Utilisation du référentiel ATT&CK pour outiller l'atelier 4

Présentation du fichier de filtrage

Contributeurs

Ludovic BORG
Laurent DUMOUSSAUD
Georges HANNA
Laurent IACOUCCI
Remi LIQUETTE
Sarra LOUSSAIEF
Jean OLIVE
Ayoub SABBAR

Responsable groupe

Valentin Lacaze

CLUBEBIOS

Sommaire

Résultat proposé

Ci-contre la partie dynamique de notre feuille d'output. Elle permet une vision de la technique sélectionnée

Ci-contre la partie filtrée de notre référentiel. C'est cette partie qui est générée à la suite du questionnaire.

Résultats de l'opération de filtrage	[Sous-]Technique sélectionnée	Critères de la [sous-]technique sélectionnée

Entrée(s): 220

Technique(s): 65

Sous-technique(s): 155

Technique	Altération du système pour une exécution automatique d'un code malveillant au démarrage
Sous-technique	*Sous-technique(s) retenue(s) par les filtres en colonne P*
Description	Un adversaire peut configurer un système pour automatiquement exécuter un ou plusieurs programmes/scripts pour conserver une emprise sur ce système ou gagner en privilèges.

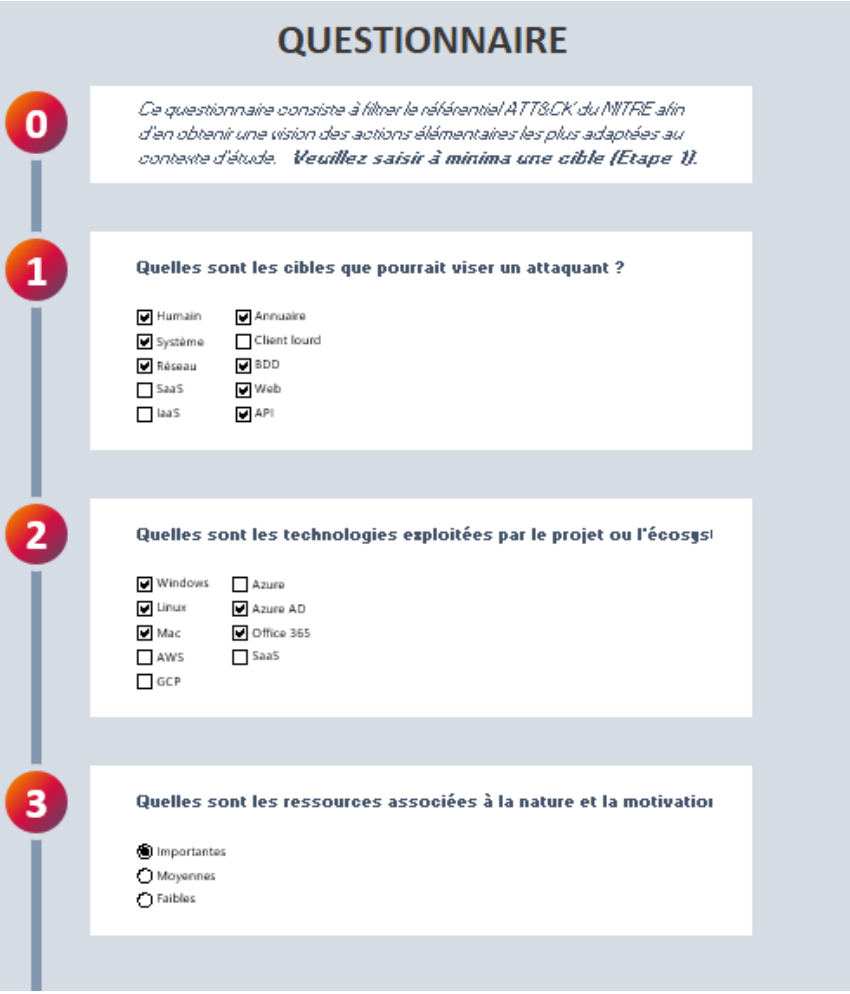
Cibles: Système

Technologies: Windows, Linux, Mac

Faibles | Moyennes | Importantes

CONNAITRE		RENTRER					TROUVER				EXPLOITER			
TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040	Liste des sous techniq
Reconnaissan	Préparation ressources	Accès initi	Execution	Persistanc	Elévation d privilèges	Evasion de défense	Récupérati d'authentifia	Découverte	Latéralisati	Collecte	Commande contrôle	Exfiltratio	Impact	
T1595 Ecoute active	T1583 Obtenir des biens supports tiers pour outiller les différentes phases d'attaques	T1566 Phishing	T1059 Exécution d'un script malveillant	T1133 Utilisation frauduleuse d'un accès distant	T1078 Usurpation de compte	T1078 Usurpation de compte	T1110 Brute force	T1087 Inventaire de compte	T1091 Propagation d'un malware via clé USB	T1056 Capture de saisie utilisateur	T1105 Installation sur un système compromis d'un C&C depuis une source	T1041 Exfiltration par canal C&C	T1486 Altération/des truction des données	T1547.001 Clé de registre / Dossier de démarrage
T1592 Collecter des informations sur le système cible	T1586 Compromettre un compte publique de la cible	T1133 Utilisation frauduleuse d'un accès distant	T1203 Exploitation d'une vulnérabilité d'un client lourd	T1078 Usurpation de compte	T1547 Altération du système pour une exécution automatique d'un code malveillant au démarrage	T1548 Elévation de privilèges par exploitation d'une vulnérabilité des mécanismes	T1056 Capture de saisie utilisateur	T1083 Exploration de fichiers et de répertoires	T1570 Exploitation de dispositifs de partage entre un système compromis et un système	T1114 Interception mail	T1132 Encodage de commandes pour le contrôle de système compromis	T1567 Exfiltration via service web	T1498 Déni de service réseau (congestion de bande passante)	T1547.002 Binaire malveillant marqué en "Authentication package"
T1589	T1584 Compromettre				T1546						T1001		T1499	

Prototype de filtrage proposé : questionnaire



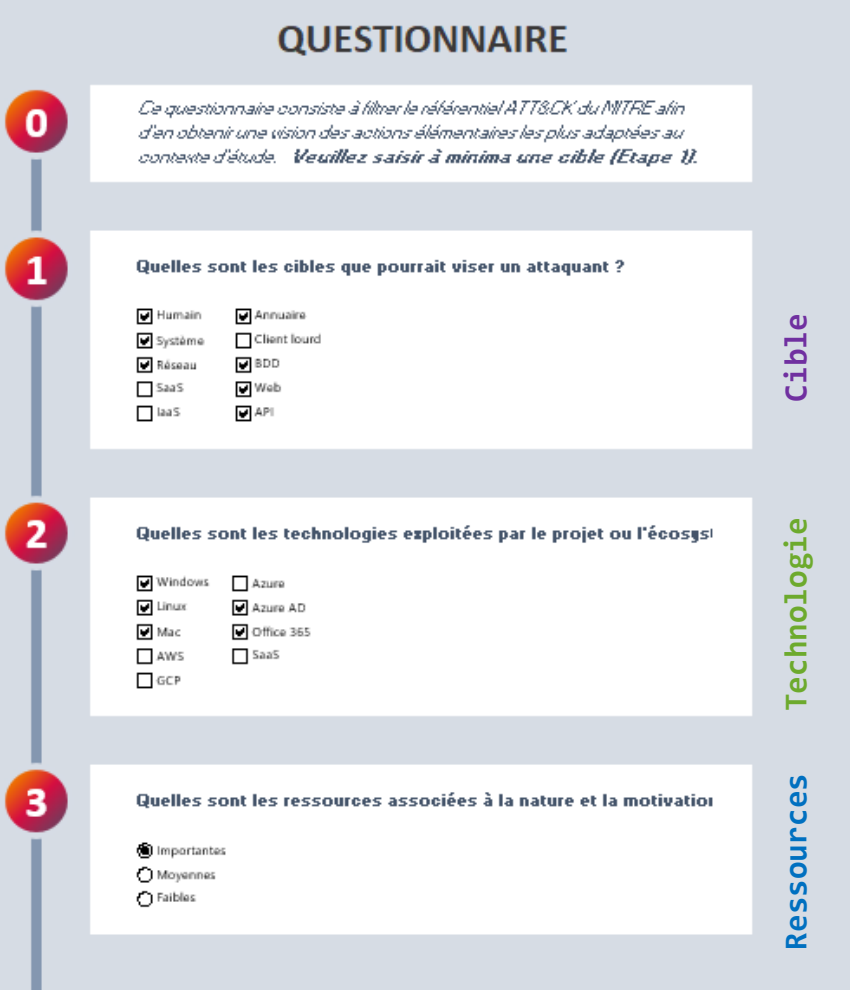
Critères de filtrage

1 : Choix des cibles visées par l'attaquant (attributs du Collège)

2 : Choix des technologies exploitées par le défenseur (attributs du MITRE)

3 : Choix des « ressources » maximales mis en œuvre par l'attaquant

Prototype de filtrage proposé : logique de filtrage




```
RessourcesMax ET (Cible1 ET Techno1 OU Cible1 ET Techno2
        OU … Cible_i ET Techno_j … OU Cible_n ET Techno_m)
OU RessourcesMax - 1 ET (Cible1 ET Techno1 OU Cible1 ET Techno2
        OU … Cible_i ET Techno_j … OU Cible_n ET Techno_m)
…
OU RessourcesMin ET (Cible1 ET Techno1 OU Cible1 ET Techno2
        OU … Cible_i ET Techno_j … OU Cible_n ET Techno_m)
```

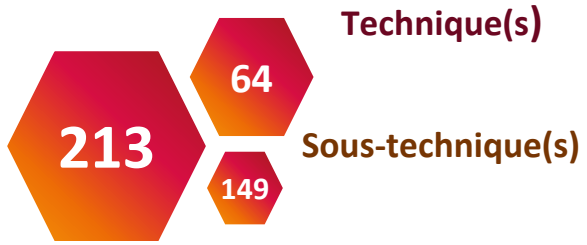
Nombre de critères de sélection :

$$RessourcesMax * n * m$$

Avec n le nombre de cibles et m le nombre de technologies sélectionnées.

⚠ Plus il y a de valeurs sélectionnées dans un même critère, moins le filtrage sera précis et plus les résultats seront nombreux.

Exemple

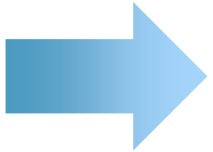


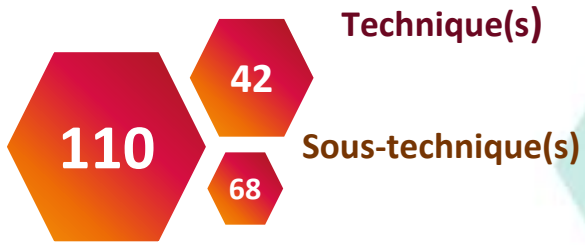
Entrée(s)

- Humain
- Système
- Réseau
- SaaS
- Annuaire
- Client lourd
- BDD
- Web
- API

- Windows
- Linux
- Mac
- Office 365

Faibles **Moyennes** **Importantes**



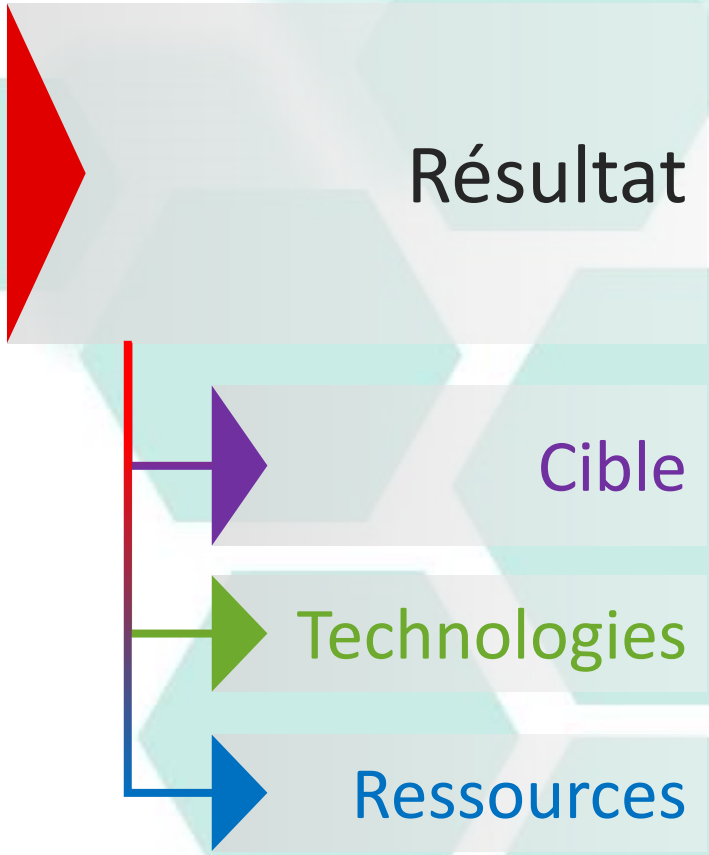


Entrée(s)

- Humain
- Système
- Réseau
- BDD
- Web
- API

- Windows
- Linux

Faibles

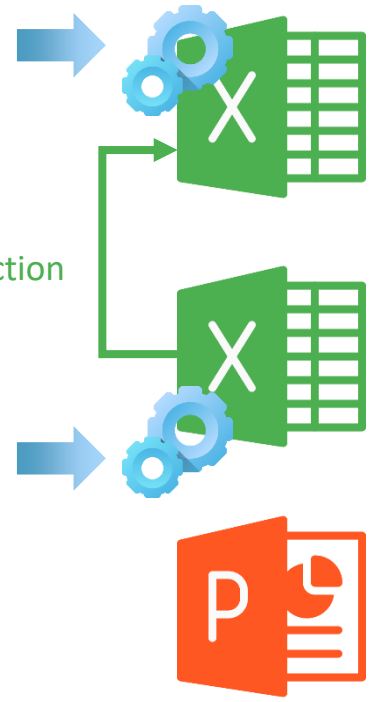


Livrable et dynamique du projet

Modification de la méthode de filtrage

Mise à jour de la base du fichier de sélection

Modification de la base du référentiel



ClubEbios_Selecteur-de-techniques_MITRE.xlsm

MITRE_ReferentielSupport_OutillageAtelier4EBIOS_FR.xlsx

Club EBIOS - Presentation du fichier de filtrage ATT&CK.pptx

Prochaines étapes

Livrer une v1.0 au Club Ebios

Challenger l'outil (notamment le filtrage)

Rechercher et remonter la présence d'éventuels bugs

Entamer les évolutions possibles du fichier (mises à jour automatique, construction de scénarios …)

Merci pour votre attention

CLUBEBIOS

Site : https://club-ebios.org
Twitter : @club_ebios
LinkedIn : https://fr.linkedin.com/company/club-ebios