Sigma : un seul outil pour les gouverner tous

Jean-Marc Pouchoulon

Octobre 2023

1 Analyse d'une règle Sigma simple

On se propose d'analyser la règle Sigma suivante:

```yaml
title: DNS Query to External Service Interaction Domains
id: aff715fa-4dd5-497a-8db3-910bea555566
status: experimental
description: Detects suspicious DNS queries to external service interaction
        domains often used for out-of-band interactions after successful RCE
references:
    - https://twitter.com/breakersall/status/1533493587828260866
author: Florian Roth (Nextron Systems), Matt Kelly (list of domains)
date: 2022/06/07
tags:
    - attack.initial_access
    - attack.t1190
    - attack.reconnaissance
    - attack.t1595.002
logsource:
    category: dns
detection:
    selection:
        query|contains:
            - '.interact.sh'
            - '.oast.pro'
            - '.oast.live'
            - '.oast.site'
            - '.oast.online'
            - '.oast.fun'
            - '.oast.me'
            - '.burpcollaborator.net'
            - '.oastify.com'
            - '.canarytokens.com'
            - '.requestbin.net'
            - '.dnslog.cn'
    condition: selection
```

```
falsepositives:
    - Unknown
level: high
```

1. Quel est l'objet global de cette règle Sigma ?
2. Quelles sont les méta-données de cette règle ?
3. Quel est le "log source" de cette règle ?
4. Quels sont les deux autres champs possibles pour un "log source" ?
5. Quelle est la condition de détection de cette règle ?
6. La réponse à la requête doit-elle "matcher" tous les domaines ?
7. Quel est l'élément de syntaxe qui permet de répondre à la question précédente ?

2 Découverte d'une règle Sigma plus complexe

On se propose d'analyser la règle suivante:

```
title: WannaCry Ransomware Activity
id: 41d40bff-377a-43e2-8e1b-2e543069e079
status: test
description: Detects WannaCry ransomware activity
references:
    - https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId
author: Florian Roth (Nextron Systems), Tom U. @c_APT_ure (collection), oscd.community, Jonhnathan Ribeiro
date: 2019/01/16
modified: 2023/02/03
tags:
    - attack.lateral_movement
    - attack.t1210
    - attack.discovery
    - attack.t1083
    - attack.defense_evasion
    - attack.t1222.001
    - attack.impact
    - attack.t1486
    - attack.t1490
    - detection.emerging_threats
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        - Image|endswith:
            - '\tasksche.exe'
            - '\mssecsvc.exe'
            - '\taskdl.exe'
            - '\taskhsvc.exe'
            - '\taskse.exe'
            - '\111.exe'
            - '\lhdfrgui.exe'
            # - '\diskpart.exe'  # cannot be used in a rule of level critical
            - '\linuxnew.exe'
            - '\wannacry.exe'
        - Image|contains: 'WanaDecryptor'
    selection2:
        - CommandLine|contains|all:
            - 'icacls'
```

```
            - '/grant'
            - 'Everyone:F'
            - '/T'
            - '/C'
            - '/Q'
        - CommandLine|contains|all:
            - 'bcdedit'
            - '/set'
            - '{default}'
            - 'recoveryenabled'
            - 'no'
        - CommandLine|contains|all:
            - 'wbadmin'
            - 'delete'
            - 'catalog'
            - '-quiet'
        - CommandLine|contains: '@Please_Read_Me@.txt'
    condition: 1 of selection*
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Unknown
level: critical
```

1. Quel est l'objet global de cette règle Sigma ?
2. Identifiez les tactiques et les techniques de l'"attaque WannaCry" en vous servant de `https://attack.mitre.org/`
3. Que veut dire "condition: 1 of selection*" ?
4. A quoi sert le "all" de "CommandLine|contains|all" ?
5. Quel est le binaire dans la liste de "sélection 1" qui fait réellement partie de Windows ?
6. Pourquoi "diskpart.exe" est-il commenté ? pourquoi avec ce commentaire relatif au niveau critique
7. Rattachez chaque tactique à une phase de la "cyber kill chain". Pour rappel la cyber kill chain est composée de 7 phases:
   - reconnaissance
   - armement
   - délivrance de la charge
   - exploitation
   - installation
   - command and control
   - réalisations des objectifs

3 Génération d'une requête "SIEM" à partir d'une règle Sigma

1. installez le package Python pysigma à l'aide de pip.
2. listez les plugins disponibles.
3. A quoi corresponde ces plugins ?
4. installez les plugins pour opensearch, splunk et elasticsearch.
5. listez les "formats" et les "pipelines".
6. générez une requête SIEM pour splunk à partir de la règle Sigma suivante.

```
wget https://raw.githubusercontent.com/SigmaHQ/sigma/master/rules/windows/dns_query/dns_query_win_susp_ipify.yml
sigma convert -t splunk -p sysmon -s dns_query_win_susp_ipify.yml
```

7. Expliquer "-t splunk -p sysmon".
8. que devriez-vous faire maintenant pour obtenir des logs?