Seculert Dashboard

Introduction

Seculert's dashboard provides unique data intelligence based on log analytics and live botnet monitoring, relating to internal and external assets.

All of our unique intelligence is available 24/7 via our dashboard.

In order to leverage Seculert's unique data with your other security solutions, such as SIEMs, Firewalls and Proxies, we provide a simple API.

This API can be used in several ways and hereunder are some best practices.

API HTTP Request Template

API link: https://portal-services.seculert.com/CustomerAPI/getinfo.aspx?key=API_KEY&format=DATA_FORMAT&type=FEED_TYPE&filter=FILTER&field=SORT_FIELD&dir=SORT_DIR&bomEnabled=BOM_VALUE

API Values:

1) **API_KEY:** Customer's API Key (located at DASHBOARD/Settings/API – API Key)

2) **DATA_FORMAT:**

   a. xls: Excel file

   b. xml: XML format

   c. sys: CSV format

3) **FEED_TYPE:**

   a. 1 – Crime Servers

   b. 2 – Threat Intelligence Records

4) **SORT_FIELD:** Field to sort by

5) **SORT_DIR:** Direction of sort (Default: ASC)

6) **BOM_VALUE:**

BOM (byte order mark) is a Unicode character used to signal the byte order of a text file or stream (http://en.wikipedia.org/wiki/Byte_order_mark):

   a. 0 or empty: BOM character will not be added to the response (Default: 0)

   b. 1: BOM will be added to the response

7) **FILTER** (JSON format of filter):

```
{"f_0_field":"FIELD_NAME_0","f_N_data_type":"DATA_TYPE_0","f_0_data_comparison":
"DATA_COMPARISON_0","f_0_data_value":"DATA_VALUE_0","f_1_field":"FIELD_NAME_1","f_1_data_
type":"DATA_TYPE_1","f_1_data_comparison":"DATA_COMPARISON_1",
"f_1_data_value":"DATA_VALUE_1","f_2_field":"FIELD_NAME_2",
"f_2_data_type":"DATA_TYPE_2","f_2_data_comparison":"DATA_COMPARISON_2",
"f_2_data_value":"DATA_VALUE_2",.............,"f_N_field":"FIELD_NAME_N",
"f_N_data_type":"DATA_TYPE_N","f_N_data_comparison":"DATA_COMPARISON_N",
"f_N_data_value":"DATA_VALUE_N"}, where:
```

7.1) **FILTER** consist of some filter expression. Each filter expression looks like:
`"f_N_field":"FIELD_NAME_N","f_N_data_type":"DATA_TYPE_N",`
`"f_N_data_comparison":"DATA_COMPARISON_N","f_N_data_value": "DATA_VALUE_N"` and consist elements:

- `"f_N_field":"FIELD_NAME_N"` mandatory
- `"f_N_data_type":"DATA_TYPE_N"` mandatory
- `"f_N_data_comparison":"DATA_COMPARISON_N"` not mandatory (only for "date" type)
- `"f_N_data_value":"DATA_VALUE_N"` mandatory

7.2) **N** - zero based number of filter expressions

7.3) **FIELD_NAME_N** - internal name of field for filter expression number "N"

7.3.1) for Crime Servers:

- Host
- Ip
- FirstSeen
- LastSeen

7.3.2) For Threat Intelligence Records:

- Timestamp
- MachineIP
- MachineCountry
- CrimeServer
- ThreatType
- AssetType
- Comments
- AddedDate
- HostStatus

7.4) **DATA_TYPE_N** - data type for filter expression number “N”:

- string
- date
- list

7.5) **DATA_COMPARISON_N** - data comparison for filter expression number (“N”only for “date” data type):

- lt
-gt
-eq

It is possible to use comparisons “lt” and “gt” simultaneously in one request.

In these cases each data comparison should be a separate filter expression.

7.6) **DATA_VALUE_N** - data value for filter expression number “N”.

7.6.1) For “list” data type the data value is the list of the values assigned for this field:

`["DATA_VALUE_N_0","DATA_VALUE_N_1","DATA_VALUE_N_2",....., "DATA_VALUE_N_K"]`

Where DATA_VALUE_N_K - data value number “K” from assigned values for this field for filter expression number “N”.

7.6.2) For “date” data type value is date in the format - mm/dd/yyyy

7.7) Mapping for creation of filter expressions:

7.7.1) Crime Servers:

Header_Name	FIELD_NAME	DATA_TYPE	DATA_VALUE
CriminalServers	Host	string	single value
IPAddress	Ip	string	single value
FirstSeen	FirstSeen	date	single value
LastSeen	LastSeen	date	single value

7.7.2) Threat Intelligence Records:

Header_Name	FIELD_NAME	DATA_TYPE	DATA_VALUE
Timestamp	Timestamp	date	single value
SourceIP	MachineIP	string	single value
Country	MachineCountry	string	single value
CrimeServer	CrimeServer	string	single value
Type	ThreatType	string	single value
AssetType	AssetType	list	values:[Internal,Hybrid,External]
Comments	Comments	string	single value
AddedDate	AddedDate	date	single value
Status	HostStatus	list	values:[New,Active,Closed]

Customer Use Case:

Harvard University - Harvard University uses Seculert's API to integrate the Seculert records with QRadar's Remote Networks. Read how Seculert offers a generic script that can be utilized to generate automated reports with active crime server lists and new threat intelligence records. To receive the script please contact us.

Mota Gur 7, Petach-Tikva, Israel.
Tel: +972-3-9193366 +1-718-305-7067
Fax: +972-3-9193636
support@seculert.com
For press inquiries please contact: pr@seculert.com
www.seculert.com