Compliance Manager Default Alert Policy Delay

Last updated by | Paulo Santana | Mar 30, 2023 at 7:31 PM CDT

Compliance Manager Default Alert Policy "Delay"

Contents

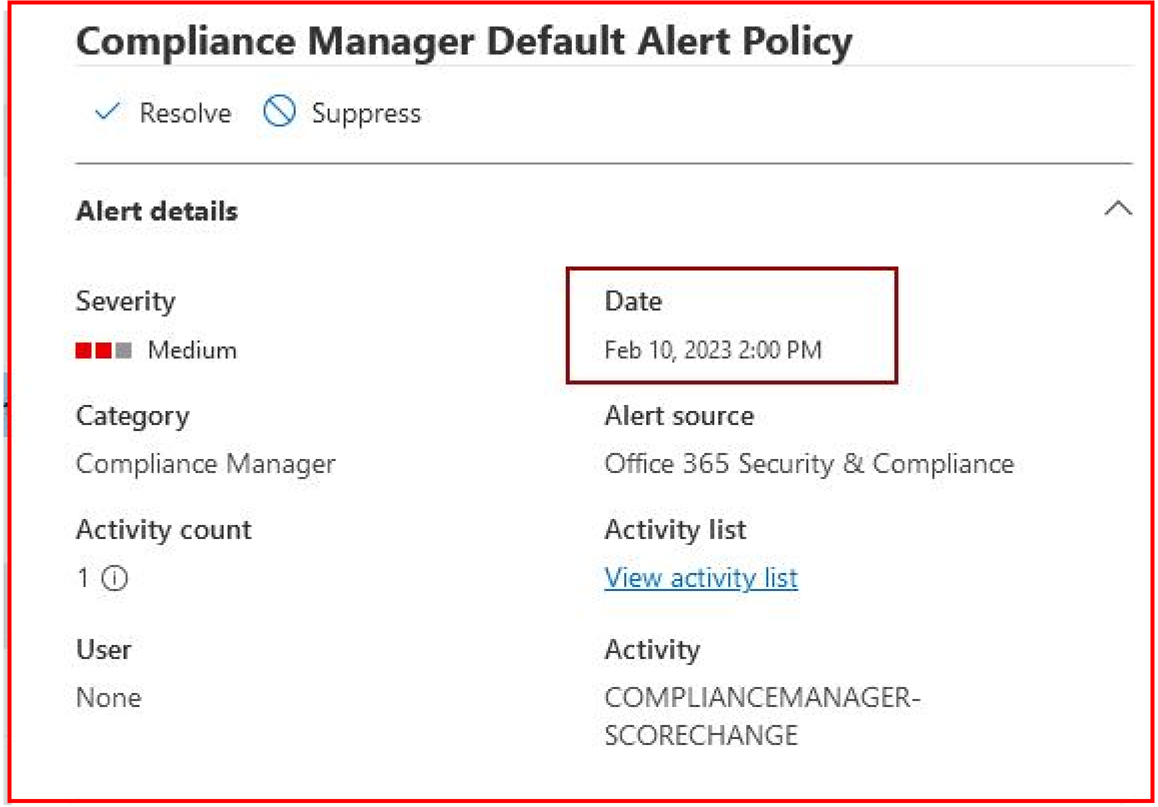
- Description
  - Main Section

Description

This section outlines a common mistake regardintg the "Compliance Manager Default Alert Policy "Delay" that can cause customers to believe there is a delay ingesting the related incident in Microsoft Sentinel.

Main Section

The Purview policy "Compliance Manager Default Alert Policy" will generate alerts in M365D like the one below:



Compliance Manager Default Alert Policy

Alert details

Severity
■■■ Medium

Date
Feb 10, 2023 2:00 PM

Category
Compliance Manager

Alert source
Office 365 Security & Compliance

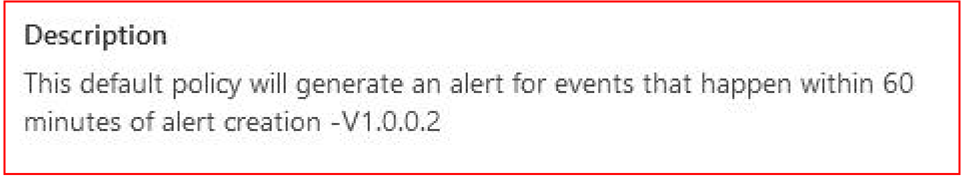
Activity count
1 ⓘ

Activity list
View activity list

User
None

Activity
COMPLIANCEMANAGER-SCORECHANGE

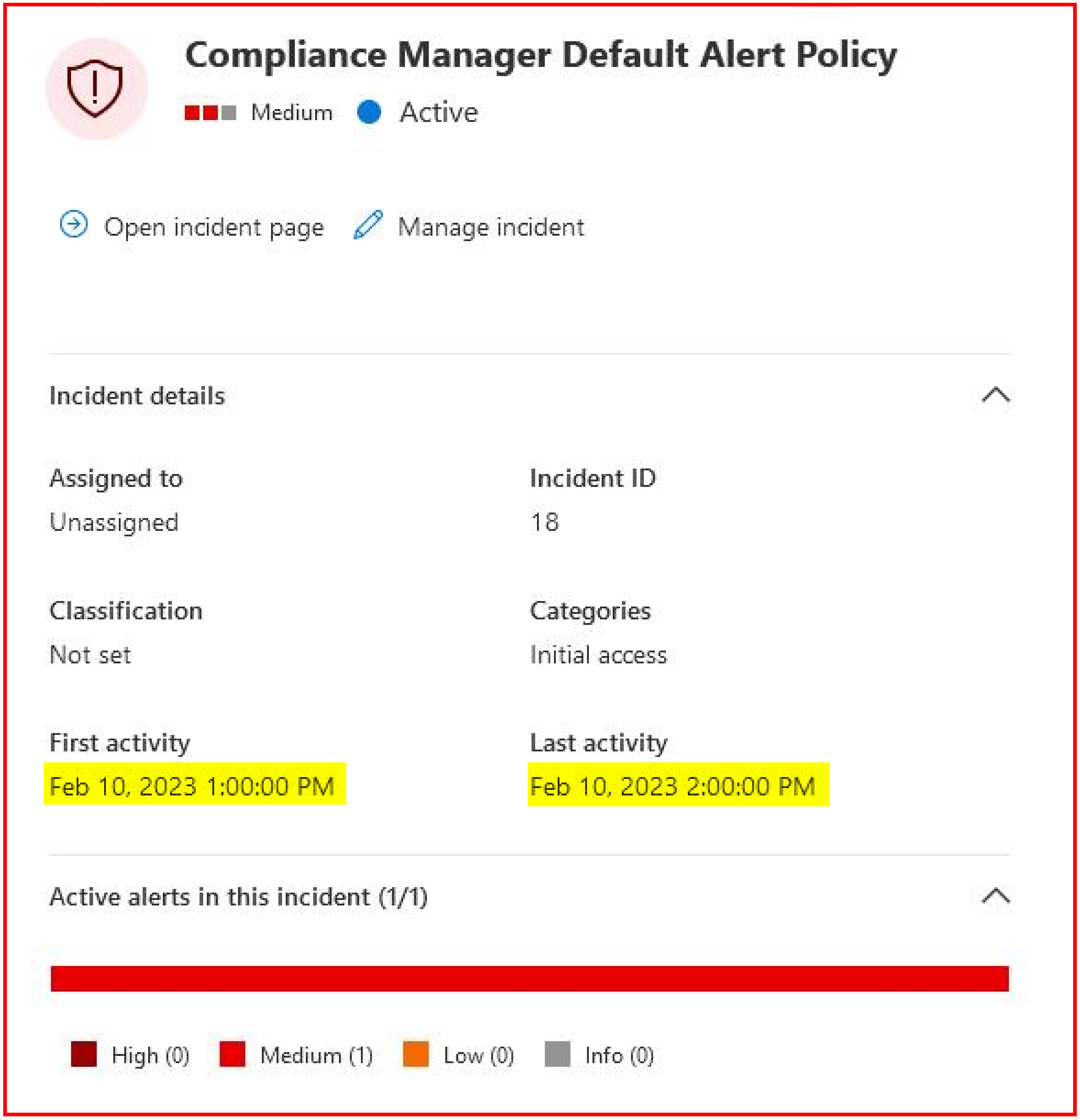
This policy runs every hour and will create an alert if there is a finding:



Description

This default policy will generate an alert for events that happen within 60 minutes of alert creation -V1.0.0.2

The Incident will show up in MDE as below without showing what time the alert was generated. (No creation time, so customers can confuse "First activity" with creation time, which does not match Time Generated in Sentinel):



Compliance Manager Default Alert Policy

Medium ● Active

Open incident page   Manage incident

Incident details

Assigned to
Unassigned

Incident ID
18

Classification
Not set

Categories
Initial access

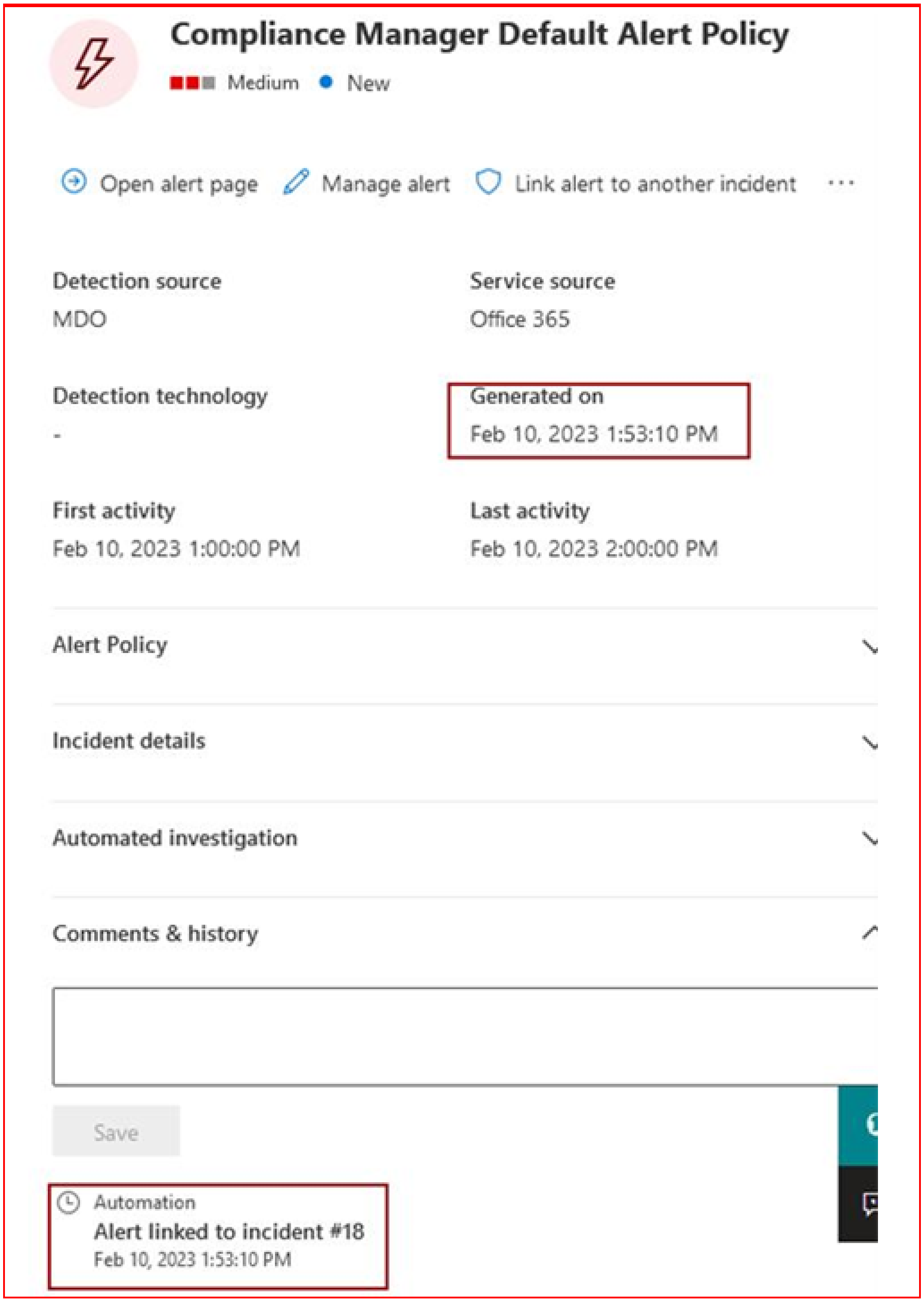
First activity
Feb 10, 2023 1:00:00 PM

Last activity
Feb 10, 2023 2:00:00 PM

Active alerts in this incident (1/1)

High (0)   Medium (1)   Low (0)   Info (0)

If we expand the incident and look at the **Alert**, we can see the "Generated on" field, and if you scroll down you see what time the alert was added to the **Incident**:



Compliance Manager Default Alert Policy

■■■ Medium ● New

Detection source
MDO

Service source
Office 365

Detection technology
-

Generated on
Feb 10, 2023 1:53:10 PM

First activity
Feb 10, 2023 1:00:00 PM

Last activity
Feb 10, 2023 2:00:00 PM

Alert Policy

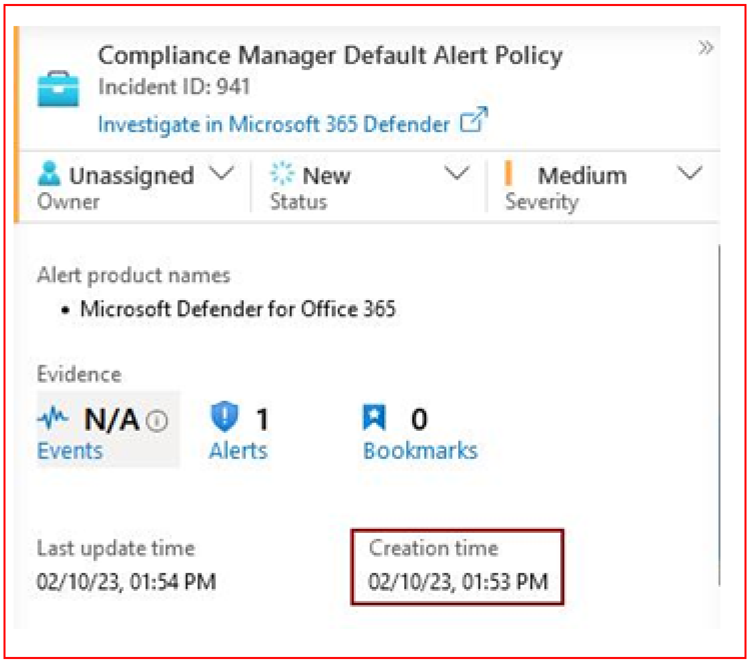
Incident details

Automated investigation

Comments & history

Automation
Alert linked to incident #18
Feb 10, 2023 1:53:10 PM

In this example, we can see below that the Incident was created in Sentinel at the exact same time as it was added to the incident in M365D and there was no delays:



Compliance Manager Default Alert Policy

Incident ID: 941

Investigate in Microsoft 365 Defender

Unassigned
Owner

New
Status

Medium
Severity

Alert product names

- Microsoft Defender for Office 365

Evidence

N/A Events | 1 Alerts | 0 Bookmarks

Last update time
02/10/23, 01:54 PM

Creation time
02/10/23, 01:53 PM

Contributor Name	Details	Date
Paulo Santana	Created this wiki page	2023-03-30