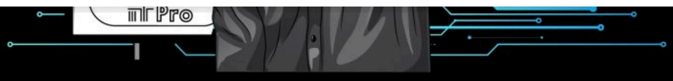


Hunting Malicious Windows Defender Activity

Posted on March 4, 2020 by Craig

Recently I was demo-ing Azure Sentinel to a large organization, and someone asked me "what if an attacker manages to compromise my system and disabled Windows Defender"

Well…what if they do, how can we flag this and investigate and remediate…why would someone intentionally disable Anti-Malware protection…inside job or clever exploitation using a Phishing technique to download a payload??

I've wrote this blog to hopefully help you combat and protect yourself from this type of scenario.

Below are some basic pre reqs to be comfortable following this blog:

Pre Reqs & Assumptions:

- Azure Experience (essential)
- IT Security Experience (essential)
- Log Analytics (essential)
- Azure Sentinel (essential)

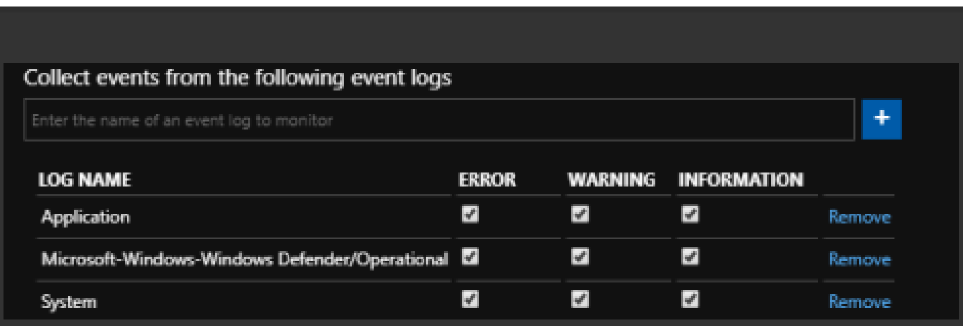
Follow me on LinkedIN

Categories

- Automation (11)
- Azure (85)
- Azure Security (36)
- Azure Sentinel (43)
- CMD (1)
- cybersecurity (5)
- Exchange (2)
- Exchange 2010 (2)
- Microsoft Sentinel (18)
- OSD Deployment (1)
- Powershell (17)
- SCCM (7)
- SCOM (1)
- Software (1)
- Terraform (1)
- Windows 10 (1)

Recent Posts

- How to Detect North Korean Threat Actors Kimsuky
  October 3, 2024



Collect events from the following event logs

Enter the name of an event log to monitor +

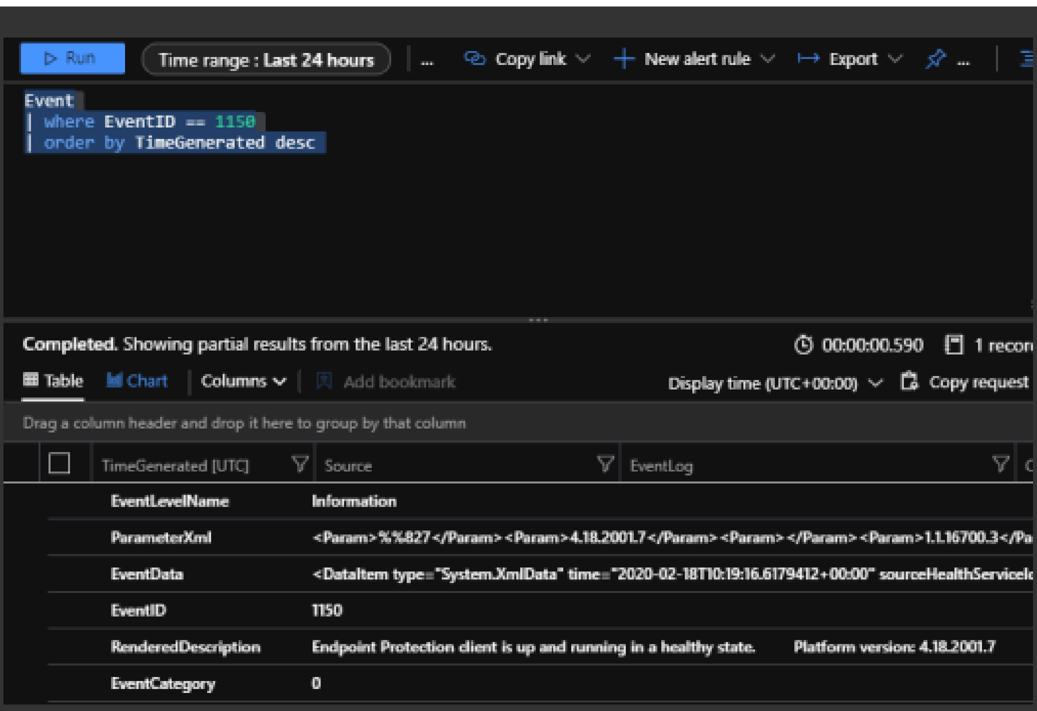
LOG NAME	ERROR	WARNING	INFORMATION	
Application	☑	☑	☑	Remove
Microsoft-Windows-Windows Defender/Operational	☑	☑	☑	Remove
System	☑	☑	☑	Remove

Once this is saved, it will take approximately 15 minutes to start collecting the data from your VM to Log Analytics.

Let's jump over to our Sentinel Workspace, and Click Logs.

We can test that our Windows Defender is reporting by running a simple query which the EventID 1150 will report on the Endpoint Protection being in a healthy state.

```
Event
| where EventID == 1150
| order by TimeGenerated desc
```



```
Event
| where EventID == 1150
| order by TimeGenerated desc
```

Completed. Showing partial results from the last 24 hours. 00:00:00.590 1 recor

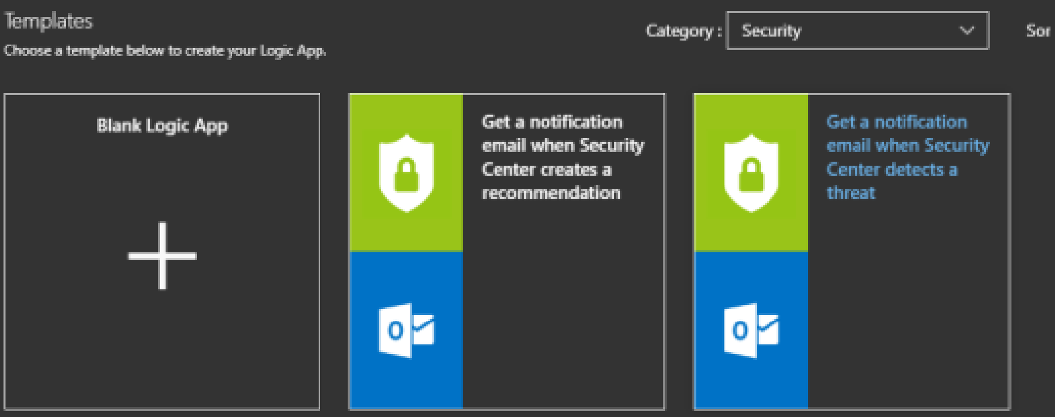
TimeGenerated [UTC]	Source	EventLog
EventLevelName	Information	
ParameterXml	<Param>%%827</Param><Param>4.18.2001.7</Param><Param></Param><Param>1.1.16700.3</Pa	
EventData	<DataItem type="System.XmlData" time="2020-02-18T10:19:16.6179412+00:00" sourceHealthServiceIc	
EventID	1150	
RenderedDescription	Endpoint Protection client is up and running in a healthy state. Platform version: 4.18.2001.7	
EventCategory	0	

Now we need to write a query which will alert us if any configuration changes happen on Windows Defender.

Before we create our Analytic Rule, we need to create a Logic App/Playbook which will alert us via an email that windows defender has had some configuration changes.

Let's go to Playbook and click "Add Playbook" give your playbook a name and click create.

Select "Blank Logic App"



Templates
Choose a template below to create your Logic App.

Category : Security

Get a notification email when Security Center creates a recommendation

Get a notification email when Security Center detects a threat

I'd like to receive and email when Sentinel picks up this alert.

August 29, 2024

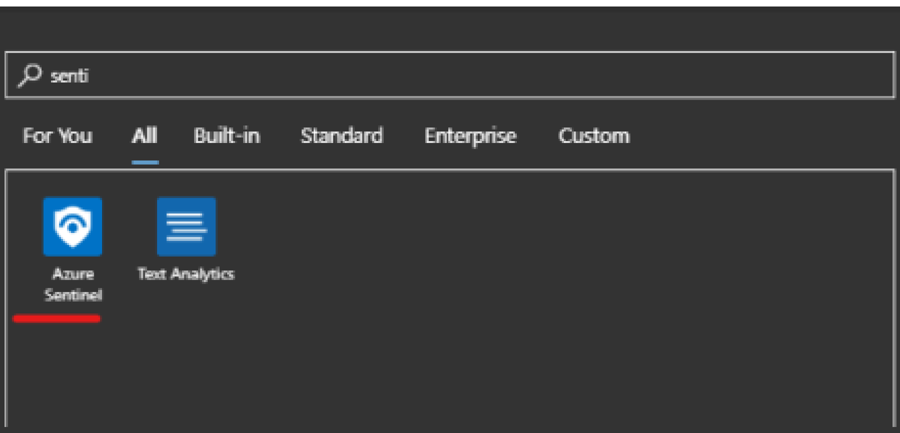
- Securing Azure AI workloads with Azure Policy
June 21, 2024

Tags

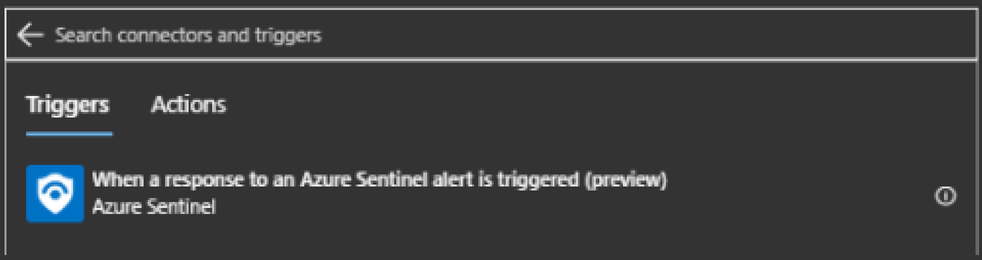
- #alwayscloud
- #alwaysready
- #alwaysthinking
- armtemplates
- Azure
- azureautomation
- azuredevops
- azure move storage account
- azurepowershell
- azure resource groups
- azureresourcemanager
- azurerm
- azurescript
- azuresecurity
- azuresecuritycenter
- azuresentinel
- Powershell
- Script
- Scripting
- sentinel

Archives

- October 2024
- September 2024
- August 2024
- June 2024
- May 2024
- April 2024
- March 2024
- February 2024
- January 2024
- December 2023
- November 2023
- October 2023
- September 2023
- August 2023
- July 2023
- June 2023

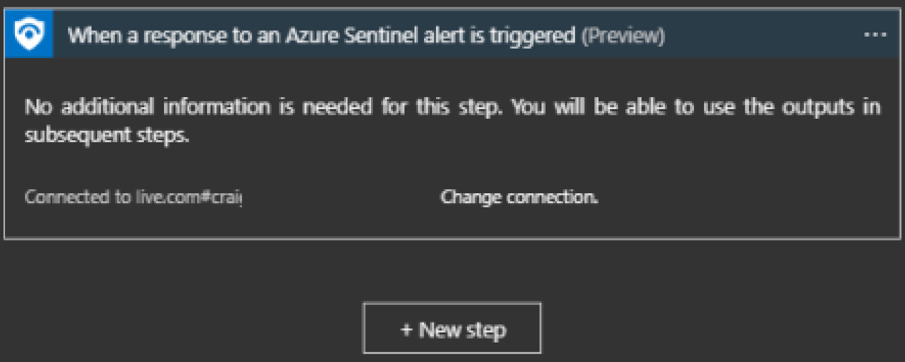


At the time of writing this there is only 1 Trigger for Sentinel.



When a response to an Azure Sentinel alert is triggered (preview)
Azure Sentinel

Make your connection to Sentinel


When a response to an Azure Sentinel alert is triggered (Preview)

No additional information is needed for this step. You will be able to use the outputs in subsequent steps.

Connected to live.com#craij

Next click + New Step and search for YOUR email action, for me, I'll be using Outlook.com

Fill in the Body, Subject and To section with which ever information you'd like to be emailed once an alert is triggered.

I've done some basic formatting inside the body of the email, so my email alert makes sense and is laid out nicely.

Click Save, we can now attach our playbook to the security query, for us to be notified of this we need to create a Scheduled Analytic Query Rule.

Let's go to our Sentinel Dashboard and click "Analytics"

July 2021
June 2021
May 2021
April 2021
March 2021
February 2021
December 2020
November 2020
October 2020
August 2020
July 2020
May 2020
March 2020
February 2020
November 2019
September 2019
June 2019
April 2019
February 2019
January 2019
November 2018
August 2018
June 2018
May 2018
April 2018
March 2018
December 2017
October 2017
September 2017
July 2017
June 2017
April 2017
February 2017
November 2016
October 2016
September 2016
August 2016
July 2016
June 2016
March 2016
January 2016
December 2015
November 2015
October 2015
September 2015
July 2015
May 2015

Let's create a New Rule.

I'm only just interested in obtaining information on the following ID's that have any relevance to being disabled are expired:

Event ID: 5101
Symbolic name: MALWAREPROTECTION_DISABLED_EXPIRED_STATE

Event ID: 5012
Symbolic name: MALWAREPROTECTION_ANTIVIRUS_DISABLED

Event ID: 5010
Symbolic name: MALWAREPROTECTION_ANTISPYWARE_DISABLED

Event ID: 5001
Symbolic name: MALWAREPROTECTION_RTP_DISABLED
Realistically these ID's should never appear, if they do…you know something is wrong.

So once we've captured them Event ID's we need to enter these into our Rule Logic, this will be our query which is below.

```
Event
| where EventID in (5101, 5001, 5012, 5010)
| order by TimeGenerated desc
```

For now I'll have the ability for alerts to trigger incidents, this way I get it displayed onto my dashboard screen.

Let's select are recently created Playbook above.

Next click review and create.

Now let's get into the juicy stuff, below is a few lines of simple PowerShell that will disable Microsoft Windows Defender
NOTE please don't use this on a production VM or your own machine!!

Before that we can see that Defender has a green tick, all healthy and running nicely.

So let's execute the code below.

```
Set-ExecutionPolicy Unrestricted -Force
Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference -DisableRemovableDriveScanning $true
Set-MpPreference -PUAProtection 1
New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows Def
```

Now after running all that, you should see a bunch of Pops notifying you that defender isn't running and it should turn Red (or have a red X)

Let's hop back to our Sentinel dashboard and check the situation out.

So we can see straight away that our Incident blade in Sentinel has captured the Analytic alert we've configured.

And after 1 or so minutes an email lands in my inbox.

Coupling all of the above will help defend how you alert and respond too Malicious Defender Activity with Azure Sentinel.

#alwayssecurity #alwaysready #alwayscloud #alwaysazure

Follow

Share this:

Twitter Facebook

Loading...

Azure Defender and Azure Sentinel Alerts Bi-Directional Sync
July 13, 2021
In "Azure"

Receive SMS Alerts from Azure Sentinel for Critical Incidents
July 15, 2020
In "Azure"

Azure Sentinel Solution Packages!!
May 13, 2021
In "Azure"

Posted in Azure, Azure Security, Azure Sentinel Tagged #alwayscloud, #alwaysready, #alwaysthinking, atp, Azure, azureautomation, azuredevops, azurescript, azuresecurity, azuresecuritycenter, azuresentinel, defender, hunting, huntingusb, maliciousactivity, Powershell, Script, Scripting, sentinel, sentinelhunting, windowsdefender

←Hunting USB Devices with Azure Sentinel Part 2

Azure Identity + Security→