SYNACKTIV

Investigation EKS InterCERT Days 2026

Noam Leipold et Théo Letailleur

2026/06/03

TLP:CLEAR

Introduction

SYNACKTIV

- **Augmentation des compromissions Kubernetes**
  - Technologie **complexe** et **abstraite**
  - Sécurité souvent secondaire face à l'usage courant

TLP:CLEAR

Tendances

Cas rencontrés

SYNACKTIV

- **AWS**, compromission d'un service de CICD (Jenkins+ArgocD) exposé sur internet
  - Persistance et vol de données
  - synacktiv.com/publications/linkpro-analyse-dun-rootkit-ebpf
- **GCP**, exploitation d'une vulnérabilité (React2Shell)
  - Installation d'un cryptominer et tentatives d'escalade de privilège

TLP:CLEAR

La RedTeam Synacktiv

Déjà mature sur ces environnements

SYNACKTIV

- **Nouvelle classe de vulnérabilité**
  - Injection de template yaml **Helm** déployé par **ArgoCD** (présentation demain au SSTIC !)

TLP:CLEAR

Investigation numérique Kubernetes

SYNACKTIV

- Le forensique Kubernetes est une discipline peu explorée
- Stratégie privilégiée : outils de supervision en amont
  - `EDR`, `Sysdig`, `Falco`, `Wiz`, etc
- Volatilité des données est un problème majeur
- Localisation des données est difficile sur de grands clusters

TLP:CLEAR

Investigation numérique Kubernetes

SYNACKTIV

En pratique, plusieurs cas de figure

1. Cluster est-il un cluster managé Azure, AWS ou GCP (ou autre) ?
2. Cluster est-il autohébergé et totalement contrôlé par l'IT ?
3. Cluster utilise-t-il des modules de sécurité (EDR) ?
4. Pod suspect a-t-il été supprimé/redémarré ?

TLP:CLEAR

SYNACKTIV

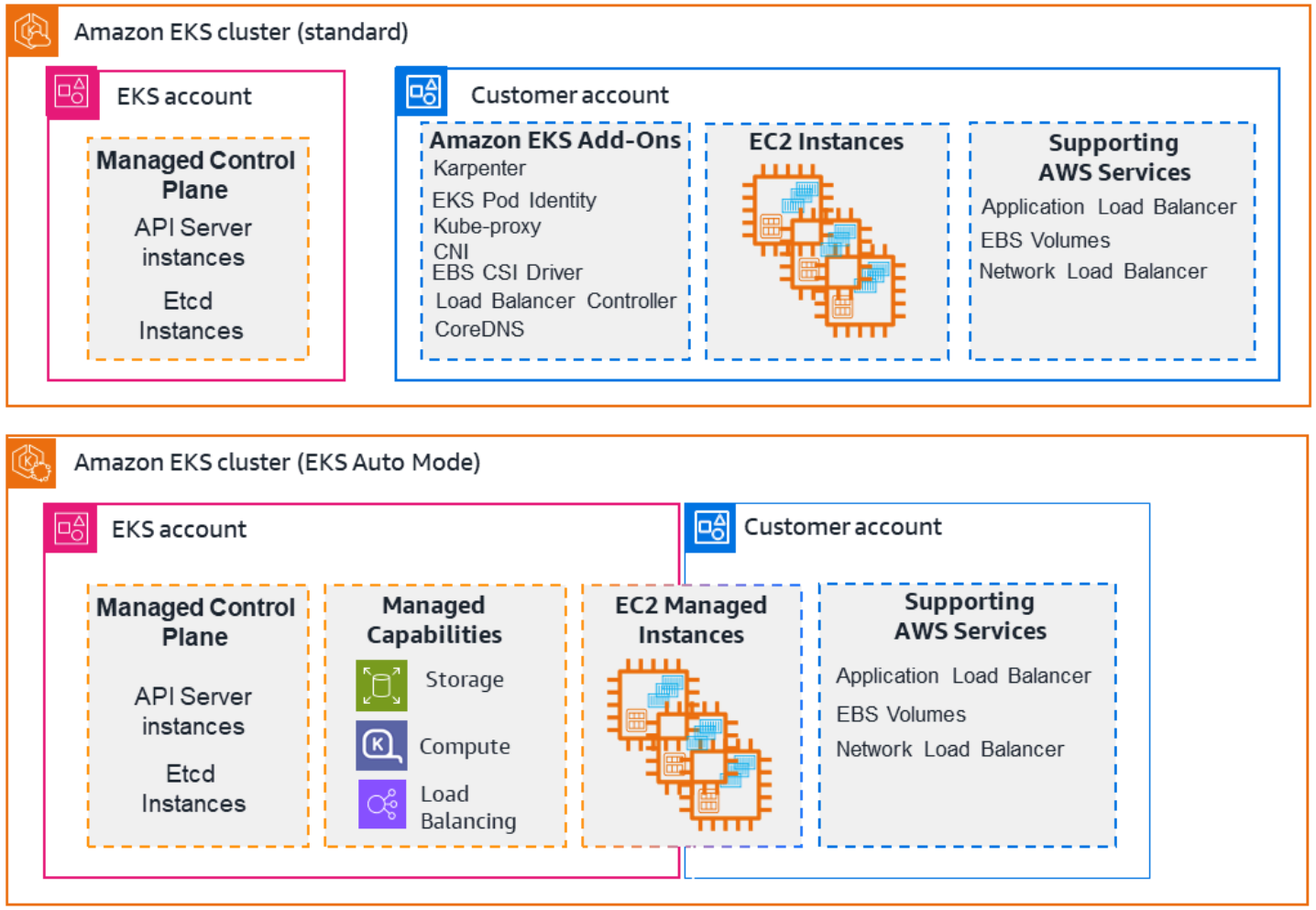
Investigation EKS

TLP:CLEAR

Investigation EKS

Amazon Elastic Kubernetes Service

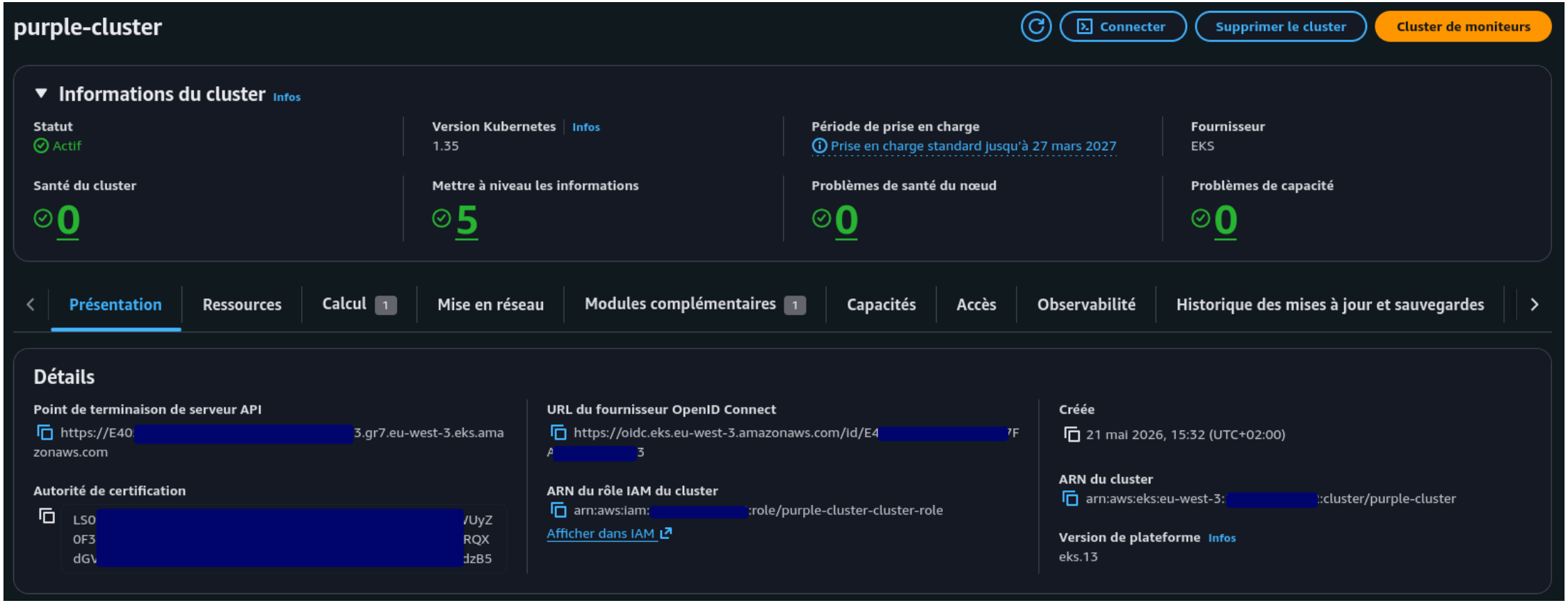
SYNACKTIV



TLP:CLEAR

Investigation EKS

SYNACKTIV

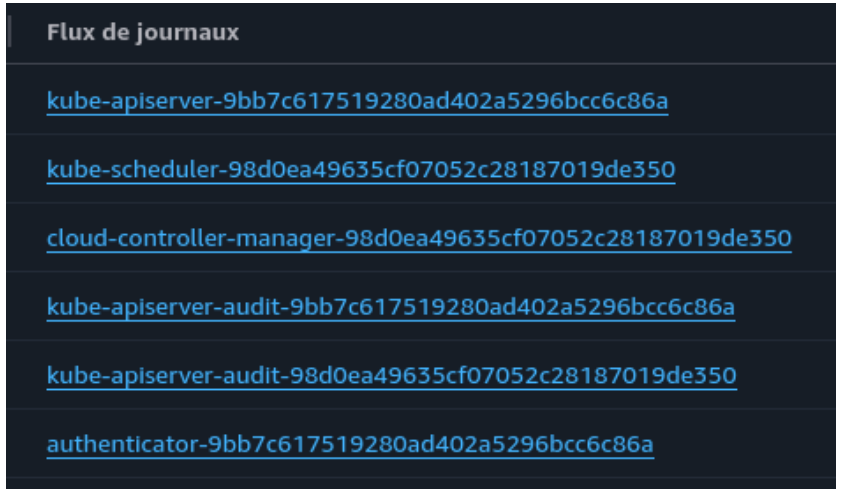


TLP:CLEAR

Investigation EKS

Journaux d'intérêts EKS

Type de log	Contenu
API Kubernetes	Interactions API serveur K8s (ex : via `kubectl`) : `create` / `update` / `patch` …
Audit Kubernetes	Événements (**très**) détaillés sur l'activité du cluster



TLP:CLEAR

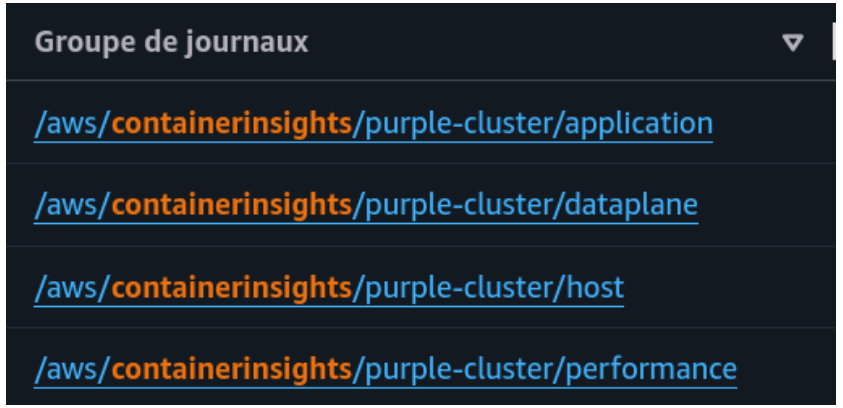
Investigation EKS

Source d'évènements Kubernetes

SYNACKTIV

- EKS plugin `amazon-cloudwatch-observability` (agents Fluentbit)
- CloudWatch : activer **Container Insights**

Type de log	Contenu
Applications	`stdout` / `stderr` des conteneurs
Host	Journaux worker : `journald`, `dmesg`
Data plane	Journaux `Kubelet`, `containerd`
Performance	Métriques système/réseau



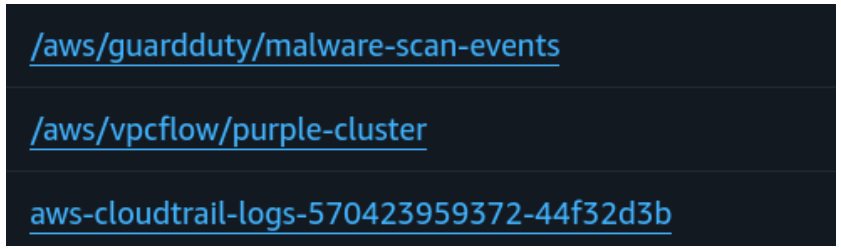
TLP:CLEAR

Investigation EKS

Source d'évènements AWS

SYNACKTIV

Source de log	Intérêt
AWS GuardDuty	Détection de la menace : **EKS Protection** et **agent runtime**
AWS CloudTrail	Surveillance de l'API AWS
VPC Flow logs	Métadonnées ECS trafic réseau VPC



- Centralisation vers **AWS CloudWatch**

Investigation EKS

GuardDuty + EKS : brique détection

SYNACKTIV

- Module **EKS Protection**
  - Analyse des logs d'**audit EKS**
- **Option :** EKS runtime monitoring
  - Syscalls workers et pods (*a la* Falco)

- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted

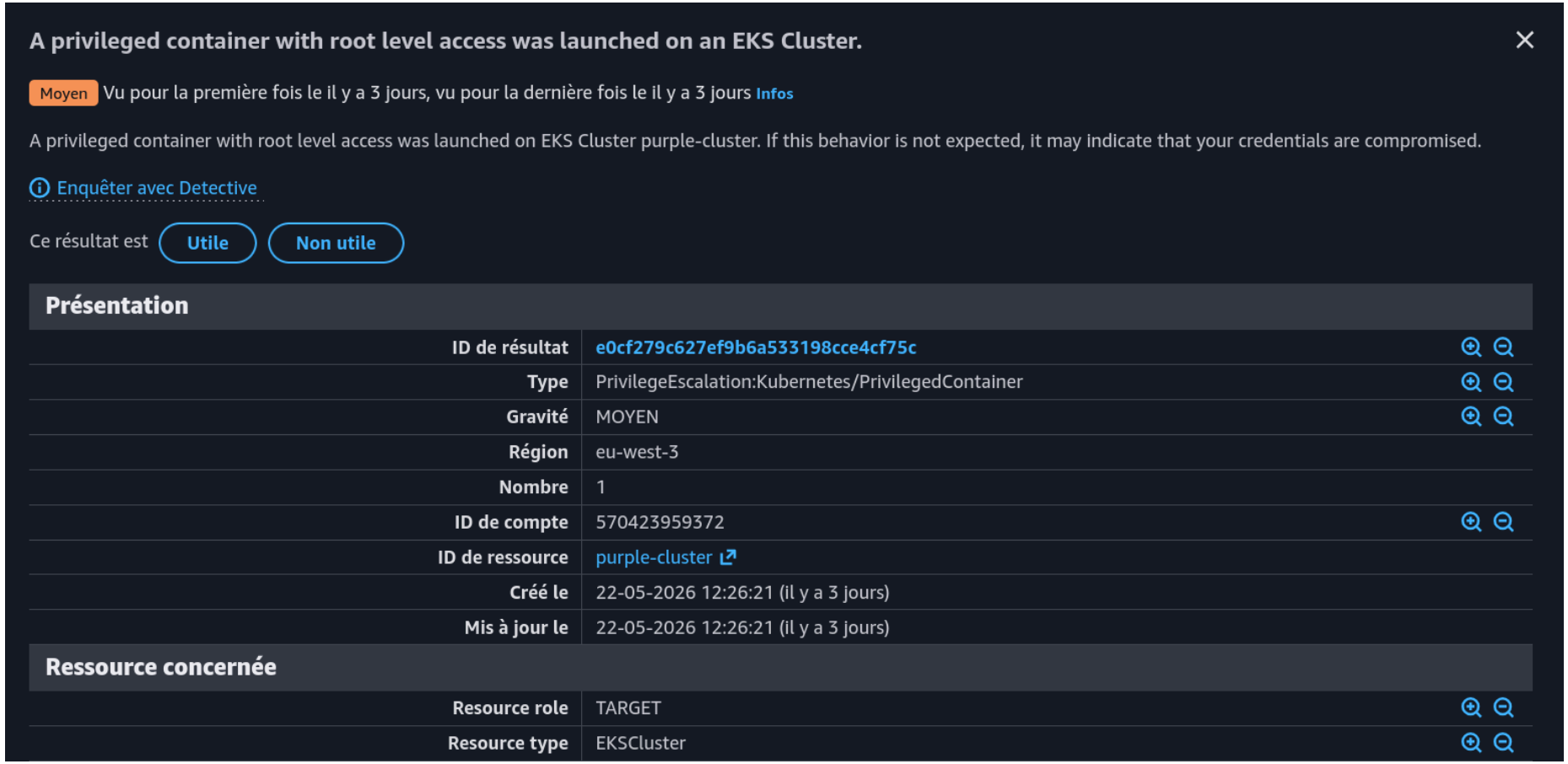
Liste des alertes existantes : https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-finding-types-eks-audit-logs.html

Investigation EKS

GuardDuty + EKS

SYNACKTIV

- `PrivilegeEscalation:Kubernetes/PrivilegedContainer` - *A privileged container with root level access was launched on an EKS Cluster.*



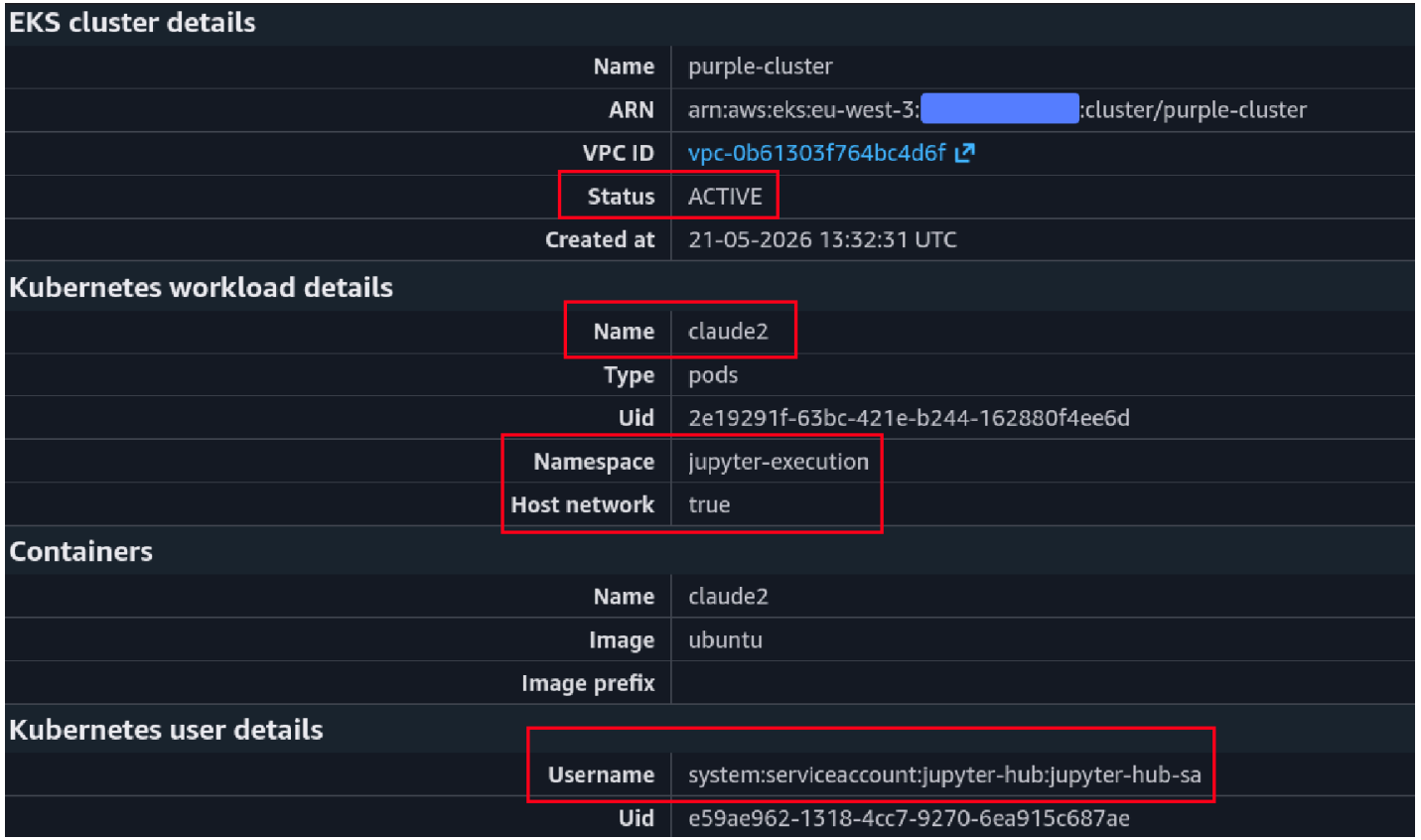
TLP:CLEAR

Investigation EKS

SYNACKTIV

GuardDuty + EKS - `PrivilegedContainer`

- Détails : pod `claude2` dans le namespace `jupyter-execution`
  - Compte de service `jupyter-hub:jupyter-hub-sa` impliqué



EKS cluster details	
Name	purple-cluster
ARN	arn:aws:eks:eu-west-3:[redacted]:cluster/purple-cluster
VPC ID	vpc-0b61303f764bc4d6f
Status	ACTIVE
Created at	21-05-2026 13:32:31 UTC
Kubernetes workload details	
Name	claude2
Type	pods
Uid	2e19291f-63bc-421e-b244-162880f4ee6d
Namespace	jupyter-execution
Host network	true
Containers	
Name	claude2
Image	ubuntu
Image prefix	
Kubernetes user details	
Username	system:serviceaccount:jupyter-hub:jupyter-hub-sa
Uid	e59ae962-1318-4cc7-9270-6ea915c687ae

TLP:CLEAR

Investigation EKS

GuardDuty + EKS - `PrivilegedContainer`

SYNACKTIV

- **Source** de l'action ?

Action	
Action type	KUBERNETES_API_CALL
Request uri	/api/v1/namespaces/jupyter-execution/pods
Verb	create
Status code	201
First seen	22-05-2026 12:26:12 (il y a 3 jours)
Last seen	22-05-2026 12:26:12 (il y a 3 jours)
Acteur	
IP address V4	51.[redacted].34
Location	
City	Paris
Country	France
Lat	48.8558
Lon	2.3494
Organization	
Asn	16509
Asn org	Amazon.com, Inc.

TLP:CLEAR

Investigation EKS

GuardDuty + EKS - `PrivilegedContainer`

SYNACKTIV

- Alerte GuardDuty en brut (json) : encore plus de détails !


```
      "KubernetesWorkloadDetails": {
        "Name": "claude2",
        "Type": "pods",
        "Uid": "2e19291f-63bc-421e-b244-162880f4ee6d",
        "Namespace": "jupyter-execution",
        "HostNetwork": true,
        "Containers": [
          {
            "Name": "claude2",
            "Image": "ubuntu",
            "ImagePrefix": "",
            "SecurityContext": {
              "Privileged": true
            }
          }
        ]
      }
    },
    "ResourceType": "EKSCluster"
  },
```


TLP:CLEAR

Investigation EKS

GuardDuty + EKS - `Persistence - HostPath`

SYNACKTIV

- `Persistence:Kubernetes/ContainerWithSensitiveMount` - *A container was launched with a sensitive host path mounted inside.*

A container was launched with a sensitive host path mounted inside.	Moyen	Persistence:Kubernetes/ ContainerWithSensitiveMount	Cluster EKS: purple-cluster

TLP:CLEAR

Investigation EKS

SYNACKTIV

- Comment le pod `claude` a-t-il été créé ?
  - Contexte utilisateur : compte de service `jupyter-hub:jupyter-hub-sa`
  - Namespace `jupyter-execution`
  - Pod privilégié
- Comportement normal :
  - notebook jupyter dans le contexte `jupyter-hub:jupyter-execution-sa`
- Recherches dans **CloudWatch Log Insights**

TLP:CLEAR

Investigation EKS

SYNACKTIV

CloudWatch : console d'investigation **Log Insights**

EKS API Audit logs

```
fields @timestamp, user.username as user, verb, objectRef.namespace as namespace,
  requestObject.spec.serviceAccountName as dest_sa, objectRef.resource as resource,
  objectRef.name as name, responseStatus.code as code, sourceIPs.0 as src_ip, userAgent
| filter user like "system:serviceaccount:jupyter-hub"
| filter user not like "scheduler"
| filter verb = "update" or verb = "patch" or verb = "create"
```

- à lire dans l'ordre chronologique inverse ci-dessous

user	verb	namespace	dest_sa	resource	name	code	src_ip	userAgent
:jupyter-hub:jupyter-execution-sa	create			selfsubjectreviews		201	51.[redacted].34	kubectl/v1.36.0 (linux/amd64)
:jupyter-hub:jupyter-execution-sa	create			selfsubjectrulesreviews		201	51.[redacted]34	kubectl/v1.36.0 (linux/amd64)
:jupyter-hub:jupyter-hub-sa	create	jupyter-hub	jupyter-execution-sa	pods	jupyter-b	201	10.64.34.…	OpenAPI-Generator/33.3.0+snap
:jupyter-hub:jupyter-hub-sa	create	jupyter-hub		persistentvolumeclaims	claim-b	201	10.64.34.…	OpenAPI-Generator/33.3.0+snap

- `selfsubjectreview` : `kubectl auth whoami`
- `selfsubjectrulesreview` : `kubectl auth can-i`

Investigation EKS

SYNACKTIV

CloudWatch : console d'investigation **Log Insights**

EKS API Audit logs

user	verb	namespace	dest_sa	resource	name	code
:jupyter-hub:jupyter-execution-sa	create	jupyter-hub	jupyter-execution-sa	pods	claude	403
:jupyter-hub:jupyter-execution-sa	create	jupyter-hub	jupyter-execution-sa	pods	claude	403
:jupyter-hub:jupyter-execution-sa	create	jupyter-hub	jupyter-execution-sa	pods	claude	403
:jupyter-hub:jupyter-execution-sa	create			selfsubjectreviews		201

- création de pod refusée : namespace protégé par PSA

responseStatus.message	pods "claude" is forbidden: violates PodSecurity "baseline:latest": hostPath volumes (volume "host-fs")
responseStatus.reason	Forbidden
responseStatus.status	Failure

```
"spec": {
  "containers": [
    {
      "args": [
        "while true; do sleep 30; done;"
      ],
      "command": [
        "/bin/bash",
        "-c",
        "--"
      ],
      "image": "ubuntu",
      "imagePullPolicy": "Always",
      "name": "claude",
      "volumeMounts": [
        {
          "mountPath": "/mnt",
          "name": "host-fs"
        }
      ]
```

PSA : https://kubernetes.io/docs/concepts/security/pod-security-admission/

TLP:CLEAR

Investigation EKS

CloudWatch : console d'investigation **Log Insights**

EKS API Audit logs

- **Mouvement latéral** vers un nouveau

  `ServiceAccount`

user	verb	namespace	dest_sa	resource	name	code
:jupyter-hub:jupyter-hub-sa	create			selfsubjectrulesreviews		201
:jupyter-hub:jupyter-hub-sa	create			selfsubjectrulesreviews		201
:jupyter-hub:jupyter-hub-sa	create			selfsubjectreviews		201
:jupyter-hub:jupyter-execution-sa	create	jupyter-hub	jupyter-hub-sa	pods	claude	201
:jupyter-hub:jupyter-execution-sa	create	jupyter-hub	jupyter-hub-sa	pods	claude	201
:jupyter-hub:jupyter-execution-sa	create	jupyter-hub	jupyter-execution-sa	pods	claude	403

- `jupyter-execution-sa` → `jupyter-hub-sa`
  - création d'un pod en tant que `jupyter-hub-sa`
  - récupération du token Kubernetes du SA

TLP:CLEAR

Investigation EKS

SYNACKTIV

- GuardDuty : `Execution:Runtime/ReverseShell`

A reverse shell was detected in EC2 instance i-09313d26e5614eebb.

Elevé Vu pour la première fois le il y a 6 jours, vu pour la dernière fois le il y a 2 jours Infos

The process bash in EC2 instance i-09313d26e5614eebb has created a reverse shell.

Action	
Action type	NETWORK_CONNECTION
Connection direction	UNKNOWN
Protocol	
Blocked	false
Local IP V4	10.64.40.195
Port name	Unknown
First seen	22-05-2026 11:34:02 (il y a 6 jours)
Last seen	26-05-2026 15:10:15 (il y a 2 jours)
IP address V4	51.[redacted].34
Port	4448
Détails de l'exécution	
Process	
Nom	bash
Chemin d'exécution	/usr/bin/bash
SHA-256 exécutable	3efccc187bafa75ff1e37d246270ab3e7aa559f242c7a52bf3ec2a1b5450bdbd
ID de processus d'espace de noms	3897839
Répertoire de travail actuel	/
ID de processus	3897839
Heure de début	26-05-2026 13:10:15 UTC

Investigation EKS

SYNACKTIV

CloudWatch : console d'investigation **Log Insights**

EKS API Audit logs

- Déplacement dans un namespace sans PSA

user	verb	namespace	dest_sa	resource	subresource	name	code
t:jupyter-hub:jupyter-hub-sa	create	jupyter-execution		pods	exec	claude2	101
t:jupyter-hub:jupyter-hub-sa	create	jupyter-execution	jupyter-execution-sa	pods		claude2	201
t:jupyter-hub:jupyter-hub-sa	patch	jupyter-execution		roles		hub	200

- `/patch/roles/hub`
  - modification de ses droits sur le namespace
- `/create/pods/exec`
  - commandes interactive (shell) dans le pod

```
spec": {
 "containers": [
   {
     "args": [
       "while true; do sleep 30; done;"
     ],
     "command": [
       "/bin/bash",
       "-c",
       "--"
     ],
     "image": "ubuntu",
     "imagePullPolicy": "Always",
     "name": "claude2",
     "securityContext": {
       "privileged": true
     },
     "volumeMounts": [
       {
         "mountPath": "/mnt",
         "name": "host-fs"
       }
     ]
   }
 ],
 "hostIPC": true,
 "hostNetwork": true,
 "hostPID": true,
```

TLP:CLEAR

Investigation EKS

Role hub

SYNACKTIV

- **Prérequis d'investigation :** avoir un compte admin EKS
- `kubectl get role hub -oyaml -n jupyter-execution`

```
kind: Role
metadata:
  labels:
    app: jupyterhub
  name: hub
  namespace: jupyter-execution
rules:
[...]
- apiGroups:
  - rbac.authorization.k8s.io
  resources:
  - roles
  verbs:
  - escalate
```

- **Vulnérabilité :** le mot-clé `escalate` sur `roles` permet à l'utilisateur de **s'attribuer de nouveaux droits** sur le namespace

TLP:CLEAR

Investigation EKS

Role hub

SYNACKTIV

```
[...]
- apiGroups:
  - ""
  resources:
  - pods/exec
  verbs:
  - create
```

- Ajout de `create` sur `pods/exec`
- `kubectl exec -it claude2 -n jupyter-execution -- /bin/bash`
  - accès au FS du noeud worker depuis un shell distant !

TLP:CLEAR

Investigation EKS

SYNACKTIV

CloudWatch : console d'investigation **Log Insights**

- **Fast-forward :** on remonte la piste jusqu'au service **ArgoCD** avec un pod suspect dans le namespace `dev-myapp`
  - CICD exposée derrière un LB `traefik` : **Container Insights** !

```
fields @timestamp, @entity.Attributes.K8s.Namespace as namespace, log_processed.ClientHost as src_ip,
  log_processed.RequestAddr as domain, log_processed.RequestPath as uri, log_processed.DownstreamStatus as status
| filter namespace in ["traefik"]
| filter domain = "argocd.internal.purple.com"
| filter uri = "/api/v1/applications/dev-myapp/sync"
```

@timestamp	namespace	src_ip	domain	uri	status
2026-05-22T10:10:19.83…	traefik	10.64.27.17	argocd.internal.purple.com	/api/v1/applications/dev-myapp/sync	200
2026-05-22T09:54:32.14…	traefik	10.64.27.17	argocd.internal.purple.com	/api/v1/applications/dev-myapp/sync	200

- `10.64.27.17` : adresse IP d'un EC2 interne mais hors cluster EKS…

Investigation EKS

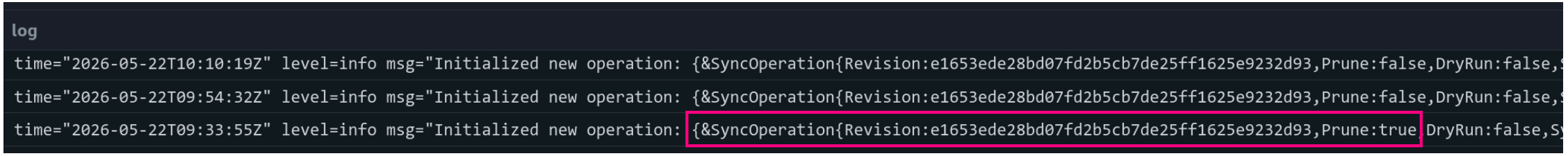
SYNACKTIV

CloudWatch : console d'investigation **Log Insights**

Container Insights

- **Journaux ArgoCD :** recherche d'info sur le `sync` du projet `dev-myapp`

```
fields @timestamp, log
| filter @entity.Attributes.K8s.Namespace in ["argo"]
| filter @entity.Attributes.K8s.Workload in ["argocd-application-controller"]
| filter log like "Initialized new operation" and log like "dev-myapp"
| sort @timestamp desc
```

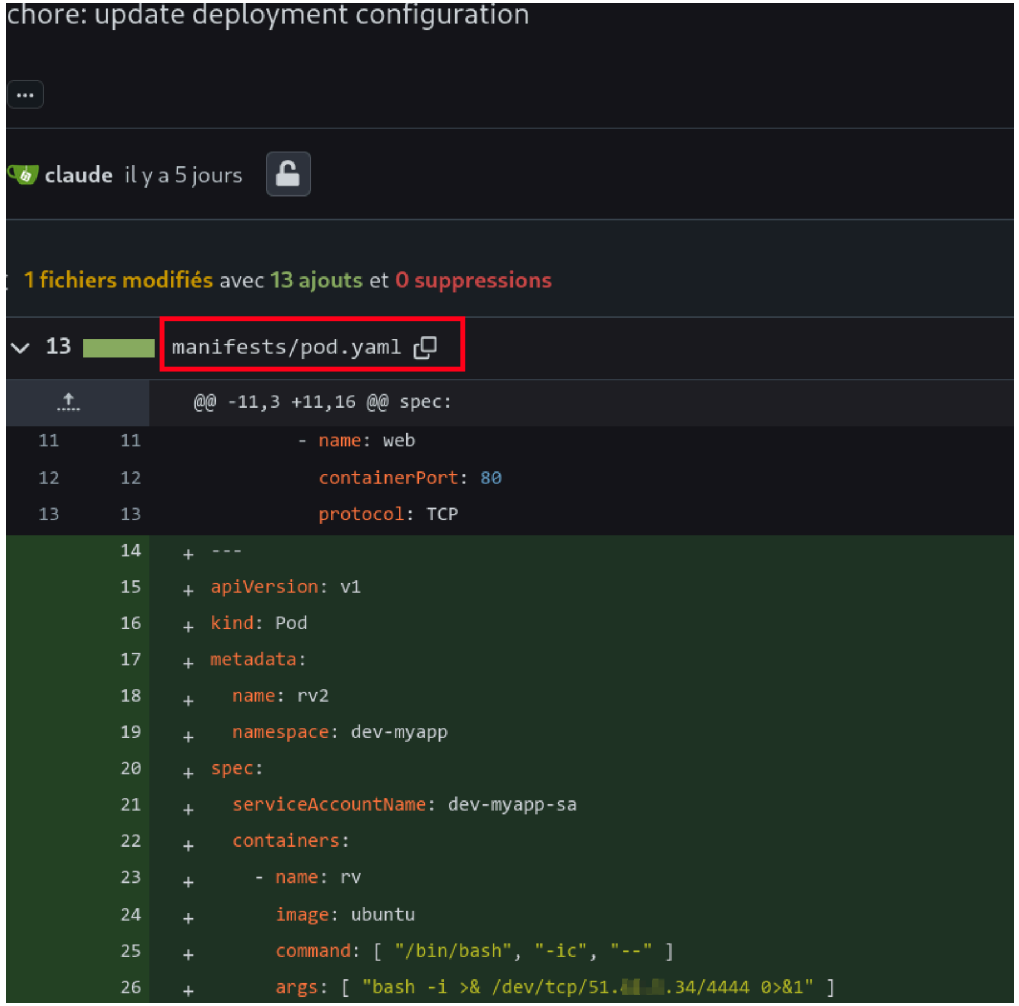


- hash de commit : `e1653ede28bd07fd2b5cb7de25ff1625e9232d93`

TLP:CLEAR

Investigation EKS

Le Graal



TLP:CLEAR

Investigation EKS

CloudTrail

SYNACKTIV

- Les **noeuds** et certains **pods** ont besoin d'une identité AWS.
- Surveillance du **cluster EKS** et de ses **workers EC2** en tant que **ressource cloud**
- `eks.amazonaws.com` : interaction des **administrateurs/services AWS** avec le cluster

- Exemple : Accès d'un **utilisateur AWS** à l'API du **Cluster EKS**


```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "A[redacted]:TheoLetailleur",
    "arn": "arn:aws:sts::[redacted]:assumed-role/AWSReservedSSO_AdministratorAccess_[redacted]/TheoLetailleur",
    "accountId": "[redacted]",
    "accessKeyId": "ASI[redacted]SFR",
```

```
"eventTime": "2026-05-22T10:47:18Z",
"eventSource": "eks.amazonaws.com",
"eventName": "ListNodegroups",
"awsRegion": "eu-west-3",
"sourceIPAddress": "1[redacted].102",
"userAgent": "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0",
"requestParameters": {
    "name": "purple-cluster"
},
```


TLP:CLEAR

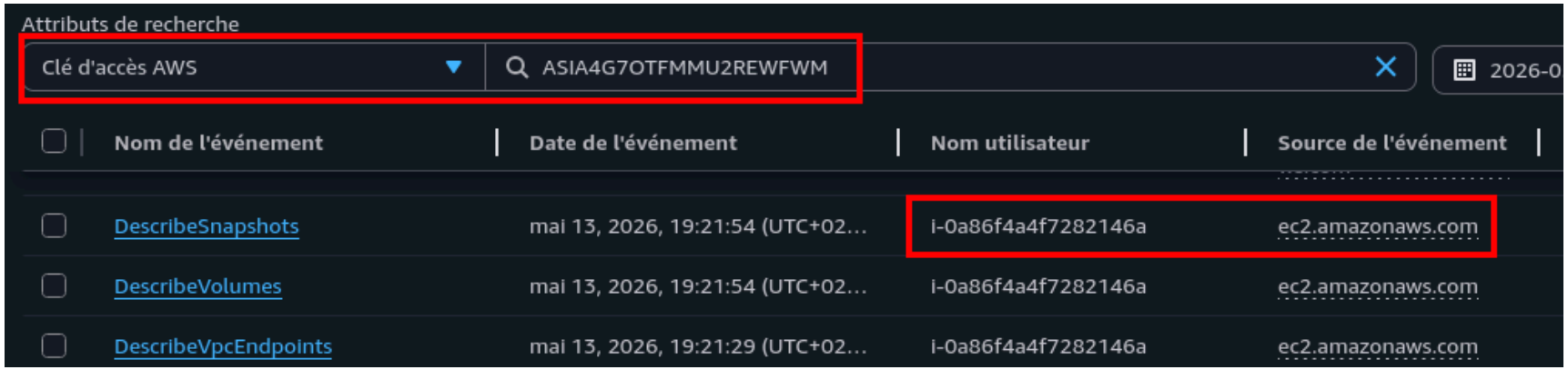
Investigation EKS

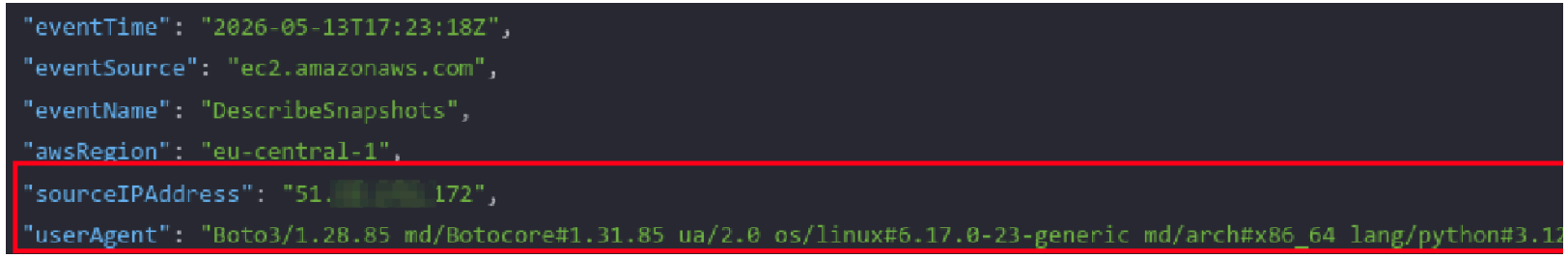
SYNACKTIV

CloudTrail

- Détecté par GuardDuty : `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`

  - *Credentials for instance role **purple-cluster-node-role** were used from an external IP address.*





- Nombreuses requêtes sur différents endpoints == découverte des ressources cloud accessibles

SYNACKTIV

Synthèse

TLP:CLEAR

Synthèse

MITRE ATT&CK Kubernetes

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access Kubernetes API server	Access cloud resources	Images from a private registry	Data destruction
Compromised image In registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Collecting data from pod	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from proxy server	Application credentials in configuration files	Exposed sensitive interfaces	Application credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container	Container service account			Access managed identity credentials	Instance Metadata API	Writable hostPath mount		
	Sidecar injection	Static pods			Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and iP spoofing		

Matrice MITRE Kubernetes par Microsoft : https://microsoft.github.io/Threat-Matrix-for-Kubernetes/

TLP:CLEAR

Synthèse

SYNACKTIV

1. **Préparer** : Activer la rétention des logs et l'Audit API avant l'incident, PSA et permissions boundary
2. **Contenir** : isolation réseau, container checkpointing
3. **Extraire** : Adapter les collecteurs forensiques classiques : source de logs, kubectl

TLP:CLEAR

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://x.com/synacktiv

https://bsky.app/profile/synacktiv.com

https://synacktiv.com