



INTEGRATION ET RECETTE DE CYBERSECURITE :

Intégration et recette de cybersécurité :

1: Exercice 1 : AuditTAP :

1.1 : Windows :

SBD-421	Disable TLS1.1 Protocol (Client)	Registry key not found.	False
---------	----------------------------------	-------------------------	-------

Le protocole TLS 1.1 (Transport Layer Security 1.1) est une version de chiffrement utilisée pour sécuriser les communications réseau entre clients et serveurs.

Les hackers peuvent avec cette version intercepter des données sensibles et altérer les communications avec une attaque de type BEAST (injection de code malveillant dans le navigateur).

Il n'est pas mis à jour et ne prends donc pas le chiffrement moderne. Il est recommandé d'avoir au minimum TLS 1.2 et les navigateurs ne supporte plus cette version obsolète.

On va désactiver TLS 1.1 et mettre TLS 1.2 avec un script powershell pour l'activer rapidement sur tous les postes du réseau : TLS.bat

1.2 : Google :

SBD-437	Disable MD5 hash	Registry key not found.	False
---------	------------------	-------------------------	-------

Le MD5 est une fonction de hachage pour créer des empreintes numériques, vérifier l'intégrité des données et stocker des mots de passe (hachés).

Deux entrées différentes peuvent produire le même hachage MD5, ce qui rend cette fonction non fiable.

Le hachage MD5 est facilement cassable en peu de temps. Les normes PCI DSS et ISO 27001 déconseillent son utilisation car les attaquants peuvent modifier le contenu d'un fichier tout en aillant le même hachage.

On va désactiver le hachage MD5 et activer SHA-256 pour le remplacer :

MD5.bat

Office :

SBD-502	Ensure Windows Defender Application ID Service is running.	AppLocker is not running. Currently: Stopped	False
---------	--	--	-------

Le Windows Defender Application contrôle quelles applications et scripts sont autorisés à s'exécuter sur un système en appliquant des règles de sécurité prédéfinies.

AppLocker n'est pas activé, des logiciels malveillants peuvent s'exécutés librement, les règles de sécurité ne sont pas appliquées.

Intégration et recette de cybersécurité :

Activation de AppLocker :

Applocker.bat

2: Exercice 2 : Comparatif d'outils :

SafetyCulture

Critère	Description	Exemple/Détails
Facilité d'utilisation	Interface intuitive	modèles personnalisables pour une prise en main rapide
Comptabilité multiplateforme	Application mobile et interface web	iOS et Android
Conformité	Renforcer la conformité	Remplaçant les évaluations faites à la main par des procédures automatisées et simplifiées sur ordinateur.
Cout et licences	Version gratuite pour 10 personnes maximum (sinon 24 \$/mois)	
Automatisation	d'automatisation pour les inspections et les audits, avec des rapports générés automatiquement.	

Safesite

Critère	Description	Exemple/Détails
Facilité d'utilisation	Interface conviviale	l'identification des causes profondes des problèmes
Comptabilité multiplateforme	Application mobile et interface web	iOS et Android
Conformité	gère les systèmes de sécurité et de garantir la conformité aux réglementations en vigueur	Garantit le respect des normes en vigueur et facilite les audits de conformité
Cout et licences	Fonctionnalité de base gratuite sinon 16 \$/mois	
Automatisation	automatiser les inspections et audits de sécurité	Génération automatique des rapports et suivi des actions correctives

Intégration et recette de cybersécurité :

FORM opX

Critère	Description	Exemple/Détails
Facilité d'utilisation	Modèles configurables	Guide les équipes tout au long du processus d'audit
Comptabilité multiplateforme	Application mobile et interface web	iOS et Android
Conformité	Réduire les risques et à améliorer les systèmes de sécurité	Collecte des données importantes et en attribuant des flux de travail.
Cout et licences	Version de base gratuite, options payantes sur demande	Tarif sur demande popur
Automatisation	Automatisation des flux de travail	Génération automatique des rapports et attribution des tâches en fonction des règles prédéfinies

3: Sources :

[Les 7 meilleurs logiciels d'audit de la sécurité de 2024](#)

[PowerShell Documentation - PowerShell | Microsoft Learn](#)

[Mobile Forms App | The Digital Assistant for the Frontline](#)

<https://safesitehq.com/>

[PCI Security Standards Council – Protect Payment Data with Industry-driven Security Standards, Training, and Programs](#)

[ISO/IEC 27001:2022 - Systèmes de management de la sécurité de l'information](#)