

## Cybersecurity Red Teaming

Le **red teaming** représente une approche proactive en cybersécurité qui va bien au-delà des tests de pénétration traditionnels en évaluant globalement la résilience d'une organisation face à des menaces réalistes. Pour structurer ces exercices, les professionnels s'appuient sur des **cadres méthodologiques** reconnus tels que le MITRE ATT&CK, l'Unified Kill Chain ainsi que des normes sectorielles comme TIBER-EU et CBEST. Les **types d'engagements** varient selon les objectifs fixés, allant des évaluations exhaustives à portée complète jusqu'aux simulations de scénarios spécifiques, en passant par les exercices collaboratifs et les discussions sur table. Ces initiatives permettent d'identifier les vulnérabilités critiques, de tester les capacités de détection des équipes de défense et de remettre en question les suppositions de sécurité. En fin de compte, l'intégration de ces pratiques favorise l'amélioration continue des protocoles de protection et renforce la posture globale de l'entreprise face à l'évolution constante des cybermenaces.

### Comment le red teaming diffère-t-il des tests de pénétration traditionnels ?

Bien que les tests de pénétration et le *red teaming* soient deux formes d'évaluations de la sécurité offensive, ils poursuivent des objectifs différents et utilisent des approches distinctes.

Voici les principales différences mises en avant :

- **Objectif principal** : Le test de pénétration cherche à **découvrir et exploiter autant de vulnérabilités que possible** de manière contrôlée, dans un périmètre et un délai définis, afin de documenter les faiblesses pour leur correction. Le *red teaming*, quant à lui, est axé sur **l'atteinte d'un objectif précis**, comme obtenir l'accès à des données sensibles ou compromettre une infrastructure critique.
- **Périmètre d'évaluation** : Les tests de pénétration s'attaquent généralement à des systèmes ou applications spécifiques. À l'inverse, le *red teaming* adopte une approche globale qui évalue

l'ensemble de l'écosystème de sécurité de l'organisation, incluant les **technologies**, les **processus** et le **facteur humain**.

- **Test des capacités de détection et de réponse** : Le test de pénétration n'évalue pas les capacités de détection ni de réponse aux attaques. Le *red teaming* est spécifiquement conçu pour **tester la capacité de l'organisation à identifier, contenir et réagir** à une attaque persistante menée sur une période prolongée.
- **Discretion et tactiques** : Alors que le test de pénétration se déroule dans un cadre restreint, le *red teaming* simule le comportement d'adversaires réels en exécutant des **attaques complexes en plusieurs étapes tout en cherchant à éviter d'être détecté**.

## Quels sont les cadres de référence du red teaming ?

Les principaux cadres de référence et méthodologies utilisés pour guider les opérations de *red teaming* sont :

- **Le cadre MITRE ATT&CK** : Il s'agit d'une base de connaissances complète qui répertorie systématiquement les tactiques, techniques et procédures (TTP) observées chez les adversaires réels. Développé par la société MITRE et structuré en différentes matrices (Enterprise, ICS, Mobile), il sert de standard dans l'industrie pour communiquer sur les attaques. Les *red teams* l'utilisent pour simuler le comportement d'attaquants et cartographier leurs activités afin de mesurer l'efficacité des contrôles de sécurité et de l'ingénierie de détection.
- **La Unified Kill Chain (UKC)** : Ce cadre conceptuel offre une vue globale du comportement de l'adversaire sur l'ensemble du cycle de vie d'une attaque. La *Unified Kill Chain* se distingue en couvrant à la fois les aspects techniques et stratégiques, liant chaque action technique aux objectifs globaux de l'attaquant (de la compromission initiale jusqu'à l'impact). Elle s'utilise en complément du cadre MITRE ATT&CK pour fournir un récit unifié de la campagne d'attaque.

- **TIBER-EU (Threat Intelligence-Based Ethical Red Teaming) :** Conçu par la Banque centrale européenne (BCE), ce cadre s'adresse aux institutions financières de l'Union européenne. Il repose sur l'utilisation du renseignement sur les menaces (*threat intelligence*) afin de personnaliser les exercices en fonction des risques réels de l'organisation. Ce cadre exige que la *red team* et l'équipe de renseignement soient des prestataires tiers indépendants, et fait intervenir cinq équipes distinctes (Threat Intelligence, Blue Team, Red Team, White Team et TIBER Team).
- **CBEST :** Établi par la Banque d'Angleterre, ce cadre guidé par le renseignement évalue et renforce la cyber-résilience des institutions financières au Royaume-Uni. Il repose sur le principe du « fil conducteur » (*golden thread*), qui assure un lien traçable entre les menaces identifiées par l'analyse de renseignement et les actions concrètes de mitigation. Il implique quatre acteurs clés : le fournisseur de renseignement, le prestataire de tests, le groupe de contrôle interne et le régulateur.

### Quels sont les différents types de missions de red teaming ?

Les exercices de *red teaming* se déclinent sous plusieurs formes adaptées aux objectifs spécifiques, à la taille, aux ressources et à la tolérance au risque de l'organisation :

- **Périmètre complet (Full-Scope) :** C'est la forme la plus vaste et la plus classique d'engagement. L'équipe utilise l'ensemble de son arsenal (cyberattaques, ingénierie sociale, sécurité physique) sur une période prolongée pour évaluer la résilience globale de l'organisation. Bien qu'elle offre une évaluation holistique, cette approche exige un investissement considérable en temps et en ressources.
- **Axé sur un objectif (Objective-Based) :** L'équipe se voit attribuer une mission précise liée à un objectif ou un risque d'affaires spécifique, comme accéder à des données sensibles ou les exfiltrer. Plus ciblées et généralement plus courtes qu'une mission *full-scope*, ces interventions permettent de mesurer de façon claire et mesurable la réussite de l'attaque sur un objectif donné.

- **Émulation d'adversaire (Adversary Emulation / Scenario-Based)** : Cette approche reproduit le cycle de vie complet d'une attaque en simulant les tactiques, techniques et procédures (TTP) d'un groupe de menace ou d'un type d'adversaire spécifique. Elle s'appuie fortement sur le renseignement sur les menaces (*threat intelligence*) pour tester la réaction de l'organisation face à des scénarios réels (ex. attaques APT, rançongiciels ou attaques sur la chaîne d'approvisionnement).
- **Équipe violette (Purple Teaming)** : Il s'agit d'un exercice collaboratif dans lequel la *red team* (offensive) et la *blue team* (défensive) travaillent conjointement en temps réel. La *red team* exécute et démontre les attaques pendant que la *blue team* s'entraîne à les détecter et à y répondre, favorisant un apprentissage mutuel et un ajustement immédiat des détections.
- **Exercice sur table (Tabletop Exercise - TTX)** : Il s'agit d'une simulation structurée sous forme de discussion guidée par un modérateur, sans déploiement d'outils ou de systèmes en direct. Cet exercice vise à évaluer la préparation organisationnelle, les politiques, la gestion de crise, la prise de décision et la communication plutôt que les capacités purement techniques.

## Comment le red teaming aide-t-il à remettre en question les hypothèses de sécurité ?

Le *red teaming* aide à remettre en question les hypothèses de sécurité en adoptant la perspective d'un adversaire afin d'évaluer la résistance réelle des défenses.

Voici comment cette démarche remet en cause les préconçus de l'organisation :

- **Dépasser la sécurité théorique et la conformité** : Les mesures de sécurité sont souvent conçues d'après des scénarios théoriques, des exigences de conformité ou des incidents passés. Si ces bases sont nécessaires, elles peuvent reposer sur des hypothèses non vérifiées ou ignorer l'évolution des menaces et l'ingéniosité des attaquants. Le *red teaming* permet de s'éloigner

d'une simple sécurité d'audit (« *checkbox security* ») pour construire des systèmes véritablement résilients.

- **Révéler les failles des processus en conditions réelles** : En simulant des comportements adverses réels, la *red team* teste la résistance des contrôles sous le stress d'une attaque et met en lumière des vulnérabilités cachées.
- **Mettre à l'épreuve les certitudes techniques** : Par exemple, une organisation peut supposer que l'authentification multi-facteurs (MFA) garantit la protection de ses comptes. La *red team* peut remettre cette certitude en question en démontrant qu'il est possible de contourner la MFA via de l'ingénierie sociale, comme le hameçonnage de jetons d'accès ou l'interception de codes SMS.
- **Instaurer une posture de défense adaptative** : En confrontant continuellement l'organisation à la réalité du terrain, le *red teaming* l'incite à réévaluer ses mécanismes de défense, à affiner ses hypothèses et à s'adapter face à l'évolution des menaces.

### Comment le red teaming aide-t-il à améliorer les autres équipes ?

Le *red teaming* ne se limite pas à identifier des vulnérabilités ; son véritable objectif est d'élever la maturité et les connaissances en sécurité de l'ensemble de l'organisation. Il contribue directement au renforcement de plusieurs équipes clés :

- **L'équipe défensive (Blue Team / SOC)** : La *red team* agit comme un partenaire d'entraînement (*sparring partner*) en simulant des scénarios d'attaque réels et en partageant la vision des adversaires. Cela permet à la *blue team* d'évaluer l'efficacité de ses alertes actuelles, de tester et d'ajuster ses outils de sécurité, de créer de nouvelles règles de détection et de renforcer sa réponse aux incidents.
- **L'équipe de renseignement sur les menaces (Threat Intelligence)** : Le partage d'informations sur les vulnérabilités exploitées, les vecteurs d'attaque et les tactiques, techniques et procédures (TTP) observées alimente directement l'équipe de renseignement. Ces données lui permettent de perfectionner ses modèles de menaces, d'optimiser la chasse aux menaces (*threat*

*hunting*) et de diffuser des avertissements plus précis et rapides au sein de l'entreprise.

- **Les équipes d'ingénierie et de développement** : La *red team* apporte une expertise ponctuelle et proactive lors du cycle de développement, notamment sur les pratiques de codage sécurisé, la modélisation des menaces et la correction de failles spécifiques (comme la neutralisation des entrées utilisateur).
- **Les employés et l'ensemble du personnel** : Les retours d'expériences issus d'attaques réelles servent à concevoir des formations de sensibilisation concrètes sur des menaces comme l'ingénierie sociale, le hameçonnage ou les logiciels malveillants. Ces apprentissages peuvent être partagés sous forme d'ateliers ou de présentations internes.
- **La direction et les équipes transversales** : L'utilisation de cadres de référence partagés (comme MITRE ATT&CK) offre un langage commun entre les équipes offensives, défensives et les dirigeants. Cela facilite la collaboration, clarifie l'alignement stratégique et soutient l'amélioration continue de la posture de sécurité.

## Comment gérer une mission de red teaming sans résultats ?

Lorsqu'une mission de *red teaming* ne permet pas d'atteindre l'objectif fixé ou ne révèle pas de vulnérabilité majeure (un engagement dit « *no-findings* »), cela ne doit pas être perçu comme un échec, car ne pas atteindre l'objectif apporte tout autant d'informations.

Voici comment analyser et valoriser ce type de résultat :

- **Valider les contrôles de sécurité existants** : L'absence d'intrusion constitue une **validation concrète des défenses en place**. Cela prouve que les contrôles de sécurité ont été correctement configurés et efficacement déployés.
- **Identifier les améliorations de l'équipe défensive** : Ce résultat s'explique souvent par la résolution récente de failles (par exemple, la clôture d'un ticket de correction) ou par l'installation de nouveaux mécanismes de protection dont l'équipe offensive n'avait pas connaissance.

- **Favoriser l'apprentissage et l'expérimentation** : Cette situation offre l'occasion d'étudier de plus près le fonctionnement des contrôles de sécurité qui ont fait obstacle et d'expérimenter de nouvelles techniques.
- **Guider la planification des futures interventions** : L'expérience acquise fournit des indications précieuses pour les engagements ultérieurs. Lors de la préparation des sessions suivantes, l'équipe peut **affiner le périmètre, réévaluer les risques et définir de nouveaux objectifs**.

En somme, une mission sans découvertes critiques est une **opportunité d'apprentissage et d'amélioration continue**, et non un signe de défaite.

### Qu'est-ce que le purple teaming ?

Le **purple teaming** est une approche collaborative où la *red team* (offensive) et la *blue team* (défensive) travaillent conjointement pour simuler des attaques et y répondre en temps réel. Plutôt que de s'opposer dans un cadre purement adversarial, l'objectif central est de favoriser l'apprentissage mutuel et l'amélioration continue.

Voici les aspects fondamentaux de cette approche :

- **Collaboration et exécution en temps réel** : La *red team* démontre et exécute des attaques simulées, tandis que la *blue team* exerce activement ses capacités de détection, de réponse et de neutralisation.
- **Rétroaction immédiate** : Ce format permet d'obtenir un retour d'information instantané afin d'ajuster et de perfectionner les règles de détection et les contrôles de sécurité directement pendant l'exercice, plutôt que lors d'une analyse a posteriori.
- **Partage de connaissances** : Il favorise une communication ouverte pour aider chaque équipe à mieux comprendre la perspective, les contraintes et le mode de pensée de l'autre, renforçant ainsi la résilience globale de l'organisation.

### Avantages et contraintes :

- **Avantages** : Collaboration directe entre attaquants et défenseurs, rétroaction instantanée pour affiner les alertes et amélioration continue de la posture de sécurité.

- **Contraintes** : Nécessite du personnel expérimenté des deux côtés et une bonne coordination ; comporte un risque de réalisme réduit si les attaques sont connues d'avance ou réalisées dans un environnement qui ne réplique pas la production ; et exige une documentation rigoureuse pour éviter que les connaissances acquises ne restent cloisonnées.

## Quels sont les avantages d'un exercice de purple teaming ?

Les principaux avantages d'un exercice de **purple teaming** sont :

- **Collaboration en temps réel (Real-Time Collaboration)** : Les équipes offensive (*red team*) et défensive (*blue team*) travaillent conjointement. La *red team* exécute et démontre l'attaque simulée pendant que la *blue team* s'entraîne activement à la détecter et à y répondre.
- **Rétroaction immédiate (Immediate Feedback)** : Cette approche permet d'obtenir un retour d'information instantané, ce qui permet d'ajuster et de perfectionner les contrôles de sécurité directement pendant l'exercice plutôt que d'attendre l'analyse post-exercice.
- **Amélioration continue (Continuous Improvement)** : Le *purple teaming* instaure une culture d'amélioration continue, permettant aux deux équipes de partager leurs observations et de renforcer la posture de sécurité globale de l'organisation de manière itérative.
- **Apprentissage mutuel et partage de connaissances** : Cet engagement favorise une communication ouverte, permettant à chaque équipe de mieux comprendre la perspective, la logique et les méthodes de l'autre.

## Quelles sont les contraintes associées au purple teaming ?

Les principales contraintes et limites associées aux exercices de **purple teaming** sont :

- **Exigence importante en ressources** : Ces exercices nécessitent la présence simultanée de professionnels expérimentés issus des deux équipes (*red team* et *blue team*), ainsi qu'une coordination étroite et un investissement en temps conséquent pour être pleinement efficaces.

- **Réduction potentielle du réalisme** : Étant donné que les deux équipes sont conscientes des attaques simulées au fur et à mesure, la réponse défensive peut ne pas être exécutée de manière aussi réaliste qu'en situation d'attaque réelle. De plus, l'utilisation d'environnements de test qui ne répliquent pas parfaitement les conditions de production peut altérer la fidélité de l'exercice.
- **Risque de création de silos de connaissances** : Sans une documentation rigoureuse, de bons rapports et une transmission des acquis, les enseignements tirés risquent de rester confinés aux seuls participants à l'exercice au lieu de bénéficier à l'ensemble de l'organisation.

## Qu'est-ce que le cadre MITRE ATT&CK ?

Le **cadre MITRE ATT&CK** (*Adversarial Tactics, Techniques, and Common Knowledge*) est une base de connaissances complète qui répertorie méthodiquement les tactiques, techniques et procédures (TTP) observées chez les adversaires tout au long de la chaîne d'attaque (*kill chain*). Développé par la société MITRE, ce cadre est régulièrement mis à jour pour refléter l'évolution du paysage des menaces et constitue le standard dans l'industrie pour communiquer sur les cyberattaques.

Voici ses caractéristiques et utilisations principales :

- **Structure en matrices** : Le cadre est divisé en plusieurs matrices adaptées à des domaines d'application spécifiques, notamment **Enterprise**, **ICS** (systèmes de contrôle industriel) et **Mobile**.
- **Langage commun et collaboration** : Il fournit un langage partagé entre les perspectives offensives et défensives, facilitant la collaboration entre les *red teams*, les *blue teams*, l'équipe de renseignement sur les menaces (*threat intel*), le SOC et la direction.
- **Émulation d'adversaires** : Les *red teams* s'appuient sur ce cadre pour reproduire fidèlement le comportement d'attaquants réels durant leurs interventions.

- **Cartographie et ingénierie de détection** : Il permet d'associer précisément chaque action de la *red team* à des TTP spécifiques, ce qui aide à analyser la qualité de l'ingénierie de détection et à évaluer l'efficacité des contrôles de sécurité.

## Quels sont les cadres pour le secteur financier ?

Les deux principaux cadres de *red teaming* spécifiquement conçus pour le secteur financier sont **TIBER-EU** et **CBEST**. Tous deux privilégient une approche axée sur le renseignement sur les menaces (*threat intelligence*) et le respect de normes de test rigoureuses.

### 1. TIBER-EU (*Threat Intelligence-Based Ethical Red Teaming*)

- **Origine et périmètre** : Développé par la Banque centrale européenne (BCE), ce cadre s'adresse aux institutions financières de l'Union européenne qui fournissent des infrastructures financières essentielles.
- **Objectif et approche** : Il utilise le renseignement sur les menaces pour adapter sur mesure les exercices de simulation aux risques réels de l'organisation. Son but est d'élever la maturité et la résilience cyber des établissements financiers en fournissant une évaluation standardisée dont les résultats sont comparables d'une institution à l'autre.
- **Acteurs impliqués** : Un exercice TIBER-EU réunit **cinq équipes distinctes** :
  - **L'équipe Threat Intelligence** : Prestataire tiers chargé d'analyser l'établissement et de fournir le profil des attaquants potentiels et leurs TTPs.
  - **La Red Team** : Prestataire tiers indépendant qui exécute l'attaque simulée.
  - **La Blue Team** : Équipe interne de l'institution responsable de la prévention, de la détection et de la réponse.
  - **La White Team** : Agents internes de confiance au sein de l'institution.
  - **La TIBER Team** : Équipe interne veillant à ce que le test respecte les exigences du cadre TIBER-EU.

## 2. CBEST

- **Origine et périmètre** : Établi par la Banque d'Angleterre (*Bank of England*), le cadre CBEST est utilisé pour évaluer et renforcer la cyber-résilience des institutions financières opérant au Royaume-Uni.
- **Objectif et principe du « fil conducteur »** : Guidé par le renseignement, CBEST priorise le test des systèmes et des fonctions critiques indispensables au fonctionnement de l'établissement. Il repose sur le principe du « **fil conducteur** » (*golden thread*), qui garantit une traçabilité directe entre les menaces identifiées par l'analyse de renseignement et les mesures concrètes de mitigation prises par l'entreprise.
- **Acteurs impliqués** : La réalisation d'un exercice CBEST fait intervenir **quatre acteurs clés** :
  - **Le fournisseur de renseignement sur les menaces** (*Threat Intelligence Service Provider*) : Prestataire tiers qui réalise l'évaluation externe, crée les scénarios d'attaque et évalue la maturité du renseignement.
  - **Le prestataire de tests de pénétration / Red Team** (*Penetration Test Service Provider*) : Prestataire tiers qui planifie et exécute les attaques basées sur les scénarios, évalue la détection/réponse et rédige le rapport.
  - **Le groupe de contrôle de l'entreprise** (*Firm/Control Group*) : Équipe interne assurant la gestion de projet, le contrôle qualité et la coordination de l'évaluation.
  - **Le régulateur** (*Regulator*) : Autorité qui fournit les directives, supervise le déroulement, examine les résultats et suit les plans de remédiation.

## Qu'est-ce que la Unified Kill Chain ?

La **Unified Kill Chain (UKC)** est un cadre conceptuel conçu comme l'évolution de plusieurs modèles antérieurs, visant à dépasser leurs limites grâce à une approche unifiée. Elle est élaborée pour offrir une vision globale du comportement d'un adversaire sur l'ensemble du cycle de vie d'une cyberattaque.

Ses caractéristiques et apports principaux sont :

- **Combinaison des aspects techniques et stratégiques** : Contrairement au cadre MITRE ATT&CK, la *Unified Kill Chain* se concentre à la fois sur les dimensions techniques et stratégiques des attaques.
- **Couverture complète du cycle d'attaque** : Elle englobe des techniques couvrant l'ensemble du parcours de l'attaquant, notamment la compromission initiale, la persistance, le déplacement latéral et l'impact.
- **Lien entre actions techniques et objectifs globaux** : Elle associe chaque action technique spécifique aux objectifs stratégiques de l'adversaire. Cela permet à l'organisation de comprendre comment chaque tactique, technique et procédure (TTP) contribue aux buts globaux de l'attaquant.
- **Alignement sur la gestion des risques** : Le modèle aligne la progression de l'attaque avec les objectifs opérationnels et de gestion des risques de l'entreprise.
- **Complémentarité avec d'autres cadres** : Sa flexibilité lui permet de compléter des référentiels comme MITRE ATT&CK en fournissant un récit unifié des campagnes d'attaque.
- **Simulation d'attaques sophistiquées** : Les *red teams* l'utilisent pour émuler des séquences d'attaque complexes et aider les organisations à tester leurs contrôles de sécurité de manière globale.

### Quels sont les avantages des missions full-scope ?

Les missions de *red teaming* à périmètre complet (*full-scope*) présentent plusieurs avantages majeurs pour mesurer la résistance d'une organisation face à des cyberattaques réelles :

- **Évaluation holistique de la résilience** : Ce type d'engagement évalue l'ensemble de l'écosystème de sécurité de l'organisation. Il permet de tester la capacité globale à détecter les attaques et à y répondre à travers tous les domaines, en intégrant les technologies, les processus et le facteur humain [30, Table 2-1].
- **Combinaison de multiples vecteurs d'attaque** : Une mission *full-scope* ne se limite pas aux seuls systèmes informatiques ; elle

combine simultanément des attaques cyber, de l'ingénierie sociale et des tests de sécurité physique [30, Table 2-1].

- **Exploitation complète de l'arsenal et durée prolongée** : La *red team* dispose du temps et de la flexibilité nécessaires pour utiliser l'intégralité de son arsenal stratégique et technique, tout en s'appuyant sur le renseignement sur les menaces (*threat intelligence*).
- **Vision exhaustive de la posture de risque** : En évaluant l'organisation dans sa globalité plutôt qu'en isolant une application ou un réseau particulier, cette approche garantit qu'aucun point faible critique n'est négligé.

### Comment se déroule un exercice sur table (TTX) ?

Un exercice sur table (*Tabletop Exercise* - TTX) est une simulation structurée et axée sur la discussion, conçue pour évaluer la préparation d'une organisation face à divers scénarios d'incident (cyberattaques, crises ou catastrophes naturelles).

Voici comment se déroule concrètement cet exercice :

- **Un cadre contrôlé sans déploiement technique** : Contrairement aux simulations en direct, l'exercice se déroule dans un environnement contrôlé où les participants discutent des réactions à adopter face à des incidents hypothétiques, **sans exécuter d'outils ni intervenir sur des systèmes actifs**.
- **Guidé par un modérateur** : La session est généralement animée par un modérateur (souvent un tiers indépendant, auquel la *red team* peut participer). Le modérateur présente le scénario, introduit des imprévus au fil de l'eau et pousse les participants à expliciter leurs stratégies de réponse.
- **Axé sur les processus et la décision** : L'exercice ne teste pas les capacités purement techniques, mais évalue la **validité des politiques, des procédures d'urgence (playbooks), de la communication et de la prise de décision**.
- **Collaboration transversale** : Il rassemble des représentants de plusieurs départements pour clarifier les rôles et responsabilités de chacun lors d'une crise et renforcer la coordination globale.

## Avantages et limites :

- **Points forts** : Il permet de repérer de manière proactive les lacunes dans les plans de réponse, d'améliorer la communication interservices et d'offrir une évaluation rentable sans mobiliser d'infrastructures lourdes.
- **Limites** : Comme il repose uniquement sur la discussion, il ne permet pas d'identifier les failles purement techniques et reste contraint par la disponibilité du personnel clé.

## Concevoir un guide récapitulatif ou une matrice comparative synthétisant l'ensemble des types d'engagements de red teaming (full-scope, objective-based, adversary emulation, purple team, tabletop)

Voici le **guide récapitulatif** et la **matrice comparative** synthétisant les cinq principaux types d'engagements de *red teaming*, leurs caractéristiques, leurs avantages et leurs contraintes.

### Matrice comparative des types d'engagements

| Type d'engagement                            | Objectif & Périmètre principal                                                                                                        | Avantages clés                                                                                                               | Limites & Contraintes                                                                                | Durée & Ressources                                                         |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Périmètre complet (Full-Scope)</b>        | Évaluation globale et approfondie de la résilience à travers les technologies, les personnes et la sécurité physique [30, Table 2-1]. | Évaluation holistique de l'organisation ; combinaison de multiples vecteurs d'attaque (cyber, social, physique) [Table 2-1]. | Très énergivore en ressources ; nécessite un investissement majeur [30, Table 2-1].                  | <b>Plusieurs mois</b> ; demande en ressources très élevée [30, Table 2-1]. |
| <b>Axé sur un objectif (Objective-Based)</b> | Atteinte d'un but précis lié à un risque d'affaires (ex. exfiltration de données ou compromission d'un système critique).             | Résultats clairs et mesurables ; optimisation des ressources ; alignement direct sur les risques prioritaires [Table 2-2].   | Périmètre étroit risquant de négliger d'autres failles ; évaluation souvent « binaire » [Table 2-2]. | <b>1 semaine à quelques mois</b> ; ressources modérées.                    |

|                                                |                                                                                                                             |                                                                                                                                      |                                                                                                                                 |                                                                                                   |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Émulation d'adversaire (Scenario-Based)</b> | Reproduction du cycle de vie complet d'une attaque selon les TTP d'un groupe de menace spécifique (APT, rançongiciel).      | Émulation réaliste basée sur le renseignement ( <i>threat intel</i> ) ; forte pertinence face aux menaces actuelles [33, Table 2-3]. | Périmètre vaste pouvant diluer la focalisation ; mesure du succès plus complexe en raison de résultats multiples [Table 2-3].   | <b>Quelques semaines à plusieurs mois</b> ; ressources élevées.                                   |
| <b>Équipe violette (Purple Team)</b>           | Collaboration directe et en temps réel entre la <i>red team</i> et la <i>blue team</i> pour l'apprentissage mutuel.         | Rétroaction immédiate ; ajustement des détections en direct ; promotion d'une culture d'amélioration continue [Table 2-4].           | Exige des spécialistes expérimentés des deux côtés ; risque de réalisme réduit si l'attaque est connue d'avance [Table 2-4].    | <b>Variable</b> ; requiert la présence simultanée des experts offensifs et défensifs [Table 2-4]. |
| <b>Exercice sur table (Tabletop - TTX)</b>     | Simulation basée sur la discussion pour tester la prise de décision, les processus et la communication en gestion de crise. | Identifie les lacunes des plans et <i>playbooks</i> ; améliore la coordination interservices ; très économique [Table 2-5].          | Ne teste pas les capacités ou configurations techniques réelles ; limité par la disponibilité des participants [36, Table 2-5]. | <b>Court</b> (quelques heures à 1-2 jours) ; coût technique faible [36, Table 2-5].               |

## Guide récapitulatif détaillé

### 1. Périmètre complet (*Full-Scope*)

- **Description** : Il s'agit du modèle classique et le plus vaste d'engagement. La *red team* déploie l'ensemble de son arsenal (cyberattaques, ingénierie sociale, intrusion physique) sur une période prolongée pour évaluer la capacité globale d'une organisation à détecter et contenir une menace [30, Table 2-1].

- **Points forts** : Il offre une **vision holistique de la résilience** en testant simultanément les technologies, les processus et le facteur humain face à des attaques multi-vecteurs [30, Table 2-1].
- **Contraintes** : Son exécution exige des **ressources financières et humaines très importantes** ainsi que des outils parfois spécifiques, ce qui rend son organisation fréquente difficile pour beaucoup d'entreprises [30, Table 2-1].

## 2. Axé sur un objectif (*Objective-Based*)

- **Description** : L'engagement est construit autour d'une mission précise alignée sur un risque stratégique (ex. accéder à une base de données clients ou manipuler des données financières).
- **Points forts** : Il offre un **résultat clair et mesurable**, optimise l'utilisation des ressources et permet à la *blue team* d'améliorer sa réponse face à des scénarios d'attaque très ciblés [Table 2-2].
- **Contraintes** : En se concentrant sur un seul but, cet exercice présente un **périmètre restreint** qui peut passer à côté d'autres vulnérabilités critiques non liées à l'objectif sélectionné [Table 2-2].

## 3. Émulation d'adversaire (*Adversary Emulation / Scenario-Based*)

- **Description** : Cette approche réplique fidèlement le comportement d'un type d'attaquant ou d'un groupe APT spécifique en reproduisant ses tactiques, techniques et procédures (TTP) tout au long du cycle de vie de l'attaque. Elle s'appuie obligatoirement sur le renseignement sur les menaces (*threat intelligence*).
- **Points forts** : Elle garantit une **haute pertinence par rapport aux risques réels** du secteur d'activité (ex. simulations de rançongiciels ou d'attaques sur la chaîne d'approvisionnement) [33, Table 2-3].
- **Contraintes** : La portée globale de ces scénarios peut **diluer l'attention** sur certaines failles plus spécifiques et rendre la mesure de la réussite plus complexe [Table 2-3].

## 4. Équipe violette (*Purple Team*)

- **Description** : Exercice collaboratif dans lequel la *red team* démontre les techniques d'attaque en direct pendant que la *blue team* s'entraîne à les repérer, à les analyser et à les bloquer [34, 35, Table 2-4].

- **Points forts** : Il fournit une **rétroaction immédiate**, permettant à la *blue team* de créer et d'ajuster ses règles de détection directement durant l'exercice plutôt qu'après coup [Table 2-4].
- **Contraintes** : Il nécessite la mobilisation simultanée de **personnel qualifié dans chaque équipe** et peut souffrir d'un **réalisme réduit** puisque la *blue team* est consciente des tests en cours [Table 2-4].

#### 5. Exercice sur table (*Tabletop Exercise - TTX*)

- **Description** : Simulation structurée sous forme de table ronde guidée par un modérateur, où les participants débattent des décisions à prendre face à un scénario de crise sans exécuter de commandes ni modifier les systèmes.
- **Points forts** : Très **rentable et facile à organiser**, il permet de déceler les failles dans les politiques de sécurité, les canaux de communication et les processus de gestion de crise [36, Table 2-5].
- **Contraintes** : Il **ne valide pas l'efficacité technique** des outils de sécurité ou des configurations réseau [Table 2-5].

### Quels sont les objectifs d'un test de pénétration ?

Les objectifs principaux d'un test de pénétration (*penetration test*) sont :

- **Découvrir un maximum de vulnérabilités** : Identifier autant de faiblesses que possible de manière contrôlée.
- **Exploiter les systèmes et documenter les faiblesses** : L'objectif consiste uniquement à exploiter les systèmes ciblés et à documenter les vulnérabilités identifiées afin de guider leur correction (*remediation*).
- **Opérer dans un cadre délimité** : L'évaluation est réalisée selon un périmètre (*scope*) et un calendrier strictement définis.

Contrairement au *red teaming*, le test de pénétration ne cherche pas à tester les capacités de détection et de réponse de l'organisation, ni à évaluer l'implication du personnel ou des processus dans la prévention des attaques.

**Explorer la manière dont les résultats d'un test de pénétration sont exploités pour la remédiation par rapport au rapport d'un exercice de red teaming**

L'exploitation des rapports issus d'un **test de pénétration** et d'un **exercice de red teaming** diffère profondément, car leurs objectifs fondamentaux et leurs périmètres d'évaluation ne sont pas les mêmes.

1. Exploitation d'un rapport de test de pénétration : Remédiation technique directe

Le rapport d'un test de pénétration fournit une liste documentée de vulnérabilités et de faiblesses techniques identifiées dans un périmètre et un délai stricts.

- **Type de remédiation : Correctifs techniques ciblés** (application de correctifs de sécurité/*patches*, modification de règles de pare-feu, correction de failles dans le code applicatif ou correction de configurations erronées).
- **Public destinataire** : Principalement les **administrateurs système/réseau** et les **développeurs**, chargés de colmater les brèches identifiées.
- **Portée des actions** : La remédiation reste localisée aux systèmes ou applications évalués pendant le test. Elle ne cherche pas à savoir si l'équipe de sécurité a détecté le testeur ou si les procédures d'alerte ont fonctionné.

2. Exploitation d'un rapport de Red Teaming : Élévation globale de la résilience

Le rapport de *red teaming* retrace l'intégralité d'un scénario d'attaque complexe. Il montre comment l'adversaire a combiné les failles informatiques, le facteur humain et les processus organisationnels pour atteindre son objectif sans se faire détecter.

Ses résultats sont exploités de manière transversale par plusieurs équipes :

- **Pour le Centre d'opérations de sécurité (SOC) et la Blue Team** :
  - **Ingénierie de détection** : Analyse des étapes où l'attaque a échappé aux radars pour ajuster les règles de détection et optimiser les outils de surveillance (SIEM, EDR).
  - **Temps de réponse et confinement** : Évaluation de la vitesse et de l'efficacité avec lesquelles l'équipe défensive parvient à identifier, répondre et contenir une menace persistante sur une période prolongée.

- **Pour l'équipe de renseignement sur les menaces (Threat Intelligence) :**
  - **Raffinage des modèles :** Utilisation des tactiques, techniques et procédures (TTP) réelles observées pour mettre à jour la modélisation des menaces et guider la chasse aux menaces (*threat hunting*).
- **Pour les processus et la gestion de crise :**
  - **Révision des playbooks :** Ajustement des procédures de réponse aux incidents, des canaux de communication et des plans de continuité des affaires.
- **Pour la sensibilisation des employés :**
  - **Formations concrètes :** Création d'ateliers ou de démonstrations basés sur les scénarios réels d'ingénierie sociale ou d'hameçonnage réussis lors de l'exercice.
- **Pour les équipes d'ingénierie et de développement :**
  - **Conception sécurisée :** Conseils ciblés sur la modélisation des menaces et l'application des bonnes pratiques de développement (comme le nettoyage des entrées utilisateur).

#### Synthèse comparative

| Critère                    | Test de pénétration                                                                    | Exercice de Red Teaming                                                                                               |
|----------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Contenu du rapport</b>  | Liste de vulnérabilités techniques sur des systèmes précis.                            | Récit d'attaque complet testant l'ensemble de l'écosystème (technologies, humain, processus).                         |
| <b>Mode de remédiation</b> | <b>Tactique :</b> Correction de bugs, <i>patching</i> et ajustements de configuration. | <b>Stratégique et opérationnel :</b> Amélioration des détections, des processus d'incidents et de la réponse humaine. |
| <b>Impact principal</b>    | Fermeture de points d'accès individuels.                                               | Optimisation de la capacité globale à détecter, répondre et récupérer.                                                |

### **Concevoir un modèle de plan d'action post-exercice (de type purple team ou red team) pour structurer la remédiation au sein de vos équipes défensives et opérationnelles**

Un modèle complet de plan d'action post-exercice pour les équipes défensives et opérationnelles a été créé et mis à disposition. Ce

document détaille le cadre directeur de la remédiation, la feuille de route d'amélioration par spécialité (Blue Team/SOC, Threat Intelligence, Ingénierie, Sensibilisation et Gouvernance), le cycle de retest en cinq phases ainsi qu'une grille opérationnelle de suivi directement réutilisable articulée autour des référentiels MITRE ATT&CK et Unified Kill Chain.

## Quels sont les rôles des équipes dans TIBER-EU ?

Dans le cadre **TIBER-EU**, un exercice de *red teaming* réunit **cinq équipes distinctes**, chacune investie de responsabilités spécifiques :

- **Threat Intelligence** : Une équipe externe indépendante chargée de la reconnaissance et de l'analyse de l'institution financière. Elle fournit la liste des acteurs de menaces crédibles ainsi que leurs tactiques, techniques et procédures (TTP).
- **Red Team** : Une équipe externe indépendante qui planifie et exécute l'attaque simulée contre l'institution financière.
- **Blue Team** : L'équipe interne de l'institution financière, responsable de la prévention, de la détection et de la réponse aux attaques.
- **White Team** : Des agents internes de confiance au sein de l'institution financière qui encadrent et gèrent le déroulement de l'exercice.
- **TIBER Team** : L'équipe interne veilleuse du respect des normes et exigences du cadre TIBER-EU tout au long du test.

Le cadre TIBER-EU impose que l'équipe de **Threat Intelligence** et la **Red Team** soient obligatoirement des prestataires tiers indépendants pour garantir un regard externe neutre et apporter des ressources spécialisées.

## Comparer cette structure avec la répartition des rôles dans le cadre britannique CBEST

Bien que **TIBER-EU** (Banque centrale européenne) et **CBEST** (Banque d'Angleterre) soient deux cadres guidés par le renseignement (*intelligence-led*) destinés au secteur financier, ils organisent leurs participants selon des structures d'équipes différentes. **TIBER-EU**

**s'appuie sur un modèle à 5 équipes**, tandis que **CBEST repose sur une structure à 4 équipes**.

Voici la comparaison détaillée des rôles entre les deux cadres :

1. Supervision et gouvernance de l'exercice

- **Dans TIBER-EU** : La gouvernance repose sur deux entités internes à l'institution financière. La **White Team** regroupe les agents internes de confiance qui encadrent l'exercice, tandis que la **TIBER Team** s'assure du respect des exigences du cadre TIBER-EU.
- **Dans CBEST** : La gouvernance intègre directement le **Régulateur** (*Regulator*) en tant qu'équipe officielle de l'exercice pour fournir les directives, superviser le test et valider les plans de remédiation. La gestion interne est centralisée au sein du **Control Group** (*Firm/Control Group*), dirigé par un coordonnateur (*Control Group Coordinator - CGC*).

2. Renseignement sur les menaces (*Threat Intelligence*)

- **Dans TIBER-EU** : L'équipe de **Threat Intelligence** (prestataire tiers indépendant) réalise la reconnaissance et fournit la liste des acteurs de menaces crédibles et leurs TTPs.
- **Dans CBEST** : Le **Threat Intelligence Service Provider** (prestataire tiers) va un cran plus loin : il réalise l'évaluation externe, élabore directement les scénarios d'attaque et évalue la maturité du renseignement de l'entreprise.

3. Exécution de l'attaque simulée (*Red Team*)

- **Dans TIBER-EU** : L'attaque est menée par la **Red Team** (prestataire tiers indépendant) qui simule l'adversaire en exploitant les TTPs fournies par l'équipe de renseignement.
- **Dans CBEST** : Ce rôle est attribué au **Penetration Test Service Provider** (prestataire tiers). En plus d'exécuter le scénario, cette équipe est formellement chargée d'évaluer les capacités de détection et de réponse de la firme et de rédiger le rapport final.

4. Place de l'équipe défensive (*Blue Team*)

- **Dans TIBER-EU** : La **Blue Team** (l'équipe interne responsable de la prévention, détection et réponse) est **explicitement comptabilisée** comme l'une des 5 équipes officielles de l'exercice.
- **Dans CBEST** : La réaction défensive est mesurée par le prestataire de test et le Control Group, mais la Blue Team n'est

pas identifiée comme un rôle distinct dans la structure officielle des 4 équipes.

### Tableau synthétique de correspondance des rôles

| Fonction / Rôle         | Structure TIBER-EU (5 équipes)          | Structure CBEST (4 équipes)                              |
|-------------------------|-----------------------------------------|----------------------------------------------------------|
| Renseignement           | <i>Threat Intelligence</i> (Tiers)      | <i>Threat Intelligence Service Provider</i> (Tiers)      |
| Attaque / Red Team      | <i>Red Team</i> (Tiers)                 | <i>Penetration Test Service Provider</i> (Tiers)         |
| Coordination interne    | <i>White Team</i> (Agents de confiance) | <i>Firm/Control Group</i> (avec CGC)                     |
| Conformité & Régulation | <i>TIBER Team</i> (Interne)             | <i>Regulator</i> (Régulateur externe)                    |
| Défense / SOC           | <i>Blue Team</i> (Interne)              | <i>Évaluée par le prestataire &amp; le Control Group</i> |

 Souhaitez-vous explorer le principe du « **fil conducteur** » (**golden thread**) propre à CBEST ou voir comment s'appliquent les exigences de neutralité des prestataires tiers dans ces deux cadres ?

## Explorer le principe du « fil conducteur » (golden thread) propre à CBEST

Le principe du « **fil conducteur** » (**golden thread**) est le concept fondamental du cadre britannique **CBEST** (Banque d'Angleterre). Il établit une continuité logique, directe et vérifiable entre l'analyse du renseignement et les actions de sécurité de l'organisation.

Voici les éléments clés pour comprendre ce principe :

### 1. Définition et objectif principal

Le *golden thread* désigne **un lien traçable entre les menaces identifiées lors de l'évaluation du renseignement et les actions concrètes de réduction des risques (mitigation)** prises par l'institution financière.

Plutôt que de mener des tests de sécurité gérés de façon générique ou isolée, le cadre CBEST impose que chaque attaque simulée et chaque mesure corrective découlent directement d'une menace réelle et documentée.

## 2. Le déroulement du fil conducteur dans l'exercice

La traçabilité du *golden thread* se déploie à travers quatre phases ordonnées :

- **Analyse du renseignement** : Le prestataire spécialisé (*Threat Intelligence Service Provider*) évalue le profil de l'institution et identifie les menaces ainsi que les vulnérabilités spécifiques auxquelles elle fait face.
- **Priorisation des fonctions critiques** : L'évaluation concentre ses efforts en priorité sur les systèmes et fonctions indispensables au fonctionnement de l'établissement (par exemple, un processeur de paiement testant ses défenses contre l'exfiltration de données).
- **Exécution sur scénarios réels** : La *red team* (*Penetration Test Service Provider*) conçoit et exécute ses attaques en se basant exclusivement sur les scénarios issus du renseignement.
- **Remédiation motivée** : Les plans d'action et corrections apportés par l'entreprise sont directement reliés à la menace initiale, garantissant une justification claire auprès du groupe de contrôle interne et du régulateur.

## 3. Avantages stratégiques

- **Alignement sur la gestion des risques** : Il garantit une cohérence totale entre les simulations offensives, la stratégie globale de gestion des risques et les priorités d'investissement de l'entreprise.
- **Redevabilité et amélioration continue** : Ce principe instaure une responsabilité claire (*accountability*) et permet de mesurer objectivement l'évolution de la cyber-résilience au fil du temps.
- **Validation réglementaire** : Il offre au régulateur une preuve méthodique que l'établissement traite activement les menaces qui le concernent le plus directement.

**Examiner les critères de sélection et de neutralité exigés pour les prestataires tiers dans les cadres CBEST et TIBER-EU**

Les cadres **TIBER-EU** et **CBEST** imposent des critères stricts de sélection et de neutralité pour les prestataires tiers afin de garantir l'objectivité, la rigueur et la pertinence des exercices de *red teaming* :

- **Exigence d'indépendance et de neutralité externe :**
  - Dans **TIBER-EU**, le cadre exige formellement que l'analyse du renseignement (*Threat Intelligence*) et l'exécution de l'attaque simulée (*Red Team*) soient confiées à des prestataires tiers indépendants. Cette indépendance garantit un regard neutre et extérieur tout en apportant des ressources et compétences spécialisées qui ne sont pas toujours disponibles en interne.
  - Dans **CBEST**, les rôles de fourniture de renseignement (*Threat Intelligence Service Provider*) et d'exécution des tests (*Penetration Test Service Provider*) sont également attribués à des équipes tierces distinctes et indépendantes.
- **Compétences et responsabilités requises par spécialité :**
  - **Prestataire de Threat Intelligence** : Il doit disposer de capacités d'analyse avancées pour effectuer la reconnaissance de l'institution et établir la liste des acteurs de menaces crédibles et de leurs TTPs. Dans le cadre CBEST, il est également sélectionné pour évaluer la maturité globale du renseignement de la firme et élaborer les scénarios d'attaque.
  - **Prestataire d'exécution (Red Team / Penetration Test Service Provider)** : Il doit être capable de planifier et d'exécuter des attaques réalistes en se basant sur les scénarios fournis par le renseignement. Dans CBEST, ce prestataire doit aussi posséder les compétences d'ingénierie défensive nécessaires pour évaluer formellement les capacités de détection et de réponse de l'organisation.
- **Supervision et étanchéité vis-à-vis des équipes internes :**
  - Les prestataires tiers opèrent sous la supervision directe de la gouvernance de l'exercice (la *White Team* et la *TIBER Team* dans TIBER-EU ; le *Control Group* et le *Regulator* dans CBEST).
  - Cette étanchéité garantit que l'équipe défensive interne (*Blue Team*) n'intervient pas dans la préparation de l'attaque et ne

dispose d'aucune information préalable sur les actions des prestataires.

### Quels types d'attaques cible le cadre TIBER-EU ?

Le cadre **TIBER-EU** (*Threat Intelligence-Based Ethical Red Teaming*), développé par la Banque centrale européenne (BCE), s'adresse spécifiquement aux **institutions financières de l'Union européenne qui fournissent des infrastructures financières essentielles**.

Plutôt que d'imposer un ensemble fixe ou générique de tests, TIBER-EU cible des attaques strictement fondées sur le **renseignement sur les menaces (threat intelligence)** :

- **Attaques sur mesure et contextualisées** : Les simulations d'attaque sont personnalisées pour répliquer les menaces réelles et spécifiques auxquelles l'institution est confrontée dans son secteur et son environnement.
- **Reproduction des TTPs d'acteurs de menaces crédibles** : Une équipe tierce spécialisée en *Threat Intelligence* réalise une phase de reconnaissance de l'établissement pour établir la liste des acteurs de menaces réels (ex. groupes ciblant la fraude bancaire ou les systèmes de paiement) ainsi que leurs tactiques, techniques et procédures (TTP).
- **Émulation d'adversaires réels** : La *Red Team* s'appuie sur ces TTPs pour exécuter des scénarios d'attaque concrets afin de tester les capacités de prévention, de détection et de réponse de l'équipe défensive (*Blue Team*).

L'objectif principal de ce ciblage est d'identifier les forces et faiblesses de l'organisation pour élever sa maturité cyber et sa résilience face aux menaces réelles les plus susceptibles de la toucher.