Tâche : KPIs Purple Teaming

Elfaiza Elkarie

Mai 2025

1 Cadre méthodologique d'évaluation des scénarios Purple Team

1.1 Objectifs de l'évaluation

Dans une approche organisée de l'équipe Purple, l'instauration d'un système d'évaluation pour chaque scénario est essentielle. Celui-ci permet de transformer des tests techniques ponctuels en éléments quantifiables, traçables et exploitables, contribuant à l'évaluation de la maturité du SOC.

Les objectifs principaux de ce système sont les suivants :

- Proposer un cadre d'analyse standardisé pour chaque scénario Purple Team, assurant l'homogénéité des évaluations.
- Évaluer la performance de la Blue Team en matière de détection, d'analyse et de réponse, à travers des indicateurs concrets.
- Garantir une traçabilité rigoureuse des tests : contexte, environnement, commandes, payloads, résultats observés.
- Centraliser les retours des équipes Red et Blue dans un format structuré facilitant l'analyse rétrospective.
- Alimenter la boucle d'amélioration continue du SOC par des données fiables et exploitables.

Cet outil aide à évaluer de manière objective le degré de maturité du SOC en termes de ses aptitudes techniques, organisationnelles et analytiques.

1.2 Présentation de la template utilisée

Dans le cadre de ce projet, une fiche standardisée a été conçue et mise en place pour organiser cette évaluation. Ce document, élaboré en format Excel, facilite la consolidation de toutes les données essentielles relatives à un scénario Purple Team spécifique.

Elle représente une entité d'étude complète, qui soutient la mise en œuvre du test de manière intégrale : de la préparation à l'exécution, y compris l'analyse des résultats et les conseils. Chaque équipe (Rouge, Bleue, Violette) dispose des champs nécessaires pour accomplir sa fonction.

Voici la configuration de la fiche :

- **Données générales** : cette partie définit le contexte, en précisant la technique MITRE ATT&CK visée, le niveau d'évasion employé et la catégorie de test.
- **Exécution de l'équipe rouge** : le document comprend les objectifs du test, les commandes exécutées, les outils employés et les configurations d'environnement.
- **Résultats de l'équipe bleue** : les alertes détectées, les journaux observés et les interventions du SOC sont consignés ici.
- **Indicateurs de performance** : cette partie examine les délais de détection, la pertinence des alertes, ainsi que les actions qui ont pu être omises.
- **Suggestions / Optimisations** : des mesures correctives sont suggérées et leur degré d'urgence est établi.
- **État de validation** : cette section permet de finaliser le test (approuvé / partiel / à refaire) et de garder un historique.

L'ensemble de cette template est conçu pour permettre une analyse homogène, traçable et alignée sur les exigences de maturité SOC.

1.3 Justification des champs et indicateurs

Chaque champ intégré dans la fiche n'a pas été choisi au hasard : il reflète une dimension clé de l'analyse *Purple Team* et contribue à la mesure de la maturité SOC.

Champ de la fiche	**Objectif métier**
Technique MITRE	Assure un alignement avec le framework ATT&CK
Commandes *Red Team*	Garantit la reproductibilité et la traçabilité des actions
Logs visibles	Permet d'évaluer la visibilité offerte par les outils de sécurité
Détection *SIEM* / alertes	Mesure la performance des cas d'usage et des corrélations
Temps de réponse	Indique la réactivité des processus de réponse SOC
Niveau d'évasion	Teste la robustesse du SOC face à différents niveaux d'adversaires
Recommandations proposées / suivies	Alimente la boucle d'amélioration continue
Statut du test	Assure le suivi de l'état des campagnes de test

TABLE 1 – Justification métier des champs de la fiche Purple Team

L'ensemble de ces champs permet une évaluation complète, aussi bien technique qu'organisationnelle, pour soutenir la montée en maturité.

1.4 Intégration dans le processus d'évaluation global

Les fiches complétées pour chaque scénario s'insèrent de manière fluide dans le processus global d'évaluation du SOC. Elles ne sont pas des composants isolés, mais contribuent à nourrir trois fondements complémentaires :

Le dossier des tests : chaque fiche constitue un justificatif de réalisation, mais également un fondement pour les contrôles internes, les examens post-incident et les évaluations par des tiers.

Le tableau de bord unifié Purple Team : en rassemblant les données provenant des fiches (techniques traitées, taux de détection, temps de réponse), on peut élaborer une perspective globale dynamique de la situation réelle de défense du SOC.

Le modèle de maturité SOC : les informations tirées des fiches peuvent être associées aux quatre axes d'évaluation du SOC spécifiés dans la Partie IV :

- **Technologie** : visibilité des logs, couverture MITRE, détection automatisée.
- **Processus** : pertinence des réponses, respect des procédures, documentation.
- **Indicateurs** : KPIs, taux de couverture, évolution dans le temps.
- **Personnel** : coordination inter-équipes, compétence technique, retour d'expérience.

Cette incorporation assure que les simulations de Purple Team ne se limitent pas à des exercices théoriques, mais constituent des outils tangibles pour améliorer la maturité du centre opérationnel de sécurité.

1.5 Métriques d'évaluation (KPIs) pour les exercices Purple Team

Pour enrichir cette démarche qualitative et méthodologique, un ensemble d'indicateurs d'évaluation quantitatifs a été établi. Ces indicateurs clés de performance (KPIs) fournissent une évaluation objective de l'efficacité du SOC face aux attaques simulées.

Objectifs des Indicateurs Clés de Performance :

- Évaluer la performance effective dans la détection des événements nuisibles.
- Évaluer la réactivité et la capacité de réponse des équipes du Centre Opérationnel de Sécurité.
- Détecter les zones non visibles ou les manques de réponse.
- Mesurer l'étendue effective des techniques MITRE ATT&CK couvertes.
- Gérer l'amélioration continue à l'aide de mesures précises et comparables.

Catégories de KPIs :

- **Couverture** : examine si les méthodes et stratégies essentielles ont été correctement testées.
- **Détection** : évalue la clarté, les corrélations et la performance des alertes.
- **Réponse** : mesure la rapidité et l'efficacité des opérations SOC.
- **Collaboration** : évalue la qualité de la documentation, des rapports et du suivi.

1.6 SYSTÈME DE NOTATION PURPLE TEAMING

1.6.1 Objectif

Le système permet d'évaluer la performance d'un SOC à partir des scénarios Purple Team exécutés, et de produire un score de maturité de 0 à 5, à partir de données factuelles et vérifiables. Il repose sur des indicateurs clés (KPIs) répartis en 4 grandes catégories.

1.6.2 AXES D'ÉVALUATION

Axe	**Ce qu'on mesure**	**Pourquoi c'est important**
Couverture	Est-ce qu'on a bien testé les bonnes choses ?	Cela montre la portée des tests
Détection	Est-ce que le SOC voit les attaques ?	La visibilité est la base
Réponse	Est-ce que le SOC agit vite et bien ?	Réduire l'impact de l'attaque
Collaboration	Est-ce que tout est documenté et suivi ?	Nécessaire pour s'améliorer

TABLE 2 – Résumé simplifié des axes évalués dans l'analyse Purple Team

Catégorie	**KPI**	**Méthode de mesure (Formule)**	**Explication et objectif visé**
Couverture	% Techniques MITRE testées	Nb techniques testées / Nb techniques cibles	Permet de mesurer la couverture des vecteurs d'attaque en fonction des objectifs définis. Plus le pourcentage est élevé, plus le test est représentatif.
	Tactiques couvertes	Nb tactiques couvertes / 14 (tactiques MITRE ATT&CK)	Indique l'étendue de l'évaluation sur le cycle complet de l'attaque (Initial Access à Impact). Permet une cartographie stratégique des tests.
Détection	Taux de détection brute	Nb événements détectés / Nb actions exécutées par la Red Team	Mesure la visibilité technique du SOC : capacité à enregistrer des événements malveillants dans les logs ou SIEM.
	Temps moyen de détection (MTTD)	Moyenne(Heure détection – Heure attaque)	Évalue la réactivité technique des systèmes et analystes. Plus le MTTD est court, plus la menace est détectée rapidement.
	Précision détection	$TP/(TP + FP)$	TP = True Positives (alertes justifiées), FP = False Positives (alertes injustifiées). Mesure la qualité des alertes générées.
Réponse	Temps de réponse (MTTR)	Moyenne(Heure containment – Heure alerte)	Évalue la réactivité opérationnelle du SOC une fois l'alerte levée. Réduit les risques d'escalade si faible.
	Actions manquées	Nb étapes non détectées ou non traitées	Compte les actions Red Team restées sans réponse. Mesure les failles dans le traitement opérationnel ou la couverture.
Collaboration	Scénarios documentés	Nb fiches renseignées / Nb scénarios exécutés	Évalue la rigueur du processus de documentation. Reflète la capacité à capitaliser les tests pour les audits ou les réutilisations.
	Recommandations appliquées	Nb recommandations appliquées / Nb proposées	Mesure la mise en œuvre des actions correctrices après test. Indicateur clé de la dynamique d'amélioration continue.

TABLE 3 – Indicateurs détaillés de performance (KPIs) pour l'évaluation Purple Team dans un contexte d'analyse de maturité SOC.

1.6.3 PONDÉRATION DES AXES

Axe	**Poids dans le calcul final**
Couverture	25 %
Détection	30 %
Réponse	25 %
Collaboration	20 %

TABLE 4 – Répartition des poids attribués à chaque axe dans le calcul final de la maturité

Ces poids reflètent l'importance relative de chaque domaine dans la réalité opérationnelle d'un SOC.

1.6.4 INDICATEURS PAR AXE

A. Couverture (25 %)

Indicateur	**Formule**
% Techniques MITRE testées	Nb testées / Nb cibles × 100
% Tactiques ATT&CK couvertes	Nb tactiques couvertes / 14 × 100

Étapes :

1. **Calculant le % Techniques MITRE testées**

$$\text{Techniques\_Score} = \left(\frac{\text{Nb techniques testées}}{\text{Nb techniques cibles}}\right) \times 100$$

2. **Calculant le % Tactiques ATT&CK couvertes**

$$\text{Tactics\_Score} = \left(\frac{\text{Nb tactiques couvertes}}{14}\right) \times 100$$

3. **Moyenne des deux :**

$$C = \frac{\text{Techniques\_Score} + \text{Tactics\_Score}}{2}$$

B. Détection (30 %)

Indicateur	**Formule**
Taux de détection	Nb événements détectés / Nb actions Red Team × 100
Précision des alertes	$TP/(TP + FP) \times 100$
Temps de détection	MTTD (en minutes), converti en score

Étapes :

1. **Calculant le Taux de détection brute**

$$\text{Detection\_Rate} = \left(\frac{\text{Nb événements détectés}}{\text{Nb actions Red Team}}\right) \times 100$$

2. **Calculant la Précision des alertes**

$$\text{Precision} = \left(\frac{TP}{TP + FP}\right) \times 100$$

3. **Évaluant le temps moyen de détection (MTTD)** :
   - < 5 min $\rightarrow 100$
   - 5–15 min $\rightarrow 80$
   - 15–30 min $\rightarrow 60$
   - 30–60 min $\rightarrow 40$
   - ≥ 60 min $\rightarrow 20$
4. **Moyenne des trois :**

$$D = \frac{\text{Detection\_Rate} + \text{Precision} + \text{MTTD\_Score}}{3}$$

C. Réponse (25 %)

Indicateur	**Formule**
Temps de réponse (MTTR)	Containment – détection $\rightarrow$ barème similaire à MTTD
% Actions Blue non manquées	$\left(1 - \frac{\text{Nb non traitées}}{\text{Nb actions Red Team}}\right) \times 100$

Étapes :

1. **Évaluant le temps moyen de réponse (MTTR)** :
   - < 10 min $\rightarrow 100$
   - 10–30 min $\rightarrow 80$
   - 30–60 min $\rightarrow 60$
   - ≥ 60 min $\rightarrow 40$

   $\Rightarrow$ On obtient `MTTR_Score`
2. **Calculant le % d'actions Red Team traitées**

$$\text{Missed\_Score} = \left(1 - \frac{\text{Nb actions manquées}}{\text{Nb actions totales}}\right) \times 100$$

3. **Moyenne des deux :**

$$R = \frac{\text{MTTR\_Score} + \text{Missed\_Score}}{2}$$

D. Collaboration (20 %)

Indicateur	**Formule**
Documentation des scénarios	Nb fiches complètes / Nb tests exécutés × 100
Recommandations appliquées	Nb appliquées / Nb proposées × 100

Étapes :

1. **Calculant le % de scénarios documentés**

$$\text{Documentation\_Score} = \left(\frac{\text{Nb fiches complètes}}{\text{Nb scénarios exécutés}}\right) \times 100$$

2. **Calculant le % de recommandations appliquées**

$$\text{Reco\_Score} = \left(\frac{\text{Nb recos appliquées}}{\text{Nb recos proposées}}\right) \times 100$$

3. **Moyenne des deux :**

$$C_o = \frac{\text{Documentation\_Score} + \text{Reco\_Score}}{2}$$

Calcul du Score Global

$$\text{Score global} = 0.25 \times C + 0.30 \times D + 0.25 \times R + 0.20 \times C_o$$

— `C` = score Couverture
— `D` = score Détection
— `R` = score Réponse
— `C_o` = score Collaboration

1.6.5 NIVEAU DE MATURITÉ FINAL

Score (%)	**Niveau**	**Signification**
0–20	0	Faible
21–40	1	Émergent
41–60	2	Structurant
61–80	3	Stabilisé
81–90	4	Piloté
91–100	5	Optimisé (exemplarité SOC)

TABLE 5 – Grille d'interprétation du score de maturité Purple Team