Documentation des processus de détection, d'investigation, et d'outillage

Ce document a pour vocation d'expliciter les processus de détection, d'investigation, ainsi que d'outillage mis en place par AEGIS CyberProtect, filiale cybersécurité du groupe AEGIS pour le compte du client Dunder Mifflin. Ce document explique synthétiquement l'architecture de supervision générale élaborée pour le client, dans l'objectif de la sécurisation de leurs systèmes d'information.

1/ Le système de détection, d'investigation, et d'outillage

a) MCO / MCD

a-1) Politiques de supervision

L'ensemble des machines du client sont surveillées en permanence par divers logiciels chargés de remonter n'importe quel évènement s'étant produit sur la machine (log). Ces logiciels diffèrent en fonction du système d'exploitation de la machine client supervisée. Pour les machines Windows, les systèmes chargés de journaliser les évènements sont Auditpol et Sysmon. Auditpol est un système Windows natif permettant la définition ainsi que la consultation de politique de supervision. Sysmon fournit quant à lui un système d'audit avancé et détaillé, ajoutant un niveau de précision supplémentaire à Auditpol.

Quant au système Linux, le système d'audit mis en place se nomme Kunai. Il s'agit d'un outil configurable non natif permettant de surveiller un système Linux.

a-2) Envoi des log

Une fois les fichiers de journalisation créés, il ne reste plus qu'à les transférer à notre premier maillon de cette architecture de supervision : Splunk. Nous utilisons un outil appelé Splunk Universal Forwarder permettant, comme son nom l'indique, de « forward » les logs, à savoir donc les transmettre à Splunk afin qu'il les ingère. Splunk Universal Forwarder est donc installé sur les machines Windows, et Linux du client.

b) Workflow d'investigation

b-1) Schéma d'investigation

Voici ci-dessous une représentation schématique synthétique explicitant le cheminement effectué par les logs tout au long de leur cycle de vie : de leur création au traitement de leurs actions inhérentes ainsi que de la communication client associée.

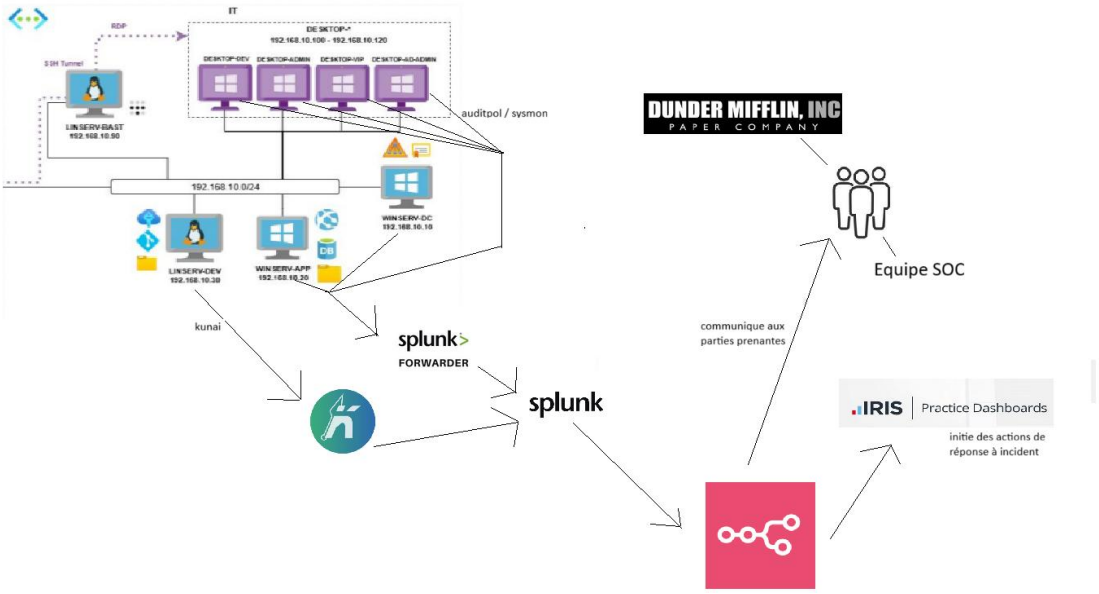

Figure 1 - Architecture générale/Workflow d'investigation

b-2) Splunk : Premier maillon

Splunk est un logiciel « SIEM » chargé d'ingérer ces logs, de les classer et de les trier. Il constitue la première étape de l'investigation que l'équipe SOC sera amenée à mener. A partir de cette interface, nous érigeons des règles associées aux logs reçus, pensées spécialement à se déclencher dans des cas d'évènements les plus suspects.

i	Heure	Événement
>	27/11/2025 19:49:46,000	{ [-] data: { [-] ancestors: /usr/lib/systemd/systemd|/usr/sbin/sshd|/usr/sbin/sshd|/usr/sbin/sshd|/usr/bin/bash command_line: cat /etc/shadow exe: { [+] } path: /etc/locale.alias } info: { [+] } }

Figure 2 - Exemple de log Splunk

Prenons l'exemple de cet évènement présent dans splunk, remonté depuis une machine Linux. Il nous indique par exemple l'exécution de la commande « cat /etc/shadow », indiquant une tentative de lecture d'un fichier sensible. Associé à cet évènement, une alerte se déclenche et alerte de façon frontale l'équipe SOC. A la suite du déclenchement de cette alerte, l'équipe SOC analyse la fiche réflexe associée à

cette règle, nous indiquant la marche à suivre : investigations à opérer pour déterminer si cette menace est avérée, actions à mener le cas échéant…

Ce système SIEM constitue le premier pilier de notre architecture de supervision.

b-3) n8n

Le second maillon de notre architecture de supervision est l'application n8n. Il s'agit d'un logiciel d'automatisation chargé de mettre en relation les alertes splunk précédemment mentionnées, avec différents modules. Il nous permet premièrement de relier ces alertes avec IRIS, un système de réponse à incident. N8n propose également un système de communication automatisé, à la fois pour les équipes techniques et le client, en fonction des alertes rencontrées. Il permet par exemple d'informer premièrement les équipes techniques qu'une attaque x a été détectée, active ensuite les systèmes de réponse appropriés sur IRIS, puis communique au client l'évènement ainsi rencontré et qu'une investigation est en cours.

b-4) IRIS

IRIS nous permet de prendre des actions de façon prédéfinie, en réponse à un type d'alerte correspondant. Cela permet une vitesse de réaction certaine, et constitue une première barrière à la menace.

b-5) Récapitulatif

Pour résumer, : l'équipe SOC reçoit sur le SIEM Splunk les logs générés par sysmon, auditpol et kunai. Des alertes sonnent, et l'équipe SOC consulte les fiches réflexes associées. Elles détaillent précisément les démarches d'investigation nécéssaires à la confirmation d'une menace, mais également les mesures préventives associées à l'alerte définies dans IRIS, ainsi que la communication client.