

/ Cyber Toolbox 
MITRE ATT&CK



MITRE ATT&CK



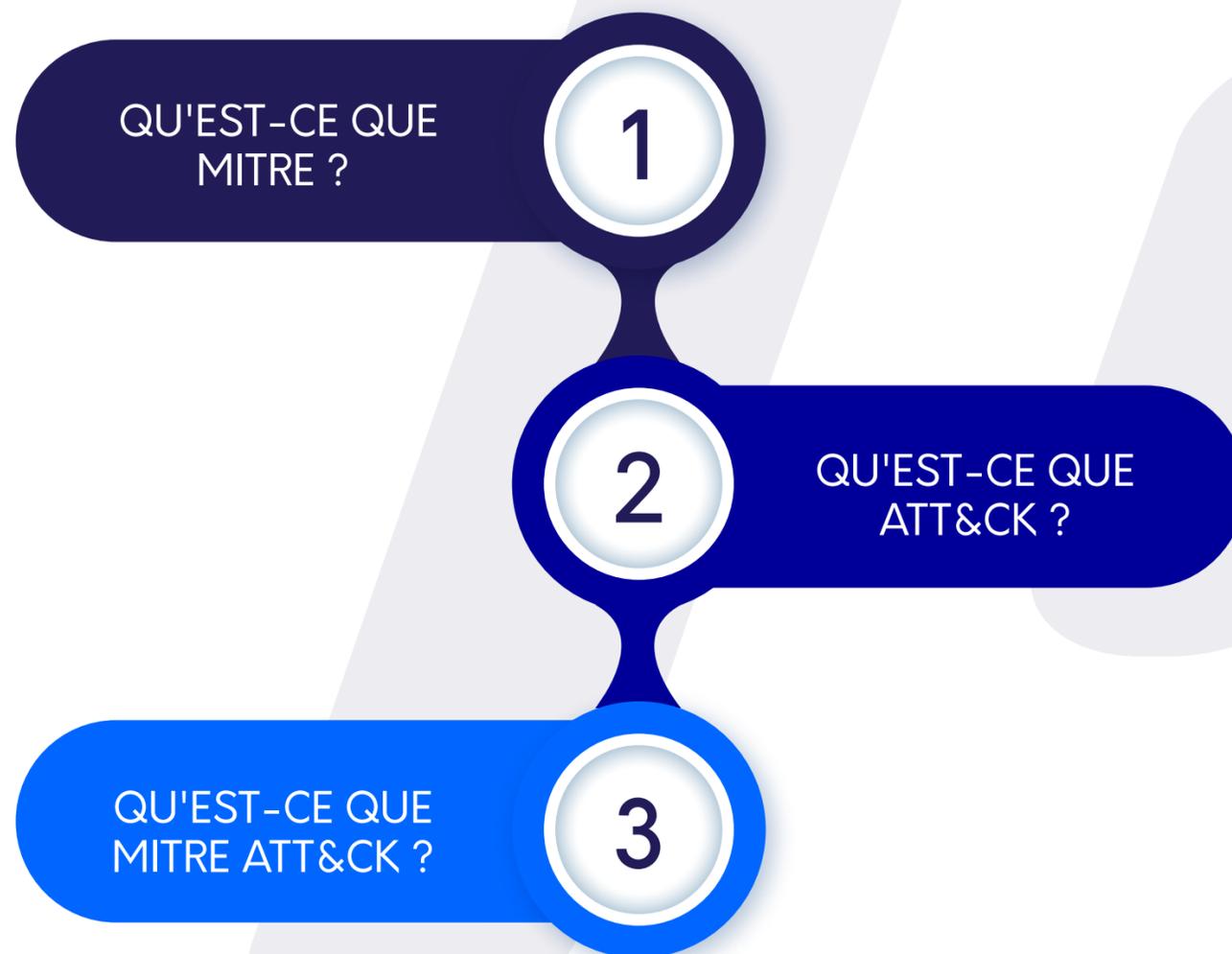
Présentation de
MITRE ATT&CK

Framework MITRE ATT&CK

MITRE ATT&CK, présentation



Présentation de 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.

→ 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

→ 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.

→ 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

→ 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*).

→ 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.

MITRE ATT&CK, le framework



Le framework 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.

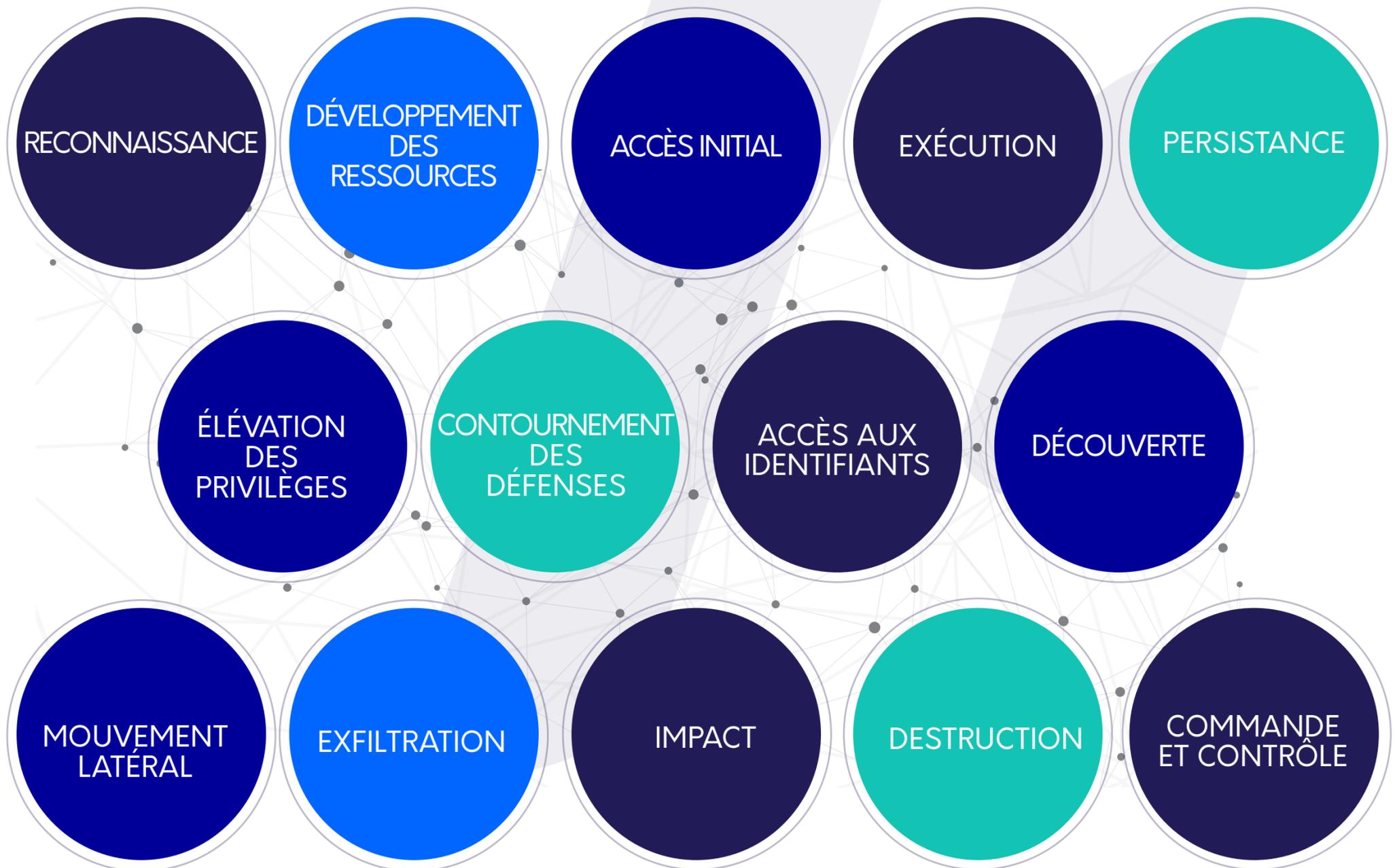
→ Avantages du framework

- / **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.

→ 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.

→ Les 14 tactiques de 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.

→ 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.

→ Les techniques de MITRE ATT&CK

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (2)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (5)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (2)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (5)	Replication Through Removable Media	Native API	Create or Modify System Process (4)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Domain Policy Modification (2)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Ingress Tool Transfer	Financial Theft
Search Open Websites/Domains (2)	Trusted Relationship	Serverless Execution	Shared Modules	Event Triggered Execution (16)	Event Triggered Execution (16)	Execution Guardrails (1)	Multi-Factor Authentication Process (8)	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Scheduled Transfer	Firmware Corruption
Search Victim-Owned Websites	Valid Accounts (4)	Software Deployment Tools	System Services (2)	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Device Driver Discovery	Data from Local System	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Inhibit System Recovery
	User Execution (3)	Windows Management Instrumentation	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Data from Removable Media	Data from Removable Media	Non-Standard Port		Network Denial of Service (2)
			Implant Internal Image	Process Injection (12)	Process Injection (12)	Hide Artifacts (11)	Network Sniffing	File and Directory Discovery	Data Staged (2)	Email Collection (3)	Protocol Tunneling		Resource Hijacking
			Modify Authentication Process (8)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Hijack Execution Flow (12)	OS Credential Dumping (8)	Group Policy Discovery	Input Capture (4)	Input Capture (4)	Proxy (4)		Service Stop
			Office Application	Valid Accounts (4)	Valid Accounts (4)	Impair Defenses (11)	Steal Application Access Token	Log Enumeration	Remote Access Software				System Shutdown/Reboot
						Indicator Removal (9)	Steal or Forge Authentication	Network Service Discovery					
						Indirect Command Execution		Network Share Discovery					
						Impersonation		Network Sniffing					
						Indicator Removal (9)		Password Policy Discovery					
						Indirect Command Execution		Peripheral Device Discovery					
						Unauthorized Access							

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

→ 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.

→ 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.

→ 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.

→ 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.

→ 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.

→ 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.



**Vous accompagner dans la maîtrise
de vos enjeux de cybersécurité.**

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



www.cinalia.com