TD2: Outils de gestion et de traitement des incidents de sécurité en entreprise

Exercice 1:

Q1. Quels sont les problèmes résolus par le SIEM ?
- **a)** Le manque de méthodes d'authentification.
- **b)** Le long délai pour découvrir les failles de sécurité.
- **c)** la complexité des technologies et la difficulté d'identifier les attaques .

Q2. L'outil de ticketing permet aux analystes de:
- **a)** créer, traiter, suivre et tracer les incidents de sécurité .
- **b)** Faire une investigation sur les causes d'un incident de sécurité
- **c)** regrouper les incidents de sécurité sur un seul outil.

Q3. Une UseCase :
- **a)** C'est la phase d'agrégation de données.
- **b)** C'est une règle de sécurité implémentée sur l'outil de ticketing.
- **c)** C'est une règle de sécurité implémentée au niveau du SIEM permettant le déclenchement d'une alerte.

Q4. Quelles sont les fonctions de base d'un SIEM ?
- **a**) La collecte, la normalisation et le stockage des log et alertes.
- **b)** gérer les informations réseau et alertes.
- **c)** gérer les événements réseau et alertes.

Exercice 2: Cas d'étude (AV)

1) Vous êtes analyste de sécurité dans une entreprise et une règle s'est déclenchée au niveau du SIEM. Ci après les informations:

Titre de la règle: Malware infection detected on a host

Log brut de la détection :

<54>Sept 18 11:43:34 AM Symantecserver3.dz SymentecServer: Virus found, source IP Address: 192.168.15.62, Computer mame: HNP029031, Source: Auto-Protect scan, Risk name= Heur-AdvML-B,Occurrences:1,File path= C:\Users\ThomasGD\Downloads\Banking.pdf.exe,Description: ,Actuel action: Quarantined, Requested action: Cleaned, Secondery action: Quarantined, Event time: 2022-09-18 11:43:34 AM, Event Insert Time: 2022-09-18 11:43:34 AM, End Time: 2022-09-18 11:43:34 AM, Last update time: 2022-09-18 11:43:34 AM, Domain Name: <domaine de l'entreprise>, Group Name : Mon entreprise\ 04 Postes en Exception\PiloteDeception, Server Neme: AVserver3, User Name: ThomasGD, Source Computer Name: , Source Computer IP= , Disposition: Bad, Download site: ,Web domain: , Downloaded by: c:/windows/explorer.exe. Prevalence: Unknown, Confidence: This file is untrustworthy., URL Tracking Status: On, First Seen: Symantec has known about this file approximately 2 days. Sensitivity: Allowed application reason: Not on the allow list, Application hash: BADB6773355019723032 78C3F53CFAAG62BF7625037338907C9007A9605BAF5, Hashtype= SHA2, Company name= , Application name: WoRK8, Application version: 1.0.0.0,Applicatien type: 127, File size (bytes=): 691200. Category set : Malware, Category type: Heuristic Virus, Location: VPN, Intensive Protection Level: O, Certificate issuer: .Certificate signer: ,Certificate thumbprint: , Signing timestamp: 0, Certificate serial number: /

Informations extraites suite au parsing de la log sur le SIEM:

Event Information:

Event Name	Virus detected
Event descritption	Virus detected
Username	ThomasGD
Start time	September 18, 2022, 11:43:34 AM
AV-Path	C:\Users\ThomasGD\Downloads\Banking.pdf.exe
AV-Action	Quarantined
AV-Action Requires	Cleaned
AV-Hostname	HNP029031
AV-Domain	N/A
AV-Emplacement	VPN
AV-Filename	Banking.pdf.exe
AV-Hash	6badb6aa8b55d18a2ec3278c3f53cfaa562bf75e5cba33b907c90c7a9605baf5
Threat Name	Heur.AdvML.B
Domain	<domaine de l'entreprise>

a) Créez un incident de sécurité sur l'outil de ticketing avec la criticité et les recommandations SOC permettant de traiter l'incident de sécurité ci-dessus.

b) Après avoir affecté le ticket à l'utilisateur concerné par cet incident, vous avez eu le retour suivant:

> Bonjour le SOC,
> Je vous remercie pour votre signalement, les actions demandées ont été effectuées.
> Ce fichier a été téléchargé suite à clique non intentionnel sur le site:
> «http://CliqueparErreur.com»
> Cordialement,

Que faites vous en tant qu'analyste?

c) Quelle raison de clôture parmi les suivantes choisissez-vous pour clôturer votre ticket.

- faux positif
- comportement légitime
- Audit
- Incident réel qualifié

2) Vous avez le même déclenchement que la règle précédente avec les mêmes informations à l'exception de l'action de l'AV qui a supprimé le fichier au lieu de le mettre en quarantaine. quelles recommandations faites-vous à l'utilisateur concerné ? quelle est la criticité de cet incident ?

3) Vous avez le même déclenchement que la règle précédente avec les mêmes informations à l'exception de l'action de l'AV qui n'a ni supprimé ni mis en quarantaine le fichier.

a) Quelles recommandations faites-vous à l'utilisateur concerné ? change the file extension to ....pdfexe.DOC

b) L'utilisateur vous fait le retour suivant après la réalisation des actions demandées:

> Bonjour le SOC,
> Je vous remercie pour votre signalement, les actions demandées ont été effectuées.
> Cependant, Je constate un ralentissement de mon ordinateur et des fenêtres pop-up s'ouvrent régulièrement sans aucune action de ma part.
> Cordialement,

Quelles recommandations faites-vous à l'utilisateur concerné? quelle est la criticité de cet incident?

Exercice 3: cas d'étude (Proxy)

1- Vous êtes analyste de sécurité et une règle s'est déclenchée au niveau du SIEM. Ci après les informations:

Titre de la règle: A potential phishing was detected

Information extraite suite au parsing de la log:

Event Information:

Event Name	A potential phishing was detected
Event descritption	A potential phishing was detected
Username	ThomasGD
Start time	September 18, 2022, 11:43:34 AM
URL	hxxps://storage.googleapis[.]com
Domain	storage.googleapis[.]com
Destination IP	142.250.148.128
Mail Subject	Votre cadeau est arrivé !!
Proxy-Action	Allowed

a) Créez un incident de sécurité sur l'outil de ticketing avec les recommandations SOC permettant de traiter l'incident de sécurité ci-dessus.

b) Quelle action supplémentaire l'analyste devrait faire pour eliminer le risque ?

c) Quelle raison de clôture parmi les suivantes vous choisissez pour clôturer votre ticket.

- faux positif
- comportement légitime
- Audit
- Incident réel qualifié

Exercice 4: cas d'étude (FW)

1- Vous êtes analyste de sécurité et une règle s'est déclenchée au niveau du SIEM. Ci après les informations:

Titre de la règle: A scan was detected

Information extraite suite au parsing de la log:

Event Information:

Event Name	A scan was detected
Event descritption	A scan was detected and denied
Username	Server34
Start time	September 18, 2022, 11:43:34 AM
Ports	0-1000
SourceIP	10.10.12.18
Destination IP	10.17.132.134
FW-Action	Denied

a) Quel est le risque de sécurité suite aux scans ?

b) Créez un incident de sécurité sur l'outil de ticketing avec les recommandations SOC permettant de traiter l'incident de sécurité ci-dessus.

c) Le responsable du serveur source vous fait le retour suivan:

> Bonjour,
> Nous vous remercions pour votre alerte.
> Il s'agit d'un audit de sécurité que nous lançons depuis l'IP 10.10.12.18 (Qualys).
> Cordialement.

Quelle action l'analyste devrait faire pour que la règle ne se déclenche plus pour cette IP source ?

d) Quelle raison de clôture parmi les suivantes vous choisissez pour clôturer votre ticket.

- faux positif
- comportement légitime
- Audit
- Incident réel qualifié