

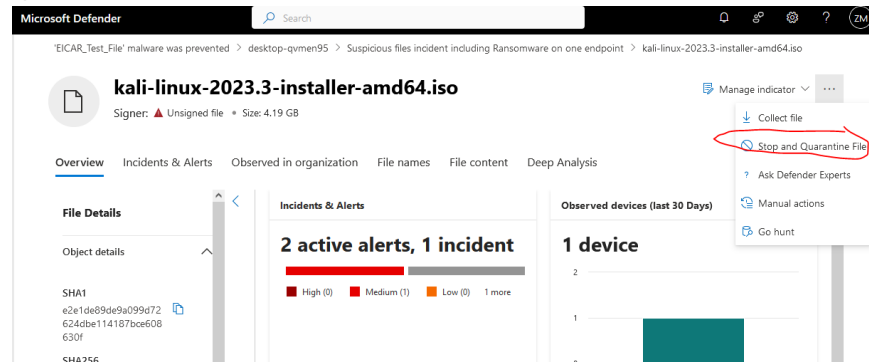
## MS Defender EDR – mitigate and remediate an incident

**Problem:** remediate an alert containing an iso file.

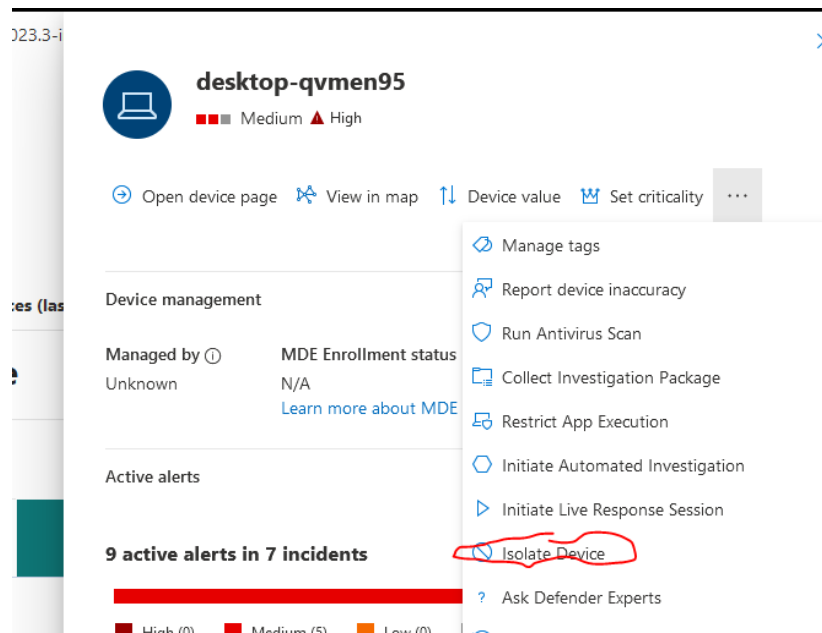
**Goal:** contain, eradicate, and recover the iso file.

### Process:

- Containment –
  - quarantine the file

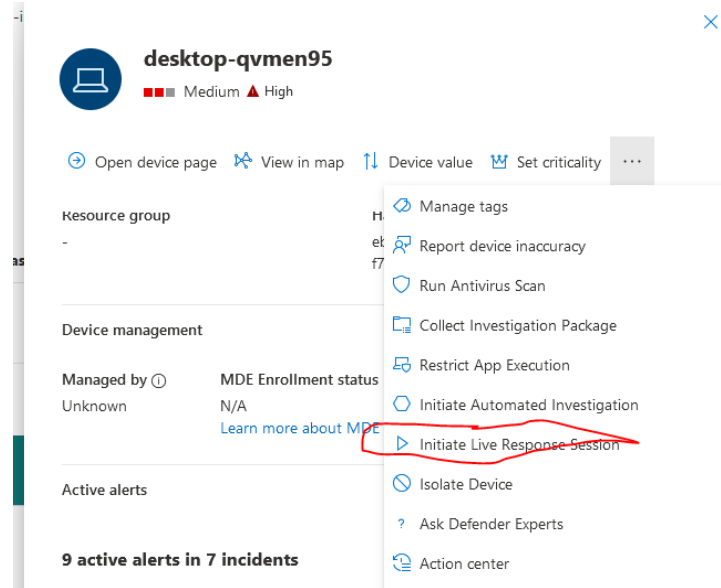


- Isolate affected device



## Eradication

- Remotely get into device and delete file
  - Open command prompt (live response of device name)



- cd to file path
- Delete file with Remediate cmd
- Run antivirus - full scan

les in

164

desktop-qvmen95

Medium High

Open device page View in map Device value Set criticality

Resource group

-

Device management

Managed by (1) MDE Enrollment status

Unknown N/A

[Learn more about MDE](#)

Active alerts

9 active alerts in 7 incidents

Manage tags

Report device inaccuracy

Run Antivirus Scan

Collect Investigation Package

Restrict App Execution

Initiate Automated Investigation

Initiate Live Response Session

Isolate Device

Ask Defender Experts

Action center

- If it is still in Incident and Alert, get the machine re-imaged

## Recovery

- Release device - isolate device tab will be ready for Release Device