DEFENDER ADOPTION HELPER RESULTS

This report describes your current situation to adopt Sentinel in Defender in terms of Table Retention, Analytics Rules and Automations Rules.

Sentinel Environment in scope: **lawsentinel**

Report Generated on date: **2025-08-28**

DEFENDER DATA ANALYSIS

[WARNING] The table ***DeviceInfo*** has a retention of 30 days - no need to ingest this data in Sentinel

[OK] The table ***DeviceNetworkInfo*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceProcessEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceNetworkEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceFileEvents*** has a retention of 180 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceRegistryEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceLogonEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceImageLoadEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[WARNING] The table ***DeviceEvents*** has a retention of 30 days - no need to ingest this data in Sentinel

[WARNING] The table ***DeviceFileCertificateInfo*** has a retention of 30 days - no need to ingest this data in Sentinel

[OK] The table ***EmailEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***EmailUrlInfo*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***EmailAttachmentInfo*** has a retention of 730 days - need to be stored in Sentinel for more retention

[WARNING] The table ***EmailPostDeliveryEvents*** has a retention of 30 days - no need to ingest this data in Sentinel

[OK] The table ***UrlClickEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[WARNING] The table ***CloudAppEvents*** has a retention of 30 days - no need to ingest this data in Sentinel

[OK] The table ***IdentityLogonEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***IdentityQueryEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***IdentityDirectoryEvents*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***AlertInfo*** has a retention of 730 days - need to be stored in Sentinel for more retention

[OK] The table ***AlertEvidence*** has a retention of 730 days - need to be stored in Sentinel for more retention

Defender Data Analysis Score: 16/21 (76.19%)

ANALYTICS ANALYSIS

[WARNING] Fusion rules will be automatically disabled after Microsoft Sentinel is onboarded in Defender

[OK] The rule ***Phishing Email received by an active account*** is configured correctly

[OK] The rule ***Multiple attempts to jailbreak a workstation*** is configured correctly

[OK] The rule ***Malicious Script executed in High Privileged devices*** is configured correctly

[WARNING] The rule ***Office Policy tampering***doesn't generate incidents. The alerts aren't visible in the Defender portal. They appear in SecurityAlerts table in Advanced Hunting

Analytics Analysis Score: 3/5 (60%)

AUTOMATION RULES ANALYSIS

[WARNING] Change the trigger condition in the automation rule ***Forward High Risky incident to WE-SOC*** to *Alert Product Name*

[WARNING] Change the trigger condition in the automation rule ***Post incident in Teams*** from *Incident Title* to *Analytics Rule Name*

[OK] The automation rule ***Notify User's Manager*** is configured correctly

Automation Rule Analysis Score: 1/3 (33.33%)

FINAL SCORE

Total number of Controls : 29

Total number of Passed Controls : 20

Total number of Not Passed Controls : 9

Final Score: 20/29 (68.97%)