Latest Version: 7.0

Question: 1

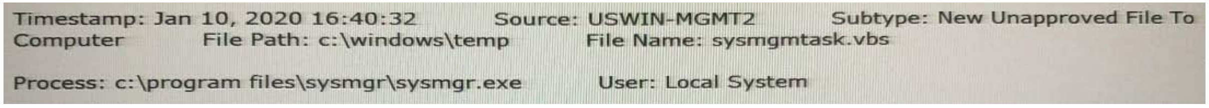
An administrator needs to check configurations using Audit across several policies and locations within the organization.
How can the administrator run the query to only these specific devices?

A. Specify endpoints on the query by selecting the check box for each device.
B. Specify endpoints on the query by typing the sensor name into the text box, selecting the device. Repeat as necessary for all devices.
C. Specify the policy for the endpoints on the query, and then select the check box for each device.
D. Specify the policy for the endpoints on the query, and then type the sensor name into the text box, selecting the devices. Repeat as necessary for all devices.

Answer: D

Question: 2

A process wrote an executable file as detailed in the following event:



```
Timestamp: Jan 10, 2020 16:40:32      Source: USWIN-MGMT2       Subtype: New Unapproved File To
Computer        File Path: c:\windows\temp          File Name: sysmgmtask.vbs

Process: c:\program files\sysmgr\sysmgr.exe          User: Local System
```

Which rule type should be used to ensure that files of the same name and path, written by that process in the future, will not be blocked when they execute?

A. Trusted Path
B. File Creation Control
C. Advances (Write-Ignore)
D. Trusted Publisher

Answer: B

Question: 3

Which enforcement level does not block unapproved files but will block files that have been specifically banned?

A. Medium Enforcement
B. Disabled
C. Visibility

D. Low Enforcement

Answer: B

The protection level applied to computers running the App Control
Agent. A range of levels from High (Block Unapproved) to None
(Disabled) enable you to specify the level of file blocking required.

Question: 4

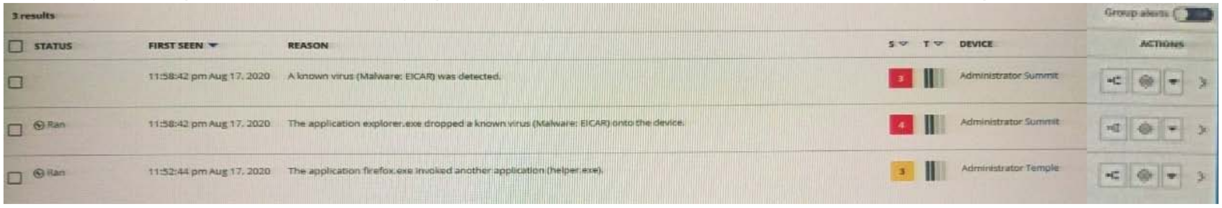
An administrator has updated a Threat Intelligence Report by turning it into a watchlist and needs to disable (Ignore) the old Threat Intelligence Report.
Where in the UI is this action not possible to perform?

A. Search Threat Reports Page
B. Threat Intelligence Feeds Page
C. Threat Report Page
D. Triage Alerts Page

Answer: B

Question: 5

An analyst navigates to the alerts page in Endpoint Standard and sees the following:



3 results

□	STATUS	FIRST SEEN	REASON	S	T	DEVICE
□		11:58:42 pm Aug 17, 2020	A known virus (Malware: EICAR) was detected.	3		Administrator Summit
□	Ran	11:58:42 pm Aug 17, 2020	The application explorer.exe dropped a known virus (Malware: EICAR) onto the device.	4		Administrator Summit
□	Ran	11:52:44 pm Aug 17, 2020	The application firefox.exe invoked another application (helper.exe).	3		Administrator Temple

What does the yellow color represent on the left side of the row?

A. It is an alert from a watchlist rather than the analytics engine.
B. It is a threat alert and warrants immediate investigation.
C. It is an observed alert and may indicate suspicious behavior.
D. It is a dismissed alert within the user interface.

Answer: A