Thank you for downloading Threat Grid Malware Analysis and Intelligence for EnCase. You will soon have the ability to conduct dynamic malware analysis, and obtain threat intelligence, with a right-click inside EnCase.

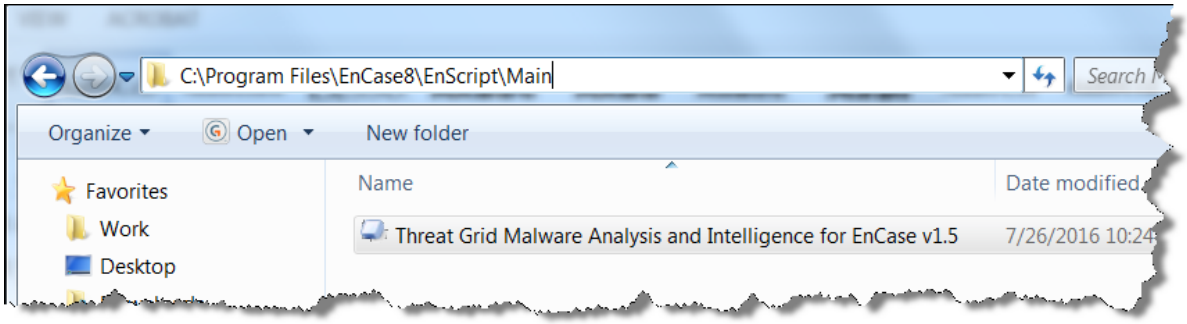
Next steps are a quick installation and entering your Threat Grid API Key. You can obtain this key with a free one hour private training via WebEx. I look forward to setting up this training with you and getting you started. The training also includes a 160+ page user guide.

Jessica Bair, EnCE, EnCEP
Sr. Manager, Business Development | Advanced Threat Solutions
Cisco Security
jbair@cisco.com | www.ThreatGrid.com

INSTALLATION

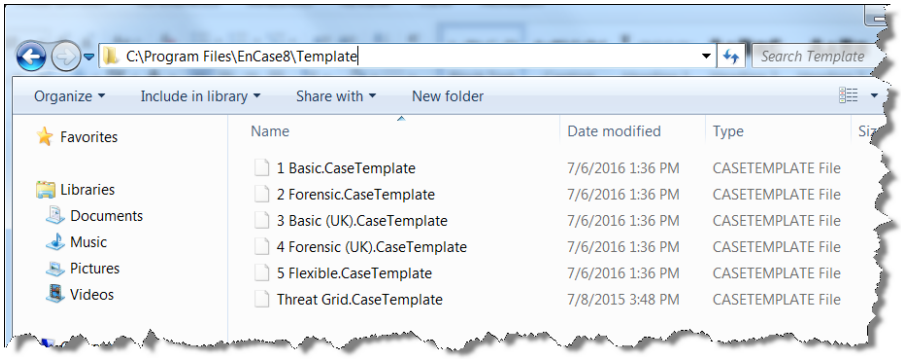
To install Threat Grid Malware Analysis and Intelligence for EnCase, copy the EnPack to `C:\Program Files\EnCase8\EnScript\Main` directory

Note: Since you downloaded the file from the Internet, you cannot directly copy the file into a `C:\Program Files` directory. You will need to save it to your local system or removable media. You will then need local Administrator permissions to copy the file. You may have to create the `Main` folder



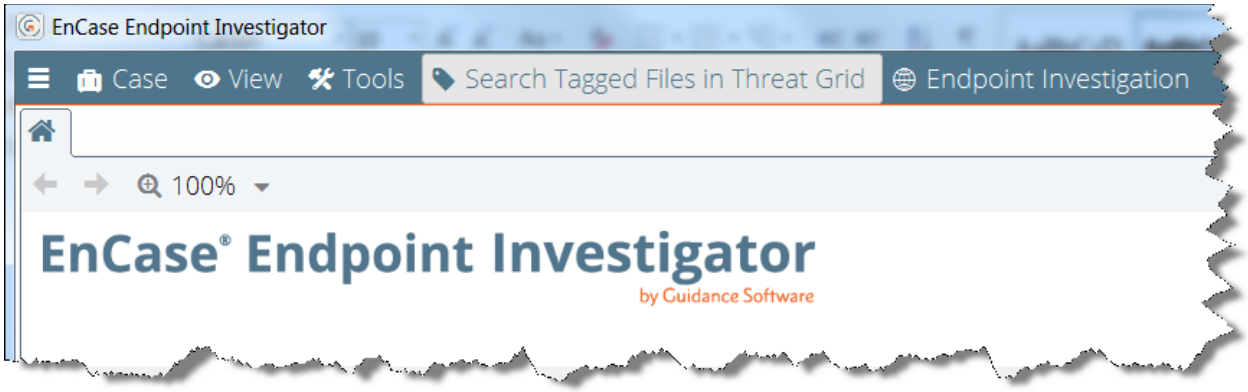
Threat Grid Malware Analysis and Intelligence for EnCase Plugin

Place the `Threat Grid.CaseTemplate` in `C:\Program Files\EnCase8\Template`



Threat Grid Malware Analysis Case Template

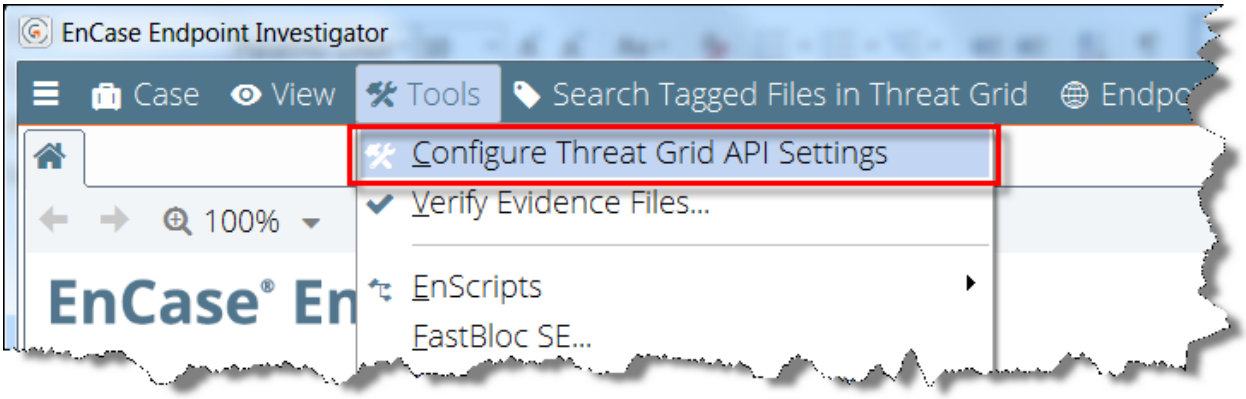
The Threat Grid plugin will load when EnCase is launched. You will see **Search Tagged Files in Threat Grid** in the tool bar.



Threat Grid for EnCase running

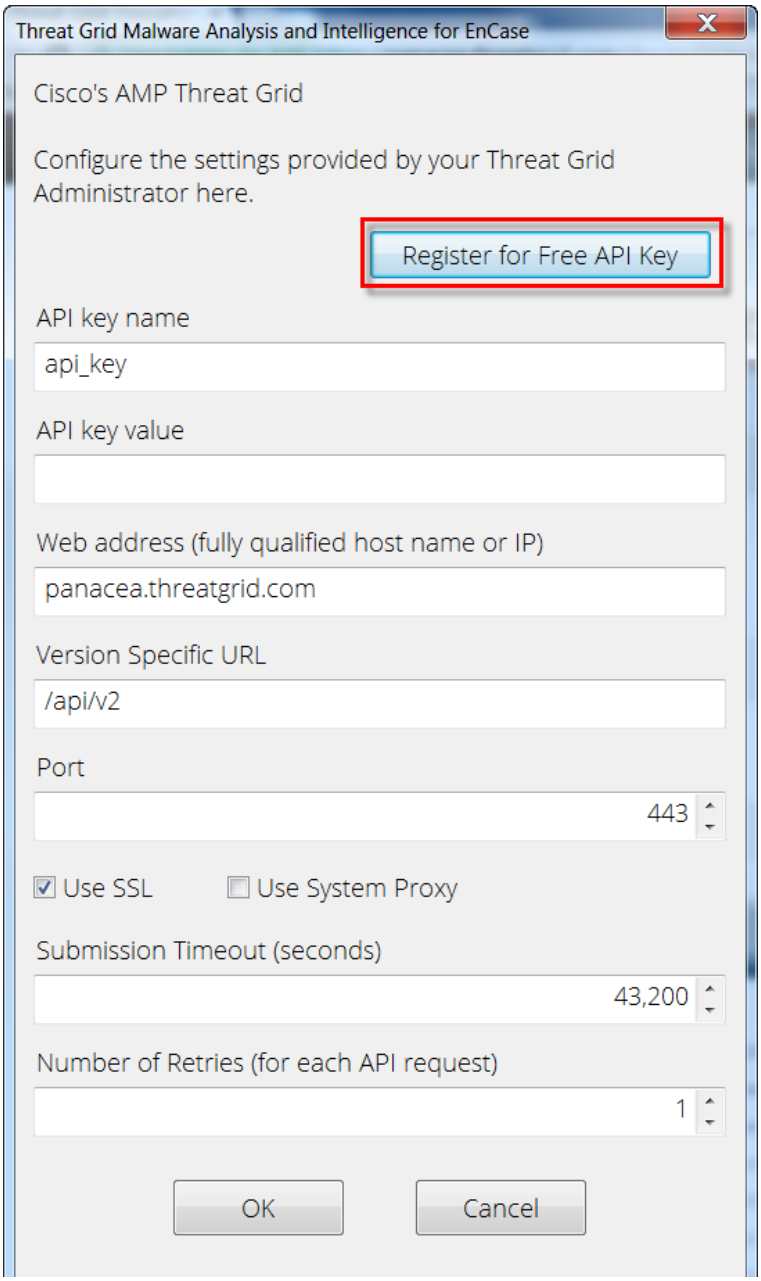
CONFIGURE THREAT GRID API

From your EnCase Enterprise interface click on the **Tools** and select **Configure Threat Grid API Settings.**



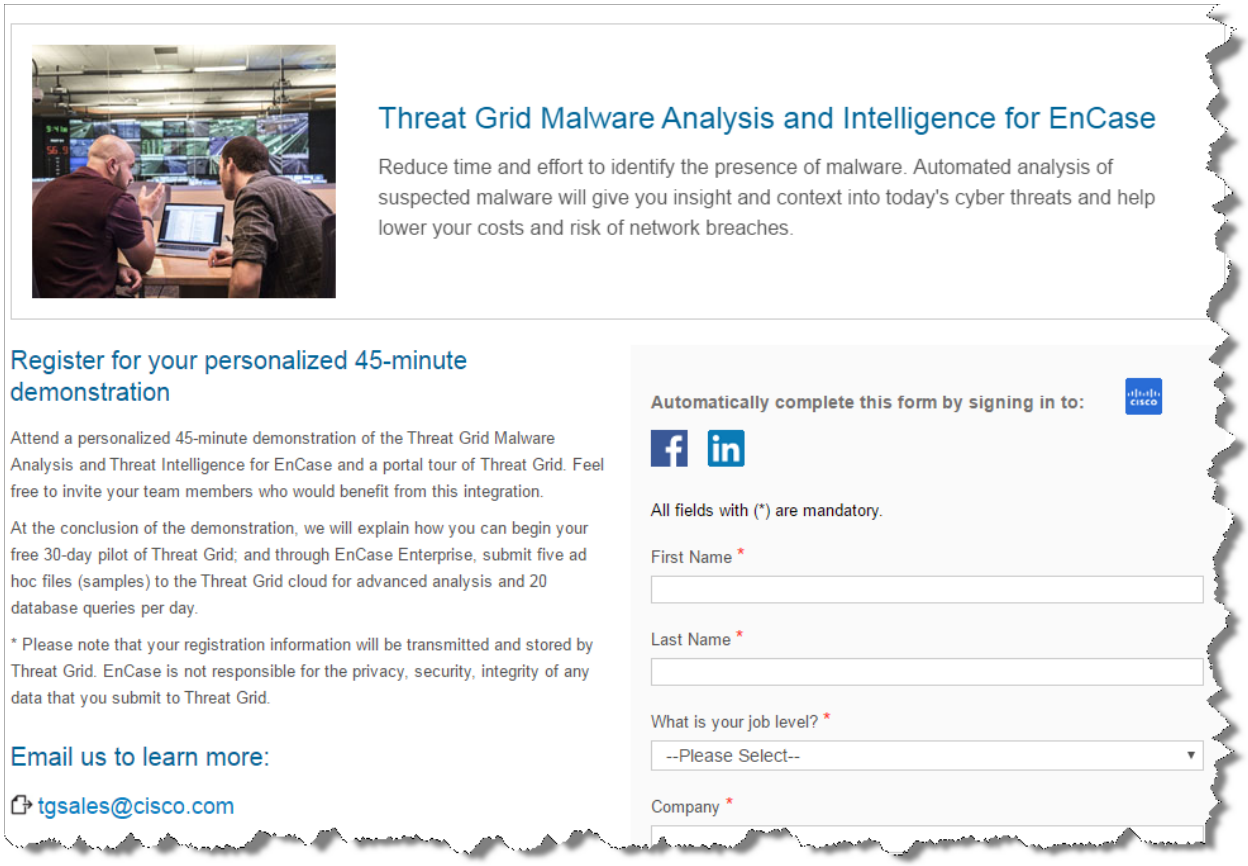
Tools> Configure Threat Grid API Settings

The Threat Grid plugin will launch and allow you to enter the API key value for your account. If you don't already have a Threat Grid account, fill out the web form or please contact tgsales@cisco.com



Threat Grid Plug-in Configuration

In the webpage, enter your full name, job title, organization name, mobile phone number and email address. http://cs.co/TG4EnCase

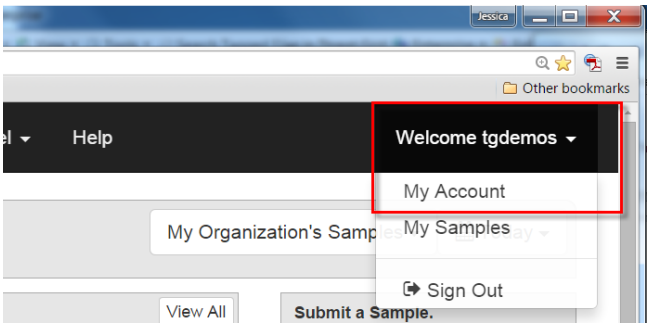


EnCase Pilot Registration

Click **Submit**. Your registration is sent to Cisco.

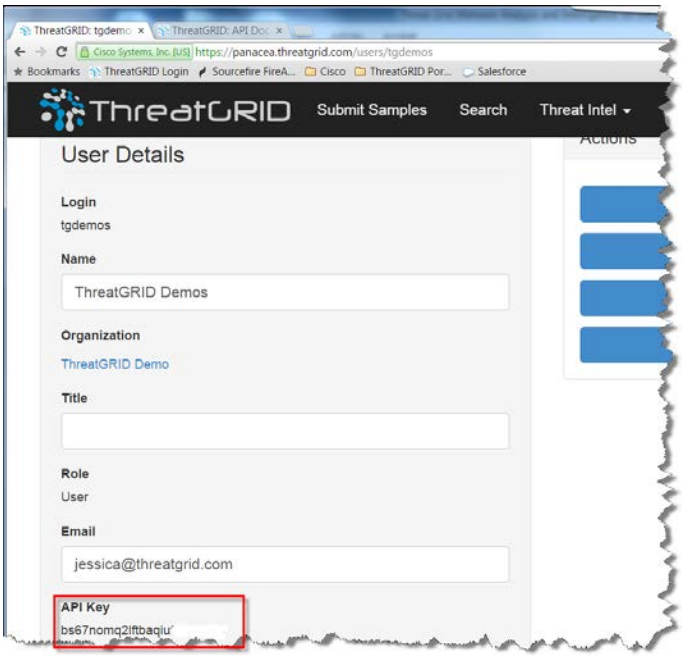
You will be contacted soon after via email set up a one-hour private training session. Once you have completed the training, and submitted the Welcome Letter, your account information is emailed to you so you can log in.

To locate your Threat Grid API key value, log into https://panacea.ThreatGrid.com with your user name and password, and from your user name click the down arrow and choose **My Account.**



Threat Grid My Account

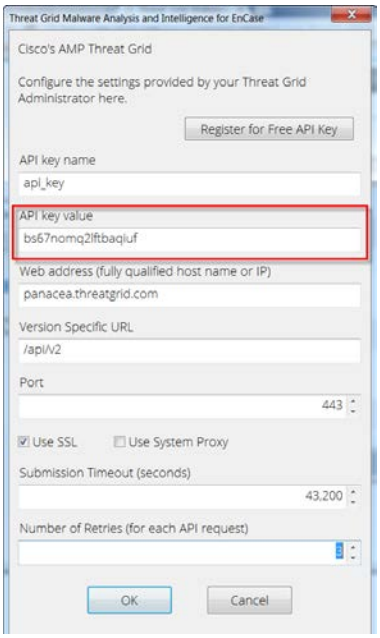
Locate your Threat Grid API key value and copy it to your clip board.



Threat Grid API Key

Paste it into the Threat Grid interface. Click **Use System Proxy** if your network requires proxy servers to communicate with the Internet. If you are using a Threat Grid appliance, you can type in the IP address in place of the Threat Grid web service.

Choose **OK**.



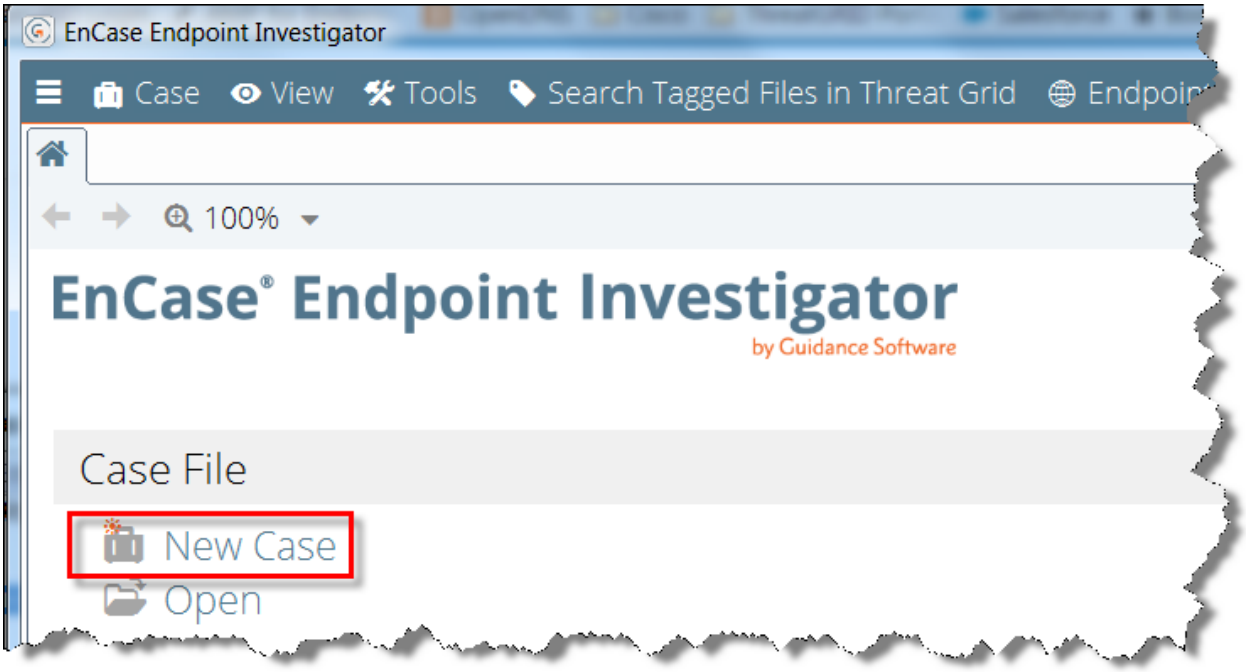
Enter Threat Grid API Key

Your 30 day trial of Threat Grid begins, and EnCase Endpoint Investigator can send five ad hoc files (samples) to the Threat Grid cloud for dynamic analysis and 20 database queries per day.

As part of the trial, you will receive a PDF of the *Threat Grid Malware Analysis and Intelligence for EnCase User Guide*, with detailed instructions and illustrations on how use it for your malware analysis inside EnCase, as well as using the Threat Grid portal. It is distributed with a Box.net share. If you have any issues, please email us at support@ThreatGrid.com

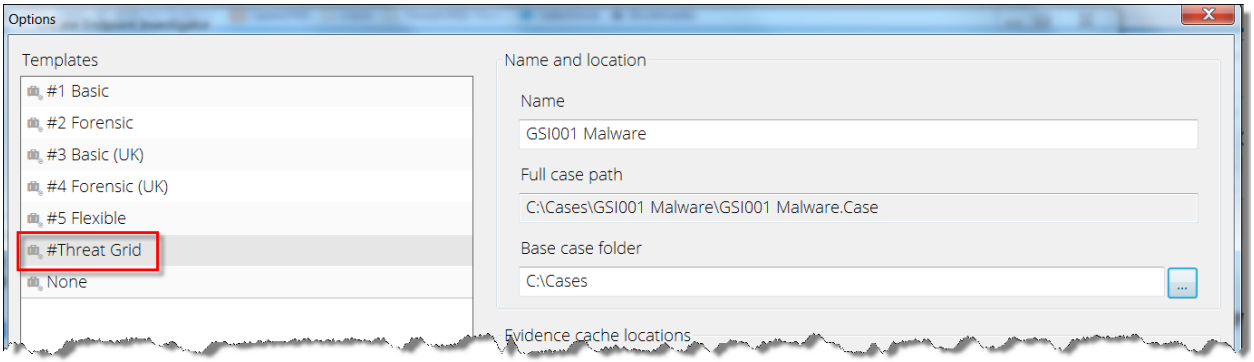
NEW CASE

When you create a New Case, the Threat Grid template will be available.



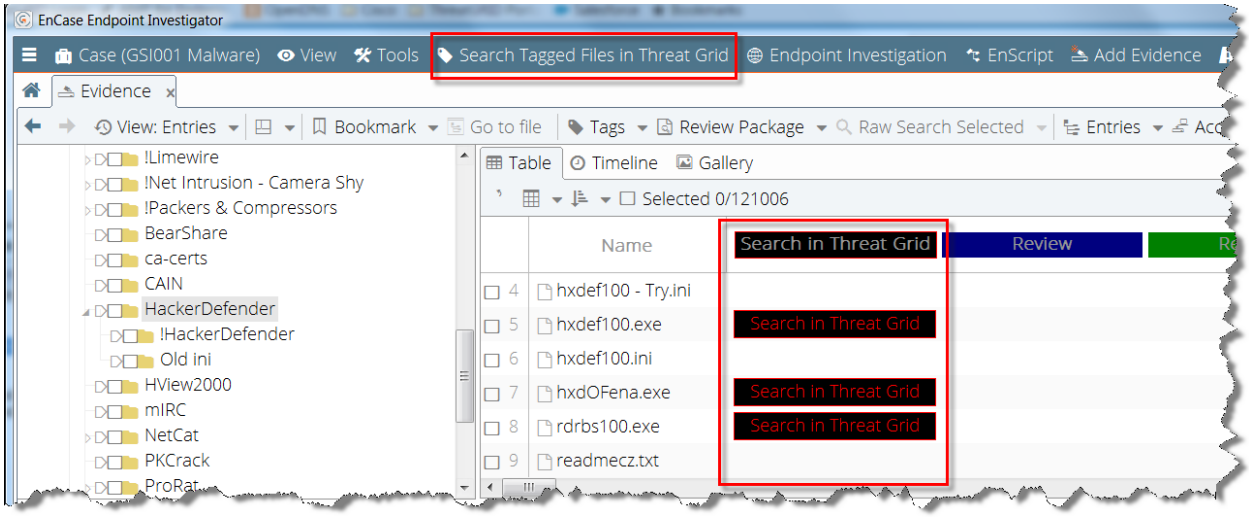
New Case

It contains a bookmark folder and notes for Malware Analysis, with the other folders of the #1 Basic EnCase Template.



Threat Grid case template

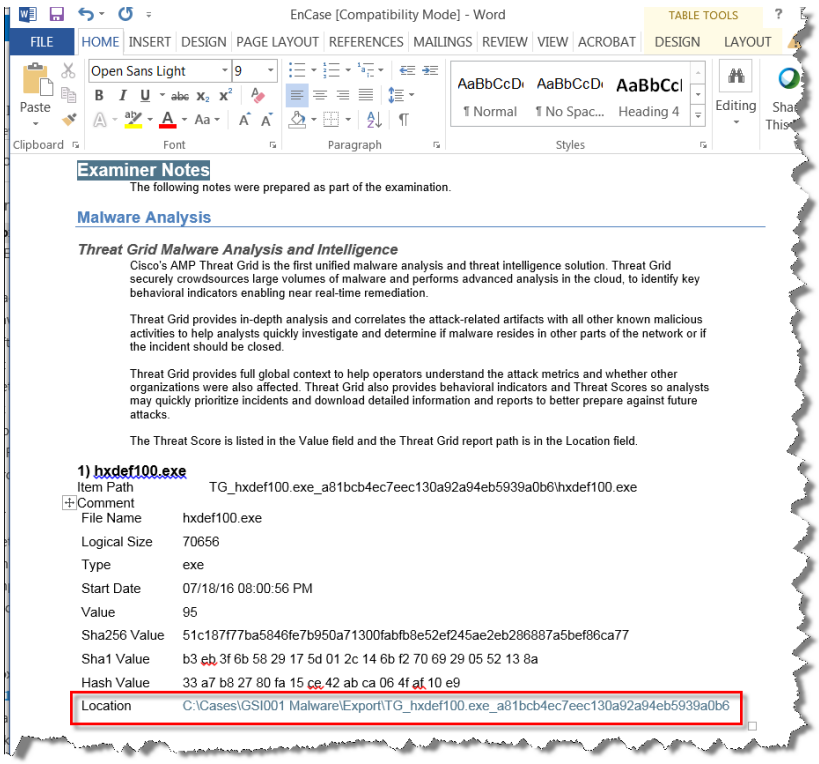
It also contains the tag **Search in Threat Grid** to allow bulk queries of files in the Threat Grid intelligence database.



Threat Grid Tag

Note: In EnCase v8, the ***Records*** view is now called ***Artifacts***.

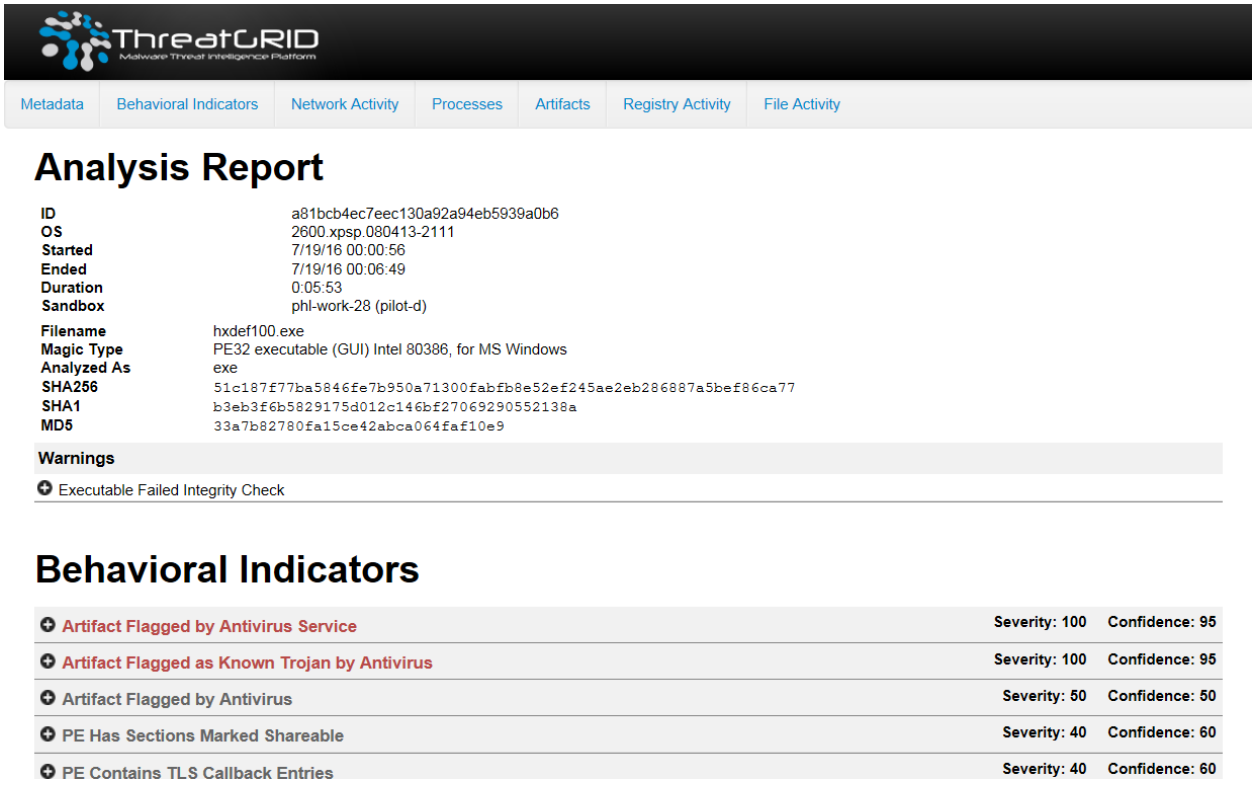
It has a bookmark folder and note to aid in your reporting. You can hyperlink the report to the downloaded Threat Grid report.



EnCase Report for Threat Grid summary

The detailed Threat Grid report opens for analysis.

Note: Use Firefox, Chrome or Opera. Internet Explorer cannot properly display the detailed reporting provided by Threat Grid.



Threat Grid analysis report