Cahier des charges : Déploiement de l'EDR CrowdStrike

1. Objectif

Déployer et configurer l'EDR CrowdStrike sur l'ensemble des postes de travail et serveurs de l'entreprise (MacOS, Windows, Linux) afin d'assurer :

- La détection et la prévention des menaces.
- La centralisation de la supervision des endpoints via CrowdStrike Falcon.
- La conformité avec les politiques de sécurité internes.

2. Périmètre

- **Postes de travail :** MacOS, Windows 10/11, Linux (Ubuntu)
  - 150 Postes Windows 11
  - 10 Postes Mac Books
- **Serveurs :** Windows Server 2016 et 2019
- **Méthodes de déploiement :** Manuelle pour les Mac Book. Automatisée pour le pc windows (via GPO avec l'utilisation d'un script fourni).

3. Prérequis

3.1. Informations nécessaires

- **Exécutable d'installation** spécifique à l'OS.
- **Identifiant client (CID)** fourni par CrowdStrike dans Stoïk Protect → Endpoint → Paramètres.
- **Permissions administratives** sur les machines.
- **Accès GPO** pour les installations automatisées.

3.2. Systèmes et versions supportées

OS	Version des OS supportée	Remarques
MacOS	15.7.3 macOS Tahoe 26.2 macOS Sequoia	Installation manuelle
Windows	Windows 11	Installation via GPO
Linux	Ubuntu 24	Installation via manuelle

4. Méthodes de déploiement disponibles sur le site officiel

4.1. MacOS (EDR CrowdStrike sur MAC)

4.2. Windows (EDR CrowdStrike sur Windows)

4.3. Linux (EDR CrowdStrike sur Linux)

5. Contrôles et validation

- Vérifier que tous les endpoints apparaissent dans **Stoïk Protect → Endpoint → Actifs surveillés**.
- Vérifier le fonctionnement du processus de l'EDR dans le gestionnaire de tâches.
- Documenter les anomalies et refaire l'installation si nécessaire.

6. Sécurité et bonnes pratiques

- Toujours utiliser le **CID officiel** pour chaque environnement.
- Effectuer l'installation avec des droits administrateurs.
- Autoriser toutes les extensions de sécurité requises sur MacOS.
- Tenir à jour l'EDR pour bénéficier des dernières protections.

7. Documentation et support

- Fournir un guide d'installation spécifique pour chaque OS.
- Maintenir un journal des installations.
- Contacter le support CrowdStrike en cas de problème de déploiement ou de compatibilité.

Adresse Mail : protect@stoik.io ou par téléphone : XX XX XX XX XX