SecurityTrailsAPI

Release 0.0.1

Dan Duffy

Jul 20, 2019

CONTENTS:

CHAPTER

ONE

SECURITYTRAILSAPI

1.1 securitytrailsapi package

1.1.1 Submodules

1.1.2 securitytrailsapi.api_handler module

class securitytrailsapi.api_handler.**SecurityTrailsAPI**(*api_key*)

Bases: object

explore_ips(*ipaddress*)

Returns the neighbors in any given IP level range and allows you to explore closeby IP addresses.

Parameters **ipaddress** (*str, required*) – The ipaddress/range you wish to find neighbours for.

Returns A dict formatted response from the Security Trails API.

Return type dict

feeds_domains(*record_type*, *search_filter*, *tld*, *ns*, *date*)

Fetch zone files including authoritative nameservers.

Parameters

- **record_type** (*str, required*) – Valid domain values are "all", "dropped", "new" or "registered"
- **search_filter** (*str, optional*) – Valid filter values are "cctld" and "gtld"
- **tld** (*str, optional*) – Can be used to only return domains of a specific tld, such as "com"
- **ns** (*bool, optional*) – Show nameservers in the list.
- **date** (*str, option*) – Date to fetch data for, format YYYY-MM-DD, e.g. 2019-06-11. Default is today.

Returns A dict formatted response from the Security Trails API.

Return type dict

find_associated_domains(*domain*, *page*)

Find all domains that are related to the given domain.

Parameters

- **domain** (*str, required*) – The domain to find associated domains for.

- **page** (*int, optional*) – The page of the returned results.

Returns A dict formatted response from the Security Trails API.

Return type dict

get_domain(*domain*)

Returns the current data about the given domain. In addition to the current data, you also get the current statistics associated with a particular record. For example, for A records you'll get how many other domains have the same IP.

Parameters **domain** (*str, required*) – The domain to find associated domains for.

Returns A dict formatted response from the Security Trails API.

Return type dict

get_whois(*domain*)

Returns the current WHOIS data about a given domain with the stats merged together.

Parameters **domain** (*str, required*) – The domain to find WHOIS data for.

Returns A dict formatted response from the Security Trails API.

Return type dict

history_by_domain(*domain, page*)

Returns historical WHOIS information about the given domain.

Parameters

- **domain** (*str, required*) – The domain to find historical WHOIS data for.
- **page** (*int, optional*) – The page of the returned results.

Returns A dict formatted response from the Security Trails API.

Return type dict

history_by_record(*domain, record_type, page*)

Lists out specific historical information about the given hostname parameter.

Parameters

- **domain** (*str, required*) – The domain to find historical data for.
- **record_type** (*str, required*) – The record type to search for. Allowed values: a, aaaa, mx, ns, soa or txt
- **page** (*int, optional*) – The page of the returned results.

Returns A dict formatted response from the Security Trails API.

Return type dict

ip_search_stats(*query*)

Lists out specific historical information about the given hostname parameter.

Parameters **query** (*str, required*) – The API query e.g. *ptr_part='amazon.com'*.

Returns A dict formatted response from the Security Trails API.

Return type dict

list_subdomains(*domain*)

Returns subdomains for a given hostname.

Parameters **domain** (*str, required*) – The domain to find subdomains for.

Returns A dict formatted response from the Security Trails API.

Return type dict

`list_tags`(*domain*)

Returns tags for a given hostname.

Parameters **`domain`** (*`str, required`*) – The domain to find tags for.

Returns A dict formatted response from the Security Trails API.

Return type dict

`ping`()

Use this function to test your authentication and access to the SecurityTrails API.

Returns A dict formatted response from the Security Trails API.

Return type dict

`search_domain_dsl`(*query*, *include_ips*, *page*, *scroll*)

Filter and search specific records using SecurityTrails DSL.

Parameters

- **`query`** (*`str, required`*) – A DSL query e.g. *whois_email='domain-contact@oracle.com'*.
- **`include_ips`** (*`bool, optional`*) – Resolves any A records and additionally returns IP addresses.
- **`page`** (*`int, optional`*) – The page of the returned results.
- **`scroll`** (*`bool, option`*) – Request scrolling. See Scrolling API .

Returns A dict formatted response from the Security Trails API.

Return type dict

`search_domain_filter`(*search_filter*, *include_ips*, *page*)

Filter and search specific records.

Parameters

- **`search_filter`** – A search filter constructed from *`SecurityTrailsAPIFilter`*.
- **`include_ips`** (*`bool, optional`*) – Resolves any A records and additionally returns IP addresses.
- **`page`** (*`int, optional`*) – The page of the returned results.

Returns A dict formatted response from the Security Trails API.

Return type dict

`search_ips`(*query*, *page*)

Search IP's using SecurityTrail's DSL.

Parameters

- **`query`** (*`str, required`*) – A DSL query e.g. *ptr_part='ns1'*.
- **`page`** (*`int, optional`*) – The page of the returned results.

Returns A dict formatted response from the Security Trails API.

Return type dict

search_statistics(*search_filter*)

Search IP's using SecurityTrail's DSL.

Parameters **search_filter** – A search filter constructed from *SecurityTrailsAPIFilter*.

Returns A dict formatted response from the Security Trails API.

Return type dict

usage()

Return your current API usage stats.

Returns A dict formatted response from the Security Trails API.

Return type dict

class securitytrailsapi.api_handler.**SecurityTrailsAPIFilter**

Bases: object

1.1.3 Module contents

CHAPTER

TWO

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

INDEX