niwis consulting gmbh
consulting training lizenzen

Symantec Threat Intelligence

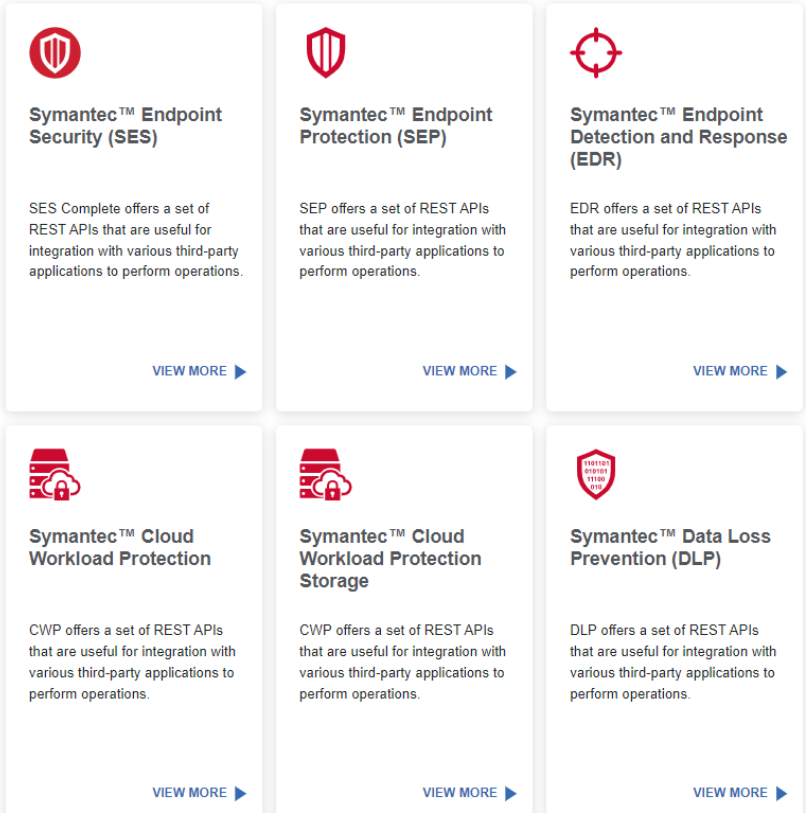
Ulf Spangenberg, niwis consulting gmbh

About Symantec Threat Intelligence

Symantec is offering a set of services to core customers with no additional costs to allow access to Broadcom Global Intelligence Network (GIN) and all telemetry collected.

About Symantec APIs

Symantec Endpoint Security and other Symantec solutions offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.



About Symantec Endpoint Security (SES)

SES delivers comprehensive protection for all your traditional and mobile devices across the entire attack chain. This single-agent solution supports on-premises, hybrid, and cloud-based deployments.

Best Protection

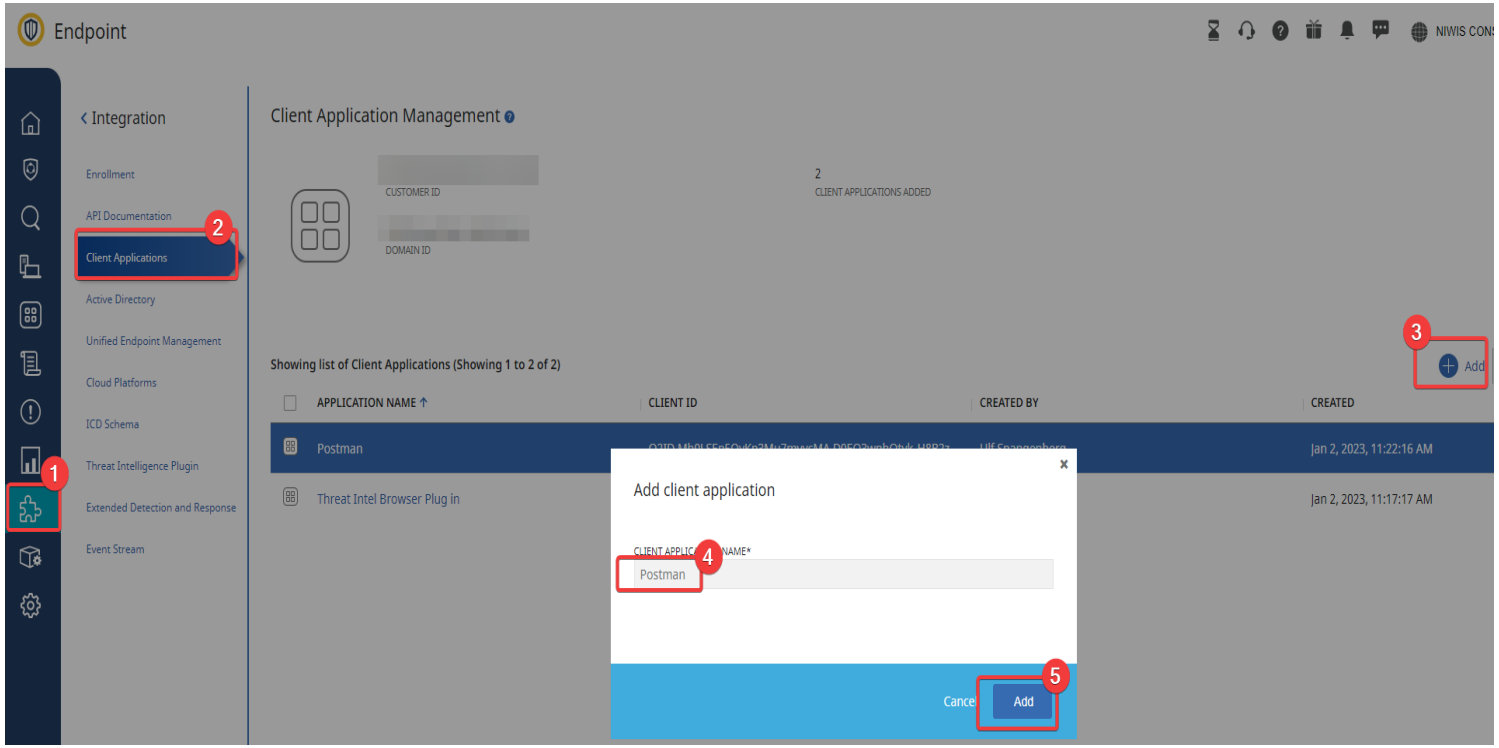
Industry-leading solution that addresses threats across the entire attack chain.

How to use the Symantec Threat API with Postman

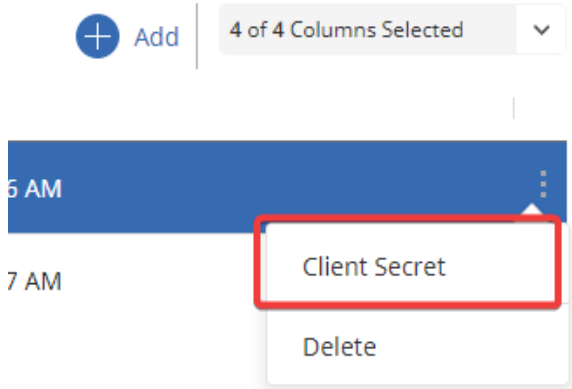
About Postman

Postman is an API platform for building and using APIs. Postman simplifies each step of the API lifecycle and streamlines collaboration so you can create better APIs—faster.

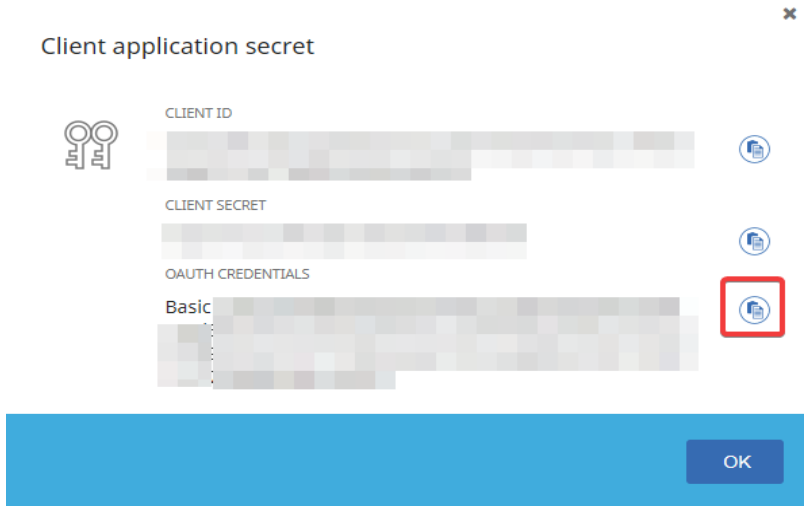
Create an application in Symantec Endpoint Security (SES)



Go to Client Secret



Copy OAUTH


Client application secret
CLIENT ID
CLIENT SECRET
OAUTH CREDENTIALS
Basic
OK

Install Postman and import collection

Download and install Postman:

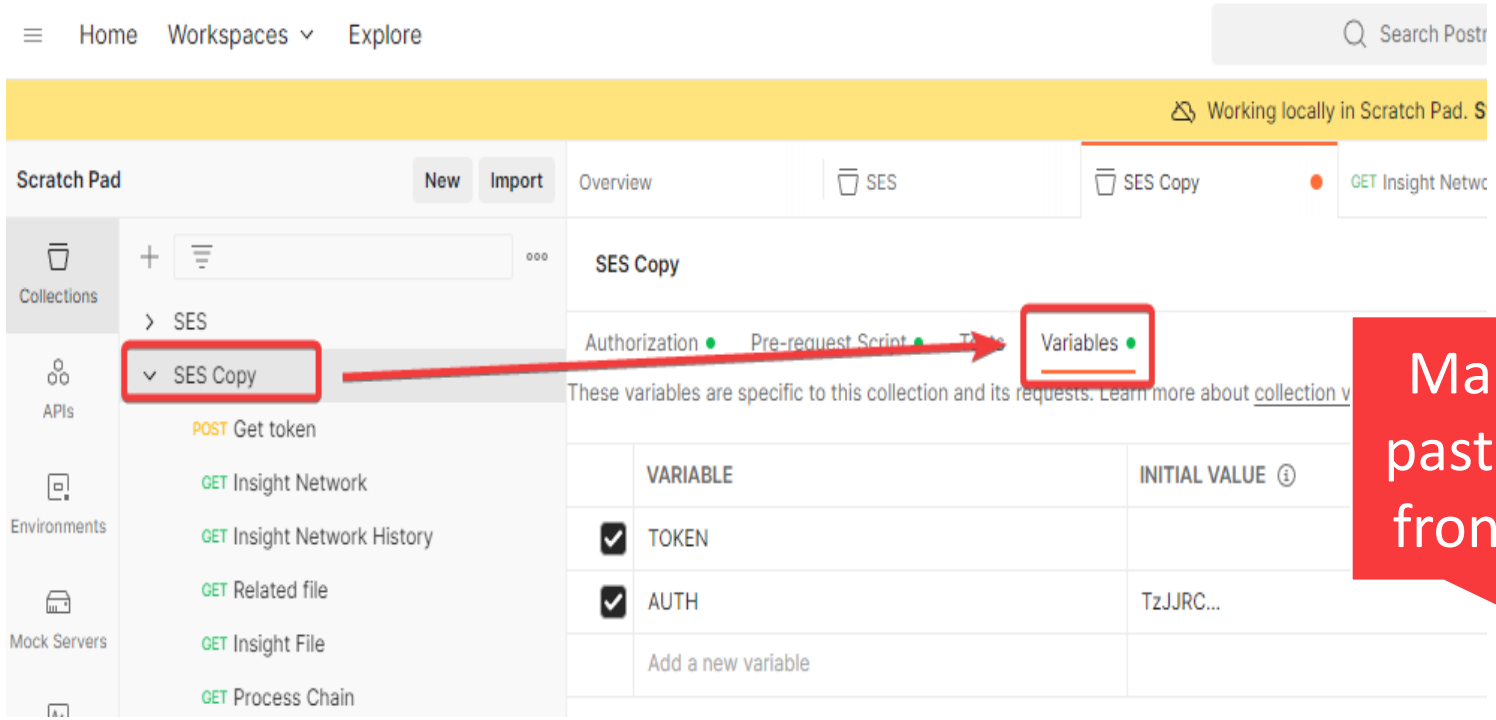
https://www.postman.com/downloads/

Download and import JSON:

https://www.niwis.com/download/threat-intelligence-json/

Fill …

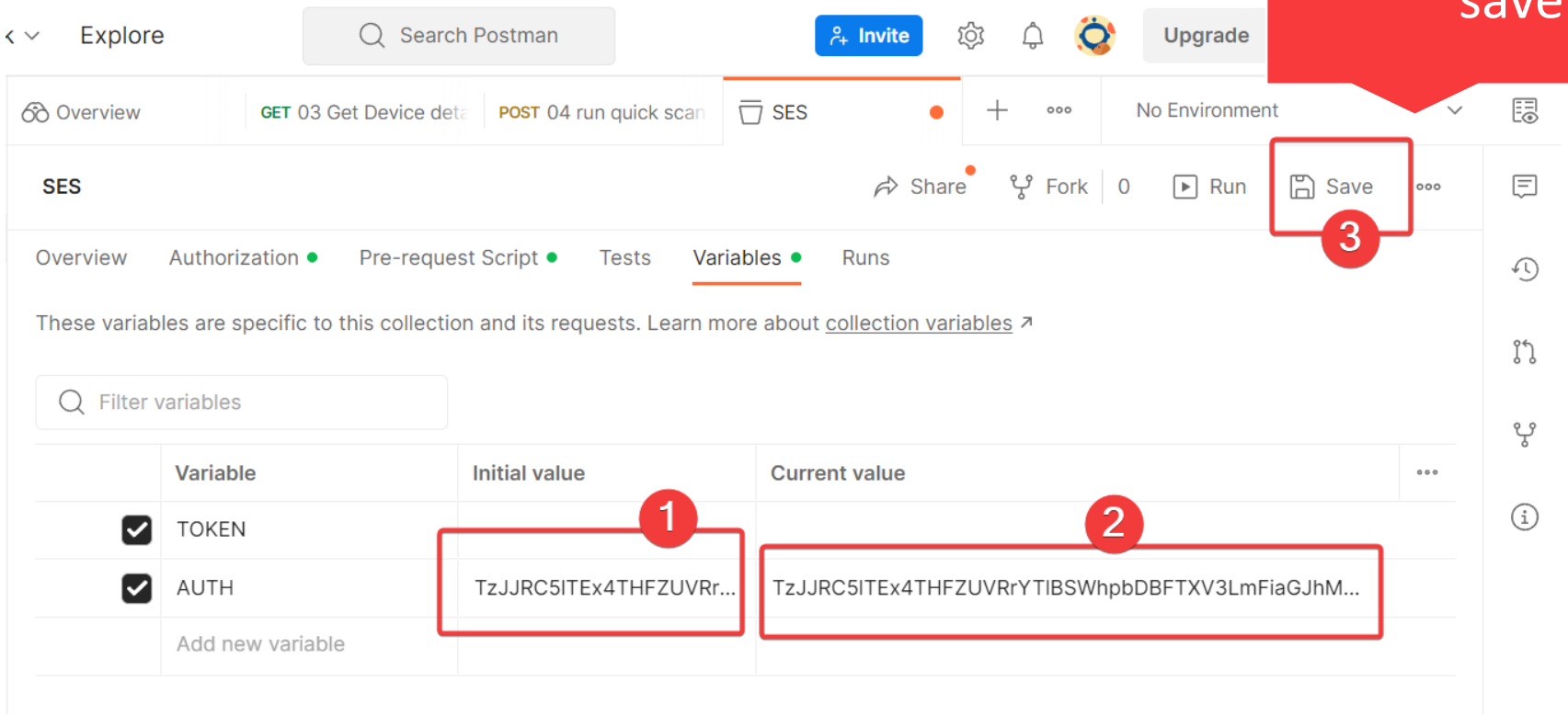
… variable “AUTH” under Main Section “SES Copy” with the clipboard value of your OAUTH credentials.



Make sure ...

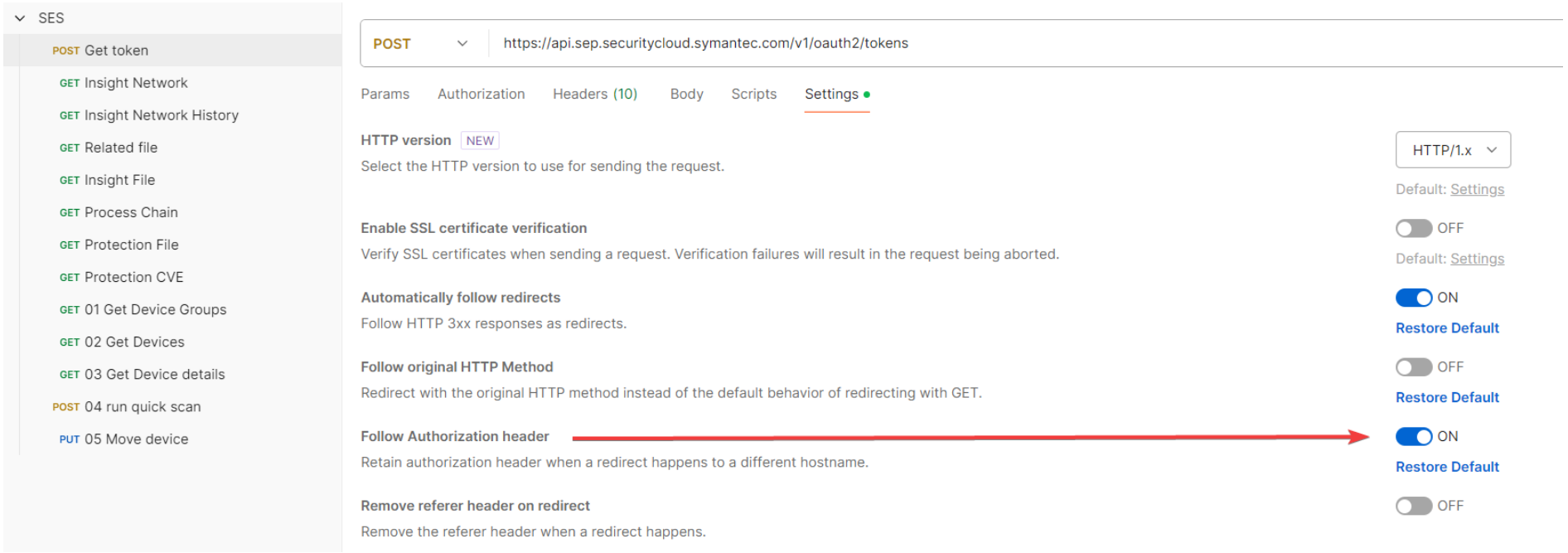
... you fill in the “Initial value” and the “Current value”.

Do not forget to save!



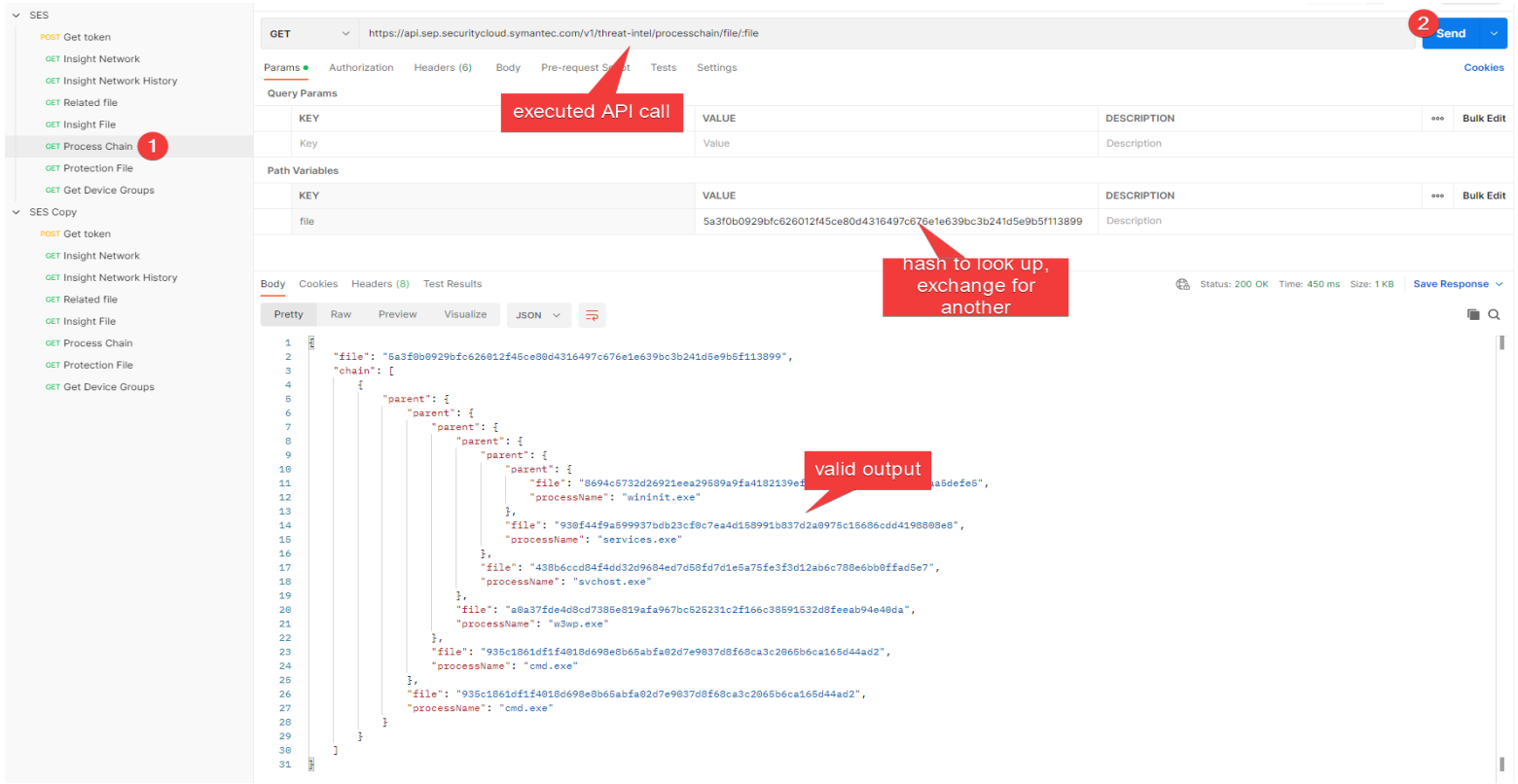
Turn on ...

... “Follow Authorization header”.



Go to …

… … any listed GET command and execute and you should get a valid output.



Additionals

More Symantec Threat Intelligence

- SES RestAPI documentation:
  https://apidocs.securitycloud.symantec.com/#/

- Threat Intel Browser Plug In:
  https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Settings/Configuring-Threat-Intel-browser-plug-in.html

- Threat Explorer (Account needed):
  https://threatexplorer.symantec.com/

More Symantec Threat Intelligence

- **SES Threat Reports*1 via Email**
  - **Link …**

*1

- **Symantec Threat Alerts Report**: Shows information about indicators of compromise (IOCs) relating to currently active, critical threats.
- **Symantec White Papers Report**: Shows information about current threats based on in-depth research by the Symantec Threat Hunter team.
- **Threat Landscape Bulletin Report**: Provides up-to-date news and intelligence from the world of cyber security.