# Supervision de poste via ESET

* Dans la tache de projet suivante, j'ai été chargé de manipuler la console web d'ESET afin de réaliser une vérification des alertes. Grâce à cette console, j'ai pu accéder à toutes les informations pertinentes concernant les alertes de sécurité détectées par l'antivirus ESET. J'ai utilisé différentes fonctionnalités offertes par la console pour analyser en détail ces alertes, telles que leur niveau de gravité, leur origine et les actions recommandées pour y remédier. Mon objectif était d'effectuer une vérification complète et rigoureuse de chaque alerte, en prenant les mesures nécessaires pour garantir la sécurité optimale des systèmes informatiques des clients de l’entreprise. Cette tache de projet est composée de trois sous taches comme le montre la capture ci-dessous :

Une image contenant texte, Police, ligne, blanc

Description générée automatiquement

## 1.1 Reconnaissance des alertes.

* Comme pour chaque tache effectuée au sein de l’entreprise, j'ai créé un ticket dans GLPI concernant cette tâche de projet. Cela permet de garder une trace claire de l’avancée de la tâche.

### Attribution du ticket.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* Dans un premier temps la première étape consistait à établir une connexion initiale à la console web d'ESET afin d'obtenir un aperçu des alertes liées aux menaces ainsi que des alertes spécifiques aux différents postes clients. Pour cela, j'ai utilisé mes identifiants d'accès fournis par l'entreprise et j'ai suivi les instructions pour me connecter à la console web d'ESET. Une fois connecté, l’interface de la console se présente de la façon suivante :

Une image contenant texte, logiciel, Icône d’ordinateur, Logiciel multimédia

Description générée automatiquement

* J’ai donc dans un premier temps exploré les différentes sections de la console qui regroupaient les informations sur les alertes de sécurité critiques détectées :

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

* Ainsi que les différents alertes présents sur les postes clients :

Une image contenant texte, logiciel, capture d’écran, Icône d’ordinateur

Description générée automatiquement

### Alimentation du ticket.

* Une fois que j’ai pris connaissance des différentes alertes, il me fallait répertorier celle-ci sous forme de tableau. Pour cela ESET fournit une fonctionnalité permettant de télécharger les alertes sous forme de tableau au format .csv comme le montre la capture ci-dessous :

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

* J’ai donc pu renseigner facilement les tableaux d’alerte dans le ticket comme le montre la capture ci-dessous :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

## 1.2 Classification des alertes.

### Attribution du ticket.

Une image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

* La seconde partie de cette tache de projet consistait en la classification des alertes en fonction de leur traitement. Les alertes traitables immédiatement ne nécessitaient pas de redémarrage ou d'actions pouvant rendre la machine indisponible et pouvant nuire à l’activité du client.
* Les alertes traitables ultérieurement impliquaient des actions pouvant rendre la machine indisponible pendant un certain temps. Cette classification m'a permis de prioriser les actions à prendre tout en minimisant les perturbations pour les utilisateurs.
* Je me suis encore servi de la fonctionnalité d’enregistrement au format csv pour effectuer cette classification. Les capture ci-dessous montre un aperçu de la classification des alertes :
* Alertes :

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

* Alertes poste :

Une image contenant texte, nombre, Police, ligne

Description générée automatiquement

### Alimentation du ticket.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

# 1.3 Plan d’action

* Parmi toutes ses alertes, j’ai choisi l’alerte suivantes pour montrer comment traiter une menace via la console web :



* Il est possible d’obtenir de plus amples détails sur cette alerte comme le montre la capture ci-dessous :

Une image contenant texte, logiciel, Police, nombre

Description générée automatiquement

* ESET offre une fonctionnalité intéressante dans sa console web qui permet d'effectuer un scan sur VirusTotal d'une menace sélectionnée comme le montre la capture suivante :

Une image contenant texte, capture d’écran, Police, reçu

Description générée automatiquement

* On peut voir alors que les différents moteurs antivirus détectent un fonctionnement anormal :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

* Une fois les résultats du scan relevé, après quelque recherche sur internet, voici les informations que l’on peut trouver sur ces programmes potentiellement indésirables :
* Application.Hacktool.KMSActivator.EJ est une dénomination utilisée par certains programmes antivirus pour identifier un outil de piratage potentiellement indésirable appelé KMS Activator. Les KMS Activators sont des logiciels utilisés pour contourner ou activer illégalement les licences logicielles, en particulier les systèmes d'exploitation et les suites bureautiques. Le KMS Activator EJ est l'une des variantes spécifiques de ces outils de piratage.
* Generik.EKBWUOO est une dénomination utilisée par certains programmes antivirus pour identifier une variante générique (non spécifique) de logiciel malveillant. L'identification d'un logiciel malveillant sous le nom Generik.EKBWUOO signifie qu'il possède des caractéristiques ou des comportements similaires à ceux d'autres malwares déjà connus, mais il n'est pas spécifiquement reconnu comme une menace connue.
* "Crack.KMS.vl!c" est une dénomination qui pourrait être utilisée par certains programmes antivirus pour identifier un potentiel logiciel de crack ou de piratage connu sous le nom de KMS.vl!c. KMS.vl!c est souvent utilisé pour contourner les protections de licence des produits Microsoft et activer illégalement des logiciels tels que Windows et Microsoft Office sans acheter de licence officielle. Cependant, l'utilisation de ces outils de piratage est illégale et peut entraîner des conséquences juridiques. Les antivirus classent généralement les outils de crack ou de piratage comme des menaces potentielles en raison de leurs caractéristiques et de leurs comportements associés à l'activation illégale des logiciels. De plus, ces outils peuvent représenter un risque pour la sécurité des systèmes, car ils peuvent être utilisés pour propager des logiciels malveillants ou introduire des vulnérabilités.
* Nous possédons maintenant suffisamment d’informations pour avoir conscience des risques associés à ce programme suspect. J'ai pris l'initiative de le mettre en quarantaine afin de prévenir tout dommage ou compromission. J’ai donc créé une tâche de mise en quarantaine pour isoler le programme incriminé. Je commence donc par créer une tâche client comme le montre la capture ci-dessous :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

* Par la suite je programme la tâche :

Une image contenant texte, capture d’écran, Police, nombre

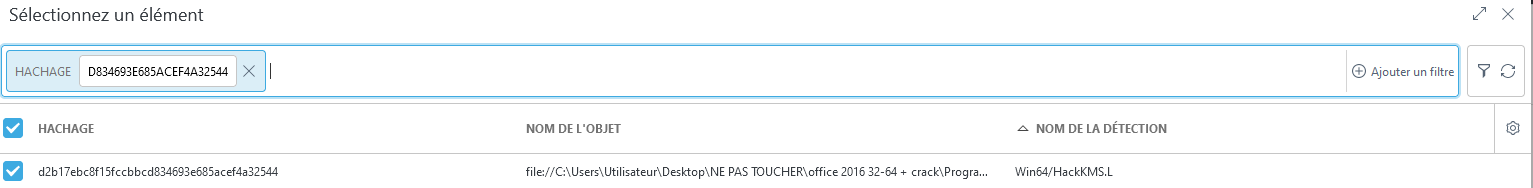
Description générée automatiquement

* J’ajoute le poste que je souhaite cibler avec cette tâche :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

* J’indique ensuite le programme que je souhaite isoler grâce à son hasch :



* Une fois la création et l’activation de cette tâche terminée, on peut se rendre dans la partie rapport de tâche afin de s’assurer que la tâche est correctement effectuée :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* La capture ci-dessous montre que l’action s’est correctement déroulée :



### Traitement des alertes postes

* En ce qui concerne le relevé des alertes sur les postes clients, pour avoir accès à celui-ci, on se dirige dans la partie ordinateur :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* La figure ci-dessous présente un aperçu des différentes alertes présente sur les postes clients :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

* Afin de pouvoir traiter efficacement ces machines, il est important de connaitre le contexte de l’alerte. Pour cela il suffit d’effectuer un clic drois puis de sélectionner détails pour avoir accès aux informations suplémentaire :

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

* On peut voir ici que la raison de l’alerte est la non-activation du produit ESET.
* Cette expérience m'a permis de développer mes compétences en matière de gestion de la sécurité et de renforcer ma compréhension des technologies antivirus. Pour traiter les alertes plus rapidement, ESET propose une fonctionnalité pratique qui permet de pré-créer des tâches, chacune accomplissant une action spécifique. Cette approche permet de gagner un temps précieux en automatisant les étapes courantes du processus de traitement des alertes. Par exemple, vous pouvez configurer une tâche pour l'analyse initiale des alertes, une autre pour la collecte des informations supplémentaires, et une autre encore pour l'envoi des rapports. En attribuant ces tâches à des actions correspondantes, il est possible d’accélérer les traitements des différentes alertes.
* Dans notre cas, nous avons besoin d’une tache d’activation qui permettra d’activer le produit ESET. On effectue donc une recherche de tâche en ajoutant un filtre permettant de rechercher toutes les tâches d’activations, puis on sélectionne l’activation qui convient comme le montre la capture suivante :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

* Une fois la validation terminée, il est possible de se rendre dans l’historique des tâches afin de s’assurer que celle-ci a été correctement accompli :

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement