Cinalia

Sécurisons votre digitalisation

Cyber Toolbox

MITRE ATT&CK

www.cinalia.com

Synelience GROUP

Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

MITRE ATT&CK

- Présentation de MITRE ATT&CK
- Framework MITRE ATT&CK

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

MITRE ATT&CK, présentation

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

Présentation de MITRE ATT&CK

1 QU'EST-CE QUE MITRE ?

2 QU'EST-CE QUE ATT&CK ?

3 QU'EST-CE QUE MITRE ATT&CK ?

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Qu’est-ce que MITRE?

MITRE est une ONG américaine qui travaille dans les domaines de l'ingénierie des systèmes, de la technologie de l'information, des concepts opérationnels et de la modernisation des entreprises.

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Qu'est-ce que MITRE?

/ Ressource gratuite et open source – fonctionne en communauté - son objectif est de soutenir la sécurité informatique défensive dans tous les secteurs, y compris les agences gouvernementales.

/ MITRE maintient la liste des CVE (Common Vulnerabilities and Exposures*).

/ En 2013, MITRE a mis en place la base de connaissance ATT&CK.

*Vulnérabilités et Expositions Communes

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Qu’est-ce que ATT&CK?

ATT&CK est l’un des projets les plus connus de MITRE. Il s’agit d’une base de connaissance des comportements de cyberattaque.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Qu’est-ce que ATT&CK?

- ATT&CK est l'acronyme de Adversarial Tactics, Techniques, and Common Knowledge*.
- Son objectif est d’aider les analystes en cybersécurité à obtenir des informations de cyberveille pour la planification et la conception de programmes de la cyberdéfense.
- Basé sur des scénarios du monde réel, il facilite la communication en fournissant un vocabulaire de référence commun.

*Tactiques, Techniques et Connaissances Communes des Adversaires

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

MITRE ATT&CK

→ Qu’est-ce que MITRE ATT&CK?

MITRE ATT&CK est un cadre de travail – « framework » – qui contient une base de connaissance des différents TTP (Tactiques, Techniques et Procédures) courants qui vont être utilisés par les groupes de menaces APT (Advanced Persistent Threat*).

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox

MITRE ATT&CK

→ Qu’est-ce que MITRE ATT&CK?

- Une campagne cyber offensive complète se compose de plusieurs étapes et nécessite la combinaison de plusieurs tactiques pour atteindre son objectif.
- MITRE ATT&CK utilise la perspective des TTP pour organiser les connaissances en cybersécurité dans un cadre hiérarchique.
- Les tactiques constituent la catégorie la plus élevée dans la hiérarchie ATT&CK et correspondent aux objectifs spécifiques que les attaquants cherchent à atteindre à différentes phases d'une attaque.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

MITRE ATT&CK, le framework

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

Le framework MITRE ATT&CK

1 PRÉSENTATION DU FRAMEWORK

2 LES TACTIQUES

3 LES TECHNIQUES

4 LES MATRICES

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Présentation du framework

Le framework offre une vision holistique des TTP. Cette base de connaissances est organisée en plusieurs niveaux :

- **Tactiques** : Les objectifs de haut niveau des attaquants (ex : Accès initial, Accès aux identifiants).
- **Techniques** : Les moyens utilisés pour atteindre les objectifs (ex : Phishing, Force brute).
- **Sous-techniques** : Des variantes spécifiques des techniques (ex : Spear phishing, Cassage de mot de passe).
- **Procédures** : Par exemple, APT33 a envoyé des courriels de spearphishing contenant des liens vers des fichiers .hta. APT41 a effectué des attaques par force brute sur le compte administrateur local.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Avantages du framework

- **Amélioration de la compréhension des menaces** : En identifiant les TTP les plus courants, les organisations peuvent mieux se préparer aux attaques.
- **Développement de défenses plus efficaces** : Le framework permet de mettre en place des contrôles de sécurité adaptés aux menaces spécifiques.
- **Meilleure collaboration** : Le langage commun fourni par ATT&CK facilite la communication et la collaboration entre les équipes de sécurité.
- **Suivi des tendances** : Le framework est mis à jour régulièrement pour refléter l'évolution des techniques d'attaque.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les tactiques de MITRE ATT&CK

Les tactiques sont au cœur du framework MITRE ATT&CK et représentent le « pourquoi » d'une technique ou d'une sous-technique ATT&CK.

www.cinalia.com

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les 14 tactiques de MITRE ATT&CK

- RECONNAISSANCE
- DÉVELOPPEMENT DES RESSOURCES
- ACCÈS INITIAL
- EXÉCUTION
- PERSISTANCE
- ÉLÉVATION DES PRIVILÈGES
- CONTOURNEMENT DES DÉFENSES
- ACCÈS AUX IDENTIFIANTS
- DÉCOUVERTE
- MOUVEMENT LATÉRAL
- EXFILTRATION
- IMPACT
- DESTRUCTION
- COMMANDE ET CONTRÔLE

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les techniques de MITRE ATT&CK

Les techniques du framework MITRE ATT&CK sont les moyens utilisés par les cyberattaquants pour atteindre leurs objectifs. Elles constituent une liste complète et détaillée des TTP connus, ce qui en fait une ressource précieuse pour les organisations qui cherchent à améliorer leur posture de cybersécurité.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les techniques de MITRE ATT&CK

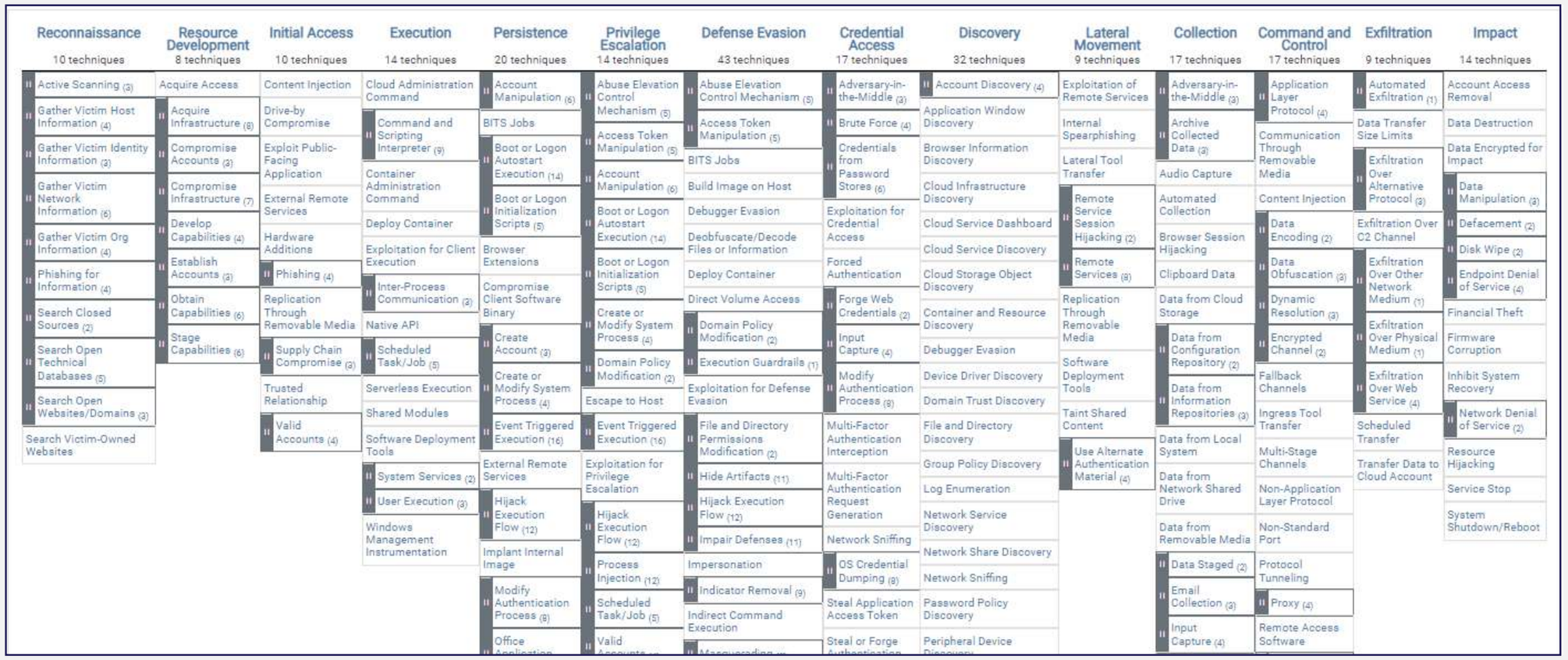
Quelques exemples :

- **Injection de contenu** : Injection de code malveillant dans une application web.
- **Phishing** : Envoi d'e-mails frauduleux pour inciter les utilisateurs à divulguer des informations sensibles.
- **Attaque par déni de service (DoS) sur l'endpoint** : Inondation d'un serveur avec du trafic malveillant afin de dégrader ses performances ou le rendre indisponible.
- **Elevation des privilèges** : Exploitation d'une vulnérabilité pour obtenir des privilèges plus élevés sur un système.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les techniques de MITRE ATT&CK



Voir le framework complet : https://attack.mitre.org/

Synelience GROUP
Smart Connection for Smart Solutions

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les matrices de MITRE ATT&CK

Les matrices MITRE ATT&CK sont des représentations tabulaires des tactiques et techniques utilisées par les cyberattaquants.

Le cadre complet MITRE ATT&CK est divisé en trois principales variantes (matrices), chacune contenant un sous-ensemble de TTP qui s'applique à des environnements informatiques cibles et spécifiques.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les matrices de MITRE ATT&CK

Il existe trois matrices de ATT&CK:

- **Matrice Enterprise** : Focus sur le comportement adversaire dans les environnements Windows, Mac, Linux et Cloud.
- **Matrice Mobile** : Focus sur le comportement adversaire dans les systèmes iOS et Android.
- **Matrice ICS (Système de Contrôle Industriel)** : Focus sur les actions qu'un adversaire peut entreprendre lorsqu'il opère au sein d'un réseau industriel.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Les matrices de MITRE ATT&CK

Les matrices MITRE ATT&CK peuvent être utilisées à plusieurs fins.

- **Cartographie des menaces** : Identifier les TTP qui constituent le plus grand risque pour une organisation.
- **Évaluation des contrôles de sécurité** : Déterminer si les contrôles existants sont efficaces contre les menaces identifiées.
- **Planification de la réponse aux incidents** : Définir les procédures à suivre en cas d'attaque.
- **Formation à la sécurité** : Sensibiliser les utilisateurs aux TTP les plus courants.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Comment utiliser une matrice MITRE ATT&CK ?

Triage des alertes, détection des menaces et réponse

De nombreuses solutions de sécurité, telles que SIEM, EDR.., peuvent intégrer les données de MITRE ATT&CK pour trier les alertes, enrichir les informations sur les menaces, et déclencher des protocoles de réponse aux incidents ou des réponses automatisées.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Comment utiliser une matrice MITRE ATT&CK ?

Recherche de menaces

C’est un exercice de sécurité proactive où sont recherchées des menaces qui ont échappé aux mesures de cybersécurité existantes tout en se basant sur les informations de MITRE ATT&CK.

Évaluation de la maturité du SOC

La matrice permet d’évaluer sa capacité à bloquer ou atténuer systématiquement les cybermenaces avec une intervention minimale ou nulle.

Cinalia
Sécurisons votre digitalisation

/ Cyber Toolbox
MITRE ATT&CK

→ Comment utiliser une matrice MITRE ATT&CK ?

Red Team/émulation d'adversaire

Les équipes de sécurité peuvent utiliser les informations de MITRE ATT&CK pour simuler des cyberattaques réelles, l'objectif est de tester l'efficacité des politiques, pratiques et solutions de sécurité mises en place, et d'aider à identifier les vulnérabilités à corriger.

Cinalia

Sécurisons votre digitalisation

Vous accompagner dans la maîtrise de vos enjeux de cybersécurité.

Un projet?
Des questions ?
N’hésitez pas à nous contacter.

www.cinalia.com

Synelience GROUP

Smart Connection for Smart Solutions