AccuKnox

Host Security Playbook

Table of Contents

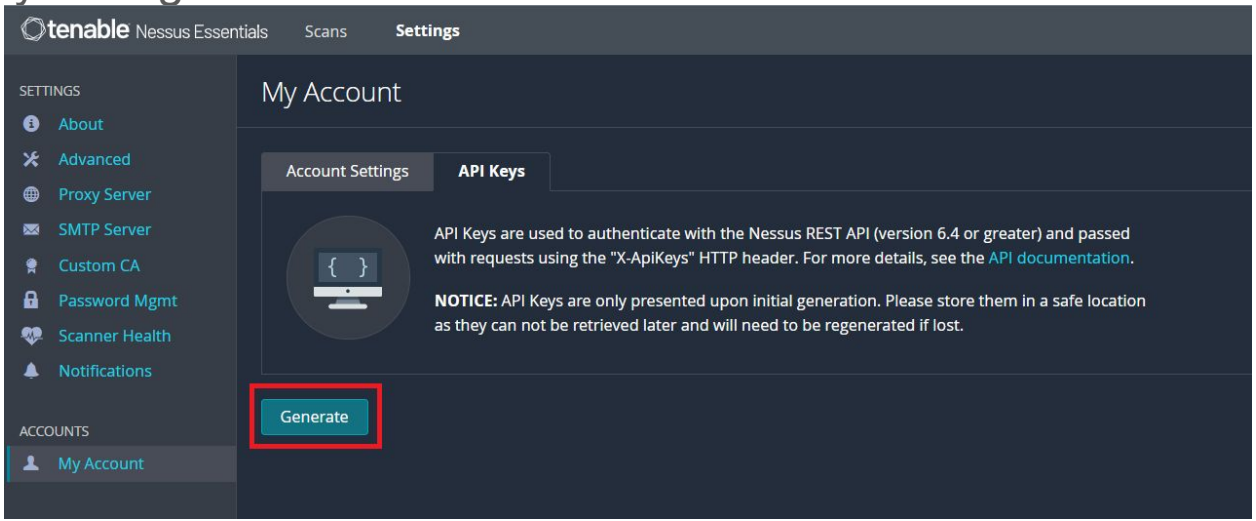
Nessus Integration Prerequisites

AccuKnox will require the following details to be able to integrate with Nessus and fetch the results:

- **URL of nessus deployment** - The URL that is used to access the Nessus deployment (Eg: http://nessus.accuknox.com:8834)
- **Access Key**
- **Secret Key**

The access and secret keys are generated in the Nessus Instance:

- Switch to the **Settings** tab, navigate to **My Account → API keys** and click on **Generate**.
- Copy the generated keys.



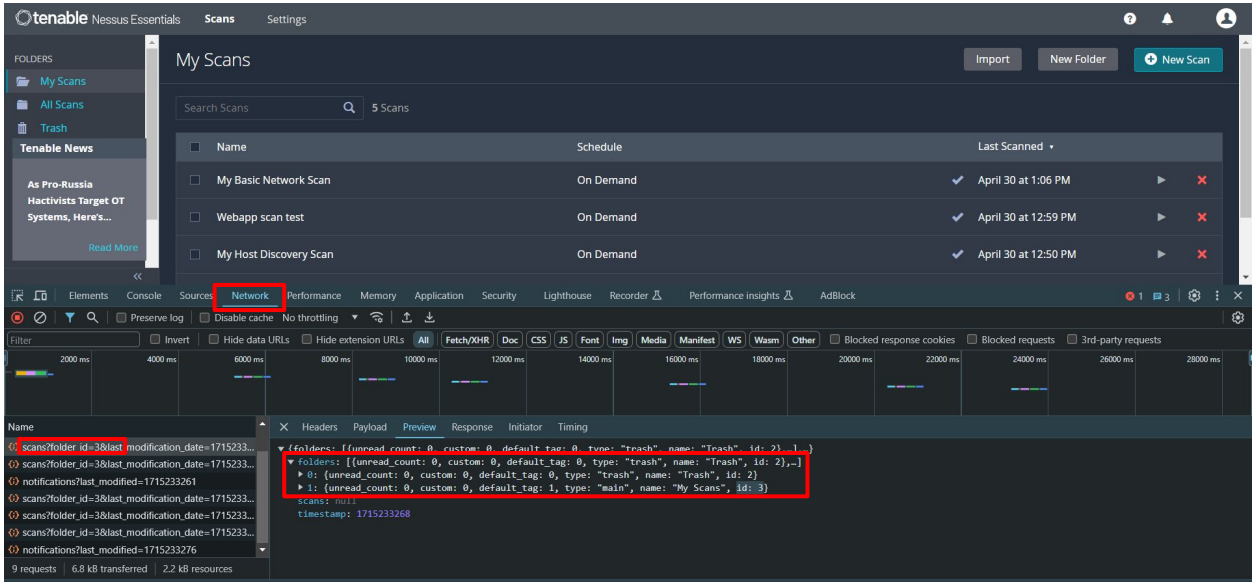
Nessus Integration Prerequisites

- **Folder ID**

Fetch the Folder ID from the Nessus Deployment where the scan results are stored:

1. Navigate to the Scans tab and select the folder where the scan results are stored
2. Inspect the page: (ctrl+Shift+J on Windows)

   a. Move to Network tab
   b. Select an entry with the folder_id variable
   c. Select the Preview tab
   d. Note the **id** next to the **name** of the folder (In the below screenshot case, the scans are stored in “My Scans” Folder and the id for it is “3”)



ACCUKNOX

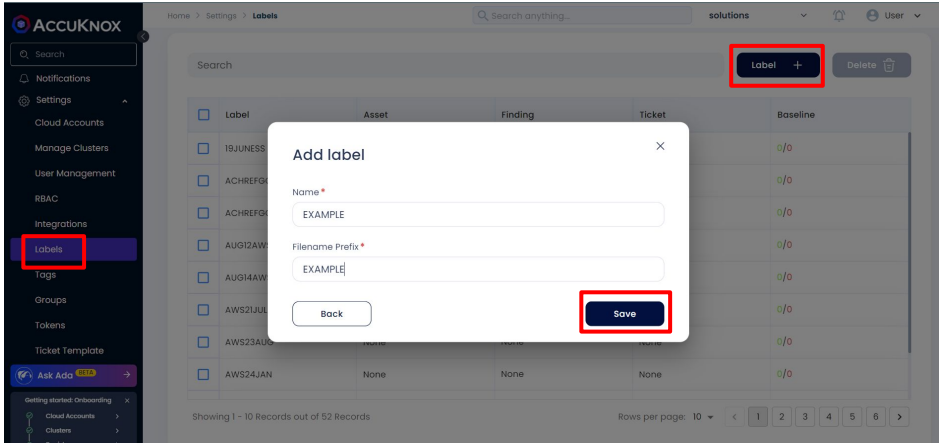
Nessus Integration

Method 1: When the Nessus URL is accessible from the AccuKnox SaaS

Forward the gathered prerequisites to AccuKnox team along with the desired scan interval and the integration will be done in the platform from the backend.

Method 2: When the Nessus URL is not accessible via the AccuKnox SaaS (In case of On Prem Nessus without internet access)

- Create a label from the AccuKnox platform
- CSPM base URL will be:
  - https://cspm.demo.accuknox.com (In case of demo)
  - https://cspm.accuknox.com (In case of SaaS subscription)
  - https://cspm.<your-domain> (In case of On Prem AccuKnox)



Nessus Integration

- Instead of the AccuKnox platform connecting to Nessus and fetching the results, the results from Nessus can be fetched and forwarded to the AccuKnox platform.
- This will only require outbound connectivity via the Firewall from the Nessus deployment to the AccuKnox SaaS via port 443.
- The data exporter is provided as a docker image available here
- Replace the $values in the below command and run on a machine that has docker installed and can reach the nessus deployment.

```
docker run --rm -it \
    -e nessus_url=$nessus_url \
    -e folder_id=$folder_id \
    -e nessus_access_key=$access_key  \
    -e nessus_secret_key=$secret_key \
    -e CSPM_BASE_URL=$cspm_url \
    -e label=$label \
    -e internal_tenant_id=$tenant_id \
    -e ARTIFACT_TOKEN=$token \
    accuknox/nessus:v1
```

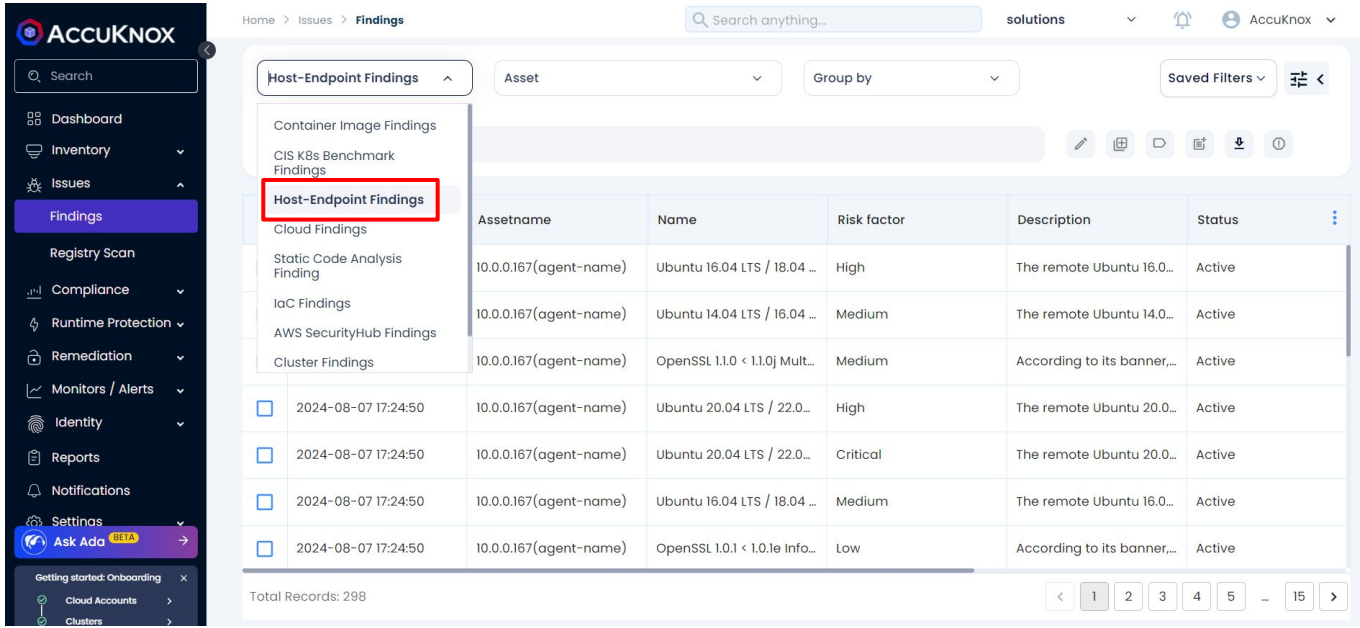
- After running the command, a message “File Received Successfully” is shown
- After this message is confirmed, wait for a few minutes and the results will be visible on the AccuKnox platform

AccuKnox

Nessus Scan

AccuKnox can integrate with Nessus to provide host scanning capabilities for the Hosts such as Windows, Unix and Linux machines.

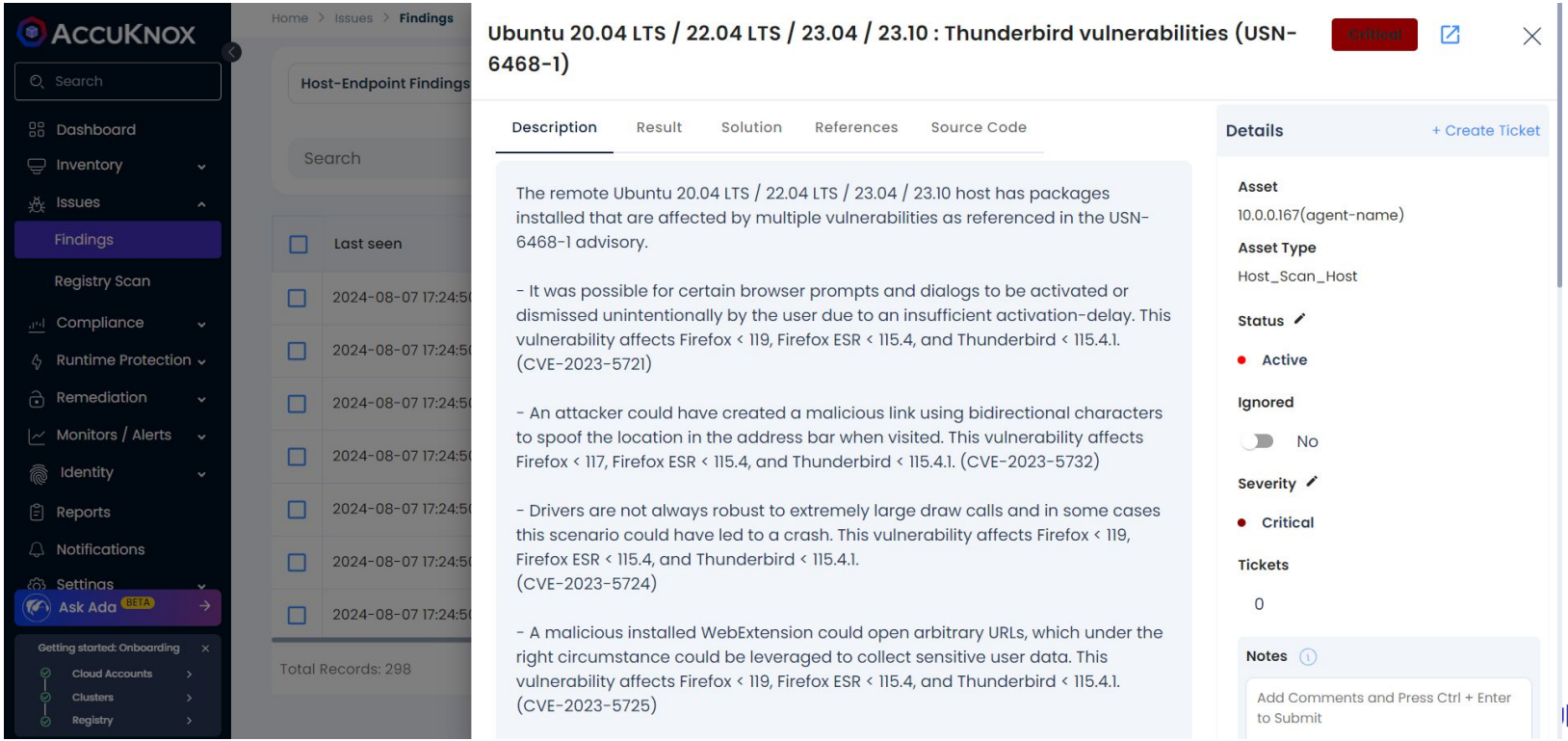
To view the results that were aggregated from Nessus, navigate to Issues → Findings and select the Filter as **Host-Endpoint Findings**



ACCUKNOX

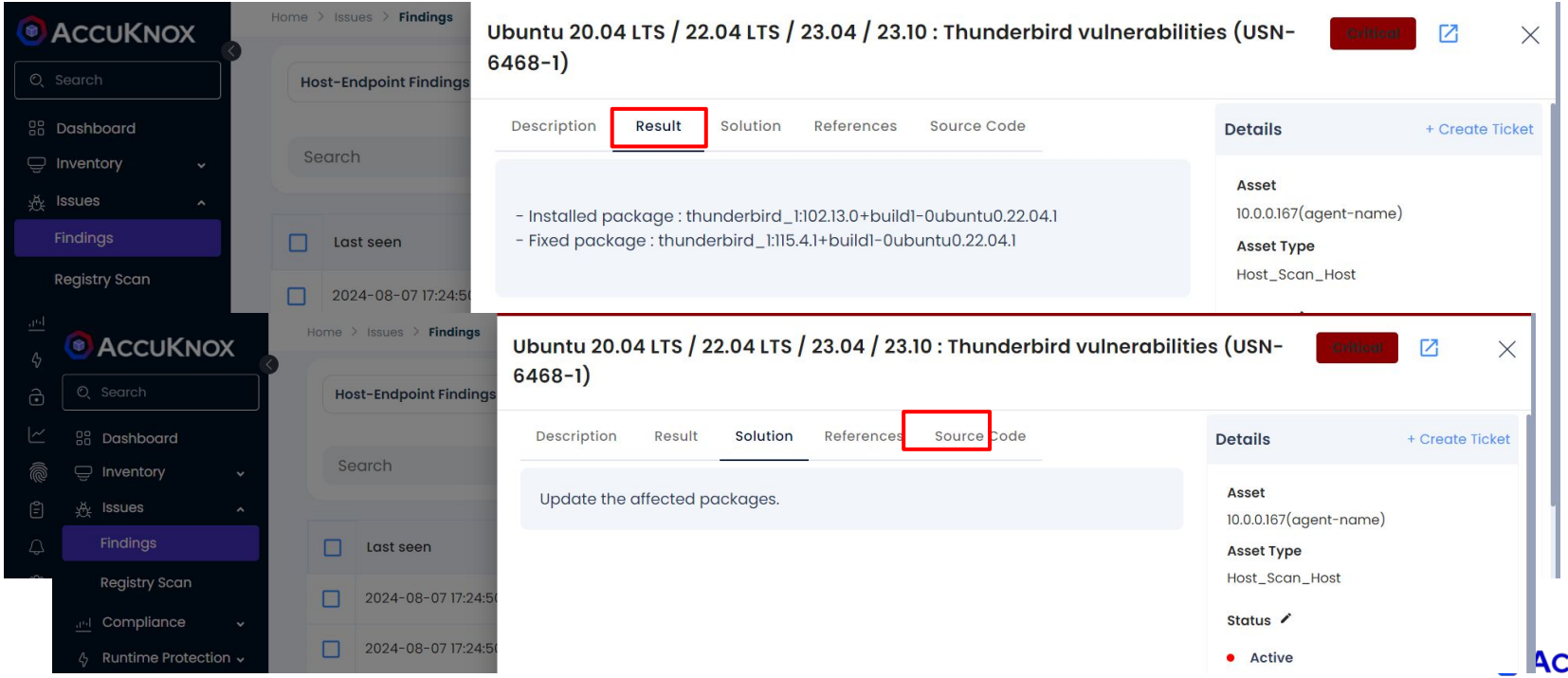
Nessus Scan - Thunderbird vulnerability on Linux

Click on the findings to show more information about the vulnerability associated with the Host. There are a set of critical CVEs associated with Thunderbird



Nessus Scan - Result & Solution for Thunderbird vulnerability

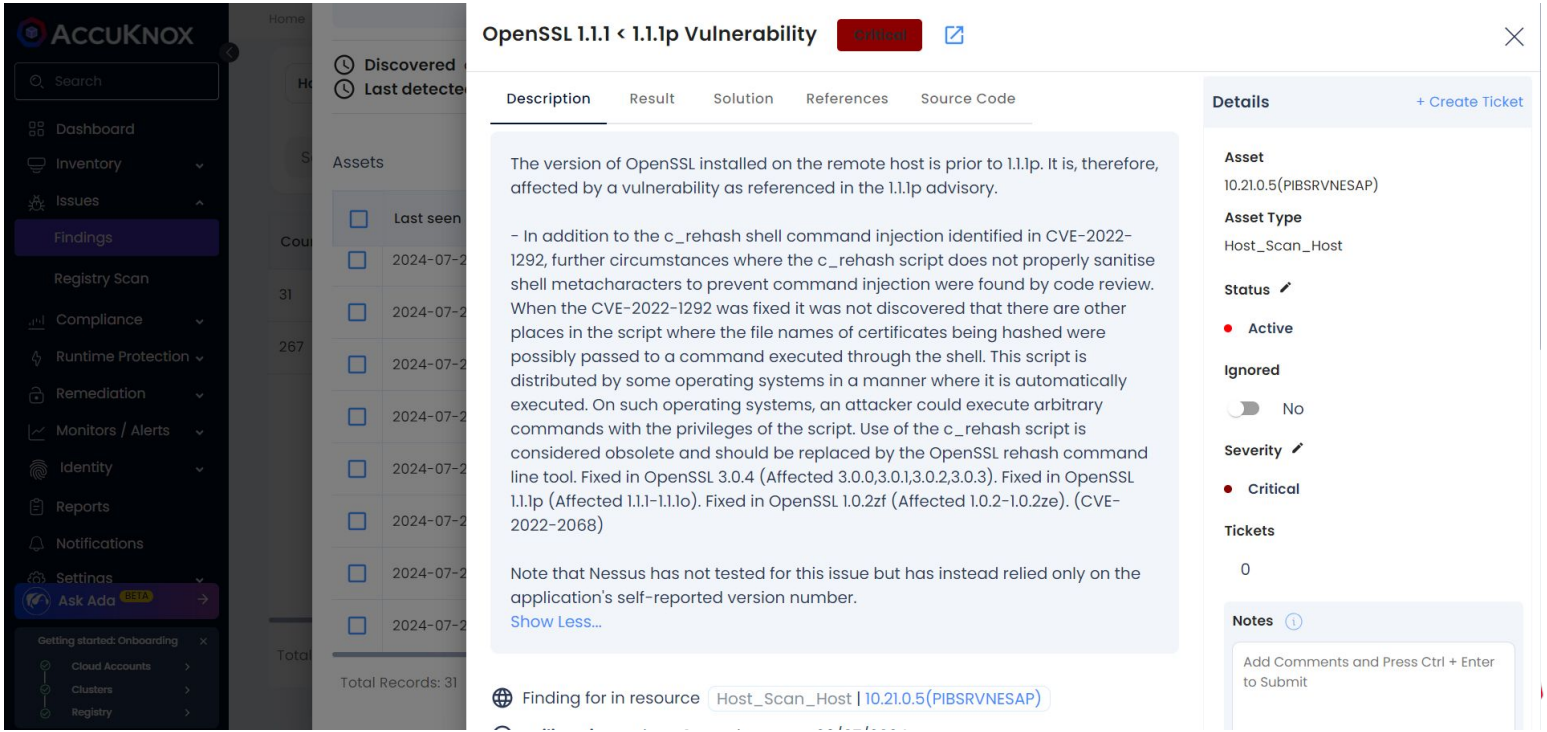
Select the **Results** tab for more info regarding the checks done. **Solutions** tab to view the fix for the vulnerability. This shows that Thunderbird needs to be updated.



ACCUKNOX

Nessus Scan - OpenSSL Vulnerability

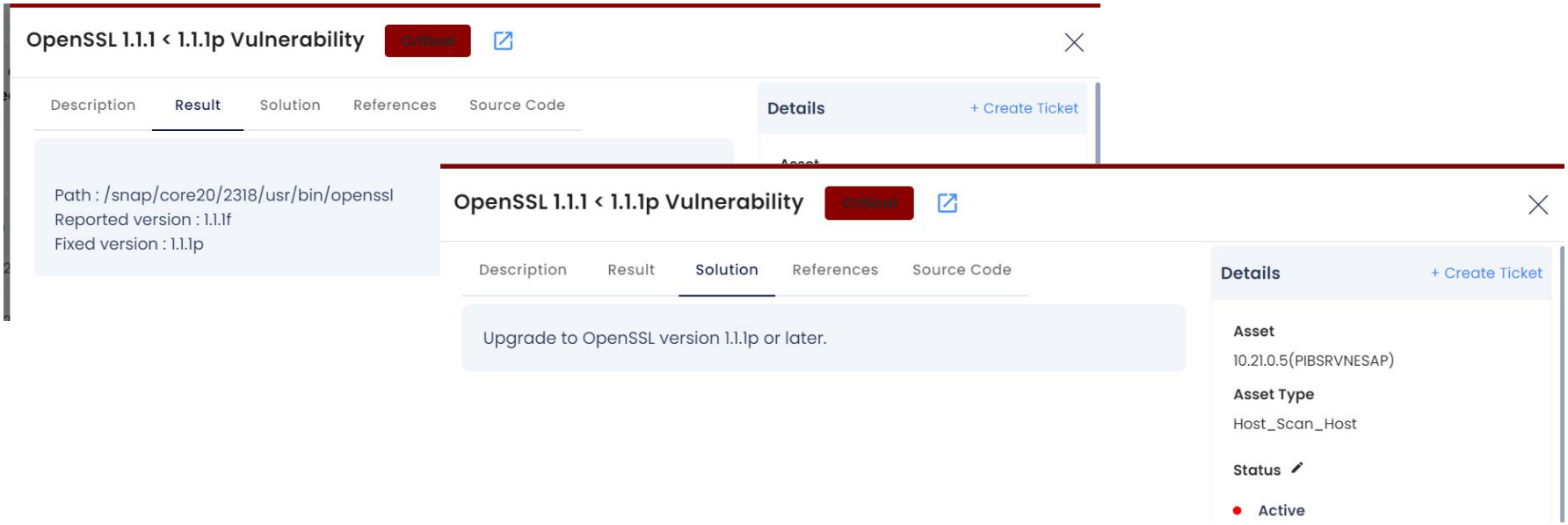
An OpenSSL related vulnerability was found that allows an attacker to perform command injection.



ACCUKNOX

Nessus Scan - OpenSSL Vulnerability

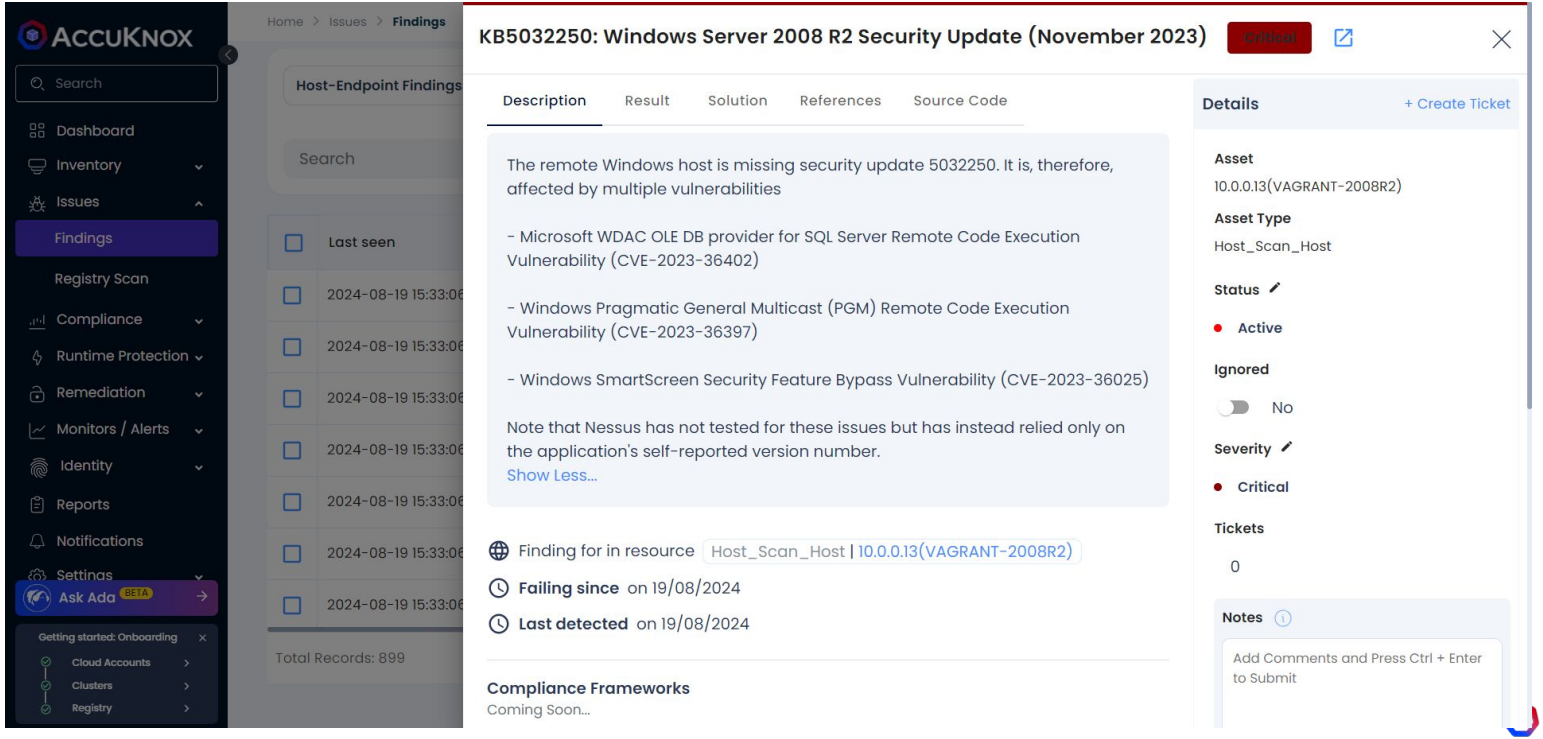
- The risk of command injection can be eliminated by upgrading the OpenSSL package as the vendor fix is already available..
- A ticket can be created to perform the update and the track progress



ACCUKNOX

Nessus Scan - Vulnerable Windows Server

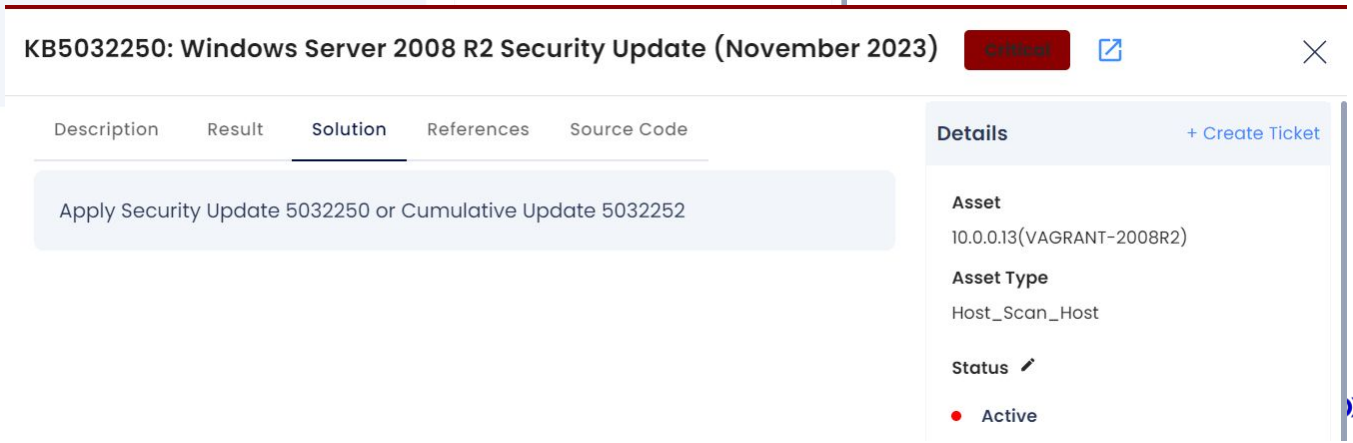
The windows server was found to be missing a security update, leading to multiple vulnerabilities



ACCUKNOX

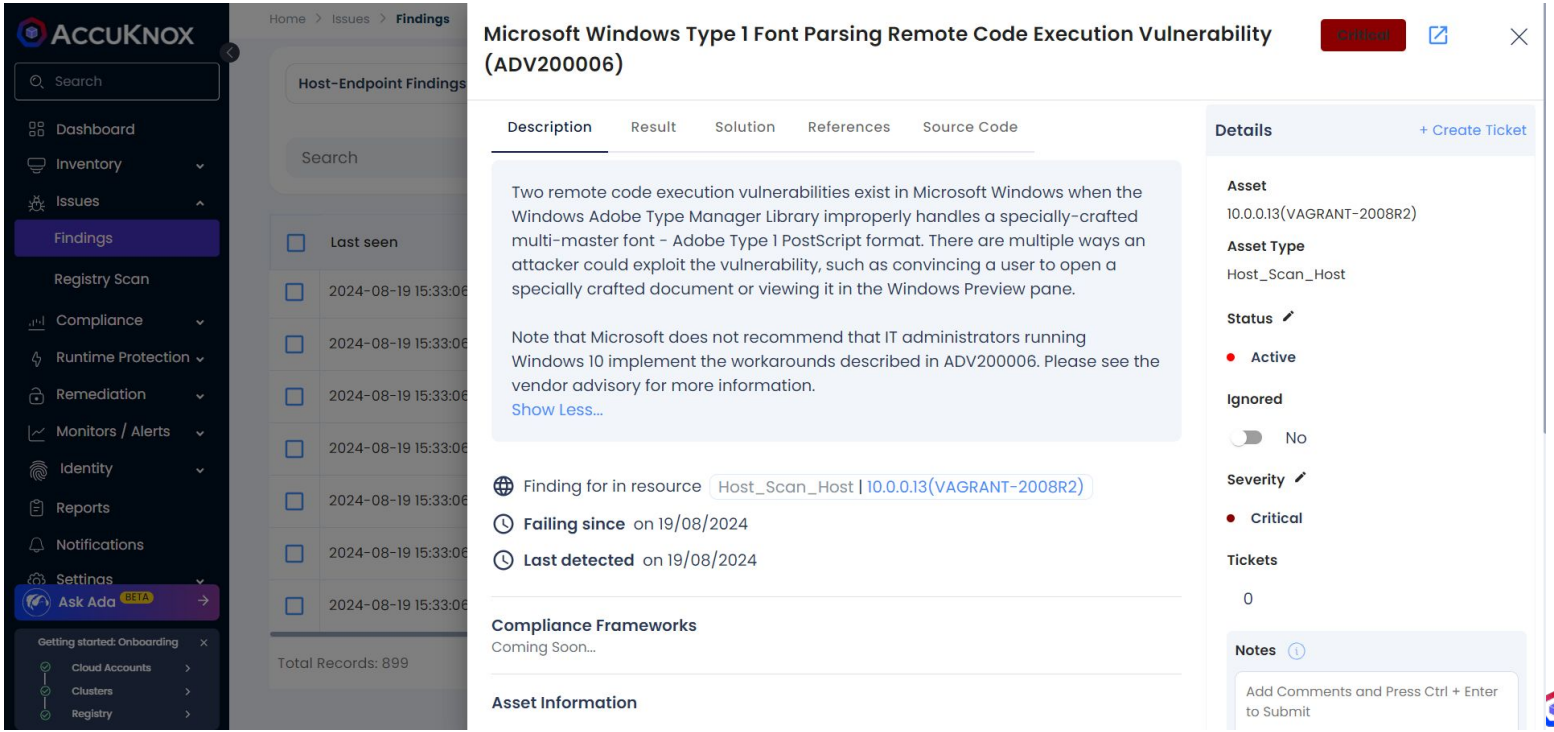
Nessus Scan - Vulnerable Windows Server

The security update to fix the vulnerabilities can be confirmed and applied.



Nessus Scan - RCE Vulnerability in Windows

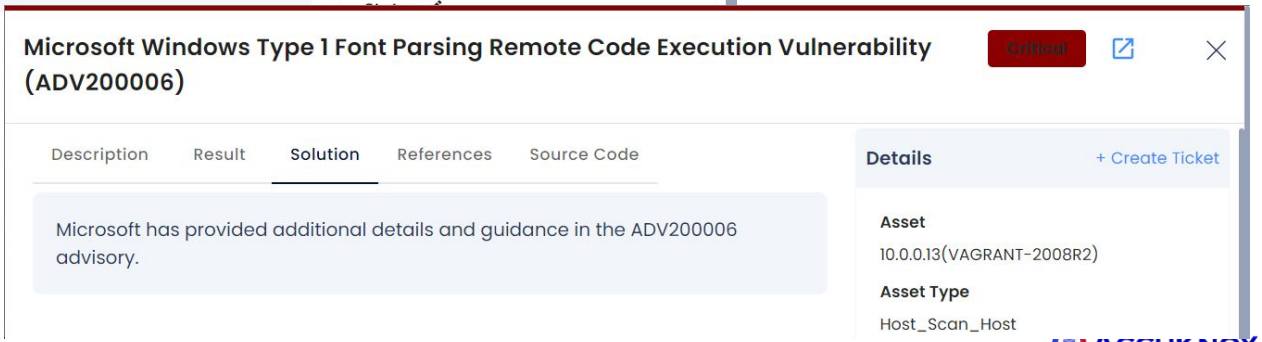
The windows operating system has a vulnerability that will result in RCE with multiple exploitation methods.



AccuKnox

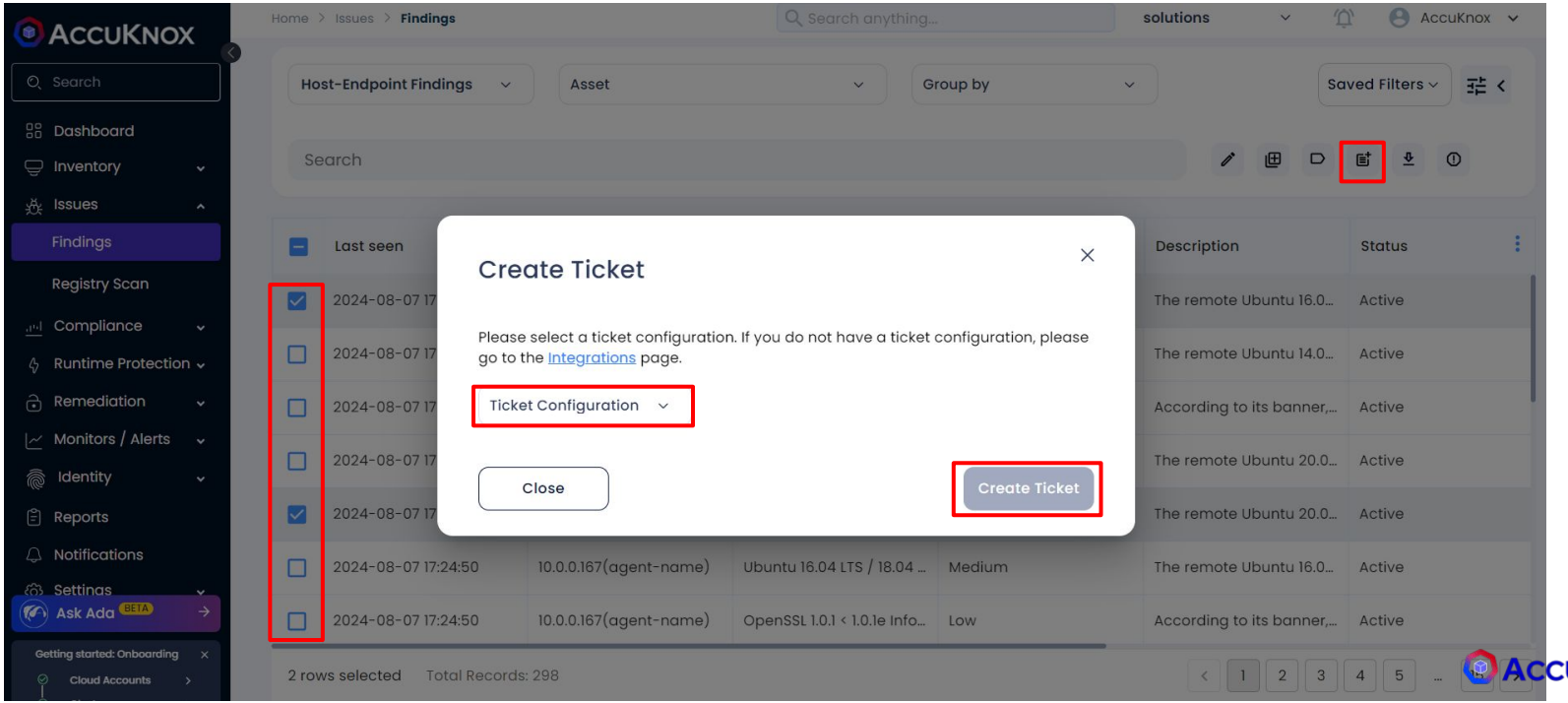
Nessus Scan - RCE Vulnerability in Windows

The advisory is shown which contains multiple methods for preventing the exploit of this vulnerability. The accepted method can be used as per your model.



Nessus Scan - Remediation

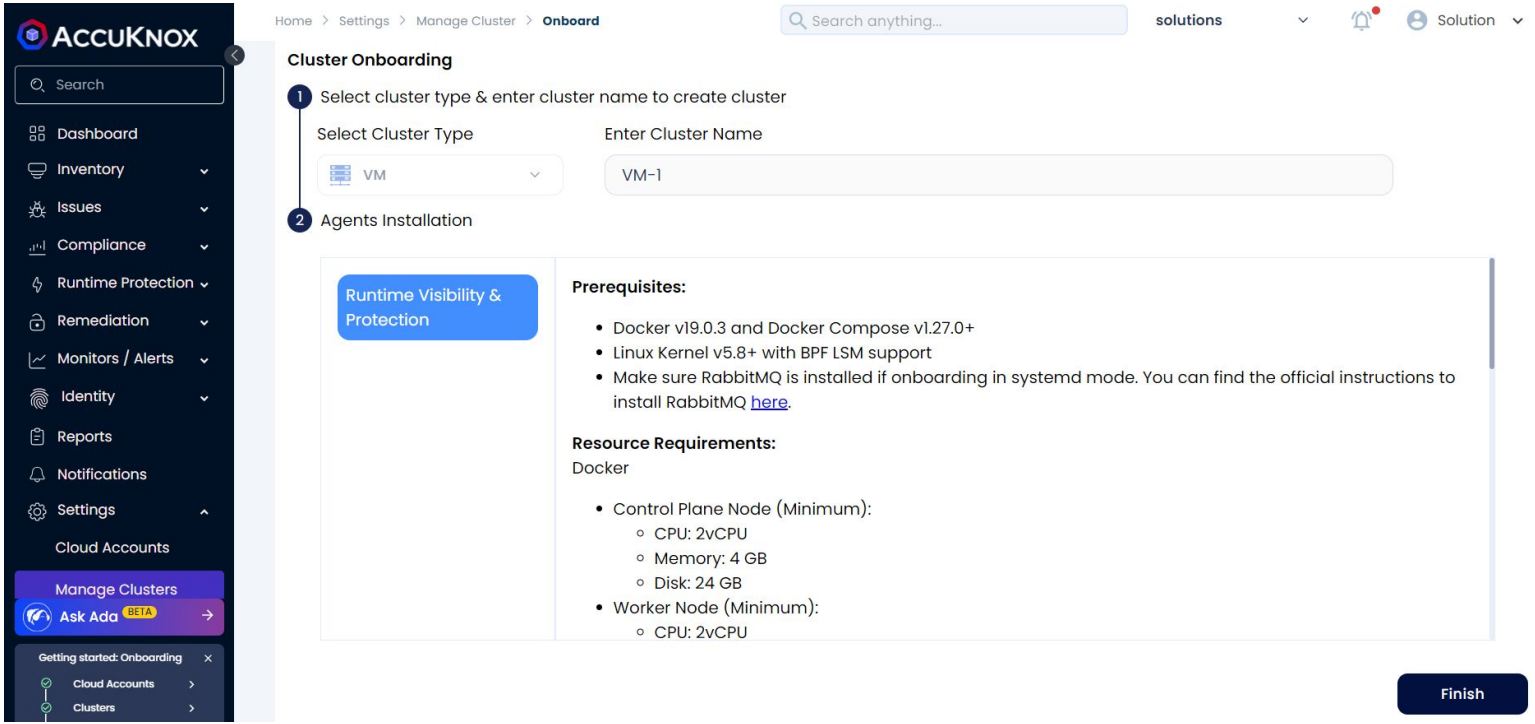
- Select the findings from the list after grouping/filtering as required and then click on Create Ticket icon.
- In the pop up, select the **Ticket Configuration** and click on **Create Ticket**



Agent Based VM Security

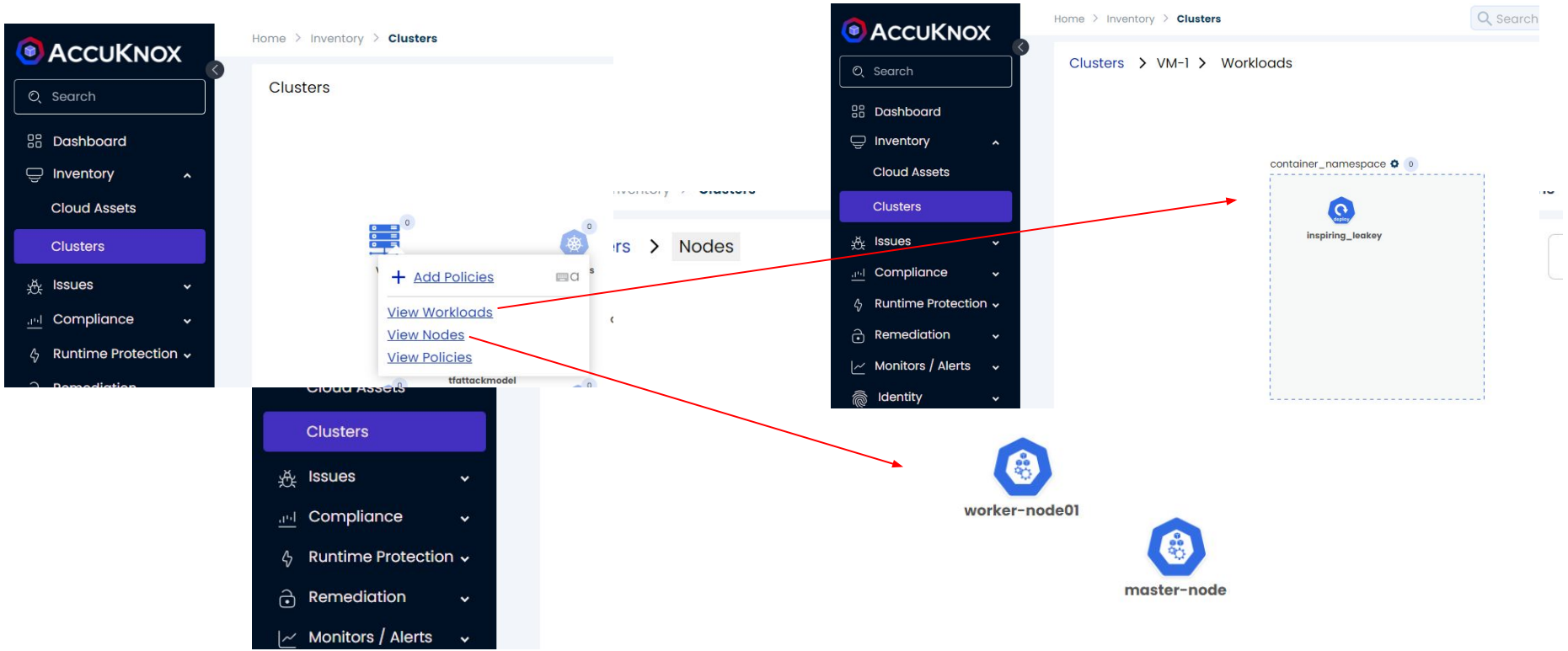
VM Onboarding

- Navigate to **Settings** → **Manage Cluster** and click on **Onboard Now**
- Select cluster type as VM, enter Name and Save. Verify prerequisites and install the agents via the commands on screen



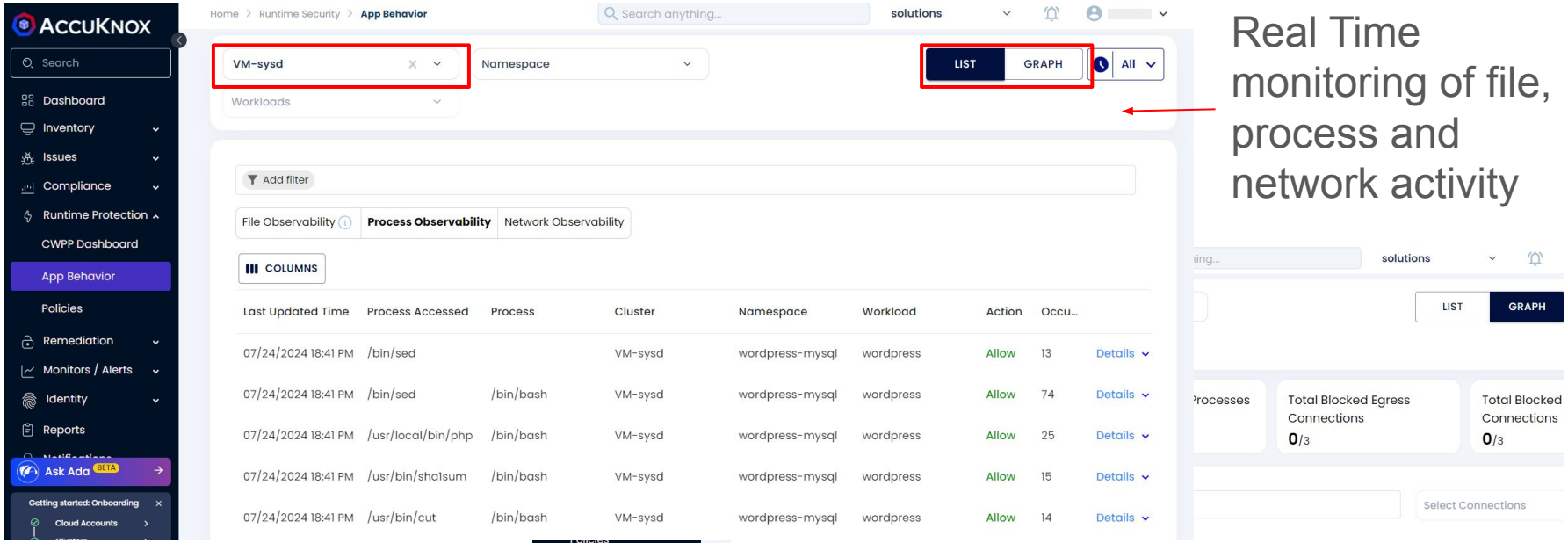
View onboarded VMs

- Navigate to **Inventory** → **Clusters** and click on the onboarded VM, select **View Nodes**
- In case docker is available, click on **View Workloads** to view the containers



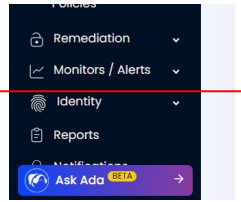
VM Behavior for Containerized Apps

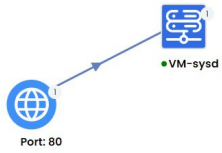
- Navigate to **Runtime Security** → **App Behavior** and select the onboarded VM



Real Time monitoring of file, process and network activity

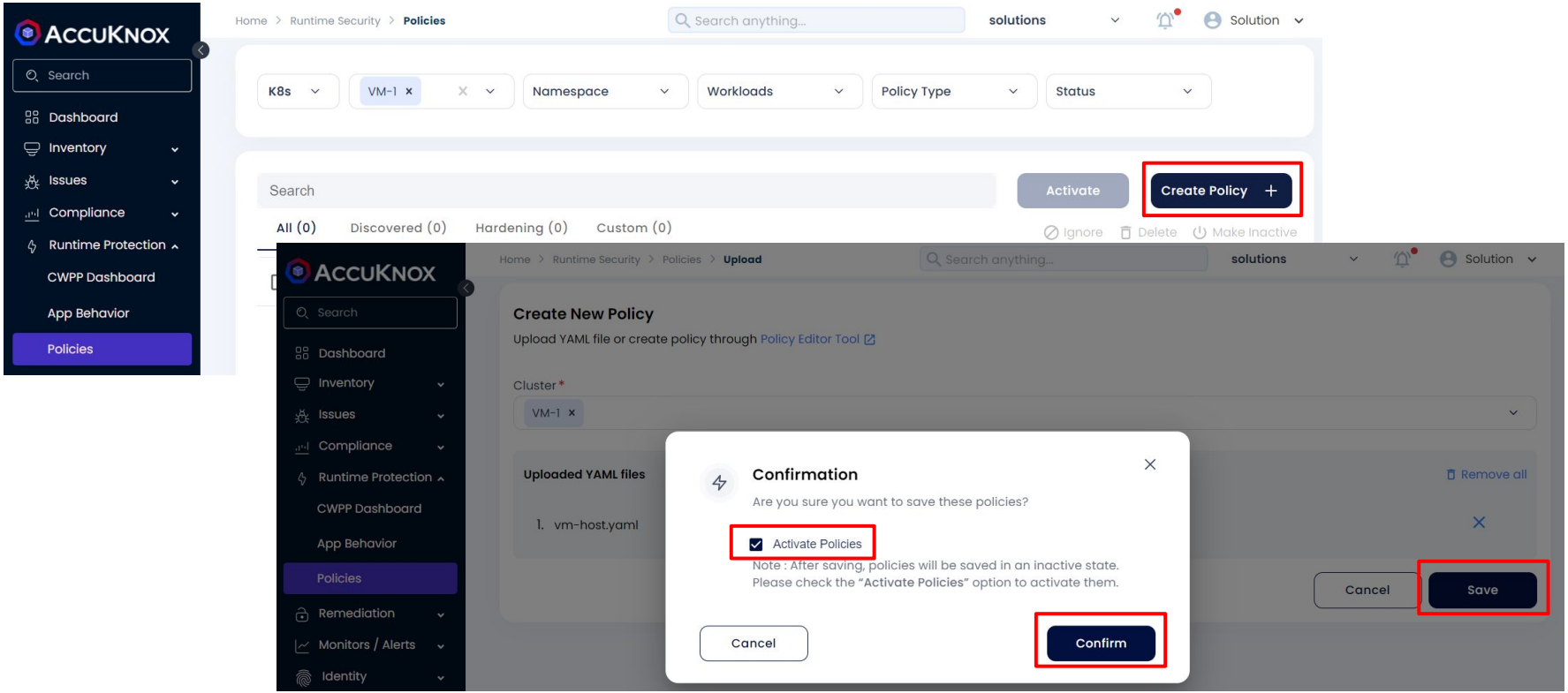
Graphical Insights of Network Connections, either to private/public IPs





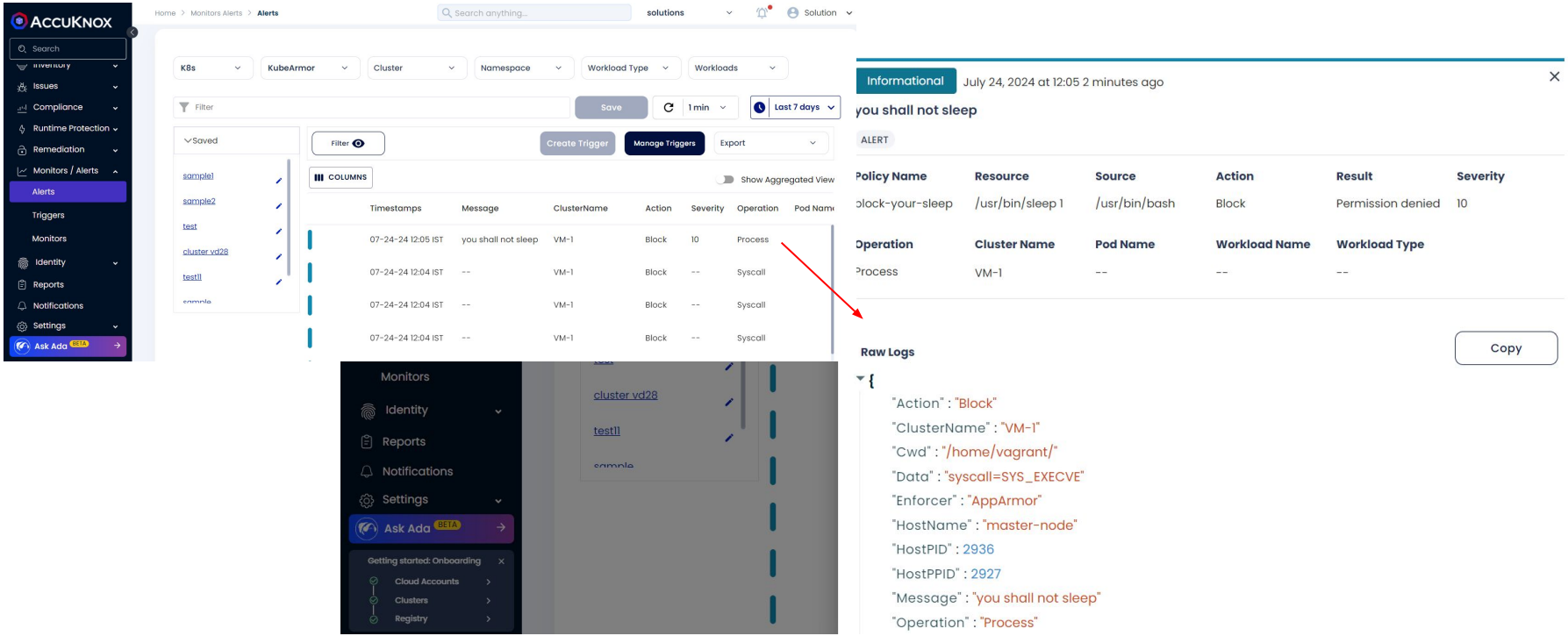
VM Hardening

- Navigate to **Runtime Security → Policies** and click on **Create Policy**
- Upload policies and click on **Save.** Select **Activate Policies** to save and activate



Policy alerts for VM

- After a policy violation occurred, navigate to **Monitors/Alerts → Alerts**
- Click on any of the alerts to view more information



VM Security Use Cases

VM Hardening - Block Execution of package managers

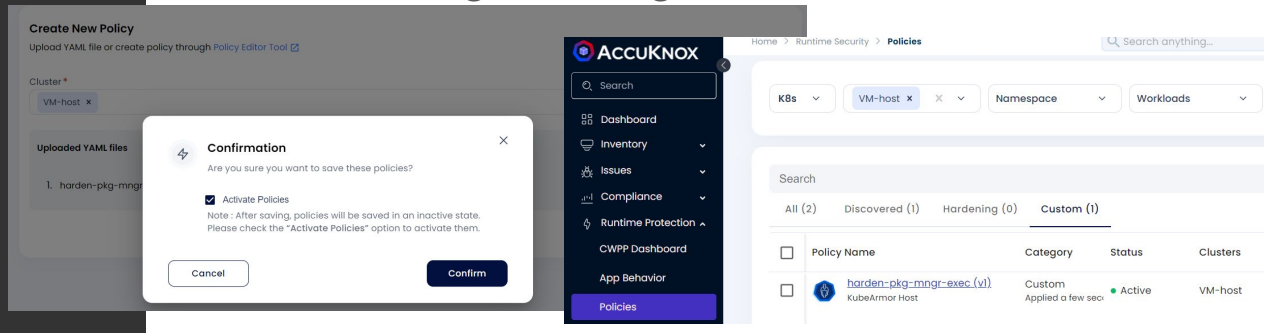
Attackers might try to download additional tools to help with exploiting the environment or downgrade packages to a vulnerable version.

```yaml
apiVersion: security.kubearmor.com/v1
kind: KubeArmorHost
Policymetadata:
  name: block-pkg-mgmt-tools
spec:
  severity: 10
  message: "Alert! Execution of package management process is denied"
  tags:
  - ALERT
  nodeSelector:
    matchLabels:
      kubearmor.io/hostname: <vm-hostname>
  process:
   matchPaths:
    - execname: apt-get
    - execname: apt
    - execname: dnf
    - execname: dpkg
    - execname: gdebi
    - execname: make
    - execname: makepkg
    - execname: pacman
    - execname: rpm
    - execname: yaourt
    - execname: yum
    - execname: zypper

  action:
    Block
  tags:
   - NIST
   - NIST_800-53_CM-7(4)
   - SI-4
   - process
   - NIST_800-53_SI-4
```

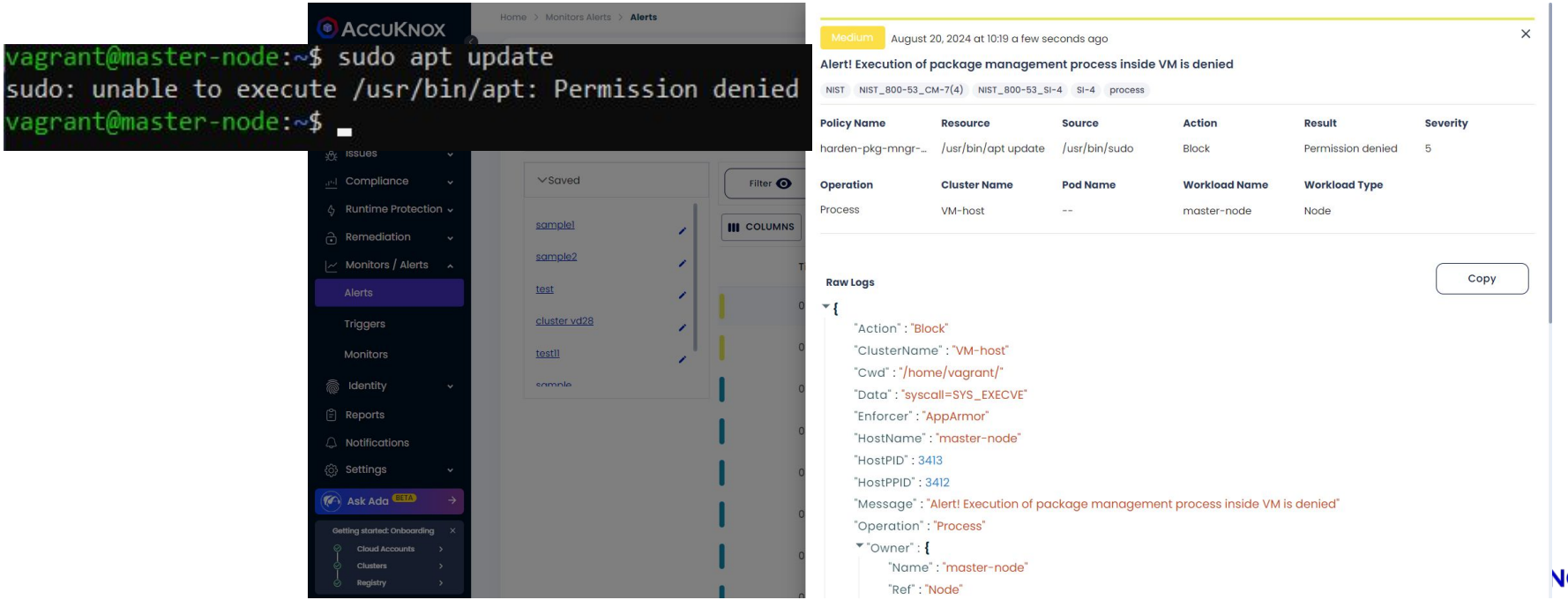
- Replace <vm-hostname> with the target VM's hostname
- Upload and Activate this policy to block the execution of the package managers on the VM

Package managers to be blocked



VM Hardening - Block Execution of package managers

- Open a new terminal session on the VM
- When a package manager is attempted to be executed, the execution will be blocked and alerts will be visible on the SaaS platform



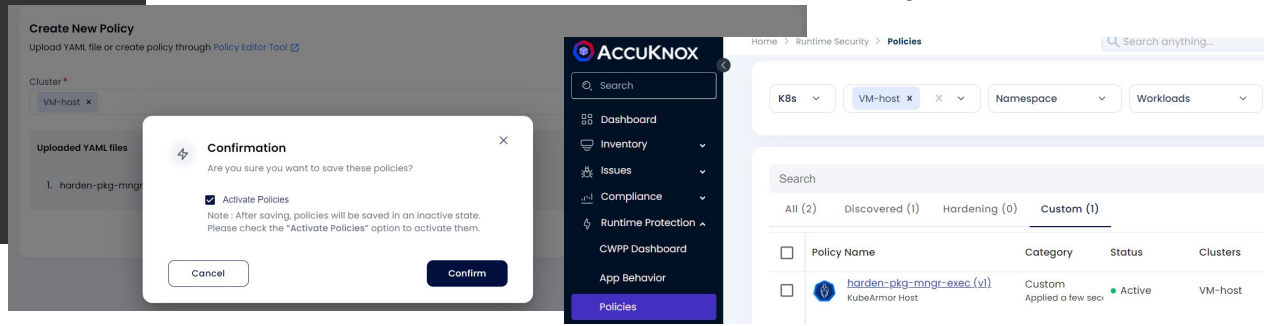
VM Hardening - File Integrity Monitoring

KubeArmor can not only monitor for changes to system binary folders, configuration paths, and credentials paths but also blocks any write attempts

```yaml
apiVersion: security.kubearmor.com/v1
kind: KubeArmorHostPolicy
metadata:
  name: hsp-File-Integrity-Monitoring
spec:
  nodeSelector:
    matchLabels:
      kubernetes.io/hostname: vm-name
  severity: 5
  message: Detected and prevented compromise to File integrity
  File:
    matchDirectories:
    - dir: /sbin/
      readOnly: true
      recursive: true
    - dir: /usr/bin/
      readOnly: true
      recursive: true
    - dir: /usr/lib/
      readOnly: true
      recursive: true
    - dir: /usr/sbin/
      readOnly: true
      recursive: true
    - dir: /bin/
      readOnly: true
      recursive: true
    - dir: /boot/
      readOnly: true
      recursive: true
  action: Block
```

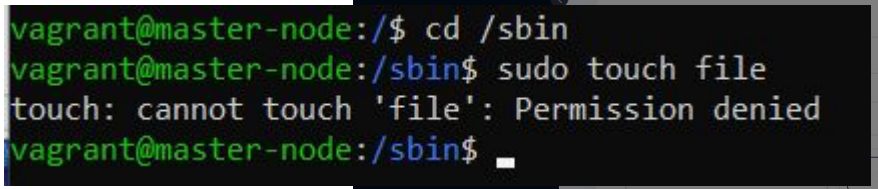
- Replace vm-name with the target VM's hostname
- Upload and Activate this policy to block any writes inside the specified directories

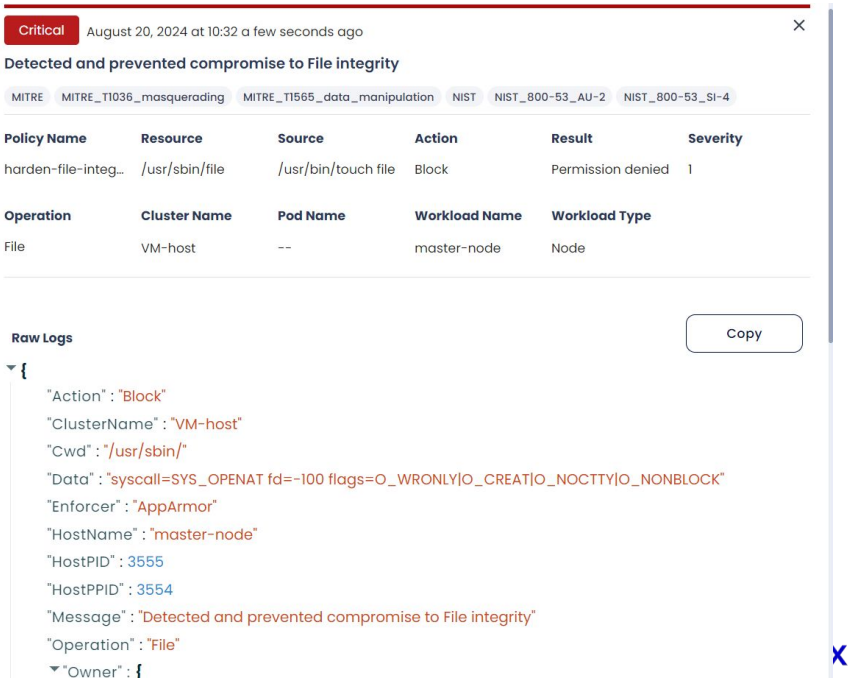
Directories with Files to be protected



VM Hardening - File Integrity Monitoring

- Open a new terminal session on the VM
- Try to modify/write to files inside the directories that are specified in the policy
- The write attempt is blocked and an alert is shown on the platform





VM Hardening - Prevent cryptominers execution

Deny execution of known cryptominers and prevent execution of binaries from tmp, prevent tampering of sensitive files to protect against Cryptojacking attacks

```yaml
apiVersion: security.kubearmor.com/v1
kind: KubeArmorHostPolicy
metadata:
  name: harden-crypto-miners
Spec:
  nodeSelector:
    matchLabels:
      kubearmor.io/hostname: vm-name
  action: Block
  file:
    matchDirectories:
    - dir: /bin/
      readOnly: true
      recursive: true
    - dir: /boot/
      readOnly: true
      recursive: true
    - dir: /sbin/
      readOnly: true
      recursive: true
    - dir: /usr/bin/
      readOnly: true
      recursive: true
    - dir: /usr/local/bin/
      readOnly: true
      recursive: true
    - dir: /var/local/bin/
      readOnly: true
      recursive: true
  message: cryptominer detected and blocked
  process:
    matchDirectories:
    - dir: /tmp/
      recursive: true
    matchPaths:
    - execname: apk
    - execname: apt
    - execname: dero-miner-linux-amd64
    - execname: dero-wallet-cli-linux-amd64
    - execname: dero
    - execname: derod-linux-amd64
    - execname: masscan
    - execname: nmap
    - execname: ntpdate
    - execname: xmrig
    - execname: zgrab2
  severity: 10
```

- Replace vm-name with the target VM's hostname
- Upload and Activate this policy to protect against cryptojacking

The file directories to be protected against tampering by attacker to mount/hide attack

Prevent execution of binaries from /tmp/ directory to prevent compromise

The binaries to be denied execution

AccuKnox

VM Hardening - Prevent cryptominers execution

- Open a new terminal session on the VM
- Try tampering the files in /bin/ directory or executing a blocked process
- The action is blocked and an alert is shown on the platform