
MITRE


ATT&CK®

Qu'est-ce que MITRE ?

- Organisation à but non lucratif, fondée en 1958 ;
- MITRE gère trois centres de recherche et développement financés par le gouvernement fédéral ;
- Domaines de recherche : intelligence artificielle, informatique de santé, sécurité spatiale, l’expertise politique et économique, etc...

TOTAL CVE Records: 187329

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs are moving to the new CVE website.

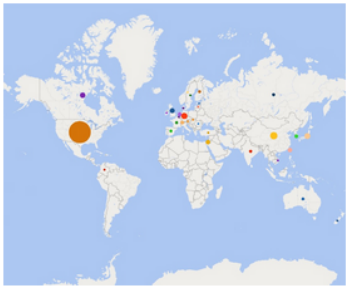
Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Go to new CVE website



Learn How to Become a CNA >>>

Newest CVE Records

Newest CVE IDs by @CVEnew

Follo

MITRE et cybersécurité

Projets/recherches que la MITRE Corporation a créés pour la communauté de la cybersécurité:

→ Le framework ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) ;

→ Base de connaissances CAR (Cyber Analytics Repository) ;

→ ENGAGE;

→ D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense) ;

→ AEP (Plans d'émulation ATT&CK)

MITRE et cybersécurité

- **Advanced Persistent Threat (APT « menace persistante avancée »)** : groupe (groupe de menace), pays (groupe d'État-nation), qui se livre à des attaques à long terme contre des organisations et/ou des pays. Les techniques utilisées par ces groupes APT sont assez courantes et peuvent être détectées avec les bonnes implémentations en place.

- **Tactics, Techniques, and Procedures (TTP) :** la tactique est le but ou l'objectif de l'adversaire ; la technique est la manière dont l'adversaire atteint le but ou l'objectif ; la procédure est la façon dont la technique est exécutée → attaques TTP

Framework ATT&CK®

- Depuis 2013 (Fort Meade Experiment, FMX) ;

- Référentiel de comportements de cyberattaques basé sur des observations concrètes de comportements adverses en cybersécurité, classés par tactiques et techniques → fournit une représentation complète des comportements d'attaque.

- Décrit les comportements adverses spécifiques aux environnements Windows, Linux, Mac, cloud et mobiles

- Alimenté par de nombreuses sources, telles que des chercheurs en sécurité et des rapports de renseignement sur les menaces. Notez qu'il ne s'agit pas seulement d'un outil pour les "blue teamers". Il est également utile aux "red teamers".

- Les entreprises puisent régulièrement dans sa base de connaissances pour élaborer des mesures offensives et défensives afin de renforcer leur position globale de sécurité.

Framework ATT&CK® et entreprises

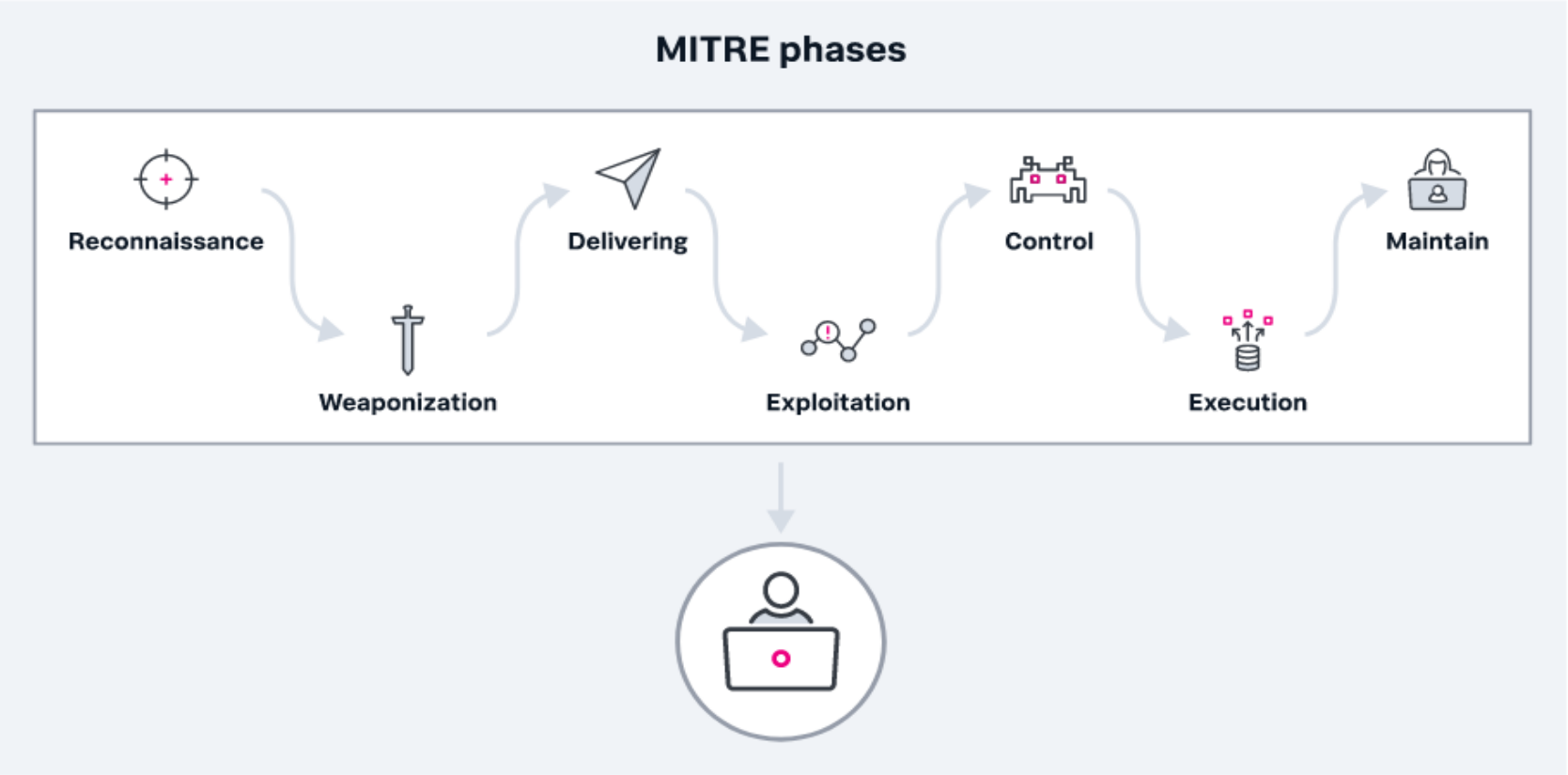
- **Sensibilisation et formation** : cette dimension comprend les programmes de sensibilisation des employés, la formation technique et les opportunités d'apprentissage.
- **Normes** : un cadre de normes de cybersécurité fournit une base commune pour l'identification, l'analyse et le partage des informations sur les menaces.
- **Outils** : MITRE fournit une gamme d'outils open-source qui aident les entreprises à analyser, détecter et prendre en charge les menaces

ATT&CK et le framework Cyber Kill Chain ?

MITRE ATT&CK Framework	Cyber Kill Chain
Initial Access	Reconnaissance
Execution	Intrusion
Persistence	Exploitation
Privilege Escalation	Privilege Escalation
Defense Evasion	Lateral Movement
Credential Access	Obfuscation/Anti-forensics
Discovery	Denial of Service
Lateral Movement	Exfiltration
Collection	
Exfiltration	
Command and Control	

Framework ATT&CK®

Cycle de vie d'une cyberattaque



But : Identifier lacunes sur les architectures de sécurité + réaliser investissements nécessaires pour renforcer défenses de sécurité

D3FEND MATRIX

- = Detection, Denial, and Disruption Framework Empowering Network Defense ;

- un graphique de connaissances des contre-mesures de cybersécurité ;

- encore en version bêta et est financé par la Direction de la cybersécurité de la NSA

ATT&CK® Emulation Plans

- **CTID** :

MITRE a créé une organisation appelée The Center of Threat-Informed Defense (CTID). Cette organisation est composée de diverses entreprises et fournisseurs du monde entier. Leur objectif est de mener des recherches sur les cybermenaces et leurs TTP et de partager ces recherches afin d'améliorer la cyberdéfense pour tous.

Quelques-unes des entreprises et des fournisseurs qui participent à la CTID :

- AttackIQ (fondateur) ;

- Verizon ;

- Microsoft (fondateur) ;

- Red Canary (fondateur) ;

- Splunk ;

→ Bibliothèque d'émulations d'adversaires et plans d'émulations ATT&CK

ATT&CK® and Threat Intelligence

- Grande spécialité de MITRE : le renseignement sur les menaces (Threat Intelligence/ TI) ou le renseignement sur les cybermenaces (CTI), l' l'information, ou les TTP, attribuée à l'adversaire ;

- Les grandes entreprises peuvent avoir une équipe interne dont l'objectif principal est de recueillir des renseignements sur les menaces pour d'autres équipes au sein de l'organisation, en plus d'utiliser les renseignements sur les menaces déjà disponibles ;

- Certaines de ces informations sur les menaces peuvent être open source ou faire l'objet d'un abonnement auprès d'un fournisseur, tel que CrowdStrike ;

Sources :

- https://julien.io/le-top-des-vulnerabilites-logicielles-mitre/
- https://www.splunk.com/fr_fr/data-insider/what-is-the-mitre-att-and-ck-framework.html
- https://attack.mitre.org/
- https://www.mandiant.com/resources/insights/apt-groups
- https://cve.mitre.org/
- https://www.cve.org/
- https://d3fend.mitre.org/
- https://cyware.com/blog/improve-detection-mechanisms-by-leveraging-cywares-mitre-car-contributions-7eda
- https://openclassrooms.com/fr/courses/1750566-optimisez-la-securite-informatique-grace-au-monitoring/7145826-ut
- https://hakin9.org/mitre-attck-framework-everything-you-need-to-know/
- https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
- https://www.logpoint.com/fr/blog/guide-logpoint-framework-mitre-att-ck/