TABLE OF CONTENTS

Defender Adoption Helper Overview

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

Sentinel environments in scope:

- Workspace name: LAWSentinel
  Resource group name: sentinelrg
  Subscription id: xyz-xyz-xyz-xyz
- Workspace name: testlaw
  Resource group name: testrg
  Subscription id: xyz-xyz-xyz-xyz

Report Generated on date: **2025-09-05**

LAWSentinel environment

This section provides details about the following Sentinel environment:

- Workspace name: **LAWSentinel**
- Resource Group name: **sentinelrg**
- Subscription ID: **xyz-xyz-xyz-xyz**

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

[OK] The rule ***User on holiday accessed to sensitive info*** is configured correctly

Analytics Analysis Score: 4/6 (66.67%)

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%)

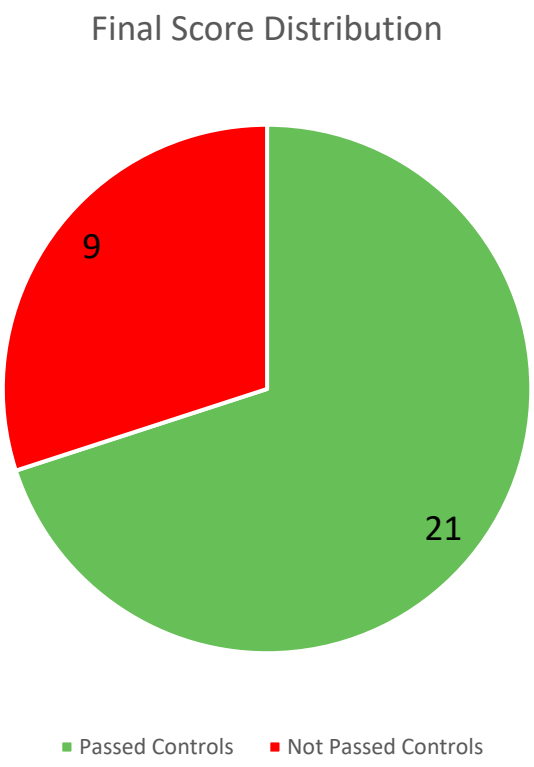
Final Score

Total number of Controls : 30

Total number of Passed Controls : 21

Total number of Not Passed Controls : 9

Final Score: 21/30 (70%)



testlaw environment

This section provides details about the following Sentinel environment:

- Workspace name: **testlaw**
- Resource Group name: **testrg**
- Subscription ID: **xyz-xyz-xyz-xyz**

Defender data analysis

[OK] The table ***DeviceInfo*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceNetworkInfo*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceProcessEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceNetworkEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceFileEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceRegistryEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceLogonEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceImageLoadEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***DeviceFileCertificateInfo*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***EmailEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***EmailUrlInfo*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***EmailAttachmentInfo*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***EmailPostDeliveryEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***UrlClickEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***CloudAppEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***IdentityLogonEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***IdentityQueryEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***IdentityDirectoryEvents*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***AlertInfo*** has a retention of 90 days - need to be stored in Sentinel for more retention

[OK] The table ***AlertEvidence*** has a retention of 90 days - need to be stored in Sentinel for more retention

Defender Data Analysis Score: 21/21 (100%)

Analytics Analysis

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

Analytics Analysis Score: 0/1 (0%)

Automation Rules Analysis

[WARNING] Change the trigger condition in the automation rule ***Close Automatically incident involving MC*** to *Alert Product Name*

Automation Rule Analysis Score: 0/1 (0%)

Final Score

Total number of Controls : 23

Total number of Passed Controls : 21

Total number of Not Passed Controls : 2

Final Score: 21/23 (91.3%)