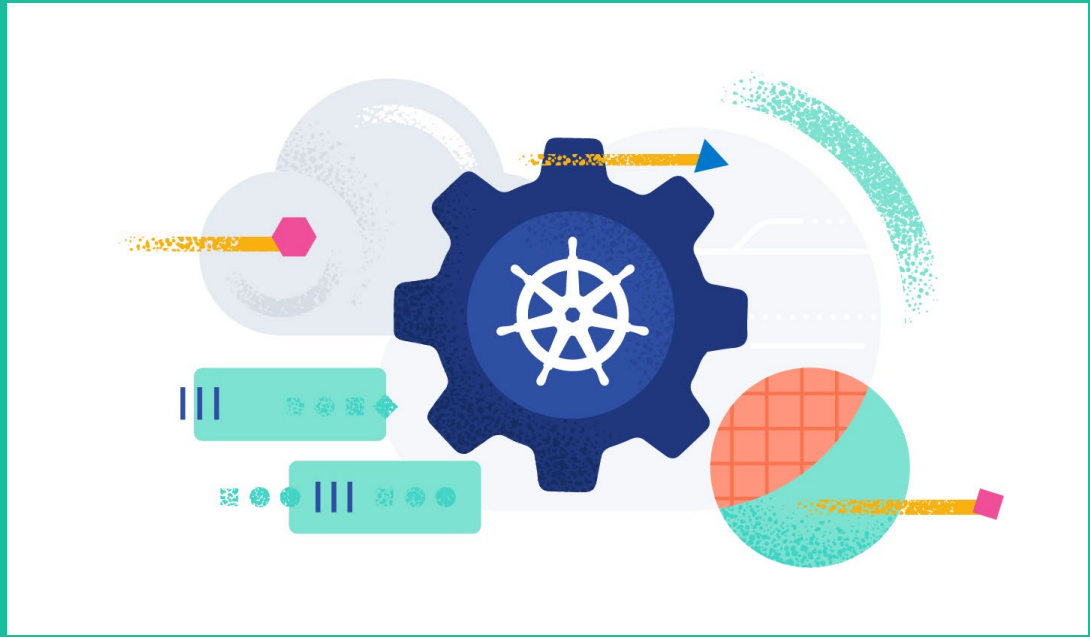
Incident Response in Kubernetes



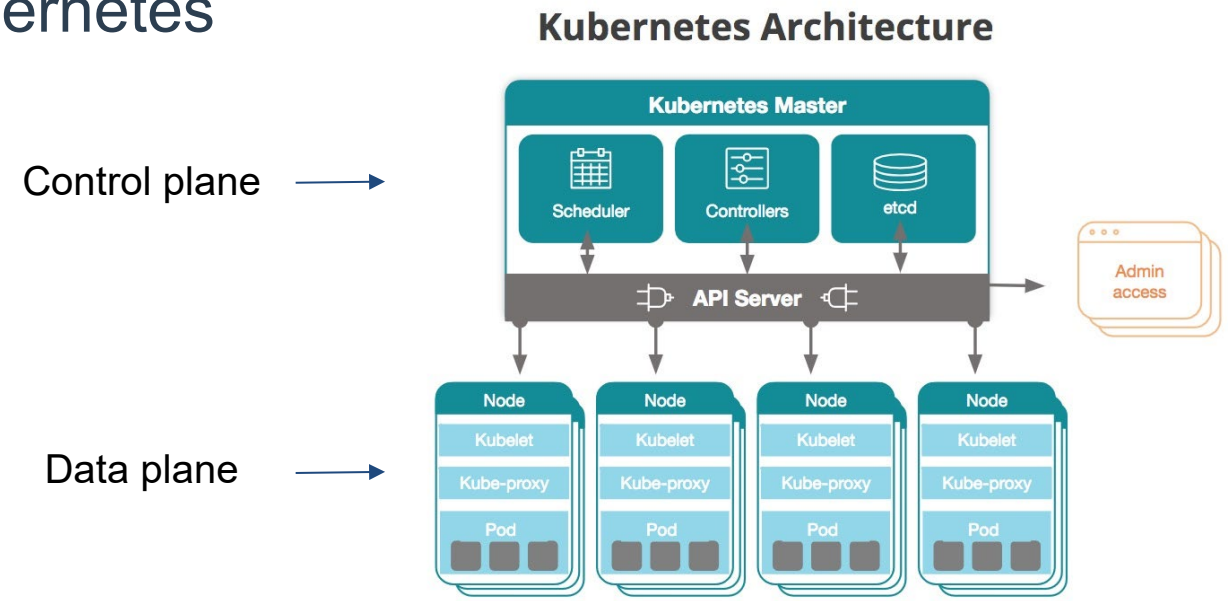
Mahdi Alizadeh
March 2025

Outline

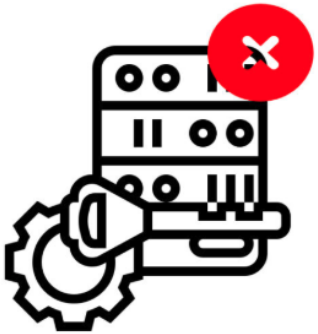
- Kubernetes
- Attack Tactics - Example scenario
- Incident response in Kubernetes
  - Important Logs
  - Disk Forensics
  - Memory Forensics
  - Live Forensics
  - Container Checkpointing

Kubernetes

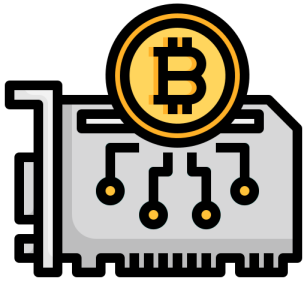
- Benefit: scalability & flexibility
- Over 50% of Fortune 100 companies have adopted Kubernetes



Security Challenges



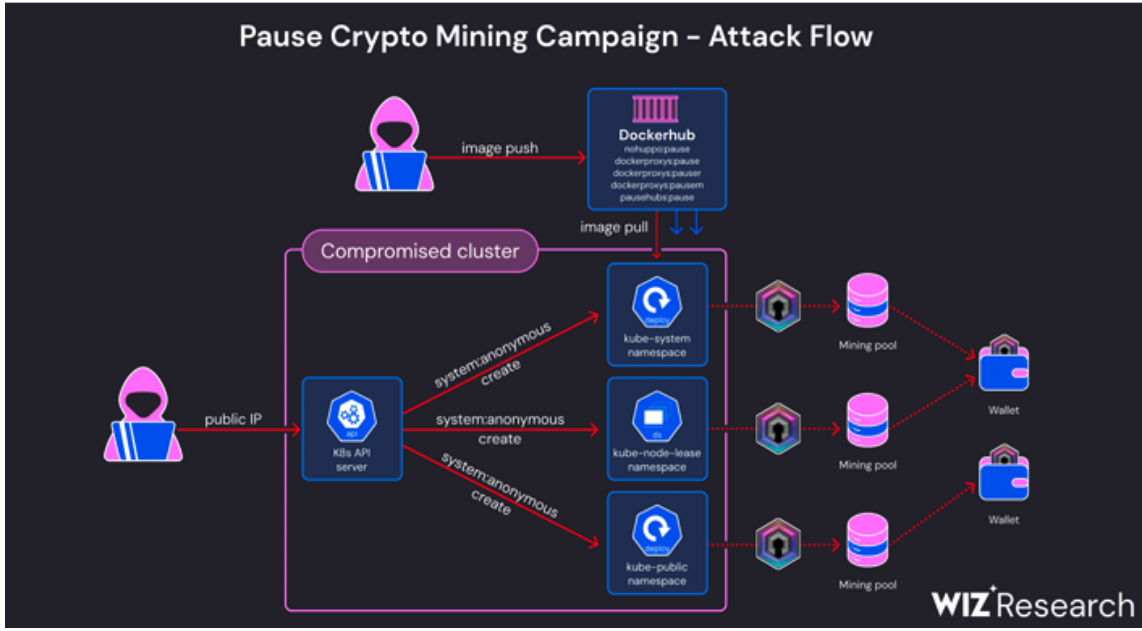
Misconfiguration/
Vulnerabilities



Crypto Mining or
Data Theft

Cryptojacking Campaign Targets Misconfigured Kubernetes Clusters

Jun 12, 2024 Ravie Lakshmanan

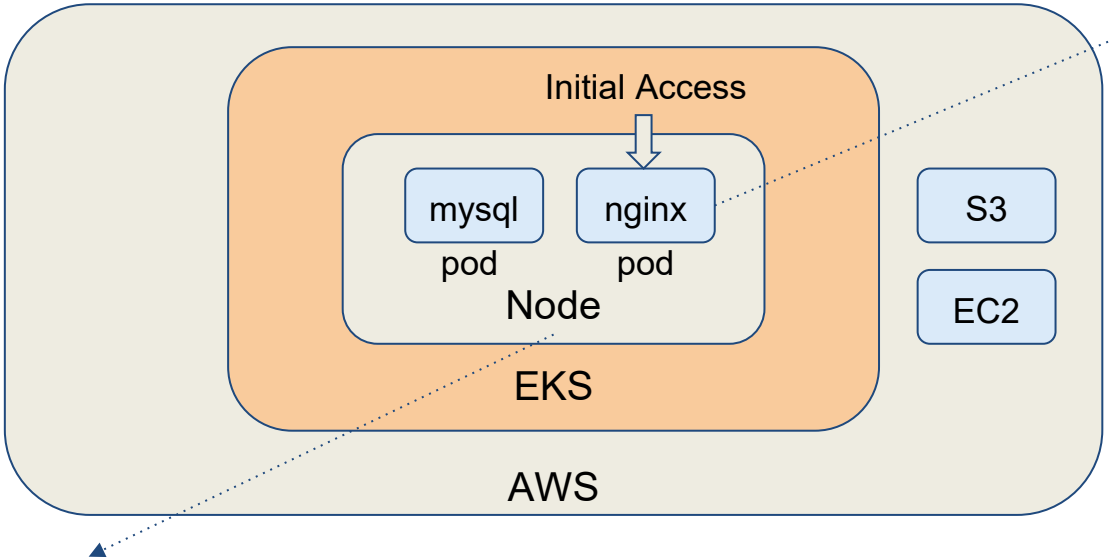


Incident Response Challenges

Limited Visibility: Ephemeral, No EDR/Logs

Complex: Multi-Layered Attack Surface + Autoscaling

Attack Scenario: Example

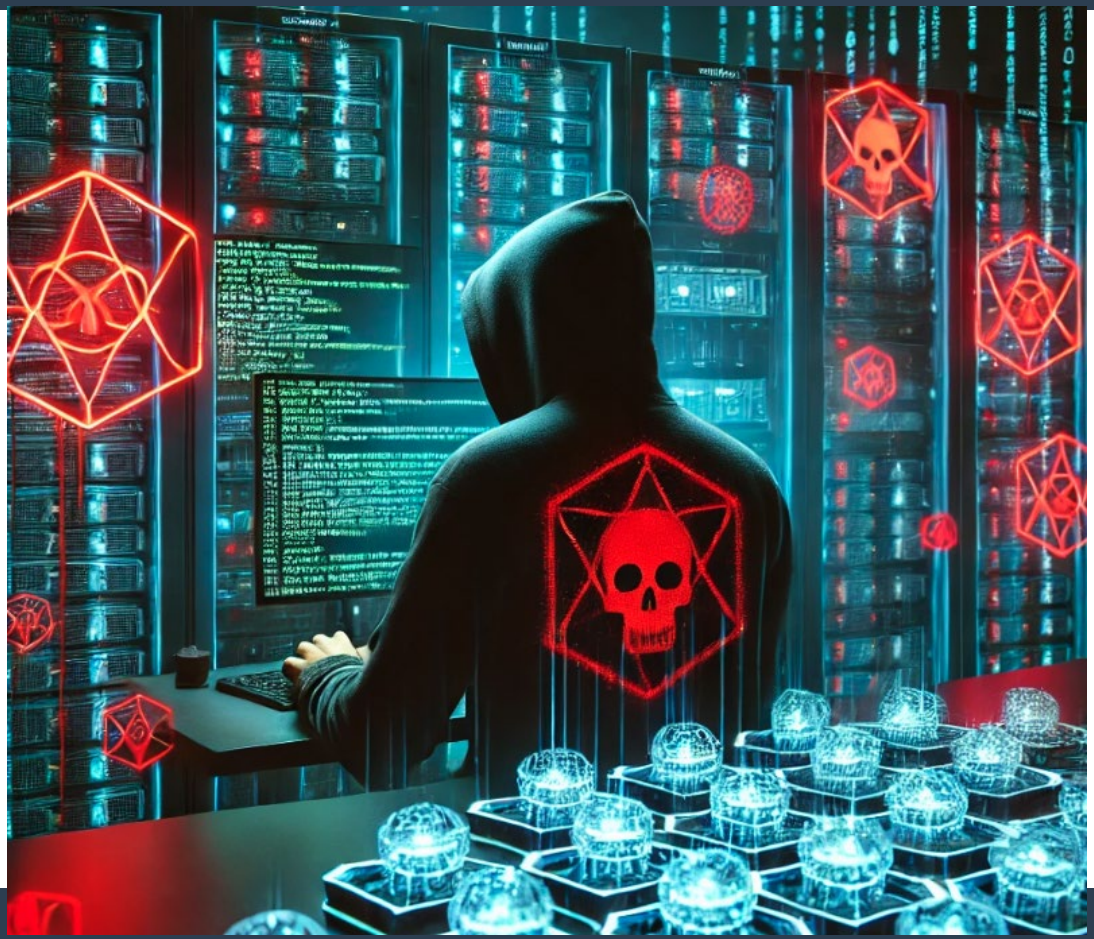


Misconfiguration: High priv role assigned to Node

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
  - name: nginx
    image: nginx:1.14.2
    ports:
      containerPort: 80
    securityContext:
      privileged: true
  nodeSelector:
    nodegroup: nodegroup-1
```

Misconfiguration: host FS accessible from pod

Demo



	Title	Severity	Finding type	Resource	Count	Account ID	Last seen
☐	The EC2 instance i-0ec6681d8e97db894 queried a Bitcoin-related domain name.	High	CryptoCurrency:EC2/BitcoinTool.B!DNS	EC2 Instance: i-0ec6681d8e97db894	2	851725445286	19 hours ago
☐	A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EKS Cluster: k8-demo	1	851725445286	19 hours ago
☐	A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EKS Cluster: k8-demo	1	851725445286	19 hours ago
☐	A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EKS Cluster: k8-demo	1	851725445286	19 hours ago
☐	A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EKS Cluster: k8-demo	1	851725445286	19 hours ago
☐	A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EKS Cluster: k8-demo	1	851725445286	19 hours ago
☐	A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EKS Cluster: k8-demo	1	851725445286	19 hours ago
☐	A privileged container with root level access was launched on an EKS Cluster.	Medium	PrivilegeEscalation:Kubernetes/PrivilegedContainer	EKS Cluster: k8-demo	1	851725445286	20 hours ago
☐	A resource of type Instance has executed a suspicious command.	Low	Execution:Runtime/SuspiciousCommand	EC2 Instance: i-06e4ab90945267a7a	1	851725445286	20 hours ago
☐	A container has mounted a host directory.	Medium	PrivilegeEscalation:Runtime/ContainerMountsH	EKS Cluster: k8-demo	1	851725445286	21 hours ago

Guard Duty Alert

A Bitcoin-related domain name was queried by EC2 instance i-0ec6681d8e97db894.

High First seen 10 minutes ago, last seen 10 minutes ago Info

The process coredns from EC2 instance i-0ec6681d8e97db894 is querying a domain name that is associated with Bitcoin-related activity.

Investigate with Detective

This finding is Useful Not useful

Overview

Finding ID	2ecadf39bc20ac47a270fec50abf6146
Type	CryptoCurrency:Runtime/BitcoinTool.BIDNS
Severity	HIGH
Region	us-east-1
Count	4
Account ID	851725445286
Resource ID	k8-demo
Created at	03-22-2025 16:23:12 (7 minutes ago)
Updated at	03-22-2025 16:23:12 (7 minutes ago)

Resource affected

Resource type	EKSCluster

EKS cluster details

Name	k8-demo

ID	AIPA4MTWK5CTNNRWBK4KV

Instance tags

aws:ec2:fleet-id	fleet-6d1daf3f-1484-cc05-8e9a-2b0a01e545a3
eks:cluster-name	k8-demo
k8s.io/cluster-autoscaler/k8-demo	owned
aws:autoscaling:groupName	eks-nodegroup-1-eacadede-bb48-6a3a-1a12-cbfcecda7238
aws:ec2launchtemplate:id	lt-08af459fe33403a28
eks:nodegroup-name	nodegroup-1
aws:eks:cluster-name	k8-demo
k8s.io/cluster-autoscaler/enabled	true
aws:ec2launchtemplate:version	1
kubernetes.io/cluster/k8-demo	owned

Network interfaces

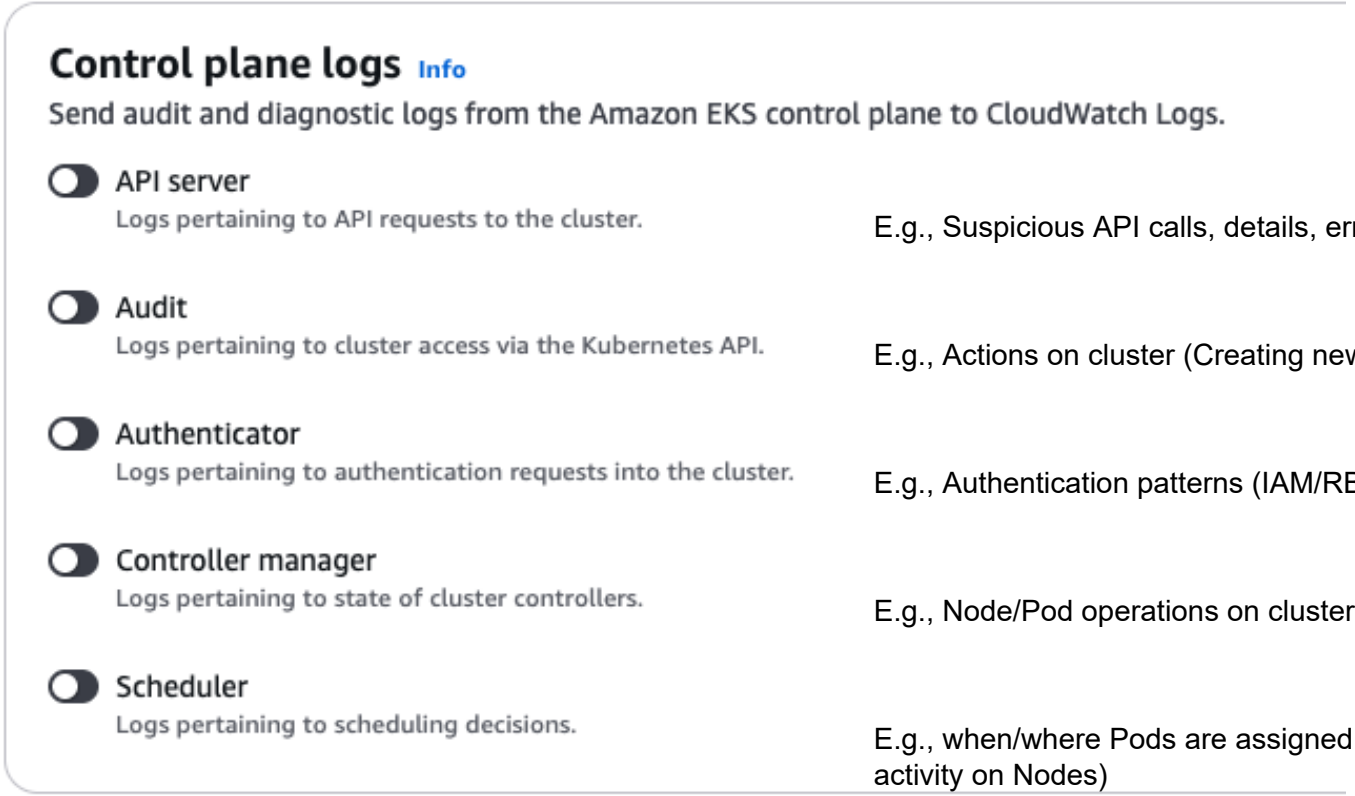
Network interface 0 (eni-083638e7c2e2887c4)

Network interface ID	eni-083638e7c2e2887c4
Private dns name	ip-172-31-36-230.ec2.internal
Private IP address	172.31.36.230
Public dns name	ec2-3-208-34-224.compute-1.amazonaws.com
Public IP	3.208.34.224
Subnet ID	subnet-046181eae6cc5e103
VPC ID	vpc-079659eab6cd006e7

Incident response in Kubernetes

- Important Logs
- Disk forensics
- Memory forensics
- Live forensics
- Container checkpointing

Important Logs



E.g., Suspicious API calls, details, errors

E.g., Actions on cluster (Creating new privileged Role)

E.g., Authentication patterns (IAM/RBAC)

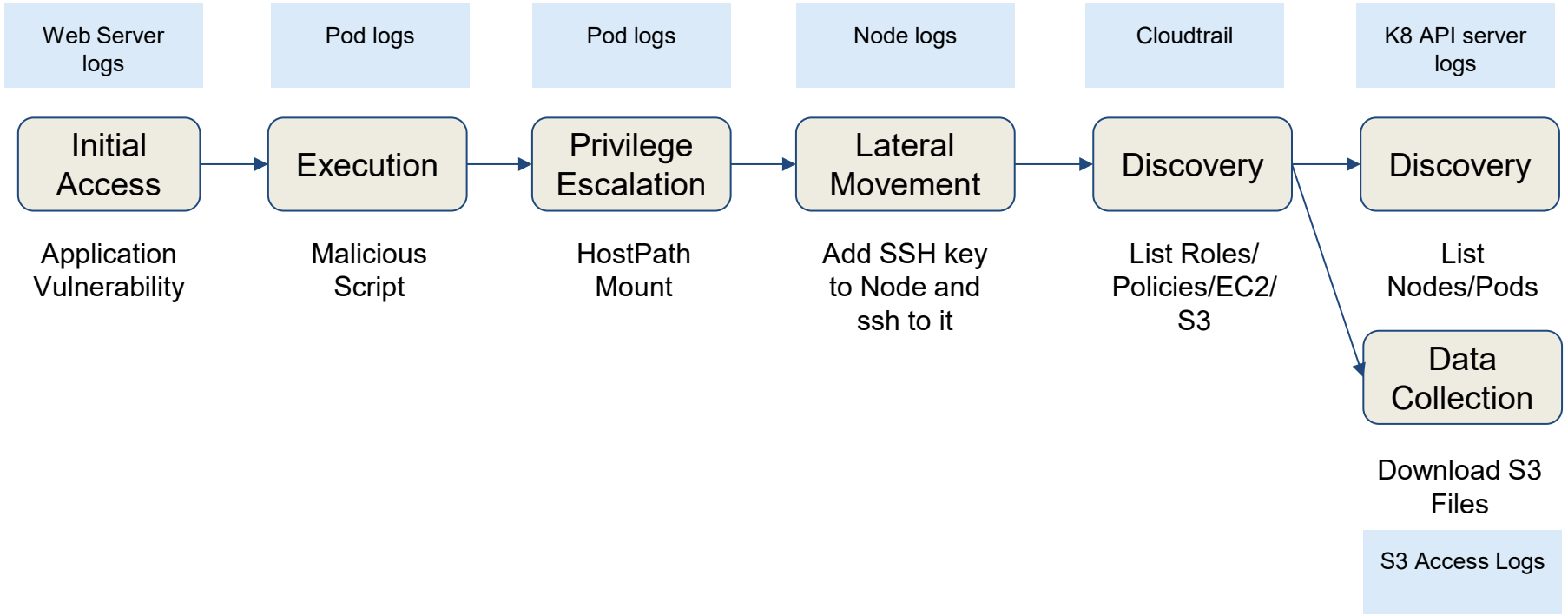
E.g., Node/Pod operations on cluster (e.g., node life cycle events)

E.g., when/where Pods are assigned & run (Identify all scheduling activity on Nodes)

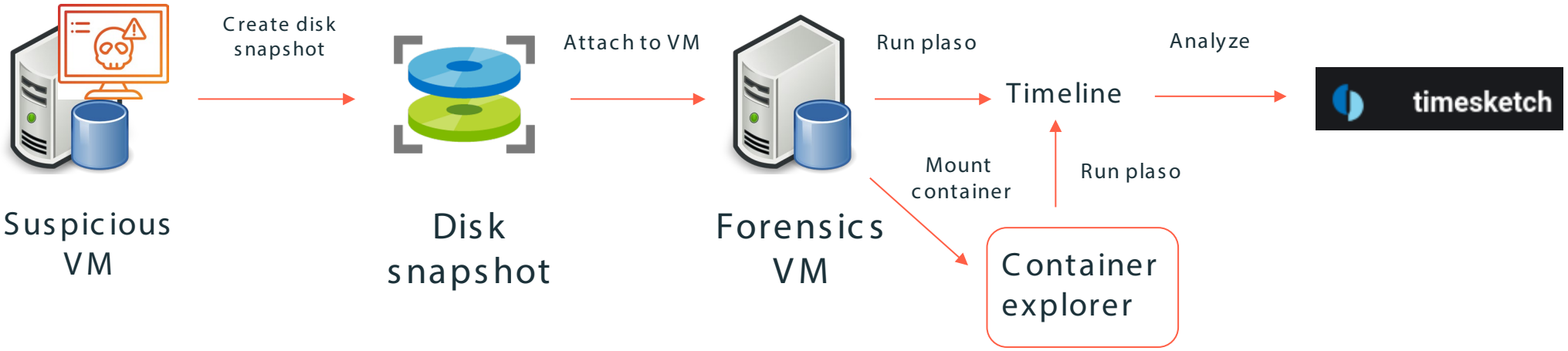
Important Logs

- **Cloud infra logs** :
  - cloudtrail (e.g., managing clusters)
  - Net-flow logs
  - DNS logs
  - Guard Duty alerts
- **Pod/Node logs** :
  - Node/Pod logs (process executions, Syslogs)
  - Application logs: Web Server logs

Attack Scenario: Example - Log sources



Disk Forensics



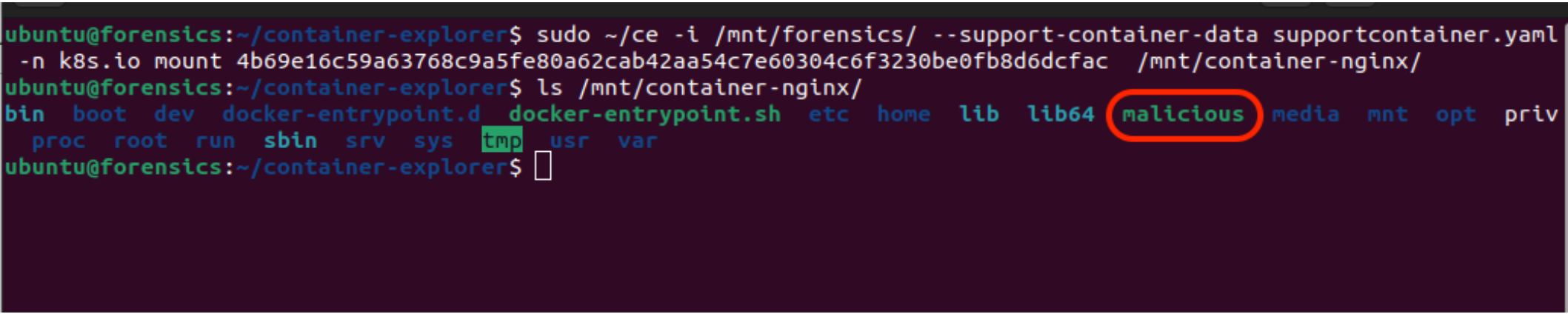
https://github.com/log2timeline/plaso
https://github.com/google/container-explorer
https://github.com/google/timesketch

Disk Forensics: Node

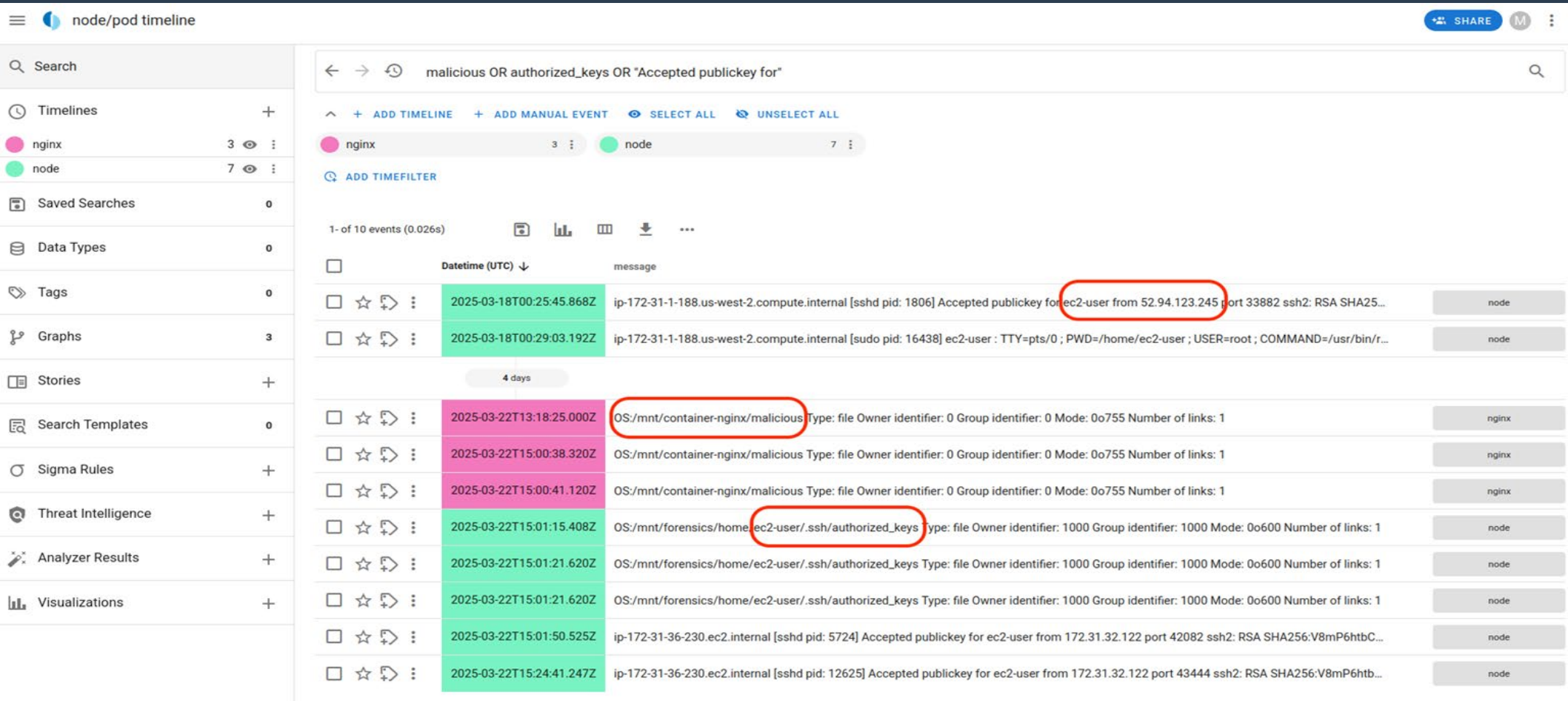
```
ubuntu@forensics:~$ cat /mnt/forensics/home/ec2-user/.bash_history
clear
aws sts get-caller-identity
aws iam list-attached-role-policies --role-name nodegroup
clear
aws ec2 describe-instances --query "Reservations[*].Instances[*].InstanceId"
aws s3 ls
aws s3 cp s3://k8demo11/file .
cat file
clear
cat <<EOF | sudo tee /etc/yum.repos.d/kubernetes.repo
[kubernetes]
name=Kubernetes
baseurl=https://pkgs.k8s.io/core:/stable:/v1.32/rpm/
enabled=1
gpgcheck=1
gpgkey=https://pkgs.k8s.io/core:/stable:/v1.32/rpm/repodata/repomd.xml.key
EOF

yum install kubectl
sudo yum install kubectl
clear
aws eks update-kubeconfig --region us-east-1 --name k8-demo
kubectl get pods
kubectl get nodes
exit
ubuntu@forensics:~$
```

Disk Forensics: nginx

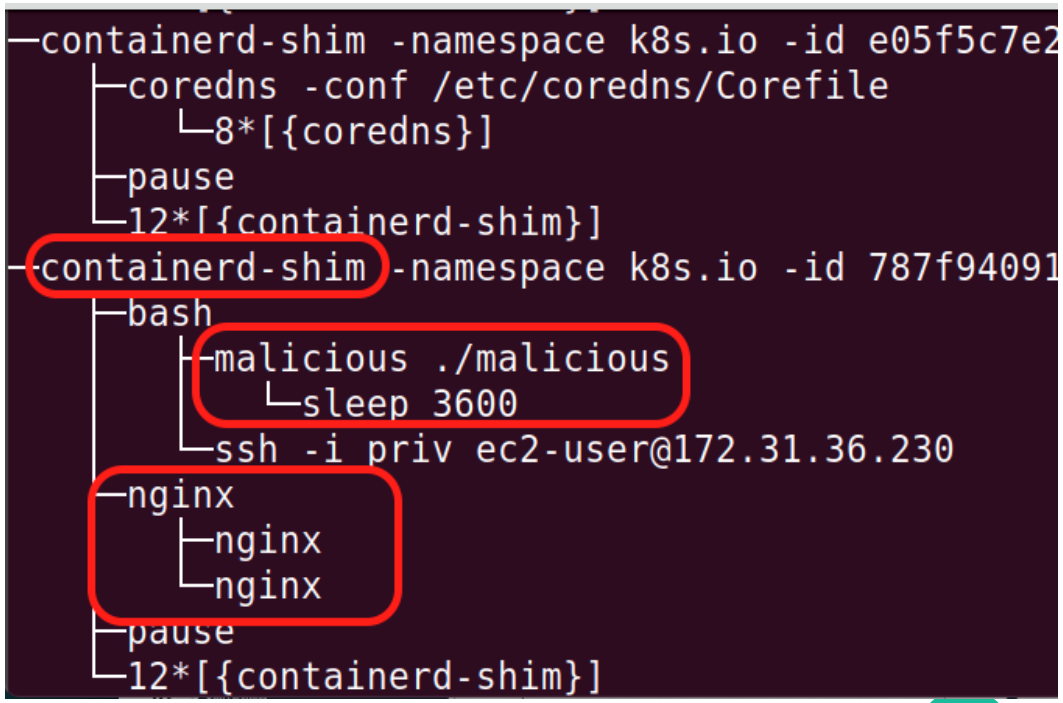


Disk Forensics: Timesketch



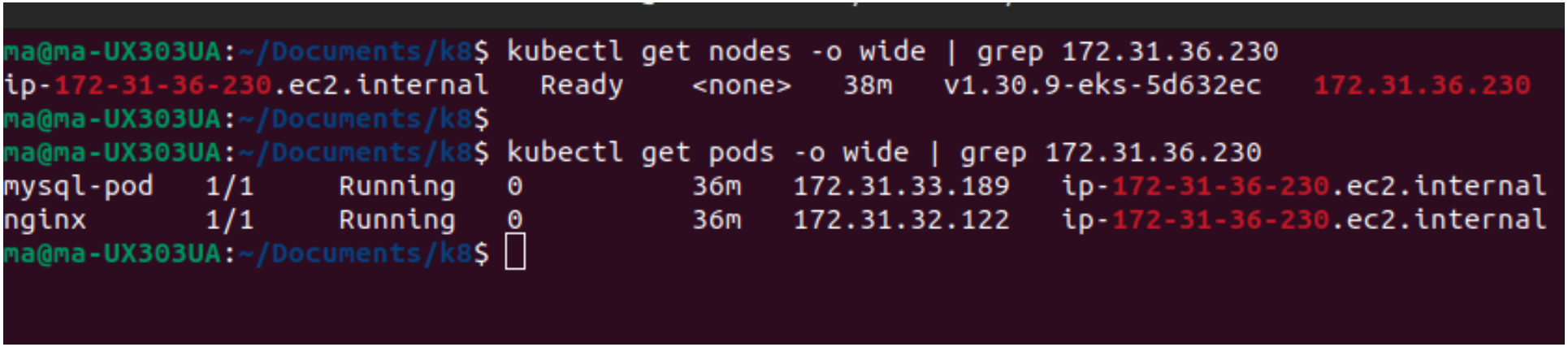
Memory Forensics

- Each pod runs as a child process of containerd -shim
- APT like attacks
  - process injection
  - rootkits
  - process dump & analysis
  - encryption keys
- Best practice:
  Collect memory from Node
- Challenge: volatility profile



Live Forensics: kubectl

- Kubectl: Tool for communicating with k8 control plane
- Possible but data collection for offline analysis is a better practice



Container Checkpointing

- Create stateful copy of a running container & restore it later in forensics lab
- Support: Kubernetes v1.25
- checkpointctl inspect <snapshot -name> –all
  - Process tree
  - Open sockets
  - Open files
  - …