Tailored: Windows Host Firewall Tampering

Incident Description

- This incident involves the changes of firewall settings.
- As reported by: Event ID 2003 — Firewall Rule Processing | Microsoft Learn

KQL

```
Event
| where EventLog == "Microsoft-Windows-Windows Firewall With Adv
| where EventID == 2003
```

Tactics and Techniques: Defense Evasion

- Impair Defenses: Disable or Modify System Firewall, Sub-technique T1562.004 - Enterprise | MITRE ATT&CK®

Initial Response Actions

- Verify the authenticity of the alert or report.
- Identify the altered settings.
- Determine how the settings were altered.
- Assess the potential impact of the incident.

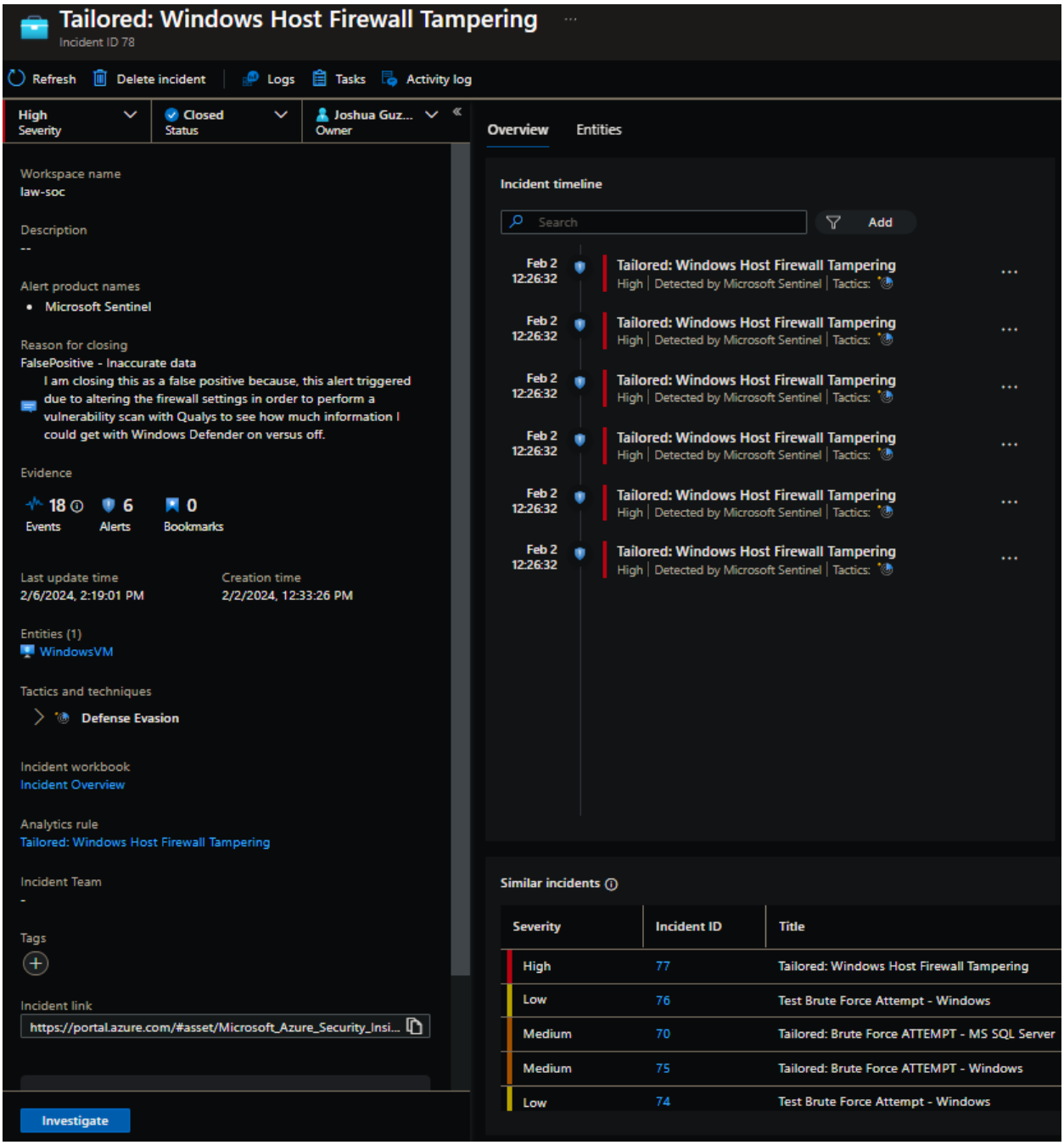
Containment and Recovery

- Revoke access to the firewall from the affected user or application immediately if unintended, otherwise skip to the documentation phase.

- Check for any other unauthorized access to the firewall and revoke it if necessary.
- Monitor other affected systems for any suspicious activity related to the incident.
- Identify the root cause of the incident and take corrective actions to prevent similar incidents from occurring in the future.

Document Findings and Close out Incident

- Example:



- Reason for closing in the example: I am closing this as a false positive because, this alert triggered due to altering the firewall settings in order to perform a vulnerability scan with Qualys to see how much information I could get with Windows Defender on versus off.