TRAÇABILITE DES ACTIONS ET POST-MORTEM : ARCHITECTURE FONCTIONNELLE, TECHNIQUE ET EXPLOITABILITE D'UN LOG-SINK

Dans un contexte où **le SI est devenu le support indispensable à toutes les entreprises**, les enjeux sont de plus en plus forts pour les DSI comme pour les attaquants. Les méthodes d'attaque sont de plus en plus sophistiquées et s'industrialisent : les temps de propagation des malwares sont de plus en plus courts et ces derniers de plus en plus invasifs.

Pourtant, à moins d'une attaque aux symptômes particulièrement sévères à l'instar de NotPetya, **le temps moyen avant détection d'une intrusion est de 197 jours**. Les entreprises sont en effet souvent « dans le noir » quant à l'activité en leur sein. À des fins de visibilité et de traçabilité des actions, elles ont besoin de mettre en place un SIEM (Security Information and Event Management) : il s'agit d'un **centre d'analyse des logs** collectés sur les serveurs du SI. Ces logs doivent donc être collectés de manière fiable et sécurisée, puis structurés en un point central pour faciliter l'exploitation des données qu'ils contiennent. Ce point central s'appelle un log-sink.

Objectif du stage

Ce stage a pour but de vous faire suivre la démarche d'un architecte, tant au niveau fonctionnel que technique. Vous serez amenés à déterminer quelle est l'architecture la plus efficace à mettre en place afin de collecter des logs et les analyser de sorte à sécuriser le SI. Une étude comparative des solutions ELK et Splunk viendra compléter cette architecture afin de déterminer quelle solution est la plus pertinente.

Le métier d'architecte étant pleinement ancré dans la réalité de l'entreprise, vous vous appuierez sur vos travaux précédents pour réaliser un démonstrateur. Celui-ci vous permettra de prouver le bon fonctionnement de votre architecture, mais également d'en tirer des bonnes pratiques empiriques directement applicables chez nos clients. Celles-ci représentent les fondations nécessaires à l'industrialisation de la solution.

Les objectifs du stage sont de :

- Appréhender les concepts d'architecture d'entreprise et les modèles de sécurité
- Identifier forces et limites des stack ELK et Splunk, leurs apports et leurs limites d'un point de vue architectural (respect des objectifs, élégance de la solution) et d'un point de vue projet (facilité d'implémentation, coût des licences, présence d'un support professionnel)
- Définir une méthode objective de structuration des logs, argumentée et appuyée sur des cas concrets
- Industrialiser le processus de collection et structuration de logs pour être en mesure d'accompagner nos clients dans la mise en place de la solution adaptée à leurs besoins

Travaux à réaliser

Appuyé par un consultant expérimenté vous aurez la responsabilité de mener les travaux suivants :

- Rédiger une note de cadrage du sujet de stage, comprenant :
  - Votre compréhension du stage
  - Le planning et les jalons clés
  - La liste des livrables à réaliser
- S'approprier et formaliser les concepts autour de l'architecture d'entreprise et les modèles de sécurité
- Définir une architecture de collecte et d'analyse de logs
- Mener une étude comparative des solutions ELK et Splunk
- Définir une méthode de structuration de logs
- Réaliser un démonstrateur autour de la solution retenue
- Industrialiser le processus de collection et structuration de logs au sein d'une DSI
- Participer à l'élaboration des séminaires « Vue d'ensemble des briques fonctionnelles de sécurité du SI » de Nexworld
- Rédiger un Livre blanc ou amender des livres blancs existants.

En parallèle, vous participerez à des missions de conseil, en intégrant une équipe de consultants Nexworld placée sous la responsabilité d'un directeur de mission.