VOLTRON
Sécurité

Proposition d'audit

Audits

Pourquoi ?

L'organisation Vignerons Indépendants cherche à améliorer la gestion de ses vignobles grâce à un nouveau système. La sécurité de ce système doit être vérifiée afin que les données à caractères sensibles soient protégées à tout moment et que les cybercriminels ne puissent pas nuire au bon fonctionnement du système.

Liste des différents audits :

Audit de conformité

Description : Cet audit a pour objectif de vérifier si une organisation se conforme aux normes, aux réglementations et aux politiques internes en matière de cybersécurité

Objectif : Cet audit compare les pratiques de sécurité de l'organisation avec les exigences spécifiques, telles que le respect du RGPD, de la norme ISO 27001… L'objectif est de s'assurer que l'organisation respecte les normes de sécurité établies.

Audit de vulnérabilité;

Description : Cet audit vise à identifier les vulnérabilités techniques présentes dans le système et les applications.

Objectif : Il consiste en l'analyse de la configuration des réseaux, des serveurs, des applications et des dispositifs pour détecter les failles potentielles qui pourraient être exploitées par des attaquants. L'objectif est de corriger ces vulnérabilités avant qu'elles ne soient exploitées pour compromettre la sécurité des systèmes.

Audit de gestion des identités et des accès

Description : Cet audit évalue les pratiques de gestion des identités et des accès d'une organisation. Il comprend l'examen des politiques d'authentification, des contrôles d'accès, des droits d'utilisation et des processus de gestion des comptes utilisateurs.

Objectif : Cet audit permet de s'assurer que les droits d'accès sont correctement attribués, que les utilisateurs authentifiés sont dûment vérifiés et que les privilèges sont correctement gérés.

Audit de tests d'intrusion

Description : Cet audit, également appelé test d'intrusion ou pentest, simule une attaque informatique sur les systèmes de l'organisation pour identifier les vulnérabilités et les faiblesses. Il comprend donc souvent les audits précédents.

Objectif : L'objectif est de détecter les failles de sécurité et de fournir des recommandations pour les corriger avant qu'elles ne soient exploitées par des attaquants réels.

Audit de red-team

Description : Cet audit, s'apparente au test d'intrusion, celui-ci s'approche plus de la réalité dans le sens ou seulement un minimum de personnes sont au courant de son exécution.
C'est un test grandeur réel où tous les moyens sont bons pour atteindre l'objectif de compromettre le système (phishing, social engineering …)

Objectif : L'objectif est de détecter les failles de sécurités techniques mais également sociales et de fournir des recommandations pour les corriger avant qu'elles ne soient exploitées par des attaquants réels.

Propositions

Chacune des propositions ont été budgétisée et leur réalisation estimée dans le temps. L'ensemble des coûts et leurs justifications sont disponibles dans les deux documents suivants:

- Tableau des coûts

Proposition minimale

La solution réfléchie par l'équipe d'experts en sécurité en ce qui concerne la proposition minimale est composée de:

- Un atelier de sensibilisation aux concepts de sécurité pour tous les employés. Cet atelier comprend des exemples d'impacts de cyberattaques ainsi que les bonnes pratiques à prendre en compte dans le cadre de l'utilisation du système d'information.
- Un audit de conformité permettant de valider les normes mise en place sur les bases de données et l'échange de données afin de respecter les normes RGPD
- Un audit de vulnérabilité simple sur les différentes applications critiques afin de voir si les technologies utilisées sont à jour et sécurisées.
- Un audit des droits sur les différents référentiels ou applications, afin de voir si les applications appliquent bien le concept du moindre droit.

Proposition intermédiaire

- L'ensemble des solutions composant la proposition minimale sont reprises et combinées aux propositions suivantes.
- Un test d'intrusion complet, dans lequel sont repris les audits précédents et auquel s'ajoute un test d'intrusion qui permet de simuler une cyberattaque.

- Un accompagnement est mis en place suite aux différentes restitutions pour aider les équipes techniques sur les résolutions des points détectés.

Proposition intégrale

Enfin, la solution réfléchie par l'équipe d'experts en intelligence artificielle en ce qui concerne la proposition intégrale est composée de:

- L'ensemble des solutions composant la proposition intermédiaire sont reprises et combinées aux propositions suivantes.
- Un audit de red-team s'ajoute au préalable du test d'intrusion pour pouvoir également tester l'aspect social de la sécurité.

Récapitulatif des propositions

	Proposition minimale	**Proposition intermédiaire**	**Proposition intégrale**
Atelier Sensibilitation à la cybersécurité	✅	✅	✅
Audit de conformité	✅	✅	✅
Audit de vulnérabilité	✅	✅	✅
Audit de gestion des identités et des accès	✅	✅	✅
Accompagnement post-audit	❌	✅	✅
Audit avec une équipe de red-team	❌	❌	✅
Accompagnement complet	❌	❌	✅