TD Méthodologie d’analyse des systèmes d’information

# Projet Data loss prevention

**Contexte projet**

Une solution de prévention contre la fuite de données sensible, plus communément appelée « solution DLP », permet uniquement d’identifier et prévenir les actions utilisateurs non conformes. La DLP fonctionne à l’aide d’agents sur les postes de travail et/ou de sondes réseaux.

Chaque action non-conforme aux règles établies génère une alerte. Cela peut se traduire par trois principaux types de procédés :

* Une remontée d’alerte vers la console d’administration, invisible pour l’utilisateur.
* Un avertissement, c’est à dire un message s’affichant momentanément sur l’écran afin d’informer l’utilisateur que l’action en cours est non-conforme aux exigences de sécurité.
* Un blocage de l’action non-conforme.

Solution Forcepoint Triton AP-Endpoint :

Triton Data Endpoint est une solution DLP simple, complète et sécurisée. L'outil permet de monitorer en temps réel le trafic réseau et d'appliquer des politiques DLP définies sur des applications et zones de stockages de fichiers. Il est également possible créer des mesures pour la découverte de documents sensibles sur le poste ou le réseau.

Triton AP-DATA analyse tous les emails envoyés depuis le poste de travail pour détecter les envois de données sensibles. Les flux webmails sont également traités par l'agent. Data Endpoint peut analyser les fichiers qui sont utilisés par les applications du poste de travail. Il peut suivre les copier/coller, les impressions et les impressions d'écran. L'agent analyse le trafic web et les flux vers les supports de stockages amovibles.

Triton AP-WEB est une technologie Forcepoint reconnue comme leader sur le marché depuis 20 ans de catégorisation d’URLs. Ce module a l’avantage de fournir l’information de contexte sur Internet. Exemple l’utilisateur A de la division B a transmis un rapport d’audit sur la nouvelle plateforme de collaboration XXX catégorie Personal and Network Storage. Cela nécessite des mises à jour fréquentes des catégories de sites web puisque des plateformes émergent régulièrement sur Internet. La mise à jour par Internet est nécessaire et celle-ci correspond à un service Windows proxifié avec authentification possible.

**Fonctionnement**

La solution permet de protéger les données sensibles contre les risques suivants :

* Fuite de données sensibles par mail
* Fuite de données sensibles vers le cloud/serveurs privés
* Fuite de données sensibles par clé USB
* Malveillance interne, protection contre la malveillance volontaire ou involontaire interne
* Malveillance interne/externe, exfiltration de données sensibles par un automate (DTP), fuite de données partielles, fuite de faible quantité de données régulièrement

Les cas d'usage définis par le métier sont les règles de l’outil qui vont remonter des alertes dans la console d'administration. Ces règles comprennent des actions interdites par l'utilisateur du poste de travail en termes de gestion des documents. Lorsqu'une action non-autorisée est réalisée, une alerte est levée.

Les alertes remontées par les clients Forcepoint des postes de travail des utilisateurs à la suite d’actions interdites sont centralisées dans une base et accessible depuis une console d’administration. Ces alertes contiennent des informations sur l'action qui a été réalisé, par qui (IP+identifiant), quand, sur quels documents.

Les fichiers sensibles ayant remontés des alertes sont sauvegardés pour les besoins de forensics.   
Lorsqu'une alerte est déclenchée, elle est ajoutée dans le tableau de bord d'administration et le fichier correspondant à l'alerte est copié sur un serveur de fichier afin d'avoir preuve de l'action interdite.

**Choix techniques**

Un agent Forcepoint Triton est installé sur chaque poste de travail. Chaque agent est identifié auprès du serveur Endpoint comme client. Le déploiement de la solution TRITON nécessite :

* Un serveur TRITON AP-DATA
* Une base de données SQL pour la sauvegarde des données de forensic

Forcepoint chiffre tous les échanges entre la console d'administration et les clients avec une PKI interne à l'outil.

Pour le module AP-WEB, il est nécessaire d'avoir un accès web pour le serveur Triton afin de se connecter à Forcepoint pour mettre à jour la liste des plateformes web que l'outil surveille.

**Objectif du projet**

L’entreprise souhaite identifier, localiser et protéger les données sensibles et l’usage qu’il en est fait. L’objectif est d’avoir un outil permettant de maitriser et de protéger son patrimoine informationnel.

Question :

Identifier les données manipulées/créées/utilisées par le projet.

Définir les enjeux de sécurité du projet et justifier en termes de besoins et d’impacts.