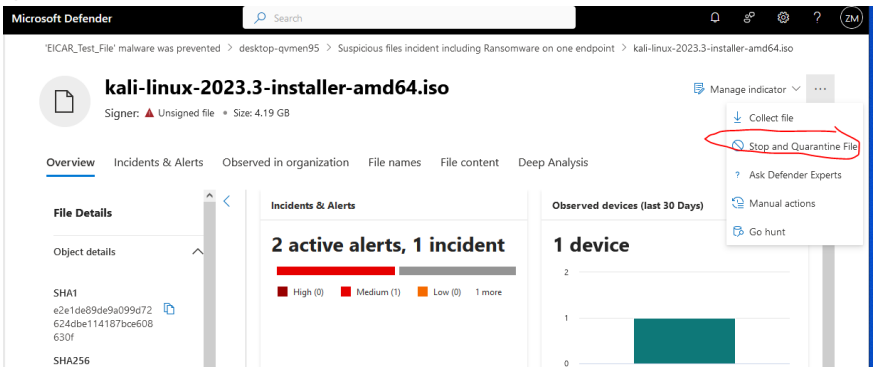
MS Defender EDR – mitigate and remediate an incident

Problem: remediate an alert containing an iso file.

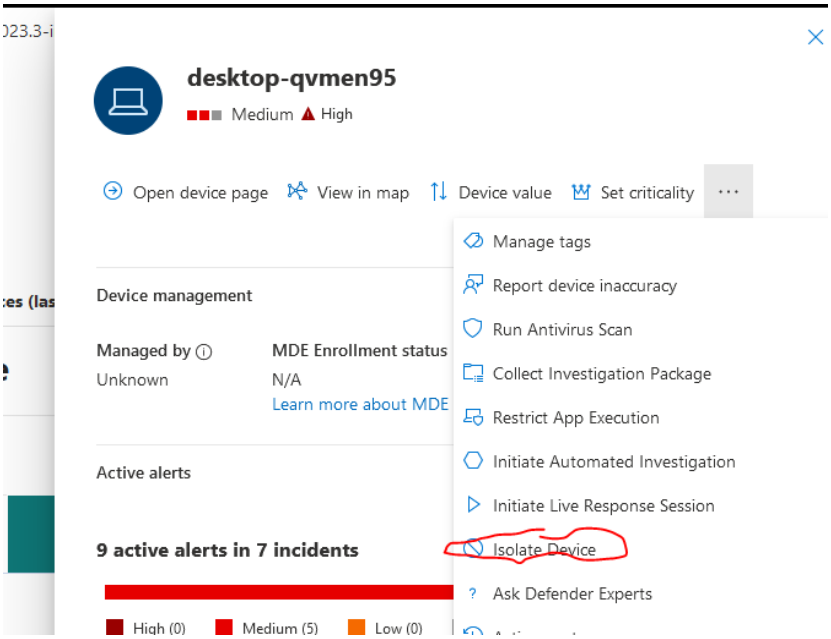
Goal: contain, eradicate, and recover the iso file.

Process:

- **Containment –**
  - quarantine the file

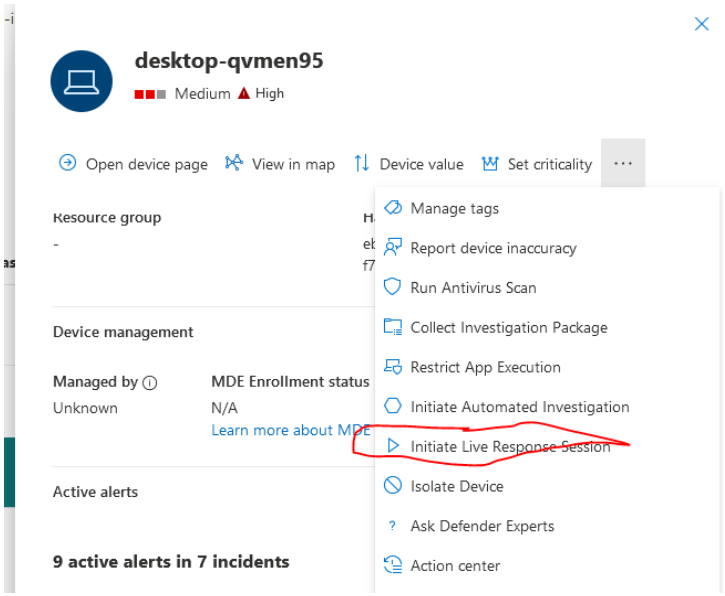


  - Isolate affected device

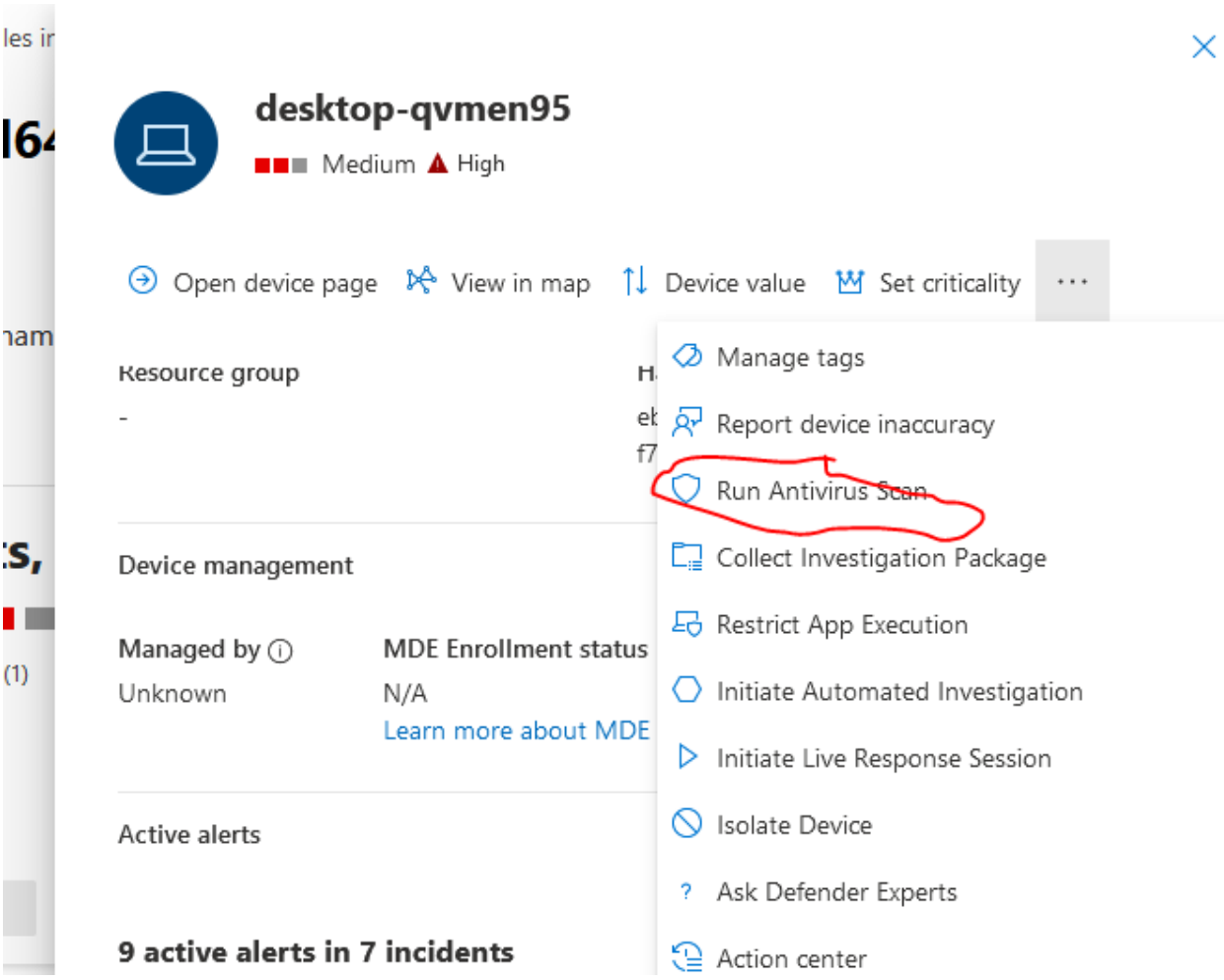


Eradication

- 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



- 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