Point d'avancement PRIM Exploitation de Cilium et Hubble pour détecter et se protéger d'attaques DNS exfiltration

30 Mai 2024

Gilles HOPIN

Professeurs : Jean-Louis ROUGIER, Patrice NIVAGGIOLI

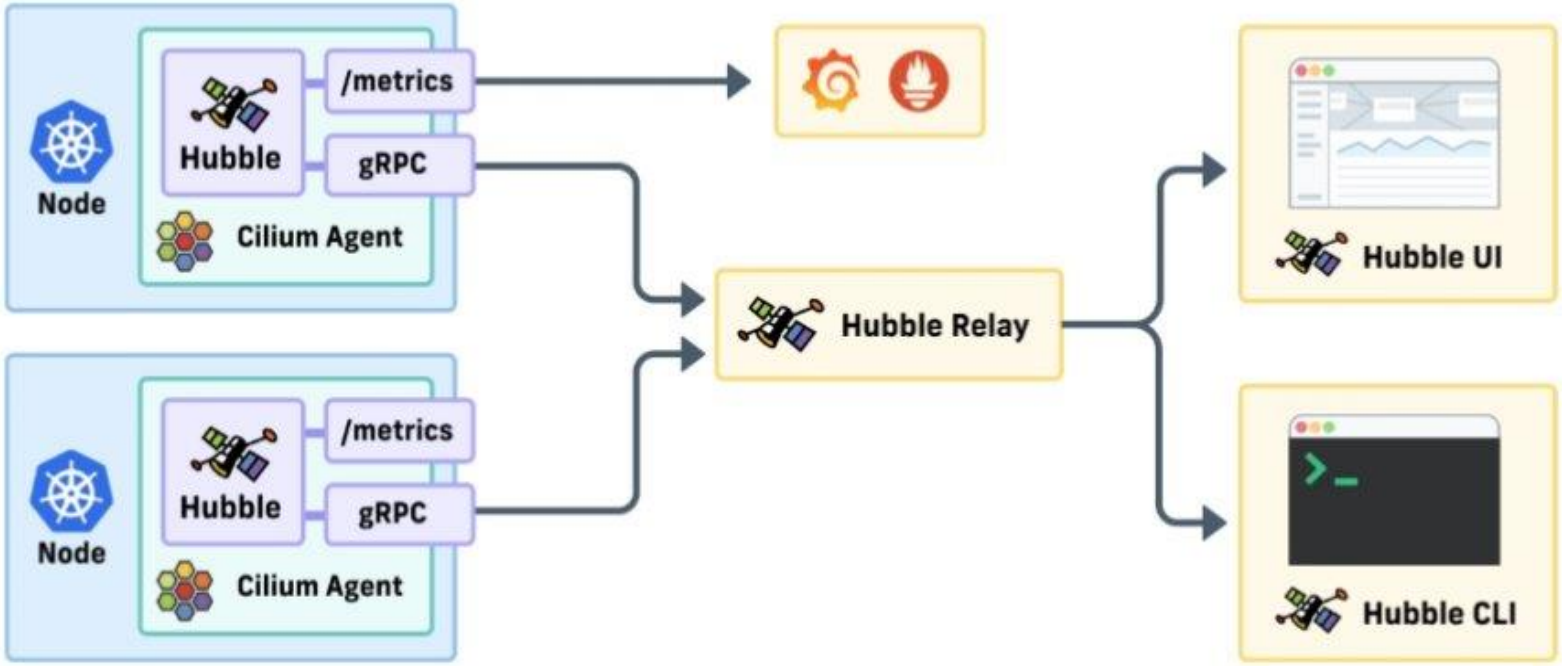
Sommaire

- Recap sur ce qu'offre hubble : metrics et logs
- Exportation des network flow logs
  - Configuration d'Hubble exporter
  - Configuration de Loki
  - Problème rencontré avec Promtail
  - Récupération des logs pour classification
- Classification => un problème de ML
  - Article Splunk : leur approche
  - Un dataset trouvé
  - Perspectives ML
- To do list

Ce qu'offre Hubble

Hubble permet de faire remonter deux types de données :

- Des metrics
- Des network flow logs



Les metrics

Une personnalisation assez limitée...

Prometheus Alerts Graph Status Help

Use local time | Enable query history | Enable autocomplete | Enable highlighting | Enable linter

hubble_dns_queries_total Execute

Table Graph

Load time: 106ms Resolution: 14s Result series: 3

Evaluation time

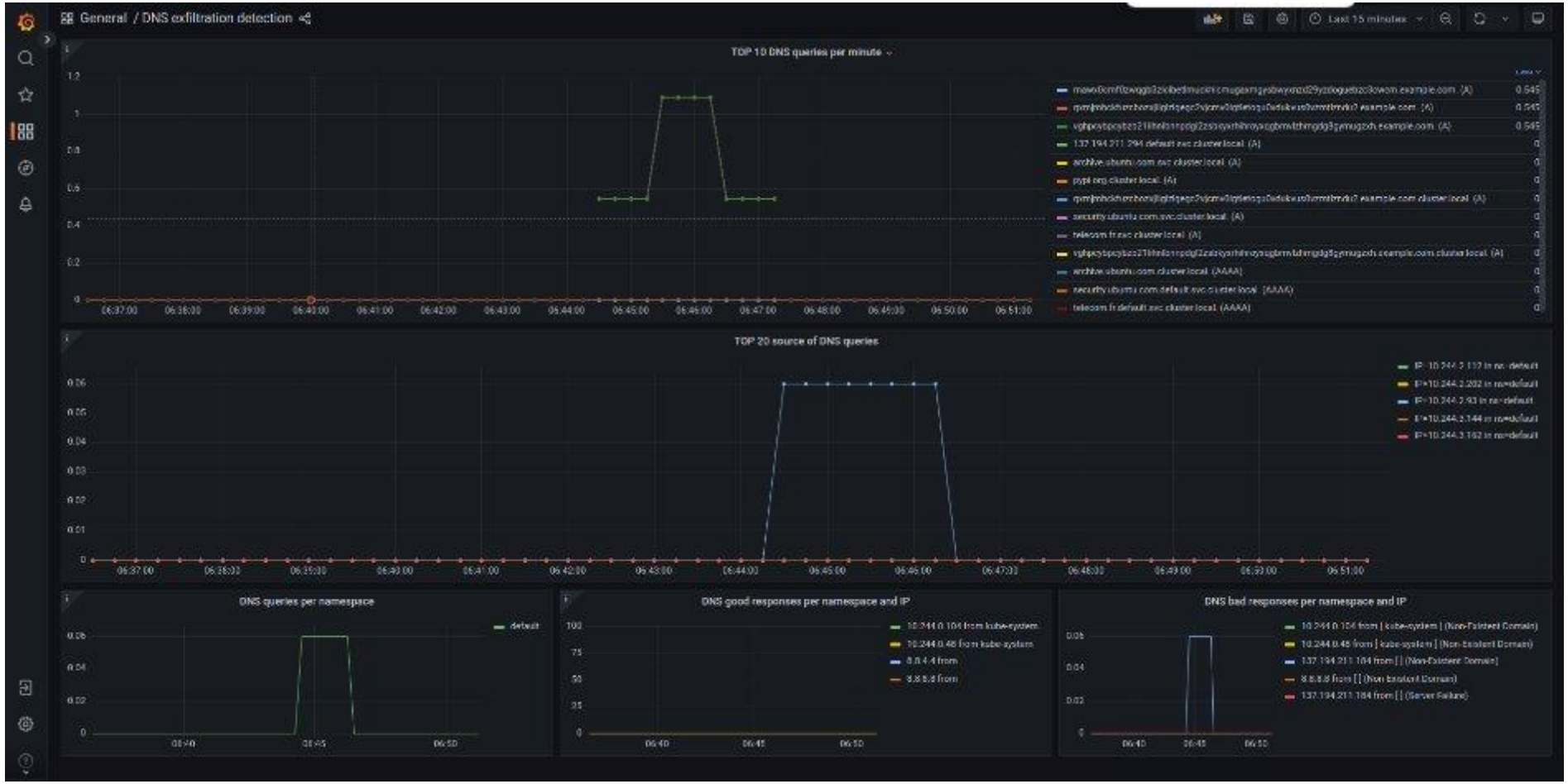
hubble_dns_queries_total{**app_kubernetes_io_managed_by**="Helm", **app_kubernetes_io_name**="hubble", **app_kubernetes_io_part_of**="cilium", **instance**="172.18.0.3:9965", **ips_returned**="0", **job**="kubernetes-service-endpoints", **k8s_app**="hubble", **namespace**="kube-system", **node**="kind-worker3", **qtypes**="A", **query**="mawx0cmf0zwqgb3zlcibetlmuckhlcmugaxmgysbwyxnzd29yzdoguebzc3cwcm.example.com.", **service**="hubble-metrics"} 43

hubble_dns_queries_total{**app_kubernetes_io_managed_by**="Helm", **app_kubernetes_io_name**="hubble", **app_kubernetes_io_part_of**="cilium", **instance**="172.18.0.3:9965", **ips_returned**="0", **job**="kubernetes-service-endpoints", **k8s_app**="hubble", **namespace**="kube-system", **node**="kind-worker3", **qtypes**="A", **query**="qxmjmhckfuzcbozxjliglzigegc2vjcmv0igtletogu0vdukvus0vzmtizndu2.example.com.", **service**="hubble-metrics"} 43

hubble_dns_queries_total{**app_kubernetes_io_managed_by**="Helm", **app_kubernetes_io_name**="hubble", **app_kubernetes_io_part_of**="cilium", **instance**="172.18.0.3:9965", **ips_returned**="0", **job**="kubernetes-service-endpoints", **k8s_app**="hubble", **namespace**="kube-system", **node**="kind-worker3", **qtypes**="A", **query**="vghpcybpcybzb21lihnlbnnpdgl2zsbkyxrhihroyxqgbmvlzhmgdg8gymugzxh.example.com.", **service**="hubble-metrics"} 43

Les metrics

...mais suffisante pour voir une anomalie



Les network flow logs

Ces logs offrent davantage d'informations

```
May 28 20:17:37.567: default/ubuntu-pod:55552 (ID:12263) -> 137.194.211.184:53 (world) policy-verdict:L4-Only EGRESS ALLOWED (UDP)
May 28 20:17:37.567: default/ubuntu-pod:55552 (ID:12263) -> 137.194.211.184:53 (world) to-proxy FORWARDED (UDP)
May 28 20:17:37.567: default/ubuntu-pod:55552 (ID:12263) -> 137.194.211.184:53 (world) dns-request proxy FORWARDED (DNS Query data.very.sensible.example.com. A)
May 28 20:17:37.567: default/ubuntu-pod:55552 (ID:12263) <- 137.194.211.184:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain TTL: 4294967295 (Proxy data.
very.sensible.example.com. A))
May 28 20:17:37.568: default/ubuntu-pod:55552 (ID:12263) <- 137.194.211.184:53 (world) to-endpoint FORWARDED (UDP)
May 28 20:17:37.597: default/ubuntu-pod:35581 (ID:12263) -> 137.194.211.184:53 (world) policy-verdict:L4-Only EGRESS ALLOWED (UDP)
May 28 20:17:37.597: default/ubuntu-pod:35581 (ID:12263) -> 137.194.211.184:53 (world) to-proxy FORWARDED (UDP)
May 28 20:17:37.597: default/ubuntu-pod:35581 (ID:12263) -> 137.194.211.184:53 (world) dns-request proxy FORWARDED (DNS Query data.very.sensible.example.com. A)
May 28 20:17:37.598: default/ubuntu-pod:35581 (ID:12263) <- 137.194.211.184:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain TTL: 4294967295 (Proxy data.
very.sensible.example.com. A))
May 28 20:17:37.598: default/ubuntu-pod:35581 (ID:12263) <- 137.194.211.184:53 (world) to-endpoint FORWARDED (UDP)
May 28 20:17:37.621: default/ubuntu-pod:57542 (ID:12263) -> 137.194.211.184:53 (world) policy-verdict:L4-Only EGRESS ALLOWED (UDP)
May 28 20:17:37.621: default/ubuntu-pod:57542 (ID:12263) -> 137.194.211.184:53 (world) to-proxy FORWARDED (UDP)
May 28 20:17:37.623: default/ubuntu-pod:57542 (ID:12263) -> 137.194.211.184:53 (world) dns-request proxy FORWARDED (DNS Query data.very.sensible.example.com. A)
May 28 20:17:37.624: default/ubuntu-pod:57542 (ID:12263) <- 137.194.211.184:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain TTL: 4294967295 (Proxy data.
very.sensible.example.com. A))
May 28 20:17:37.624: default/ubuntu-pod:57542 (ID:12263) <- 137.194.211.184:53 (world) to-endpoint FORWARDED (UDP)
May 28 20:17:37.654: default/ubuntu-pod:51566 (ID:12263) -> 137.194.211.184:53 (world) policy-verdict:L4-Only EGRESS ALLOWED (UDP)
May 28 20:17:37.654: default/ubuntu-pod:51566 (ID:12263) -> 137.194.211.184:53 (world) to-proxy FORWARDED (UDP)
May 28 20:17:37.655: default/ubuntu-pod:51566 (ID:12263) -> 137.194.211.184:53 (world) dns-request proxy FORWARDED (DNS Query data.very.sensible.example.com. A)
May 28 20:17:37.655: default/ubuntu-pod:51566 (ID:12263) <- 137.194.211.184:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain TTL: 4294967295 (Proxy data.
very.sensible.example.com. A))
May 28 20:17:37.655: default/ubuntu-pod:51566 (ID:12263) <- 137.194.211.184:53 (world) to-endpoint FORWARDED (UDP)
ubuntu@kind-2:~/Cilium$
```

Configuration d'Hubble exporter

Très simple à configurer !

Autres options :

- file rotation
- size limits,
- filters
- And field masks

cilium-values.yaml

```yaml
USER-SUPPLIED VALUES:
hubble:
  enabled: true
  metrics:
    enableOpenMetrics: true
    enabled:
    - drop
    - 'dns:query;sourceContext;identity;destinationContext:d
    - tcp
    - flow
    - port-distribution
    - icmp
    - httpv2:expamplars=true
  relay:
    enabled: true
  ui:
    enabled: true
  export:
    static:
      enabled: true
      filePath: /var/run/cilium/hubble/events.log
operator:
  prometheus:
    enabled: true
prometheus:
  enabled: true
```

Configuration d'Hubble exporter

- Attention : il y a un fichier de logs par nœud => ne pas se tromper de nœud !

```
ubuntu@kind-2:~$ hubble observe --protocol dns  --since=30s
Jun 12 11:02:52.514: default/python-script-runner:40228 (ID:12263) -> 8.8.8.8:53 (world) dns-request proxy FORWARDED (DNS Query vghpcybpcybzb21lihnlbnnpdgl2zs
bkyxrhihroyxqgbmvlzhmgdg8gymugzxh.example.com. A)
Jun 12 11:02:52.603: default/python-script-runner:40228 (ID:12263) <- 8.8.8.8:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain T
TL: 4294967295 (Proxy vghpcybpcybzb21lihnlbnnpdgl2zsbkyxrhihroyxqgbmvlzhmgdg8gymugzxh.example.com. A))
Jun 12 11:02:52.605: default/python-script-runner:51693 (ID:12263) -> 8.8.8.8:53 (world) dns-request proxy FORWARDED (DNS Query mawx0cmf0zwqgb3zlcibetlmuckhlc
mugaxmgysbwyxnzd29yzdoguebzc3cwcm.example.com. A)
Jun 12 11:02:52.693: default/python-script-runner:51693 (ID:12263) <- 8.8.8.8:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain T
TL: 4294967295 (Proxy mawx0cmf0zwqgb3zlcibetlmuckhlcmugaxmgysbwyxnzd29yzdoguebzc3cwcm.example.com. A))
Jun 12 11:02:52.696: default/python-script-runner:45304 (ID:12263) -> 8.8.8.8:53 (world) dns-request proxy FORWARDED (DNS Query qxmjmhckfuzcbozxjliglzigegc2vj
cmv0igtletogu0vdukvus0vzmtizndu2.example.com. A)
Jun 12 11:02:52.783: default/python-script-runner:45304 (ID:12263) <- 8.8.8.8:53 (world) dns-response proxy FORWARDED (DNS Answer RCode: Non-Existent Domain T
TL: 4294967295 (Proxy qxmjmhckfuzcbozxjliglzigegc2vjcmv0igtletogu0vdukvus0vzmtizndu2.example.com. A))
ubuntu@kind-2:~$ kubectl -n kube-system exec ds/cilium -- tail -f /var/run/cilium/hubble/events.log | grep dns
Defaulted container "cilium-agent" out of: cilium-agent, config (init), mount-cgroup (init), apply-sysctl-overwrites (init), mount-bpf-fs (init), clean-cilium
-state (init), install-cni-binaries (init)
```

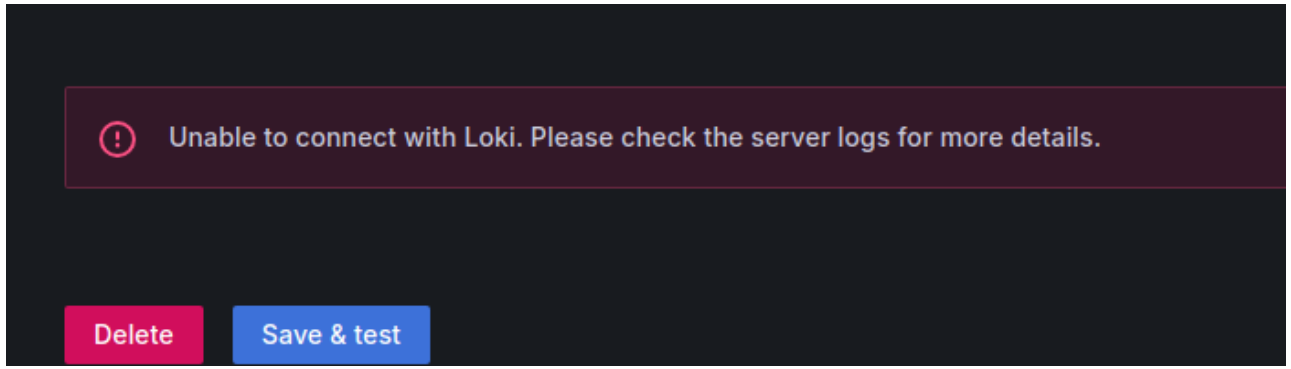
Ici, les logs DNS sont bien affichés par Hubble CLI, mais ils ne sont pas dans les logs que l'on consulte

Configuration de Loki

Utiliser un agrégateur de logs ? Loki !

```
helm upgrade --install --values loki.yaml loki grafana/loki-stack -n
grafana-loki --create-namespace
```

Intégration dans grafana comme data source, mais...



Configuration de Loki

La réponse :

[Loki-stack] Bundled loki version is extremely out of date! #2873

New issue

Open **MegaShinySnivy** opened this issue on Dec 29, 2023 · 11 comments · Fixed by #2875

MegaShinySnivy commented on Dec 29, 2023

As per the title, the default loki version is extremely out of date, and cannot connect to modern grafana versions. It should be bumped to a more recent version, like 2.9.3. This bit me in this issue (#79846).

6

Assignees

No one assigned

Labels

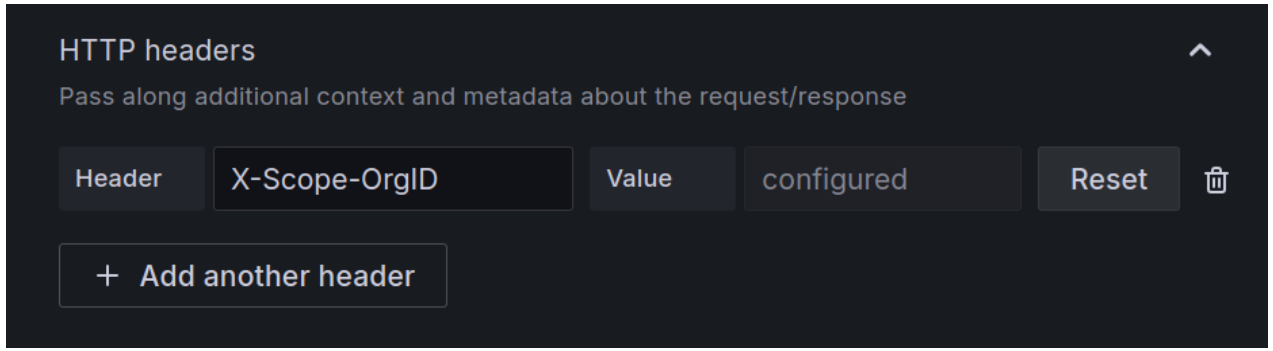
None yet

Configuration de Loki

Version la plus récente de Loki, compatible avec Grafana :

```
ubuntu@kind-2:~$ helm install --values Cilium/loki.yaml loki --namespace=monitoring grafana/loki
NAME: loki
LAST DEPLOYED: Tue Jun 11 17:35:42 2024
NAMESPACE: monitoring
STATUS: deployed
REVISION: 1
NOTES:
***********************************************************************
 Welcome to Grafana Loki
 Chart version: 6.6.3
 Chart Name: loki
 Loki version: 3.0.0
***********************************************************************
```

Ne pas oublier le HTTP header en plus dans Grafana:



Configuration de Loki

Outline | loki | Split | Add to dashboard | Last 1 hour | Run query | Live

A (loki)

Kick start your query | Label browser | Explain query | Builder | Code

Label filters

namespace = kube-system | pod = cilium-qxd62 | node_name = kind-worker3

Line contains | + Operations | hint: add logfmt parser

Text to find

{namespace="kube-system", pod="cilium-qxd62", node_name="kind-worker3"} |= ``

Options Type: Range Line limit: 1000

+ Add query | Query history | Query inspector

Logs volume

Logs | Logs | Table

Time | Unique labels | Wrap lines | Prettify JSON | Deduplication: None | Exact | Numbers | Signature | Display results: Newest first | Oldest first

Common labels: cilium-agent cilium-agent kube-system/cilium-agent kube-system kind-worker3 cilium-qxd62 cilium-agent Line limit: 1000 (38 returned) Total bytes processed: 10.2 kB Download

```
> 2024-06-12 13:17:51.771 time="2024-06-12T11:17:51Z" level=error msg="Envoy: Version check failed" error="envoy version 801c612e442298b3be55f1a1089c44386570880d/1.29.4/Distribution/RELEASE/BoringSSL does not match with required version 8fccf45a8ab9da13824e0f14122
  d5db35673f3bb" subsys=envoy-proxy
> 2024-06-12 13:17:51.771 time=2024-06-12T11:17:51Z level=error msg="Timer job errored" module=agent.controlplane.envoy-proxy name=version-check func="envoy.registerEnvoyVersionCheck.func2 (pkg/envoy/cell.go:262)" error="envoy version 801c612e442298b3be55f1a1089c4
  4386570880d/1.29.4/Distribution/RELEASE/BoringSSL does not match with required version 8fccf45a8ab9da13824e0f14122d5db35673f3bb"
> 2024-06-12 13:17:51.771 time="2024-06-12T11:17:51Z" level=info msg="Envoy: Version 801c612e442298b3be55f1a1089c44386570880d/1.29.4/Distribution/RELEASE/BoringSSL" subsys=envoy-manager
> 2024-06-12 13:12:51.770 time=2024-06-12T11:12:51Z level=error msg="Timer job errored" module=agent.controlplane.envoy-proxy name=version-check func="envoy.registerEnvoyVersionCheck.func2 (pkg/envoy/cell.go:262)" error="envoy version 801c612e442298b3be55f1a1089c4
  4386570880d/1.29.4/Distribution/RELEASE/BoringSSL does not match with required version 8fccf45a8ab9da13824e0f14122d5db35673f3bb"
> 2024-06-12 13:12:51.770 time="2024-06-12T11:12:51Z" level=error msg="Envoy: Version check failed" error="envoy version 801c612e442298b3be55f1a1089c44386570880d/1.29.4/Distribution/RELEASE/BoringSSL does not match with required version 8fccf45a8ab9da13824e0f14122
```

Start of range

13:17:51 — 12:22:51

Problème rencontré avec Promtail

- Promtail récupère les logs et les envoie à Loki, qui les agrège => un pod promtail par nœud
- On ajoute les logs d'Hubble en target

```yaml
scrape_configs:

  # New job for Hubble logs
  - job_name: hubble-logs
    kubernetes_sd_configs:        # we aim for pods
      - role: pod
    relabel_configs:
      - source_labels:            # with the label k8s-app=cilium
        - __meta_kubernetes_pod_label_k8s_app
        regex: cilium
        action: keep
      - source_labels:            # in the namespace kube-system
        - __meta_kubernetes_namespace
        regex: kube-system
        action: keep
      - source_labels:            # we change the labels for readability
        - __meta_kubernetes_namespace
        action: replace
        target_label: namespace
      - source_labels:
        - __meta_kubernetes_pod_name
        action: replace
        target_label: pod
      - action: replace         # path of the logs
        replacement: /var/run/cilium/hubble/events.log
        target_label: __path__
    pipeline_stages:
      - json:
          expressions:
            qtype: flow.l7.dns.qtypes[0]
            query: flow.l7.dns.query
            source: flow.IP.source
            destination: flow.IP.destination
            direction: flow.traffic_direction
```

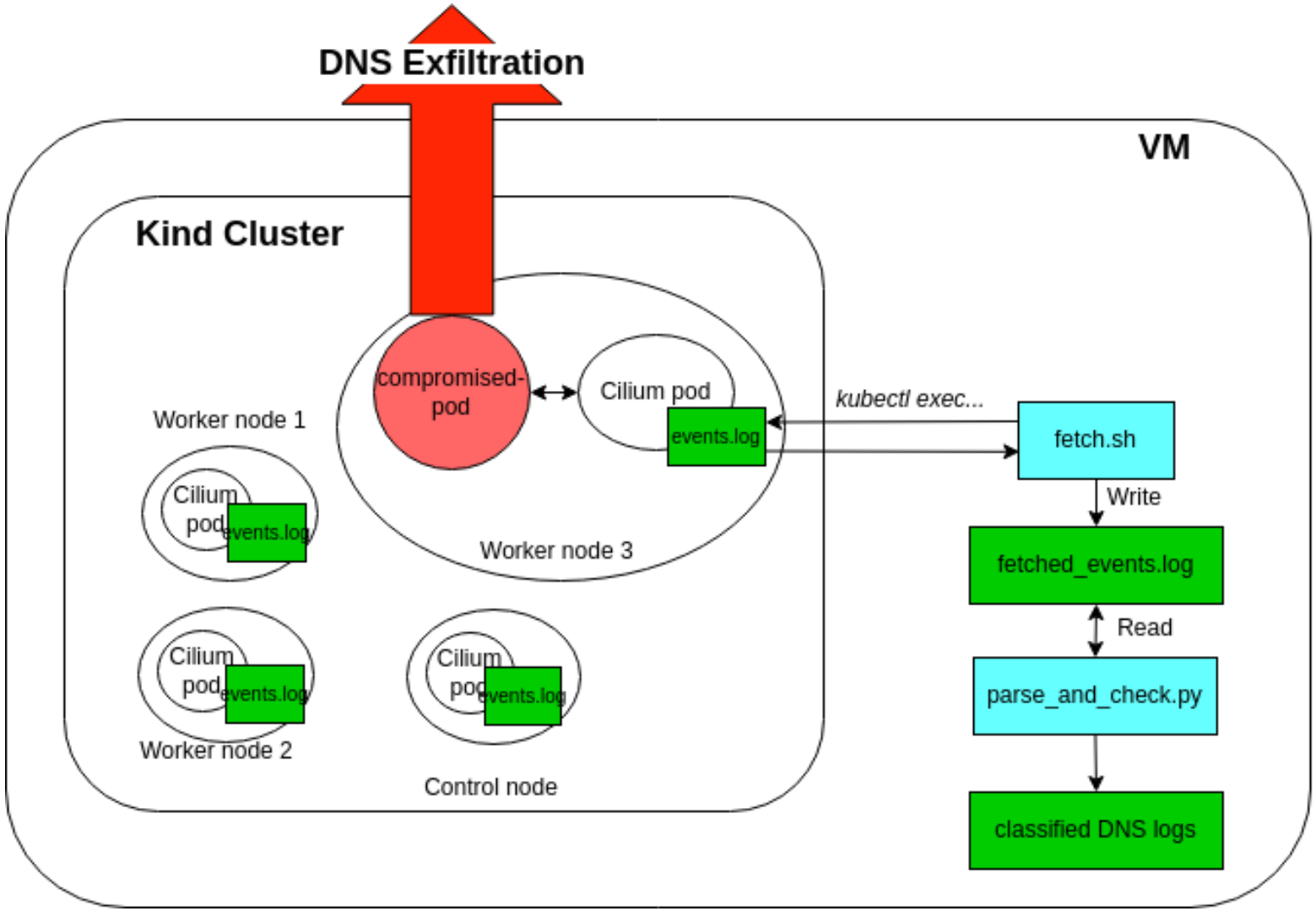
Problème rencontré avec Promtail

La target est bien ajoutée ...

```
level=info ts=2024-06-12T09:08:22.353308756Z caller=tailer.go:147 component=tailer msg="tail routine: started" path=/var/log/pods/k
ube-system_cilium-qxd62_ac2c173b-7c70-4557-8e22-8e8dc93bdb16/mount-cgroup/0.log
level=info ts=2024-06-12T09:08:22.353503983Z caller=filetarget.go:313 msg="watching new directory" directory=/var/log/pods/kube-sys
tem_cilium-qxd62_ac2c173b-7c70-4557-8e22-8e8dc93bdb16/mount-bpf-fs
level=info ts=2024-06-12T09:08:22.353775478Z caller=filetargetmanager.go:372 msg="Adding target" key="/var/run/cilium/hubble/events
.log:{namespace=\"kube-system\", pod=\"cilium-qxd62\"}"
level=info ts=2024-06-12T09:08:22.353780397Z caller=filetarget.go:313 msg="watching new directory" directory=/var/log/pods/kube-sys
tem_cilium-qxd62_ac2c173b-7c70-4557-8e22-8e8dc93bdb16/clean-cilium-state
level=info ts=2024-06-12T09:08:22.353933634Z caller=filetarget.go:313 msg="watching new directory" directory=/var/log/pods/kube-sys
tem_cilium-qxd62_ac2c173b-7c70-4557-8e22-8e8dc93bdb16/install-cni-binaries
```

Cependant, les logs ne remontent pas à Loki

Récupération des logs pour classification



Récupération des logs pour classification

Démo !

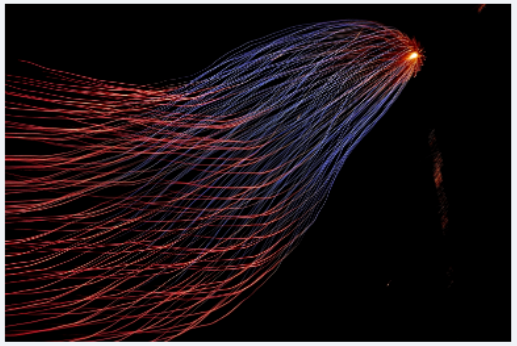
DNS exfiltration classification : Splunk's approach

splunk> a CISCO company | Products | Solutions | Why Splunk? | Resources | Company | Support | Free Splunk

Splunk Blogs | Security | DevOps | Artificial Intelligence | Platform | Leadership | Partners | .conf | Splunk Life | More

Security JULY 07, 2023 | 8 MINUTE READ

Machine Learning in Security: Detect DNS Data Exfiltration Using Deep Learning



DNS exfiltration classification : Splunk's approach

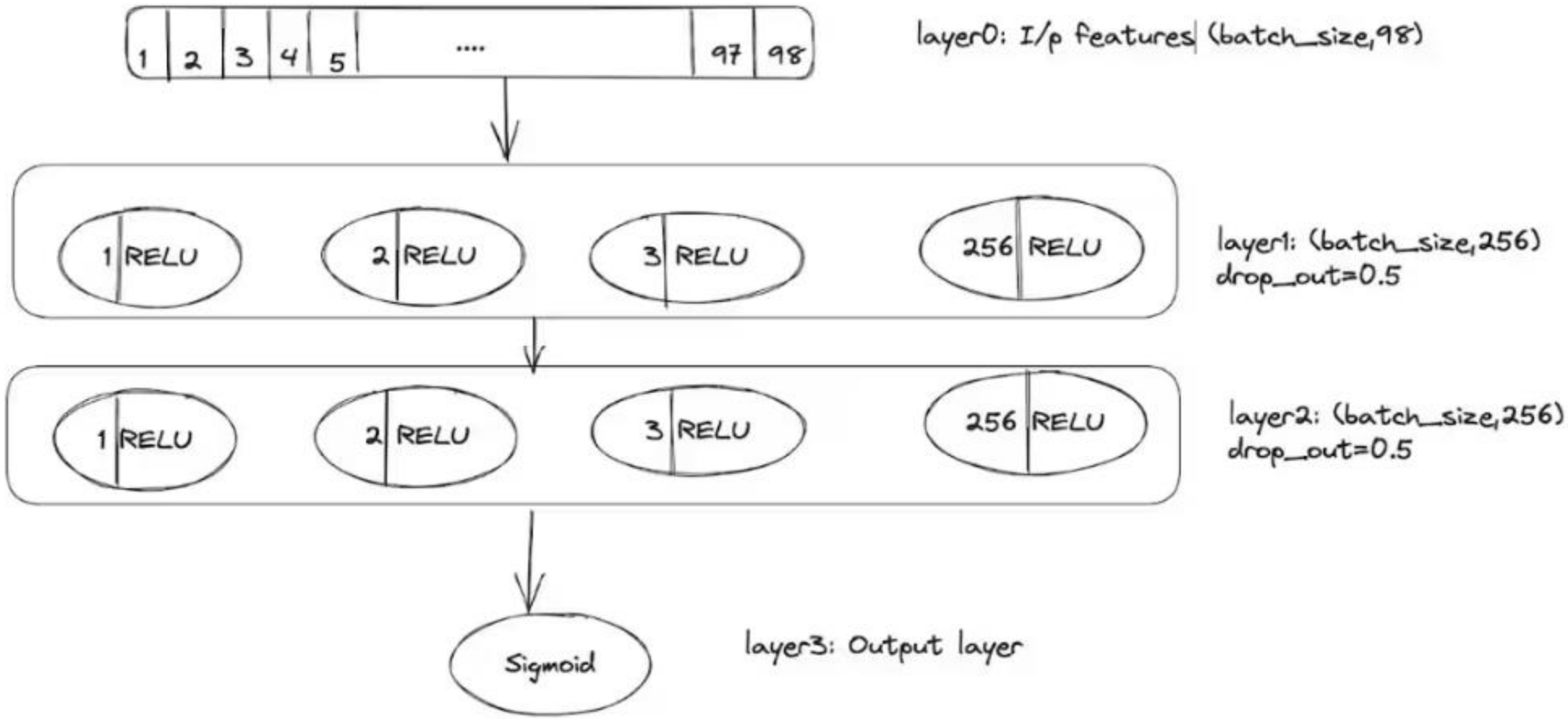
High volume DNS exfiltrations are easy to spot (e.g. with our Grafana dashboard !)

But low volume DNS exfiltrations require to look at DNS queries one by one => the following elements are taken into account :

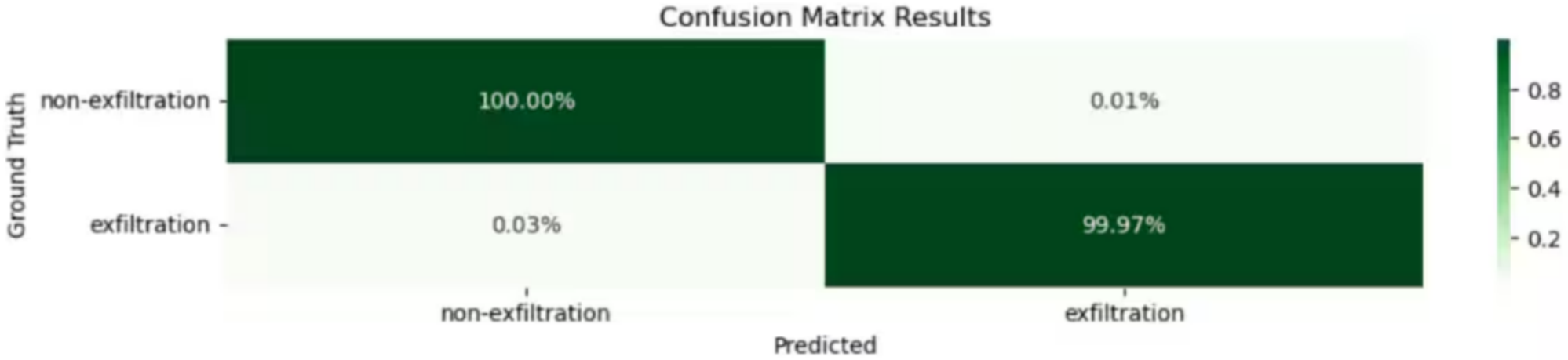
- Tokenized DNS request (94 characters)
- Length
- Entropy
- Average length over sliding window (past events between (source, dns_server))
- Average entropy over sliding window (past events between (source, dns_server))

['0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', '!', '"', '#', '$', '%', '&', '"', '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '>', '?', '@', '[', '\\', ']', '^', '_', '`', '{', '|', '}', '~']

DNS exfiltration classification : Splunk's approach



DNS exfiltration classification : Splunk's approach



Splunk, 2023, Confusion Matrix

Un dataset trouvé

Mendeley Data

DNS Exfiltration Dataset

Published: 11 July 2023 | Version 3 | DOI: 10.17632/c4n7fckkz3.3
Contributors: Kristijan Ziza, Pavle Vuletić, Predrag Tadić

Description

DNS exfiltration dataset was recorded in a realistic network environment. More than 50 million DNS requests were recorded on one of the ISP's DNS servers. The data in the dataset was anonymised by changing all IP addresses using injective mapping.
Features in the dataset are split into single request and aggregate features. Single request or DNS label-based features can be calculated for each DNS request independently using only the textual characteristics of the request. On the other hand, aggregate features are calculated using multiple subsequent request from one client to a particular TLD. This reduces the size of the dataset to about 35 million records. The complete list of features with descriptions can be found in dataset_description.txt file. For all of the features which are based on finding English words in the request we used about 60.000 most commom English words. The list of used words can be found in english_words.txt.
The main dataset (dataset.csv) contains regular requests and exfiltrations performed using DNSExfiltrator and Iodine tools. Additional dataset (dataset_modified.csv) contains only exfiltrations executed with modified DNSExfiltrator tool. Waiting times between two consecutive requests in this dataset are randomised and the requests also have lower entropy causing the detection to be much harder.

Perspective ML

- Inspecter le dataset
- Tester un NN simple sur le dataset, et voir les performances

To do list

1. Entrainement ML
2. Intégration dans "parse and classify"
3. Hubble et les traces ? Démo trouvée, à tester
4. Revenir sur les limites des metrics (nombre de labels max, pk que certains, etc.)
5. Cilium policy rule pour bloquer certaines exfiltrations