APPLICATION PROGRAMMING INTERFACE

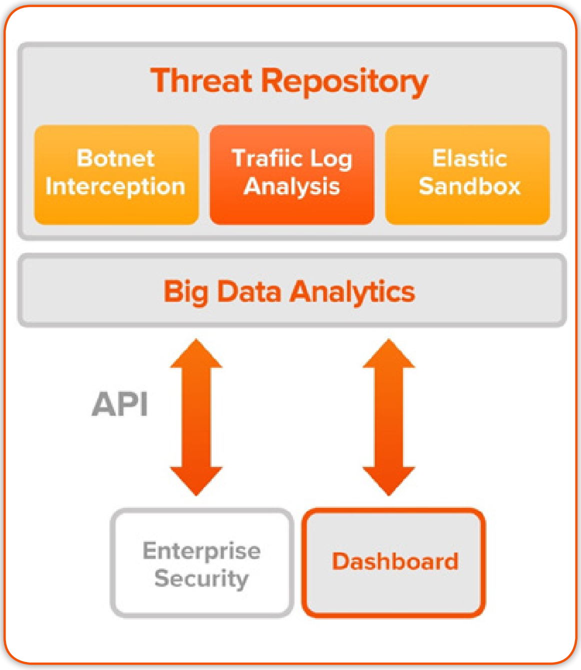
INTRODUCTION

Customers can use Seculert's Application Programming Interface (API) to integrate their existing security devices and applications with Seculert. With Seculert's API you can now seamlessly extend your security perimeter with the dynamic threat intelligence provided by the Seculert Advanced Threat Protection Solution.

Seculert's API is designed to enable Seculert's technologies to augment your existing on-premises security devices and enhance your defenses against advanced threats and APT. Designed from the cloud down to be easy-to-use, flexible and powerful, Seculert's API transforms your existing security devices into a comprehensive APT solution. Below are just a few of the many benefits you can experience by using Seculert's API:

- Keep your devices up-to-date by easily synchronizing blacklisted IPs and domain names of command and control servers on a regular basis.
- Retrieve log analysis results, providing additional insight into your network activity.
- Update your existing security devices with the latest malware profiles from Seculert.
- Deliver dynamic forensics on botnet communications to your perimeter immediately blocking further access.
- Detect compromised mobile devices and help you to meet the security challenges of BYOD.

Seculert is a comprehensive cloud-based solution for protecting organizations from advanced malware, APTs and zero-day attacks. Seculert combines several key detection and protection technologies – an Elastic Sandbox environment, Botnet Interception, and Traffic Log Analysis - in one simple solution that proactively identifies new threats as they emerge.



HOW THE API WORKS

Seculert's API allows customers to expand upon the core functionality provided by Seculert's Advanced Threat Protection Solution. In particular, it allows external applications and devices to retrieve data from the platform making integration simple.

Use Seculert's API Methods to access the unique intelligence in our platform that you wish to affect. These include Crime Servers, Botnet Interception, Log Analysis and an Elastic Sandbox.

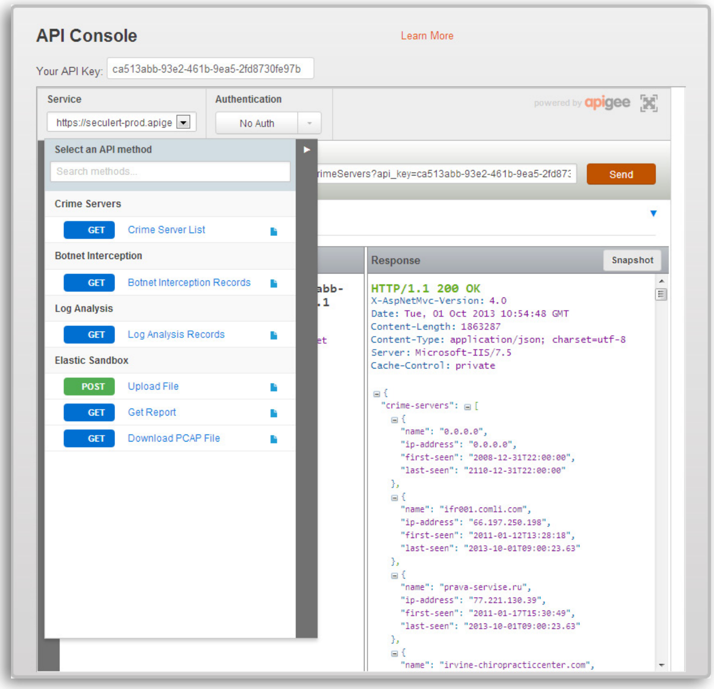
RESTFUL WEB API

Seculert API is a web-based API implemented using HTTP and REST principles. REST-style architectures consist of clients (Seculert customers) and servers (Seculert platform). Seculert customers initiate requests to the platform; the request is processed and appropriate responses are returned. Requests and responses are built around the transfer of representations of API methods.

Seculert’s RESTful API allows customers with any number of security devices to interface with the data generated by the platform. The hypertext driven API is scalable and device neutral.

API CONSOLE

Seculert provides an API Console featuring an easy-to-use interface by providing a GUI which acts as cURL on steroids for exploring our API’s resources and executing its methods.



API Console

Your API Key: ca513abb-93e2-461b-9ea5-2fd8730fe97b

Service: https://seculert-prod.apige

Authentication: No Auth

rimeServers?api_key=ca513abb-93e2-461b-9ea5-2fd873

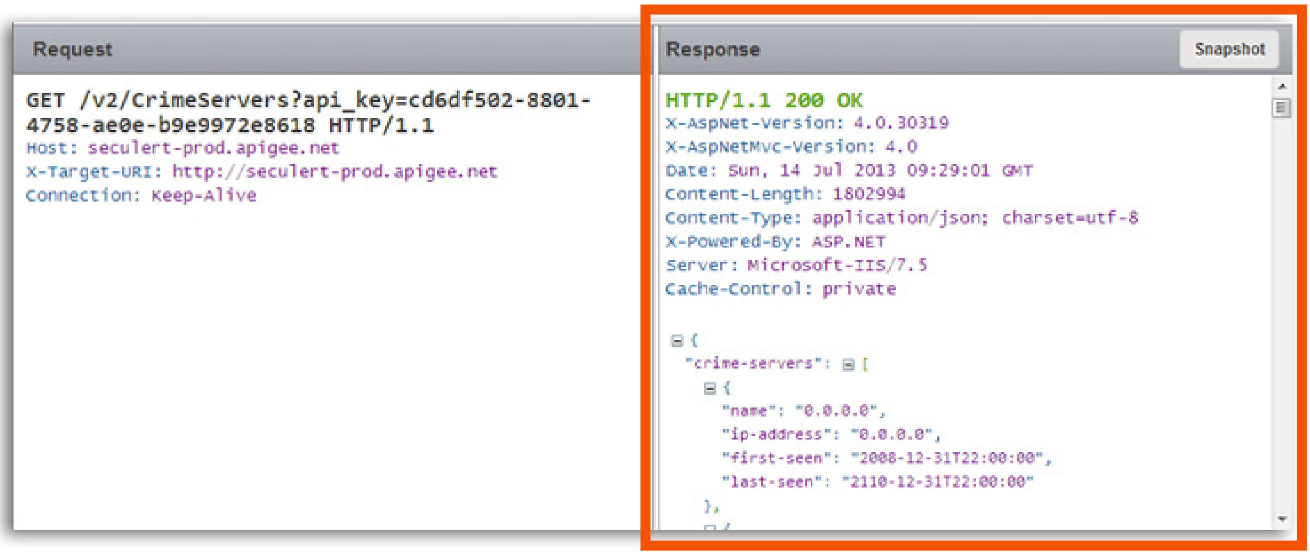
```
HTTP/1.1 200 OK
X-AspNetMvc-Version: 4.0
Date: Tue, 01 Oct 2013 10:54:48 GMT
Content-Length: 1863287
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/7.5
Cache-Control: private

⊟{
  "crime-servers": ⊟[
    ⊟{
      "name": "0.0.0.0",
      "ip-address": "0.0.0.0",
      "first-seen": "2008-12-31T22:00:00",
      "last-seen": "2110-12-31T22:00:00"
    },
    ⊟{
      "name": "ifr001.comli.com",
      "ip-address": "66.197.250.198",
      "first-seen": "2011-01-12T13:28:18",
      "last-seen": "2013-10-01T09:00:23.63"
    },
    ⊟{
      "name": "prava-servise.ru",
      "ip-address": "77.221.130.39",
      "first-seen": "2011-01-17T15:30:49",
      "last-seen": "2013-10-01T09:00:23.63"
    },
    ⊟{
      "name": "irvine-chiropracticcenter.com",
```

Formats

Seculert’s API can accept data and return data in the form of a HTTP request and a JSON object over HTTP response. These formats allow you to write your applications and simple scripts in any programming language that can read HTTP and JSON.

Request/Response

Once your response is generated it will appear in the right side of the Request/Response Table of the API Console.



```
GET /v2/CrimeServers?api_key=cd6df502-8801-
4758-ae0e-b9e9972e8618 HTTP/1.1
Host: seculert-prod.apigee.net
X-Target-URI: http://seculert-prod.apigee.net
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
X-AspNet-Version: 4.0.30319
X-AspNetMvc-Version: 4.0
Date: Sun, 14 Jul 2013 09:29:01 GMT
Content-Length: 1802994
Content-Type: application/json; charset=utf-8
X-Powered-By: ASP.NET
Server: Microsoft-IIS/7.5
Cache-Control: private

⊟{
  "crime-servers": ⊟[
    ⊟{
      "name": "0.0.0.0",
      "ip-address": "0.0.0.0",
      "first-seen": "2008-12-31T22:00:00",
      "last-seen": "2110-12-31T22:00:00"
    },
```

Reviewing the response in the API Console allows you to understand its format and the meaning of the data in the most efficient way; faster than reading dense technical documentation.

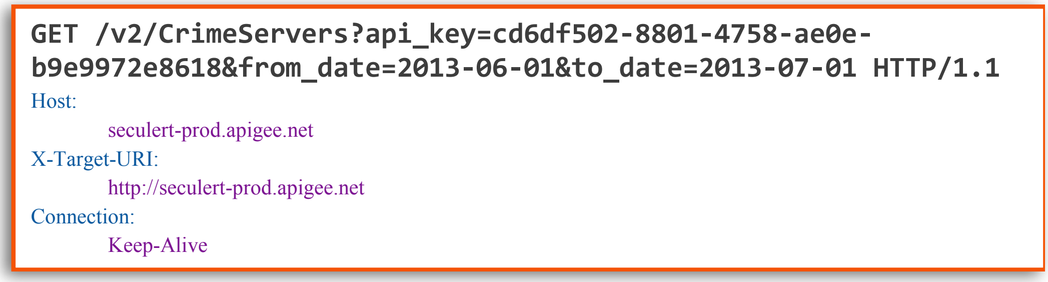
You can also check the Request section of the table on left side for the exact HTTP request you sent and the target URL.

LEVERAGING THE DATA

Data Generated

The data generated by Seculert can transform your existing security defenses into a complete APT solution. The data from each of Seculert's unique technologies can be accessed via the API. Subsequently, the returned data and format are different for each method. For specifics please refer to our API Guide.

You can filter the data pulled in order to focus on specific dates, times and drill down to a specific incident. This is accomplished by setting different parameters in your query prior to pulling from the API. For example, if you want to pull information regard the most recent threats, you would specify a date range that would reflect your request.



```
GET /v2/CrimeServers?api_key=cd6df502-8801-4758-ae0e-
b9e9972e8618&from_date=2013-06-01&to_date=2013-07-01 HTTP/1.1
Host:
        seculert-prod.apigee.net
X-Target-URI:
        http://seculert-prod.apigee.net
Connection:
        Keep-Alive
```

Example of JSON Filter

Botnet Interception

Through the API a GET can retrieve two types of data feeds from collected by botnet interception- crime servers and threat intelligence records. The data feed could include a list of crime servers and the time period they were observed to be active; as well as display all the incidents that were detected by Seculert for you, including the employees' internal and remote access, partners and customers.

Properties of Data Feed for Crime Servers

Header Name	Description	Data Type
Name	The name of the crime server	string
IP-Address	The IP address of the crime server	string value
First-Seen	The date and time	datetime
Last-Seen	The date and time	datetime

Properties of Data Feed for Threat Intelligence Records

Field Name	Description	Data Type
ID	Unique identifier	number
Bot-ID	The name of the botnet	string
Crime-Server-Name	The name of the machine	string
First-Seen	The date and time	datetime
IP-Country-Code	IP code of the crime server's country	string
Last-Seen	The date and time	datetime
Source-IP	IP address of the crime server	string value
State	Status of the incident: ۱ open, ۲ ignored, ۳ closed	number
Threat-Type-Name	Name of the threat family	string
Total-Records	Number of occurrences	
Zone-Name	Degree of separation from your internal network	
Records		list of objects
• Raw-Data	The data in the intercepted communication	string
• Domains	The domains mentioned in the communication	string
• Emails	The emails mentioned in the communication	string
• Added-Date	The date and time	datetime
• Timestamp	The time the communication occurred	datetime
• Visited-Domains	The domains visited that triggered the communication	string

Automated Traffic Log Analysis

Through automated traffic log analysis you can understand which computers are compromised and could potentially show evidence of an APT attack. In order to optimize your security, your organization would upload the following HTTP log data to Seculert either manually or automatically:

Basic parameters of log analysis

Field Name	Description	Data Type
Timestamp	The date and time of the request	datetime
MachineIP	The IP address of the source machine	string value
Method	HTTP request method (GET/POST)	string
URI Host	HTTP request identifier	string
URI Path	HTTP request	string
URI Query	HTTP request	string
User-Agent	Internet client software	string
Referrer	HTTP request referrer (optional)	string

An API GET call will can retrieve the results of the log analysis.

Properties of the results of traffic log analysis

Field Name	Description	Data Type
ID	Log ID	number
Crime-Server-Name	The name of the machine	string
First-Seen	The date and time	datetime
Last-Seen	The date and time	datetime
Source-IP	The IP of the machine	string value
State	Status of the incident: 1 open, 2 ignored, 3 closed	string
Threat-Type-Name	Name of the threat family	string
Total-Records	Number of records	string
Records		list of objects
• Added-Date	The date and time	datetime
• Timestamp	The date and time	datetime
• Raw-Data	The data in the log	string

Elastic Sandbox

The API features three simple calls for uploading and retrieving data related to the Elastic Sandbox:

- A web request that uploads files via HTTP, followed by a response including the upload's identification key
- A request that retrieves the results of the analysis using the identification key
- A request that retrieves the network capture file (.PCAP) of the network traffic triggered by the running of the suspicious files

Properties of returned results of the scan

Field Name	Description	Data Type
ScanDate	The date the file was scanned	datetime
Classification	Was the file malicious? If so, what kind?	string
DnsRecords	DNS activities of the file	list of objects
• Domain	Domain name	string
• IP	IP address	string value
URLRecords	URL activities of the file	list of objects
• URL	URL address	string
• Method	HTTP request method	string
• IP	IP address	string value

DATA APPLICATIONS

The data generated by Seculert transforms existing perimeter security defenses into a complete APT solution. The data from each of Seculert's unique technologies accessed via the API and integrated with your on-premises devices allows you to get information on new threats as they emerge, identify current threats within your organization, determine what information has been compromised, prioritize attack incidents and coordinate your response. Additional applications include:

- Filtering data based on specific times to identify the most recent threats
- Accessing lists of URLs to block
- Correlating data regarding incidents, including machine names and source IPs, into your SIEM
- Directing firewalls to temporarily block compromised computers from entering crucial zones within your network and accessing sensitive company information
- Keeping internal firewalls up-to-date
- Pushing malicious files quarantined by your antivirus solution into the elastic sandbox for analysis to better assess the likelihood of an advanced malware attack
- Determining which SIEM incidents require further investigation or escalation
- Writing a plugin to mail servers to push suspicious files from inbound emails to the elastic sandbox for analysis
- Updating corporate web proxies or secure web gateways with Seculert's list of crime servers to block
- Ensuring that botnet infected computers do not continue to communicate with the crime servers
- Uploading identifying factors compromised computers into the firewall policies to isolate infected computers and block them from accessing internal assets and data centers
- Pinpointing the information that has been compromised, such as credentials of remote employees or customers

BEST PRACTICES

In order to maximize the impact Seculert's API can have on your network security, keep these best practices in mind.

- Use the API. The more frequent your pulls from the API the more up-to-date your threat protection capabilities stay.
- Always try to combine multiple API calls into a single TCP connection when possible. This will streamline the process saving you time.
- Avoid making duplicate requests, as it will slow down your response time.
- Learn how to best integrate the data with your current systems by seeing where it provides you the most value.
- Keep your devices linked to the API, increasing their ability to protect your network and alert you as threats occur.
- Integrate the API with your SIEM so incidents can be correlated efficiently.
- The best way to use the API is to learn from experience.