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. The report analyses Sentinel environments, **considering them all good candidates to be Primary Workspaces. The choice depends on your needs.**

Sentinel environments in scope:

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

Defender XDR data
You can query and **correlate your Defender XDR logs** (30 days of default retention) **with third-party logs from Microsoft Sentinel without ingesting the Microsoft Defender XDR logs into Microsoft Sentinel.** If you have detection use cases that involve both Defender XDR and Microsoft Sentinel data, where you don't need to retain Defender XDR data for more than 30 days, Microsoft recommends creating custom detection rules that query data from both Microsoft Sentinel and Defender XDR tables.

Analytics Rules
Fusion rules will be automatically disabled after Microsoft Sentinel is onboarded to Defender However, you will not lose the alert correlation functionality. The alert correlation functionality previously managed by Fusion will now be handled by the Defender XDR engine, which consolidates all signals in one place. While the engines are different, they serve the same purpose.

If you have Microsoft Sentinel analytics rules configured to trigger alerts only, with incident creation turned off, these **alerts aren't visible in the Defender portal.** You can use the *SecurityAlerts* table to have visibilty about them.

Automation Rules
The Defender portal uses a unique engine to correlate incidents and alerts. When onboarding your workspace to the Defender portal, **existing incident names might be changed if the correlation is applied.** For this reason, change the trigger condition from *Incident Title* to *Analytics Rule Name*. Also the *Incident provider condition* property is removed, as all incidents have Microsoft XDR as the incident provider (the value in the *ProviderName* field).

Analytics Rules or Custom Detection Rules
This section does not contribute to the final score. Its purpose is to analyse the current Analytics Rules and their configuration to understand whether they can be migrated to Custom Detection Rules based on the features in Public Preview/General Availability as of today (September 12, 2025).

Report Generated on date: **2025-09-12**

LAWSentinel environment

This section provides details about the following Sentinel environment:

- Workspace name: **LAWSentinel**
- Resource Group name: **sentinelrg**
- Subscription ID: xyz-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*** from *Incident Provider* 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%)

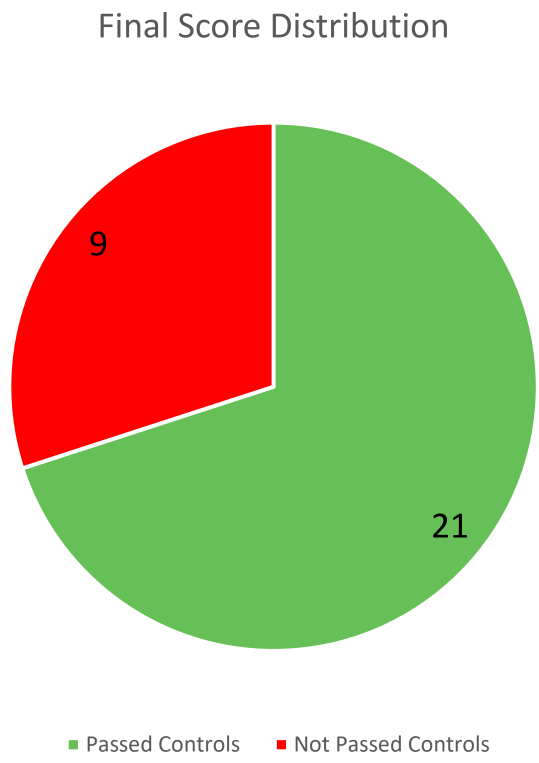
Final Score

Total number of Controls : 30

Total number of Passed Controls : 21

Total number of Not Passed Controls : 9

Final Score: 21/30 (70%)



Appendix - Analytics Rules or Scheduled Rules Analysis

Rule *Phishing Email received by an active account*

- **Entity Mapping Analysis**
  [WARNING] You can associate only one of the ***3*** mapped fields for the *Account entity*

- **Alert Details Override Analysis**
  [WARNING] Found an unsupported details override property - Custom Detection Rules doesn't support it

- **Incident Re-Opening Analysis**
  [OK] No incident reopening defined

- **Suppression Analysis**
  [WARNING] Suppression rule defined. Custom Detection Rules doesn't support it

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [WARNING] The scheduled rule is executed with a frequency or lookback not supported by Custom Detection Rules by default. If the rules uses only Sentinel data you can select a custom frequency in the Custom Detection Rule.

Rule *Multiple attempts to jailbreak a workstation*

- **Entity Mapping Analysis**
  [WARNING] You can associate only one of the ***2*** mapped fields for the *Host entity*

- **Alert Details Override Analysis**
  [WARNING] Found an unsupported details override property - Custom Detection Rules doesn't support it

- **Incident Re-Opening Analysis**
  [WARNING] Incident reopening defined. Custom Detection Rules doesn't support it

- **Suppression Analysis**
  [WARNING] Suppression rule defined. Custom Detection Rules doesn't support it

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [WARNING] The scheduled rule is executed with a frequency or lookback not supported by Custom Detection Rules by default. If the rules uses only Sentinel data you can select a custom frequency in the Custom Detection Rule.

Rule *Malicious Script executed in High Privileged devices*

- **Entity Mapping Analysis**
  [WARNING] You can associate only one of the ***2*** mapped fields for the *File entity*

- **Alert Details Override Analysis**
  [OK] No alert details override defined

- **Incident Re-Opening Analysis**
  [OK] No incident reopening defined

- **Suppression Analysis**
  [WARNING] Suppression rule defined. Custom Detection Rules doesn't support it

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [WARNING] The scheduled rule is executed with a frequency or lookback not supported by Custom Detection Rules by default. If the rules uses only Sentinel data you can select a custom frequency in the Custom Detection Rule.

Rule ***Office Policy tampering***

- **Entity Mapping Analysis**
  [OK] No entity mapping defined

- **Alert Details Override Analysis**
  [OK] No alert details override defined

- **Incident Re-Opening Analysis**
  [OK] No incident reopening defined

- **Suppression Analysis**
  [OK] No suppression rule defined

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [OK] The scheduled rule is executed every 12 hours and looks back 2 days - Custom Detection Rules supports it

Rule ***User on holiday accessed to sensitive info***

- **Entity Mapping Analysis**
  [OK] No entity mapping defined

- **Alert Details Override Analysis**
  [OK] Alert display name override defined. Custom Detection Rules supports it

[WARNING] Found an unsupported details override property - Custom Detection Rules doesn't support it

- **Incident Re-Opening Analysis**
  [OK] No incident reopening defined

- **Suppression Analysis**
  [OK] No suppression rule defined

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [WARNING] The scheduled rule is executed with a frequency or lookback not supported by Custom Detection Rules by default. If the rules uses only Sentinel data you can select a custom frequency in the Custom Detection Rule.

Rule *NRT Access to Break Glass Account*

- **Entity Mapping Analysis**
  [OK] No entity mapping defined

- **Alert Details Override Analysis**
  [OK] No alert details override defined

- **Incident Re-Opening Analysis**
  [OK] No incident reopening defined

- **Suppression Analysis**
  [OK] No suppression rule defined

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [WARNING] The scheduled rule is executed with a frequency or lookback not supported by Custom Detection Rules by default. If the rules uses only Sentinel data you can select a custom frequency in the Custom Detection Rule.

- **NRT Rules Analysis**
  [WARNING] If the rule uses only Defender data and target one single table, you can consider to migrate it to a Custom Detection Rule in Defender

testlaw environment

This section provides details about the following Sentinel environment:

- Workspace name: **testlaw**
- Resource Group name: **testrg**
- Subscription ID: xyz-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*** from *Incident Provider* to *Alert Product Name*

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

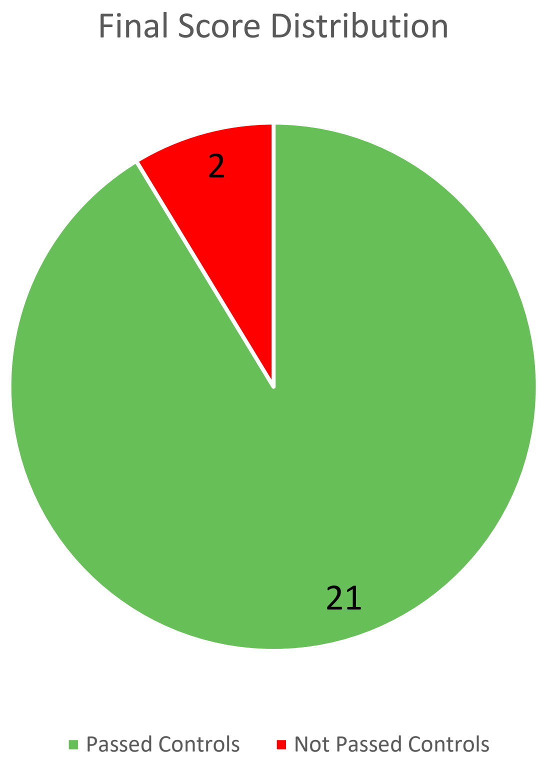
Final Score

Total number of Controls : 23

Total number of Passed Controls : 21

Total number of Not Passed Controls : 2

Final Score: 21/23 (91.3%)



Appendix - Analytics Rules or Scheduled Rules Analysis

Rule *testNRT*

- **Entity Mapping Analysis**
  [OK] No entity mapping defined

- **Alert Details Override Analysis**
  [OK] No alert details override defined

- **Incident Re-Opening Analysis**
  [OK] No incident reopening defined

- **Suppression Analysis**
  [OK] No suppression rule defined

- **Threshold Analysis**
  [WARNING] Trigger threshold defined. Custom Detection Rules doesn't support it

- **Lookback Analysis**
  [WARNING] The scheduled rule is executed with a frequency or lookback not supported by Custom Detection Rules by default. If the rules uses only Sentinel data you can select a custom frequency in the Custom Detection Rule.

- **NRT Rules Analysis**
  [WARNING] If the rule uses only Defender data and target one single table, you can consider to migrate it to a Custom Detection Rule in Defender