Lab 5

Antivirus and Malware Scanning and Compliance

Protect and test all systems against malware and regularly update antivirus software or programs

Summary:

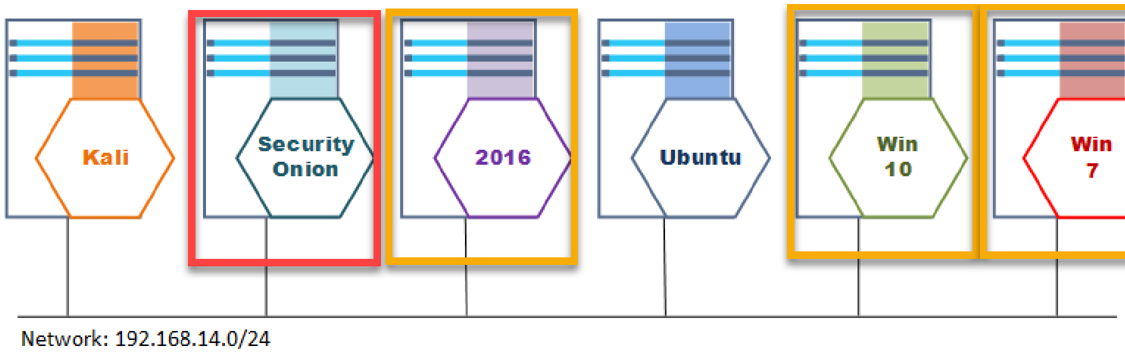
Antivirus software capable of detecting, removing and protecting against all known types of malware (e.g. viruses, worms and Trojans) must be used on all systems commonly affected by malware to protect them from threats. For systems not commonly affected by malware, evolving malware threats should be periodically evaluated to determine if antivirus software is needed. Antivirus mechanisms must be maintained and kept actively running, and should only be disabled if formally authorized for a specific purpose.

Lab Setup:

Security onion is collecting log data from all of the systems on the network. In this exercise we will be filtering these logs to confirm compliance that Windows Defender Antivirus Definitions are being updated as required. We can build a simple filter to search for the installation of KB2267602 which identifies a Defender Definition update. Once found, we will check the install dates to be sure that installation is happening promptly within the guidelines of our policy.

PCI_DSS Mapping:

5.2 Ensure that all anti-virus mechanisms are maintained as follows:
- Are kept current,
- Perform periodic scans
- Generate audit logs which are retained per PCI DSS Requirement 10.7



Windows Logs:

Common events:

We use this to find any Windows Defender Definition Updates.

[data.EventChannel.EventData.updateTitle:]

KB Number	Definition
KB2267602	EVERY Windows Defender definition update Note: Will usually appear once a day for new malware definitions.

In Kibana:

Key Fields for Parsing Defender Definitions:

Note: This is very similar to parsing any other event but is specialized for this.

Field	**Description**
data.EventChannel.System.ProviderName	The Windows Event Viewer log source **[Microsoft-Windows-WindowsUpdateClient/Operational]**
event_id	The Windows Event ID
data.EventChannel.EventData.updateTitle	This is the Windows Update Name (search for KB2267602)
data.EventChannel.System.SystemTime	The Time an Event was logged to the windows machine (Remember all times on Sec Onion are UTC) vs likely timezone setting on Windows machine. To set timezone: Management -> Advanced Settings.

Basic Search strings:

To find a specific event_id:

```
>_ event_id:<id number.>
```

Audit HowTo:

To find all Windows Defender Update Events:

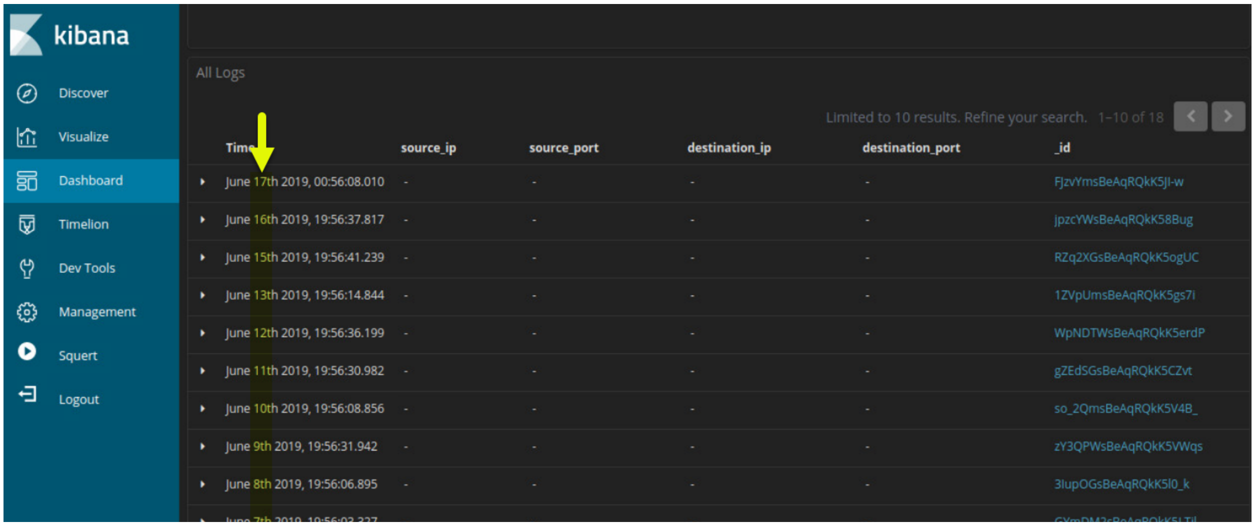
```
>_ data.EventChannel.EventData.updateTitle:KB2267602
```

To find all Windows Defender Update Events on a specific machine:

```
>_ data.EventChannel.EventData.updateTitle:KB2267602 AND agent.ip:192.168.14.105
```

We want to confirm that the Windows Defender Updates are being installed on a regular basis.

What you are looking for if the updates are running properly:
The updates should run almost once a day up to the current date. If not the machine you are auditing needs to be checked.



All Logs

Limited to 10 results. Refine your search. 1-10 of 18

Time	source_ip	source_port	destination_ip	destination_port	_id
June 17th 2019, 00:56:08.010	-	-	-	-	FJzvYmsBeAqRQkK5Jl-w
June 16th 2019, 19:56:37.817	-	-	-	-	jpzcYWsBeAqRQkK58Bug
June 15th 2019, 19:56:41.239	-	-	-	-	RZq2XGsBeAqRQkK5ogUC
June 13th 2019, 19:56:14.844	-	-	-	-	1ZVpUmsBeAqRQkK5gs7i
June 12th 2019, 19:56:36.199	-	-	-	-	WpNDTWsBeAqRQkK5erdP
June 11th 2019, 19:56:30.982	-	-	-	-	gZEdSGsBeAqRQkK5CZvt
June 10th 2019, 19:56:08.856	-	-	-	-	so_2QmsBeAqRQkK5V4B_
June 9th 2019, 19:56:31.942	-	-	-	-	zY3QPWsBeAqRQkK5VWqs
June 8th 2019, 19:56:06.895	-	-	-	-	3lupOGsBeAqRQkK5l0_k
June 7th 2019, 19:56:03.327					GYmDM2sBeAqRQkK5LTil

ToDo:

1. Have any of the Windows machines never received a Windows Defender Definition Update? If so which machine: ____

2. If not receiving updates what can this indicate? ___________________________

3. Are there any Windows machines on the network Not receiving Windows Defender Updates? ____