aqua

Aqua Warden

The Automated Runtime Security Control Testing Tool

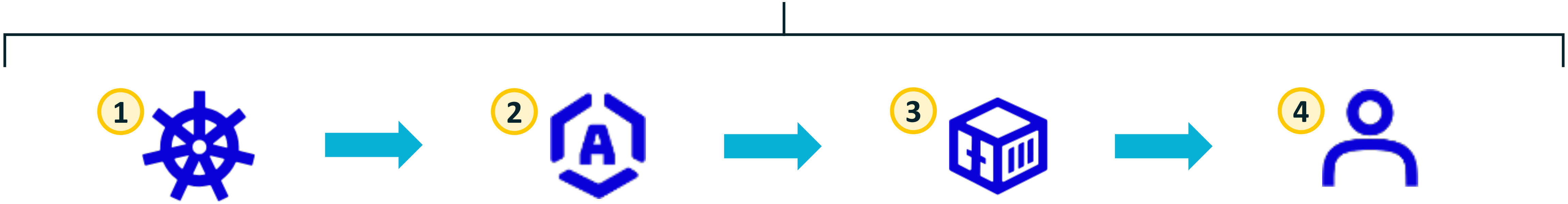
Introduction

aqua

What is Aqua Warden?

Aqua Warden

A tool written completely in bash to run in any Linux/Mac that is connected to a K8s cluster with Aqua Enforcer deployed



1. Detects if it is connected to a **K8s cluster**

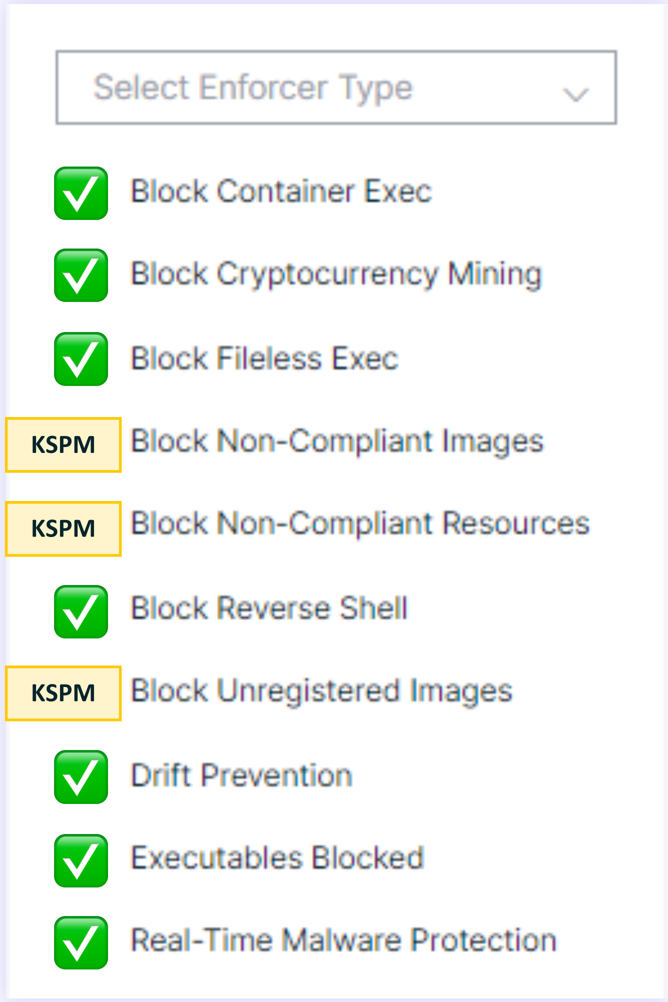
2. Detects if **Aqua Enforcer** is deployed in the K8s cluster

3. Deploys **Aqua Test Container**

4. Enables user to follow the guided options to **execute Aqua Runtime Security test cases**

Supported Container Runtime Security Controls (Custom Policies)

1. **Real-time Malware Protection [Delete action]**
2. **Block Container Exec**
3. **Block Cryptocurrency Mining**
4. **Block Fileless Execution**
5. **Block Reverse Shell**
6. **Drift Prevention**
7. **Executables Blocked [ps]**



Select Enforcer Type

✓ Block Container Exec

✓ Block Cryptocurrency Mining

✓ Block Fileless Exec

KSPM Block Non-Compliant Images

KSPM Block Non-Compliant Resources

✓ Block Reverse Shell

KSPM Block Unregistered Images

✓ Drift Prevention

✓ Executables Blocked

✓ Real-Time Malware Protection

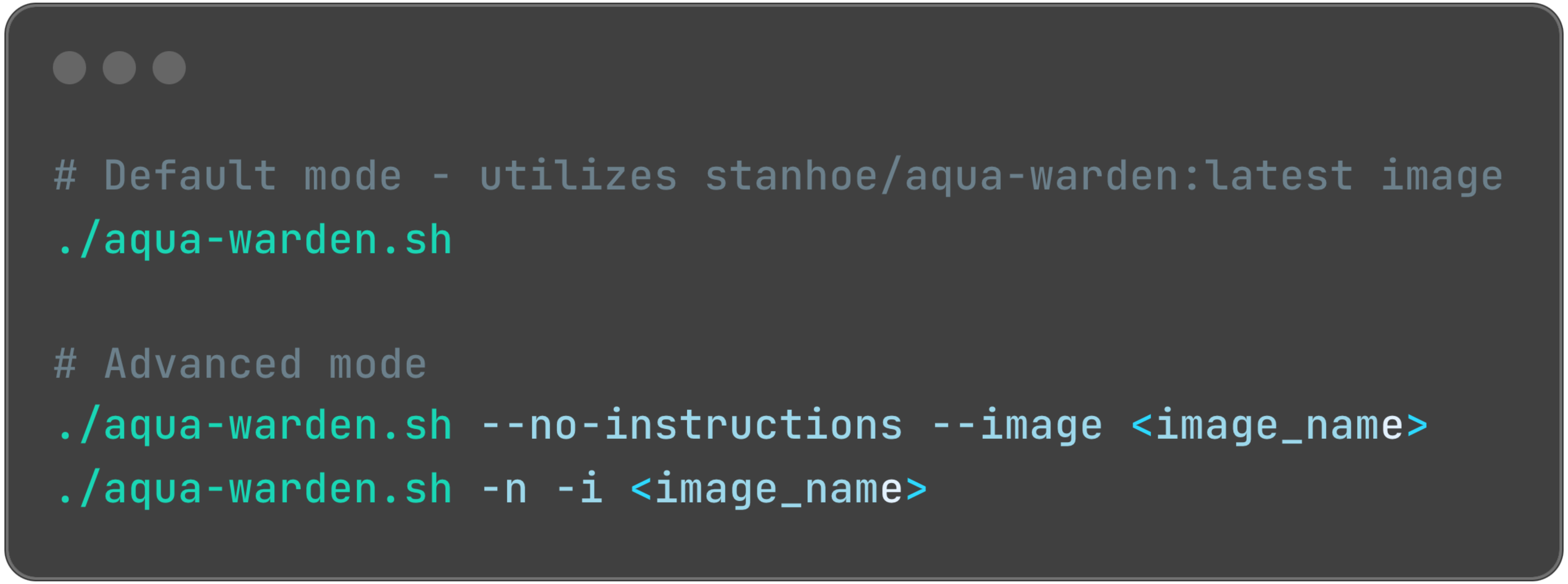
Usage

Requirements

- Bash shell
- kubectl configured to connect to a Kubernetes cluster
- Aqua Enforcer daemonset deployed in the Kubernetes cluster
- Internet access to docker registry or push aqua-warden test image (stanhoe/aqua-warden:latest) to local registry
- Permissions to deploy container in the Kubernetes cluster (stanhoe/aqua-warden:latest)

Running Aqua-Warden

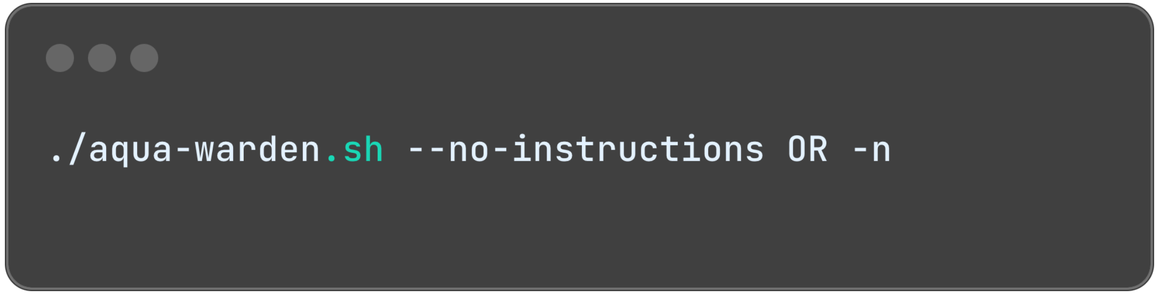
- **Standard bash script execution in Linux/Mac terminal**



```
# Default mode - utilizes stanhoe/aqua-warden:latest image
./aqua-warden.sh

# Advanced mode
./aqua-warden.sh --no-instructions --image <image_name>
./aqua-warden.sh -n -i <image_name>
```

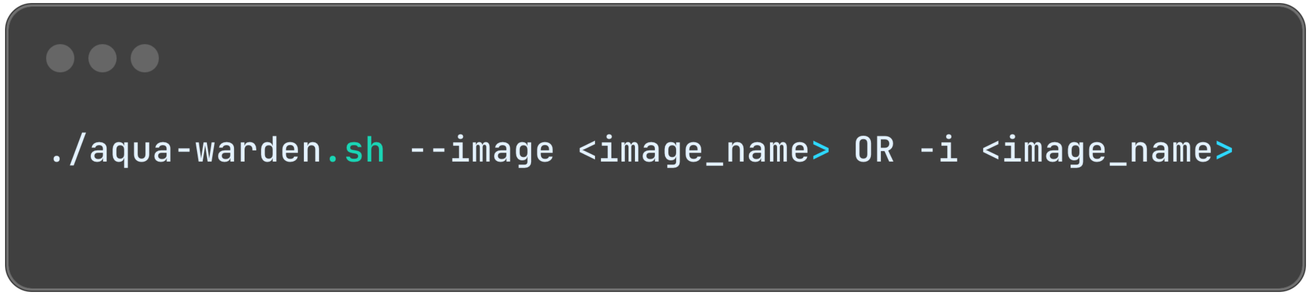
Additional Commands (Advanced Mode)

- Skip test prerequisites instructions



```
./aqua-warden.sh --no-instructions OR -n
```

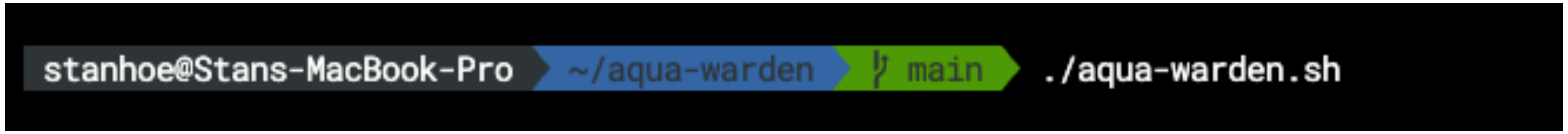
- Reference local registry image for the aqua-warden test container (e.g. Air-gapped env)



```
./aqua-warden.sh --image <image_name> OR -i <image_name>
```

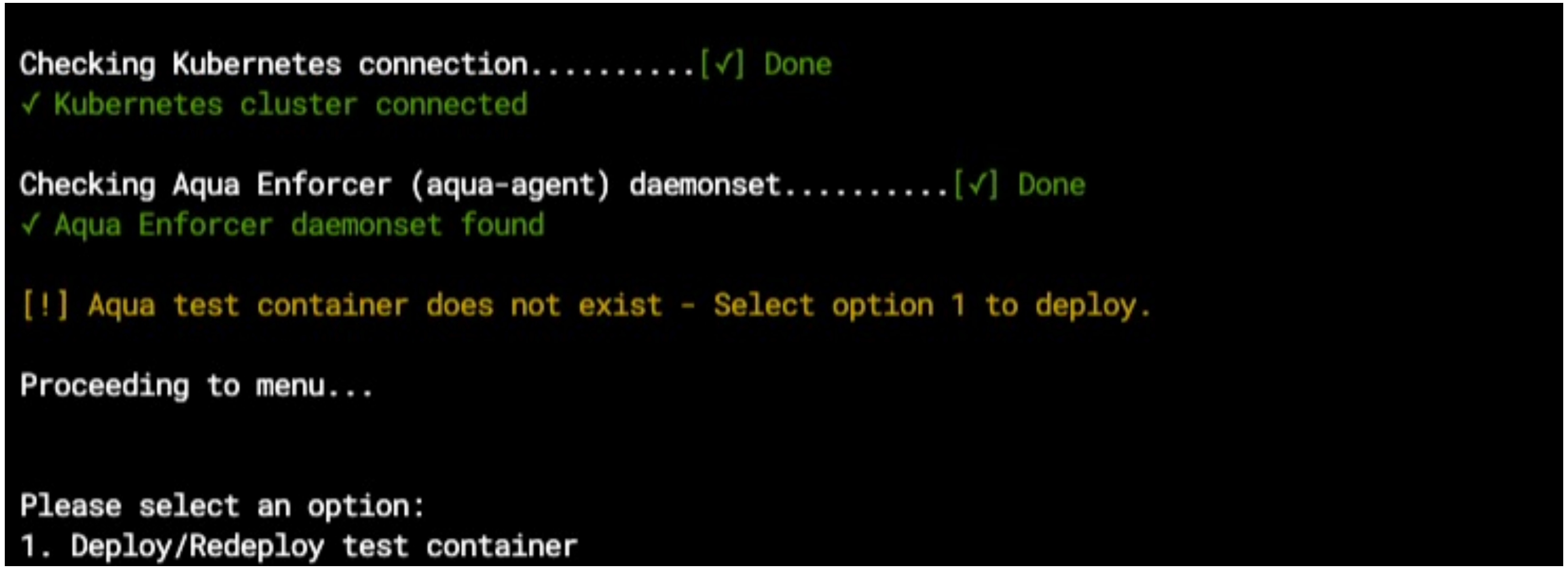
Step-by-step Guide

1. **Run Aqua Warden**



```
stanhoe@Stans-MacBook-Pro  ~/aqua-warden   main  ./aqua-warden.sh
```

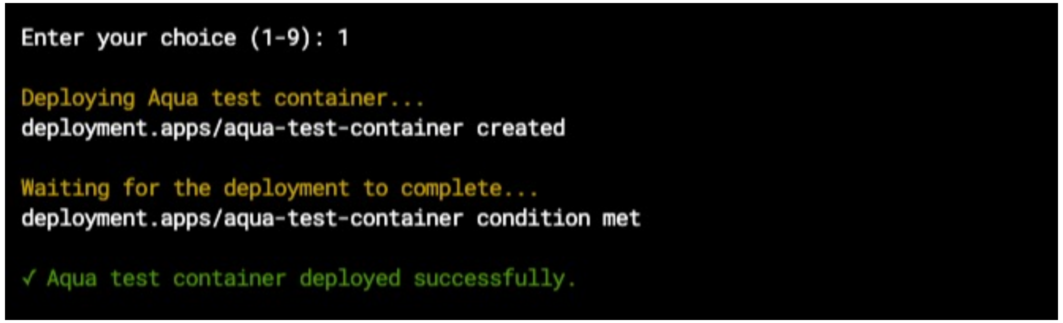
2. **Kubernetes cluster and Aqua Enforcers are detected**



```
Checking Kubernetes connection..........[✓] Done
✓ Kubernetes cluster connected

Checking Aqua Enforcer (aqua-agent) daemonset.........[✓] Done
✓ Aqua Enforcer daemonset found

[!] Aqua test container does not exist - Select option 1 to deploy.

Proceeding to menu...


Please select an option:
1. Deploy/Redeploy test container
```

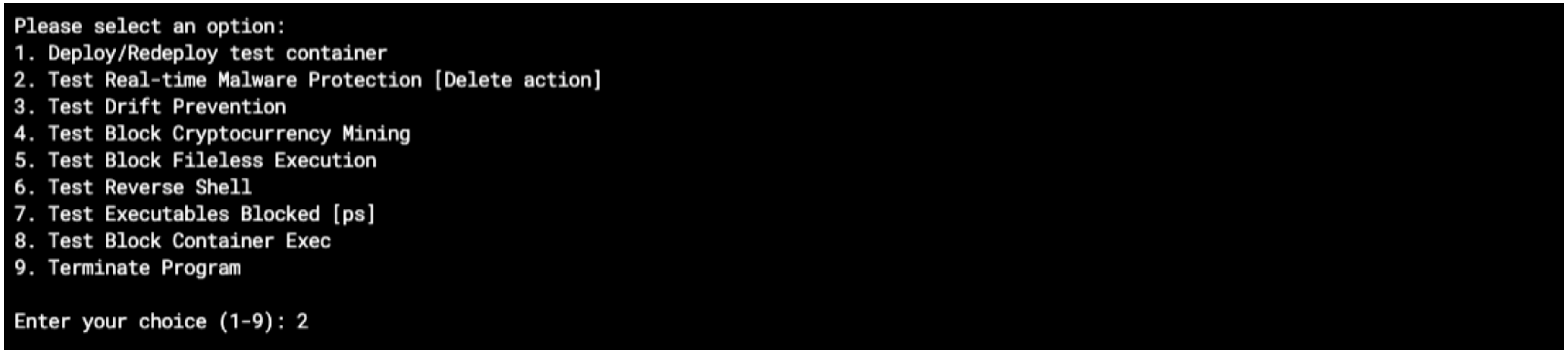
Step-by-step Guide

3. Deploy Test Container (Enter option 1 in the terminal)



```
Enter your choice (1-9): 1

Deploying Aqua test container...
deployment.apps/aqua-test-container created

Waiting for the deployment to complete...
deployment.apps/aqua-test-container condition met

✓ Aqua test container deployed successfully.
```

4. Execute Runtime Security Test Cases (Enter option 2~8 in the terminal)

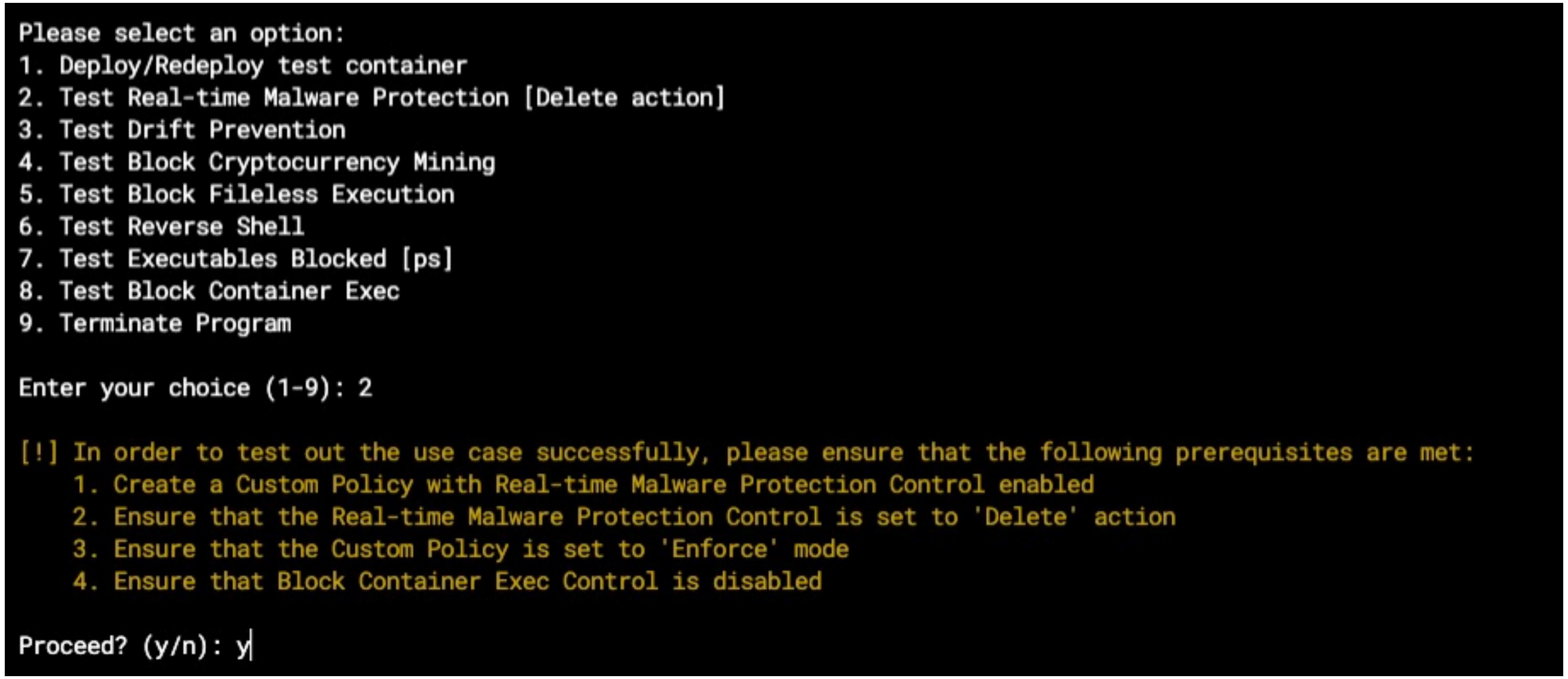


```
Please select an option:
1. Deploy/Redeploy test container
2. Test Real-time Malware Protection [Delete action]
3. Test Drift Prevention
4. Test Block Cryptocurrency Mining
5. Test Block Fileless Execution
6. Test Reverse Shell
7. Test Executables Blocked [ps]
8. Test Block Container Exec
9. Terminate Program

Enter your choice (1-9): 2
```

Step-by-step Guide

5. **Review the pre-requisite instructions and enter Y to proceed.**

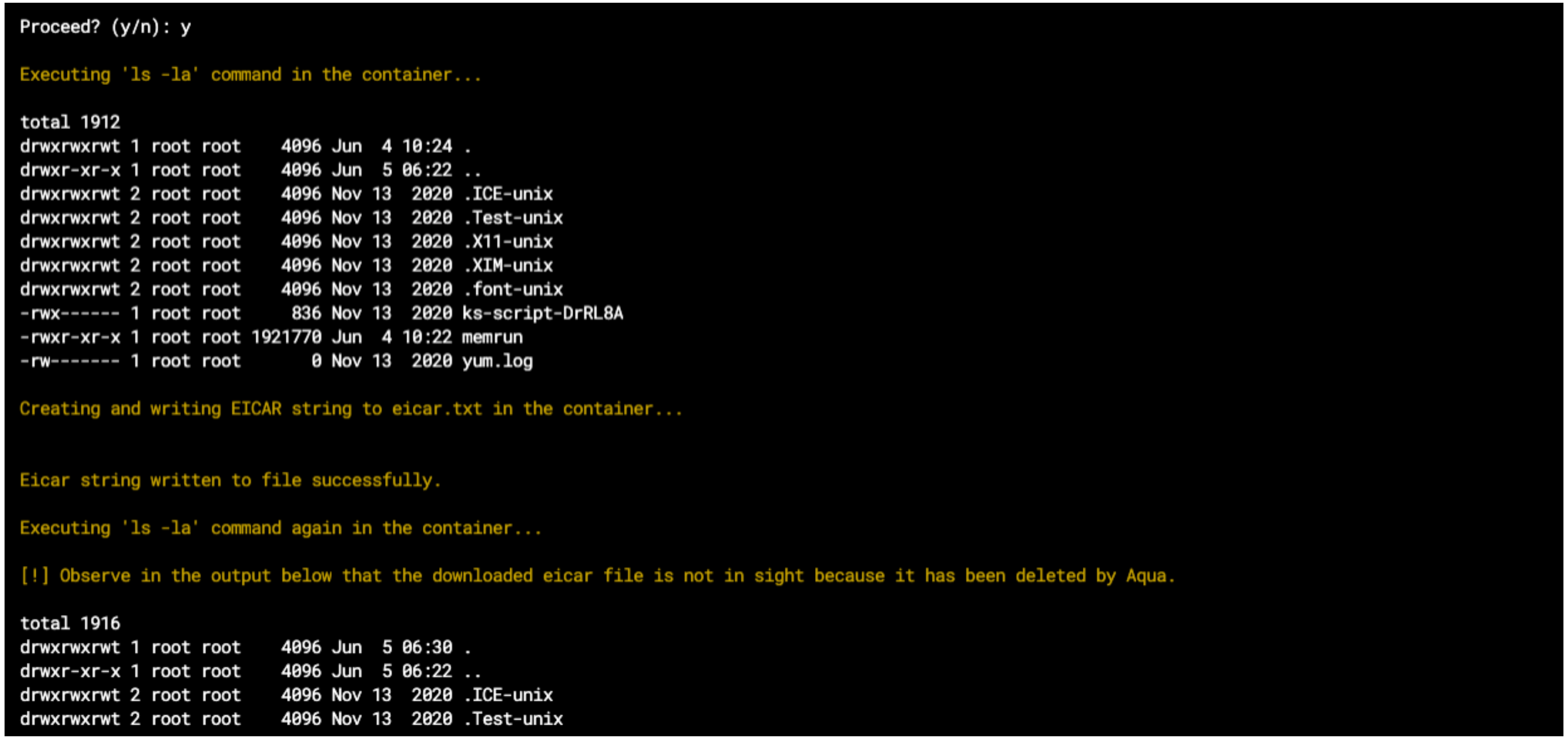
***Note: This page will not appear if the --n OR --no-instructions flag is set**



```
Please select an option:
1. Deploy/Redeploy test container
2. Test Real-time Malware Protection [Delete action]
3. Test Drift Prevention
4. Test Block Cryptocurrency Mining
5. Test Block Fileless Execution
6. Test Reverse Shell
7. Test Executables Blocked [ps]
8. Test Block Container Exec
9. Terminate Program

Enter your choice (1-9): 2

[!] In order to test out the use case successfully, please ensure that the following prerequisites are met:
    1. Create a Custom Policy with Real-time Malware Protection Control enabled
    2. Ensure that the Real-time Malware Protection Control is set to 'Delete' action
    3. Ensure that the Custom Policy is set to 'Enforce' mode
    4. Ensure that Block Container Exec Control is disabled

Proceed? (y/n): y
```

Step-by-step Guide

6. **Runtime Security Test Case will be executed automatically. Refer to the Aqua Console UI's Incident Screen to review the security event**

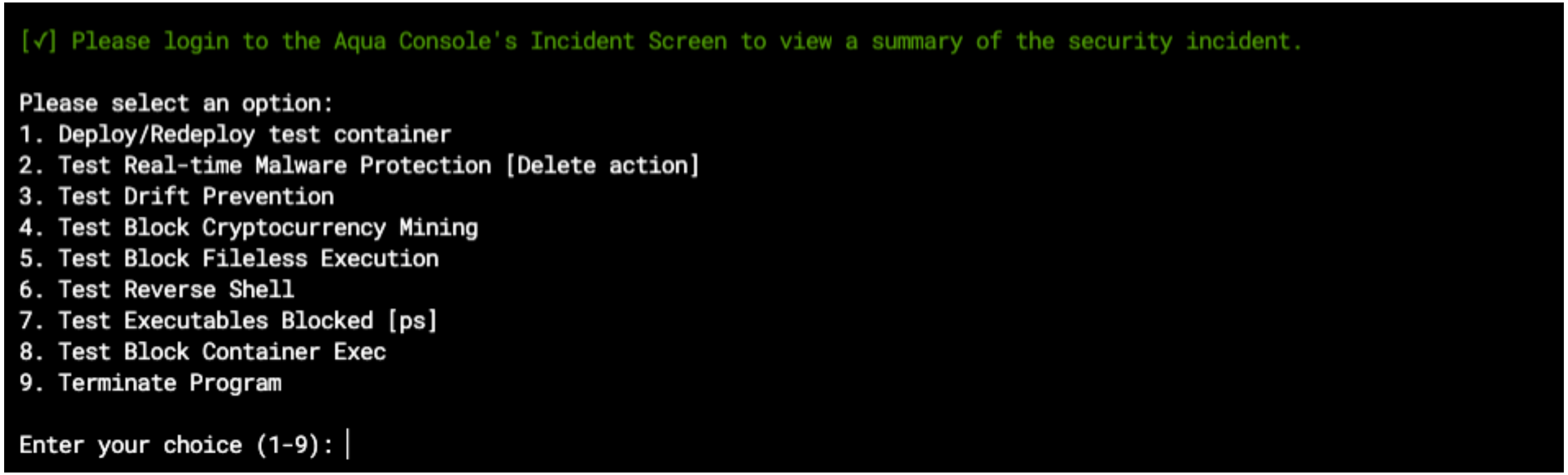


```
Proceed? (y/n): y

Executing 'ls -la' command in the container...

total 1912
drwxrwxrwt 1 root root    4096 Jun  4 10:24 .
drwxr-xr-x 1 root root    4096 Jun  5 06:22 ..
drwxrwxrwt 2 root root    4096 Nov 13  2020 .ICE-unix
drwxrwxrwt 2 root root    4096 Nov 13  2020 .Test-unix
drwxrwxrwt 2 root root    4096 Nov 13  2020 .X11-unix
drwxrwxrwt 2 root root    4096 Nov 13  2020 .XIM-unix
drwxrwxrwt 2 root root    4096 Nov 13  2020 .font-unix
-rwx------ 1 root root     836 Nov 13  2020 ks-script-DrRL8A
-rwxr-xr-x 1 root root 1921770 Jun  4 10:22 memrun
-rw------- 1 root root       0 Nov 13  2020 yum.log

Creating and writing EICAR string to eicar.txt in the container...


Eicar string written to file successfully.

Executing 'ls -la' command again in the container...

[!] Observe in the output below that the downloaded eicar file is not in sight because it has been deleted by Aqua.

total 1916
drwxrwxrwt 1 root root    4096 Jun  5 06:30 .
drwxr-xr-x 1 root root    4096 Jun  5 06:22 ..
drwxrwxrwt 2 root root    4096 Nov 13  2020 .ICE-unix
drwxrwxrwt 2 root root    4096 Nov 13  2020 .Test-unix
```

Step-by-step Guide

7. Proceed to enter another option (2~8) to test out other runtime security test cases.

   Alternatively, enter option 9 to exit Aqua Warden



```
[✓] Please login to the Aqua Console's Incident Screen to view a summary of the security incident.

Please select an option:
1. Deploy/Redeploy test container
2. Test Real-time Malware Protection [Delete action]
3. Test Drift Prevention
4. Test Block Cryptocurrency Mining
5. Test Block Fileless Execution
6. Test Reverse Shell
7. Test Executables Blocked [ps]
8. Test Block Container Exec
9. Terminate Program

Enter your choice (1-9):
```

Download Aqua Warden

- **GitHub Repository:** https://github.com/stanezil/aqua-warden
- **Test Container Image:** docker.io/stanhoe/aqua-warden:latest

Thanks

aqua