SCHOLIA

Document de qualification des alertes

d'après les fiches réflexes de traitement des alertes cybersécurité - client Scholia

Procédure de gestion des alertes dans The Hive

Une fois connecté à The Hive, à l'aide des instructions fournies :

1. *Allez dans l'onglet "Alerts".*
2. *Choisissez l'alerte que vous souhaitez investiguer en cliquant sur le bouton "Preview and Import".*
3. *Une fois l'alerte visualisée, cliquez sur "Yes, Import" et choisissez le Case Template adéquat, du même nom que l'alerte, et créez le Case.*
4. *Une fois sur le Case, vous pouvez travailler sur les tâches demandées "Tasks". Ces Tasks reprennent les mêmes étapes que celles des fiches réflexes présentées ci-dessous.*
5. *Ajouter vos commentaires d'analyse dans les Tasks Logs d'une Task. Lorsqu'une analyse de logs est demandée, vous utiliserez le SIEM qui vous a été fourni au travers de la machine virtuelle Elastic.*
6. *Une fois l'analyse finalisée, vous pouvez **qualifier le Case** et ajouter une **justification** ainsi qu'une **capture d'écran** de votre qualification.*

Alerte 1/3 : création d'un compte local

Étape 1 : Comprendre la détection

À l'aide :

- du **titre** de l'alerte,
- de sa **description**,
- et de vos **recherches**, définissez :
    1. l'étape de la kill-chain correspondante ;
    2. la ou les Tactics et Techniques MITRE ATT&CK.

Vous ajouterez ces informations comme "tags" sur le Case.

3. Évaluez le **risque de faux positif** et **justifiez** votre réponse.
4. Décrivez en une phrase simple **la règle de détection** contenue dans le champ description de l'alerte.
   ex. : "Une alerte est créée quand…"

Risque de faux positif : Elevé

Justification :
- Jean Dubois a utilisé un compte sans privilèges pour signaler une mise à jour, celle-ci semble légitime mais il est essentiel de vérifier auprés de la direction et de Jean Dubois pour s'en assurer.

Etape kill-chain : Exploitation
Tactics MITRE ATT&CK : *Persistence.*
Technique MITRE ATT&CK : *T1136 - Create Account.*

Règle de détection : *Une alerte est créée lorsque la création d'un compte local est détectée sur un poste de travail ou un serveur.*

1. Identifiez le **nom** de la machine affectée par l'alerte.
   Ex. : firewall
2. Quelles **informations** pouvez-vous en tirer ? *Est-ce un poste de travail, un serveur, une appliance réseau, une ressource cloud ? La machine semble-t-elle liée à un projet ?*
3. Enrichissez ce nom à l'aide d'informations que vous pouvez trouver dans les sources d'informations du SI à votre disposition :
    a. annuaire,
    b. CMDB,
    c. tickets…

- Nom du serveur affecté : *SRV-FORMASUP-1*

- Informations :
- Création du serveur SRV-FORMASUP-1 via le compte Administrateur ADM_JDUBOIS .
- Enrichissement :
- Annuaire : *Aucune information*
- CMDB : *Appli métiers - Serveur appli formation Education nationale -*
- Tickets : *(ID ticket : CHANGE5900)*
Signalement d'une mise à jour de l'application FORMASUP via le compte sans privilèges de Jean Dubois.

Étape 3 : Analyser l'observable "account"

1. Identifiez le **nom** de la machine affectée par l'alerte.
2. Quelles **informations** pouvez-vous en tirer ?
3. **Enrichissez** ce nom à l'aide d'informations que vous pouvez trouver dans les sources d'informations du SI à votre disposition :
    - annuaire,
    - CMDB,
    - tickets...

Nom de la machine affectée : *ADM_JDUBOIS*
Informations: *Compte attribué à Jean Dubois, administrateur système.*
Enrichissement des Informations :
- Annuaire :
- Compte : *ADM_DUBOIS (compte avec privilèges)*
- Utilisateur : *Jean Dubois Organisation : IT Département : Système*
- CMDB : *Aucune information.*
- Tickets : *Aucun tickets provenant de ce compte*

Étape 4 : Analyser l'événement d'intérêt

À l'aide d'une recherche dans le SIEM :

1. Récupérez le **log correspondant à l'événement** de la création du process ayant déclenché l'alerte.
    - Ressource : ECS fields | Winlogbeat Reference [master] | Elastic
2. Analysez-le, en particulier le nom du process, la ligne de commande, le process parent.
3. Affichez uniquement les champs pertinents à l'investigation et exportez les résultats obtenus. Vous les ajouterez en pièce jointe de la Task Log The Hive et les joindrez à ce document en tant que livrable du projet.

Le processus qui a levé l'alerte semble-t-il malicieux ?

Nom du processus : *net.exe*
Ligne de commande : *La commande inclut user FORMASUP ... /ADD, confirmant la création d'un compte utilisateur.*
Utilisateur initiateur : *ADM_JDUBOIS*

le processus net.exe, exécuté par ADM_JDUBOIS, est le processus ayant déclenché l'alerte liée à la création de compte.

Le processus initial qui a déclenché la création du compte est net.exe, car :
- Il est directement lancé par powershell_ise.exe, un processus parent pertinent.
- Il exécute la commande de création de compte utilisateur (net.exe user FORMASUP ...).

Le processus net1.exe semble être une continuation de cette action, probablement une sous-commande exécutée par net.exe.

Étape 5 : Qualifier le case

Qualifiez l'alerte en vrai positif ou faux positif avec une **justification** et une **capture d'écran** attestant de votre qualification.

Risque de faux positif : Elevé

Justification :

- Jean Dubois a utilisé un compte sans privilèges pour signaler une mise à jour, celle-ci semble légitime mais il est essentiel de vérifier auprés de la direction et de Jean Dubois pour s'en assurer.

Légitimité de la mise à jour : *Vérifier si elle était prévue et autorisée par les politiques de l'organisation.*

Si nécessaire:
Analyse des changements : *Déterminer s'ils présentent des risques de sécurité ou compromettent les serveur applications voir l'intégrité du système.*
Analyse des comptes : *Examiner les deux comptes de Jean Dubois pour des signes de compromission, comme des activités inhabituelles ou non autorisées.*

Alerte 2/3 : Exécution de powershell avec l'argument "Download"

Étape 1 : Comprendre la détection

À l'aide :

- du **titre** de l'alerte,
- de sa **description**,
- et de vos **recherches**, définissez :
    1. l'étape de la kill-chain correspondante ;
    2. la ou les Tactics et Techniques MITRE ATT&CK.

Vous ajouterez ces informations comme "tags" sur le case.

3. Évaluez le **risque de faux positif** et **justifiez** votre réponse.
4. Décrivez en une phrase simple la règle de détection contenue dans le champ description.

Faux positif : *Elevé*
Justification: *Cette activité semble être un test de sécurité.*
Dans les tickets, ce test a été planifié pour le 29 novembre 2022.

- Etape kill-chain : Exploitation
- Tactics MITRE ATT&CK : *Execution*
- Technique MITRE ATT&CK : *- T1059 - Command and Scripting Interpreter*
- T1105 - Ingress Tool Transfer

Règle de détection : *Une alerte est créé lorsqu'une commande de PowerShell tente de télécharger un fichier depuis une URL externe.*

Étape 2 : Analyser l'URL

1. Identifiez dans l'observable "commandline", **l'URL** qui est requêtée.
2. Quel est le **domaine** ?
3. Quel est le **chemin** du fichier ?
4. Quelles **informations** pouvez-vous en tirer ? *Le fichier téléchargé peut-il être malicieux ?*

Ressources : utilisez des outils tels que virustotal pour vérifier la **réputation** du domaine ou de l'URL.

- URL: *"hxxps://github[.]com/zaproxy/zaproxy/releases/download/v2[.]12[.]0/ZAP_2_12_0_windows[.]exe"*
- Domaine : *github.com*
- Chemin du fichier : */zaproxy/zaproxy/releases/download/v2.12.0/ZAP_2_12_0_windows.exe*
- Détection par les fournisseurs de sécurité : *Aucun fournisseur n'a signalé l'URL comme malveillante.*
- Réponse HTTP : *Code de statut 200, indiquant une réponse réussie.*
- Adresse IP : *140.82.114.3*
- Catégories : *Aucun signalement de catégorie malveillante.*

Conclusion : *D'après l'analyse de VirusTotal, l'URL semble légitime et le fichier téléchargé est probablement aussi un outil de sécurité légitime .*

Étape 3 : Analyser l'observable "account"

1. Identifiez le **nom** de la machine affectée par l'alerte.
2. Quelles **informations** pouvez-vous en tirer ? Est-ce un compte de service ? Générique ou bien nominatif ? Semble-t-il avoir des privilèges ?
3. **Enrichissez** ce nom à l'aide d'informations que vous pouvez trouver dans les sources d'informations du SI à votre disposition :
    - annuaire,
    - CMDB,
    - tickets...

- Nom de l'utilisateur : Mohammed Beziz
- Privilèges : *Non.*

Enrichissement :
- Annuaire : *Mohammed Beziz est ingénieur dans le département sécurité et tests d'intrusions.*
- CMDB : *Mohammed Beziz utilise la machine DESKTOP-EDZ84, configurée pour les tests de sécurité.*
- Tickets : *(ID Ticket : REQUEST3562) Mohammed Beziz à signalé le test dans le cadre du projet MYSCHOOL.*

Étape 4 : Analyser l'observable "hostname"

1. Identifiez le **nom** de la machine affectée par l'alerte.
2. Quelles **informations** pouvez-vous en tirer ? Est-ce un poste de travail, un serveur, une appliance réseau, une ressource cloud ? La machine semble-t-elle liée à un projet ?
3. Enrichissez ce nom à l'aide d'informations que vous pouvez trouver dans les sources d'informations du SI à votre disposition :
    - annuaire,
    - CMDB,
    - tickets...

- Nom de la machine : *DESKTOP-EDZ84.*
- Information : *Il s'agit d'un poste de travail utilisé par l'équipe de sécurité.*

Enrichissement :
- Annuaire : *Machine attribuée à Mohammed.Beziz, ingénieur, membre du département sécurité et tests intrusions.*
- CMDB : *DESKTOP-EDZ84 est configuré pour des tests de sécurité.*
- Tickets : *Aucun incident signalé pour cette machine.*

Étape 5 : Qualifier le case

Qualifiez l'alerte en vrai positif ou faux positif avec une **justification** et une **capture d'écran** attestant de votre qualification.

Faux positif : Elevé

Justification : *Cette activité semble être un test de sécurité légitime car l'analyse URL n'a révélé aucun signe de malveillance. Aussi ce test a bien été planifié et signalé.*

Mohamed Beziz a déclaré ce test d'intrusion dans les tickets :

"Dans le cadre du projet MYSCHOOL, je réaliserai un test d'intrusion (pentest) le 29 novembre 2022. Cibles : SRV-MYSCHOOL-PRP-01 (10.2.8.12), SRV-MYSCHOOL-PRP-02 (10.2.8.12) URL : preprod.myschool.scholia.internal. J'utiliserai mon poste de travail habituel DESKTOP-EDZ84 et un compte local de pentest."

Conclusion : *Les informations tirées de la CMDB, des tickets et de l'annuaire montrent que cette activité est liée à des tests de sécurité planifiés.*

Alerte 3/3 : Mail suspect

Voir document pdf (Qualification mail suspect)

Étape 1 : Investiguer auprès de l'utilisateur

Listez les questions à poser à l'utilisateur pendant l'entretien.

ex. : expéditeur, principes du phishing, messages d'alertes, récurrences, étendues, interactions ?

Étape 2 : Analyser les composants du mail

Décrivez la méthodologie :

1. En-têtes du mail

2. Corps du mail
    - *pièces jointes ?*
    - *url ?*

3. Qualification de la menace
    - *Menace pour l'utilisateur*
    - *Menace pour l'entreprise*

4. Faut-il sensibiliser les utilisateurs ? Si oui, comment ?

Étape 3 : Qualifier le case