# Incident Response in Kubernetes



Mahdi Alizadeh March 2025



### . 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
   Kubernetes Architecture



# **Security Challenges**





Misconfiguration/ Vulnerabilities Crypto Mining or Data Theft

#### Cryptojacking Campaign Targets Misconfigured Kubernetes Clusters

🛗 Jun 12, 2024 🛛 🛔 Ravie Lakshmanan



4

### **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

8

FS accessible from pod





Title	Severity ⊽	Finding type ▼	Resource $\nabla$	Count	Account ID  ▼	Last seen 🔻
The EC2 Instance I-0ec6681d8e97db894 queried a Bitcoin-related domain name.	High	CryptoCurrency:EC2 /BitcoinTool.BIDNS	EC2 Instance: I-0ec6681d8e97db 894	2	851725445286	19 hours ago
A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/ SuspiciousComman d	EKS Cluster: k8- demo	1	851725445286	19 hours ago
A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/ SuspiciousComman d	EKS Cluster: k8- demo	1	851725445286	19 hours ago
A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/ SuspiciousComman d	EKS Cluster: k8- demo	1	851725445286	19 hours ago
A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/ SuspiciousComman d	EKS Cluster: k8- demo	1	851725445286	19 hours ago
A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/ SuspiciousComman d	EKS Cluster: k8- demo	1	851725445286	19 hours ago
A resource of type EKSCluster has executed a suspicious command.	Low	Execution:Runtime/ SuspiciousComman d	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/ SuspiciousComman d	EC2 Instance: i-06e4ab90945267 a7a	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 guerying a domain name that is associated with Bitcoin-related activity.

X

#### Investigate with Detective

This finding is Useful Not useful

Overview					
Finding ID	2ecadf39bc20ac47a270fec50abf6146	ΘQ			
Туре	CryptoCurrency:Runtime/BitcoinTool.BIDNS	ΘQ			
Severity	HIGH	ΘQ			
Region	us-east-1				
Count	4				
Account ID	851725445286	ΘQ			
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	ΘQ			
EKS cluster details					
Name	k8-demo	ΘQ			

D	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-083638e7	c2e2887c4) 🔻
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 🖪

11

# Incident response in Kubernetes

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

# **Important Logs**

#### Control plane logs Info

Send audit and diagnostic logs from the Amazon EKS control plane to CloudWatch Logs.

#### API server

Logs pertaining to API requests to the cluster.

#### 🕽 Audit

Logs pertaining to cluster access via the Kubernetes API.

#### Authenticator

Logs pertaining to authentication requests into the cluster.

#### Controller manager

Logs pertaining to state of cluster controllers.

#### Scheduler

Logs pertaining to scheduling decisions.

- E.g., Actions on cluster (Creating new privileged Role)
- E.g., Authentication patterns (IAM/RBAC)

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

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)
  - $\circ$  Application logs: Web Server logs

### Attack Scenario: Example - Log sources



S3 Access Logs

## **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/vum.repos.d/kubernetes.repo</pre> [kubernetes] name=Kubernetes baseurl=https://pkgs.k8s.io/core:/stable:/v1.32/rpm/ enabled=1 apacheck=1 qpgkey=https://pkgs.k8s.io/core:/stable:/v1.32/rpm/repodata/repomd.xml.key EOF vum install kubectl sudo vum 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

≡ 🌗 node/pod timeline					🔹 SHARE M 🗄
Q Search		$\leftrightarrow$ $\rightarrow$ $\odot$ matrix	alicious OR authorized_keys	s OR "Accepted publickey for"	Q
( Timelines	+	A + ADD TIMELIN	NE + ADD MANUAL EVEN	SELECT ALL 🗞 UNSELECT ALL	
🛑 nginx	3 💿 🗄	onginx	3 :	node 7 E	
🔵 node	7 👁 :	C ADD TIMEFILTER			
Saved Searches	o				
🖯 Data Types	0	1- of 10 events (0.026s	;) 💽 📶 🛙	message	
🛇 Tags	0		2025-03-18T00:25:45.868Z	ip-172-31-1-188.us-west-2.compute.internal [sshd pid: 1806] Accepted publickey for ec2-user from 52.94.123.245 port 33882 ssh2: RSA SHA25	node
្ទ្រ Graphs	3		2025-03-18T00:29:03.192Z	ip-172-31-1-188.us-west-2.compute.internal [sudo pid: 16438] ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/usr/bin/r	node
Stories	+		4 days		
C Search Templates	0		2025-03-22T13:18:25.000Z	OS:/mnt/container-nginx/malicious Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o755 Number of links: 1	nginx
C Sigma Bules	т.		2025-03-22T15:00:38.320Z	OS:/mnt/container-nginx/malicious Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o755 Number of links: 1	nginx
O Sigina Rales	T		2025-03-22T15:00:41.120Z	OS:/mnt/container-nginx/malicious Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o755 Number of links: 1	nginx
Threat Intelligence	+		2025-03-22T15:01:15.408Z	OS:/mnt/forensics/home.ec2-user/.ssh/authorized_keys ype: file Owner identifier: 1000 Group identifier: 1000 Mode: 0o600 Number of links: 1	node
Analyzer Results	+		2025-03-22T15:01:21.620Z	OS:/mnt/forensics/home/ec2-user/.ssh/authorized_keys Type: file Owner identifier: 1000 Group identifier: 1000 Mode: 0o600 Number of links: 1	node
Usualizations	+	□ ☆ ₽ :	2025-03-22T15:01:21.620Z	OS:/mnt/forensics/home/ec2-user/.ssh/authorized_keys Type: file Owner identifier: 1000 Group identifier: 1000 Mode: 0o600 Number of links: 1	node
			2025-03-22T15:01:50.525Z	ip-172-31-36-230.ec2.internal [sshd pid: 5724] Accepted publickey for ec2-user from 172.31.32.122 port 42082 ssh2: RSA SHA256:V8mP6htbC	node
		□ ☆ ₽ :	2025-03-22T15:24:41.247Z	ip-172-31-36-230.ec2.internal [sshd pid: 12625] Accepted publickey for ec2-user from 172.31.32.122 port 43444 ssh2: RSA SHA256:V8mP6htb	node

# **Memory Forensics**

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



20

# Live Forensics: kubectl

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

ma@ma-UX303UA:~/Documents/k8\$ kubectl get nodes -o wide   grep 172.31.36.230 ip-172-31-36-230.ec2.internal Ready <none> 38m v1.30.9-eks-5d632ec 172</none>	.31.36.230
ma@ma-UX303UA:~/Documents/k8\$	
<pre>ma@ma-UX303UA:~/Documents/k8\$ kubectl get pods -o wide   grep 172.31.36.230</pre>	
mysql-pod 1/1 Running 0 36m 172.31.33.189 ip-172-31-36-230.eq	c2.internal
nginx 1/1 Running <u>0</u> 36m 172.31.32.122 ip-172-31-36-230.ee	c2.internal
ma@ma-UX303UA:~/Documents/k8\$	

# **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

0 ...

```
.0.0:80 -> 0.0.0.0:0 (+ 64.0 KB + 85.3 KB)
                            80 -> :::0 (+ 64.0 KB + 85.3 KB)
                 /dev/null
                  pipe[48674]
                  pipe[48675]
                    unix[49203 (49204) ]
                  pipe[48675]
                       48674
                           49206 (49205)
                        EVENTPOLL.27
                      EVENTFD.28
                 131 EVENTED.29
                          .0.0.0:80 -> 0.0.0.0:0 (+ 64.0 KB + 85.3 KB)
                        :::80 -> :::0 (+ 64.0 KB + 85.3 KB)
        [UNIX (STREAM)]
Open files
             /dev/null
              pipe[48674]
```

