RED TEAM

1 – Concept

Une équipe rouge de cybersécurité est un groupe d'individus simulant des cyberattaques réelles contre les systèmes et les défenses d'une organisation. L'objectif d'une équipe rouge est de tester les défenses de l'organisation et d'identifier les faiblesses ou les vulnérabilités qu'un véritable attaquant pourrait exploiter. Les équipes rouges utilisent généralement une variété de tactiques et de techniques, telles que l'ingénierie sociale, les tests de pénétration du réseau et les tests de sécurité physique, pour imiter les méthodes qu'un attaquant pourrait utiliser. Les résultats d'un exercice d'équipe rouge peuvent aider les organisations à améliorer leurs défenses et à mieux se préparer à d'éventuelles cyberattaques. Les équipes rouges sont souvent utilisées avec une « **équipe bleue** », qui est responsable de la défense des systèmes de l'organisation contre les attaques de **l'équipe rouge.**

1 – 1 - Comment une équipe rouge peut-elle aider les organisations à se protéger contre les cybermenaces?

L'objectif d'une équipe rouge est de tester les défenses de l'organisation et d'identifier les faiblesses ou les vulnérabilités qu'un véritable attaquant pourrait exploiter. Une équipe rouge utilise généralement une variété de tactiques et de techniques, telles que l'ingénierie sociale, les tests de pénétration réseau et les tests de sécurité physique, pour imiter les méthodes qu'un attaquant pourrait utiliser.

L'un des principaux moyens par lesquels une équipe rouge peut aider les entreprises à rester à l'abri des cybermenaces consiste à fournir un test réaliste des défenses de l'organisation. Une équipe rouge peut aider à identifier les faiblesses ou les vulnérabilités que les mesures de sécurité traditionnelles pourraient ne pas détecter en simulant des attaques réelles. Cela peut aider les organisations à hiérarchiser leurs efforts de sécurité et à se concentrer sur les zones les plus à risque.

En plus d'identifier les vulnérabilités, les équipes rouges peuvent aider les entreprises à améliorer leur posture de sécurité grâce à des recommandations d'amélioration. Après une simulation d'attaque, une équipe rouge peut fournir un rapport complet à l'organisation décrivant les vulnérabilités trouvées et offrant des suggestions pour y

remédier. Cela peut aider les entreprises à renforcer leurs défenses et à se préparer à des attaques potentielles.

De plus, les équipes rouges peuvent également aider les organisations à rester en sécurité grâce à la formation et à l'éducation des employés. En menant des exercices de « tir réel », une équipe rouge peut aider les employés à mieux comprendre les attaques qu'ils peuvent rencontrer et comment y répondre efficacement. Cela peut aider à améliorer la posture de sécurité globale de l'organisation et à accroître sa résilience aux cybermenaces.

1 – 2 - Quelle est la différence entre Blue Team et Red Team en matière de cybersécurité ?

La principale différence entre les équipes bleue et rouge réside dans leurs rôles et responsabilités. L'équipe bleue protège les systèmes informatiques et les réseaux d'une organisation contre les cyberattaques. Dans le même temps, l'équipe rouge simule des attaques pour tester l'efficacité des défenses de l'équipe bleue. Les activités de l'Équipe bleue peuvent inclure la mise en œuvre de contrôles de sécurité, la réalisation d'évaluations régulières de la sécurité et l'intervention en cas d'incidents de sécurité. Les activités de l'équipe rouge peuvent inclure la simulation d'attaques réelles, telles que des campagnes d'hameçonnage ou des infections de logiciels malveillants, et la fourniture de commentaires et de recommandations à l'équipe bleue. Les deux équipes travaillent ensemble pour améliorer la posture de cybersécurité d'une organisation et se préparer aux menaces potentielles.

La principale différence entre les équipes rouges et violettes en matière de cybersécurité réside dans leurs rôles et objectifs respectifs. Une équipe rouge est un groupe d'individus simulant des cyberattaques réelles contre les systèmes et les défenses d'une organisation. L'objectif d'une équipe rouge est de tester les défenses de l'organisation et d'identifier les faiblesses ou les vulnérabilités qu'un véritable attaquant pourrait exploiter.

En revanche, une équipe violette est un groupe de personnes responsables des fonctions des équipes rouge et bleue d'une organisation. Le but d'une équipe violette est de combler le fossé entre l'équipe rouge, qui simule les attaques, et l'équipe bleue, qui défend contre les attaques. Cela permet à l'équipe violette d'intégrer les idées et les enseignements tirés des simulations d'attaque de l'équipe rouge dans les stratégies de défense de l'équipe bleue et vice versa.

La principale différence entre les équipes rouges et violettes est que les équipes rouges se concentrent exclusivement sur la simulation d'attaques. En revanche, une équipe violette adopte une approche plus holistique, y compris la simulation d'attaque et la défense. Cela permet à une équipe violette d'identifier et de traiter les vulnérabilités plus efficacement et d'améliorer la posture de sécurité de l'organisation.

1 – 3 - Que fait une équipe rouge ?

L'objectif d'une équipe rouge est de tester les défenses de l'organisation et d'identifier les faiblesses ou les vulnérabilités qu'un véritable attaquant pourrait exploiter. Pour atteindre cet objectif, une équipe rouge utilise généralement une variété de tactiques et de techniques pour imiter les méthodes qu'un attaquant pourrait utiliser. Cela peut inclure l'ingénierie sociale, la pénétration du réseau et les tests de sécurité physique. L'équipe rouge utilisera ces méthodes pour tenter de violer les défenses de l'organisation et accéder à des données ou des systèmes sensibles.

Une fois que l'équipe rouge a effectué sa simulation d'attaque, elle fournira généralement à l'organisation un rapport détaillé décrivant les vulnérabilités découvertes et offrant des recommandations sur la façon de les résoudre. Cela peut aider l'organisation à améliorer ses défenses et à se préparer à des attaques potentielles. Voici une liste de ce que fait l'équipe rouge:

1. Simuler des cyberattaques réelles contre les systèmes et les défenses d'une organisation
2. Testez les défenses de l'organisation et identifiez les faiblesses ou les vulnérabilités qu'un véritable attaquant pourrait exploiter
3. Utilisez une variété de tactiques et de techniques pour imiter les méthodes qu'un attaquant pourrait utiliser, telles que l'ingénierie sociale et les tests de pénétration du réseau
4. Tentative de violation des défenses de l'organisation et d'accès à des données ou des systèmes sensibles
5. Fournir à l'organisation un rapport détaillé décrivant les vulnérabilités découvertes et offrant des recommandations sur la façon de les corriger.
6. Aidez l'organisation à améliorer ses défenses et à mieux se préparer aux attaques potentielles.

Dans l'ensemble, l'objectif d'une équipe rouge est de fournir aux organisations un test réaliste de leurs défenses et de les aider à identifier et à corriger les vulnérabilités avant qu'un véritable attaquant ne les exploite.

Pour plus d'informations sur l'équipe rouge et son essor dans toutes les industries, on recommande le livre ***Red Team*** de **Micah Zenko**.

1 – 4 - Quelles sont les compétences requises pour les membres de l'équipe rouge?

Les membres de l'équipe rouge sont généralement des personnes hautement qualifiées et expérimentées qui comprennent parfaitement les cybermenaces et les tactiques et techniques que les attaquants peuvent utiliser. En tant que tel, plusieurs compétences clés sont importantes pour les membres de l'équipe rouge. Certaines des compétences les plus importantes pour les membres de l'équipe rouge incluent:

- **Expertise technique** : Les membres de l'équipe Red doivent avoir une compréhension approfondie de divers aspects techniques de la cybersécurité, tels que la sécurité du réseau, le cryptage des données et la gestion des vulnérabilités.
- **Créativité et résolution de problèmes** : les membres de l'équipe rouge doivent sortir des sentiers battus et concevoir des moyens créatifs de simuler des attaques et de violer les défenses d'une organisation.
- **Communication et collaboration** : Les membres de l'équipe rouge doivent être en mesure de communiquer et de collaborer efficacement avec les autres membres de l'équipe, ainsi qu'avec l'équipe bleue de l'organisation et les autres parties prenantes.
- **Souci du détail** : Les membres de l'équipe rouge doivent être très attentifs aux détails pour identifier et exploiter les plus petites vulnérabilités.
- **Adaptabilité et flexibilité** : Les membres de l'équipe rouge doivent s'adapter aux conditions et aux scénarios changeants et passer rapidement à de nouvelles tactiques et techniques.

1 – 5 - Quels sont les types de hackers: Black Hat, White Hat & Gray Hat Hackers

Les types de pirates informatiques font référence aux différentes motivations, méthodes et éthique des individus qui se livrent à des activités de piratage. Les trois principales

catégories de types de hackers sont les hackers black hat, les hackers white hat et les hackers chapeau gris.

Les **pirates informatiques Black Hat** sont des individus qui se livrent à des activités de piratage illégales ou malveillantes, souvent pour voler des informations sensibles ou causer des dommages aux systèmes informatiques. Ils peuvent utiliser leurs compétences pour obtenir un accès non autorisé aux réseaux, voler des mots de passe ou des informations de carte de crédit, ou propager des logiciels malveillants. Les hackers Black Hat sont souvent motivés par le profit ou d'autres gains personnels, et leurs activités peuvent avoir de graves conséquences juridiques et financières.

D'autre part, les **pirates informatiques au chapeau blanc** s'engagent dans des activités de piratage éthiques, souvent pour améliorer la sécurité et se protéger contre les cyberattaques. Ils peuvent utiliser leurs compétences pour tester les défenses des systèmes et réseaux informatiques d'une organisation, identifier les vulnérabilités et fournir des recommandations d'amélioration. Les hackers White Hat sont souvent employés par des organisations ou embauchés comme consultants, et leurs activités sont généralement légales et sanctionnées.

Les **hackers au chapeau gris** se situent quelque part entre les hackers black hat et white hat. Ils peuvent se livrer à des activités de piratage qui ne sont pas strictement légales mais qui ne sont pas nécessairement malveillantes ou nuisibles. Par exemple, un pirate informatique au chapeau gris peut découvrir et signaler une faille de sécurité dans le système d'une organisation sans demander la permission ou une compensation ou peut se livrer à un « hacktivisme » en participant à des manifestations ou à d'autres activités politiques à l'aide de techniques de piratage. Les hackers au chapeau gris peuvent avoir une variété de motivations, et leurs activités peuvent parfois être difficiles à classer comme bonnes ou mauvaises.

1 – 6 – Historique

Le concept d'équipe rouge et d'équipe bleue est apparu au début des années 1960. L'un des premiers exemples d'équipe rouge impliquait le groupe de réflexion **RAND Corporation**, qui effectuait des simulations pour l'armée américaine pendant la guerre froide. L'« équipe rouge » et la couleur rouge sont utilisées pour représenter l'Union soviétique, et l'« équipe bleue » et la couleur bleue sont utilisées pour représenter les États-Unis. Un autre exemple précoce concernait le secrétaire américain à la Défense Robert McNamara, qui réuni une équipe rouge et une équipe bleue pour

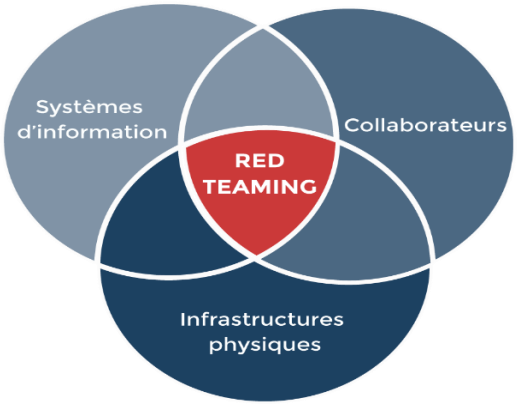
déterminer quel entrepreneur gouvernemental devrait se voir attribuer un contrat d'avion expérimental. Un autre exemple précoce modela la négociation d'un traité de maîtrise des armements et l'évaluation de son efficacité.

Au début des années 2000, il existe des exemples d'équipes rouges utilisées pour des exercices sur table. Un exercice sur table est souvent utilisé par les premiers intervenants et implique d'agir et de planifier les pires scénarios, comme si vous jouiez à un jeu de société sur table. En réponse aux attentats du 11 septembre, avec l'antiterrorisme à l'esprit, la Central Intelligence Agency créé une nouvelle cellule rouge, et des équipes rouges sont utilisées pour modéliser les réponses à la guerre asymétrique comme le terrorisme. En réponse aux échecs de la guerre en Irak, les équipes rouges deviennent courantes dans l'armée américaine

Au fil du temps, l'usage d'équipe rouge s'est étendue à d'autres industries et organisations, y compris les entreprises, les agences gouvernementales et les organisations à but non lucratif. L'approche est devenue de plus en plus populaire dans le monde de la cybersécurité, où les équipes rouges sont utilisées pour simuler des attaques réelles contre l'infrastructure numérique d'une organisation et tester l'efficacité de leurs mesures de cybersécurité.

2 – Le RED TEAMING

Le Red Teaming est la pratique qui consiste à tester la sécurité des systèmes en essayant de les pirater. Une Red Team (« équipe rouge ») peut être un groupe externe de pentesters (testeurs d'intrusion) ou une équipe au sein de votre propre organisation. Dans les deux cas, son rôle est le même : émuler un acteur réellement malveillant et tenter de pénétrer dans vos systèmes.



2 – 1 – Présentation du Red Teaming

Red Teaming teste vigoureusement les politiques, les plans, les systèmes et les hypothèses de sécurité à l'aide d'une approche contradictoire. Grâce à ces scénarios d'attaque, la stratégie de sécurité d'un système et sa réponse contre un attaquant sont visualisées en détail par un groupe externe d'experts en cybersécurité.

La méthode et l'objectif sont d'imiter un attaquant malveillant et de pénétrer dans le système d'une organisation. Cette simulation rend la méthodologie Red Team plus fiable car elle découvre les vulnérabilités du système et met en œuvre son exploitation possible.

les phases de red teaming choisies par toutes les Red Teams :

2 - 2 - Différentes phases du Red Teaming

2 – 2 – 1 - Collecte d'informations ou reconnaissance

Le processus de l'équipe rouge commence par une reconnaissance où les membres de l'équipe recueillent toutes les informations requises sur la cible. Ces informations comprennent :

des données personnelles telles que des identités, des adresses e-mail, des numéros de contact, etc. des salariés,

les détails des ports ou services ouverts, du fournisseur d'hébergement et de la plage IP du réseau externe,

Points de terminaison d'API, applications mobiles ou Web,

a déjà violé les informations d'identification, et

tout autre IoT ou système embarqué présent dans l'infrastructure de l'entreprise.

2 – 2 – 2 -Planification et cartographie de l'attaque

Une fois que l'équipe rouge acquiert des connaissances sur le système, elle cartographie les types de cyberattaques qui seront lancées et l'approche de leur exécution. Les facteurs pris en compte par ces équipes sont les suivants :

déterminer les sous-domaines cachés de l'accès public,

erreurs de configuration dans l'infrastructure cloud du client,

la vérification des informations d'identification faibles ou par défaut,

les risques qui existent dans le réseau ou les applications Web;

tactiques d'exploitation possibles pour toutes les faiblesses découvertes.

2 – 2 – 3 - Exécution de l'attaque et tests de pénétration

La grande quantité d'informations collectées au cours des phases précédentes sert de base à toutes les attaques ciblant le système. Ces attaques ciblent les services via :

problèmes de sécurité précédemment cartographiés,

compromettre les systèmes utilisés pour développer des applications,

l'accès aux serveurs du système à l'aide d'informations d'identification divulguées ou d'une approche par force brute,

cibler les employés qui utilisent des méthodologies d'ingénierie sociale, et attaquez les applications côté client.

2 – 2 – 4 - Rapports et documentation

Le reporting est la partie finale et la plus cruciale de l'ensemble du processus de l'équipe rouge, car il analyse et comprend les résultats de l'évaluation de l'équipe rouge. Le rapport contient idéalement une description des types de cyberattaques menées et de leur impact sur le système. Il répertorie les risques de sécurité et les vulnérabilités précédemment inconnus découverts au cours de la procédure.

Le rapport fournit également les mesures correctives que les organisations doivent prendre pour résoudre toutes les lacunes et les failles de sécurité présentes et les conséquences qui peuvent survenir si aucune solution n'est mise en œuvre.

2 – 3 - Avantages du red teaming

Les principaux avantages de l'exécution de la méthodologie Red Team dans une organisation sont les suivants:

- **Evaluati**on**:** Du système de **défense** de l'organisation tout en étant exposé à plusieurs cyberattaques, aide l'organisation à savoir à quel point ses politiques sont sécurisées.
- **Évaluation du risque:** La méthodologie Red Team permet de classer tous les actifs associés en fonction de leur niveau de risque**.**
- **Exposer les vulnérabilités :** Il aide à découvrir et à exposer tous les problèmes de sécurité et les failles **présentes dans le système**.
- **Augmentation du retour sur investissement :** Cela permet également **de** maximiser le retour sur investissement **réalisé dans la sécurisation**

d’une organisation. Les tests de l’équipe rouge évaluent le fonctionnement du système de sécurité de votre organisation en cas d’attaque.

- **Conformité:** L’analyse Red Team aide les entreprises à visualiser les zones de sécurité qui ne sont pas conformes aux normes réglementaires afin de les corriger au plus tôt.
- **Établissement des priorités :** Les tactiques de l’équipe rouge peuvent aider à hiérarchiser la correction des vulnérabilités, la mise en œuvre de mesures de cybersécurité et même les dépenses de sécurité.$

2 – 4 Quels sont les outils et tactiques courants de Red Teaming

Certaines des techniques courantes de l'équipe rouge comprennent :

- **Pentesting d'application**

  Le test d'intrusion d'applications fait référence au processus d'identification et d'exploitation des vulnérabilités au sein d'applications telles que les applications Web ou mobiles et leurs API pour comprendre l'impact des vulnérabilités actuelles. Ce processus contribue à sa correction rapide, réduisant ainsi les risques d'attaque réelle.

- **Ingénierie sociale**

  Il s'agit d'exploits effectués sur des personnes pour tenter d'obtenir d'elles des informations sensibles telles que des mots de passe ou des clés d'accès par le biais de manipulations. L'ingénierie sociale est généralement réalisée par le biais d'escroqueries par hameçonnage ou en fournissant des informations falsifiées.

- **Contrôles de sécurité physique**

  Il s'agit de contrôles effectués dans les locaux physiques d'un actif ou de son entreprise pour voir dans quelle mesure sa sécurité physique est bien entretenue. Les testeurs tentent de surmonter les contrôles de sécurité physiques mis en place pour accéder aux postes de travail et aux systèmes des employés.

- **Test de sécurité réseau**

  Ici, les réseaux sur lesquels opèrent divers actifs au sein d'une organisation sont soigneusement vérifiés pour détecter toute vulnérabilité qui pourrait le rendre vulnérable à une attaque entraînant une violation de données, une perte ou un vol.

2 – 5 - Comment fonctionne le Red Teaming ?

La meilleure façon de comprendre le fonctionnement précis du Red Teaming, c'est d'examiner le déroulement d'un exercice représentatif. Le processus typique suivi par une Red Team compte plusieurs étapes :

- **Une organisation** convient de l'objectif de l'exercice avec sa Red Team (interne ou externe). Par exemple, cet objectif peut être l'extraction d'informations sensibles sur un serveur particulier.
- **La Red Team** effectue ensuite une reconnaissance de la cible. Il en résulte une carte des systèmes cibles, notamment des services réseau, des applications Web et des portails employés.
- **Des vulnérabilités** sont alors découvertes dans un système cible, généralement exploitées au moyen de techniques de phishing ou encore de cross-site scripting (XSS).
- **Une fois des jetons d'accès valides** obtenus, la Red Team utilise son accès pour sonder d'autres vulnérabilités.
- **Si d'autres vulnérabilités** sont détectées, la Red Team s'efforce d'augmenter son niveau d'accès jusqu'au niveau requis pour accéder à la cible.
- **Une fois cette opération effectuée**, les données ou l'actif ciblés sont atteints.

En pratique, un membre expérimenté d'une Red Team utilisera un vaste choix de techniques pour chacune de ces étapes. Le principal point à retenir du scénario d'attaque ci-dessus, c'est que de petites vulnérabilités dans des systèmes uniques peuvent entraîner des pannes catastrophiques lorsqu'elles sont associées.

2 – 6 - Outils et tactiques courantes des Red Team

Lorsqu'il est mis en œuvre correctement, le Red Teaming constitue une attaque de grande envergure sur vos réseaux, utilisant tous les outils et techniques dont disposent les pirates informatiques, notamment les suivants :

- **Tests d'intrusion d'applications** : visent à identifier les failles des couches applicatives, telles que la falsification de requêtes intersites, les failles d'injection, la mauvaise gestion des sessions, et bien plus encore.

- **Tests d'intrusion du réseau** : visent à identifier les failles du réseau et des systèmes, notamment les mauvaises configurations, les vulnérabilités des réseaux sans fil, les services malveillants, etc.
- **Tests d'intrusion physique** : visent à vérifier la fiabilité et l'efficacité des contrôles de sécurité physique par exploitation en conditions réelles.
- **Tests d'ingénierie sociale** : visent à exploiter les faiblesses des personnes et de la nature humaine, à tester la sensibilité humaine à la persuasion et à la manipulation trompeuses, au moyen de tentatives de phishing par e-mail, téléphone et SMS, et du « pretexting » physique et sur site.
- **Tous les tests ci-dessus** : le **Red Teaming** est une simulation d'attaque complète sur plusieurs niveaux, conçue pour mesurer la capacité de votre personnel, de vos réseaux, de vos applications et de vos contrôles de sécurité physique à résister à l'attaque d'un adversaire réel.

2 – 7 – Outils de red teaming

- **Nmapname** – https://nmap.org

  Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau.

- **SQLmap** – https://sqlmap.org

  sqlmap est un outil de test d'intrusion open source qui automatise le processus de détection et d'exploitation des failles d'injection SQL et de prise en charge des serveurs de base de données. Il est livré avec un puissant moteur de détection, de nombreuses fonctionnalités de niche pour le testeur d'intrusion ultime et une large gamme de commutateurs allant de l'empreinte digitale de base de données, à la récupération de données à partir de la base de données, à l'accès au système de fichiers sous-jacent et à l'exécution de commandes sur le système d'exploitation via des connexions hors bande.

- **Niktro-** https://github.com/sullo/niktro

  Nikto est un scanner de serveur Web Open Source (GPL) qui effectue des tests complets sur les serveurs Web pour plusieurs éléments, y compris plus de 6700 fichiers / programmes potentiellement dangereux, vérifie les versions obsolètes de plus de 1250 serveurs et les problèmes spécifiques à la version sur plus de 270 serveurs. Il vérifie également les éléments de configuration du serveur tels

que la présence de plusieurs fichiers d'index, les options de serveur HTTP et tente d'identifier les serveurs Web et les logiciels installés. Les éléments d'analyse et les plug-ins sont fréquemment mis à jour et peuvent être mis à jour automatiquement.

- **OpenVas –** https://www.openvas.org

  Il signale les faiblesses potentielles ou avérées du matériel testé (machines, équipement réseau).
  OpenVAS est capable de scanner un équipement (machine ou matériel réseau), un ensemble d'équipements (à partir d'un fichier ou d'une plage IP) ou encore un réseau entier.
  Le résultat du scan fournira :
  la liste des vulnérabilités par niveaux de criticité,
  une description des vulnérabilités,
  et surtout la méthode ou un lien pour corriger le problème

- **Shodan** – https://www.shodan.io

  Shodan est un site web spécialisé dans la recherche d'objets connectés à Internet, et ayant donc une adresse IP visible sur le réseau. Il permet ainsi de trouver une variété de serveurs web, de routeurs ainsi que de nombreux périphériques tels que des imprimantes ou des caméras. Une telle requête est traitée avec une simple analyse de l'entête HTTP renvoyée par l'appareil ou le serveur[1]. Il est alors possible de récupérer des listes d'éléments spécifiques. Pour chaque résultat, on trouve l'adresse IP du serveur ainsi que d'autres types d'informations sensibles mais accessibles.
  Selon son créateur, John Matherly, ce site a été conçu pour permettre aux entreprises de « traquer » l'utilisation de leurs logiciels

- **Metasploit –** https://www.metasploit.com

  Le framework Metasploit est un outil open source, permettant la recherche, l'analyse et l'exploitation de vulnérabilités informatiques. Il dispose de nombreux modules et outils qui peuvent être très utiles dans le cadre de tests d'intrusions, que ce soit sur des applications Web ou sur le système informatique d'une entreprise. Il est utilisé par les professionnels de la sécurité pour tester la sécurité de leurs propres systèmes, mais également par les pirates informatiques pour pénétrer dans les systèmes d'autres personnes

2 – 8 – sociétés partenaires

- **OUTPOST24 -** https://outpost24.com/fr/services/red-teaming

  La totalité de nos évaluations Red Teaming sont effectuées par Ghost Labs – notre équipe interne de pirates éthiques. Lors d'une évaluation Red Teaming, notre équipe de sécurité offensive expérimentée travaillera avec vous afin de déterminer quels sont vos bien les plus précieux et tentera de les atteindre en utilisant les outils, tactiques et procédures des pirates informatiques. Nous évaluerons comment votre organisation (Blue Team) résiste aux différents

scénarios d'attaque, et nous en recueillerons les preuves pour un établir un rapport détaillé.

- **VARONIS – https://www.varonis.com/**
  Varonis Systems est une société de logiciels dont le siège est à New York et les bureaux de R&D à Herzliya, en Israël. La société développe une plate-forme logicielle de sécurité permettant aux organisations de gérer et de protéger leurs données non structurées[1]. Varonis effectue des analyses du comportement des utilisateurs (UBA) qui identifient les comportements anormaux liés aux cyberattaques[2]. Leur logiciel extrait les métadonnées de l'infrastructure informatique d'une entreprise et utilise ces informations pour cartographier les relations entre les employés, les objets de données, le contenu et l'utilisation
- **Intrinsec -** https://www.intrinsec.com/
  Intrinsec est pure-player du domaine de la cyber-sécurité ayant pour dessein la protection du métier de ses clients et ayant l'ambition de développer une posture d'excellence et de partenaire de référence chez ses clients. L'offre de service est développée pour traiter des enjeux de protection de l'information, des savoir-faire et des activités, de lutte contre les menaces numériques sous différentes formes (cyber criminalité, cyber défense, lutte contre la fraude...) et généralement de prise en compte de la cyber sécurité dans les activités de nos clients en tant que besoin ou opportunité.
  Spécialisations
  Information Security, Audit, Penetration testing, Consultancy, SOC, CERT, MSSP, Threat Intelligence, Incident Response, Forensic, Red Team, Purple **Team**, MSSP, CISO, Shared-Time CISO, Awareness, FR/EU Compliance, Data leaks, CTI, Threat Hunting, Crisis management, EDR, MDR et Vulnerability management
- **CrowdStrike -** https://www.crowdstrike.fr/
  Le mélange unique de CrowdStrike de services, de technologie et d'intelligence de premier ordre permet à **son équipe rouge** de cibler stratégiquement les zones et les vecteurs d'attaque les plus pertinents pour votre organisation, sur la base des informations réelles et de notre expérience de réponse aux incidents dans le monde réel. Plutôt que de s'appuyer sur des tactiques, des techniques et des procédures à l'emporte-pièce, CrowdStrike utilise des renseignements sur les dernières attaques rencontrées par ses intervenants sur le terrain et celles identifiées par l'équipe interne de renseignement sur les menaces de l'entreprise.
- **Intrinsec -** https://www.intrinsec.com/red-team/

3 -Test d'intrusion

On confond souvent Red Teaming et tests d'intrusion, mais les deux techniques sont légèrement différentes. Ou, plus précisément, les tests d'intrusion ne sont que l'une des techniques pouvant être utilisées par les Red Team.

Communément appelé « pentest » (de l'anglais « Penetration Testing »), **le test d'intrusion est un audit de cybersécurité** dont l'objectif est de mettre à l'épreuve une application ou un système d'information face à des attaques réalistes.

Cette méthode est utilisée en sécurité informatique pour identifier les vulnérabilités d'un système d'information. Le test d'intrusion consiste à se mettre dans la peau d'un pirate (hacker) malveillant et d'essayer de pénétrer une cible donnée qui sera, dans ce cas, le client.

La cible peut être de différent type : une IP, une application, un serveur web ou encore un réseau complet.

Un test d'intrusion peut inclure des tests en boite noire, en boite grise ou en boite blanche. Les tests en boite noire ciblent la surface d'attaque accessible à n'importe quel attaquant externe, tandis que des tests en boite grise vont concerner des éléments disponibles uniquement à des clients, des partenaires ou des salariés d'une entreprise. L'audit en boite blanche quant à lui permet d'analyser le niveau de sécurité en disposant des mêmes accès qu'un administrateur du système (serveur, application…).

Grâce à ces tests en découle un rapport indiquant les vulnérabilités identifiées et classifiées par niveau de criticité ainsi qu'un plan d'actions à suivre pour remédier techniquement aux vulnérabilités soulevées.

3 - 1 Quand effectuer un test d'intrusion ?

La plupart des entreprises attendent de soupçonner une cyberattaque ou un piratage pour mener un test d'intrusion. **Nous conseillons fortement d'être proactif en effectuant un test d'intrusion** afin d'être informé à l'avance des menaces qui pourraient peser sur votre organisation.

Après avoir réalisé le premier test, souvent se pose la question de la fréquence. Celle-ci est à adapter selon l'entreprise, la criticité de ses données, les enjeux réglementaires ou encore selon la fréquence des évolutions techniques et fonctionnelles réalisées.

Dans certains cas, le choix sera d'un pentest par mois, dans d'autres cas ce sera un pentest par an.

Une entreprise hébergeant des données de santé sera plus souvent soumise à la réalisation d'un test d'intrusion plutôt qu'un éditeur de logiciel par exemple.

3 – 2 - Méthodologie d'un test d'intrusion

Le PTES (Penetration Testing Execution Standard) ,est un ensemble générique de bonnes pratiques qui établissent les principes fondamentaux pour la bonne réalisation d'un test d'intrusion. Le mot "générique" est important ici car le PTES peut aussi bien être appliqué lors d'un pentest d'une application mobile que lors d'un test d'intrusion dans les locaux d'une entreprise**.**

Le PTES décompose chaque pentest en 7 grandes étapes **:**

➢ Les interactions avec le pentest

Cette phase regroupe l'ensemble des échanges, les accords contractuels et financiers, l'établissement des canaux de communication sécurisés ainsi que la préparation du pentest.
L'objectif est d'établir un cadre légal, technique et organisationnel, validé par le client et le prestataire et ainsi garantir une réalisation à hauteur des attentes des deux partie

➢ La collecte d'informations

C'est une phase très importante pour chaque pentest car elle permet d'identifier les cibles potentielles, d'amasser des informations utiles lors des étapes postérieures et d'identifier dès le départ de possibles pistes d'attaque via des méthodes telles que l'énumération réseau, l'identification du système d'exploitation, les requêtes Whois, les requêtes SNMP, le scan de ports, etc.). Les informations obtenues sur la cible procurent ainsi de précieuses indications sur les processus de sécurité mis en place.

➢ La modélisation des menaces

l'objectif de cette phase est d'identifier les principales cibles au sein d'une entreprise (aussi bien en termes d'actifs qu'en termes de processus) et les sources de menaces les plus probables (leur origine et leur capacités techniques).

➢ L'analyse de vulnérabilité

rès avoir identifié le type d'attaque le plus efficace à mener contre la cible, il faut maintenant savoir comment y accéder. Au cours de cette étape, les informations collectées lors des phases précédentes sont mises en relation pour déterminer si l'attaque choisie est réalisable. Les informations recueillies grâce à des scans de ports, des scans de vulnérabilités, ou celles issues de la collecte de renseignements sont notamment prises en considération.

➢ L'exploitation

La variété de scénarios d'exploitations est très large. Elle dépend du type de pentest et des cibles et peut aller des attaques sur les acteurs humains (phishing, usurpation d'identité) jusqu'à la recherche de failles "0 day" si toutes les autres méthodes ont échoué en passant par de la rétro-ingénierie, la manipulation de requêtes, la mise en place de scénarios "Man in the Middle" ou le fuzzing (injections de données erronées). Le tout en essayant d'éviter les moyens de protection et de détection en place si les conditions du pentest l'exigent.
Le pentesteur doit toujours vérifier que les techniques d'exploitations utilisées correspondent au périmètre et aux conditions d'engagement convenues avec le client.

➢ La phase post-exploitation

La phase postérieure à l'exploitation est une phase critique dans un test d'intrusion. Elle commence après l'intrusion dans le système attaqué et consiste à déterminer sur celui-ci les informations qui ont le plus de valeur. Il s'agit de montrer l'impact financier que pourrait avoir une fuite ou une perte de ces informations sur l'entreprise.

- **Le rapport**

  La phase d'élaboration du rapport est sans nul doute la phase la plus importante d'un test d'intrusion, car l'intérêt de sa réalisation doit s'y trouver justifié. Le rapport établit ce qui a été réalisé lors du test d'intrusion ainsi que la manière utilisée. Il doit surtout mettre en lumière quelles sont les faiblesses à corriger et comment le système cible peut être protégé contre de telles attaques.

4 – Projet "DEFENSE FRANCE" - https://redteamdefense.org/

La Red Team Défense offre une projection dans le futur au ministère des Armées. Elle anticipe les risques technologiques, économiques, sociétaux et environnementaux susceptibles d'engendrer de potentielles conflictualités à l'horizon 2030-2060. Elle est pilotée par l'agence de l'innovation de défense (AID) en coopération avec l'État-major des armées (EMA), la Direction générale de l'armement (DGA) et la Direction générale des relations internationales et de la stratégie (DGRIS)

Ce programme lancé en 2019 par le ministère des Armées est composé d'auteurs, de scénaristes et de dessinateurs de science-fiction indépendants qui imaginent des scénarios de menaces du futur. La Red Team travaille étroitement avec des experts scientifiques de l'Université Paris Sciences & Lettres (PSL) et des militaires, pour mieux se préparer aux réponses et contrer ces éventuellement menaces.

4 – 1 – composition du projet

Au terme d'une procédure de dialogue compétitif, l'Université Paris sciences & lettres (PSL) a été retenue par le ministère des Armées pour constituer les équipes, les animer et en restituer les travaux. Ce réseau est piloté par Cédric Denis-Remis, vice-Président Développement, innovation et entrepreneuriat de l'Université PSL Pour Alain Fuchs, Président de l'Université PSL, « L'invention de l'avenir est une mission essentielle de l'Université. La caractéristique de PSL est sa capacité à croiser sciences dures, ingénierie, arts, sciences humaines et sociales. Cette interdisciplinarité fait d'elle un lieu idéal pour allier science et imagination et les mettre au service de l'action publique ». L'auteur de polar DOA, la sociologue et directrice de recherche au CNRS Virginie Tournay, les auteurs de space opera Laurent Genefort et Romain Lucazeau, le scénariste de BD Xavier Dorison, le romancier Xavier Mauméjean, le dessinateur François Schuiten, ainsi que la designeuse Jeanne Bregeon ont conçu les deux scripts de la première saison : Chronique d'une mort culturelle annoncée, anticipation d'une société de communautés virtuelles sur fond d'attaque bioterroriste, et La Sublime Porte s'ouvre à nouveau, anticipation d'une révolution technologique qui bouleverse les pratiques de guerre.

4 – 2 – les différents scénarios

4 – 2 – 1- Scénarios de la saison 0

La saison 0 s'intéresse aux nouveaux pirates.

#1- scénario : P-nation

aborde de nombreux sujets et envisage la création d'un ascenseur spatial sur la base de Kourou, en Guyane française aux alentours de 2030, dans le but de relancer la course à l'espace. La construction de dizaines de milliers de kilomètres de câbles de carbone doit permettre de faire baisser les prix de l'accès à l'espace et de faciliter l'exploitation minière de la Lune, de Mars, et de la ceinture d'astéroïdes. De même, le puçage se généralise. Une puce contenant les données médicales, financières et civiles des individus permet d'augmenter la sécurité face aux migrations massives de la population. Mais certaines personnes résistent à cette politique et deviennent une nation pirate, apatride, menant une guerre contre l'État. Ce scénario envisage une menace à moyen terme, reposant sur la contestation d'une politique sécuritaire radicale.

#2 – scénario 2 :Barbaresque 3.0,

les auteurs envisagent la création d'un protocole d'interface neurale développé par le ministère des Armées à partir de 2026. Cette technologie est issue des recherches de Neuralink, l'entreprise d'Elon Musk spécialisée dans les neurotechnologies. Le NeTAM (Neuro Terre Air Mer) permet aux militaires de diriger des systèmes d'armement. Toutefois, des hackers parviennent à s'introduire dans ce système et à prendre le contrôle d'équipements miliaires.

La saison 0 montre l'intérêt de l'armée française pour les individus agissant en réaction à l'autorité de l'État et pouvant constituer une menace pour la sécurité intérieure.

4 – 2 - 2 - Scénarios de la saison 1

#1 Scénario ruse : Chronique d'une mort culturelle annoncée

Le développement de bulles communautaires, ou *safe sphères* (REZ), a profondément modifié le rapport à la réalité. Les individus peuvent désormais se plonger selon leurs affinités et intérêts (religieux, identitaires…) dans des réalités alternatives dépendantes de la subjectivité de leur communauté d'appartenance. En 2040, 90 % des Européens y sont connectés, si bien qu'il n'y a plus de réel commun partagé. À Grande-City, l'État s'efface face aux *safe sphères* et une balkanisation de la population s'opère. En 2045, la menace d'une attaque bioterroriste finit de déstabiliser la ville, déjà ravagée par une crue centennale. Une véritable guerre cognitive s'enclenche entre *safe sphères* concurrentes, où les croisements d'informations et les diffamations sont monnaie courante.

L'armée française intervient dans ce climat particulièrement instable et incertain pour évacuer des populations sous mandat de l'Union Européenne. C'est l'opération **Omanyd.** Une opération extérieure qui fait face à de nombreux défis : absence d'informations fiables sur le terrain, défiance des populations à évacuer, contestation des populations nationales face au rapatriement de civils potentiellement infectés… L'armée française doit conjointement assurer la réussite de l'opération et convaincre de

la légitimité de son intervention. Après ce premier temps d'opération relativement rapide, faisant face à l'urgence de la situation biologique à Grande-city, les armées françaises sont sollicitées pour aider l'ancien pouvoir en place à sécuriser le réel, c'est-à-dire à réduire l'influence des safe sphères sur les populations locales. Plusieurs années seront nécessaires pour désactiver les safe sphères les plus virulentes

#2 Hyperforteresse : La Sublime Porte s'ouvre à nouveau

Autour de la Méditerranée les forces politiques et économiques se recomposent. Après une période d'instabilité, une junte nationaliste prend le pouvoir à Troie. Dans leur volonté d'étendre la sphère d'influence de la puissance troyenne, ces officiers tournent leurs appétits vers les cités périphériques. Face à cette menace, les Ioniens et les Thraces se réarment, avec l'appui de Carthage qui investit lourdement dans son programme « Salambo », visant à doter la frontière orientale de l'Europe d'un réseau impénétrable d'hyperforteresses.

Ces nouveaux systèmes défensifs ont été créés pour contrer la généralisation des armes hypervéloces. Ces engins, capables d'atteindre des vitesses vertigineuses, redéfinissent les règles du combat. Ils constituent une épée de Damoclès permanente. Afin de s'en protéger, les belligérants développent des dispositifs de défense sophistiqués dans lesquels systèmes de détection et de protection s'entremêlent. À la fin des années 40, ce réseau de technologies a un nom : **l'hyperforteresse.**

Pendant des années, le conflit s'enlise. Les hyperforteresses adverses se font face, sans qu'aucune ne parvienne à avancer. Seule une attaque troyenne en 2043 touche et à endommage un vaisseau carthaginois. S'en suivent des contre-attaques, mais Ioniens et Thraces se brisent sur le réseau d'hyperforteresses troyen. Cyberattaque, mission de sabotage, infiltration… différentes tactiques se déploient pour percer les lignes ennemies jusqu'à l'explosion d'une arme nucléaire rustique dans l'atmosphère et l'intervention de Carthage en soutien à ses alliés ioniens et thraces

4 – 2 – 3 – Scénarios de la saison 2

 # Scénario 1 : Après la nuit carbonique.

Urgence dans la jungle. Une équipe de scientifiques fait face à l'assaut de rebelles et doit être rapidement rapatriée. L'opération d'exfiltration se situe dans un contexte de tensions internationales qui a provoqué une réglementation drastique de la consommation énergétique. Les forces armées devront intervenir rapidement en utilisant des technologies très peu énergivores. Face aux attaques répétées des rebelles et à la destruction progressive de leur matériel, les soldats arriveront-t-ils à conserver assez d'énergie pour libérer les scientifiques avant le début de la mousson ?

 # Scénario 2 : Une guerre écosystémique.

La nature se rebelle. Des manipulations biogénétiques à usages ciblés ont provoqué des effets désastreux. Incontrôlable, la nature s'est transformée en zones vertes mortifères qui s'étendent dorénavant sur l'ensemble du terrain d'opération. La mission des armées est bouleversée. Plus qu'intervenir dans des zones devenues dangereuses,

elles doivent maintenant gérer les effets d'un Tchernobyl vert de plus en plus menaçant.

4 – 2 – 4 – saison 3 (et dernière)

Pour cette troisième et dernière saison, les scénarios sont construits autour de 2 thématiques : la conflictualité dans l'espace et l'accès massif et immédiat aux compétences.

#1 - Scénario 1 : « La ruée vers l'espace »

la ruée vers l'espace » imagine une montée des tensions et de la conflictualité entre différents acteurs dans leurs conquêtes du domaine spatial à des fins économiques et de puissance.

Ce scénario projette une explosion de la démocratisation de l'accès à l'espace à la suite d'innovations industrielles et technologiques. Les ressources spatiales, tant sur la Lune que dans les ceintures d'astéroïdes plus lointaines, deviennent abordables et nourrissent les appétits industriels et économiques d'acteurs étatiques et privés. Des rapprochements s'opèrent, des alliances se créent pour assurer leur exploitation. Cette course aux ressources aboutit à une compétition économique qui se traduit par des pratiques de sabotage et de déni d'accès, avant d'escalader vers une confrontation spatiale ouverte. Dans ce contexte, quel serait le seuil de déclenchement d'une guerre spatiale ?

2 - Scénario 2 : « Face à l'Hydre »

Le scénario imagine l'eshu, implant d'un nouveau genre qui permet l'assimilation instantanée de nouvelles connaissances pour tout individu qui en est équipé. Ces connaissances sont réversibles et n'influent en rien les volontés individuelles. Peu à peu, ces implants se diffusent et leur utilisation se généralise dans certaines régions. Ils deviennent des leviers de création ad hoc et immédiate d'une armée à partir de populations civiles par l'injection de savoirs militaires. Cette armée prend le nom de l'Hydre, empruntant à l'animal mythologique sa capacité à se renouveler constamment, chaque individu volontaire pouvant s'implanter à tout moment des connaissances adéquates en fonction du besoin. Progressivement, les capacités de l'eshu s'étendent et ouvrent la voie à la possibilité d'un agir collectif : les individus dotés d'un eshu communiquent les uns avec les autres de manière décentralisée et instantanée, voire symbiotique.

4 -3 – PLS : mettre d'œuvre

Lancée à l'été 2019, l'initiative Red Team est un exercice de prospective innovant dont l'objectif est de nourrir les réflexions stratégiques, opérationnelles, technologiques et organisationnelles du ministère des Armées et d'acteurs extérieurs. Ses travaux se répartissent en quatre saisons et mobilisent auteurs et scénaristes de science-fiction, experts scientifiques et militaires.

Au terme d'une procédure de dialogue compétitif, **l'Université Paris sciences & lettres** (PSL) a été retenue par le ministère des Armées pour constituer les équipes, les animer

et en restituer les travaux. Ce réseau est piloté par Cédric Denis-Remis, vice-Président Développement, innovation et entrepreneuriat de l'Université PSL.
Pour Alain Fuchs, Président de l'Université PSL, *« L'invention de l'avenir est une mission essentielle de l'Université. La caractéristique de PSL est sa capacité à croiser sciences dures, ingénierie, arts, sciences humaines et sociales. Cette interdisciplinarité fait d'elle un lieu idéal pour allier science et imagination et les mettre au service de l'action publique »*.
L'auteur de polar DOA, la sociologue et directrice de recherche au CNRS Virginie Tournay, les auteurs de *space opera* Laurent Genefort et Romain Lucazeau, le scénariste de BD Xavier Dorison, le romancier Xavier Mauméjean, le dessinateur François Schuiten, ainsi que la designeuse Jeanne Bregeon ont conçu les deux scripts de la première saison : Chronique d'une mort culturelle annoncée, anticipation d'une société de communautés virtuelles sur fond d'attaque bioterroriste, et La Sublime Porte s'ouvre à nouveau, anticipation d'une révolution technologique qui bouleverse les pratiques de guerre.
L'annexe 2 donne les éléments caractéristiques de l'université Paris Science & lettre,

Annexe 1 : Bibliographie

- https://www.sentinelone.com/cybersecurity-101/what-is-a-red-team/
- https://developer.nvidia.com/blog/nvidia-ai-red-team-an-introduction/
- https://www.crowdstrike.com/cybersecurity-101/purple-teaming/
- https://www.synetis.com/tests-dintrusion-lapproche-red-team/
- https://www.varonis.com/fr/blog/red-teaming
- https://github.com/infosecn1nja/Red-Teamjng-Toolkit
- https://www.getastra.com/blog/security-audit/red-teaming-vs-penetration-testing/?
- https://www.infogene.fr/actualite-blog-expert/test-intrusion-pentest/

Document Asprom

Le cyber-rating -2019- https://asprom.com/dossier/cyber_rating/pdf
La fonction sécurité – CDSE- 2022 – https://asprom.com/dossier/cdse.pdf

Annexe 2 ; Université PSL – https://psl.eu

Située au cœur de Paris, **l'Université PSL** fait dialoguer tous les domaines du savoir, de l'innovation et de la création en sciences, sciences humaines et sociales, ingénierie et arts. Sélective et engagée en faveur de l'égalité des chances, elle forme au plus près de la recherche en train de se faire, des chercheurs, artistes, entrepreneurs et des dirigeants conscients de leur responsabilité sociale, individuelle et collective. Avec 2 900 enseignants-chercheurs, 17 000 étudiants, 140 laboratoires et une dizaine d'incubateurs, fablabs et espaces de coworking, PSL est une université à taille humaine.
Elle figure parmi les 50 premières universités mondiales selon les classements de Shanghai, du THE (Times Higher Education), CWUR et QS (Quacquarelli Symonds) et au 1er rang des universités de moins de 50 ans du classement Young du TH

PSL → Paris Science & Lettre
Création : 2022

Composition de l' Université **PSL** :

- Collège de France
- Conservatoire National Supérieur d'Art dramatique –PSL
- Dauphine - PSL
- École nationale des chartes - PSL
- École nationale supérieure de Chimie de Paris - PSL
- École normale supérieure - PSL
- École Pratique des Hautes Études - PSL
- ESPCI Paris - PSL
- Mines Paris - PSL Observatoire de Paris –
- PSL Collège de France Institut Curie CNRS, Inserm, Inria

PSL bénéfice du soutien de : Cnrs ,Inria, Insern,

Partenaires de PSL :

- Ecole Française d'Extrême-Orient
- Institut National du Service Public
- Institut Superiure d' Architecture Pais- Malaquais
- Lycée Louis-le-Grand
- Conservatoire national supérieur de Musique et de danse de Paris
- Ecole des Arts Décoratifs Paris

        - Le Fémis
        - Les Beaux Arts de Paris
        - Lycée Henry IV
- Institut Louis Bachelier

Annexe 3 : ouvrage sur le Red Team –

- **Ces guerres qui nous attendent 2030- 2060 –** 2 volumes

  Editeur : Des equateurs

  Red team/PSL

  La Red Team n'est pas la nouvelle série de Netflix. Et pourtant sous ce nom de code un commando a mené une opération pionnière particulièrement haletante. Pour la première fois, le ministère français des Armées et l'Université Paris Sciences et Lettres ont lancé un projet de prospection novateur. Analystes et chercheurs ont partagé librement leurs réflexions avec des auteurs de romans noirs, de science-fiction et de dessinateurs pour imaginer les conflits possibles à l'horizon 2030-2060 : création d'une nouvelle nation pirate née des changements climatiques, hacking possible des implants neuronaux, émergence de sphères communautaires développant une réalité alternative, fragmentation du réel, crises environnementales et bioterrorisme, guerres cognitives s'appuyant sur la désinformation de masse, polarisation du monde en hyperforteresses et hyperclouds.

- **Equipe Rouge Professionnelle** (Professional Red Teaming) – electronique

  Editeur Apress

  Jacob G oakley

  Explique comment la réalisation d'engagements de cybersécurité implique plus que l'exploitation d'ordinateurs, l'exécution de scripts ou l'utilisation d'outils
  Vous présente comment contrer l'association rouge avancée des menaces persistantes (association CAPTR) en tant que méthodologie d'équipe rouge inversée pour relever les défis rencontrés par les menaces persistantes avancées (APT)
  Rédigé par un praticien chevronné de la sécurité offensive et un universitaire publié qui apporte une approche pratique, réelle et tempérée des cyberopérations

- **Red Team Development and operations ; A practical guide broché (anglais)**

  Zero day edition

  Joe Vest, james Tuberville

  Ce livre est l'aboutissement d'années d'expérience dans le domaine des technologies de l'information et de la cybersécurité. Les composants de ce livre ont existé sous forme de notes approximatives, d'idées, de processus informels et formels développés et adoptés par les auteurs alors qu'ils dirigeaient et exécutaient les engagements de l'équipe rouge pendant de nombreuses années. Les concepts décrits dans ce livre ont été utilisés pour planifier, livrer et exécuter avec succès des engagements professionnels d'équipe rouge de toutes tailles et complexités. Certains de ces concepts ont été vaguement documentés et intégrés dans les processus de gestion de l'équipe rouge, et une grande partie a été conservée en tant que savoir tribal.

- **RTFM Red Team Field Manual**

  The RTFM – distribue rakusen

  Clark Ben

  Il y a plus de 8 ans, le manuel de terrain de l'équipe rouge (RTFM) est né des notes de terrain de l'opérateur inspirées par des années de missions de l'équipe rouge. Alors que les outils et les techniques changent, les opérateurs se retrouvent toujours dans des environnements d'exploitation communs, avec le temps qui presse. Le RTFM a fourni une référence rapide lorsqu'il n'y a pas le temps de parcourir Internet pour trouver cette commande parfaite.

  La version 2 de RTFM a été complètement remaniée, avec l'ajout de plus de 290 nouvelles commandes et techniques. Il a également été soigneusement mis à jour et testé pour s'assurer qu'il fonctionne avec les systèmes d'exploitation modernes. La version 2 comprend une nouvelle section Mac OS et une section décrivant les considérations commerciales. La recherche a été simplifiée grâce à une table des matières et une annexe élargies, et la lisibilité a été considérablement améliorée grâce à une nouvelle mise en forme du texte. Enfin, RTFM v2 sera disponible en plusieurs formats, y compris le livre de poche, le livre relié (à venir en août 2022), l'eBook Kindle et une toute nouvelle édition de prise de notes à large marge.

- **Red team – lesregles**
  - Auteur(s) : Collectif
  - Editeur : Panini Comic

  Eddie Mellinger, Trudy Giroux, Duke Wylie et George Winburn forment la Red Team, une unité issue de la section criminelle de la police de New York. Une surveillance attentive, une bonne dose de violence et une absence totale de scrupule dans la manipulation des preuves leur ont permis d'arrêter plusieurs gros bonnets de la drogue. Et pour se débarrasser d'un gangster plus gênant que les autres, l'équipe est prête à tout, même à franchir le point de non-retour. Ainsi commence une histoire brute de décoffrage, écrite par Garth Ennis (The Punisher, The Boys, Crossed) et dessinée par Craig Cermak.

- **Red Team : Comment réussir en pensant comme l'ennemi (Anglais)**
- **Red Team : How to succeed by thinking like a Enemy**

  Éditeur : Basic Books; 1er édition (3 novembre 2015)

  Aujourd'hui, les équipes rouges sont largement utilisées dans les secteurs public et privé par ceux qui cherchent à mieux comprendre les intérêts, les intentions et les capacités des rivaux institutionnels. Dans les bonnes circonstances, les équipes rouges peuvent donner des résultats impressionnants, donnant aux entreprises un avantage sur leurs concurrents, creusant des trous dans les estimations de renseignements vitaux et dépanneant les missions militaires dangereuses bien avant que les bottes ne soient sur le terrain. Mais toutes les équipes rouges ne sont pas créées égales; En effet, certains causent plus de dégâts qu'ils n'en préviennent. S'appuyant sur une gamme fascinante d'études de cas, *Red Team* montre non seulement comment créer et responsabiliser des équipes rouges, mais

aussi ce qu’il faut faire avec les informations qu’elles produisent.

Annexe 3 : Jeux vidéo

il existe plusieurs jeux vidéo qui présentent le concept de l'équipe rouge ou l'intègrent dans leur gameplay. Voici quelques exemples:

- **"Red Team"** (2006) : ce jeu de tir à la première personne développé par Cauldron est centré sur un conflit fictif entre deux sociétés militaires privées : Red Team et Blue Team. Les joueurs jouent le rôle d'un membre de l'équipe rouge et s'engagent dans diverses missions de combat.

- Série "**Red Faction":** Cette série de jeux de tir à la première personne, développée par Volition, se concentre sur le conflit entre la Red Faction, un groupe de rebelles luttant contre des régimes oppressifs, et diverses forces antagonistes. La série comprend des jeux comme "Red Faction" (2001), "Red Faction II" (2002) et "Red Faction Guerrilla" (2009).

- "**Team Fortress** 2": Bien qu'il ne soit pas spécifiquement nommé "Red Team", ce jeu de tir à la première personne multijoueur en équipe développé par Valve Corporation présente deux équipes, Rouge et Bleu, qui s'affrontent dans différents modes de jeu. Les joueurs peuvent rejoindre l'équipe rouge et participer à un gameplay basé sur des objectifs.

- "**Tom Clancy's Rainbow Six Siege**": Ce jeu de tir tactique à la première personne développé par Ubisoft propose un mode multijoueur en équipe où les joueurs peuvent être affectés à l'équipe rouge (attaquants) ou à l'équipe bleue (défenseurs). Le jeu met l'accent sur la planification stratégique et le travail d'équipe.

- Série « **Counter-Strike** » : dans la populaire série multijoueur de tir à la première personne « Counter-Strike », les joueurs peuvent rejoindre soit les terroristes (souvent représentés par un logo rouge), soit les contre-terroristes (souvent représentés par un logo bleu). Les équipes s'affrontent dans des scénarios basés sur des objectifs.

Il est important de noter que le concept d'équipe rouge varie selon les jeux et les contextes. Parfois, il fait référence à une équipe ou à une faction spécifique dans la tradition du jeu, tandis que dans d'autres cas, il représente simplement l'un des deux camps opposés dans un environnement multijoueur.