RAPPORT D'OPTIMISATION DE LA DETECTION

CELLULE SOC

Août 2024

Version	Date	Propriétaire	Rédacteur / Autorité
1.0	25/08/2024	Cellule SOC	Nicolas Clerbout
Finale			

Table des matières

Règles

Cette section principale du rapport présente les règles proposées par l'équipe sécurité et les recommandations concernant celles à mettre en place et celles qui ne doivent pas être implémentées.

Règles proposées par l'équipe sécurité

1	Détection de la connexion d'une IP privée à une IP publique sur les ports 80/443
2	Détection d'une connexion interactive réussie d'un compte de service
3	Détection de nombreux accès à des fichiers publiques différents sur OneDrive
4	Détection de l'espace disque d'un serveur rempli à 70%
5	Détection d'un scan de ports provenant d'une IP non autorisée à scanner

Règles non retenues et justification

- Règle 1 (détection de connexions sortantes sur les ports 80/443)

Justification

Une telle règle provoquerait une alerte pour n'importe quelle connexion de type HTTP (port 80) ou HTTPS (port 443) sortante. Le SOC ferait alors face à une énorme quantité d'alertes.

Or, la grande majorité du trafic web des utilisateurs est légitime. Nous ferions alors face à un trop grand nombre de faux positifs qui rendraient d'autant plus difficile la détection de connexions web malveillantes.

Il serait plus efficace de filtrer le trafic au moyen du firewall/proxy en établissant une liste blanche (« white list ») de sites web légitimes auxquels les utilisateurs peuvent se connecter.

- Règle 3 (détection d'accès à des fichiers publiques sur OneDrive)

Justification

Dans la mesure où les fichiers en question sont étiquetés comme « publiques », le fait qu'ils soient accessibles sur OneDrive a été préalablement identifié comme non dangereux du point de vue des exigences de sécurité de l'entreprise. Il est donc inutile de définir une règle de détection pour ce type d'événement.

- Règle 4 (espace disque d'un server utilisé supérieur à 70%)

Justification

La part d'utilisation d'espace disque des différents équipements correspond à un indicateur de performance. Cet indicateur ne concerne pas les enjeux de sécurité – confidentialité, disponibilité ou intégrité – du Système d'Informations (SI) d'Oiseau Rouge.

Règles retenues

Règle 2

Détection d'une connexion interactive réussie d'un compte de service.

Justification

Les comptes de service servent à lancer les différents services qui tournent en arrière-plan sur les différentes machines du réseau d'Oiseau Rouge. Certaines de leurs caractéristiques sont le fait qu'ils ne nécessitent normalement pas d'intervention d'un utilisateur et surtout qu'ils disposent des privilèges (souvent élevés) nécessaires à leur fonction.

Une connexion **interactive** suppose l'intervention d'un utilisateur qui fournit un facteur d'authentification. En d'autres termes, une connexion interactive indique qu'une personne a voulu accéder au compte de service en question et à ses privilèges. Par conséquent, une telle connexion indique très probablement une infraction sérieuse à la sécurité du SI de l'entreprise.

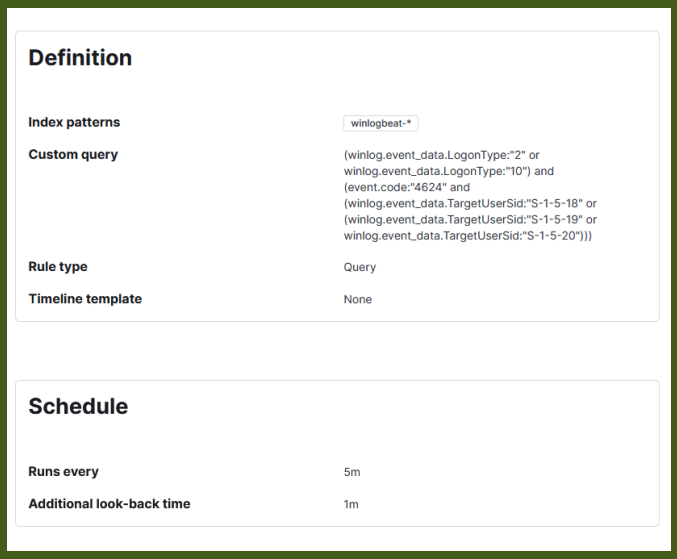
Contenu de la règle

On veut repérer chaque connexion interactive réussie d'un compte de service. Trois éléments-clés constituent la règle.

- Le type de Logon : une connexion interactive est identifiée par la valeur « `2` » ou « `10` » (interactive *à distance*) dans le champ `winlog.event_data.LogonType` ;
- La réussite de la connexion : identifiée par la valeur « `4624` » dans le champ `event.code` ;
- Le Sid du compte auquel la connexion est effectuée : les valeurs « `S-1-5-18` », « `S-1-5-19` » et « `S-1-5-20` » du champ `winlog.data_event.TargetUserSid` désignent les comptes de service.

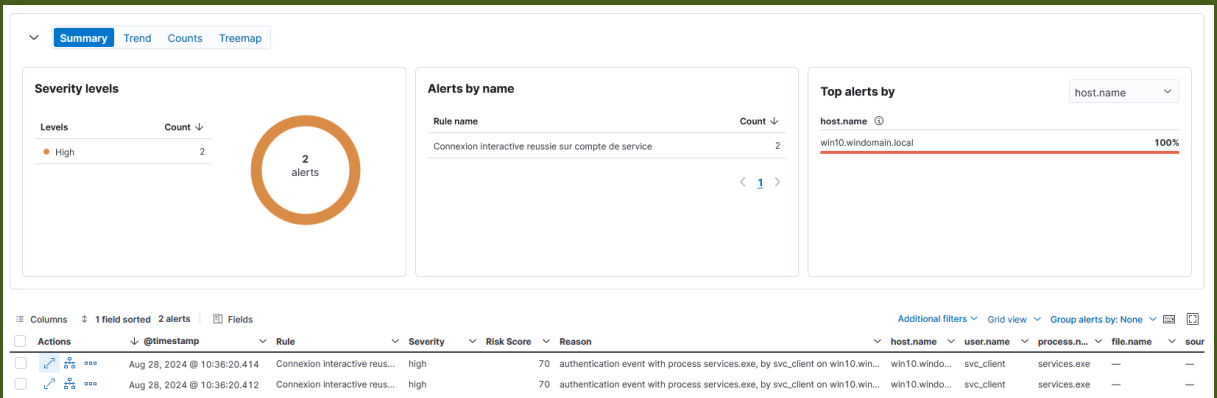
Pour cette règle, l'index à surveiller est « `winlogbeat` ».

La capture d'écran ci-dessous résume les éléments de la règle. Une capture d'écran de la règle entière, au format JSON, se trouve en Annexe A.



Exemple d'implémentation

A titre de test, des logs correspondant à des connexions interactives réussies sur un compte de service ont été générés. Comme on peut le constater dans la capture d'écran ci-dessous, ils ont été correctement signalés.



Règle 5

Détection d'un scan de ports provenant d'une IP non autorisée à scanner

Justification

Le scan de ports est une technique de diagnostic réseau qui peut être utilisée à des fins malveillantes, notamment de reconnaissance (MITRE ATT&CK : `TA0043`) incluant la recherche de vulnérabilités.

Il est donc nécessaire de veiller à ce que tout scan de ports sur notre réseau corresponde à une activité légitime provenant uniquement d'IP(s) autorisée(s). Par conséquent, il faut pouvoir détecter ceux provenant d'IPs non autorisées à effectuer des scans de diagnostic.

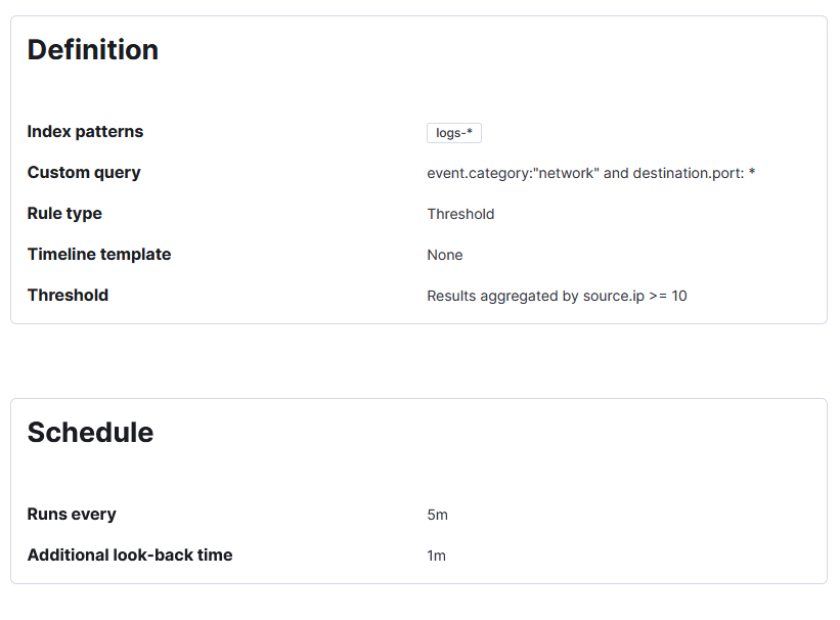
Contenu de la règle

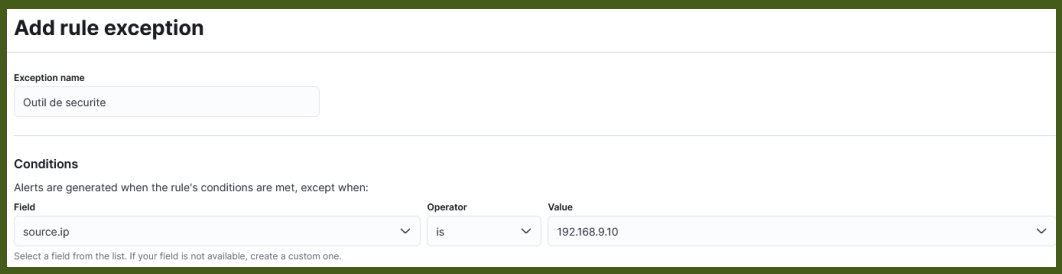
Les éléments-clés pour repérer un potentiel scan de réseau sont les suivants.

- On surveille les événements de type réseau et donc ayant la valeur « `network` » dans le champ `event.category` ;
- On restreint la recherche aux événements où il y a bien un port qui est contacté : donc on utilise la wildcard « `*` » pour le champ `destination.port` ;
- Une caractéristique du scan de ports est un grand nombre de ports contactés en peu de temps : on utilise donc une règle de type « *threshold* » en regroupant les résultats par IP source (champ `source.ip`) et en fixant le « seuil » à plus de 10 ports contactés par IP ;
- On compte le nombre de ports uniques contactés par IP dès lors que ce nombre est supérieur à 10 ;

- Puisqu'on veut limiter les alertes aux adresses IPs qui ne sont pas censées effectuer de scan de port, il faut créer une exception pour la règle pour que les scans effectués par notre outil de sécurité (IP : `192.168.9.10`) ne provoquent pas d'alerte.

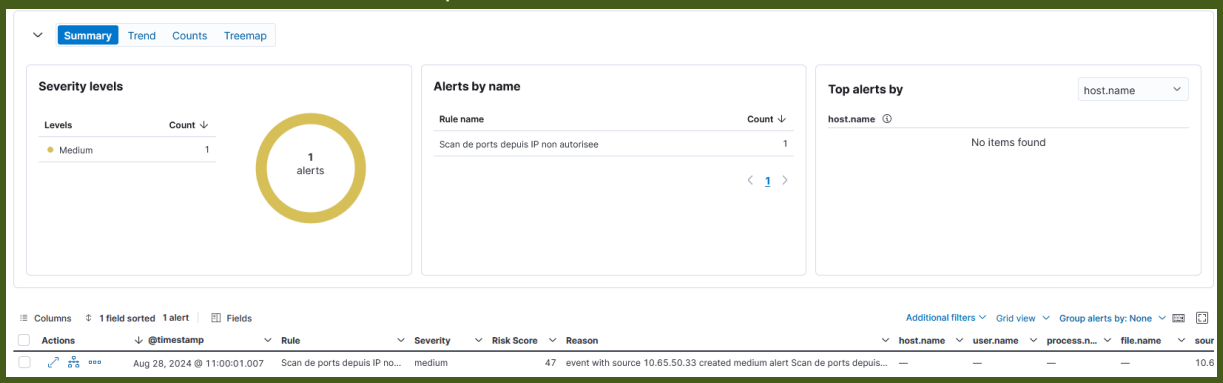
Pour cette règle, l'index à surveiller est « `logs` ». Les captures d'écran ci-dessous illustrent les éléments décrits. Une capture d'écran de la règle entière, au format JSON, se trouve en Annexe B.





Exemple d'implémentation

A titre de test, des logs correspondant à un scan de ports sont générés. L'alerte se déclenche pour une adresse IP non autorisée, comme on peut le conster dans la capture d'écran suivante.


Summary
Trend
Counts
Treemap
Severity levels
Levels
Count
Medium
1
1
alerts
Alerts by name
Rule name
Count
Scan de ports depuis IP non autorisee
1
1
Top alerts by
host.name
host.name
No items found
Columns
1 field sorted
1 alert
Fields
Additional filters
Grid view
Group alerts by: None
Actions
@timestamp
Rule
Severity
Risk Score
Reason
host.name
user.name
process.n...
file.name
sour
Aug 28, 2024 @ 11:00:01.007
Scan de ports depuis IP no...
medium
47
event with source 10.65.50.33 created medium alert Scan de ports depuis...
10.6

Annexe A : Capture d’écran règle « connexion interactive réussie sur compte de service »

{"id":"7dc62c00-6516-11ef-a615-ff96b6545dfd",
"updated_at":"2024-08-28T08:21:16.315Z",
"updated_by":"analyst",
"created_at":"2024-08-28T08:21:14.831Z",
"created_by":"analyst",
"name":"Connexion interactive reussie sur compte de service",
"tags":[],
"interval":"5m",
"enabled":true,
"description":"Repere les connexions interactives (locales ou a distance) reussies sur un compte de service",
"risk_score":70,
"severity":"high",
"license":"",
"output_index":"",
"meta":{
"from":"1m",
"kibana_siem_app_url":"http://127.0.0.1:5601/app/security"
},
"author":[],
"false_positives":[],
"from":"now-360s",
"rule_id":"46c2db07-bd66-4c50-a263-744ce9c53826",
"max_signals":100,
"risk_score_mapping":[],
"severity_mapping":[],
"threat":[],
"to":"now",
"references":[],
"version":1,
"exceptions_list":[],
"immutable":false,"related_integrations":[],
"required_fields":[],
"setup":"",
"type":"query",
"language":"kuery",
"index":["winlogbeat-*"],
"query":"(winlog.event_data.LogonType:\"2\" or winlog.event_data.LogonType:\"10\") and (event.code:\"4624\" and (winlog.event_data.TargetUserSid:\"S-1-5-18\" or (winlog.event_data.TargetUserSid:\"S-1-5-19\" or winlog.event_data.TargetUserSid:\"S-1-5-20\")))",
"filters":[],
"throttle":"no_actions",
"actions":[]}

{"exported_count":1,"exported_rules_count":1,"missing_rules":[],"missing_rules_count":0,"exported_exception_list_count":0,"exported_exception_list_item_count":0,"missing_exception_list_item_count":0,"missing_exception_list_items":[],"missing_exception_lists":[],"missing_exception_lists_count":0,"exported_action_connector_count":0,"missing_action_connection_count":0,"missing_action_connections":[],"excluded_action_connection_count":0,"excluded_action_connections":[]}

Annexe B : Capture d’écran règle « scan de port provenant d’une IP non autorisée »

{"id":"1890ad90-6518-11ef-a615-ff96b6545dfd",
"updated_at":"2024-08-28T08:57:28.155Z",
"updated_by":"analyst",
"created_at":"2024-08-28T08:32:43.758Z",
"created_by":"analyst",
"name":"Scan de ports depuis IP non autorisee",
"tags":[],
"interval":"5m",
"enabled":true,
"description":"Repere les potentiels scans de ports effectues depuis adresses IP non autorisees",
"risk_score":47,
"severity":"medium",
"license":"",
"output_index":"",
"meta":{
"from":"1m",
"kibana_siem_app_url":"http://127.0.0.1:5601/app/security"
},
"author":[],
"false_positives":[],
"from":"now-360s",
"rule_id":"44bb5aa2-693d-4596-99e9-f4e1dd18d6e8",
"max_signals":100,
"risk_score_mapping":[],
"severity_mapping":[],
"threat":[],
"to":"now",
"references":[],
"version":3,
"exceptions_list":[
{"list_id":"02d38d88-d88b-4da0-aa82-539a77657dfc",
"namespace_type":"single",
"id":"4eeb7910-6518-11ef-a615-ff96b6545dfd",
"type":"rule_default"}
],
"immutable":false,
"related_integrations":[],
"required_fields":[],
"setup":"",
"type":"threshold",
"language":"kuery",
"index":["logs-*"],
"query":"event.category:\"network\" and destination.port: *",
"filters":[],"threshold":{"field":["source.ip"],"value":10,"cardinality":[]},"throttle":"no_actions","actions":[]}

{"_version":"WzMxMDIyLDIwXQ==","created_at":"2024-08-28T08:34:14.945Z","created_by":"analyst","description":"Exception list containing exceptions for rule with id: 1890ad90-6518-11ef-a615-ff96b6545dfd","id":"4eeb7910-6518-11ef-a615-ff96b6545dfd","immutable":false,"list_id":"02d38d88-d88b-4da0-aa82-539a77657dfc","name":"Exceptions for rule - Scan de ports depuis IP non autorisee","namespace_type":"single","os_types":[],"tags":["default_rule_exception_list"],"tie_breaker_id":"5d28cfce-f924-4479-a368-bf0fda45641b","type":"rule_default","updated_at":"2024-08-28T08:34:14.945Z","updated_by":"analyst","version":1}

{"_version":"WzMxMDI0LDIwXQ==","comments":[],"created_at":"2024-08-28T08:34:16.765Z","created_by":"analyst","description":"Exception list item","entries":[{"field":"source.ip","operator":"included","type":"match","value":"192.168.9.10"}],"id":"50012ed0-6518-11ef-a615-ff96b6545dfd","item_id":"27da4f65-7a65-4dc9-ad93-5bc9a5064206","list_id":"02d38d88-d88b-4da0-aa82-539a77657dfc","name":"Outil de securite","namespace_type":"single","os_types":[],"tags":[],"tie_breaker_id":"4afcbc73-0b79-4649-9971-70705fbe35ea","type":"simple","updated_at":"2024-08-28T08:34:16.765Z","updated_by":"analyst"}

{"exported_count":3,"exported_rules_count":1,"missing_rules":[],"missing_rules_count":0,"exported_exception_list_count":1,"exported_exception_list_item_count":1,"missing_exception_list_item_count":0,"missing_exception_list_items":[],"missing_exception_lists":[],"missing_exception_lists_count":0,"exported_action_connector_count":0,"missing_action_connection_count":0,"missing_action_connections":[],"excluded_action_connection_count":0,"excluded_action_connections":[]}