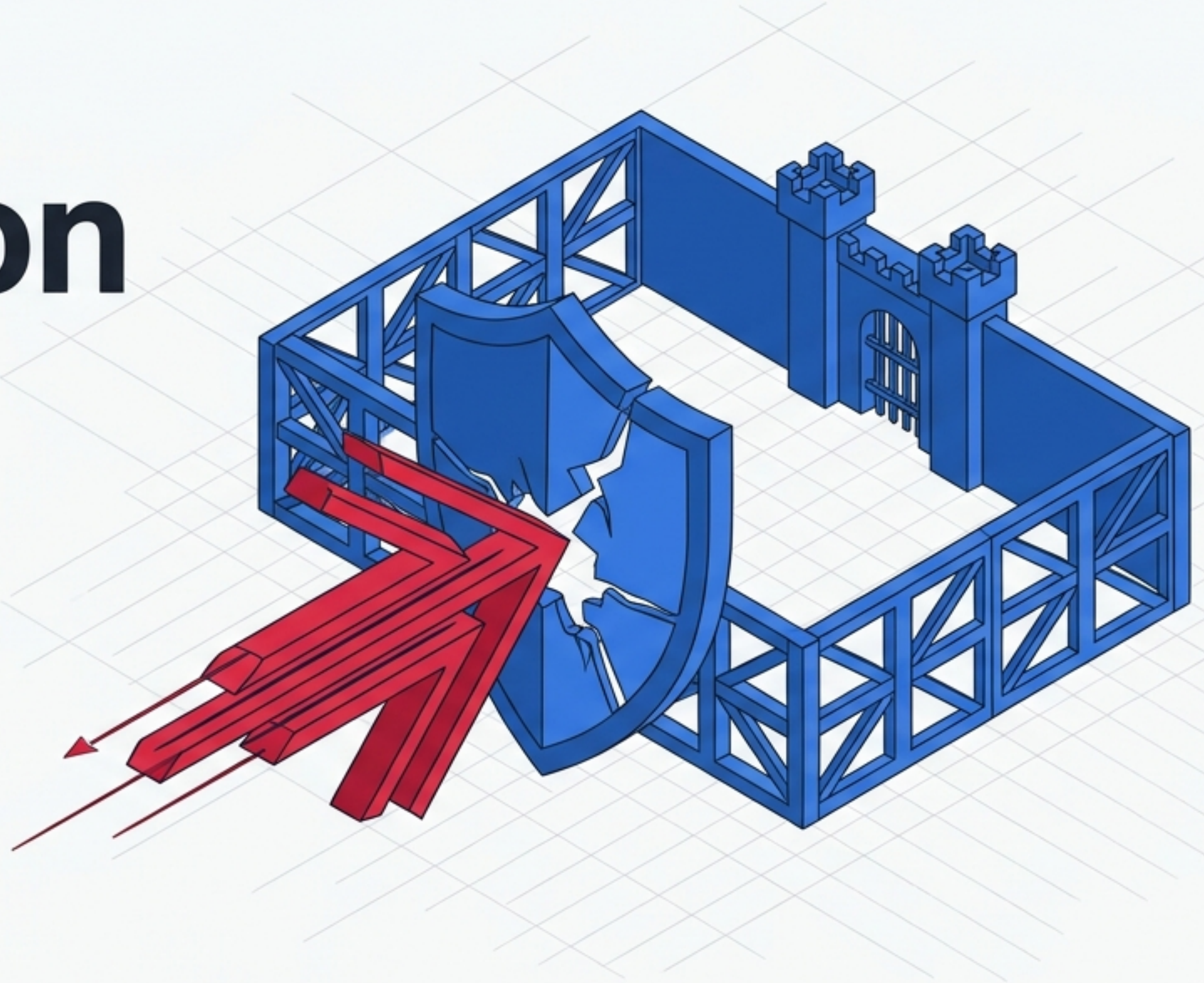


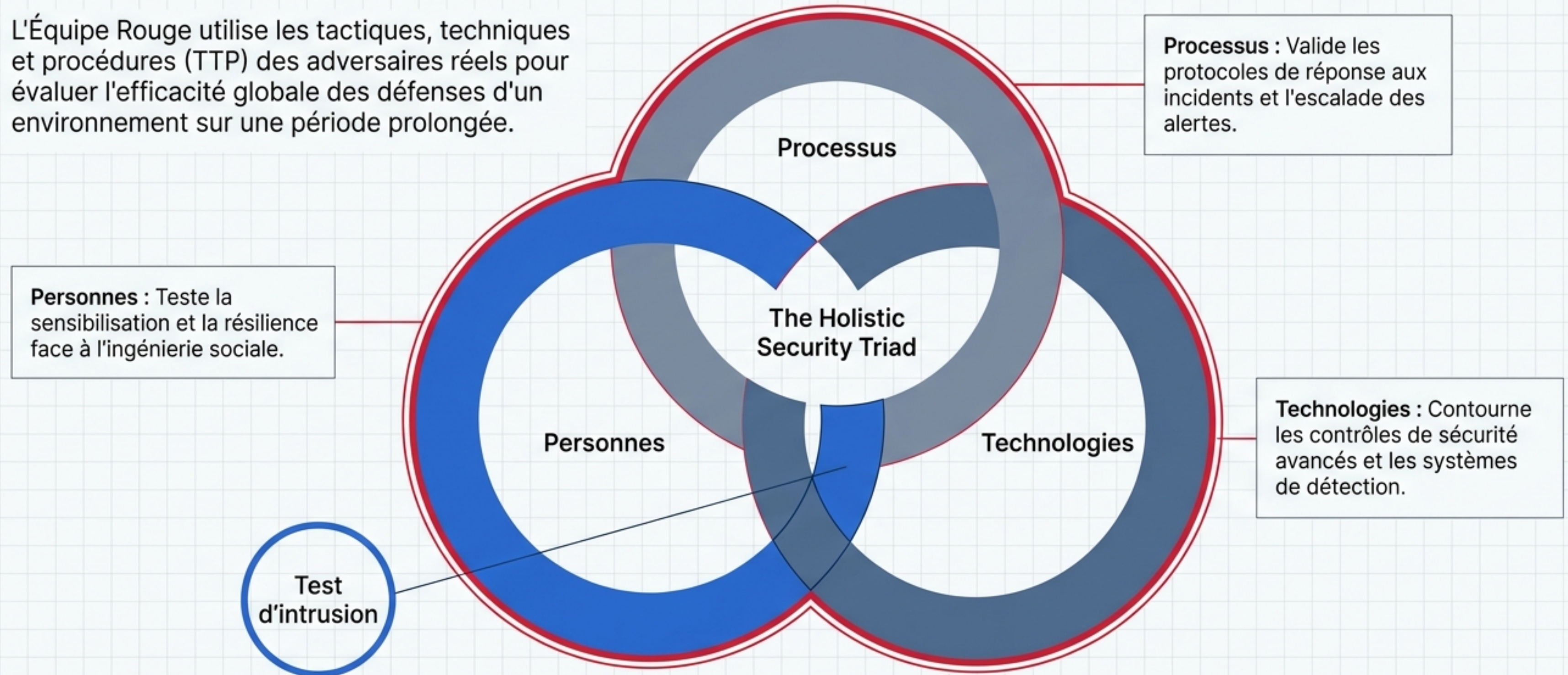
Introduction à l'Équipe Rouge

L'art de l'évaluation offensive
pour une cybersécurité
résiliente.



Plus qu'un simple test technique : une perspective d'adversaire.

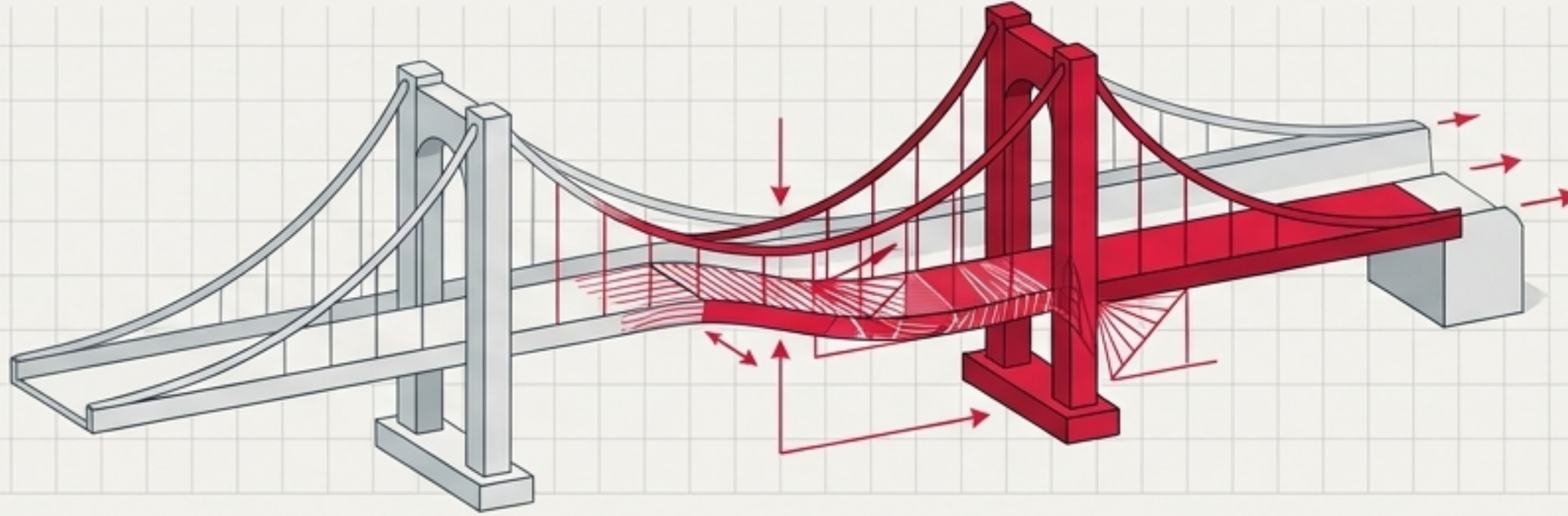
L'Équipe Rouge utilise les tactiques, techniques et procédures (TTP) des adversaires réels pour évaluer l'efficacité globale des défenses d'un environnement sur une période prolongée.



Ne confondez pas l'exploitation avec la simulation.

	Test d'Intrusion	Équipe Rouge
Objectif	Trouver un maximum de failles pour correction.	Atteindre un objectif spécifique en contournant la détection.
Portée & Approche	Limitée et contrôlée. Approche souvent bruyante et rapide.	Globale (Holistique). Approche furtive, créative et persistante (multi-étapes).
Cible Principale	Vulnérabilités technologiques isolées.	Capacités de détection et de réponse de l'organisation (Technologie + Humain + Processus).

Passer de la sécurité théorique à la résilience prouvée.



Identifier les Vulnérabilités Critiques

Garantit que les mesures de sécurité sont robustes face à des attaques complexes et multi-vectérielles, et pas seulement en isolation.

Remettre en Question les Hypothèses

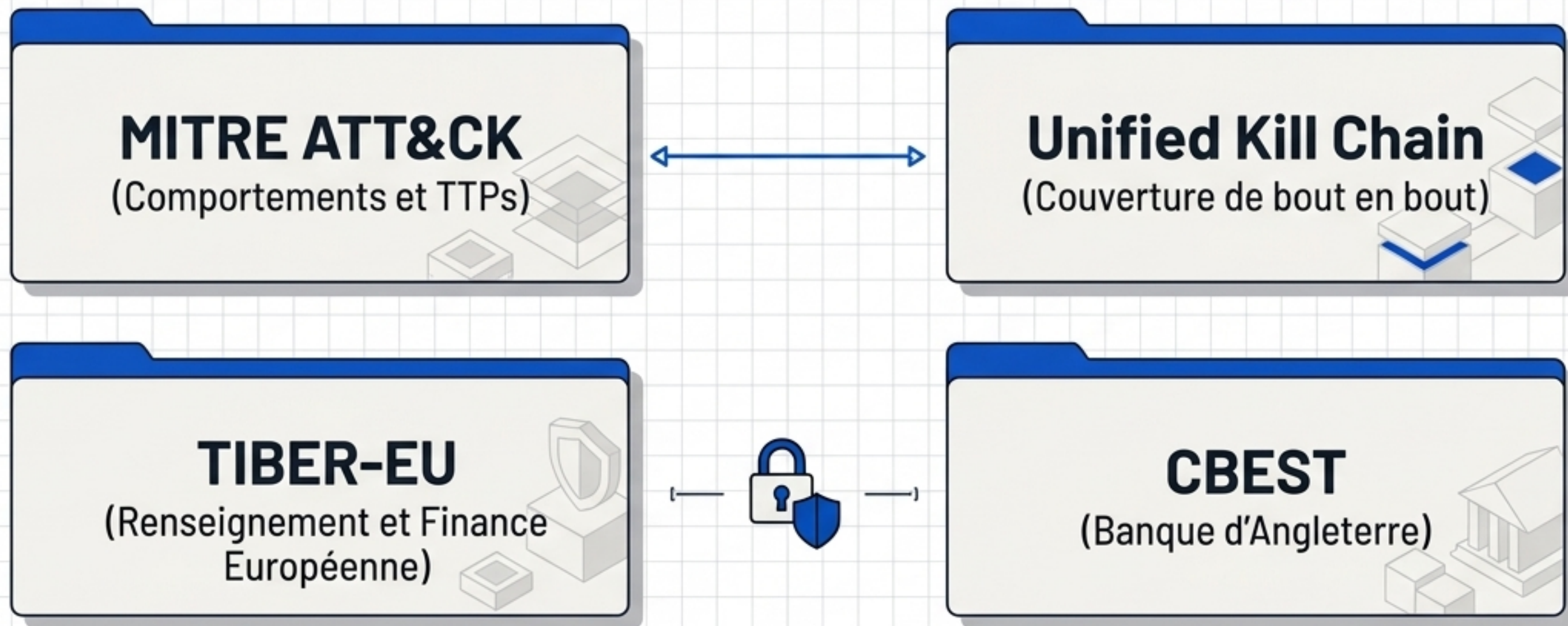
La sécurité basée sur la conformité est insuffisante.
Exemple : L'hypothèse qu'une authentification multifacteur (MFA) suffit peut être démentie par une Équipe Rouge utilisant l'hameçonnage de jetons (tokens) ou l'interception de SMS.

Émuler les Menaces Sectorielles

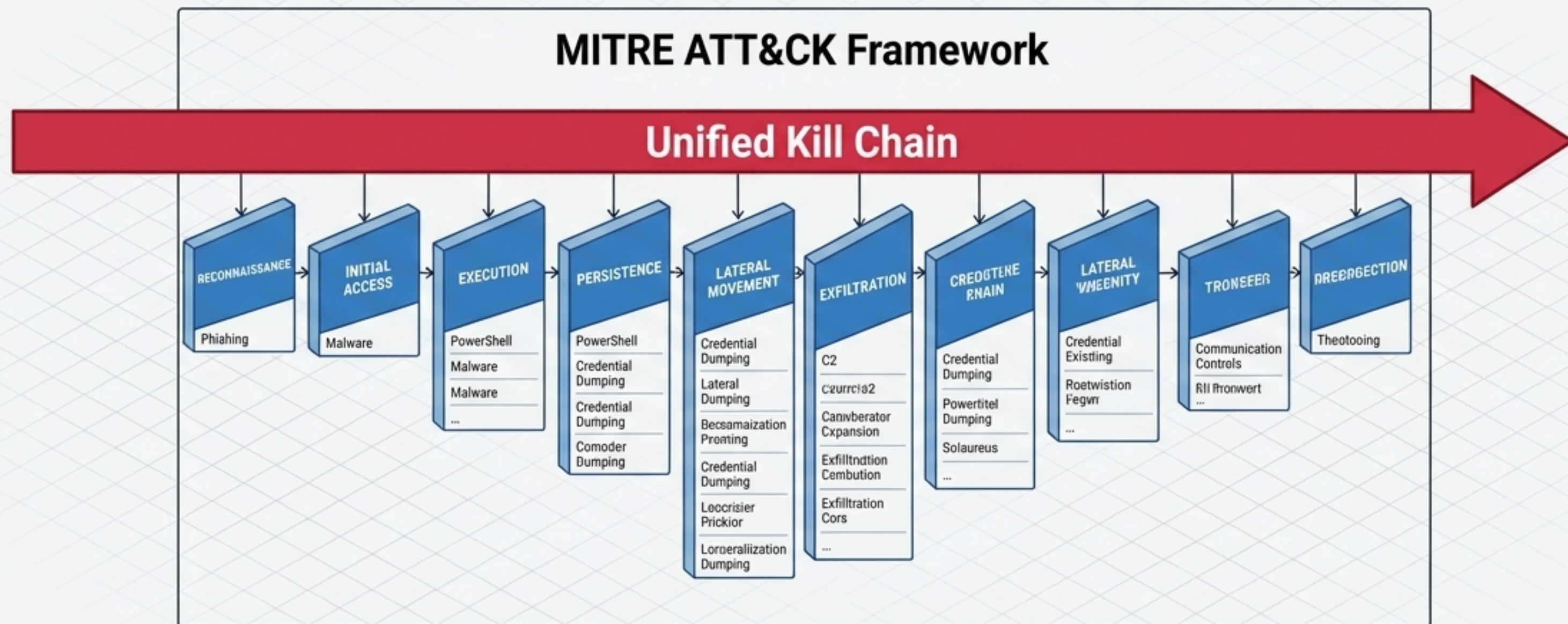
Aligner les tests sur la réalité du paysage des menaces.
Finance : Groupes spécialisés en fraude bancaire.
Santé : Ransomwares visant à perturber les systèmes critiques et exfiltrer les dossiers patients.

Standardiser l'attaque pour mieux communiquer la défense.

Les cadres méthodologiques comblent le fossé entre les opérations offensives et défensives. Ils fournissent un langage commun pour transformer les résultats techniques en ingénierie de détection.



De la technique isolée à la campagne globale



MITRE ATT&CK

La norme de l'industrie.

Catalogue systématiquement les comportements des adversaires à travers divers domaines (Entreprise, ICS, Mobile). Indispensable pour cartographier les activités et mesurer l'efficacité des contrôles.

Unified Kill Chain

L'approche holistique.

Intègre les aspects techniques et stratégiques. Lie les actions spécifiques (compromission initiale, mouvement latéral) aux objectifs globaux de l'adversaire, complétant ainsi MITRE en offrant un récit narratif unifié.

L'exigence de la haute finance : Les cadres basés sur le renseignement.



TIBER-EU (Europe)

- **Origine** : Banque Centrale Européenne (BCE).
- **Principe** : Utilise le renseignement sur les menaces pour adapter les tests. Nécessite l'intervention de tiers indépendants.
- **Écosystème (5 Équipes)** : Renseignement (3e partie, Crimson Red), Bleue (Interne, Cobalt Blue), Rouge (3e partie, Crimson Red), Blanche (Agents de confiance internes, Charcoal), TIBER (Conformité, Cobalt Blue).



CBEST (Royaume-Uni)

- **Origine** : Banque d'Angleterre.
- **Principe** : Le Fil d'Or (Golden Thread) — un lien traçable entre l'évaluation des menaces identifiées et les actions d'atténuation. Priorise les systèmes et fonctions critiques.
- **Écosystème (4 Acteurs)** : Fournisseur de Renseignement (Crimson Red), Fournisseur de Test d'Intrusion (Crimson Red), Groupe de Contrôle (Interne, Cobalt Blue), Régulateur (Cobalt Blue).

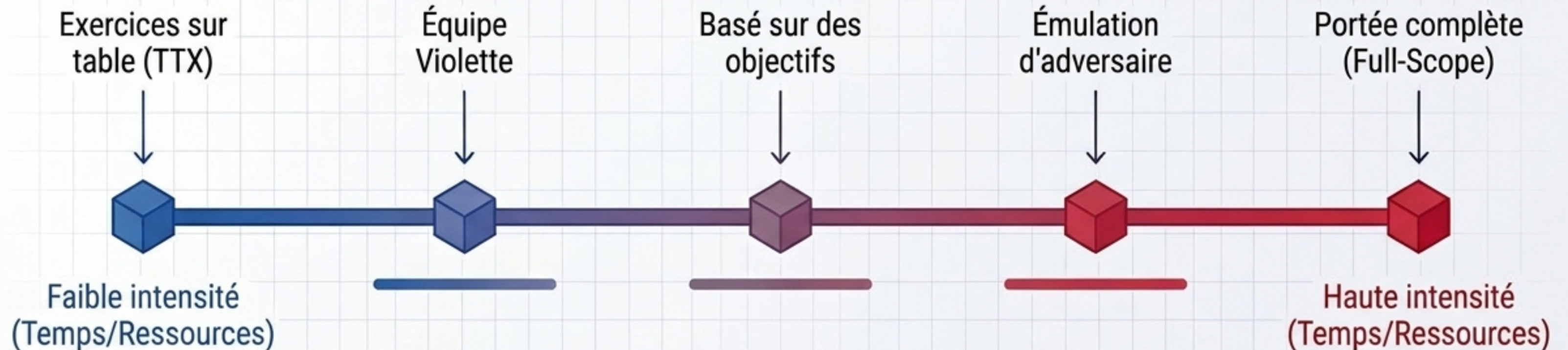
Le Spectre des Engagements : Choisir le bon outil.

Le choix de l'engagement dépend de la taille de l'organisation, de sa tolérance au risque et de ses objectifs. Utiliser un marteau pour visser une vis est inefficace.

Faible intensité
(Temps/Ressources)

The Engagement Spectrum

Haute intensité
(Temps/Ressources)



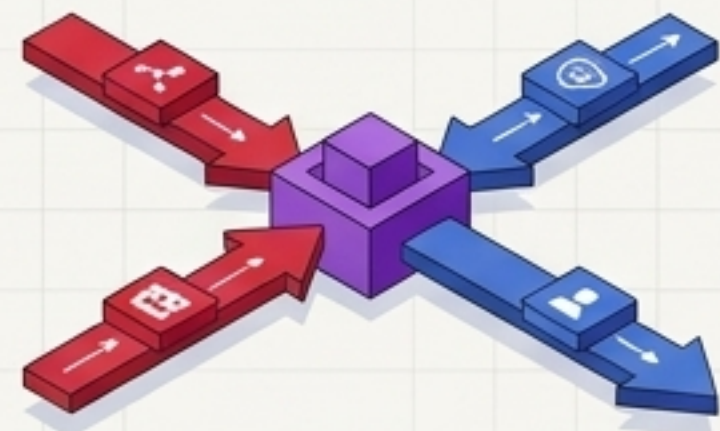
Préparation et Collaboration en Temps Réel.

Exercices sur Table (TTX)



- **Concept** : Simulations basées sur la discussion (ex: cyberattaque, catastrophe). Aucun déploiement technique.
- **Valeur** : Teste les politiques, la communication et la prise de décision. Identifie les lacunes des plans de réponse.

Équipe Violette (Purple Team)



- **Concept** : L'Équipe Rouge exécute l'attaque pendant que l'Équipe Bleue s'entraîne à la détection et à la réponse simultanément.

Tableau 2-4 : Avantages/Inconvénients de l'Engagement Équipe Violette

Avantages	Inconvénients
Collaboration en temps réel : Les équipes rouges et bleues travaillent ensemble, l'équipe rouge démontrant l'attaque tandis que l'équipe bleue s'entraîne à la détection et à la réponse.	Extrêmement gourmand en ressources : Une équipe violette efficace nécessite du personnel expérimenté des deux équipes, une coordination et du temps pour mener des exercices significatifs.
Rétroaction immédiate : Cette approche permet un retour immédiat, améliorant les contrôles de sécurité pendant l'exercice plutôt que lors de l'analyse post-exercice.	Risque de silos de connaissances sans documentation : Sans une documentation appropriée, des rapports et une formation croisée du personnel, les connaissances acquises au cours d'un exercice peuvent ne pas être diffusées au-delà des participants.
Culture d'amélioration continue : Le travail en équipe violette favorise une culture d'amélioration continue, permettant aux deux équipes de partager leurs connaissances et d'améliorer la posture de sécurité globale de manière itérative.	Potentiel de réalisme réduit (environnement de test vs production) : Lorsque les deux équipes sont conscientes des attaques simulées, la réponse peut ne pas être entièrement exécutée et testée. Cela peut être dû à des hypothèses et à l'utilisation d'un environnement de test qui ne reproduit pas la production.

Engagements Ciblés : Répondre aux risques d'affaires

Concept : Un objectif clair et défini (ex: exfiltrer la propriété intellectuelle ou contourner la sécurité physique) avec un début et une fin précis.



Avantages clés	Points de vigilance (Inconvénients)
• Résultats clairs et mesurables. • Optimisation efficace des ressources. • Alignement direct sur les risques commerciaux prioritaires. • Amélioration ciblée de la réponse aux incidents. • Adaptabilité rapide aux menaces émergentes.	• Portée étroite risquant d'ignorer d'autres vulnérabilités critiques. • Évaluation binaire (succès/échec) due à une dépendance excessive aux résultats prédéfinis. • Forte dépendance à une sélection pertinente de l'objectif initial.

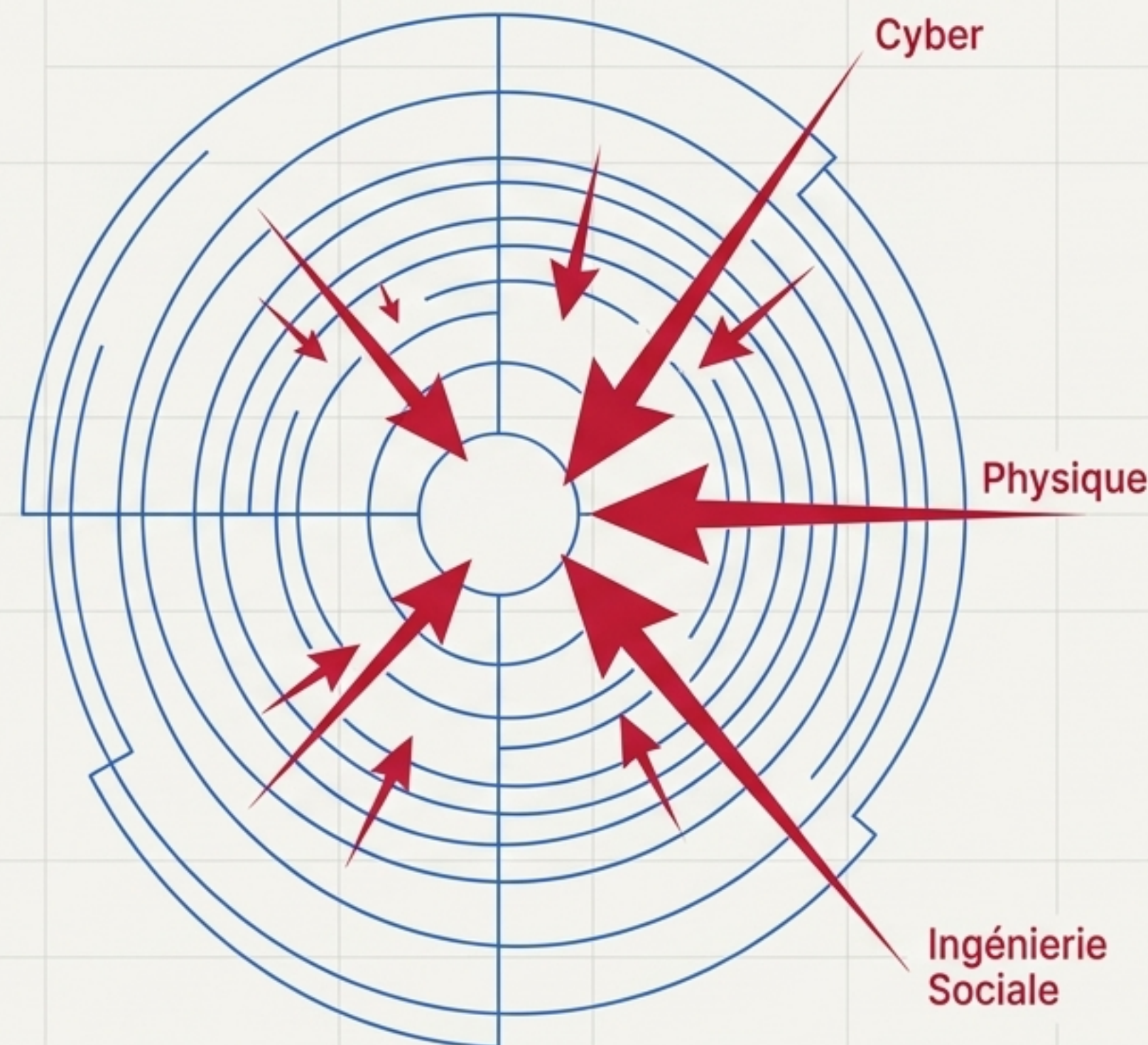
L'Épreuve Ultime : Émulation et Portée Complète.

Émulation d'Adversaire (Basé sur des scénarios)

- **Concept** : Imiter le cycle de vie complet d'un acteur de menace spécifique (ex: APT) basé sur le cyber-renseignement.
- **Avantages** : Pertinence ancrée dans le monde réel (TTPs actuels) ; vision holistique globale des défenses.
- **Inconvénients** : Portée très large diluant parfois l'attention ; difficulté à mesurer le succès face à des résultats multiples.

Portée Complète (Full-Scope)

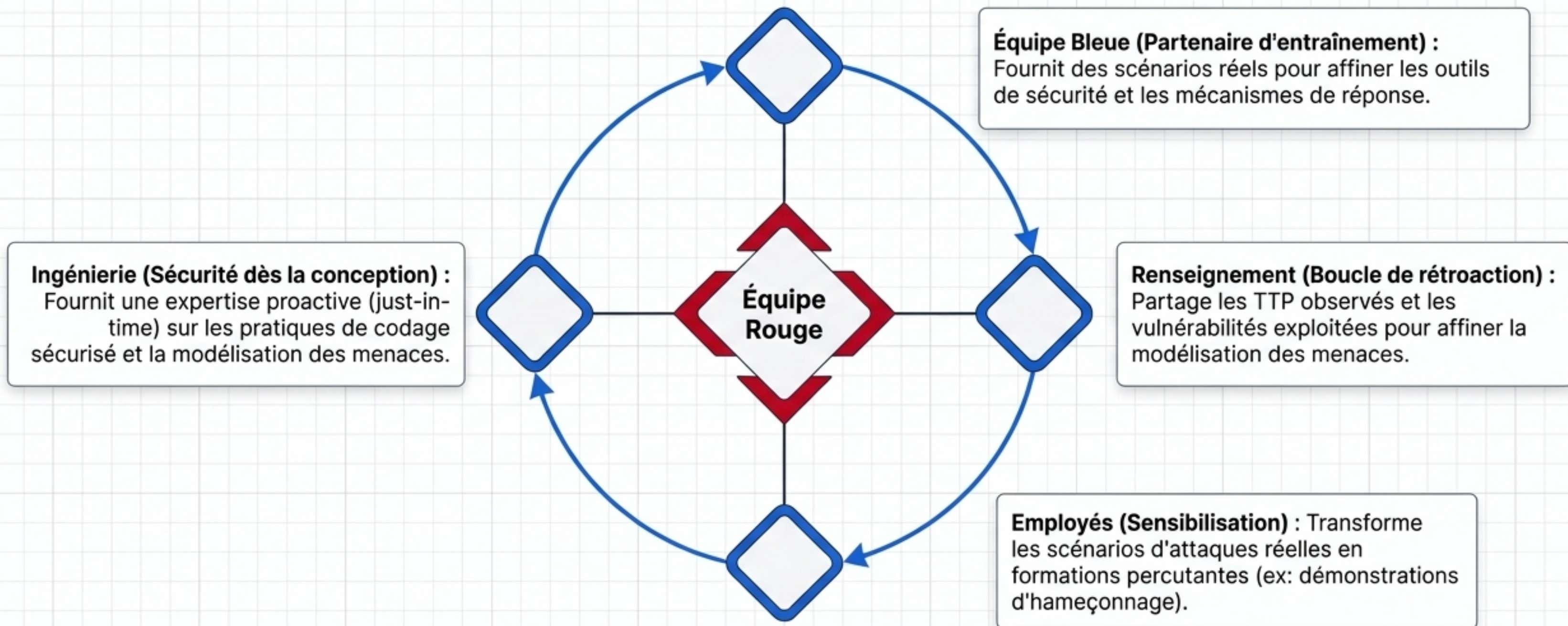
- **Concept** : L'engagement classique et le plus extensif. Utilise l'arsenal complet (cyber, physique, social).
- **Avantages** : Évaluation holistique absolue de la résilience globale sur de multiples vecteurs.
- **Inconvénients** : Extrêmement intense en ressources ; durée très longue (des mois pour la reconnaissance et l'ingénierie sociale).



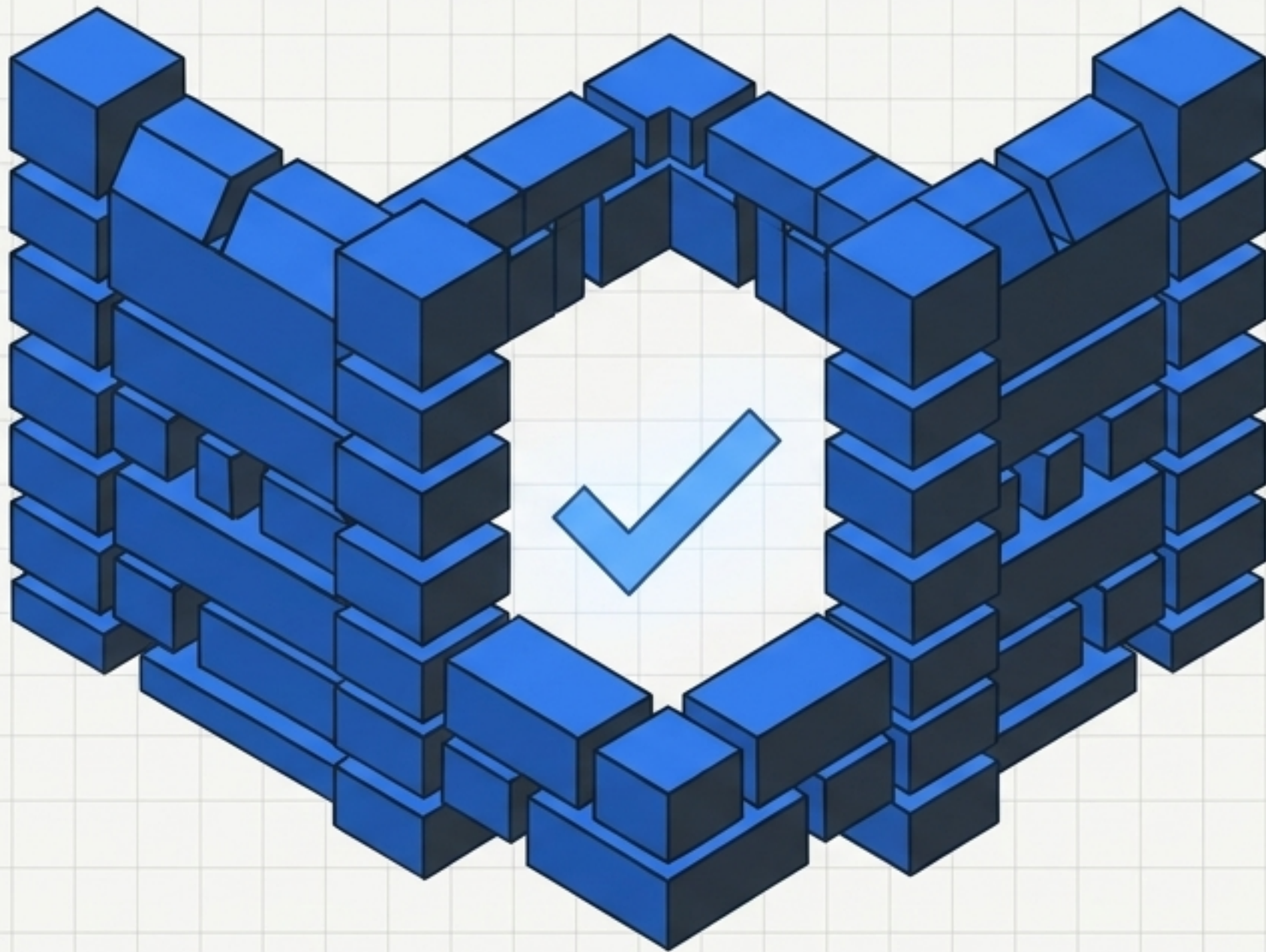
L'Écosystème de la Résilience : Un multiplicateur de force.

La véritable valeur d'une Équipe Rouge mature n'est pas seulement d'identifier des failles, mais d'élever le niveau de connaissances de toute l'organisation.

La Boucle de Rétroaction



Redéfinir le Succès : L'absence de failles n'est pas un échec.



Ne rien trouver lors d'un engagement est tout aussi instructif. C'est la validation ultime que vos contrôles de sécurité sont configurés et mis en œuvre correctement.

- ► **Célébrez la maturité** : Cela prouve l'efficacité d'un nouveau contrôle ou la réactivité de l'Équipe Bleue.
- ► **Expérimentez** : C'est l'occasion d'apprendre comment le système réagit sous un stress maîtrisé.
- ►► **Élevez la barre** : Profitez-en pour affiner la portée, réévaluer les risques et définir de nouveaux objectifs plus complexes pour le prochain engagement.

Résumé Stratégique : Bâtir une défense adaptative.



Le Périmètre : Allez au-delà des technologies. Une résilience prouvée exige de tester de manière holistique les individus, les processus et les infrastructures face à des attaques multi-vectorielles.



Les Fondations : Intégrez des méthodologies standardisées (ATT&CK, UKC, TIBER-EU, CBEST) pour transformer l'offensive en un langage compréhensible et exploitable par la défense.



L'Écosystème : Sélectionnez un engagement adapté à la maturité de votre organisation et utilisez les résultats pour alimenter la boucle de rétroaction avec vos équipes Bleue, Renseignement et Ingénierie.