KubeCon | CloudNativeCon

Europe 2022

WELCOME TO VALENCIA

KubeCon CloudNativeCon Europe 2022

Threat Hunting at Scale: Auditing Thousands of Clusters With Falco + Fluent

Furkan Türkal & Emin Aktaş, Trendyol

Who are we?

Furkan Türkal

Platform Engineer

Trendyol

@Dentrax

@furkan.turkal

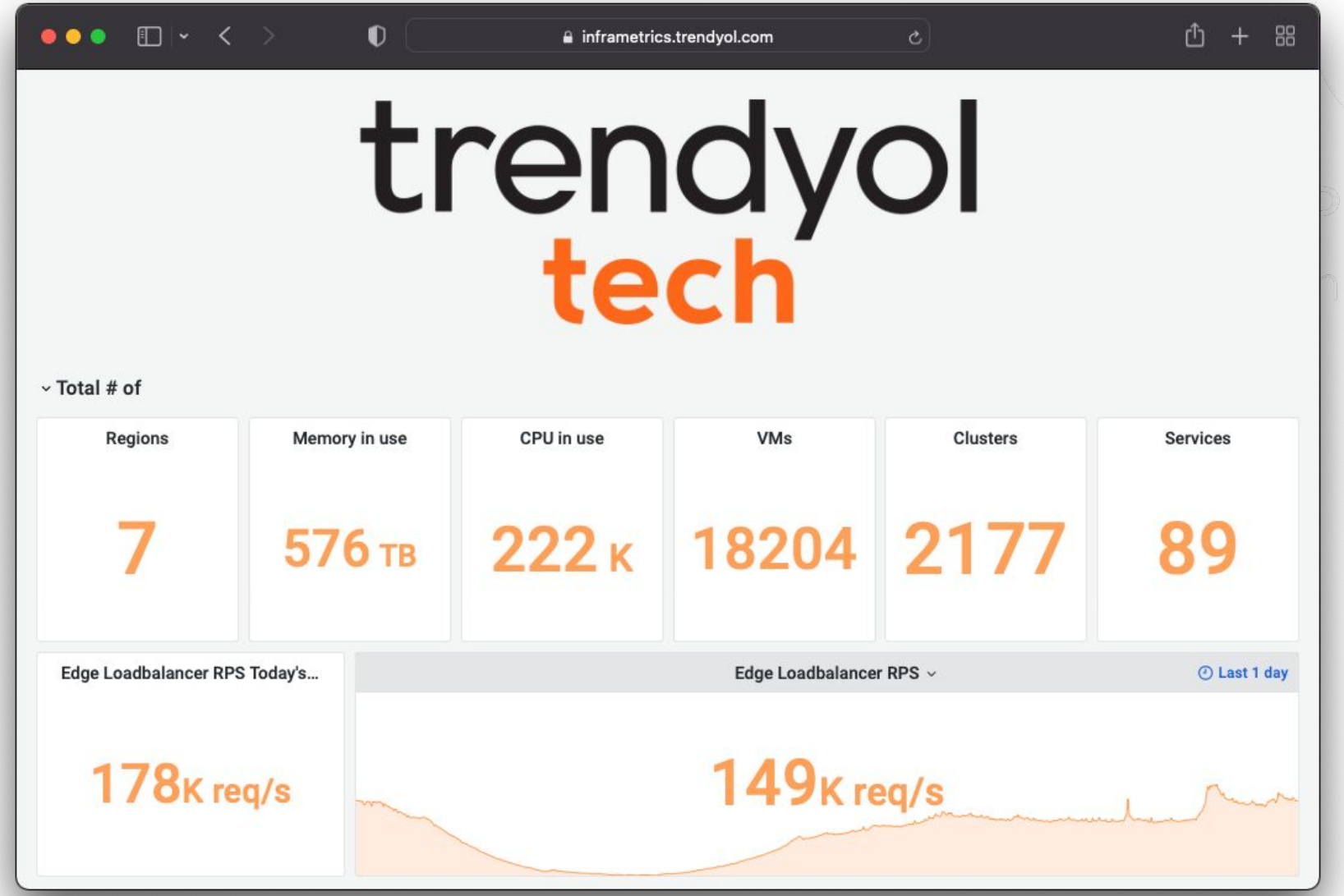
Emin Aktaş

Platform Engineer

Trendyol

@eminaktas

@emminaktas



inframetrics.trendyol.com

You will gain ...

- knowledge for threat detection
- a perspective on malicious behavior detection using audit logs
- instruction of monitoring at runtime

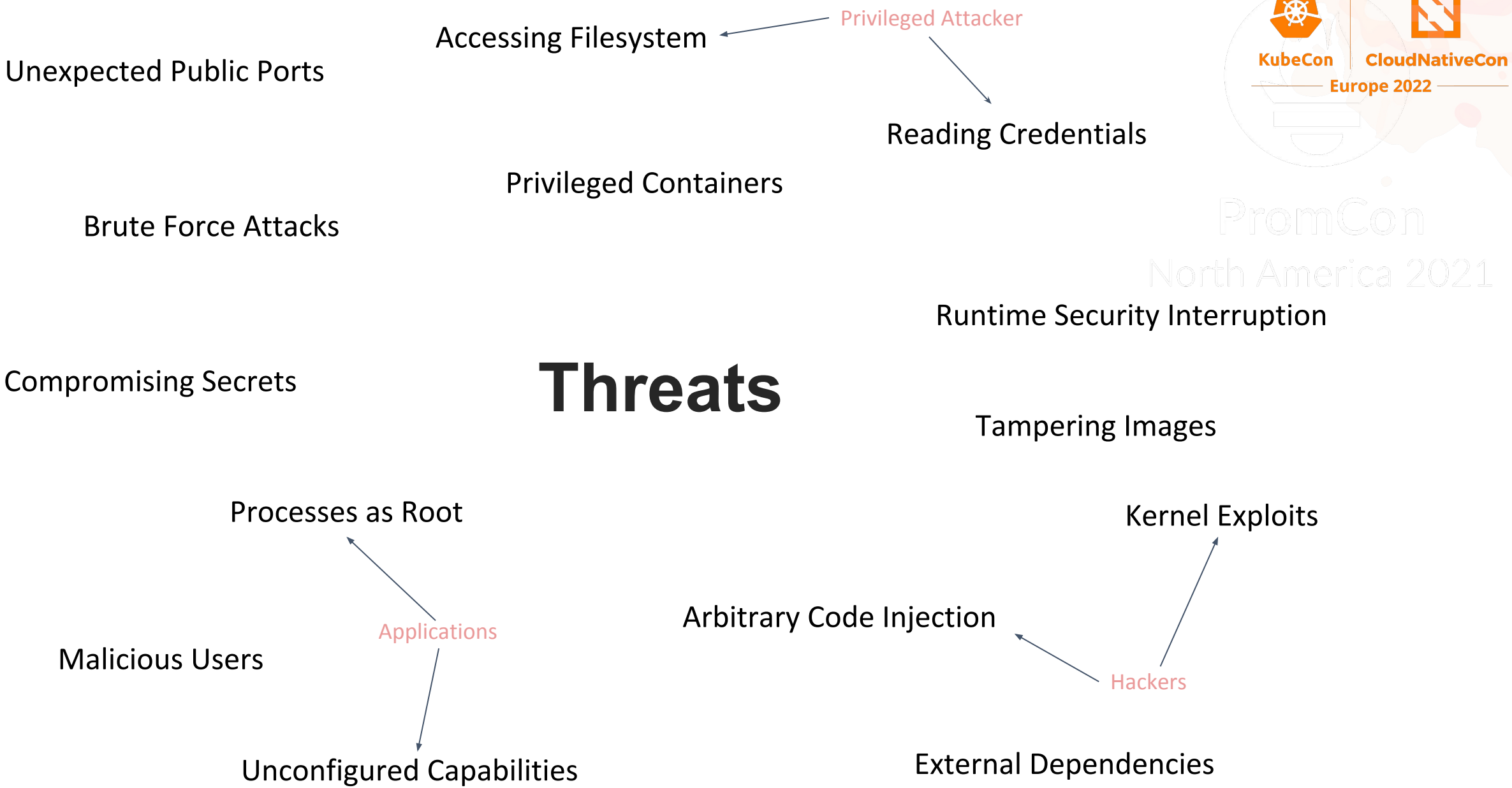
This session is for everyone

Intro to session

- Threats
- Security Pipeline at Runtime
- Audit Logs
- Runtime Security (Falco)
- Log Processing (Fluent Bit)
- Monitoring (Loki)
- Demo
- What is next?

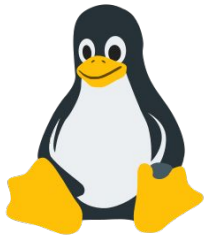
What is Threat?

Covid-19 is a threat to **humans**.



Security Pipeline at Runtime

Generate Audit



Scan

Collect Audit Logs

Monitoring

Audit Logs

[1] *Auditing*. (2021, December 19). Kubernetes. https://kubernetes.io/docs/tasks/debug-application-cluster/audit

Kubernetes Audit Events


```
--audit-log-path=/var/log/kubernetes/audit/audit.log
--audit-policy-file=/etc/kubernetes/audit-policy.yaml
--audit-log-maxage=30
--audit-log-maxbackup=5
--audit-log-maxsize=200
```

Enable


```
{
  "kind": "Event",
  "apiVersion": "audit.k8s.io/v1",
  "level": "Metadata",
  "auditID": "5fb41580-31e0-4397-aea1-5a6d325d3c27",
  "stage": "ResponseComplete",
  "requestURI": "/api/v1/namespaces/monitoring/secrets/etcd-certs",
  "verb": "get",
  "user": {
    "username": "kubernetes-admin",
    "groups": [ "system:masters", "system:authenticated" ]
  },
  "sourceIPs": [ "127.0.0.1", "10.11.22.33" ],
  "userAgent": "kubectl/v1.23.3 (darwin/amd64) kubernetes/816c97a",
  "objectRef": {
    "resource": "secrets",
    "namespace": "monitoring",
    "name": "etcd-certs",
    "apiVersion": "v1"
  },
  "responseStatus": { "metadata": {}, "code": 200 },
  "requestReceivedTimestamp": "2022-03-17T16:25:11.523930Z",
  "stageTimestamp": "2022-03-17T16:25:11.525764Z",
  "annotations": {
    "authorization.k8s.io/decision": "allow",
    "authorization.k8s.io/reason": ""
  }
}
```

What should be recorded?

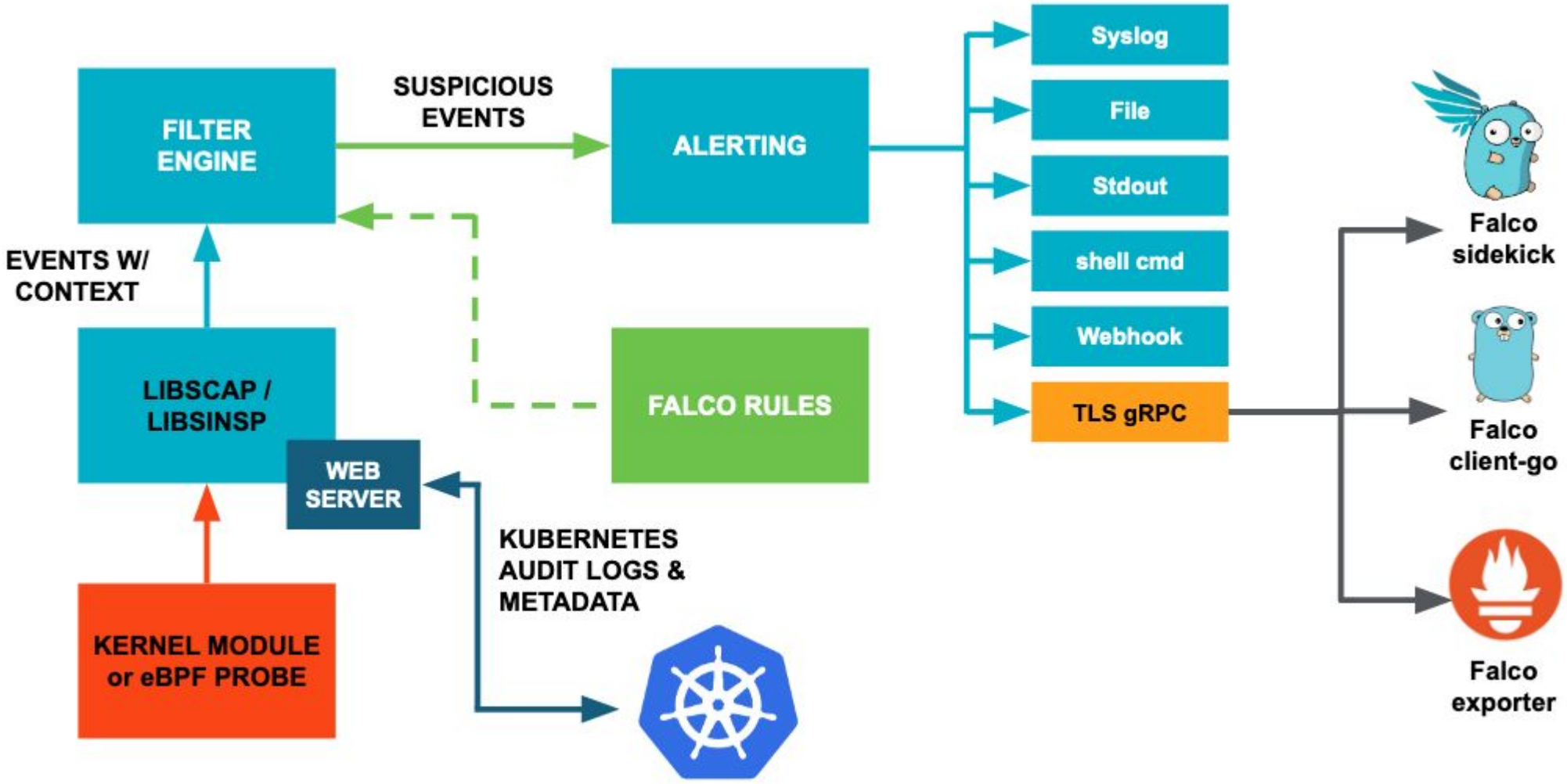

```yaml
apiVersion: audit.k8s.io/v1
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "RequestReceived"
rules:
  # Log pod changes at RequestResponse level
  - level: RequestResponse
    resources:
    - group: ""
      resources: ["pods"]
  # Log "pods/log", "pods/status" at Metadata level
  - level: Metadata
    resources:
    - group: ""
      resources: ["pods/log", "pods/status"]

  # Don't log requests to a configmap called "controller-leader"
  - level: None
    resources:
    - group: ""
      resources: ["configmaps"]
      resourceNames: ["controller-leader"]
```

A Runtime Security Engine

- Cloud-Native runtime security project
- Kubernetes audit events support
- Parsing the Linux system calls from the kernel at runtime
- Detecting unexpected behavior, intrusions, and data theft in real time
- Asserting the stream against a powerful rules engine to check the kernel for unusual behaviors
- Alerting when a rule is violated
- Drivers: Kernel module, eBPF probe, userspace instrumentation

https://falco.org

Falco Architecture



Source: https://www.cncf.io/wp-content/uploads/2020/08/Kubernetes-Runtime-Security-with-Falco-and-Sysdig.pdf

Falco Configuration

- Enabled embedded web server to accept Kubernetes audit events on (/k8s-audit: 8765)
- Managed by Helm Chart
- JSON output type

```
...
jsonOutput: true
jsonIncludeOutputProperty: false
webserver:
  enabled: true
  listenPort: 8765
  k8sAuditEndpoint: /k8s-audit
rulesFile:
  - /etc/falco/falco_rules.yaml
  - /etc/falco/falco_rules.local.yaml
  - /etc/falco/k8s_audit_rules.yaml
...
```

Find more: https://github.com/falcosecurity/charts

override

Add override rules
according to business requirements

postgres

Postgres Specific Rules
Allow file prefixes, inbound/outbound ports, etc.

consul

Consul Specific Rules
Allow TCP connections, file read/write, syscalls

kubernetes

Kubernetes Specific Rules
for api-server, scheduler, dns, proxy, etc.

Falco Rules

and Profiles

fim

File Integrity Module
Kernel module modification, file permission change, etc.

elasticsearch

Elasticsearch Specific Rules
Allow inbound ports, some plugins, etc.

mitre

Common Security Standards
Spawn procs, sensitive file read, ssh, spawn shell, etc.

haproxy

HAProxy Specific Rules
Allow cache path, image reference, etc.

nginx

nginx Specific Rules
Allow inbound/outbound ports, processes, etc.

etcd

ETCD Specific Rules
Allow file prefixes, inbound/outbound ports, etc.

Overriding Falco Rules

- Create fine-tuned rules by defining allow list for events
- Define override rules for tribe, team and project according to business requirements

```yaml
- rule: Launch Privileged Container
  desc: Detect the initial process started in a privileged
container. Exceptions are made for known trusted images.
  condition: >
    container_started and container
    and container.privileged=true
    and not user_privileged_containers
  output: Privileged container started (user=%user.name
user_loginuid=%user.loginuid command=%proc.cmdline
%container.info
image=%container.image.repository:%container.image.tag)
  priority: INFO
  tags: [container, cis, mitre_privilege_escalation,
mitre_lateral_movement]

- macro: user_privileged_containers
  condition: (never_true)
```

Overrides

Per Tribe
Per Team
Per Project

```yaml
customRules:
  override-rules.yaml: |-

    - list: user_privileged_allow_list
      items: [registry.test.com/foo/bar/baz]

    # Overrides the user_privileged_containers macro
    - macro: user_privileged_containers
      condition: container.image.repository in (user_privileged_allow_list)
```

Eliminating False-Positives

with Falco Rule Exceptions


```
exceptions:
- name: allow_consul_do_curl
  fields: [container.image, proc.cmdline]
  comps: [contains, =]
  values:
  - [consul, curl http://127.0.0.1:8500/v1/status/leader]
```

```
exceptions:
- name: allow_nginx_8081
  fields: [proc.cmdline, container.image, k8s.pod.name, fd.sport]
  comps: [=, contains, contains, =]
  values:
    - [nginx, nginx, nginx, 8081]
```

```
exceptions:
- name: allow_read_data_dir
  fields: [proc.cmdline, container.image, k8s.pod.name]
  comps: [contains, contains, contains]
  values:
    - [/data, redis, redis]
```

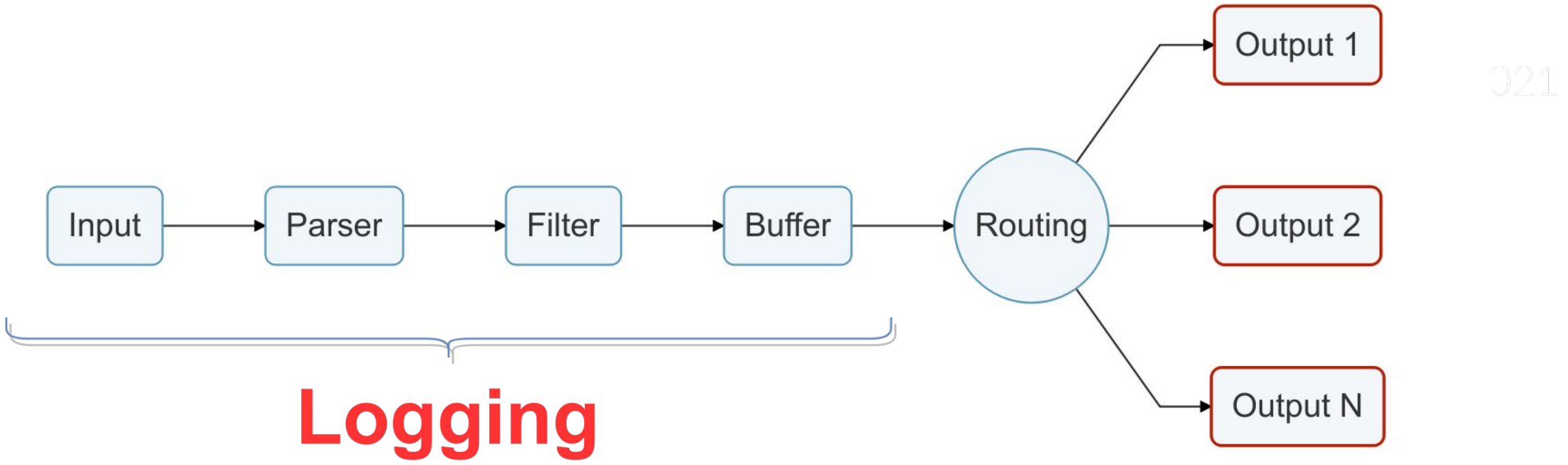
Apply

Fluent Bit

An End to End Observability Pipeline

- High scale data observability in distributed environment
- Built in buffering and error-handling capabilities
- Prometheus and OpenTelemetry compatible
- Lightweight and asynchronous design
- Pluggable architecture and extensibility
- Unstructured data parsing
- Resiliency and reliability: Backpressure handling, buffering, retries

Pipeline



- Input plugins ： https://docs.fluentbit.io/manual/pipeline/inputs
- Parser plugins: https://docs.fluentbit.io/manual/pipeline/parsers
- Filter plugins ： https://docs.fluentbit.io/manual/pipeline/filters

Configuring Fluent Bit based on our needs

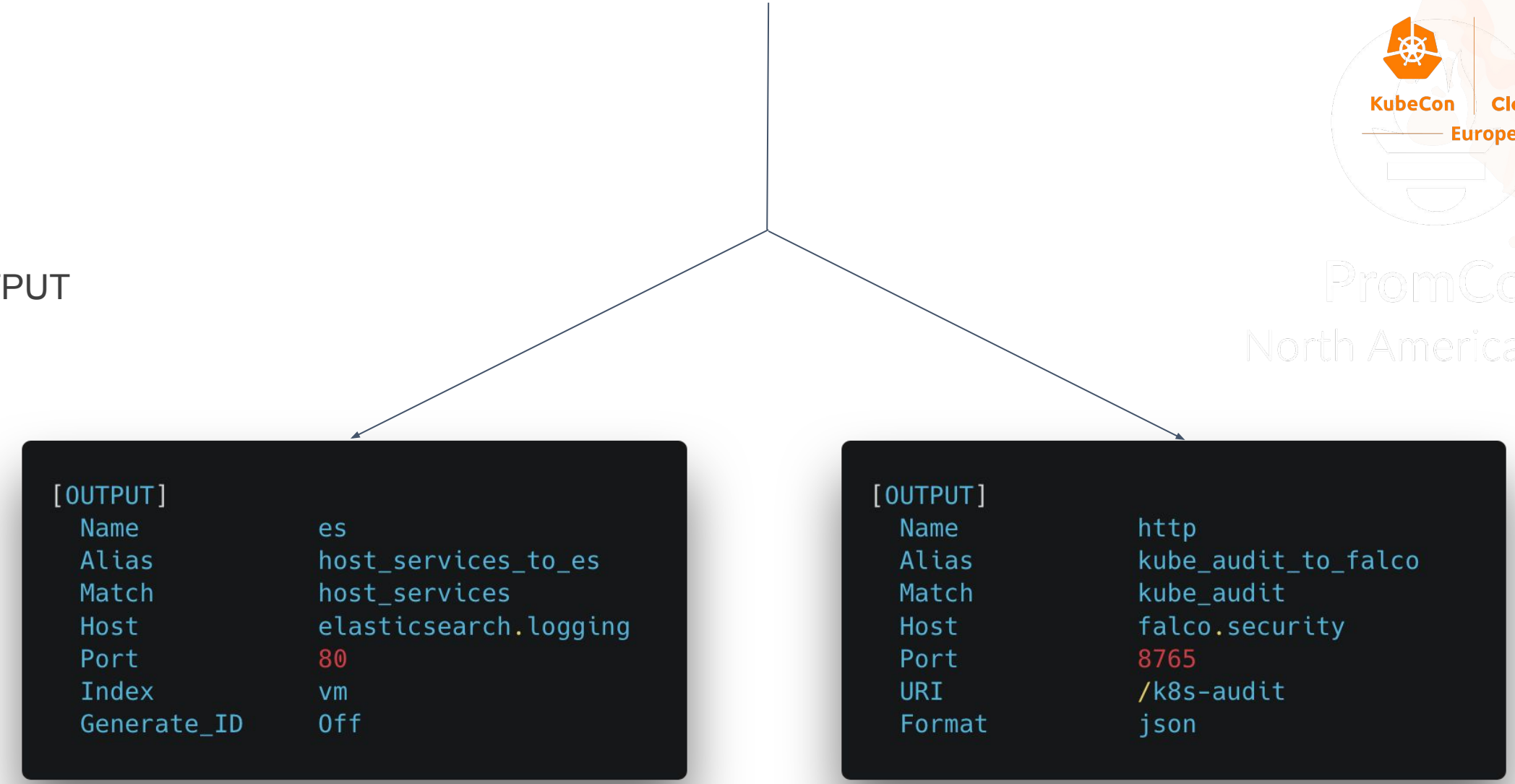
1. INPUT

```
[INPUT]
  Name              tail
  Alias             kube_audit
  Tag               kube_audit
  Buffer_Chunk_Size 512k
  Buffer_Max_Size   5m
  Path              /var/log/kubernetes/audit/kube-apiserver-audit.log
  Parser            json
  DB                /var/log/flb_kube_audit.db
  Mem_Buf_Limit     128MB
  Skip_Long_Lines   On
  Refresh_Interval  10
```

2. FILTER

```
[FILTER]
  Name          modify
  Alias         kube_audit_modify
  Match_Regex ^(kube_audit)$
  Add           x_region ${REGION}
  Add           x_team ${TEAM}
  Add           x_environment ${ENVIRONMENT}
  Add           x_cluster ${CLUSTER}
```

3. OUTPUT



```
[OUTPUT]
  Name            es
  Alias           host_services_to_es
  Match           host_services
  Host            elasticsearch.logging
  Port            80
  Index           vm
  Generate_ID     Off
```

```
[OUTPUT]
  Name            http
  Alias           kube_audit_to_falco
  Match           kube_audit
  Host            falco.security
  Port            8765
  URI             /k8s-audit
  Format          json
```

Why Fluent Bit with Log Backend over Kubernetes Webhook Backend

Fluent Bit

- More resilient and built-in reliability
- Prometheus metrics *per output*
- Easy defining alert rules *per output*
- Send audits to *multiple* destinations: Falco and Elasticsearch
- Easy to reconfigure pipeline according to business requirements
- Compatible with our pull-based architecture
- Sweet logo

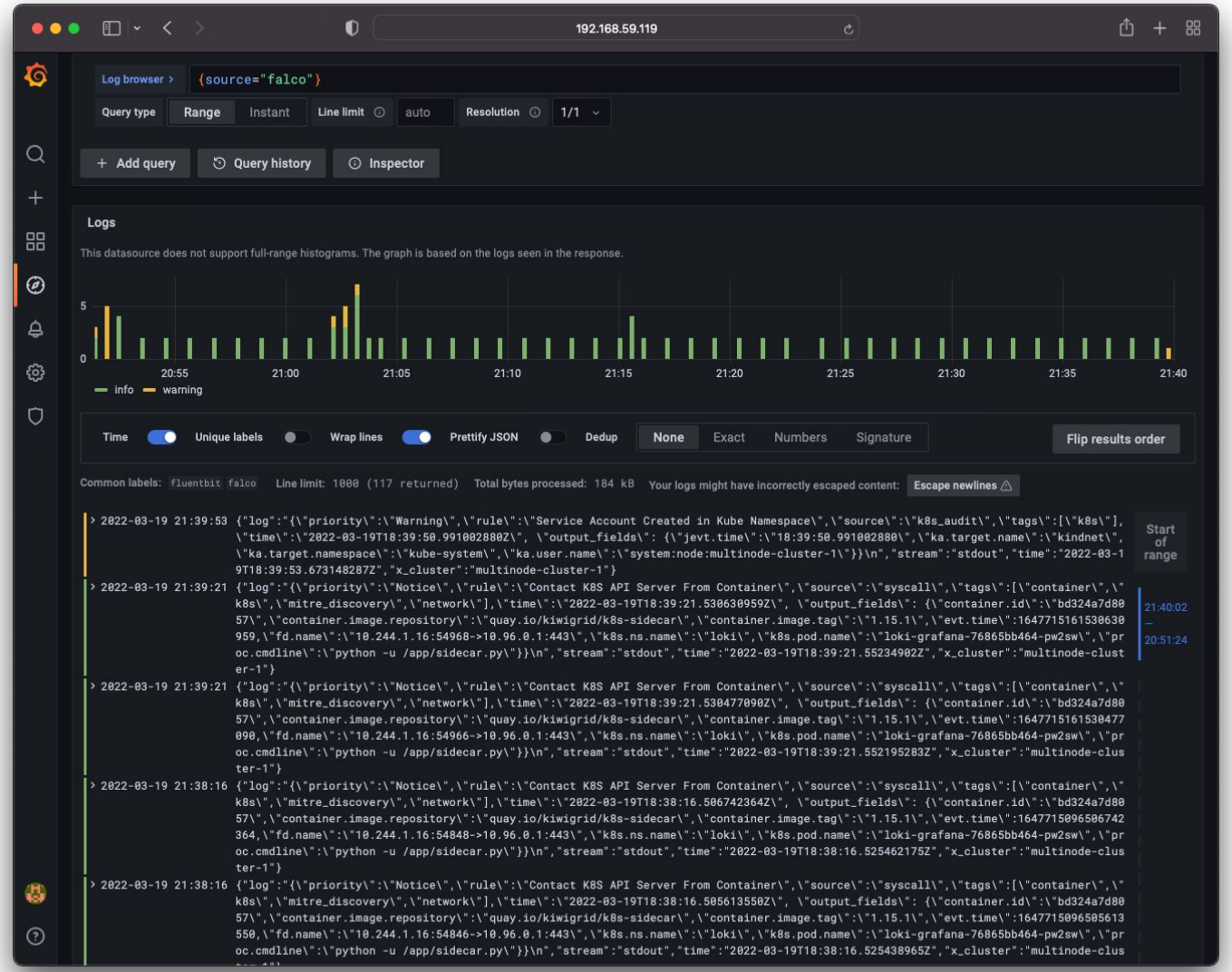
Kubernetes Webhook Backend

- Resiliency with exponential backoff
- Prometheus metrics: events, errors, rejected
- Easy defining alert rules
- Send audits to *single* destination: Falco
- API server network request overhead

Source: https://github.com/kubernetes/kubernetes/blob/master/staging/src/k8s.io/apiserver/plugin/pkg/audit/webhook/webhook.go

Monitoring

Log Query



optional log pipeline

filter operator

- `|=` line filter expression
- `!=` line filter expression
- `|~` line filter expression
- `!~` line filter expression

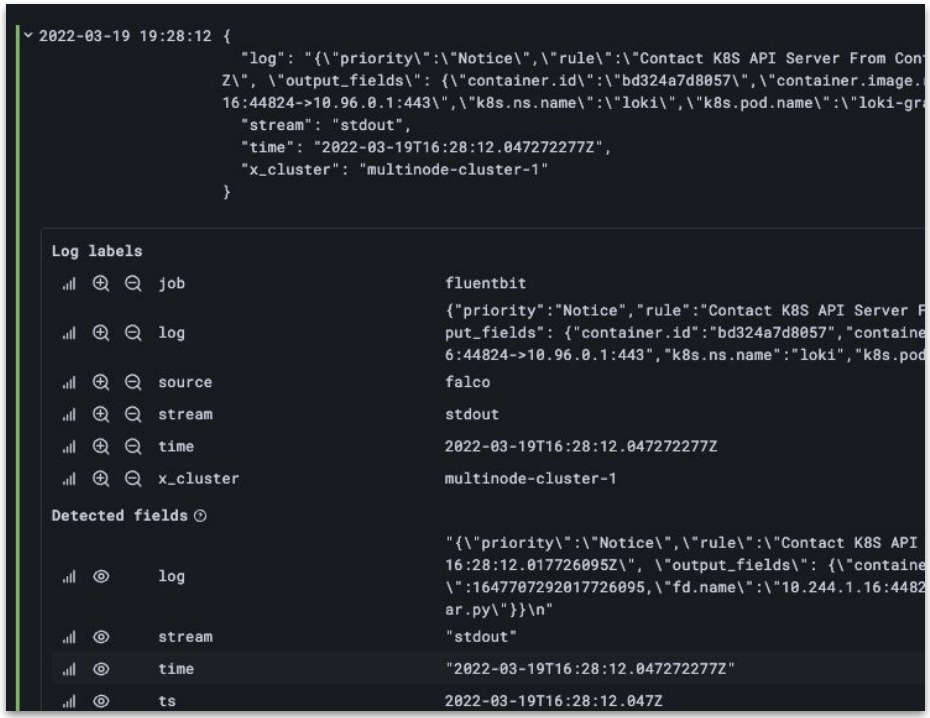
{ stream selector }

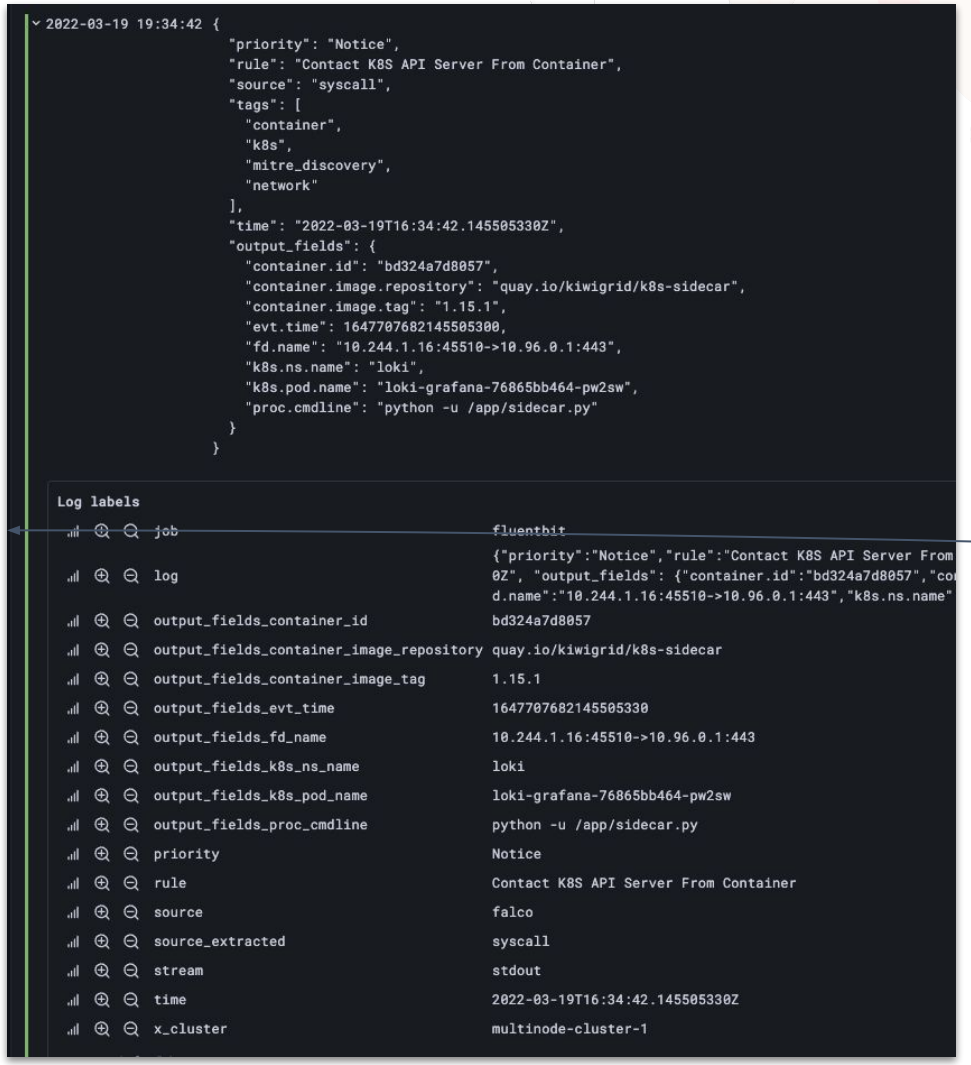
- `=` label filter expression
- `!=` label filter expression
- `=~` label filter expression
- `!~` label filter expression
- `>` `>=` label filter expression
- `<` `<=` label filter expression

parser expression
line format expression
label format expression

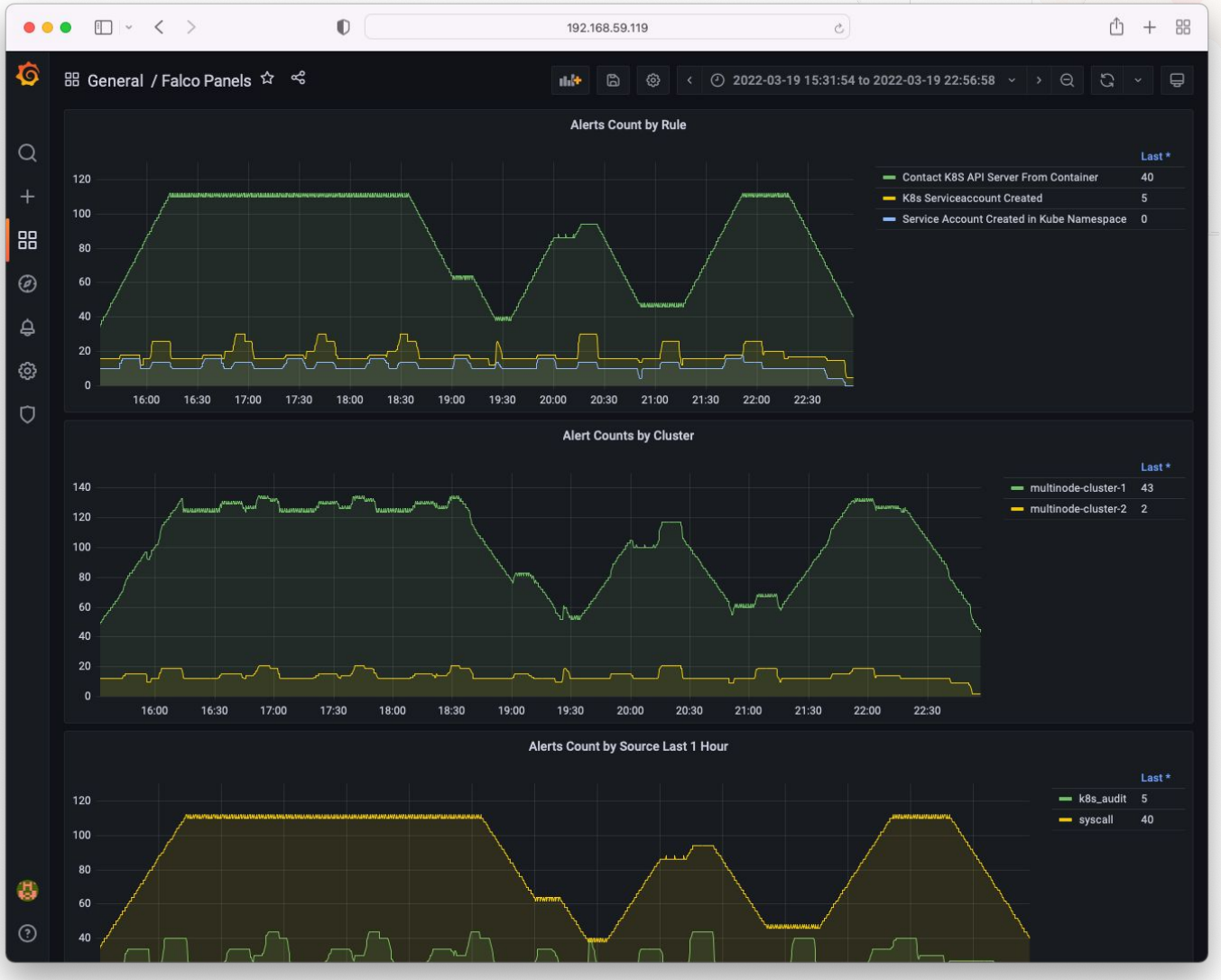
```
{source="falco"}
  | json
```

```
{source="falco"}
  | json
  | line_format "{{.log}}"
  | json
```





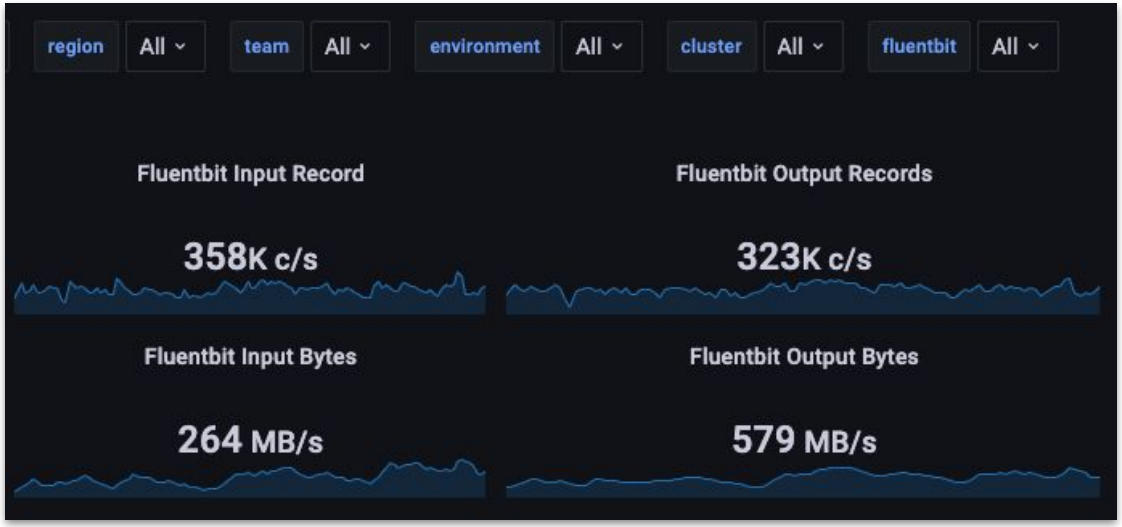
```
sum by (rule)
(count_over_time(
  {source="falco"}
    | json
    | line_format "{{.log}}"
    | json [1h]))
```

Challenges at High Scale

- Requires manual task for tuning the rules to eliminate false positives
- Overriding fine-tuned rules per team or project is time-consuming
- Tremendous amount of audits generated every minute
- Keeping sliding time window short
- Data storage grows every second
- Building efficient HA backend

What Happens in Seconds



(No Filter - All Outputs)

358K

Fluent Bit Output Records
per second

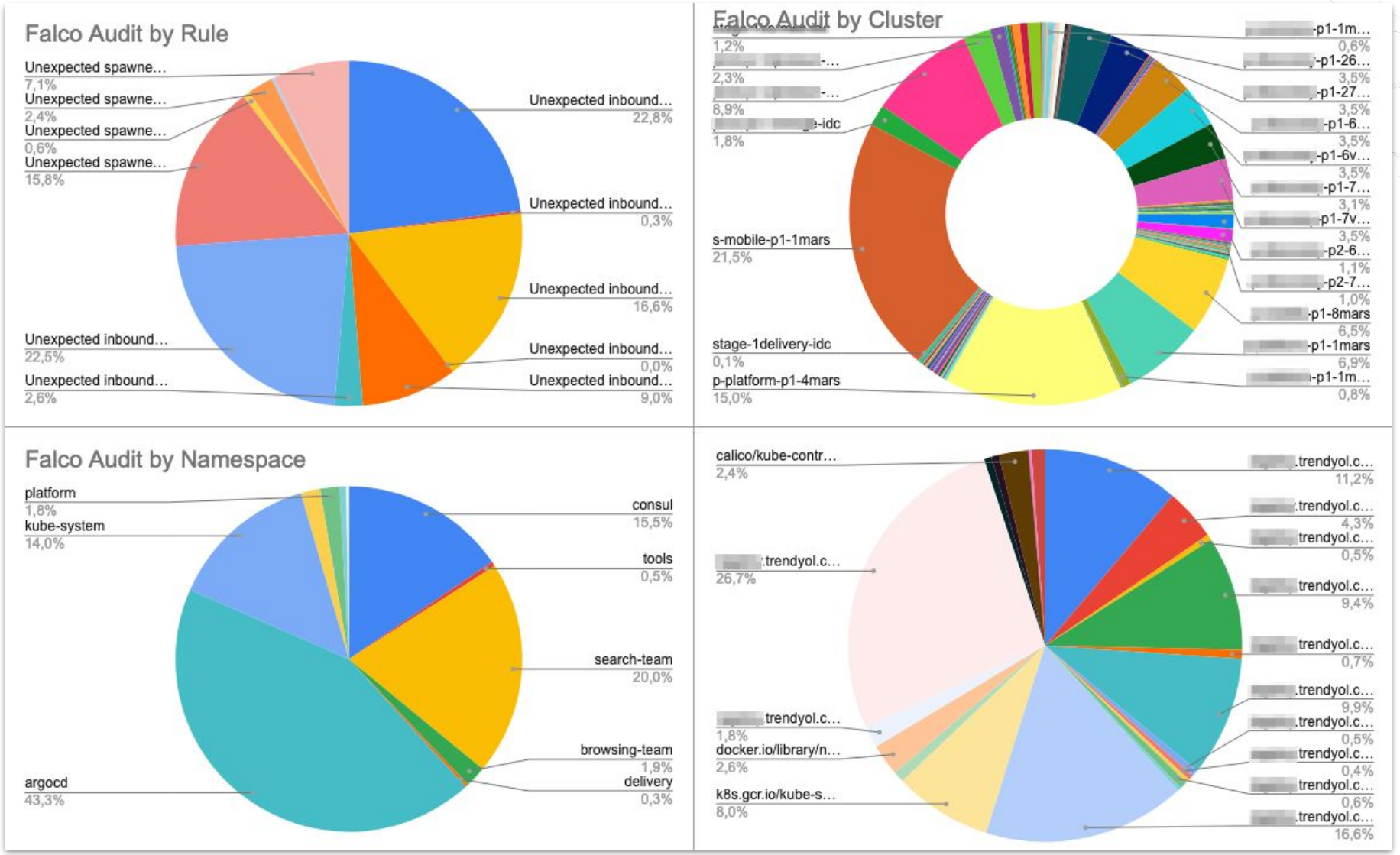
487K

Kubernetes Audit Events
per minute

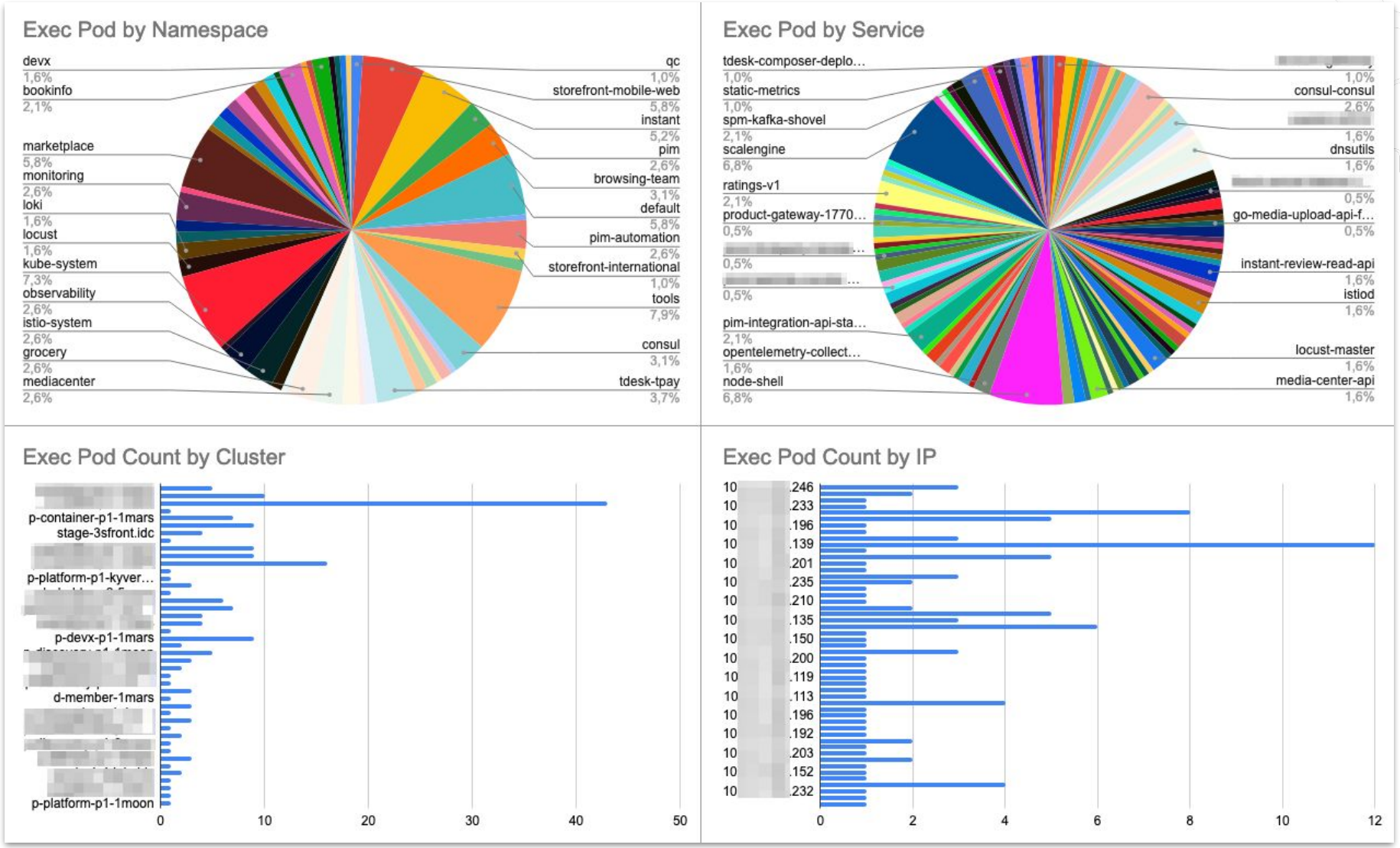
8K

Kubernetes Audits *scanned by Falco*
per second

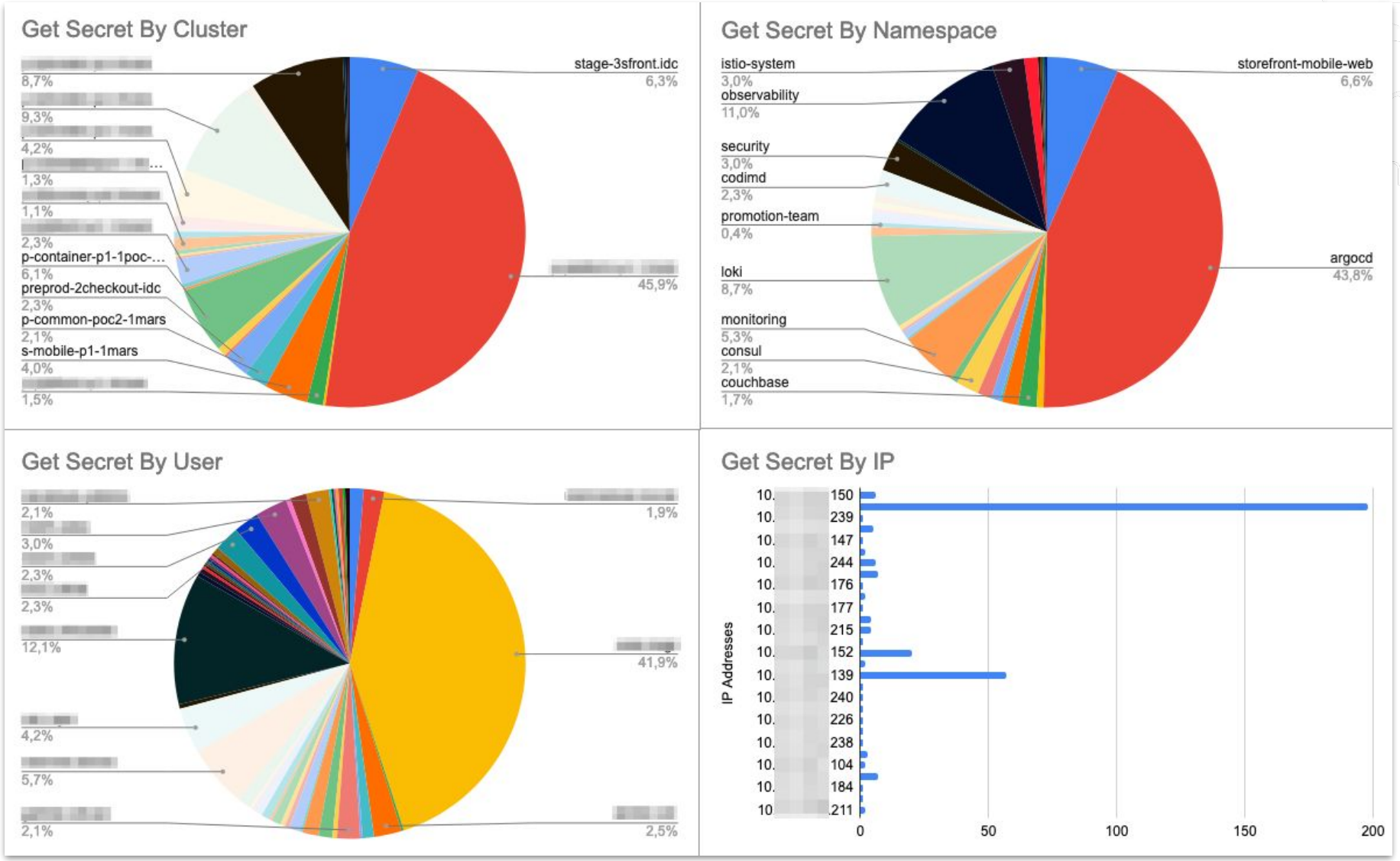
Falco Audit Events



Exec Pod Events



Get Secret Events

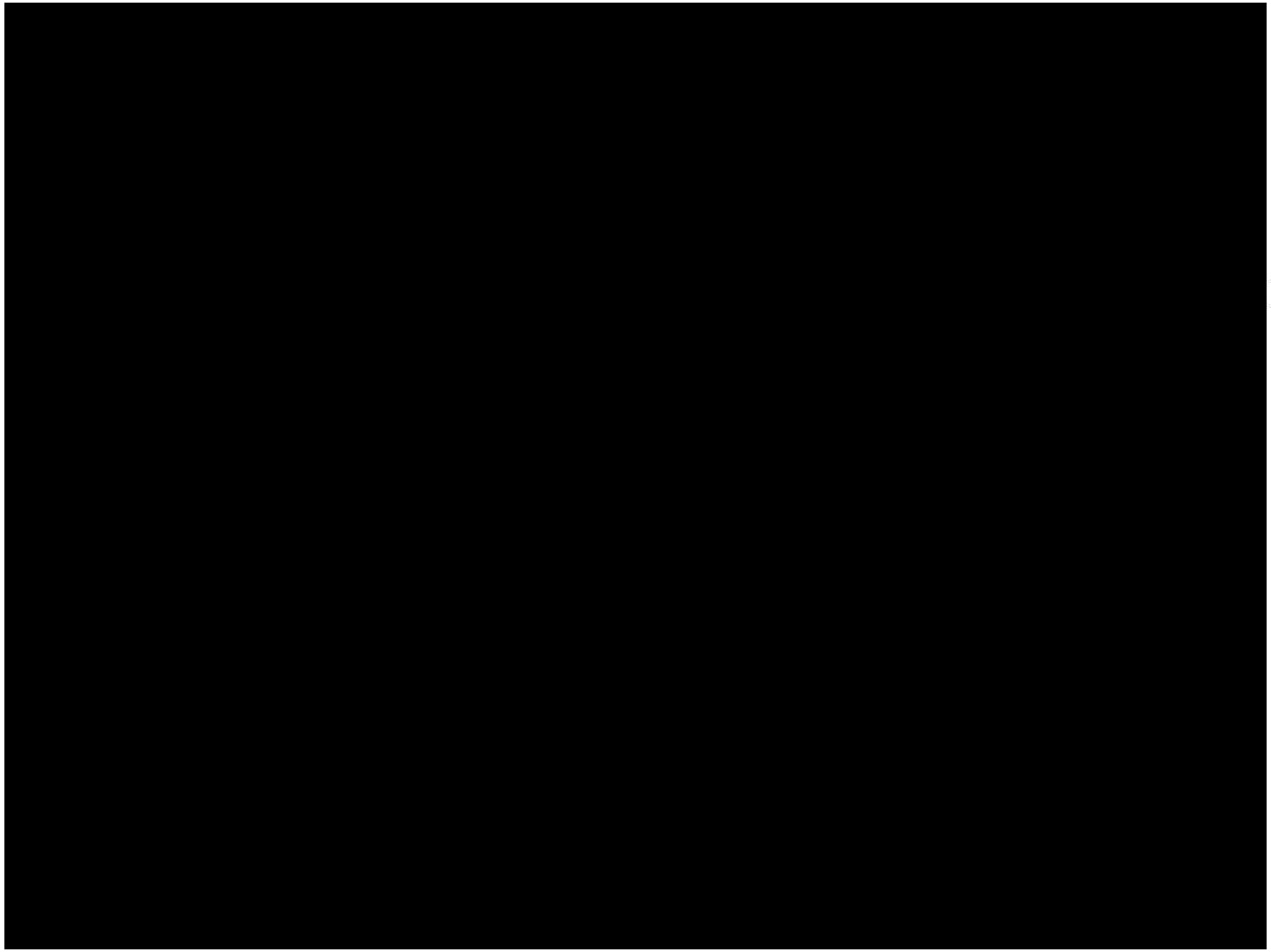


Weekly Report

Kubernetes - Pod Exec Detection - Weekly Report

Pod	Namespace	Cluster	IP	URI	Details	Time	Count	Remote IP	user
t-gateway-preprod-deployment-687b784d4d-wksmq	zeus	p-mobile-p1-3moon		/api/v1/namespaces/zeus/pods/-gateway-preprod-deployment-687b784d4d-wksmq/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=-gateway-preprod&stdin=true&stdout=true&tty=true	zeus : -gateway-preprod-deployment-687b784d4d-wksmq (1)	Fri Mar 18 09:54:32 2022	1		
argocd-applicationset-controller-6b94ff6d96-k5p2n	argocd	s-mobile-p1-1mars		/api/v1/namespaces/argocd/pods/argocd-applicationset-controller-6b94ff6d96-k5p2n/exec?command=sh&container=argocd-applicationset-controller&stderr=true&stdin=true&stdout=true&tty=true	argocd : argocd-applicationset-controller-6b94ff6d96-k5p2n (1)	Fri Mar 18 14:47:26 2022	1		
-api-cb-prod-578dcbf5d9-ft7k6	product-international	p-product-p1-1moon		/api/v1/namespaces/product-international /pods/-api-cb-prod-578dcbf5d9-ft7k6/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=main&stdin=true&stdout=true&tty=true	product-international : -api-cb-prod-578dcbf5d9-ft7k6 (1)	Thu Mar 17 17:54:25 2022	1		
-6b787bc684-vp5bt	instant	s-mobile-p1-1mars		/api/v1/namespaces/instant/pods/-6b787bc684-vp5bt/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=&stdin=true&stdout=true&tty=true	instant : -6b787bc684-vp5bt (1)	Wed Mar 16 14:55:49 2022	1		
-6b787bc684-vp5bt	instant	s-mobile-p1-1mars		/api/v1/namespaces/instant/pods/-6b787bc684-vp5bt/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=&stdin=true&stdout=true&tty=true	instant : -6b787bc684-vp5bt (1)	Wed Mar 16 16:25:16 2022	1		
c73dd-gng6xt5-api-5d74595d9-nzdsg	pim-automation	s-mobile-p1-1mars		/api/v1/namespaces/pim-automation/pods/c73dd-gng6xt5-api-5d74595d9-nzdsg/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=api&stdin=true&stdout=true&tty=true	pim-automation : c73dd-gng6xt5-api-5d74595d9-nzdsg (1)	Mon Mar 14 14:52:36 2022	1		
-consumer-deployment-77bcdz796l	supply-management	p-tyaas-p1-1moon		/api/v1/namespaces/supply-management /pods/-consumer-deployment-77bcdz796l/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=-consumer&stdin=true&stdout=true&tty=true	supply-management : -consumer-deployment-77bcdz796l (1)	Fri Mar 18 14:39:27 2022	1		
-api-deployment-7bcc4b4b5c-76z9g	ecomswat	p-ecomcore-p1-1moon		/api/v1/namespaces/ecomswat/pods/-api-deployment-7bcc4b4b5c-76z9g/exec?command=sh&command=-c&command=clear%3B+%28bash+%7C%7C+ash+%7C%7C+sh%29&container=&stdin=true&stdout=true&tty=true	ecomswat : -api-deployment-7bcc4b4b5c-76z9g (1)	Tue Mar 15 17:06:30 2022	1		
consul-consul-885ql	consul	p-common-p1-1mars		/api/v1/namespaces/consul/pods/consul-consul-885ql/exec?command=%2Fbin%2Fsh&container=consul&stdin=true&stdout=true&tty=true	consul : consul-consul-885ql (1)	Mon Mar 14 16:01:29 2022	1		
consul-consul-sync-catalog-674d4485b6-hlf2d	consul	p-common-p1-1mars		/api/v1/namespaces/consul/pods/consul-consul-sync-catalog-674d4485b6-hlf2d/exec?command=%2Fbin%2Fsh&container=consul-sync-catalog&stdin=true&stdout=true&tty=true	consul : consul-consul-sync-catalog-674d4485b6-hlf2d (1)	Mon Mar 14 16:04:17 2022	1		

Demo



github.com/eminaktas/threat-hunting-at-scale-demo

P.S: We encourage you to do it yourself at home.

What’s Next?

- Response Engine
- Policy Engine
- SoC Team
- On-Call Alerts
- .
- .

Thank You!

@trendyoltech

jobs.lever.co/trendyol