10 façons de passer **MITRE ATT&CK du plan à l'action**

Guide de mise en œuvre d'une défense informée contre les menaces dans votre entreprise

splunk> turn data into doing™

10 façons de passer MITRE ATT&CK
Du plan à l'action

Le framework MITRE ATT&CK existe depuis plusieurs années mais les entreprises l'adoptent aujourd'hui de plus en plus. En effet, elles comprennent l'importance d'avoir une équipe de sécurité solide, et de nouveaux budgets sont débloqués pour améliorer la maturité des programmes de sécurité informatique.

Les entreprises n'investissent pas seulement dans des technologies de prévention. Elles mettent aussi en place des fonctionnalités de détection précoce et de réponse aux incidents. Elles abandonnent une approche axée sur un fournisseur pour adopter une démarche de sécurité axée sur l'analyse.

> **« Dans un monde numérique, les données sont devenues incontournables dans la planification stratégique des équipes de sécurité pour la détection des menaces et la réponse aux incidents pour protéger les activités, les clients et les collaborateurs d'une entreprise. »**
>
> – Matthias Maier, CISSP & CEH, évangéliste sécurité, Splunk

Pour les professionnels de la sécurité comme pour les entreprises, il est essentiel de comprendre quelles tactiques et techniques spécifiques sont utilisées dans les cyberattaques provenant de différents groupes de menaces.

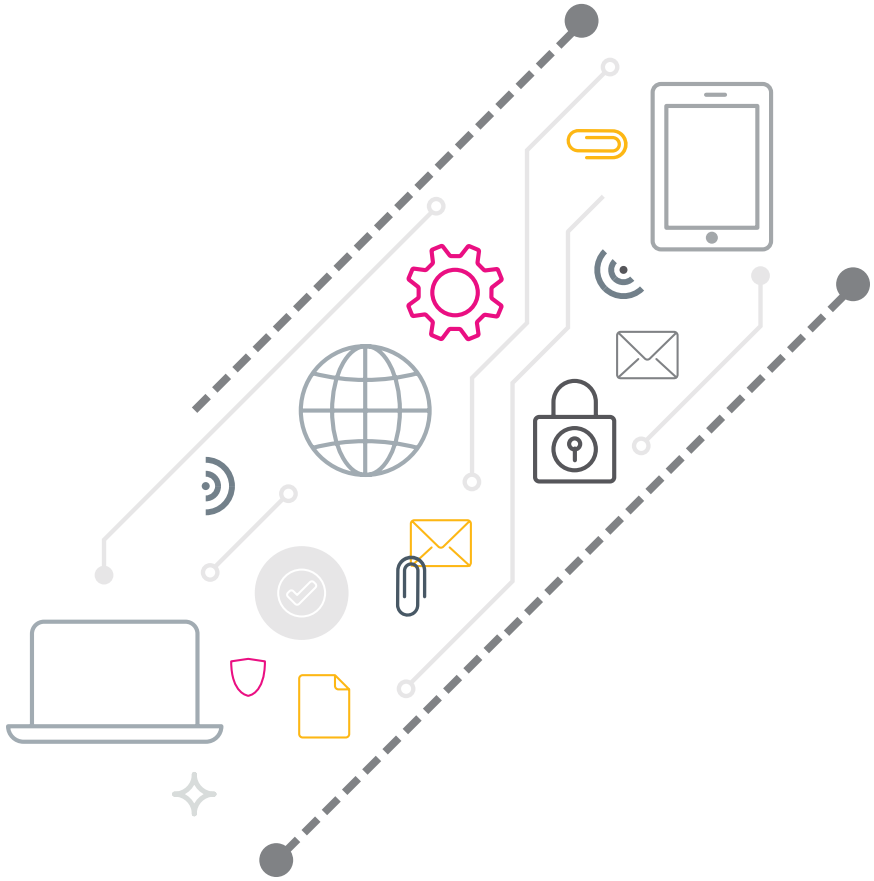
Cette approche aide les entreprises à mieux gérer les risques, à prévoir les données qu'elles doivent garder à disposition pour enquêter sur un incident de sécurité, et à établir des points de détection précoce là où les technologies traditionnelles de prévention échouent ou sont trop strictes pour les employés.

Le framework MITRE ATT&CK ne s'arrête pas aux professionnels de la sécurité : il peut être utilisé de nombreuses autres manières pour améliorer la visibilité et communiquer l'efficacité des efforts de sécurité à l'échelle d'une entreprise – et ce, quelle que soit la taille de l'équipe de sécurité. Vous cherchez un autre exemple d'utilisation du framework MITRE ATT&CK ? Consultez cet article de blog.

Comment le framework MITRE ATT&CK donne **de nouveaux moyens à différentes Équipes**

Dans cet e-book, nous étudions la façon dont le framework MITRE ATT&CK vient aider différents départements de l'entreprise :

1. Le chef des opérations sécurité, pour établir une stratégie de prévention, de détection, de prise en charge et d'amélioration
2. Les développeurs de contenus de sécurité ou « blue team », pour réagir avec des délais d'analyse courts
3. Les architectes SIEM, pour valider la couverture
4. Les ingénieurs SOC, pour justifier ses besoins en données auprès de l'équipe des Opérations IT
5. Les responsables de sécurité informatique, qui doivent prendre et documenter des décisions liées aux risques en fonction des logs et composants
6. Les RSSI, pour renforcer la posture de sécurité, étendre les efforts de surveillance et justifier de nouveaux investissements
7. Les analystes SOC, pour développer un modèle d'alerte fondé sur les risques (RBA)
8. Les administrateurs SIEM, pour assurer la qualité de l'importation des données et déterminer les besoins de couverture
9. Les testeurs et « red teams », qui réalisent des tests de pénétration et doivent documenter et communiquer les efforts d'amélioration
10. Le service des achats et les décideurs informatiques, pour définir les bases de la sécurité tactique et les besoins en matière de réponses aux incidents et supervision



1

Donnez au chef de votre équipe d'opérations sécurité les moyens d'établir une stratégie fondée sur la prévention, la détection et la réponse.

Grâce aux techniques documentées dans le framework MITRE ATT&CK, les entreprises peuvent mettre au point une feuille de route allant au-delà de la prévention et se concentrant sur les processus de détection, de réponse et d'amélioration.

L'équipe de sécurité de SIEMENS EAGLE Datacenter suit cette approche et a mis sur pied un processus d'assurance qualité et d'amélioration permanente. Sa priorité numéro 1 est d'arrêter toutes les menaces possibles. Et ce que l'équipe ne peut empêcher, elle tient à pouvoir le détecter aussi tôt que possible et à en être avertie. À partir de là, l'équipe répond en menant une enquête, en tirant des enseignements du scénario, puis en ajustant la détection ou en configurant une mesure de prévention, si possible, à des fins d'amélioration.

Le Framework NIST de Cybersecurité décrit un concept similaire: identifier le risque, protéger, détecter, répondre et restaurer.

« Nous voulons prendre les devants autant que possible avec la prévention pour nous éviter d'avoir à la gérer quotidiennement. Quand nous ne pouvons pas prendre les devants, nous visons à détecter correctement et prendre en charge les menaces de façon appropriée. La connaissance que nous tirons de nos activités quotidiennes est injectée dans l'amélioration, pour que la situation soit couverte demain. »

– Oliver Kollenberg, EAGLE DataCenter, Siemens AG

Les fonctions fondamentales du framework de cybersécurité NIST organisent les activités à leur plus haut niveau.

Les deux exemples reposent sur une équipe de sécurité qui applique un principe de défense fondé sur la connaissance des menaces et la disponibilité des données à interroger pour savoir ce qui se passe dans son environnement.

2

Donnez aux développeurs de contenus de Sécurité - ou « Blue Teams » les moyens de réagir avec des délais d'analyse courts.

Le framework MITRE ATT&CK permet aux "blue teams" et aux développeurs de contenus de sécurité d'associer rapidement les nouvelles cyberattaques évoquées dans les médias aux techniques utilisées, à identifier les besoins en données et à élaborer les analyses permettant de les détecter aux différentes étapes tactiques mises en œuvre par les adversaires.

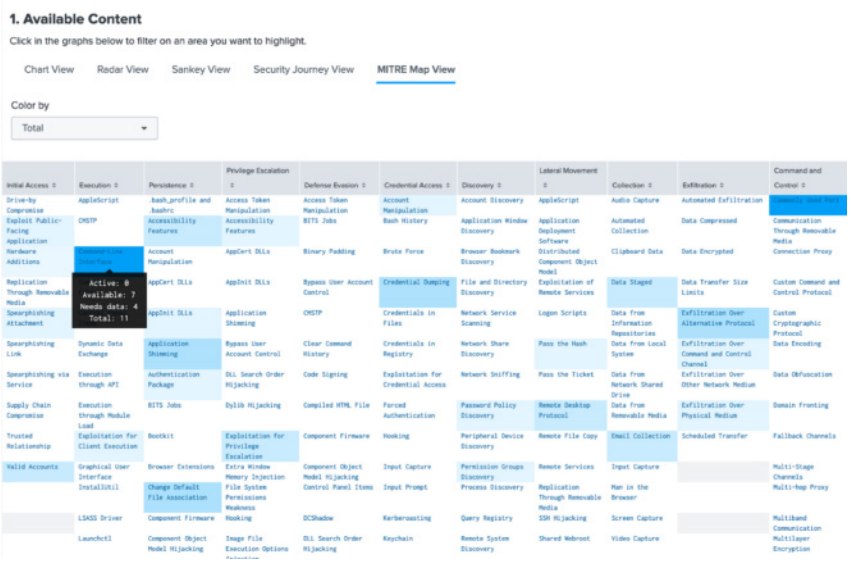
« Il faut s'attacher à détecter une opération et non l'attaque. Vous connaissez certainement le concept de kill-chain ou le framework MITRE ATT&CK. Si vous essayez simplement de détecter l'attaque en tant que telle, vous jouerez certainement de malchance un jour ou l'autre. Si vous effectuez des analyses à l'étape de la livraison, d'autres à l'étape d'exploration et d'autres encore à l'étape C2, vous pouvez détecter l'opération en cours. Nous avons enregistré notre délai le plus court quand nous avons développé, en 2 heures seulement, une nouvelle manière de détecter les attaques quand nous avons appris l'apparition d'un nouveau comportement : on ne peut pas aller voir son fournisseur pour lui demander d'implémenter un nouveau système de détection dans son produit, puis attendre 3 mois qu'il publie la mise à jour. »

– Jonathan Paget, Chef du Centre de défense de sécurité, Bank of England

3

Donnez aux Architectes SIEM les outils pour valider la couverture et mesurer l'adoption.

Les architectes SIEM ont souvent des difficultés à répondre à la question « quelle partie de l'infrastructure est effectivement couverte par le SIEM ? », en particulier lorsque la définition de la couverture est plus complexe qu'une simple liste de systèmes et de composants produisant des logs. Elle doit être définie si les bonnes actions produisent un événement enregistré par le dispositif source. La seconde partie du travail consiste à identifier si le contenu actif du SIEM recherche les bons événements. Pour ces raisons, le framework MITRE ATT&CK est idéal pour les architectes SIEM qui souhaitent cartographier leur couverture.



Liste tabulaire de toutes les tactiques et techniques d'ATT&CK mettant en évidence les analyses disponibles dans Spunk. Vous repérez le contenu Actif, Disponible mais inactif, et En attente de données. Plus la couleur est foncée, plus la quantité de contenu est importante. Source : Conseiller analytique de l'application Splunk Security Essentials (Version 2.4)

4

Donnez aux ingénieurs SOC les moyens de justifier les besoins en données auprès des équipes des opérations informatiques.

Habituellement, l'ingénieur SOC n'est pas le propriétaire des systèmes et des applications qu'il doit protéger. Il peut être très difficile d'expliquer à l'équipe des opérations IT quelles données sont requises pour délivrer la visibilité nécessaire. En particulier lorsqu'on communique les types d'actions contrôlées et conservées, l'équipe des opérations IT peut avoir besoin de beaucoup de temps pour examiner les niveaux de journalisation et leur configuration. Le framework MITRE ATT&CK permet aux ingénieurs SOC de documenter et de communiquer plus précisément leurs besoins concernant les événements de certaines activités, comme la création d'une tâche planifiée sur une machine Windows ou un journal PowerShell. Il permet également aux équipes des opérations IT de déterminer comment recueillir les données en fonction de la technologie la plus adaptée sur le plan architectural. Par exemple, on collecte l'activité native d'un point de terminaison avec une configuration sysmon de SwiftOnSecurity ou à l'aide d'une solution de protection ponctuelle.

5

Donnez aux responsables de sécurité informatique les moyens de prendre et de documenter des décisions de risque sur la couverture des logs et des composants.

Le framework MITRE ATT&CK permet aux responsables de la sécurité informatique de spécifier plus précisément les directives d'audit et de journalisation au sein des contrôles de sécurité d'une entreprise. Cela permet par exemple à un ingénieur SOC de mieux comprendre le niveau de risque accepté par une entreprise, afin de savoir quels sont vraiment les besoins.

Par exemple, ISO/IEC 27002 définit ce qui suit dans les directives de la section Journalisation des événements : « Les logs d'événements doivent inclure, lorsque c'est utile : … les activités du système ; …

Le framework MITRE ATT&CK permet à un responsable de la sécurité informatique de définir un contrôle tel que : [10 %] des techniques de la tactique [accès initial] doivent être couvertes de la collecte des événements à la corrélation des événements.

6

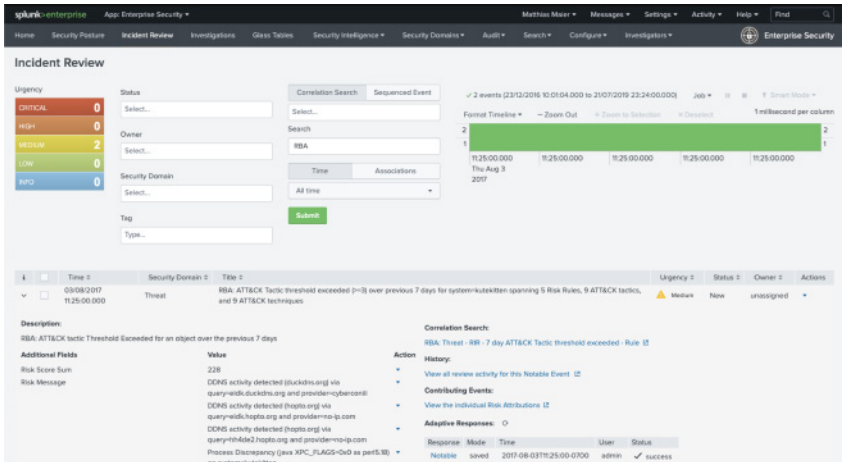
Donnez aux RSSI les moyens de renforcer la posture de sécurité, d'étendre les efforts de surveillance et justifier les nouveaux investissements.

Plutôt que d'avoir une politique unique, le cadre ATT&CK permet à un RSSI d'établir une posture de sécurité basée sur les besoins et le profil de risque de l'organisation. En établissant une correspondance avec les risques spécifiques, les attaques expérimentées, les groupes de menaces et les rapports de menace APT documentés, la direction de la sécurité peut identifier les lacunes de sa stratégie et élaborer une feuille de route pour renforcer le système de sécurité de l'organisation, que cela signifie une augmentation des effectifs, une plus grande visibilité ou de nouveaux outils de sécurité. Le cadre ATT&CK permet aux RSSI de concentrer leurs efforts de sécurité en fonction de la couche d'abstraction, de la criticité des applications ou des niveaux de journalisation. Par exemple, les vulnérabilités des actifs essentiels peuvent être couvertes par un ensemble spécifique de techniques MITRE, alors que d'autres techniques sont moins pertinentes pour les besoins de l'organisation. Un RSSI peut positionner le SOC pour investir plus de ressources dans ces techniques qui protègent les actifs les plus précieux, en s'assurant que les bonnes données sont collectées plus fréquemment et mises à disposition de manière centralisée en cas d'incident de sécurité majeur.

7

Donnez aux analystes SOC les moyens de développer un modèle d'alerte fondé sur les risques (RBA).

Quand les développeurs de contenus SIEM élaborent et mettent en place des systèmes de détection pour les techniques MITRE ATT&CK, les analystes peuvent être submergés par la quantité d'alertes générées. Pour hiérarchiser les techniques MITRE ATT&CK, les alertes peuvent être converties et transmises sous la forme de signaux capables d'associer une valeur de risque à un actif. En fonction du type de technique et de comportement observés, la valeur de risque peut être accrue ; on peut également appliquer un multiplicateur au calcul selon l'actif ou l'utilisateur impliqué. Cela crée une couche d'abstraction qui évite aux analystes SOC d'être submergés par les alertes et leur permet de se concentrer sur les actifs et les utilisateurs qui présentent le score de risque le plus élevé, afin de les examiner en priorité.



Titre de l'alerte : RBA : ATT&CK Seuil tactique dépassé (>=3) au cours des 7 derniers jours pour système=kutekitten spanning 5 - Règles de risque, 9 tactiques ATT&CK, et 9 techniques ATT&CK. Somme des scores de risque : 228.
Source : Splunk Enterprise Security

8

Donnez aux administrateurs SIEM les moyens d'assurer la qualité des données importées et les besoins de couverture.

Le travail de l'administrateur du SIEM est facilité lorsque l'équipe des opérations de sécurité et l'organisation dans son ensemble peuvent identifier les données, les logs et les événements dont ils ont besoin pour la lutte contre les menaces, la surveillance de la sécurité ou l'investigation sur les incidents. En utilisant le cadre MITRE ATT&CK, l'administrateur SIEM peut vérifier les données pendant le processus d'onboarding pour s'assurer que les besoins du SOC sont satisfaits ou si des outils supplémentaires sont nécessaires. La simulation des activités et des anomalies liées aux menaces est un mécanisme supplémentaire permettant de garantir la qualité et la couverture des données.

> **« Simulez des adversaires et créez des données pour vérifier si vos mécanismes de détection fonctionnent de bout en bout. »**
>
> – Dave Herrald, stratège en sécurité du personnel, Splunk

9

Donnez aux testeurs et aux "Red Teams" les moyens de prendre et documenter des décisions liées au risque en termes de couverture des logs et des composants.

Ceux qui réalisent les tests de pénétration et les red teams, ont pour objectif de trouver les points faibles dans un réseau informatique. La plupart du temps, la première question est : que doit-on faire pour prévenir le point faible ? Mais une question toute aussi importante (qui est souvent négligée) est celle de l'examination des activités qui conduisent à l'exploitation d'une faille et qui n'ont pas été détectées par le SOC. En bref, que vous travailliez avec une équipe de test de pénétration tierce ou avec votre SOC interne, le cadre MITRE ATT&CK est un excellent moyen de normaliser la communication. Une fois que tout le monde travaille avec le même cadre, il est plus facile et plus efficace d'examiner les tactiques et les techniques utilisées dans l'investigation et de déterminer l'emplacement des failles dans le système de sécurité.

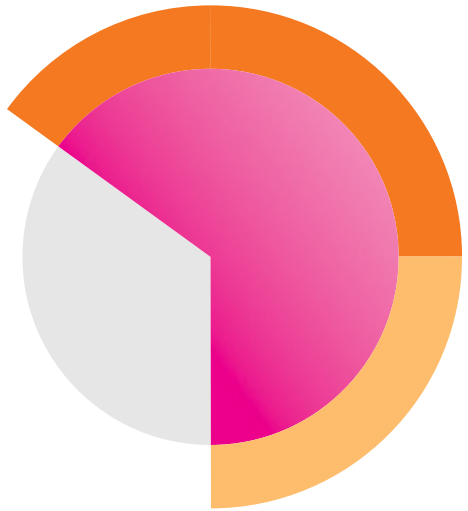
10

Donnez au service des achats et aux décideurs informatiques les moyens de définir les bases de la sécurité tactique et les besoins en matière de supervision et de réponses aux incidents

L'achat d'outils et de services auprès de tiers est une procédure opérationnelle standard pour les responsables informatiques et les chefs d'entreprise. Pour ces fournisseurs, s'assurer que leurs produits sont sécurisés et répondent aux exigences de conformité est une priorité. Ils sont régulièrement audités par leurs clients et les organismes de réglementation afin de valider leurs pratiques de sécurité. Pour les applications très critiques, le cadre MITRE ATT&CK offre une excellente couche pour définir plus en détails les exigences et dépasser les frameworks de gouvernance IT tels que les certificats ISO27001 et NIST-800-53. En particulier dans un modèle à responsabilité partagée, où la sécurité informatique d'une entreprise reste responsable d'une partie du service, il est essentiel que le prestataire autorise la collecte automatisée des suivis d'audit, et veille à ce que celui-ci contienne les bonnes données d'événements. Il faudra donc définir « les bonnes données d'événement » sur une couche d'abstraction indépendante de l'architecture du fournisseur, de l'évolution des menaces ou des nouveaux systèmes d'exploitation et fonctionnalités susceptibles d'être exploités par les pirates.

« Dans un monde numérique, les données sont devenues une obligation dans la planification stratégique des équipes de sécurité pour la détection des menaces et la réponse aux incidents pour protéger les activités, les clients et les collaborateurs d'une entreprise. »

– Matthias Maier, CISSP & CEH, évangéliste, Splunk



Pour commencer.

Avez-vous les bonnes données ? Posez-vous les bonnes questions ?

Découvrez les vastes possibilités de Splunk, la puissance du Search Processing Language (SPL), et essayez l'application Splunk Security Essentials App à retrouver sur Splunkbase.

20-47401-10-Ways-to-Take-Your-MITRE-ATT_CK-From-Plan-to-Action-FR-103-11x8.5-EB

splunk> turn data into doing™