Simulate a Live Attack for Kubernetes (lite)

The Wiz Runtime Sensor collects runtime events on Kubernetes workloads and translates them to detections.

Below are a set of commands that can be run on most environments to help you quickly test the Runtime Sensor detections. These commands do not require the deployment of a custom container image.

> This scenario uses non-malicious commands for the simulation and should be safe to execute in your environment. Some of these commands will make changes to the container in which they are run, so we recommend using a dedicated target container in test or demo environments only.

Step 1: Deploy the Runtime Sensor evaluation pod

Step 2: Run attack-simulation commands

Step 3: Clean-up (remove the Runtime Sensor evaluation pod)

Prerequisites

- Kubernetes version 1.20 or higher, where the Runtime Sensor was successfully deployed on a cluster.
- Access credentials with permissions to deploy a pod and execute commands on it.
- Access to the Kubernetes cluster API from your machine with the ability to run `kubectl` commands.
- A local installation of `kubectl`.
- Wiz Sensor installed on the Kubernetes cluster.

Deploy the Runtime Sensor evaluation pod

1. Download the wiz-privileged-demo-pod.yaml file.
2. Deploy the target pod on your Kubernetes cluster:

```
kubectl apply -f wiz-privileged-demo-pod.yaml
```

3. Initiate an interactive shell with the pod:

```
kubectl exec -it wiz-demo-pod -- bash
```

Run attack-simulation commands

In this step, you will run a series of commands on the target pod via the shell you just created and review the events generated by the Runtime Sensor. The Runtime Sensor detections are represented under the Explorer > Cloud Events page in your Wiz portal.

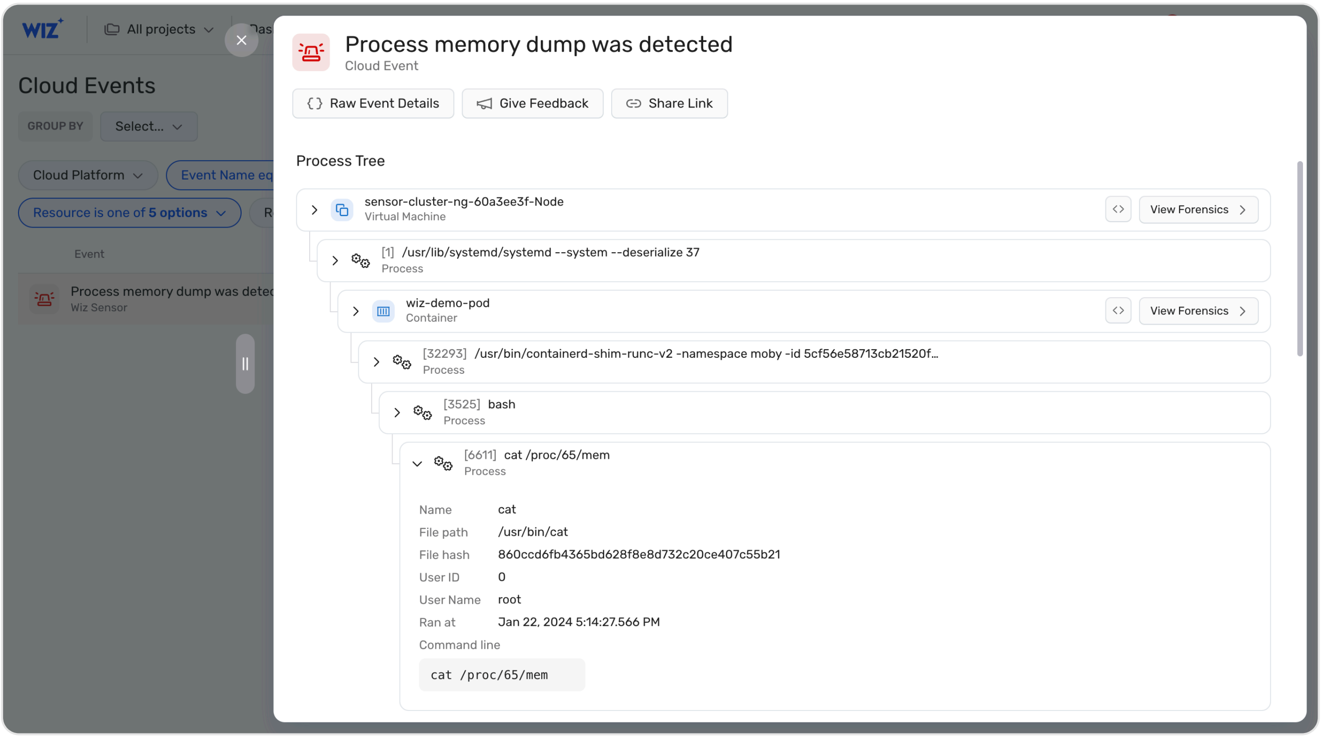
Suspicious access to process memory

Command to execute

Execute the following command: */usr/bin/cat /proc/$/mem 2> /dev/null*

Expected detection(s) in Wiz

- Process memory dump was detected (T1003.007 OS Credential Dumping: Proc Filesystem)



Process memory dump was detected
Cloud Event

Process Tree

sensor-cluster-ng-60a3ee3f-Node
Virtual Machine

[1] /usr/lib/systemd/systemd --system --deserialize 37
Process

wiz-demo-pod
Container

[32293] /usr/bin/containerd-shim-runc-v2 -namespace moby -id 5cf56e58713cb21520f...
Process

[3525] bash
Process

[6611] cat /proc/65/mem
Process

Name	cat
File path	/usr/bin/cat
File hash	860ccd6fb4365bd628f8e8d732c20ce407c55b21
User ID	0
User Name	root
Ran at	Jan 22, 2024 5:14:27.566 PM

Command line

```
cat /proc/65/mem
```

- Process memory data file was accessed (T1003.007 OS Credential Dumping: Proc Filesystem)

English ▲

Dropper detection

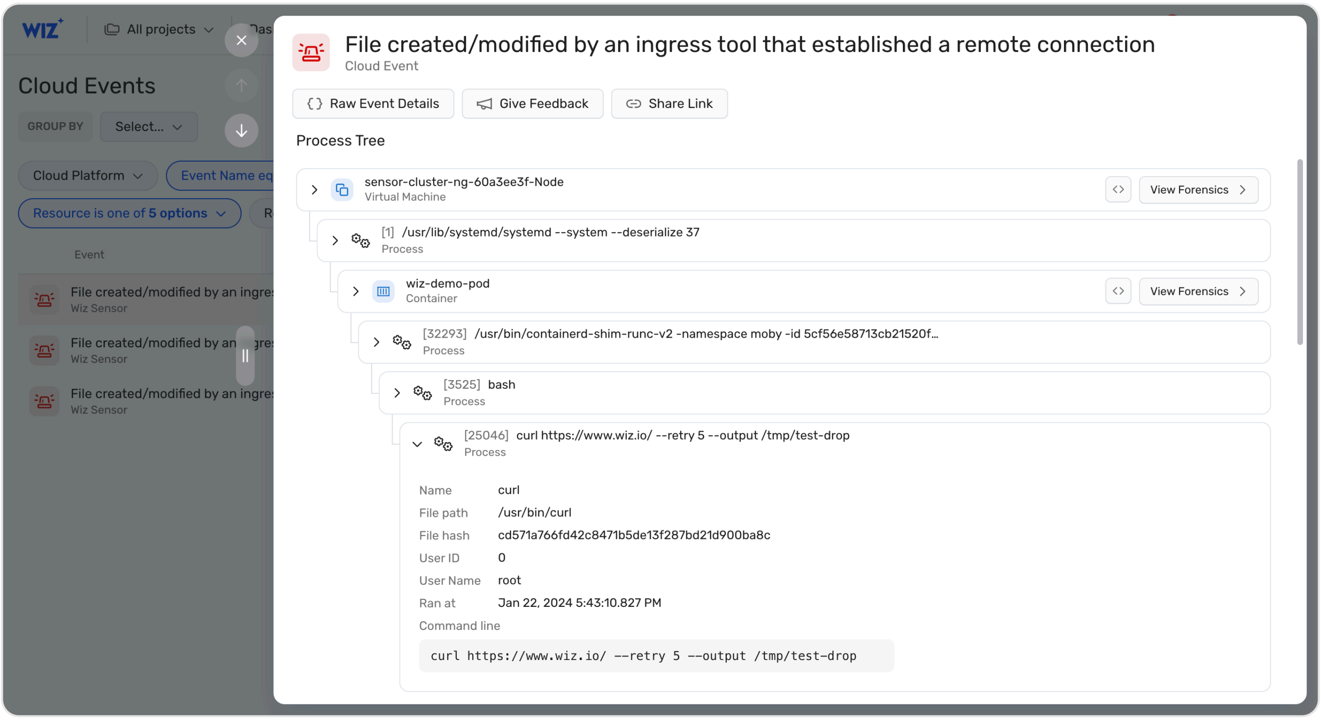
Command to execute

Execute the following command:

```
/usr/bin/curl https://www.wiz.io/ --retry 5 --output /tmp/test-drop &&
/usr/bin/chmod +x /tmp/test-drop
```

Expected detection(s) in Wiz

- Suspected drop and execute–ingress tool with payload decode or file/folder permission change commands were executed (T1222.002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification)
- File created/modified by an ingress tool that established a remote connection (T1105 Ingress Tool Transfer)



File created/modified by an ingress tool that established a remote connection
Cloud Event

Process Tree

sensor-cluster-ng-60a3ee3f-Node
Virtual Machine

[1] /usr/lib/systemd/systemd --system --deserialize 37
Process

wiz-demo-pod
Container

[32293] /usr/bin/containerd-shim-runc-v2 -namespace moby -id 5cf56e58713cb21520f...
Process

[3525] bash
Process

[25046] curl https://www.wiz.io/ --retry 5 --output /tmp/test-drop
Process

Name	curl
File path	/usr/bin/curl
File hash	cd571a766fd42c8471b5de13f287bd21d900ba8c
User ID	0
User Name	root
Ran at	Jan 22, 2024 5:43:10.827 PM

Command line

```
curl https://www.wiz.io/ --retry 5 --output /tmp/test-drop
```

- Ingress tool was executed (T1105 Ingress Tool Transfer)

Evasion via hidden files

Command to execute

```
/usr/bin/mkdir -p /tmp/.testdir && cp /usr/bin/whoami /tmp/.testdir/test &&
/usr/bin/chmod +x /tmp/.testdir/test && /tmp/.testdir/test
```

Expected detection(s) in Wiz

English ▲

- Process was executed from hidden location (T1564.001 Hide Artifacts: Hidden Files and Directories)
- Hidden directory was created (T1564.001 Hide Artifacts: Hidden Files and Directories)

Possible credential manipulation

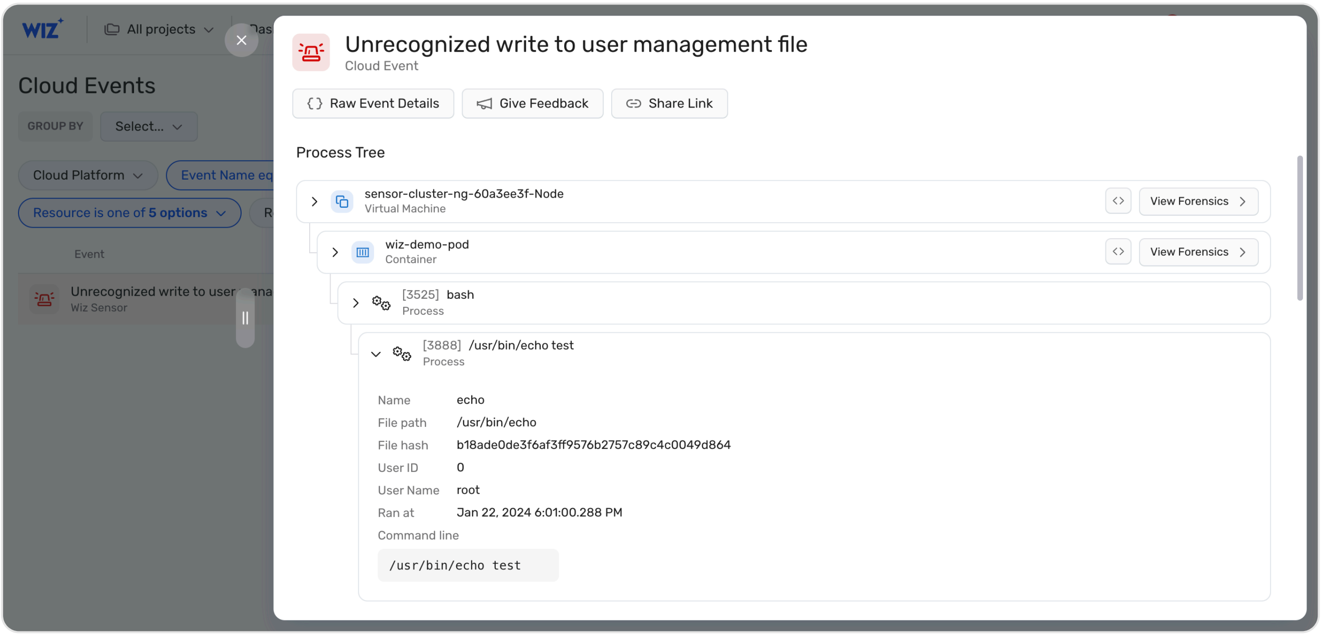
Command to execute

Execute the following command:

```
/usr/bin/echo test  >> /etc/shadow
```

Expected detection(s) in Wiz

- Unrecognized write to user management file (T1078.003 Valid Accounts: Local Accounts)



Unrecognized write to user management file
Cloud Event

Process Tree

sensor-cluster-ng-60a3ee3f-Node
Virtual Machine

wiz-demo-pod
Container

[3525] bash
Process

[3888] /usr/bin/echo test
Process

Name echo
File path /usr/bin/echo
File hash b18ade0de3f6af3ff9576b2757c89c4c0049d864
User ID 0
User Name root
Ran at Jan 22, 2024 6:01:00.288 PM
Command line

```
/usr/bin/echo test
```

Evasion via renamed binaries (living-off-the-land variant)

Command to execute

Execute the following command:

```
ls -1 /bin/*sh | grep -v \\.sh | xargs -I {} /usr/bin/cp -f {} {}.lotl
```

Expected detection(s) in Wiz

- File created or modified in bin folder (T1554 Compromise Client Software Binary)

Possible container escape via mount with cgroups

Command to execute

Execute the following command:

```
/usr/bin/mkdir -p /tmp/test && /usr/bin/mount -t cgroup /tmp/test 2>/dev/null
```

Expected detection(s) in Wiz

- Mount with type cgroup was executed inside a container (T1611 Escape to Host)

Hijack Execution Flow: Dynamic Linker Hijacking

Command to execute

```
/usr/bin/touch /etc/ld.so.preload && /usr/bin/echo test >> /etc/ld.so.preload
```

Expected detection(s) in Wiz

- Library preload configuration file was added/modified (T1574.006 Hijack Execution Flow: Dynamic Linker Hijacking)

Clean up (remove the Runtime Sensor evaluation pod)

To remove the pod, run:

```
kubectl delete -f wiz-privileged-demo-pod.yaml
```

Updated 3 months ago

← Attack Simulations for Runtime Sensors

Simulate a Live Attack for Kubernetes →

English ▲