SOPHOS
Security made simple.

Sophos Endpoint Detection and Response

Early Access Program - **Testing Guide**

Prerequisites for performing exercises:

- 2 Endpoints – both enrolled in EDR EAP
- Download 'Sophos HIPS Test (exe)'***** from http://sophostest.com on both endpoints
- Download 'Unknown.exe'***** from: http://sophostest.com/reputation/index.html on both endpoints
- Wait about 20 minutes before running tests

***** EAP endpoints will be enhanced so that details on detected or suspicious portable executable files will be frequently sent to Sophos Central (approx. every 15 minutes). This then gives the admin the ability to search for file names or SHA-256 hashes to identify which endpoints have seen those suspect files to investigate further or take action. Searches can also be run on processes from within an existing Threat Case (formerly RCA). Keep in mind that Sophos Central will only store details on portable executable files that have a bad or uncertain reputation and therefore will only return results on those files where a query is matched**.** The test files downloaded for these exercises have an uncertain reputation and therefore details will be sent to Central on those files.

Exercise 1 will walk through a scenario where there has been an endpoint detection event and will walk through the typical investigation of a detection and how new capabilities can be leveraged for this investigation

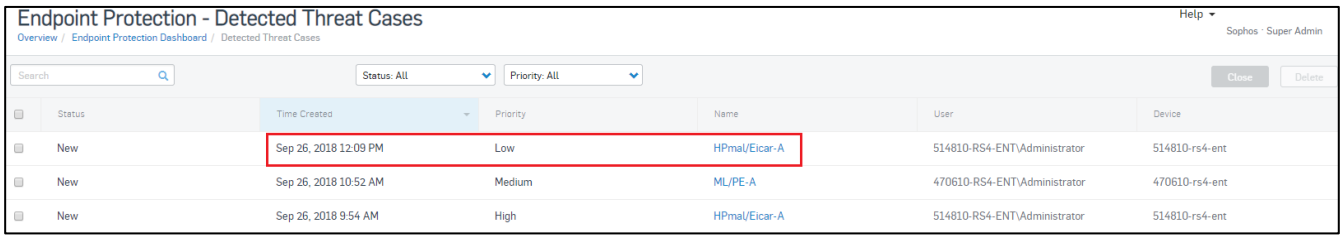
New Functionality Tested: Threat Case new look and feel, Requesting Labs latest intelligence, Admin Led Isolation, Item Search Result from Threat Case

1. Run Sophos HIPs Test (exe) on endpoint 1
    a. -Detection- Toast message displays bottom right corner

2. Within a few minutes a new Threat Case should appear in Sophos Central for the detection, Check Sophos Central > Endpoint Protection > Threat Case.

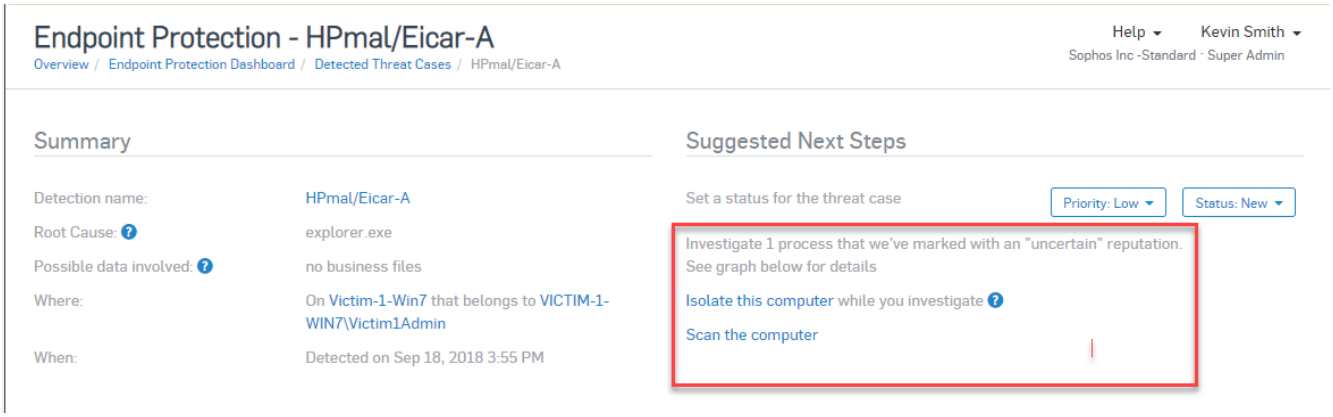
   Note: The Threat Case is the new name for what used to be referred to as the Root Cause Analysis (RCA). We have implemented several additional features to make it easier for admins to conduct deeper investigation into detected threats.

3. When the Threat Case has been uploaded you should see the most recent Threat Case named “HPmal/Eicar-A”

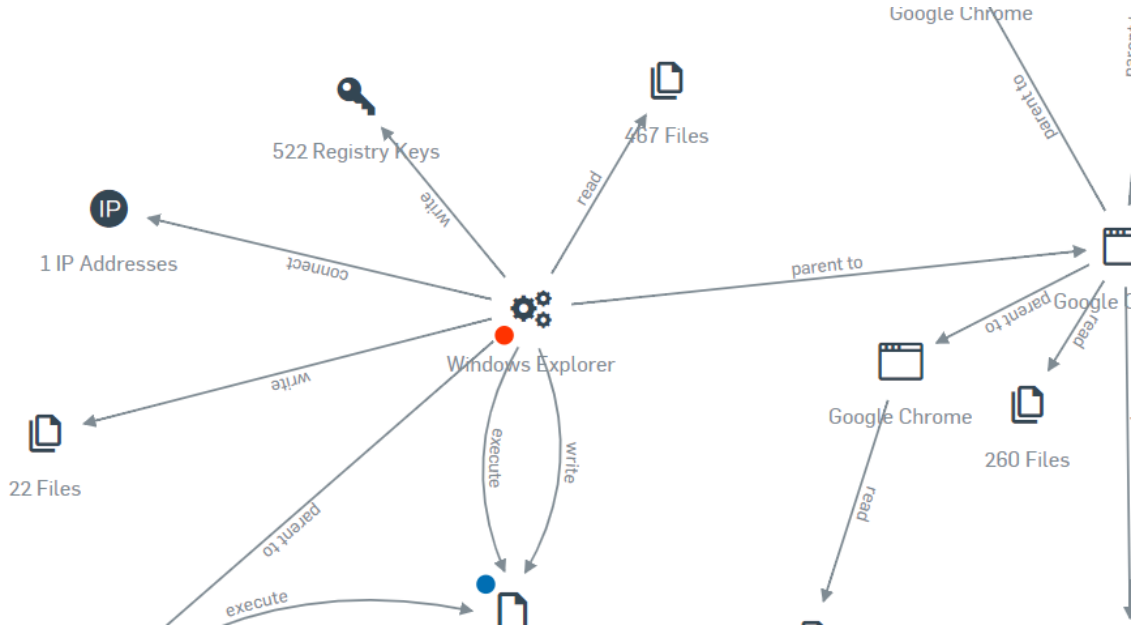


On Entering the Threat Case, note the new look of the threat case, there are a few new things to be aware of.

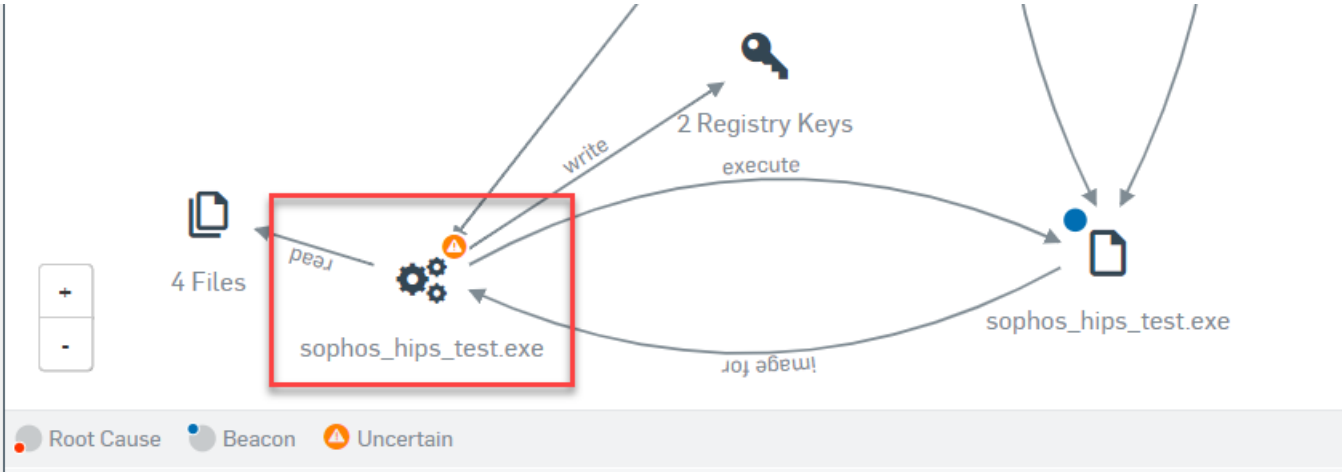
Note the new ‘Suggested Next Steps’ section that highlights any processes in the threat chain that have an uncertain reputation which may require further investigation, also note the new actions available in the suggested next steps.



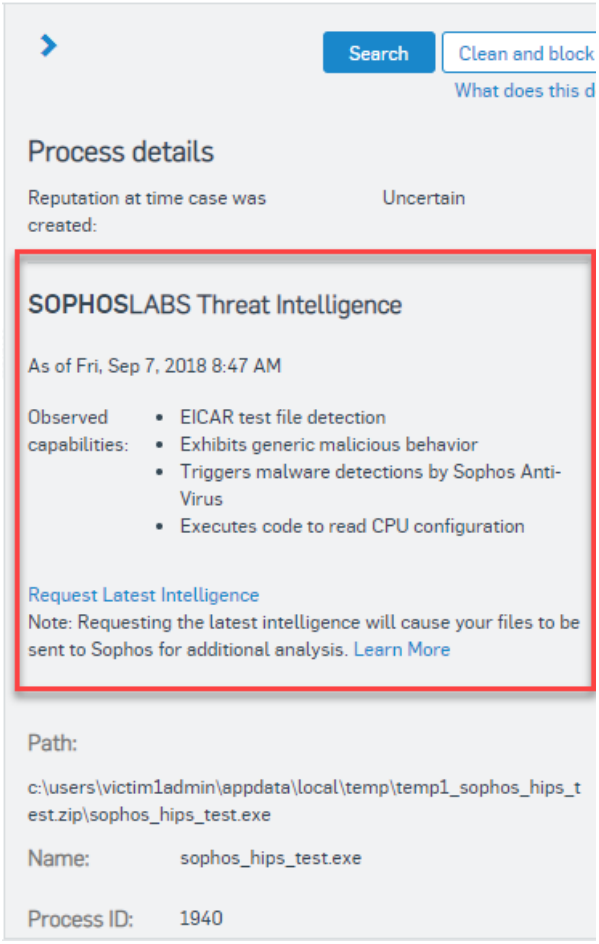
New iconography is used to represent the different types of artefacts in the Threat Cases:



Finally note how processes with an uncertain reputation are also highlighted in the graph to distinguish artefacts that may warrant further investigation:

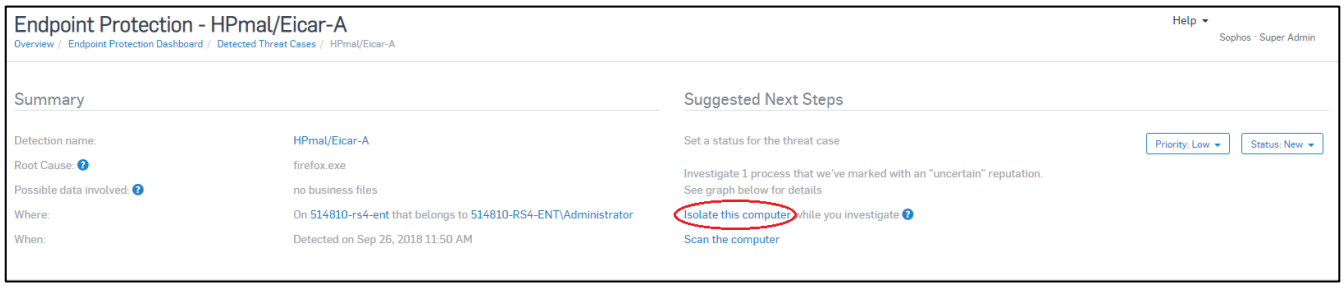


4. Click on the Sophos_hips_test.exe file to expand the flyout to get more detail on this file with an uncertain reputation:

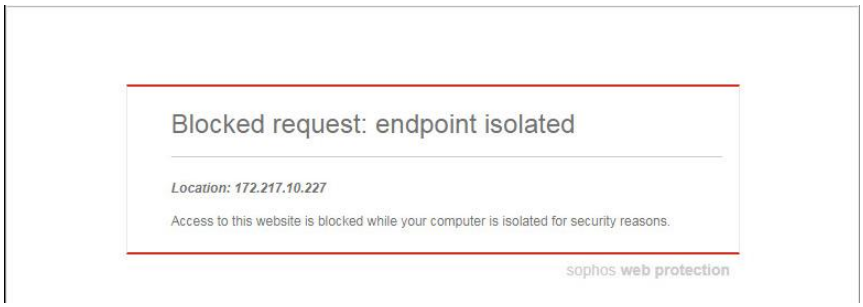


Note when clicking on the flyout, the SHA-256 hash of this process is checked with SophosLabs and existing Labs intelligence on the file is displayed on the file. The date provided details when the file was last analysed. The Observed capabilities section will highlight suspicious behaviours of the file. If looking to get the very latest intelligence on a file, click the link to 'Request the Latest Intelligence' this sends a command from Sophos Central to the endpoint in question and the file is submitted to SophosLabs for a detailed analysis. The feedback will be provided in a few minutes. Only portable executable files that have been highlighted as process images in the Threat Case can be submitted for analysis at this point in time.

5. At this point let's assume we think there is something bad happening on the endpoint where the detection occurred, and we want to isolate the endpoint. At the top of the Threat Case click "Isolate this computer"



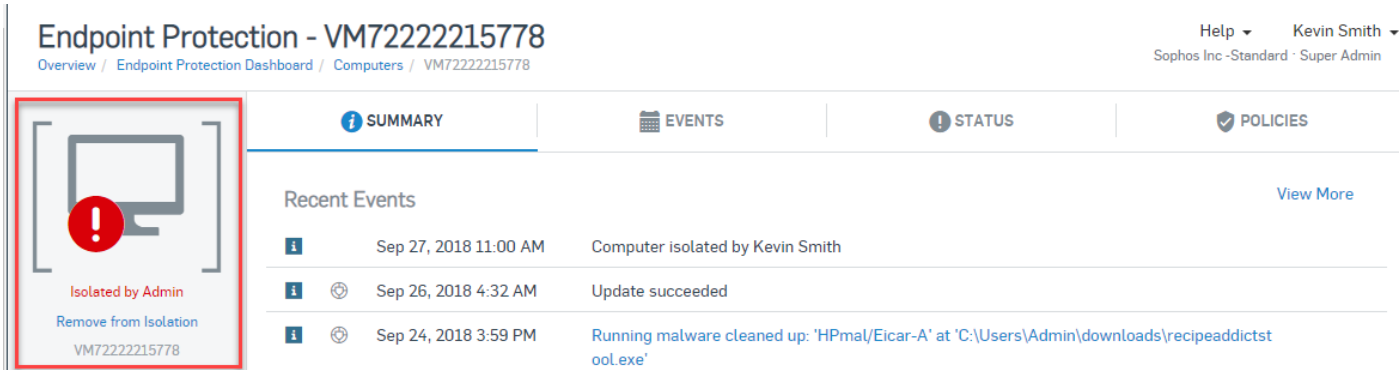
After clicking the button, a command is sent from Central to isolate the endpoint. Within a few minutes the endpoint should pop up an alert that the endpoint has been isolated. Once isolated all TCP and UDP connections should be blocked by the endpoint. From browser http connections a block page similar to the one below should be seen on the isolated endpoint:



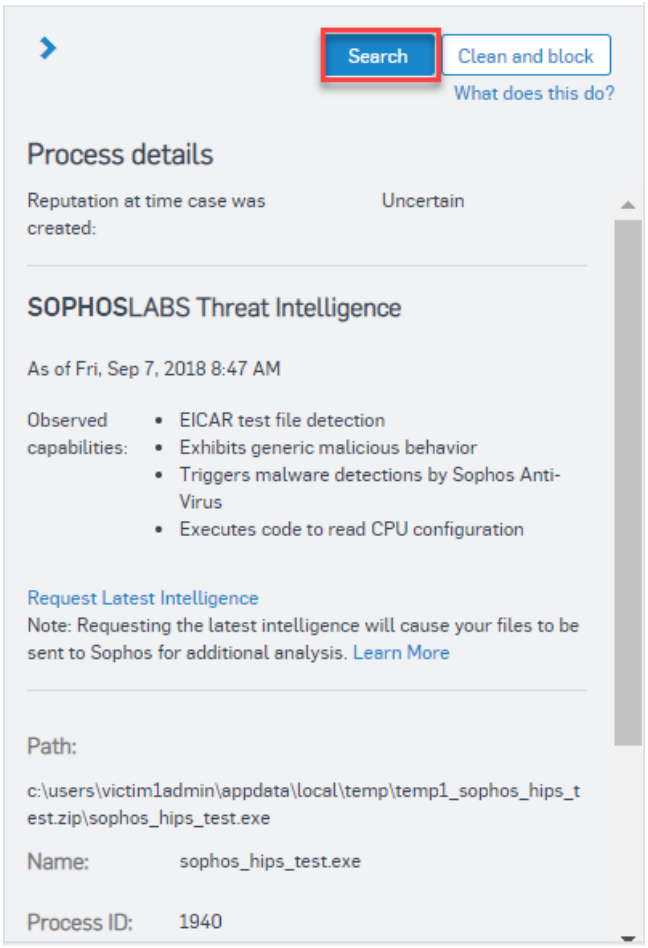
6. On the Configure > Settings page under Endpoint Protection the Admin Isolated Computers page will provide a list of all computers that are currently Admin Isolated.

7. Select the endpoint that was isolated and click the button to Remove from Isolation

Note: Endpoints can also be Admin Isolated directly from the Manage Protection > Computers page when you select an endpoint:

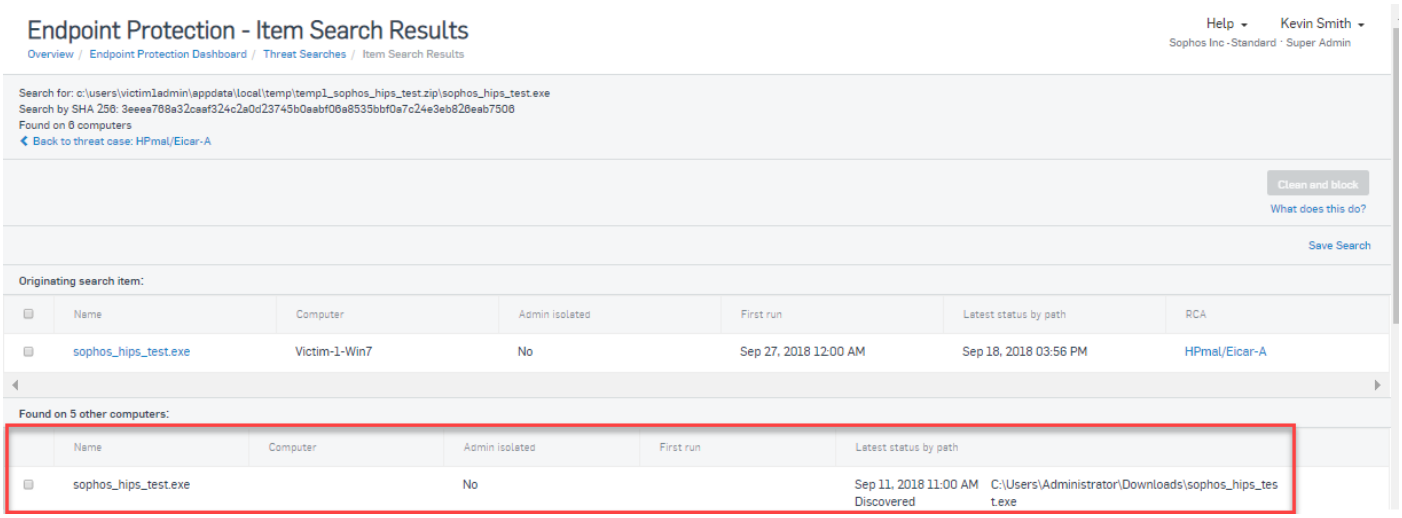


8. At this stage of the test we want to identify if any other endpoints have seen this potentially malicious file. Go back into the Threat Case for this detection and click on the Sophos_hips_test.exe file in the Threat Case graph. From the flyout click the option to perform a search:



Note: Endpoints enrolled in the EDR early access program will start submitting metadata on portable executable files that have a poor or uncertain reputation to Sophos Central. The search in this case is running a query on this metadata to see if any other endpoints have seen the SHA-256 hash of this file.

9. In the search results we should see that the file was also seen on the second endpoint the file was downloaded to, as the file wasn't run on the second endpoint the 'First run' date should be blank

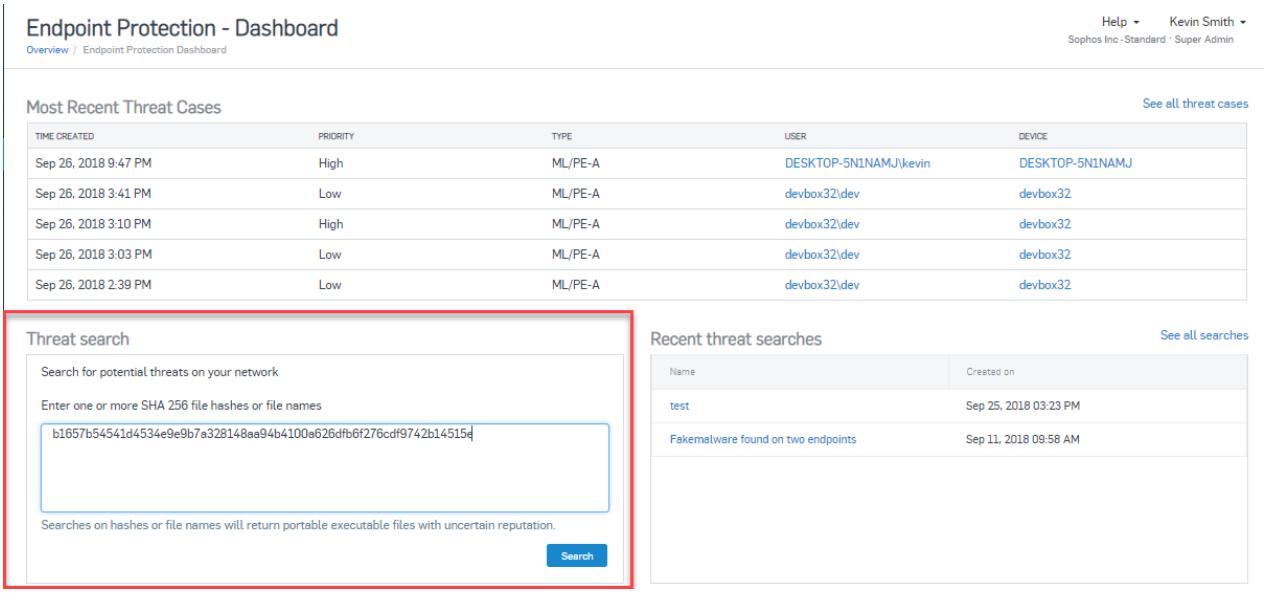


Exercise 2 will walk through a scenario where we have received intelligence on a potential new threat to be aware of. In the example we've been given a file hash and have been asked to investigate.

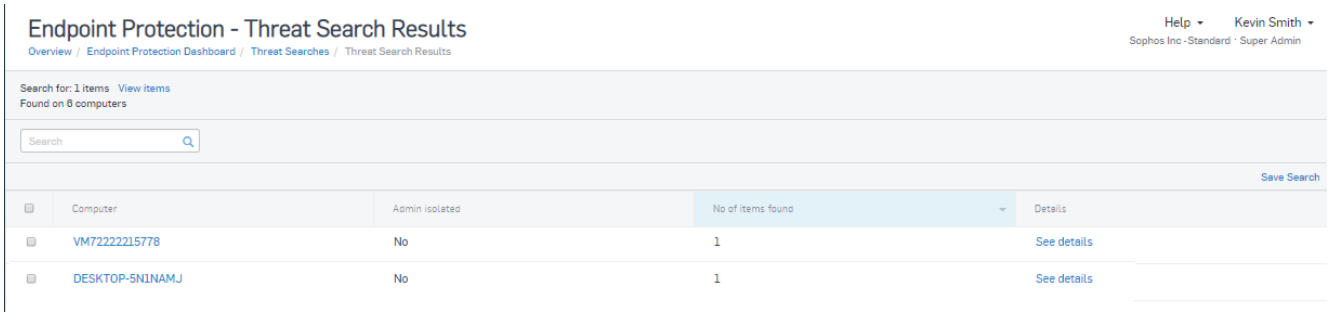
New Functionality Tested: Threat Search, Clean and Block capability

1. On one your endpoints, run the unknown.exe that was downloaded as part of the pre-requisites. Note the file will open and run and there is no detection in this case.

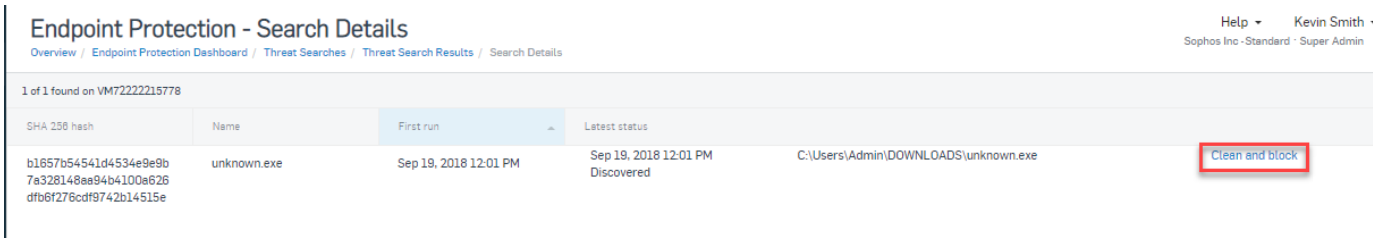
2. In the next step let's run a search across the estate to see what endpoints have seen the file hash we are interested in. From the Endpoint Protection Dashboard in Sophos Central, paste 'b1657b54541d4534e9e9b7a328148aa94b4100a626dfb6f276cdf9742b14515e' into the Threat Search window and click the Search button (this is the SHA-256 hash of the unknown.exe file dropped on to our test systems as part of the requisites):



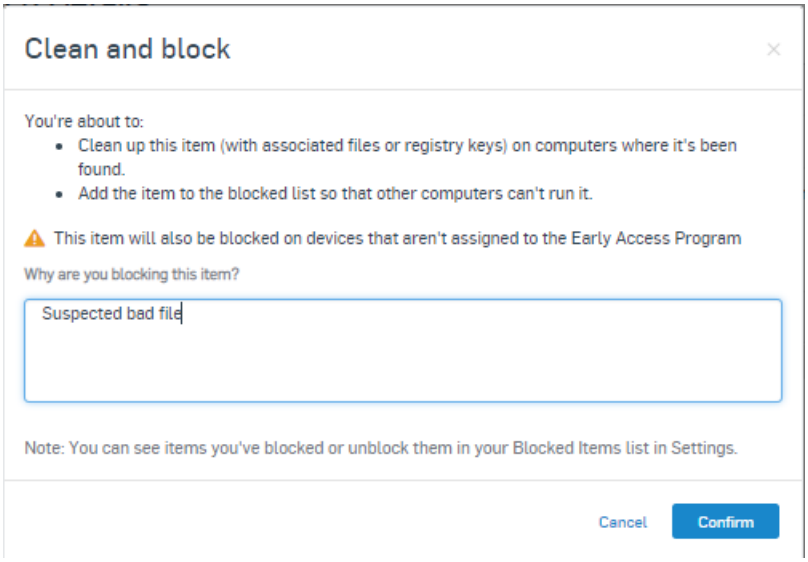
3. The search results should return that both endpoints have seen this file:



4. Click on the See Details link to see what was specifically found on one of the endpoints. Assuming we believe the file to be bad, let's click the Clean and Block action:



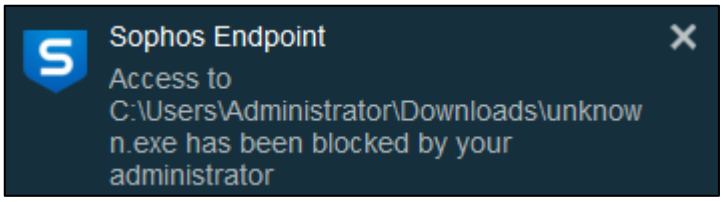
5. You are asked to provide the reason why you are adding the file to the Clean and block list, enter some text and click Confirm:



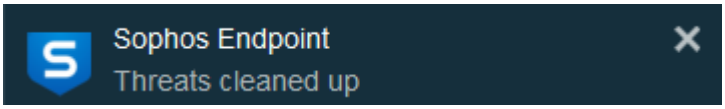
Note: The Clean and Block action will apply to portable executable files only and will not apply to PE files that have a good reputation according to Sophos. **The Blocked Items list will apply to all endpoints in the estate. *Note to EAP customers the Blocked Items list will also apply to all endpoints regardless of whether they are assigned to the EAP or not.**

6. Within a few minutes your endpoints will receive new policy that should prevent the Unknown.exe file from being executed. Run Unknown.exe on either endpoint

    a. Unknown.exe should **not** run. We should see a toast message saying the item has been blocked by admin



7. Shortly after adding to the Block list, Unknown.exe should be cleaned from both endpoints



8. If we realise an error was made and we want to remove the SHA-256 hash for unknown.exe from the Blocked Items list, go to Global Settings > Endpoint Protection > Blocked Items. From the Blocked Items page select the SHA-256 hash we added and click the Remove button. Then click the Save button:

9. Within a few minutes as the new policy is applied to the endpoints the unkown.exe should be released from quarantine and should again be executable.

This concludes the testing guide, as new capabilities are released the guide will be updated to help test new functionality.