilisées** dans les attaques réelles et les plus critiques pour votre environnement. Pour les environnements Windows et Active Directory (la majorité des entreprises), les techniques prioritaires incluent : le *credential dumping* (extraction de mots de passe depuis la mémoire de lsass.exe via Mimikatz ou équivalents), le **mouvement latéral via PsExec et WMI** (exécution de commandes sur des systèmes distants), l'**escalade de privilèges via Kerberoasting et ASREPRoasting** (extraction et cracking de tickets Kerberos), la **persistence via tâches planifiées et clés de registre** (maintien d'accès après redémarrage), et l'**exfiltration via DNS et HTTPS** (transfert de données vers l'extérieur). Pour les environnements cloud, ajoutez la **compromission de tokens d'accès**, l'**abus de permissions IAM** et la **création de règles de transfert email**. Consultez notre article sur le relay NTLM pour une technique avancée à inclure dans vos exercices intermédiaires et notre guide sur les abus d'ACL pour les scénarios d'escalade de privilèges furtifs.

Mesurer l'impact du programme Purple Team

La mesure de l'impact du programme Purple Team repose sur des **indicateurs objectifs**. Le premier indicateur est l'**évolution de la couverture ATT&CK validée** : le pourcentage de techniques ATT&CK que le SOC détecte réellement (non théoriquement) doit augmenter après chaque exercice. Maintenez une matrice ATT&CK avec trois statuts pour chaque technique : non couverte (pas de règle), couverte (règle en place mais non testée), et validée (règle testée avec succès lors du dernier exercice). L'objectif est d'augmenter le pourcentage de techniques validées. Le deuxième indicateur est le **nombre de nouvelles détections créées** ou de détections existantes corrigées suite à chaque exercice. Le troisième indicateur est l'**amélioration du MTTD** pour les techniques testées : mesurez le temps entre l'exécution de la technique et la détection par le SOC, et suivez son évolution entre les exercices. Le quatrième indicateur est le **nombre de techniques non détectées** qui diminue au fil des exercices. Un programme Purple Team efficace devrait réduire le taux de techniques non détectées de 10 à 20 points de pourcentage par exercice trimestriel. Pour le suivi des métriques, consultez notre article sur les solutions EDR/XDR qui offrent des capacités de validation de détection intégrées.

À retenir : Le Purple Team est la méthodologie la plus efficace pour valider et améliorer concrètement les capacités de détection du SOC. Basé sur la collaboration transparente entre équipes offensives et défensives, il produit un ROI immédiat sous forme de détections nouvelles

ou corrigées. Commencez par un exercice ciblant 10-15 techniques ATT&CK prioritaires, mesurez le taux de détection initial, améliorez les détections défaillantes et répétez trimestriellement pour une amélioration continue et mesurable.

Quand avez-vous testé pour la dernière fois si vos règles SIEM détectent réellement les techniques d'attaque qu'elles prétendent couvrir ?

Sources et références : MITRE ATT&CK · MITRE CAR

Perspectives et prochaines étapes

L'avenir du Purple Team sera facilité par des plateformes d'émulation d'adversaire de plus en plus automatisées, capables d'exécuter des scénarios complets de techniques ATT&CK et de vérifier automatiquement les détections SIEM. L'IA va progressivement assister la génération de nouvelles variantes de techniques pour tester la robustesse des détections. Pour lancer votre programme Purple Team, identifiez un partenaire ou une équipe interne avec des compétences offensives, sélectionnez les 10 techniques ATT&CK les plus pertinentes pour votre profil de menace, et planifiez votre premier exercice de 2 jours. Chaque exercice vous rapprochera d'un SOC dont l'efficacité est prouvée et non supposée.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr