SOPHOS
Security made simple.

Sophos Endpoint Detection and Response - Early Access Program

Known Issues and Important Info

October 8th, 2018

- When files are submitted for analysis using the new Deep Learning Malware Analysis functionality, a popup will appear when file analysis is complete with a link to the associated report. Currently the pop up incorrectly states that a Threat Case has been created rather than reporting that the Threat Intelligence report is ready.

- With the new Deep Learning Malware Analysis functionality administrators are no longer able to check for existing intelligence, or submit a file for analysis when analysing Server Threat Cases.

September 14th, 2018

- Due to planned changes in how the endpoint agent monitors and logs system changes, Sophos are recommending that Endpoints enrolled in the Early Access program have a minimum of 15 GB of free hard disk space available. These log files could theoretically grow to take up 37.5 GB of disk space but this would be highly unlikely. Sophos is investigating how to best tune and compress these logs for when the product becomes generally available.

- The Blocked Items list will apply to all endpoints regardless of whether they are assigned to the EAP or not.

- 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.

July 2nd, 2018

- Due to some pagination issues and issues scrolling when viewing the Root Cause visualisation we request that customers do not use Internet Explorer or Microsoft Edge as the browser to manage Sophos Central during the Early Access Program

- When examining a process from either the Root Cause Visualisation or via the Artifact table in a Threat Case, if the Endpoint has not been assigned to the Early Access Program there will be the ability to query Sophos to see if any current intelligence exists for that file, but the endpoint will not support the ability to ‘Request the Latest Intelligence’ which submits that file to Sophos for analysis and that link will not be viewable for those endpoints.

- On an endpoint assigned to the Early Access Program, when examining a process from either the Root Cause Visualisation or via the Artifact table in a Threat Case where that process was actually detected and cleaned, if the link to ‘Request the Latest Intelligence’ is clicked, it will result in an error that ‘the file cannot be found or may have changed’.