cybereason | Advens

5 ETAPES POUR RENFORCER SA SECURITE OPERATIONNELLE GRACE AU FRAMEWORK ATT&CK DU MITRE_

De multiples référentiels de sécurité existaient avant l'introduction du framework ATT&CK DU MITRE: les normes ISO-17799, puis ISO-27000, Cobit, NIST, etc. Toutefois, ces cadres n'ont jamais vraiment donné lieu à des travaux complets répondant aux besoins des équipes de sécurité opérationnelle (SecOps). Certains référentiels comme celui du NIST (National Institute of Standards and Technology) ont abordé ce sujet. Mais avant le lancement d'ATT&CK, aucun framework n'a réellement permis de procéder à des tests concrets ni proposé un cadre propice à l'amélioration des solutions de détection et de protection.

Selon le MITRE,

> Le framework ATT&CK™ est une vaste base de connaissances accessible dans le monde entier et qui répertorie des tactiques et des techniques offensives sur la base d'observations du monde réel. C'est bien plus que ça!

Le référentiel ATT&CK s'appuie sur deux éléments majeurs : un ensemble de techniques, tactiques et procédures (TTP), et des directives concernant la simulation d'attaques et de tests d'intrusion (AEP — Adverse Emulation Planning). Les TTP forment la base des techniques ATT&CK qui se positionnent au cœur du framework et sont également les plus couramment utilisées. Ces connaissances sont très utiles pour établir un vocabulaire commun grâce auquel les analystes Sécurité et les fournisseurs de solutions de sécurité peuvent discuter des attaques et des techniques de remédiation. Pour leur part, les directives AEP forment des processus conçus pour identifier et remédier aux faiblesses de la posture de sécurité des entreprises et des technologies utilisées. Bien que particulièrement importants, ces processus sont fréquemment négligés par les experts en sécurité accaparés par la « guerre de tranchées » que représentent les activités de sécurité quotidiennes. Certes très utiles, les TTP du référentiel ATT&CK sont encore plus efficaces lorsqu'elles sont associées à des directives AEP.

Ces directives représentent la fonctionnalité la plus importante pour mettre en place un programme de sécurité opérationnelle adapté à votre secteur d'activité. Les TTP évoluent, mais le processus général qui consiste à les réunir au sein d'une simulation d'attaque réelle (dont l'efficacité peut être mesurée) en constitue le véritable intérêt. Les directives AEP permettent de simuler une attaque réelle en association avec des TTP — qui peuvent être exécutées par rapport à votre infrastructure de sécurité au cours d'une offensive lancée par la Red Team. Elles permettent de noter où et quand des attaques sont vues ou non, à quel moment les alertes sont lancées ou demeurent silencieuses, et dans quels cas les objectifs sont atteints ou bloqués.

Ces efforts peuvent être mesurés quantitativement, ce qui permet d'analyser et de combler rapidement toute lacune au sein de vos défenses.

Vous disposez ainsi d'une visibilité accrue de votre environnement et pouvez soulager la charge de travail des équipes de sécurité en renforçant vos barrières de protection avant que les attaquants ne les atteignent. Ce document va vous aider à mettre en place un processus d'amélioration simple de votre sécurité opérationnelle en s'appuyant sur la puissance du référentiel ATT&CK.

POINTS-CLÉS

1 » **L'équipe Cybereason a identifié cinq étapes indispensables à la mise en place d'une infrastructure de défense efficace et itérative basée sur le référentiel MITRE ATT&CK. Elle s'appuie sur trois piliers : groupes d'opposants, posture de défense et sécurité opérationnelle (SecOps).**

2 » **Il est essentiel de comprendre le lien entre les TTP, les directives AEP et les groupes d'opposants pour créer une stratégie de sécurité intégrée et efficace, capable de répondre aux attentes de votre secteur d'activité.**

3 » **En suivant ces étapes, vous disposerez d'une visibilité accrue au sein de votre environnement et réduirez la charge de travail de votre équipe Sécurité en comblant les lacunes de votre infrastructure de défense.**

RECOMMANDATIONS DE SÉCURITÉ

1 » **Créez un plan de simulation d'attaques qu'utiliseront votre Red Team et votre équipe de chasseurs de menaces (Threat Hunters). Le fait de structurer un plan autour du framework ATT&CK permet de créer un langage commun et un processus répétable.**

2 » **Identifiez et caractérisez les groupes d'adversaires qui ciblent votre secteur d'activité (comme indiqué en Table 1 et, de façon approfondie, au sein de la section Groups du référentiel ATT&CK). Documentez ces groupes en fonction de leur niveau de priorité et de menace (comme indiqué en Table 2).**

3 » **Documentez vos directives AEP et plans de simulation d'attaques (en vous appuyant sur les Tables 2 et 3). Enregistrez les techniques et activités accomplies par votre Red Team, le résultat des exploits, les détections, les activités de remédiation, et le niveau de priorité dans le cadre d'un plan de simulation d'attaque (comme indiqué en Table 4).**

DANIELLE WOOD
SENIOR DIRECTOR, SECURITY SERVICES
CYBEREASON

ALLIE MELLEN
SENIOR CONTENT WRITER
CYBEREASON

AU CŒUR DU FRAMEWORK ATT&CK_

Le site dédié au référentiel ATT&CK du Mitre propose des tactiques, des groupes d'opposants, et des outils de planification qui sont utilisés pour construire des processus répétables dont le rôle est d'améliorer votre sécurité. Ces étapes sont disponibles sur le site du Mitre ATT&CK, mais elles ne sont pas organisées selon une approche progressive contrairement au référentiel du NIST.

BIEN CHOISIR LES MENACES

La section groups du framework ATT&CK fournit des renseignements sur près de 80 groupes d'attaquants identifiés, sur les techniques connues utilisées par chacun d'entre eux, ainsi que sur les marchés verticaux et les entreprises qui constituent leurs cibles privilégiées. Il convient de sélectionner les groupes spécifiques dont vous souhaitez simuler les offensives en commençant par ceux qui représentent la menace la plus immédiate pour votre entreprise. Par exemple, une société spécialisée dans les soins de santé commencera probablement par un groupe comme Deep Panda (MITRE ATT&CK ID G0009), réputé pour son intrusion à l'intérieur de la société Anthem (Tableau 1). Lorsque vous sélectionnez un groupe, le site du Mitre permet de lancer une recherche dans une liste des techniques communes aux groupes par identifiant, ainsi que dans une liste des logiciels et malware les plus couramment employés.

Secteur d'activité	Exemple de groupe d'opposants
FINANCE	APT19
SANTÉ	Deep Panda
PRODUCTION	menuPass
JURIDIQUE	APT19
HYDROCARBURES (O&G)	OilRig
ENSEIGNEMENT SUPÉRIEUR	Turla
ADMINISTRATIONS	BRONZE BUTLER
INFRASTRUCTURES CRITIQUES	Dragonfly 2.0

Table 1: Exemples de groupes de menaces par secteur d'activité et type d'entreprise

Avant de définir votre stratégie de défense, il est important de bien cerner les besoins de votre entreprise et d'identifier vos principaux groupes d'adversaires. Certains experts affirment qu'en détectant la totalité des éléments du framework ATT&CK, vous vous protégerez contre les attaques lancées par n'importe quel groupe d'opposants identifiés par le Mitre. Certes, cette théorie est techniquement exacte. Mais si la visibilité est effectivement très importante, bon nombre d'éléments des TTP ATT&CK ne sont pas malveillants et peuvent générer un nombre élevé de faux positifs — ce qui peut se traduire par une cyberfatigue et abaisser le niveau d'efficacité des équipes SecOps.

Pour maximiser l'efficacité de votre défense, il est capital de réduire les tâches manuelles tout en maintenant un haut niveau de visibilité. Par exemple, la liste des techniques de découverte de compte (Account Discovery) (MITRE ATT&CK ID T1087) renferme à elle seule 33 éléments et contient des actions bénignes telles que l'exécution de la commande « net user /domain ». Lancer une alerte dès que cette commande est exécutée dans un domaine risque de créer un nombre d'alertes significatif, et ainsi d'affaiblir l'action de l'équipe SecOps. De plus, faute de contexte (« qui a activé la commande ? », « quel était son processus parent ? », « est-ce que l'accès à distance était impliqué ? », etc.), votre équipe SecOps aura du mal, voire sera dans incapable de savoir si la commande a été exécutée de façon malveillante ou non. Au bout du compte, l'équipe désactivera l'alerte au lieu de l'utiliser, ce qui ne correspond pas vraiment à sa mission.

Une meilleure approche consiste à tester les contrôles existants par rapport à une simulation d'attaque complète qui prend en compte diverses techniques, et par rapport à votre infrastructure. Vous verrez ainsi à quels endroits des données de contexte doivent être ajoutées. Des journaux n'ont peut-être pas été enregistrés alors qu'ils doivent l'être; ou alors, il est important d'ajouter de nouvelles règles et technologies.

Les alertes *"basse fidélité" de type "alert me when net user /domain is run » sont aussi utiles dans le contexte que des alertes haute-fidélité telles que "alert me when net user /domain is run by a non-shell process or by a domain user under a shell whose parent tree doesn't contain explorer when that user is not a member of domain admins".*

UTILISER DES GROUPES POUR SIMULER UNE ATTAQUE

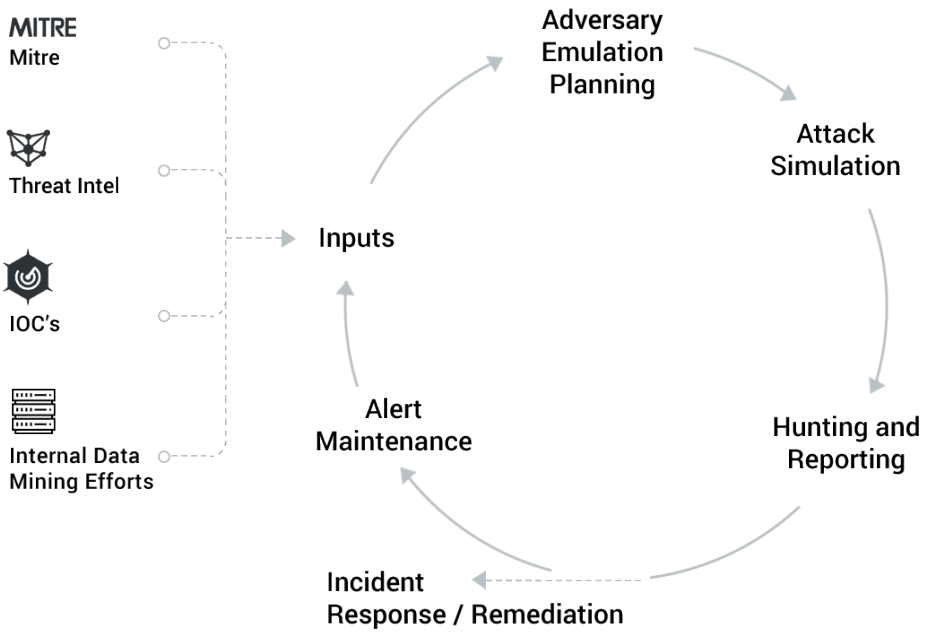
Vous pouvez utiliser ces informations de groupe et les plans de simulation d'attaques APT 3 pour bâtir votre plan de simulation d'attaque et de test d'intrusion. Ensuite, vous pourrez aisément créer un scénario d'attaque pour votre Red Team. Les groupes peuvent être organisés en un simple tableau afin de montrer la priorité et le statut de toute simulation.

Ce tableau indique la priorité et le statut de tout plan de simulation d'attaque, ainsi que la façon dont progresse la construction de la simulation.

Groupe	Priorité	Menace	État AEP	Création du scénario d'attaque	Date prévue	Titulaire
DEEP PANDA	Haute	Haute	Terminé	En cours	12 janv. 2019	John Smith
APT3	Haute	Haute	Terminé	Terminé	28 déc. 2018	John Smith
MENUPASS	Haute	Haute	Non entamé	Non entamé	N/A	N/A
ORANGEWORM	Haute	Haute	Non entamé	Non entamé	N/A	N/A

Table 2: Exemple de groupes d'attaques avec leur état et leur degré de priorité

OPTIMISER L'UTILISATION DU REFERENTIEL ATT&CK_



L'utilisation d'ATT&CK pour créer ce processus de sécurité qui tient à la fois compte des adversaires, des moyens de défense et des activités de sécurité n'a rien de complexe. Nous avons décomposé ce processus en cinq étapes:

01. INJECTION DE DONNÉES

02. PLANIFICATION DES SIMULATIONS D'ATTAQUES

03. SIMULATION D'ATTAQUES

04. HUNTING ET REPORTING

05. MAINTENANCE DES ALERTES

Ces cinq étapes doivent couvrir la majorité de vos initiatives de cybersécurité.

ÉTAPE 1: INJECTION DE DONNÉES

Pour créer un cycle d'amélioration efficace en matière de chasse aux menaces (threat hunting), de lancement d'alerte et de remédiation, il est important d'utiliser d'autres données venant compléter les informations du framework ATT&CK. Des flux de données supplémentaires, plus traditionnelles, peuvent enrichir le cycle grâce à des informations qui permettront de prendre des décisions plus pertinentes en matière d'alerte et de défense.

RENSEIGNEMENTS SUR LES MENACES (THREAT INTEL)

Les renseignements sur les menaces extérieures (la threat intelligence) sont utiles pour deux raisons : les nouvelles TTP d'attaque, et la validation et l'identification des attaques. La threat intelligence peut être utilisée pour simuler des attaques ponctuelles basées sur des événements récents tels que des campagnes exécutées par le groupe iranien de cyberespionnage APT 39, ovoire des attaques plus connues comme NotPetya ou WannaCry. Alternativement, la threat intelligence sera utilisée pour valider les informations figurant dans la liste de groupes ATT&CK ou signaler à quel moment tel ou tel groupe malveillant exécute des campagnes nouvelles ou déjà connues.

INDICATEURS DE COMPROMISSION (IOC)

Les Indicators of compromise (IOC) sont probablement les entrants les moins utiles pour la construction de défenses génériques; néanmoins, ils permettent d'identifier les intrusions de divers groupes. Des IOC tels que les noms de domaine ou les hachages de fichiers peuvent être ajoutés aux planifications de simulation pour identifier les groupes malveillants à la volée et renforcer la sécurité par des signatures statiques. Par exemple, vous pouvez ajouter des alertes pour les hachages uniques associés à l'outil d'un groupe d'adversaires spécifique dans le but d'ajouter du contexte à des alertes statiques.

EXPLORATION DE DONNÉES (DATA MINING)

Le data mining est un outil particulièrement utile pour les chasseurs de menaces et les défenseurs qui identifient de nouveaux schémas d'attaque. Malheureusement, la plupart des entreprises ne sont pas armées pour tirer parti de ces capacités en raison de contraintes liées à leur infrastructure. L'exploration de données est une tâche extrêmement complexe et particulière qui requiert une grande expertise et de solides ressources. Le manque d'infrastructures telles que les lacs de données (data lakes), utilitaires d'indexation et autres installations de traitement parallèle — sans oublier l'incapacité de conserver l'expertise nécessaire pour les créer —, constitue un défi de taille pour la plupart des sociétés. Cependant, si l'option est disponible, l'utilisation d'outils comme Splunk, Elasticsearch, ou Hadoop, fait du deep data mining une solution très performante qui peut rapporter gros, tant pour chasser les menaces que pour les identifier.

STAGE 2: SIMULATIONS D'ATTAQUES

Il est essentiel de planifier la simulation des attaques pour chacun des groupes d'opposants susceptibles d'attaquer votre entreprise. Bien que l'approche idéale serait de constituer un plan de simulation pour chacun des groupes identifiés dans le framework ATT&CK, la meilleure façon d'utiliser vos ressources reste de se concentrer sur les groupes qui ciblent votre société ou vos données. Si votre entreprise dispose des ressources nécessaires pour gérer les plans de simulation correspondant à l'ensemble des groupes d'opposants, tant mieux — même si un tel objectif est difficile à atteindre. Il est en effet nécessaire de rafraîchir la planification des techniques d'attaque au moins une fois par an. Un guide d'aide à la construction d'un plan de simulation des attaques et un exemple de plan portant sur les menaces APT-3 sont disponibles sur le site MITRE ATT&CK.

Vous pouvez suivre l'état de vos plans de simulation à l'aide d'un simple tableau. Chaque TTP gérée par votre équipe doit correspondre à un état de la planification indiquant sa progression.

ÉTAT DE LA PLANIFICATION

01. **DOCUMENTÉ:** Les TTP ont été correctement documentées pour le groupe d'opposants.
02. **CODÉ:** Les TTP ont été codées en un exploit effectif à l'usage de la Red Team.
03. **EXÉCUTÉ:** Les TTP codées ont été exécutées avec succès.
04. **SUCCÈS/ÉCHEC:** L'exécution des TTP a atteint ou non son objectif
05. **DÉTECTÉ/NON DÉTECTÉ:** L'exécution des TTP a réussi ; les TTP ont été détectées ou non.

En page suivante, vous trouverez un exemple de plan de simulation d'attaques. Par sa présentation simplifiée, ce tableau vous aidera à suivre la progression de votre plan. Cependant, au fur et à mesure de son évolution, nous vous recommandons d'ajouter davantage de contexte et d'informations.

Comme nous l'avons vu précédemment, un plan de simulation doit se composer d'une série d'étapes et non de techniques individuelles. C'est pourquoi nous recommandons d'ajouter une chronologie, une hiérarchie, un type de TTP, des notes et autres détails, si nécessaire.

DEEP PANDA — EXEMPLE D'UN PLAN DE SIMULATION D'ATTAQUES			
ID	Nom	Description du plan	État
T1015	Fonctions d'accessibilité	Deep Panda a utilisé la technique des touches rémanentes (sticky keys) pour contourner l'écran de connexion RDP (Remote Desktop Protocol) sur les systèmes distants au cours d'intrusions. Par exemple, en utilisant la technique indiquée ci-dessus sur vos serveurs connectés à Internet.	Documenté
T1066	Retrait de l'indicateur dans les outils (Indicator Removal from Tools)	Deep Panda a actualisé et modifié son malware, créant des valeurs de hachage différentes qui échappent à la détection.	Documenté, codé
T1086	PowerShell	Deep Panda a utilisé des scripts PowerShell pour télécharger et exécuter des programmes dans la mémoire sans écrire sur le disque.	Documenté, codé
T1057	Découverte de processus Process Discovery	Deep Panda utilise l'utilitaire Microsoft Tasklist pour lister les processus exécutés sur les systèmes.	Documenté
T1117	Commande Regsvr32	Deep Panda a utilisé la commande regsvr32.exe pour exécuter une variante serveur de Derusbi dans les réseaux victimes	Documenté
T1018	Découverte de système distant Remote System Discovery	Deep Panda a utilisé la commande ping pour identifier d'autres machines présentant un intérêt.	Documenté
T1064	Scripts	Deep Panda a utilisé des scripts PowerShell pour télécharger et exécuter des programmes dans la mémoire sans écrire sur le disque.	Documenté
T1100	Web Shell	Deep Panda utilise des scripts "Web shell" sur des serveurs publics pour évaluer les réseaux victimes.	Documenté
T1077	Partages administratifs sous (Windows Admin Shares)	Deep Panda utilise la commande net.exe pour se connecter aux partages de réseau en exploitant les commandes Net Use avec des identifiants infectés.	Documenté, Codé
T1047	WMI (Windows Management Instrumentation)	Le groupe Deep Panda est connu pour utiliser WMI pour les déplacements latéraux.	Documenté, Codé

Table 3: Exemple d'un plan de simulation d'attaques et état correspondant

ÉTAPE 3: SIMULATION D'ATTAQUES

Utilisez une Red Team interne ou externe pour créer des simulations d'attaques qui suivent au plus près les plans de simulation au niveau de la technologie comme des processus. Il est essentiel que les exercices de votre Red Team simulent des ressources d'attaque réelles : systèmes C2 (Command & Control) externes, infiltration et exploitation appropriées, exfiltration de données. La non-exécution de ces étapes dans le plan de simulation peut entraîner l'oubli de certaines étapes lors d'une attaque réelle, ce qui peut entraîner de graves conséquences.

Des outils automatiques de simulation des attaques comme CALDERA du Mitre doivent être envisagés au moment de créer une simulation d'attaque. Ces outils peuvent permettre à vos équipes Red et Blue d'imiter le comportement d'assaillants après une infection. Cette approche peut donner à votre Red Team la liberté de se concentrer sur les tâches qu'elle juge plus importantes, mais également d'automatiser certaines parties du test en cas de main-d'œuvre insuffisante.

ÉTAPE 4: HUNTING ET REPORTING

CHASSE AUX MENACES

Il est important de documenter l'ensemble des ressources utilisées par votre Red Team et de maintenir une communication constante. Vous devez assurer que l'exécution des véritables attaques n'est pas masquée par l'activité de la Red Team. Toute détection fructueuse doit être consignée et documentée aux fins d'évaluation à l'issue du processus de simulation des attaques.

Dans un framework de chasse aux menaces, l'utilisation de plans de simulation de comportements et d'attaque poursuit deux objectifs: tout d'abord, renseigner vos opérations de chasse, de telle sorte que votre équipe pourra rechercher quotidiennement des techniques dans le monde réel. Deuxièmement, les plans AEP fournissent une feuille de route pour automatiser l'identification des attaques avec un haut degré de fidélité. **Tout ceci n'est toutefois possible que si votre entreprise a la capacité de détecter les bonnes techniques, tactiques et procédures.** Si ce n'est pas le cas, c'est l'occasion de rechercher de nouveaux outils ou de nouvelles méthodes pour collecter de données.

A minima, les Red Teams doivent utiliser des plans de simulation d'attaques et des TTP aux fins d'exécution et rendre compte activement du succès de leurs activités. Dans cette optique, elles peuvent utiliser des outils automatiques pour simuler le comportement des assaillants. Si les actions de la Red Team ne sont détectées à aucun moment, votre équipe SecOps doit immédiatement en évaluer la cause. Les raisons potentielles sont trop nombreuses, qu'il s'agisse d'un nombre d'alertes trop élevé ou d'un manque de données, voire d'une erreur humaine. Votre évaluation **doit absolument** se traduire par une amélioration de la panoplie d'outils ou des processus. Il importe de souligner que le reporting concernant les activités de la Red Team doit être **impeccable** et **sans erreur**. Le respect de ces principes assurera de meilleurs résultats grâce au reporting et permettra d'améliorer les processus par une meilleure collaboration.

REPORTING

Toute simulation doit être évaluée quantitativement, même à l'aide d'une approche aussi élémentaire qu'un schéma basé sur le nombre de TTP utilisées par rapport au nombre de TTP détectées, y compris les résultats de la chasse. Toutes les TTP, détectées ou non, doivent être classées selon la méthodologie ATT&CK et la méthode de détection générale la mieux adaptée à votre architecture interne. Outre une mesure quantifiable, vous pouvez rendre le processus de notation plus ludique pour votre équipe. Certains scores de TTP individuelles peuvent être annulés à discrétion si une détection fiable et haute-fidélité n'est pas possible ou si d'autres détections atténuent le problème.

Les rapports concernant les activités de votre Red Team doivent inclure la description des plans d'attaque exécutés, le résultat des attaques et les mesures correctives que vous devez prendre pour remédier aux problèmes constatés. Chaque attaque doit être entièrement documentée dans le rapport, en indiquant la technique utilisée, l'endroit où ces activités ont été enregistrées, détectées

et contrées, ainsi que toute méthode devant être utilisée pour améliorer le processus de détection. Toute recommandation en matière de remédiation doit être assortie d'un niveau de priorité calculé en fonction d'une combinaison de la probabilité d'un exploit et des dommages potentiels de cet exploit. Dans de nombreux cas, une technologie de télémétrie montre les effets d'une attaque, mais il est possible que vous ne disposiez pas d'alertes utilisant cette télémétrie. Le tableau ci-dessous présente un reporting simplifié pour chaque technique ; c'est un bon point de départ pour le processus de reporting.

PLAN DE SIMULATION D'UNE ATTAQUE: AEP 20190107 (DEEP PANDA)					
Technique	Activité	Résultats de l'exploit	Détections (Détecté/ Télémétrie/Manqué)	Remédiation	Priorité
TT1015	Sticky Keys	A remplacé SetHC. exe par cmd.exe	Écriture de fichiers vue par le système de gestion des informations et des événements de sécurité (SIEM); détectée comme une opération malveillante (« malop ») lorsque le remplacement a été exécuté via powershell.	Inutile	Aucune
TT1066	Malware binaire unique	Exécution via Powershell	Écriture de fichiers dans Télémétrie à partir du SIEM; pas de détection	Ajouter une exécution binaire non signée entre "temp" et le jeu de règles « malop »	Moyenne

Table 4: Compte-rendu minimum devant être fourni par votre Red Team à propos d'une attaque

Les rapports doivent inclure des détails techniques, ainsi que toutes les recommandations découlant de l'exécution de votre plan de simulation d'attaque. Il convient de souligner que l'identification détaillée des différentes TTP n'est pas toujours possible, et qu'à ce titre, il peut s'avérer nécessaire de collecter des informations de contexte supplémentaires lors de l'exécution. Par exemple, l'exécution d'un codage binaire non signé dans une grande entreprise (exemple TT1066 ci-dessus) générerait un grand nombre de faux positifs si les alertes étaient lancées individuellement. Cependant, couplée et corrélée à d'autres détails tels que la chaîne d'exécution ou l'activité du réseau, cette alerte peut devenir une alerte haute-fidélité.

ÉTAPE 5: MAINTENANCE DES ALERTES

Créez un plan d'amélioration des processus et de la technologie reposant sur les résultats et les TTP identifiées lors des activités de votre Red Team. Les plans d'amélioration des processus doivent être suffisamment flexibles pour incorporer les résultats de plusieurs simulations, dans la mesure où les changements qui en découlent peuvent considérablement influencer les décisions technologiques.
L'amélioration de vos alertes est liée à la qualité de votre reporting. Lorsque vous identifiez les mesures correctives du rapport final de votre Red Team, il est important d'inclure les moyens de détection et les méthodes de prévention.

Cette décision peut accroître sensiblement l'efficacité des alertes.

Certaines techniques, tactiques et procédures peuvent être facilement interprétées à tort comme des actions communes — par exemple, la création d'un nouveau compte utilisateur par l'administrateur à partir de la ligne de commande. Cette opération difficile à identifier peut vous noyer dans un flux d'alertes. Afin de les identifier correctement, vous devez suivre l'**effet des actions qui suivent les événements**. Vous disposerez d'un contexte plus fourni pour comprendre ce qui ne va pas, et pourquoi.

Afin de suivre la gestion des alertes liées à l'exécution de l'attaque, ajoutez des mesures de suivi corrigées au tableau de reporting du plan AEP (Tableau 3). Il peut s'agir d'informations concernant le système à modifier, l'état des modifications et leur propriétaire. Il est important de noter que si vous prévoyez d'ajouter des outils pour combler les lacunes en matière de défense de sécurité, une évaluation approfondie risque de s'avérer nécessaire, pouvant inclure des tests supplémentaires de la Red Team, un budget accru, des preuves de concept (PoC), etc.

UTILISER ATT&CK POUR AMELIORER LE NIVEAU DE SECURITE_

De nombreux référentiels de sécurité existaient avant le framework ATT&CK du Mitre, mais il leur manquait un élément clé : des explications complètes sur les besoins tactiques des équipes SecOps. Le référentiel ATT&CK constitue à ce titre un outil polyvalent pour les équipes et un ajout essentiel à l'environnement de sécurité. De nombreuses entreprises utilisent efficacement ATT&CK comme outil de test pour leurs produits en utilisant les techniques, tactiques et procédures (TTP). Mais c'est une image limitée de la puissance de ce framework. Avec les plans de simulation d'attaque, le référentiel ATT&CK du Mitre permet de créer des simulations d'attaques réelles fusionnées avec des TTP. Vous pouvez les exécuter dans votre infrastructure à l'occasion d'une simulation effectuée par la Red Team afin de savoir quelles attaques sont identifiées, quelles alertes sont activées et quels objectifs sont atteints. Vous disposez ainsi d'une visibilité exhaustive de votre système et pouvez créer un cycle d'amélioration itératif pour vos opérations de sécurité.

Ce livre blanc est une introduction à la mise en œuvre de ce processus de sécurité itératif. Cependant, son application peut s'avérer beaucoup plus complexe. Si vous souhaitez utiliser cette méthode dans votre environnement, les équipes Cybereason et Advens se tiennent à votre disposition.