Symantec
by Broadcom Software

Data Feeds API Guide: Email Security.cloud

Table of Contents

Introduction

Overview

Published 1/6/2024

The Email Security.cloud Data Feeds API is an HTTP interface that offers Email Security.cloud, Email Threat Detection and Response and Email Threat Isolation customers comprehensive actionable threat intelligence data on all of the email that Email Security.cloud scans. Though this HTTP interface is not a REST API, it is similar to one in that it has no functional state maintained on the server.

Using this nearly real-time data, you can provide reporting and dashboards across the multiple services that your clients use. The extracted data is returned in JSON format. You can feed the data into your SIEM so that it can be integrated with other security-related data and used for your security monitoring requirements.

The use of HTTPS is enforced, which secures and encrypts the data transmitted. Feed requests are authorized using Basic Authentication. Standard HTTP status codes are used during the processing of all data feeds.

You enable access to the data feed by checking a box in the Email Security.cloud portal. The portal also provides a downloadable sample script and *Data Feeds API Guide: Email Security.cloud* (this document) to help you get started quickly. You can use the script to access the feed and save feed data locally, and then point your SIEM to the saved files. You can also configure your SIEM to poll the web service directly.

The Symantec Email Security.cloud support team continually monitors and proactively manages the collection of data into the Symantec Email Security.cloud central data warehouse.

Symantec Email Security.cloud data feeds are streamed on request through one primary URL that includes all of the available data for your organization. Data for some services (such as Anti-Spam) is included for all customers. Other services (such as Threat Isolation) require separate purchase. Your primary feed will include data for all services that you have purchased in addition to the data provided for all customers. You can also choose to stream various subsets of the data, although streaming all of the available data is recommended.

Note to legacy Email Security.cloud Email Data Feeds API users

A small number of Email Security.cloud ATP customers use a previous version of the Data Feeds API. That previous version provides data only for the email that is identified as malware, in CSV format. This newer version of the Data Feeds API provides JSON data for all email, additional data points for the email that Malware detects, along with URL and Attachment Isolation (called Threat Isolation) data, Click-time URL Protection data, Anti-Spam data, data for URLs in clean inbound email and attachments, Email Threat Analytics data, and email delivery and TLS information.

Because this new API handles data for a much larger amount of Email Security.cloud-processed mail, it has been completely redesigned and re-architected. As a result, previous customers must rework how they use the data that the new API produces. Existing API client implementations cannot consume data from the new feeds without alteration.

Symantec recommends that you keep your original implementation in place until you have experimented with the new feed. Once you are satisfied with your new implementation, you can decommission your previous feed along with its client application.

More information

See the https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/email-security-cloud/1-0.html topic "Email Threat Detection and Response: Email Data Feed" for information about how to configure Email Security.cloud to enable the feed.

Detailed Design

Service API details

The Symantec Email Security.cloud Email Data Feeds API consists of three components: a client application, an API server application, and the central data warehouse. Symantec Email Security.cloud develops and manages the API server application and the central data warehouse. The API server application and data warehouse reside internally within the Symantec Email Security.cloud infrastructure. The service keeps seven days of rolling data, so that you can reset your stream to start consuming data up to seven days in the past.

Your organization can choose to use a plugin specifically created to work with your SIEM, such as Splunk or IBM QRadar. Your organization can also choose to develop and maintain a client application. You can use the sample Python script available on the Related Documents page along with the test data feed to get a head-start on developing your own client application.

Client application

The client application is usually a non-browser-based application.

The client application submits an HTTPS `GET` request to the URI provided by Symantec Email Security.cloud and processes the data stream that is returned. For security authentication, the request must provide valid Email Security.cloud portal login credentials and must handle any HTTP status codes returned.

The client application must accept, store, and include stored cookies in requests as specified in RFC 6265, so as to maintain proper session state and avoid duplicating or missing data.

HTTP status codes

The Data Feeds API conforms to the HTTP/1.1 standard per rfc2616 (see http://www.w3.org/Protocols/).

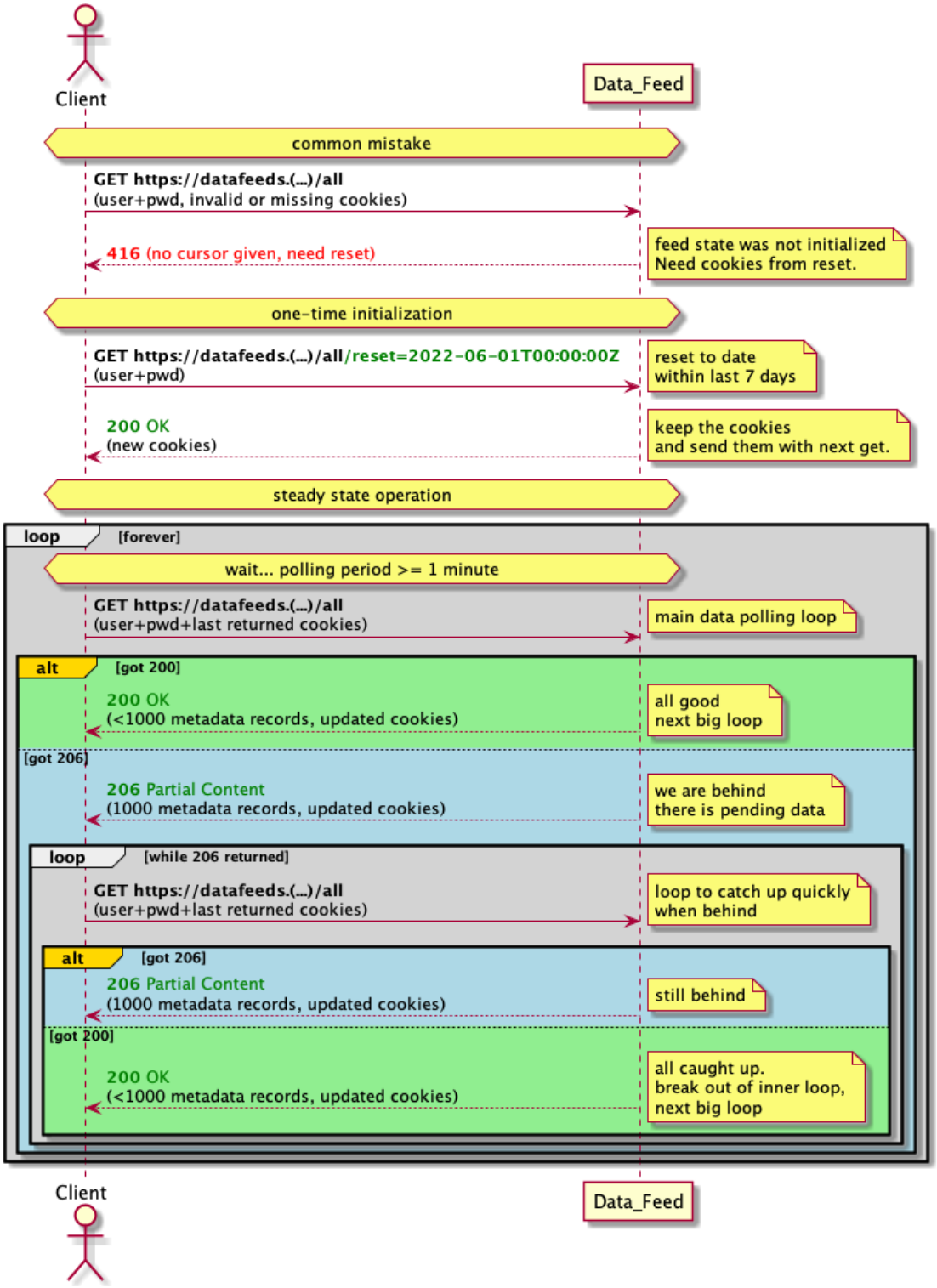
Under normal operation, successful requests will return HTTP 2xx status codes, whereas problems will be indicated by returning HTTP 4xx or HTTP 5xx status codes (where xx is any digit).

The current maximum number of records that can be returned in one request is 1000. If the number of records returned is greater than 1000 (indicated by the HTTP status code 206), then you submit another request. Continue submitting requests until the HTTP status code 200 is returned.

Other status codes are returned based on different conditions. For information about these status codes, see Responses.

Client-Service interaction

The following sequence diagram shows a client application interacting with the Email Data Feed API. Please note that this figure mostly ignores error flows, and is intended to show proper initialization and steady-state polling, including the ability to quickly catch up to the latest data when required. To simplify the messages, the URL has been shortened, but it should read https://datafeeds.emailsecurity.symantec.com/all, which in this example refers to the `all` feed.



Initialization is done through a reset operation. This sets the point in time within the service's seven-day rolling buffer from which you are interested in starting to retrieve data. The reset operation, if it succeeds, will return the code 200 and some cookies, but no data.

The cookies contain the state of the stream. The client application must accept, store, and include stored cookies in requests as specified in RFC 6265 to maintain proper session state and avoid duplicating or missing data.

IMPORTANT: Limit the use of reset

The reset option on the URIs is meant for only two use cases:

1) Initial setup of the feed.

2) Bulk re-download of missing data because of a disaster at the client site.

All other uses will cause duplicates and/or data gaps because of the (intentionally) limited reset time resolution. The proper way to keep track of where you are in the feed is to provide the last cookies and save the updated cookies for each query as documented above. The state of the stream is stored in the cookies, and the downloaded data will be complete when the cookies are provided.

Data streams

The client application receives a stream of data in the JSON format that contains the metadata describing your organization's email. You can choose to receive information from different streams, by changing the last part of the path of the URL.

- `all` This feed contains a superset of the content of all of the streams for the services you have purchased. It also includes metadata for URLs in clean inbound email and attachments, and can optionally include email delivery data by appending the URL parameter like this: `…/all?include=delivery` . If for some reason you can't use the `all` feed and want a specific subset of the available data, you can use the following streams:

- `malware` (email with detected malware only).
- `test` (email data that you use to learn about the format and contents of the data available to you from the feeds).
- Threat `isolation` (URL and Attachment Isolation event data only).
- `clicktime` (Click-time URL Protection event data only).
- Anti-`spam` (spam detection and action data only).
- Email Threat Analytics (`ec_reports`): (information about all emails blocked by Email Security.cloud's Anti-Malware service, as well as emails blocked because their attachments are determined to be malicious through Cynic sandbox execution).
- `delivery` (information about email delivery and TLS compliance)

The best way to learn more about the feeds is to review information about the metadata elements that are included in them. See All email data feed elements.

To learn about the structure of the JSON data that the feeds produce, use the sample script to connect to the `test` feed. You can then examine the generated data. You can also review the example data that the other available feeds produce. See Sample JSON files produced by data feeds.

Redundancy and failover

The API server application is hosted on Symantec Email Security.cloud, which uses distributed services with redundancy for data storage, processing, and serving. This architecture allows Symantec to experience server failures and compensate for them without affecting users.

Getting started

Overview

The easiest way to get started working with the data generated by the Data Feeds API is to use the sample Python script supplied through the portal to connect to the `test` data feed. (You can also download the sample Python script from the Related Documents page of the online help.) Once you have access to data that resembles your own customer-specific email metadata, you can determine how best to structure your client application to make the data available to your SIEM, dashboard or correlation application. You can use the Python script as-is, or as a model on which to base a similar script or program in a different language. Once you have examined and worked with the data provided by the `test` feed, you can edit the script so that it points to the `all`, `malware`, Threat `isolation`, `clicktime` URL Protection, Email Threat Analytics, Anti-`spam`, `reports`, or `delivery` feeds. You can use the script to access the feed and save feed data locally, and then point your SIEM to the saved files. You can also configure your SIEM to poll the web service directly.

What you need to begin

The following three tasks must be performed before you begin implementing your API client application. All three tasks are performed in the Email Security.cloud portal by someone with portal administrator credentials. For detailed instructions on how to perform these steps, open the portal's online help (https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/email-security-cloud/1-0.html) and search for a topic called "Email Threat Detection and Response: Email Data Feed."

- Ensure that your Email Security.cloud portal administrator has created at least one new user account in the portal for authentication to the Email Data Feed service. The user account must have **View Statistics** permissions for the Email Threat Detection and Response service.
  - If you have purchased additional services in addition to Email Threat Detection and Response (such as URL or Attachment Isolation or Click-time URL Protection) and want to access data from these services in your feeds, then the user accounts used to access the feeds must have **View Statistics** permissions for the additional services in addition to **View Statistics** permissions for Email Threat Detection and Response.
  - You can use a single set of credentials to access multiple feeds, or to access the same feed multiple times, provided that you configure your client to save cookies separately to prevent overwriting. Standard rate limiting applies to data feed access, so we recommend that you do not download multiple copies of the same data. Instead, save copies locally if you need feed data in more than one location.
- Ensure that your portal administrator has downloaded the sample Python script that helps you connect to the feed URI. The script is contained in a compressed file called `NdfConfig.zip` that is saved to the administrator's computer by default.
- Ensure that your portal administrator has downloaded the *Data Feeds API Guide: Email Security.cloud* (this document), which explains how to use the script to access feed data.

Accessing and using test data with the sample Python application

To access and use `test` data from the Data Feeds API, you edit the configuration file, run the Python script, and examine the resulting data to determine how to use the data in your SIEM or other security monitoring applications.

Prerequisites

1. Locate and download an appropriate Python interpreter (version 3 and above) for your environment, and ensure that your system recognizes files with the .py extension and associates them with the interpreter.
2. Decompress the `NdfConfig.zip` file that contains the Python configuration and script files, and save them to a directory.

Edit the configuration file

1. Using a text editor such as Notepad++, open the configuration file `NdfConfig.json`:

```
{
 "user" : "USERNAME",
 "password" : "PASSWORD",
 "uri": "https://datafeeds.emailsecurity.symantec.com/test",
 "resetUri": "https://datafeeds.emailsecurity.symantec.com/
test?reset=2016-09-01T00:00:00Z",
 "files" : {
     "cookiesFilePath" : "C:\\EXAMPLE_FILE_PATH",
     "logsFilePath" : "C:\\EXAMPLE_FILE_PATH"
 }
}
```

2. Replace `USERNAME` and `PASSWORD` with the Email Security.cloud portal credentials provided by your administrator.
3. In the `uri` and `resetUri` fields, ensure that `FEED_NAME` is `test`, which is the default state for the configuration file.
4. In the `resetURI` field, change the time to the right of `reset=` to the date and time from which you want to start to read metadata.

   NOTE

   The `resetURI` mechanism is not used when you access data from the `test` feed, although it is required for the `all`, `malware`, Threat `isolation`, `clicktime` URL Protection, Anti-`spam`, Email Threat Analytics (`ec_reports`), and `delivery` feeds. It is included in the configuration file for use later when you want to access these other feeds. The Python script ignores the `resetUri` when it accesses the `test` feed.
5. On the `cookiesFilePath` line, specify the path at which to store the persistent cookies that are used to mark your place in the feed.
6. On the `logsFilePath` line, specify the path at which to store the log files that the Data Feeds API connection session produces.
7. Save and close `NdfConfig.json`.

Run the Python script

The `NdfConfig.zip` file you download from the Email Security.cloud portal contains both the configuration file and the Python script file itself, called `NdfScript.py`. To use the Python script to access `test` feed data:

- Run `NdfScript.py`. If you specified the `test` URI in the configuration file, then you should begin to receive feed data immediately. If you specified `all`, `malware`, `isolation`, `clicktime`, Email Threat Analytics (`ec_reports`), `spam`, or `delivery` in the configuration file, then you must also have specified a time as part of the `resetUri`. Feed data becomes available at the time you specified.

Examine the `test` feed contents

The best way to understand the structure and content of the data that the Data Feeds API returns is to examine the data you receive from the `test` URI. In addition, you can also examine representations of the JSON files that are included in this document that illustrate a variety of scenarios and conditions. See Sample JSON files produced by data feeds.

Using the Splunk plug-in application

You can use the Splunk application to collect data from the Data Feeds API (and some complimentary feeds). Download the app along with instructions for its use at https://tipp-integrations.broadcom.com/partner-downloads/splunk.

Using the IBM QRadar plug-in application

You can use the IBM QRadar application to collect data from the Data Feeds API (and some complimentary feeds). Download the app along with instructions for its use at https://exchange.xforce.ibmcloud.com/hub/extension/5d544958d8b44844315889c432f07e04.

Building your client application

The ways you intend to use the data available through the Data Feeds API, along with your own preferences concerning programming languages and environments, determine the characteristics of the client application that you build. If simply accessing feed data is your goal, then using a script like `NdfScript.py` may meet your needs.

If you intend to sort or otherwise process data from the feeds as a prerequisite for importing the data to a SIEM or other system, then you may need to build a more complex application. You can extend the functionality of `NdfScript.py` itself, or write additional scripts in Python. You can also use `NdfScript.py` and `NdfConfig.json` as examples to speed the process of building a client in your preferred language or environment.

Your client application must meet the following minimum requirements:

- Support the storage of Email Security.cloud credentials that are configured initially by your Email Security.cloud portal administrator.
- Specify the desired feed URI (`all`, `malware`, Threat `isolation`, `clicktime`, `spam`, `delivery`, `ec_reports`, or `test`).
- Support the storage of persistent cookies that are received from the Data Feeds API's HTTP response(s). If the same client accesses multiple feeds, cookies must be stored separately so that they are not inadvertently overwritten. The client application must accept, store, and include stored cookies in requests as specified in RFC 6265, so as to maintain proper session state and avoid duplicating or missing data.
- Support the storage of log data for monitoring and debugging.
- Support sending an HTTP `GET` request to 'reset' to obtain the initial cookie and to bootstrap the feed. For subsequent requests, the client must accept and pass back persistent cookies to the service so that its place in the feed updates properly.

  The reset request is sent as a string representing the date from which to start reading the metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When you call the service for the first time, if you don’t provide the reset request a 416 status code is returned. The reset request itself returns a 200 status code, but no data items. Requests that follow the initial reset request return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC). You must run the Python script again to return data from that point onward.

  The Python script must be called repeatedly to get the most recent data, using a utility such as Cron (for UNIX-like environments) or Task Scheduler (for Windows). We recommend calling the script once per minute for organizations of 20,000 seats or more, and once every 5 minutes for smaller organizations. To consume the data that the script returns, point your SIEM to the directory that contains the JSON files. Your client application should clean this directory periodically to avoid the accumulation of previously consumed JSON files.

Data feed

Introduction

This chapter provides detailed information about the Data Feeds API's available feeds:

Feed name	Description	Further information
`all`	Contains metadata for all scanned email. This feed contains a superset of the data in all of the available feeds for the services you have purchased. Also includes metadata for URLs in clean inbound email and attachments.	Included in the Email Security.cloud service. No additional purchase required.
`malware`	Contains data about malware-containing email only.	Included in the Email Security.cloud service. No additional purchase required.
`test`	Contains generic metadata that is not specific to your company that can be used to learn more about the feed and to implement your client application or SIEM integration.	Included in the Email Security.cloud service. No additional purchase required.
Threat `isolation`	Contains data from events logged by the URL and Attachment Isolation features, which ensure threats are executed in an isolation platform.	Requires purchase of Email Threat Detection and Response service and the Threat Isolation feature.
`clicktime`	Contains metadata from events generated by end-user clicks on URLs that were rewritten by the Click-time URL Protection feature.	Requires purchase of Email Threat Detection and Response service and the Click-time URL Protection service.
Anti-`spam`	Contains metadata about email that the Anti-Spam service has detected as spam, as well as the action taken as a result of that detection.	Included in the Email Security.cloud service. No additional purchase required.
Email Threat Analytics (`ec_reports`)	Contains contextual information about all emails blocked by Email Security.cloud's Anti-Malware service, as well as emails blocked because their attachments are determined to be malicious through Cynic sandbox execution. This information can be used to gauge the level of risk an email attack poses, so that customers can differentiate focused attacks from mass campaigns.	Requires purchase of Email Threat Detection and Response.
Email `delivery` data	Contains metadata that describes both inbound and outbound email delivery to provide visibility into email tracing, TLS compliance, and routing.	Included in the Email Security.cloud service. No additional purchase required.

Customers who have purchased the Email Threat Isolation or Click-time URL Protection services in addition to the Email Threat Detection and Response service can choose to access their Anti-Spam, Threat (URL/Attachment) Isolation, Click-time URL Protection events, or Email Threat Analytics data as part of the `all` data feed, or they can access their Threat Isolation, Click-time URL Protection, Anti-Spam, or Email Threat Analytics data separately in the `isolation`, `clicktime`, `spam`, `ec_reports`, or `delivery` feeds. See Feed for Threat data, or Feed for URL Protection data, or Feed for Anti-spam data, or Feed for Email Threat Analytics (ec_reports) data or Feed for email delivery data for information on how to configure your permissions to control whether feed data is accessed via the `all` feed or is viewed only in the individual feeds.

Version information

Version: 1.0

URI schemes

For the `all`, `malware`, `test`, Threat `isolation`, `clicktime`, Anti-`spam`, Email Threat Analytics (`ec_reports`), and Email `delivery` data feeds:

Host: https://datafeed.emailsecurity.symantec.com

Scheme: HTTPS

Feed for all email data

The `all` email data feed contains metadata for all email processed by Email Security.cloud, but your ability to access this data is controlled by the services you have purchased and the permissions you have set on the ClientNet accounts used to access the feed.

For example, if you have purchased the Click-time URL Protection service and have added **View Statistics** permissions for Clicktime URL Protection to the ClientNet account used to access the feed, the `all` feed will allow you to access Click-time URL Protection events data through the `all` feed. The `all` feed also contains Anti-Spam data. Details about attachment files are included in the stream. Metadata for email that is blocked or rejected during the SMTP conversation is not included in the feeds.

The `all` feed also includes metadata for URLs contained in clean inbound email, limited to the first 125 unique URLs in the email body and to the first 125 unique URLs found in attachments. The maximum length for URLs is 2,048 characters. Whitelisted URLs are included in the metadata.

> **NOTE**
>
> Because the average inbound email includes approximately 10 URLs, the inclusion of clean URL metadata in the `all` feed results in an approximately 40% increase in average record size. Symantec recommends that you verify that your systems have the capacity to handle this change in data size.

See All email data feed elements.

Get metadata for all emails

```
GET /all[?reset=YYYY-MM-ddThh:mm:ssZ]
```

Description

Returns metadata for all of your emails. Contains Threat Isolation and Click-time URL Protection events data if you have purchased the Email Threat Isolation and Click-time Protection features in addition to Email Threat Detection and Response. Also contains Email Threat Analytics data if you have purchased Email Threat Detection and Response. The `all` feed also contains metadata about Anti-Spam detections and actions and metadata for URLs contained in clean inbound email. It can contain metadata that describes both inbound and outbound email delivery to provide visibility into email tracing, TLS compliance, and routing, but you must opt in by appending a parameter to have email delivery data included in the `all` feed.

Parameters

Type	Name	Description	Schema
Header	Cookie optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - could mean unauthorized, or mismatch between credentials and authorization cookie.	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Produces

`application/json`

Security

Type	Name
basic	BasicAuth

Feed for malware data

The `malware` feed contains metadata for all email that is blocked by Email Security.cloud because it contains malware. Details about attachment files are included in the stream. Metadata for email that is blocked or rejected during the SMTP conversation is not included in the feeds.

See Malware data feed elements.

Get metadata for malware emails

```
GET /malware[?reset=YYYY-MM-ddThh:mm:ssZ]
```

Description

Returns metadata for emails that contain malware.

Parameters

Type	Name	Description	Schema
Header	Cookie optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onwards.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Security

Table 1:

Type	Name
basic	BasicAuth

Produces

`application/json`

Feed for test data

The `test` feed returns a set of metadata that demonstrates the range of individual data items that can appear in your `all`, `malware`, Threat `isolation`, `clicktime`, anti-`spam`, and email `delivery` feeds. However, the `test` feed does not contain data for URLs in clean inbound email and attachments. You can use the `test` data to set up your client application as well as to configure the receiving SIEM to properly handle production feed data.

> **NOTE**
>
> Unlike the `all`, `malware`, Threat `isolation`, `clicktime`, Email Threat Analytics (`ec_reports`), Anti-`spam`, and email `delivery` feeds, the `test` feed does not use a cursor mechanism to keep track of the date and time on which the feed was last accessed, and thus does not require a reset request to obtain the initial cookie and bootstrap the feed. Accordingly, the sample Python script does not call a reset on `test` URIs.

Get test metadata

`GET /test`

Description

Returns a set of test metadata useful for debugging a feed client. Use this when you don't want to consume your actual feed but you want to test interactions with the feed and the format of the JSON data that is returned.

Parameters

Type	Name	Description	Schema
Header	Cookie Optional	**Note:** The following information is not applicable to the `test` feed. It applies to the `all`, `malware`, Threat `isolation`, `clicktime` URL Protection, Email Threat Analytics (`ec_reports`), Anti-`spam`, and email `delivery` feeds only. However, it is technically optional, so it is described here. The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset Optional	**Note:** The following information is not applicable to the `test` feed. It applies to the `all`, `malware`, Threat `isolation`, `clicktime` URL Protection, Email Threat Analytics (`ec_reports`), Anti-`spam`, and email `delivery` feeds only. However, it is technically optional, so it is described here. A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Security

Type	Name
basic	BasicAuth

Produces

`application/json`

Feed for Threat isolation data

The Threat Isolation feature ensures URLs and attachments are executed in an isolation platform, which isolates malicious content and prevents it from being delivered to your network or end users' devices. Events are logged when URLs and attachments are isolated. The Threat `isolation` feed provides metadata from these logged events. You must purchase the Email Threat Isolation service in addition to the Email Threat Detection and Response service to receive Threat `isolation` data.

> **NOTE**
>
> Customers who have purchased the Email Threat Isolation service in addition to the Email Threat Detection and Response service can choose to access Threat Isolation events data either as part of their `all` feed, or in a separate Threat `isolation` feed that contains Threat Isolation data only. You control whether Threat Isolation data can be viewed as part of your `all` feed or viewed in a separate `isolation` feed through the permissions you assign to the ClientNet accounts that you set up to access feed data. If you create an account that contains **View Statistics** permissions for both Email Threat Detection and Response and Email Threat Isolation, then the `isolation` data is accessible through your `all` feed.

See Threat data feed elements.

Get Threat isolation metadata

`GET /isolation[?reset=YYYY-MM-ddThh:mm:ssZ]`

Description

Returns metadata from events logged by the Threat Isolation feature, which executes URLs and attachments in an isolation platform to block delivery of malicious content to your network or end users.

Parameters

Type	Name	Description	Schema
Header	Cookie Optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset Optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Security

Type	Name
basic	BasicAuth

Produces

`application/json`

Feed for Clicktime URL Protection data

The Click-time URL Protection feature rewrites and performs checks on URLs in the emails that are delivered to your organization's users. The `clicktime` URL Protection feed provides metadata from events generated by end-user clicks on these rewritten URLs.

> **NOTE**
>
> Customers who have purchased the Click-time URL Protection service in addition to the Email Threat Detection and Response service can choose to access Clicktime events data either as part of their `all` feed, or in a separate `clicktime` feed that contains non-isolated Click-time data only. You control whether Click-time data is accessible in your `all` feed or provided in a separate `clicktime` feed through the permissions you assign to the ClientNet accounts that you set up to access feed data. If you create an account that contains **View Statistics** permissions for both Email Threat Detection and Response and Click-time URL Protection, then the `clicktime` data is accessible as part of your `all` feed.

See URL Protection data feed elements.

Get Clicktime metadata

```
GET /clicktime[?reset=YYYY-MM-ddThh:mm:ssZ]
```

Description

Returns metadata from events logged by the Click-time URL Protection feature, which rewrites and performs checks on URLs in the body of HTTP and HTTPS emails that are delivered to your organization's users. URLs in attachments are not rewritten. Rewriting allows the Email Security.cloud service to manage access to the URL to ensure the destination remain free of spam, phishing, or other malicious content.

URLs that are rewritten by Click-time URL Protection are checked every time an end-user clicks on them. Events are also logged when users click the rewritten URLs. The `clicktime` feed provides metadata about these events.

If your organization has also purchased the Threat Isolation feature, you can use the URL Isolation metadata from the Threat `isolation` feed in combination with the data from the `clicktime` feed to form a complete picture of all URLs clicked by your end users, whether isolated or not.

The Email Threat Detection and Response service is a prerequisite for both Threat Isolation and Click-time URL Protection.

Parameters

Type	Name	Description	Schema
Header	Cookie Optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset Optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Security

Type	Name
basic	BasicAuth

Produces

`application/json`

Feed for Anti-spam data

The Anti-Spam service lets you define the detection methods used to detect spam messages, as well as the action taken when spam is detected. The Anti-`spam` feed provides metadata about email detected as spam, as well as the action taken as a result of that detection.

See Anti-spam data feed elements.

Get Anti-spam metadata

```
GET /spam[?reset=YYYY-MM-ddThh:mm:ssZ]
```

Description

Returns metadata from events logged by the Anti-Spam service, which lets you define the detection methods to use to detect spam messages, as well as the action to take when spam is detected.

Parameters

Type	Name	Description	Schema
Header	Cookie Optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset Optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content

HTTP Code	Description	Schema
503	Service Unavailable - try again later	No Content

Security

Type	Name
basic	BasicAuth

Produces

`application/json`

Feed for Email Threat Analytics (ec_reports) data

The Email Threat Analytics (ETA) service provides customers with contextual information about all emails blocked by Email Security.cloud's Anti-Malware service, as well as emails blocked because their attachments are determined to be malicious through Cynic sandbox execution. ETA evaluates blocked emails to gauge the level of risk an email attack poses, so that customers can differentiate focused attacks from mass campaigns. The service helps customers assess how unique they are as victims, whether an email is part of a broader attack campaign aimed at similar enterprises, and what possible countermeasures are likely to be most effective.

See Email Threat Analytics (ec_reports) data feed elements.

Get Email Threat Analytics metadata

`GET /ec_reports[?reset=YYYY-MM-ddThh:mm:ssZ]`

Description

Returns metadata from the Email Threat Analytics reporting service, which provides daily intelligence reports about relevant emails blocked by Symantec for each organization. Customers can then assess the risk associated to those emails and prioritize further investigations. Email-borne malware detections are clustered across all Symantec customers by finding links between related attacks using machine learning. Global and customer-centric stats are calculated from those clusters in order to understand better the following:

- Timeline of the attack.
- Number of Symantec customers experiencing the same email threat.
- Attack characterization (detection name, geographical region, IPs, IOCs, etc.).
- Exposure of the customer's organization versus other Symantec Email Security.Cloud customers.
- Most exposed accounts in the customer's organization.
- Email threat profile (highly focused, focused, or mass).

Symantec ranks email threats depending on how many customers have been targeted and the number of emails related to that attack as follows:

- Highly focused: less than five related emails or seen in less than five customers.
- Focused: less than 20 related emails or seen in less than 20 customers.
- Mass: widespread attack affecting many customers.

While attacks are calculated over emails that have been blocked by Symantec over the last 30 days, ETA reports only contain attacks that overlap a two-week moving window; the previous two weeks are used as a baseline. Therefore, the

attack profile used to characterize a particular email can change as newer malicious email data becomes available to the service.

Parameters

Type	Name	Description	Schema
Header	Cookie Optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset Optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Security

Type	Name
basic	BasicAuth

Produces

`application/json`

Feed for Email Delivery data

The Email Data Feed service already contains metadata about clean email, malware, spam, Click-time-protection clicks, Isolation events, and email targeted attacks. The service now includes metadata for email delivery. This delivery data includes information about:

- sender and recipient
- delivery status and attempts
- Connection host name
- banner
- IP addresses and responses
- TLS information
- DKIM signature
- Cross-reference to other records for the same email: `xMsgRef`

The delivery feed contains one record per attempt, for both inbound and outbound deliveries. The feed stores 7 days' worth of delivery records. Notification emails are not supported.

See Email delivery data feed elements.

Get metadata for email delivery

By default, the `/all` feed will not return any delivery data. You can opt in to consume delivery data (which can cause a 10-15% increase in data volume) by using the following query, post-reset: `GET /all?include=delivery`.

Once you choose whether to include delivery, avoid changing the URL used to poll the service for production use. There is also a new delivery-specific endpoint: `GET /delivery`.

Description

The Email Delivery data feed returns metadata that describes both inbound and outbound email delivery to provide visibility into email tracing, TLS compliance, and routing. The delivery data includes information about:

- sender and recipient delivery status and attempts
- Connection host name, banner, IP addresses and responses
- TLS information
- DKIM signature
- Cross-reference to other records for the same email: `xMsgRef`

The delivery feed contains one record per attempt, for both inbound and outbound deliveries. The feed stores 7 days' worth of delivery records. Notification emails are not supported.

Parameters

Type	Name	Description	Schema
Header	Cookie Optional	The first request a client must make is a reset request to obtain the initial cookie. Failure to do the initial reset request will cause a 416 status code to be returned. The reset request itself returns a 200 status code, but no data items. For subsequent requests, the client must accept and pass back persistent cookies to the service so that their place in the feed updates properly.	string
Query	Reset Optional	A string representing the date from which to start reading metadata with the format `YYYY-MM-ddThh:mm:ssZ`. When calling the service for the first time, if you don't provide the reset option a 416 status code will be returned. The reset request itself returns a 200 status code, but no data items. Requests following the initial reset request will return the latest data. For example, using the URI `https://datafeeds.emailsecurity.symantec.com/ all?reset=2016-09-01T00:00:00Z` would reset the cursor for the `all` feed to midnight on the first of September 2016 (UTC) and start returning data from that point onward.	string

Responses

HTTP Code	Description	Schema
200	OK	string
204	No Content - successful request, but no new content is available	No Content
206	Partial Content - successful request but due to size restrictions only a portion of the data was returned. Query again for subsequent data	string
401	Bad Request - unauthorized, or mismatch between credentials and authorization cookie	No Content
416	Invalid or missing cursor - a reset of the cursor is required	No Content
429	Rate Limiting in effect - you are sending too many requests. Please reduce query rate and try again later	No Content
503	Service Unavailable - try again later	No Content

Security

Type	Name
basic	BasicAuth

Produces

`application/json`

Security

BasicAuth

Basic authentication is used to allow access to the feed.

Type: basic

Overall feed security

Using Basic Authentication over SSL is generally accepted within the industry as secure. In addition to Basic Authentication over SSL, Symantec Email Security.cloud restricts users to particular customers, domains, and services. This security model is the same as the model that is deployed for the ClientNet application.

The client application passes a valid ClientNet logon and password to gain access to the HTTPS URIs. The logon credentials are authenticated against the ClientNet database through the ClientNet Web services client application. The API provides a unique `userid` and `customerid` which are authenticated against the **View Statistics** role in ClientNet. Only valid users who have the 'View Statistics' role on the associated service for the given `customerid` can receive data.

Metadata items in the feeds

All email data feed elements

The following metadata items are available in the `all` Email Security.cloud Email Threat Detection and Response data feed. The `all` feed contains a superset of the metadata items contained in all of the other feeds. If you have purchased the Email Threat Isolation service, the Click-time URL Protection feature, and the Email Threat Analytics service, then your `all` feed will also contain metadata from URL/Attachment Isolation, Click-time URL Protection, and Email Threat Analytics events if you add **View Statistics** permissions for Email Threat Isolation, Click-time URL Protection, and Email Threat Analytics to the ClientNet account used to access the `all` feed. The `all` feed also contains metadata from events logged by the Anti-Spam service, as well as metadata about URLs contained in clean inbound email and attachments. See Feed for email data for more information about clean URL metadata.

See Email Threat Isolation data feed elements for descriptions of URL/Attachment Isolation data feed elements. See URL Protection data feed elements for descriptions of Click-time URL Protection data feed elements. See Email Threat Analytics (ec_reports) data feed elements for descriptions of Email Threat Analytics data elements. See Anti-spam data feed elements for descriptions of the Anti-Spam data elements. See Email delivery data feed elements for descriptions of metadata that describes both inbound and outbound email delivery to provide visibility into email tracing, TLS compliance, and routing.

Metadata element	Element type
Message ID	Clean email
Message direction (inbound or outbound)	Clean email
Message ref	Clean email
Message size	Clean email
Subject	Clean email
Envelope from	Clean email
Header from	Clean email
Raw header from	Clean email
Reply to	Clean email
Envelope to	Clean email
Header to	Clean email
Sending server IP address	Clean email
Sending server HELO	Clean email
Attachment file name	Clean email
Attachment file size	Clean email
Attachment MD5	Clean email
Attachment SH2	Clean email
Attachment file type	Clean email
Scan time	Clean email

Metadata element	Element type
TLS information (if applicable) • tlsAdvertised • tlsUsed • tlsPolicy • tlsProtocol • tlsCipher • tlsKeyLength • tlsFallbackReason • tlsForwardSecrecy • tlsNegotiationFailed	Information on TLS connection used for communication.
newDomainAge • domain (string) • ageInDays (int) • foundIn (enum): where the new domain is mentioned. Possible values: – ENV – HEADER (domain found in "From" or "Reply-To") – BODY – HELO	Information about sender domain age.
Security service	Malware. Type: string. Value = "Anti-Malware"
Detection method	Malware. Type: string. Values: "Skeptic Signatures", "Signatures", "Skeptic Heuristics", "Cynic".
Verdict	Malware
Scan action	Malware. Type: string. For the Anti-Malware security service, the action is set to "Block" if malware is detected. In the case of a delivered DMAS incident the action is set to "Delivered."
Severity	Malware. Possible values: UNSET_SEVERITY, LOW, MEDIUM, HIGH, CRITICAL. For all incident types except the following, severity is set to LOW. When detection method is "Cynic", severity is set to HIGH if email was not delivered to the customer, and CRITICAL if some of the customer's recipients received the email. UNSET_SEVERITY indicates a bug in program logic.
Pen name	Malware (Useful for malware only, but provided with each email.)
DMAS delivered	Malware
DMAS JSON data	Malware
Malware container size*	Malware
Malware container name*	Malware
Malware container type*	Malware
Malware container MD5*	Malware
Malware container SHA2*	Malware
Malware item name*	Malware
Malware item category*	Malware
Malware item file name*	Malware
Malware item file size*	Malware
Malware item MD5*	Malware
Malware item SHA2*	Malware

Metadata element	Element type
Malware item URL*	Malware
Link following destination URL*	Malware
Link following redirect type*	Malware
Link following malware name*	Malware
Link following malware category*	Malware
Link following file name*	Malware
Link following file size*	Malware
Link following MD5*	Malware
Link following SHA2*	Malware
action	Threat Isolation (URL)/Isolate, Block, Allow, and Pass
action_reason	Threat Isolation (URL)/Examples: Sub Resource, Policy Rule
content_type	Threat Isolation (URL)/Example: image/png
destination_ip	Threat Isolation (URL)/Example: 123.0.12.34
details	Threat Isolation (URL)/Examples: Download blocked; File infected with virus: BIGG.Bad.XP (Engine: CheckPoint SandBlast Zero-Day Protection)
event	Threat Isolation (URL)/Examples: File View, File Download
file_path	Threat Isolation (URL and Attachment)/If this is a document-isolation-related event, contains the file name. For URL events, this is empty.
file_type	Threat Isolation (URL)/Example: .msi
geoip_country_name	Threat Isolation (URL)
host	Threat Isolation (URL)
mime_type	Threat Isolation (URL)
password_supplied	Threat Isolation (URL)
referer_url	Threat Isolation (URL)/Example: https://www.smith.edu/files/Thesis-and-Dissertation-Template.doc
request_method	Threat Isolation (URL)/Example: GET
resource_request_headers	Threat Isolation (URL)/Type: map<string,string>
resource_response_headers	Threat Isolation (URL)/Type: map<string,string>
resource_type	Threat Isolation (URL)/Examples: content_type, mime_type, resource_type
response_status_code	Threat Isolation (URL)/Examples: 200, 404
rule_id	Threat Isolation (URL)/Type: long
rule_name	Threat Isolation (URL)/Example: Allowed Social Networks
service	Threat Isolation (URL)/Examples: Threat Isolation Engine, Proxy
sha256	Threat Isolation (URL and Attachment)/If this is a document-isolation event, contains the file hash. For URL events, this is empty.
source_ip	Threat Isolation (URL)/Example: 123.456.78.910
tenant_id	Threat Isolation (URL)
text	Threat Isolation (URL)
timestamp	Threat Isolation (URL)/Example: 2016-02-28T16:12:01.437Z
top_level_url	Threat Isolation (URL)
total_bytes	Threat Isolation (URL)/Type: long

Metadata element	Element type
total_bytes_sent	Threat Isolation (URL)/Type: long
url	Threat Isolation (URL)/Example: https://www.jones.edu/files/Thesis-and-Dissertation-Template.doc
url_categories	Threat Isolation (URL)/Type: array<string>
url_parent_categories	Threat Isolation (URL)/Type: array<string>
url_risk	Threat Isolation (URL)/Type: int
user_agent	Threat Isolation (URL)/Examples: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
xmsgref	Threat Isolation (URL) This is provided via the API as a dedicated field, in the "long" format, e.g.: server-4.tower-72.messagelabs.com!1507663721!7116!1 On the NDF side, this is converted to the short format before being given to the customer, e.g. 150766372100000000071160001072004.
Allowed/Blocked/Warned	Click-time URL Protection/A click is either allowed, blocked, or warned (with the option to continue to the URL).
DateURLAccess	Click-time URL Protection/Timestamp of Click-time Protection click.
risk	Click-time URL Protection/Risk score assessed for this URL.
urlCategories	Click-time URL Protection/Categories determined for this URL.
URLOriginal	Click-time URL Protection/The URL as it appeared before rewriting.
MalwareType	Click-time URL Protection/Malware name returned by Link Following.
SQURLClickerIP	Click-time URL Protection/Remote IPv4 address (likely to be a customer gateway) for the click request.
SQURLRecipient	Click-time URL Protection/Email **to** address.
xMsgRef	Click-time URL Protection/Email xMsgRef header added by mail server. The xMsgRef is the key linking all records relating to a particular email. Information about the original email (e.g. the subject) can be located by finding records with the same xMsgRef on your SIEM.

Incident information (if applicable):
• severity
• securityService
• detectionMethod
• verdict
• action
• reason
• filesAndLinks
  • urlRiskScore
  • urlCategories
• scanTimeMs
• dmasInfo
• dmasDelivered
	Click-time URL Protection/Note that these fields are only populated when applicable. If a click is Allowed, then there is no incident, and this information does not appear in your feed for that click.

Action	Anti-Spam/Examples: Block and Delete, Append header and redirect Bulk mail, Append header and allow through, Tag subject, Quarantine Email.
Detection Method	Anti-Spam/Examples: Blocked recipient list, Blocked senders list, Brightmail, DMARC, Dynamic IP block list, Skeptic-AS, SPF.
Reason	Anti-Spam/Example: additional information found in diagnostics field in spam logs.
Scan Time	Anti-Spam/Time stamp on scan.

Metadata element	Element type
Security Service	Anti-Spam/Example: Anti-Spam.
Unique message identifier	Anti-Spam/Unique ID of email scanned.
Verdict	Anti-Spam/Examples: Filtered by Brightmail, Filtered by Cynic, Filtered by DMARC, Filtered by Signaturing System, IP in blacklist, Newsletter, Recipient in blacklist, Sender has failed SPF validation, Sender in blackhole Alias, Sender in blackhole DUL, Sender in blackhole ORBS, Sender in blackhole RBL, Sender in blackhole RSS, Sender in blacklist, Spam detected heuristically.
All report fields and elements	Email Threat Analytics/ Email Threat Analytics (ec_reports) data feed elements

* Not an explicit field. Displayed under `filesandlinks` within an `incident`.

Malware data feed elements

The following metadata items are available in the `malware` data feed. The `malware` feed contains metadata for email detected as malware.

NOTE

Users of the Email Security.cloud Email Threat Detection and Response data feed that was available prior to the release of this one should note that there were two items present in the earlier feed that are not included in this one. These items are **Release Status** and **Country**.

Metadata element	Element type
Security service	Malware. Type: string. Value = "Anti-Malware"
Detection method	Malware. Type: string. Values: "Skeptic Signatures", "Signatures", "Skeptic Heuristics", "Cynic".
Verdict	Malware.
Scan action	Malware. Type: string. For the Anti-Malware security service, the action is set to "Block" if malware is detected. In the case of a delivered DMAS incident the action is set to "Delivered."
Severity	Malware. Possible values: UNSET_SEVERITY, LOW, MEDIUM, HIGH, CRITICAL. For all incident types except the following, severity is set to LOW. When detection method is "Cynic", severity is set to HIGH if email was not delivered to the customer, and CRITICAL if some of the customer's recipients received the email. UNSET_SEVERITY indicates a bug in program logic.
Pen name	Malware (Useful for malware only, but provided with each email.)
DMAS delivered	Malware
DMAS JSON data	Malware
Malware container size*	Malware
Malware container name*	Malware
Malware container type*	Malware
Malware container MD5*	Malware
Malware container SHA2*	Malware
Malware item name*	Malware
Malware item category*	Malware
Malware item file name*	Malware
Malware item file size*	Malware

Metadata element	Element type
Malware item MD5*	Malware
Malware item SHA2*	Malware
Malware item URL*	Malware
Link following destination URL*	Malware
Link following redirect type*	Malware
Link following malware name*	Malware
Link following malware category*	Malware
Link following file name*	Malware
Link following file size*	Malware
Link following MD5*	Malware
Link following SHA2*	Malware

* Not an explicit field. Displayed under `filesandlinks` within an `incident`.

Threat isolation data feed elements

The following metadata items are available in the Threat `isolation` data feed, which includes both URL and attachment isolation events. The Threat Isolation feature ensures URLs and attachments are executed in an isolation platform, which isolates malicious content and prevents it from being delivered to your network or end users' devices. Events are logged when URLs or attachments are isolated. The Threat `isolation` feed contains metadata from these logged events. You must purchase the Email Threat Isolation service to receive Threat Isolation data.

NOTE

Customers who have purchased both the Email Threat Isolation service and the Email Threat Detection and Response service can choose to receive Threat Isolation events data either as part of their `all` feed, or in a separate `isolation` feed that contains Threat Isolation data only. If you have purchased both services, you control whether Threat Isolation data can be accessed through your `all` feed or provided in a separate `isolation` feed through the permissions you assign to the ClientNet accounts that you set up to access feed data. If you create an account that contains **View Statistics** permissions for both Email Threat Detection and Response and Email Threat Isolation and use that account to access the `all` feed, then the `isolation` data is accessible through that feed.

Metadata element	Element type/Examples (if any), or Type
action	Threat Isolation (URL)/Isolate, Block, Allow, and Pass
action_reason	Threat Isolation (URL)/Examples: Sub Resource, Policy Rule
content_type	Threat Isolation (URL)/Example: image/png
destination_ip	Threat Isolation (URL)/Example: 123.0.12.34
details	Threat Isolation (URL)/Examples: Download blocked; File infected with virus: BIGG.Bad.XP (Engine: CheckPoint SandBlast Zero-Day Protection)
event	Threat Isolation (URL)/Examples: File View, File Download
file_path	Threat Isolation (URL and Attachment)/If this is a document-isolation-related event, contains the file name. For URL events, this is empty.
file_type	Threat Isolation (URL)/Example: .msi
geoip_country_name	Threat Isolation (URL)
host	Threat Isolation (URL)

Metadata element	Element type/Examples (if any), or Type
mime_type	Threat Isolation (URL)
password_supplied	Threat Isolation (URL)
referer_url	Threat Isolation (URL)/Example: https://www.smith.edu/files/Thesis-and-Dissertation-Template.doc
request_method	Threat Isolation (URL)/Example: GET
resource_request_headers	Threat Isolation (URL)/Type: map<string,string>
resource_response_headers	Threat Isolation (URL)/Type: map<string,string>
resource_type	Threat Isolation (URL)/Examples: content_type, mime_type, resource_type
response_status_code	Threat Isolation (URL)/Examples: 200, 404
rule_id	Threat Isolation (URL)/Type: long
rule_name	Threat Isolation (URL)/Example: Allowed Social Networks
service	Threat Isolation (URL)/Examples: Threat Isolation Engine, Proxy
sha256	Threat Isolation (URL and Attachment)/If this is a document-isolation event, contains the file hash. For URL events, this is empty.
source_ip	Threat Isolation (URL)/Example: 123.456.78.910
tenant_id	Threat Isolation (URL)
text	Threat Isolation (URL)
timestamp	Threat Isolation (URL)/Example: 2016-02-28T16:12:01.437Z
top_level_url	Threat Isolation (URL)
total_bytes	Threat Isolation (URL)/Type: long
total_bytes_sent	Threat Isolation (URL)/Type: long
url	Threat Isolation (URL)/Example: https://www.jones.edu/files/Thesis-and-Dissertation-Template.doc
url_categories	Threat Isolation (URL)/Type: array<string>
url_parent_categories	Threat Isolation (URL)/Type: array<string>
url_risk	Threat Isolation (URL)/Type: int
user_agent	Threat Isolation (URL)/Examples: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
xmsgref	Threat Isolation (URL) This is provided via the API as a dedicated field, in the "long" format, e.g.: server-4.tower-72.messagelabs.com!1507663721!7116!1 On the NDF side, this is converted to the short format before being given to the customer, e.g. 150766372100000000071160001072004.

Clicktime URL Protection data feed elements

The following metadata items are available in the `clicktime` URL Protection data feed. The Click-time URL Protection feature rewrites and performs checks on URLs in the emails that are delivered to your organization's users. The `clicktime` URL Protection feed provides metadata from events generated by end-user clicks on these rewritten URLs. You must purchase the Click-time URL Protection service to receive Click-time URL Protection data.

NOTE

Customers who have purchased both the Click-time URL Protection service and the Email Threat Detection and Response service can choose to receive Click-time URL Protection events data either as part of their `all` feed, or in a separate `clicktime` feed that contains Click-time URL Protection data only. If you have purchased

both services, you control whether Click-time URL Protection data is accessible through your `all` feed or only through the separate `clicktime` feed through the permissions you assign to the ClientNet accounts that you set up to access feed data. If you create an account that contains **View Statistics** permissions for both Email Threat Detection and Response and Click-time URL Protection and use it to access your `all` feed, then the `clicktime` data is accessible through that feed. Please note that feed data is not filtered based on permissions. If you have the correct permissions, then you receive data through the feed. If you do not have the correct permissions, then you do not receive any data.

Metadata element	Element type/Examples (if any), or Type
Allowed/Blocked/Warned	Click-time URL Protection/A click is either allowed, blocked, or warned (with the option to continue to the URL). Note that if a click is Allowed, then you will not receive incident information for that click, because there is no incident.
DateURLAccess	Click-time URL Protection/Timestamp of Click-time Protection click.
risk	Click-time URL Protection/Risk score assessed for this URL.
urlCategories	Click-time URL Protection/Categories determined for this URL.
URLOriginal	Click-time URL Protection/The URL as it appeared before rewriting.
MalwareType	Click-time URL Protection/Malware name returned by Link Following.
SQURLClickerIP	Click-time URL Protection/Remote IPv4 address (likely to be a customer gateway) for the click request.
SQURLRecipient	Click-time URL Protection/Email **to** address.
xMsgRef	Click-time URL Protection/Email xMsgRef header added by mail server. The xMsgRef is the key linking all records relating to a particular email. Information about the original email (e.g. the subject) can be located by finding records with the same xMsgRef on your SIEM.
Incident information (if applicable): • severity • securityService • detectionMethod • verdict • action • reason • filesAndLinks • scanTimeMs • dmasInfo • dmasDelivered	Click-time URL Protection/Note that these fields are only populated when applicable. If a click is Allowed, then these incident descripions do not appear in your feed for that click.

Anti-spam data feed elements

The following metadata items are available in the Anti-`spam` data feed. The Anti-Spam service detects unwanted email and newsletters, and processes them according to the policies that you set up. It also helps authenticate senders using SPF, DKIM and DMARC.

Metadata element	Element type/Examples (if any), or Type
Action	Anti-Spam/Examples: Block and Delete, Append header and redirect Bulk mail, Append header and allow through, Tag subject, Quarantine Email.
Detection Method	Anti-Spam/Examples: Blocked recipient list, Blocked senders list, Brightmail, DMARC, Dynamic IP block list, Skeptic-AS, SPF.
Reason	Anti-Spam/Example: additional information found in diagnostics field in spam logs.

Metadata element	Element type/Examples (if any), or Type
Scan Time	Anti-Spam/Time stamp for scan.
Security Service	Anti-Spam/Example: Anti-Spam.
Unique message identifier	Anti-Spam/Unique ID of email scanned.
Verdict	Anti-Spam/Examples: Filtered by Brightmail, Filtered by Cynic, Filtered by DMARC, Filtered by Signaturing System, IP in blocklist, Newsletter, Recipient in blocklist, Sender has failed SPF validation, Sender in blackhole Alias, Sender in blackhole DUL, Sender in blackhole ORBS, Sender in blackhole RBL, Sender in blackhole RSS, Sender in blocklist, Spam detected heuristically.

Email Threat Analytics (ec_reports) data feed elements

The following metadata items are available in the Email Threat Analytics (ETA) data feed. Instead of a large self-contained report, ETA reports are split by attack campaigns. Therefore, a customer can receive as many reports as there are attacks campaigns (but a report can contain more than one attack). Explanations of fields are below.

Table 2: Report

Metadata element	Element type	Comment
Attacks	Collection of "Attack"	Contains relevant information about an email attack.
reportWindowStartTime	Unix epoch	Start of the time window over which report has been generated.
reportWindowEndTime	Unix epoch	End of the time window over which report has been generated.
topAttacked	Collection of “Recipient”	Top 20 email accounts in your organization who were intended recipients of malicious emails during the report period.

Table 3: Recipient

Metadata element	Element type	Comment
Key	String	Identifier (email address or recipient domain) that has at least one email blocked by Symantec.
Value	Numeric	Number of emails blocked for that identifier.
Type	String	Number of emails blocked for that identifier.

Table 4: Timeline

Metadata element	Element type	Comment
Key	String	Date when emails were blocked, encoded as a string.
Value	Numeric	Number of blocked emails on a particular date.
Type	String	Set to "count" by default.

Table 5: IpSource

Metadata element	Element type	Comment
Key	String	Sending IP address.
Value	Numeric	Percentage of blocked emails of this attack from this IP address.
Type	String	Set to "percentage" by default.

Table 6: GeoIpSource

Metadata element	Element type	Comment
Key	String	Two-letter (ISO 3166) country of origin code based on sender IP address.
Value	Numeric	Percentage of emails sent from country based on originating IP for this attack.
Type	String	Set to "percentage" by default.

Table 7: ThreatName

Metadata element	Element type	Comment
Key	String	Detection name.
Value	Numeric	Percentage of blocked emails for this attack which had this detection name.
Type	String	Set to "percentage" by default.

Table 8: Trait

Metadata element	Element type	Comment
IOC	String	Indicator-of-Compromise name. Currently supported IOCs: • Sender • SHA2 • URL • Subject
Value	String	IOC value.
Weight	Numeric	Percentage of malicious email messages which contained this particular IOC.
Type	String	Set to "percentage" by default.

Table 9: Attack

Metadata element	Element type	Comment
attackedOrgsGlobal	Numeric	Number of Symantec Email.cloud customers affected by this attack.
attackedMailboxesGlobal	Numeric	Number of mailboxes associated with this threat campaign (based on all Symantec Email.Cloud customers).
attackVolumeGlobal	Numeric	Total number of emails blocked as part of this attack (An email can be sent to many mailboxes therefore number of mailboxes can differ from number of emails).
avgMailboxesGlobal	Numeric	Average number of mailboxes potentially associated with this threat campaign for all Symantec Email Security.cloud customers.
attackedMailboxesLocal	Numeric	Number of mailboxes associated with this threat campaign in your organization.
attackVolumeLocal	Numeric	Number of blocked email messages for this threat campaign in your organization.
globalTimeline	Collection of "Timeline"	Histogram of blocked emails for this attack and for all the customers.
localTimeline	Collection of "Timeline"	Histogram of blocked emails for this attack and your enterprise.
cluster	String	Cluster ID. While some attacks may retain the same cluster id in consecutive reports this generally won't be the case.
attackType	String	Three possible email threat campaign profiles: • Mass: Widespread • Focused: less than 20 related emails or seen in less than 20 customers • Highly-focused: less than 5 related emails or seen in less than 5 customers How an email is characterized as one of these profiles depends on malicious email volume as well as the volume of affected enterprises.
attackDescription	String	Textual description of the attack type.
ipSources	Collection of "ipSource"	Top 20 most common sending IPs for this campaign.
geoIpSources	Collection of "geoIpSource"	Top 20 most common originating countries (based on gelocation of the sender IP address) for this campaign.
threatNames	Collection of "threatName"	Top 20 most common threat names for this campaign, based on Symantec Threat names.
affectedUsers	Collection of "Recipient"	Histogram of email accounts targeted by this campaign, including email volume per user for your organization.
affectedUsersByDomain	Collection of "Recipient"	Histogram of company email domains targeted by this campaign, including malicious email volume per domain for your organization.
traitImportance	Collection of "Trait"	Contains top 20 IOCs for a particular threat campaign.

Metadata element	Element type	Comment
msgrefs	Collection of Strings	List of xMsgRef for your organization that can be used to correlate report findings against NDF data. NOTE: this field will be truncated to top 1,000 xMsgRef for Mass attacks.

Email Delivery data feed elements

The Email Delivery data feed returns metadata that describes both inbound and outbound email delivery to provide visibility into email tracing, TLS compliance, and routing. The following metadata items are available in the feed.

Metadata element	Element type	Comment
IsOutbound	Boolean	Indicates whether the email is inbound or outbound.
senderDomain	String	Domain from which the email was sent.
senderName	String	Name of the email sender.
rcptDomain	String	Domain to which the email was sent.
rcptName	String	Name of the email recipient(s).
deliveryStatus	DeliveryStatusType	Possible values: Delivered, Permfail, Tempfail.
attempt	Int	Indicates the count of the attempts made to deliver the email. For example, if the value in this field is 3, then this record's data describes the third attempt to deliver the message.
timeStampZms	Long	The UTC time (in milliseconds) at which the email was delivered or received.
connectionIP	String	IP address of the connection used to send or receive the email.
connectionHostName	String	Host name of the email's sender/receiver.
banner	String	The SMTP banner is the initial SMTP connection response that a messaging server receives after it connects to a Microsoft Exchange server. This string contains the text in the banner of the email that was sent/received.
smtpResponseCode		The response code generated by SMTP (RFC 5321). The first digit of the status code specifies one of five standard classes of responses: 1xx (Informational); 2xx (Successful); 3xx (Redirection); 4xx (Client Error) or 5xx (Server Error).
smtpResponseMessage	String	The response message generated by SMTP (RFC 5321).
tlsAdvertised	Boolean	Indicates whether the Transport Layer Security (TLS) protocol (RFC 8446) is "advertised" as being in use by the sender/recipient of the email.
tlsUsed	Boolean	Indicates whether the Transport Layer Security (TLS) protocol (RFC 8446) is actually used by the sender/recipient of the email.
tlsPolicy	TLSPolicyType	Possible values: Enforced, Opportunistic, None.
tlsProtocol	String	Indicates the version of the TLS protocol.
tlsCipher	String	Indicates the name of the cipher suite.

Metadata element	Element type	Comment
tlsKeyLength	Int	The length (in bits) of the TLS encryption key used to send or receive the email. The list of enabled cipher suites determine the algorithms and key length to use. The client and server negotiate a cipher suite that both have enabled. The server chooses among shared candidates.
tlsFallbackReason	String	This field is not currently populated. It is reserved for future use.
tlsForwardSecrecy	Boolean	This field set to true if the cipher used supports Perfect Forward Secrecy for the TLS session with the remote MTA.
tlsNegotiationFailed	Boolean	This field set to true if the server could not negotiate a TLS connection with the remote MTA.
dkimSignature	String	Domain Keys Identified Mail (DKIM, defined in RFC 6376) is an email authentication method designed to detect forged sender addresses in emails. DKIM allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It achieves this by affixing a signature, linked to a domain name, to each outgoing email message. The recipient system can verify this by looking up the sender's public key published in the DNS. This string contains the DKIM signature used by the sending/receiving system.

Example data

Sample JSON files produced by data feeds

The examples in this section are provided to help you understand the structure and contents of the data available through the Email Security.cloud Data Feeds API. These JSON files have been edited to remove any identifying or confidential information, and linebreaks have been added as necessary to improve readability on the page.

Sample1.json


```
[
  {
    "emailInfo": {
      "xMsgRef": "000012345600000000012340001012345",
      "longMsgRef": "server-1.tower-2.companyname.com!1500589137!6648!1",
      "messageId": "20081201213501.GA2205@virus.reg.test",
      "isOutbound": false,
      "messageSize": 602,
      "mailProcessingStartTime": 1500589138,
      "subject": "Latest SKEPTIC XML FILES",
      "envFrom": "envfrom@somedomain.test",
      "headerFrom": "senderUsr1@somedomain.test",
      "rawHeaderFrom": "",
      "headerReplyTo": "",
      "envTo": [
        "user@tnt1.test"
      ],
      "headerTo": [
        "recepientUsr1@tnt1.test"
      ],
      "senderIp": "10.01.0.10",
      "country": "",
      "HELOString": "test-host.stream72",
      "avQuarantinePenId": "12341_1234567890",
      "filesAndLinks": [
        {
          "nodeType": "FILE_INCLUDED",
          "fileNameOrURL": "SMTP Envelope (1)",
          "fileSize": 31,
          "fileType": "Email/HeaderPart",
          "md5": "b890eb3d872b3176009fee9bbb8799d3",
          "sha256": "33c923e316ed71599b42546e5c1b9fe3ad255ace876844c4ea14a6fe81525d3e",
          "urlCategories": null,
          "urlRiskScore": null,
          "index": 2,
          "parentIndex": 1,
          "linkSource": "BASIC_EMAIL_INFO"
        },
        {
          "nodeType": "FILE_INCLUDED",
```

```
        "fileNameOrURL": "SMTP Envelope (0)",
        "fileSize": 571,
        "fileType": "Email/Header",
        "md5": "f217a11b069a94e1ecfa0e246ad053fb",
        "sha256": "55a17ddcde3e07b21e2ef03695c5ee3f24108ba5b16326eaaf9b0ac08a12d670",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 1,
        "parentIndex": 0,
        "linkSource": "BASIC_EMAIL_INFO"
      }
    ],
    "tlsInfo": null
  },
  "incidents": [
    {
      "xMsgRef": "000012345600000000012340001012345",
      "addressContexts": [
        {
          "name": "user",
          "domain": "tnt1.test",
          "isSender": false
        }
      ],
      "severity": "LOW",
      "securityService": "Anti-Malware",
      "detectionMethod": "Signatures",
      "verdict": "Malware",
      "action": "Block",
      "reason": "unknown",
      "filesAndLinks": [
        {
          "nodeType": "FILE_INCLUDED",
          "fileNameOrURL": "",
          "fileSize": 0,
          "fileType": "",
          "md5": null,
          "sha256": null,
          "malwareName": "Trojan.pidief",
          "malwareCategory": "Virus",
          "urlCategories": null,
          "urlRiskScore": null,
          "index": 3,
          "parentIndex": 0,
          "xMsgRef": "000012345600000000012340001012345",
          "linkSource": "INCIDENT"
        }
      ],
      "dmasInfo": [],
      "dmasDelivered": false
    }
  ]
}
```

```
]
```


Sample2.json


```
[
  {
    "emailInfo": {
      "xMsgRef": "11001234550000000001234001012001",
      "longMsgRef": "server-1.tower-1.myfirm.com!1200123455!1234!1",
      "messageId": "20081201213501.AB1235@virus.reg.test",
      "isOutbound": false,
      "messageSize": 602,
      "mailProcessingStartTime": 1500589304,
      "subject": "Latest SKEPTIC XML FILES",
      "envFrom": "envfrom@somedomain.test",
      "headerFrom": "senderUsr1@somedomain.test",
      "rawHeaderFrom": "",
      "headerReplyTo": "",
      "envTo": [
        "user@tnt1.test"
      ],
      "headerTo": [
        "recepientUsr1@tnt1.test"
      ],
      "senderIp": "01.10.0.10",
      "country": "",
      "HELOString": "main-host.stream5",
      "avQuarantinePenId": "00001_1234123401",
      "filesAndLinks": [
        {
          "nodeType": "FILE_INCLUDED",
          "fileNameOrURL": "SMTP Envelope (1)",
          "fileSize": 31,
          "fileType": "Email/HeaderPart",
          "md5": "b890eb3d872b3176009fee9bbb8799d3",
          "sha256": "33c923e316ed71599b42546e5c1b9fe3ad255ace876844c4ea14a6fe81525d3e",
          "urlCategories": null,
          "urlRiskScore": null,
          "index": 2,
          "parentIndex": 1,
          "linkSource": "BASIC_EMAIL_INFO"
        },
        {
          "nodeType": "FILE_INCLUDED",
          "fileNameOrURL": "SMTP Envelope (0)",
          "fileSize": 571,
          "fileType": "Email/Header",
          "md5": "8e57c7e9be4614d135192550353a0b6e",
          "sha256": "ffd4fe709bdf7519711b421d65fc46fbebbfc7c0518a80507bc76a8522de2ef0",
          "urlCategories": null,
          "urlRiskScore": null,
          "index": 1,
          "parentIndex": 0,
```

```
          "linkSource": "BASIC_EMAIL_INFO"
        }
      ],
      "tlsInfo": null
    },
    "incidents": [
      {
        "xMsgRef": "1100123455000000000001234001012001",
        "addressContexts": [
          {
            "name": "user",
            "domain": "tnt1.test",
            "isSender": false
          }
        ],
        "severity": "LOW",
        "securityService": "Anti-Malware",
        "detectionMethod": "Skeptic Signatures",
        "verdict": "Malware",
        "action": "Block",
        "reason": "unknown",
        "filesAndLinks": [
          {
            "nodeType": "FILE_INCLUDED",
            "fileNameOrURL": "TestAttachment.zip",
            "fileSize": 0,
            "fileType": "",
            "md5": "8d2fb355a719aa37b0292df5f7e3f032",
            "sha256": "d424abf92b126223f436e1230b313a450483f65c2bb9835d0744729d91ae7cfc",
            "urlCategories": null,
            "urlRiskScore": null,
            "malwareName": "Trojan.gen",
            "malwareCategory": "Trojan",
            "index": 3,
            "parentIndex": 0,
            "xMsgRef": "1100123455000000000001234001012001",
            "linkSource": "INCIDENT"
          }
        ],
        "dmasInfo": [],
        "dmasDelivered": false
      }
    ]
  }
]
```


Sample3.json


```
[
  {
    "emailInfo": {
      "xMsgRef": "100012345600000000012300001012345",
      "longMsgRef": "server-9.tower-1.somecompany.com!1234512345!1234!1",
```

```
    "messageId": "20081201213501.AB1234@virus.reg.test",
    "isOutbound": false,
    "messageSize": 602,
    "mailProcessingStartTime": 1500589649,
    "subject": "Latest SKEPTIC XML FILES",
    "envFrom": "envfrom@somedomain.test",
    "headerFrom": "senderUsr1@somedomain.test",
    "rawHeaderFrom": "",
    "headerReplyTo": "",
    "envTo": [
      "user@tnt1.test"
    ],
    "headerTo": [
      "recepientUsr1@tnt1.test"
    ],
    "senderIp": "01.10.0.10",
    "country": "",
    "HELOString": "test-host.stream1",
    "avQuarantinePenId": "12345_1234512345",
    "filesAndLinks": [
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "SMTP Envelope (1)",
        "fileSize": 31,
        "fileType": "Email/HeaderPart",
        "md5": "b890eb3d872b3176009fee9bbb8799d3",
        "sha256": "33c923e316ed71599b42546e5c1b9fe3ad255ace876844c4ea14a6fe81525d3e",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 2,
        "parentIndex": 1,
        "linkSource": "BASIC_EMAIL_INFO"
      },
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "SMTP Envelope (0)",
        "fileSize": 571,
        "fileType": "Email/Header",
        "md5": "4096ae86c6092e01f9b63985246bff93",
        "sha256": "8bbc02c16e4aa57248fdff456d001a239ad3140eb7c10a414cae252b9a17d7dd",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 1,
        "parentIndex": 0,
        "linkSource": "BASIC_EMAIL_INFO"
      }
    ],
    "tlsInfo": null
  },
  "incidents": [
    {
      "xMsgRef": "10001234560000000001230000010123 45",
      "addressContexts": [
```

```
          {
            "name": "user",
            "domain": "tnt1.test",
            "isSender": false
          }
        ],
        "severity": "LOW",
        "securityService": "Anti-Malware",
        "detectionMethod": "Skeptic Heuristics",
        "verdict": "Malware",
        "action": "Block",
        "reason": "unknown",
        "filesAndLinks": [
          {
            "nodeType": "FILE_INCLUDED",
            "fileNameOrURL": "Picasa Slideshow.exe",
            "fileSize": 0,
            "fileType": "",
            "md5": "9662e2e429154ab118a3ee034fb4eed4",
            "sha256": "cf9ff75461a2c1e83406d37c983b44ba0dc6cd1ed209998889eaf6ee4f6f8a3b",
            "malwareName": "AVE/W32.Spyrat",
            "malwareCategory": "uncategorized",
            "urlCategories": null,
            "urlRiskScore": null,
            "index": 4,
            "parentIndex": 3,
            "xMsgRef": "10001234560000000001230000101234 5",
            "linkSource": "INCIDENT"
          },
          {
            "nodeType": "FILE_INCLUDED",
            "fileNameOrURL": "Picasa Slideshow.zip",
            "fileSize": 0,
            "fileType": "",
            "md5": "0becaf21ba28f52d9c309c12b9178f9a",
            "sha256": "cd8ff75461a2c1e83406d37c983b44ba0dc6cd1ed209998889eaf6ee4f6f8e4c",
            "malwareName": "unknown",
            "malwareCategory": "uncategorized",
            "urlCategories": null,
            "urlRiskScore": null,
            "index": 3,
            "parentIndex": 0,
            "xMsgRef": "10001234560000000001230000101234 5",
            "linkSource": "INCIDENT"
          }
        ],
        "dmasInfo": [],
        "dmasDelivered": false
      }
    ]
  }
]
```

Sample4.json


```
[
  {
    "emailInfo": {
      "xMsgRef": "12345123450000000000123450010123 45",
      "longMsgRef": "server-4.tower-72.yourfirm.com!1234567890!1234!1",
      "messageId": "20081201213501.AB2205@virus.reg.test",
      "isOutbound": false,
      "messageSize": 602,
      "mailProcessingStartTime": 1497561376,
      "subject": "Latest SKEPTIC XML FILES",
      "envFrom": "envfrom1@pi-dmas-auto001-d001.test",
      "headerFrom": "senderUsr1@somedomain.test",
      "rawHeaderFrom": "",
      "headerReplyTo": "",
      "envTo": [
        "user1@tnt1.test",
        "user2@tnt2.test",
        "user3@tnt1.test",
        "user4@tnt-auto002-d001.test"
      ],
      "headerTo": [
        "recepientUsr1@tnt1.test"
      ],
      "senderIp": "10.01.0.10",
      "country": "",
      "HELOString": "test-host.stream01",
      "avQuarantinePenId": "12345_1234567891",
      "filesAndLinks": [
        {
          "nodeType": "FILE_INCLUDED",
          "fileNameOrURL": "SMTP Envelope (1)",
          "fileSize": 31,
          "fileType": "Email/HeaderPart",
          "md5": "b890eb3d872b3176009fee9bbb8799d3",
          "sha256": "33c923e316ed71599b42546e5c1b9fe3ad255ace876844c4ea14a6fe81525d3e",
          "urlCategories": null,
          "urlRiskScore": null,
          "index": 2,
          "parentIndex": 1,
          "linkSource": "BASIC_EMAIL_INFO"
        },
        {
          "nodeType": "FILE_INCLUDED",
          "fileNameOrURL": "SMTP Envelope (0)",
          "fileSize": 571,
          "fileType": "Email/Header",
          "md5": "9fe733f3b025695e3dab39658e64786d",
          "sha256": "e8f98d7ab6f00111c6cc363b41e7a07e9080ce101d9da3ceba241ce4ff1778e2",
          "urlCategories": null,
          "urlRiskScore": null,
          "index": 1,
```

```
      "parentIndex": 0,
      "linkSource": "BASIC_EMAIL_INFO"
    }
  ],
  "tlsInfo": null
},
"incidents": [
  {
    "xMsgRef": "12345123450000000001234500101234 5",
    "addressContexts": [
      {
        "name": "user1",
        "domain": "tnt1.test",
        "isSender": false
      },
      {
        "name": "user2",
        "domain": "tnt2.test",
        "isSender": false
      },
      {
        "name": "user3",
        "domain": "tnt1.test",
        "isSender": false
      }
    ],
    "severity": "LOW",
    "securityService": "Anti-Malware",
    "detectionMethod": "Skeptic Signatures",
    "verdict": "Malware",
    "action": "Block",
    "reason": "unknown",
    "filesAndLinks": [
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "TestAttachment.zip",
        "fileSize": 0,
        "fileType": "",
        "md5": "8d2fb355a719aa37b0292df5f7e3f032",
        "sha256": "d424abf92b126223f436e1230b313a450483f65c2bb9835d0744729d91ae7cfc",
        "malwareName": "Trojan.gen",
        "malwareCategory": "Trojan",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 3,
        "parentIndex": 0,
        "xMsgRef": "12345123450000000001234500101234 5",
        "linkSource": "INCIDENT"
      }
    ],
    "dmasInfo": [],
    "dmasDelivered": false
  }
```

```
    ]
  }
]
```


Sample5.json: Email with Spam incident


```
{
  "emailInfo": {
    "xMsgRef": "154504479900000063920260001401026",
    "longMsgRef": "server-26.tower-401.messagelabs.com!1545044799!6392026!1",
    "messageId": "ac647535e51d4f6d8658b563c9e9f6b1TONQWOZKDMVXHIZLSIRUWOZLTOR6FG3LUOA======@microsoft.com",
    "isOutbound": false,
    "messageSize": 22799,
    "mailProcessingStartTime": 1545044801,
    "subject": "Weekly digest: Office 365 changes",
    "envFrom": "o365mc@microsoft.com",
    "headerFrom": "o365mc@microsoft.com",
    "rawHeaderFrom": "",
    "headerReplyTo": "",
    "envTo": [
      "anant@spinachworks.com"
    ],
    "headerTo": [
      "anant@spinachworks.com"
    ],
    "senderIp": "65.55.52.237",
    "senderMailserver": "co1gmehub08.msn.com",
    "country": "",
    "HELOString": "smtpi.msn.com",
    "avQuarantinePenId": "56989_1545044801",
    "authResults": null,
    "filesAndLinks": [
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "message.txt",
        "fileSize": 24,
        "fileType": "text/plain",
        "md5": "e7d0bcc0d6c608e7460844c15f491b70",
        "sha256": "bba0f33e5fe05354c81df55a4a14da2fda3fb79efe3d7f5de1de951fc0a8c987",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 3,
        "parentIndex": 2,
        "linkSource": "BASIC_EMAIL_INFO"
      },
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "SMTP Envelope (1)",
        "fileSize": 168,
        "fileType": "Email/HeaderPart",
        "md5": "3a2da5567a58c0c4f5b1abc0ec5517c1",
        "sha256": "796f6df6e9958f729355e2ad2312e490c8a99adc3135fb89407fdb201919f18e",
        "urlCategories": null,
```

```
        "urlRiskScore": null,
        "index": 2,
        "parentIndex": 1,
        "linkSource": "BASIC_EMAIL_INFO"
      },
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "SMTP Envelope (0)",
        "fileSize": 1424,
        "fileType": "Email/Header",
        "md5": "0aee00d2baa53a58aa74e26855e8afbd",
        "sha256": "dbebefb064316bd201e9aaf3187a55f16b61a8deee12279ecd035f1ac8aefde2",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 1,
        "parentIndex": 0,
        "linkSource": "BASIC_EMAIL_INFO"
      }
    ],
    "tlsInfo": null
  },
  "incidents": [
    {
      "xMsgRef": "154504479900000063920260001401026",
      "addressContexts": [
        {
          "name": "anant",
          "domain": "spinachworks.com",
          "isSender": false
        }
      ],
      "severity": "LOW",
      "securityService": "Anti-Spam",
      "detectionMethod": "Skeptic-AS",
      "verdict": "Spam detected heuristically",
      "action": "Tagged",
      "reason": "Yes, hits=0.8 required=7.0 tests=newsletters: ,newsletters: Newsletter detected: 5.12 >
 5,newsletters: Newsletter detected: 5.12 > 5,HTML_MESSAGE,MIME_HTML_MOSTLY,MPART_ALT_DIFF,received_headers:
 No Received headers,Newsletter detected heuristically [ML_RADAR_NL_1,
 ML_RADAR_NL_2,ML_RADAR_NL_2A,ML_RADAR_NL_2CP]:5.12 > 5",
      "filesAndLinks": [],
      "dmasInfo": null,
      "dmasDelivered": null
    }
  ]
}
```


Sample6.json: Threat Isolation (URL)


```
{
    "fireglass_log": {
      "timestamp": "2018-12-07T15:59:13.053Z",
      "event": "Network Request",
```

```
"source_ip": "172.31.42.67",
"url": "http://ncu.rcnpv.com.tw/Uploads/2013123110323273856174 4.pdf",
"referer_url": "",
"request_method": "GET",
"user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4)
 AppleWebKit/605.1.15 (KHTML, like Gecko)
 Version/11.1 Safari/605.1.15",
"destination_ip": "192.185.35.58",
"action": "Isolate",
"action_reason": "Policy Rule",
"text": "",
"rule_id": 6,
"rule_name": "",
"service": "Threat Isolation Engine",
"mime_type": "",
"password_supplied": "",
"file_type": "",
"content_type": "application/pdf",
"host": "email-isolation1-us-west",
"geoip_country_name": "",
"top_level_url": "http://ncu.rcnpv.com.tw/Uploads/
 2013123110323273856174 4.pdf",
"response_status_code": 200,
"resource_request_headers": {
  "User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/65.0.3309.6 Safari/537.36",
  "Referer": "",
  "Accept-Language": "en-us",
  "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,
   image/webp,image/apng,*/*;q=0.8",
  "Upgrade-Insecure-Requests": "1"
},
"resource_response_headers": {
  "Accept-Ranges": "bytes",
  "Server": "nginx/1.14.1",
  "Connection": "keep-alive",
  "Last-Modified": "Thu, 11 Aug 2016 03:27:38 GMT",
  "Content-Length": "39762",
  "Date": "Fri, 07 Dec 2018 15:59:11 GMT",
  "Content-Type": "application/pdf"
},
"resource_type": "Main Frame",
"total_bytes": 0,
"total_bytes_sent": 0,
"md5": "00000000000000000000000000000000",
"file_path": "",
"url_categories": [
  "Uncategorized"
],
"details": "",
"url_parent_categories": [
  "Unknown"
```

```
      ],
      "url_risk": 5,
      "tenant_id": "97438",
      "xMsgRef": "154273665600000039331070001381019"
    }
  }
```


Sample7.json: Clicktime


```
[
 {
   "clicktimeInfo" : {
  "xMsgRef" : "17043880570000000001579000109500 3",
  "squrlClickerIp" : "192.168.1.2",
  "squrlRecipient" : "email@recipient.com;",
  "url" : "https://testrating.webfilter.bluecoat.com/threatrisk/level/5?locale=en_US",
  "dateUrlAccess" : 1704388078800,
  "risk" : 5,
  "urlCategories" : [ "Technology/Internet" ]
   },
   "incident" : {
  "xMsgRef" : "17043880570000000001579000109500 3",
  "addressContexts" : [ {
    "name" : "",
    "domain" : "",
    "isSender" : false
  } ],
  "severity" : "UNSET_SEVERITY",
  "securityService" : "Clicktime",
  "detectionMethod" : "Isolation",
  "verdict" : "isolate",
  "action" : "ISOLATE",
  "reason" : "{\"policyname\":\"If URL Risk Score > 3 Then Pass to Isolation\",\"risk\":5}",
  "filesAndLinks" : [ {
    "nodeType" : "LINK_INCLUDED",
    "fileNameOrURL" : "https://testrating.webfilter.bluecoat.com/threatrisk/level/5?locale=en_US",
    "fileSize" : 0,
    "fileType" : "",
    "md5" : null,
    "sha256" : null,
    "malwareName" : null,
    "malwareCategory" : null,
    "urlCategories" : [ "Technology/Internet" ],
    "urlRiskScore" : 5,
    "index" : 0,
    "parentIndex" : 0,
    "xMsgRef" : "17043880570000000001579000109500 3",
    "linkSource" : "INCIDENT"
  } ],
  "dmasInfo" : null,
  "dmasDelivered" : null
   }
```

```
  }
]
```


Sample8.json: Email Threat Analytics


```
{
 "attacks": [{
  "attackedOrgsGlobal": 1,
  "attackedMailboxesLocal": 1,
  "ipSources": [{
    "key": "192.168.1.7",
    "value": 100,
    "type": "percentage"
   }
  ],
  "attackedMailboxesGlobal": 1,
  "globalTimeline": [{
    "key": "2019-07-28",
    "value": 1,
    "type": "count"
   }
  ],
  "avgMailboxesGlobal": 1.0,
  "attackVolumeLocal": 1,
  "threatNames": [{
    "key": "Exploit/Phishing.bb",
    "value": 100,
    "type": "percentage"
   }
  ],
  "attackType": "Highly-focused",
  "geoIpSources": [{
    "key": "US",
    "value": 100,
    "type": "percentage"
   }
  ],
  "attackVolumeGlobal": 1,
  "localTimeline": [{
    "key": "2019-07-28",
    "value": 1,
    "type": "count"
   }
  ],
  "affectedUsers": [{
    "key": "test@customer.domain",
    "value": 1,
    "type": "count"
   }
  ],
  "affectedUsersByDomain": [{
    "key": "customer.domain",
    "value": 1,
```

```
    "type": "count"
   }
  ],
  "traitImportance": [{
    "IOC": "sender",
    "value": "phish@malware.com",
    "weight": 33,
    "type": "percentage"
   }, {
    "IOC": "SHA2",
    "value": "c7ab407c84b2f405153799fd593d123a53bb0178f45f3989d77ada7b94f41071",
    "weight": 33,
    "type": "percentage"
   }, {
    "IOC": "subject",
    "value": "[Request received] Online Authentication Process",
    "weight": 33,
    "type": "percentage"
   }
  ],
  "msgRefs": ["111111111100000001111100001111021"],
  "internalCustomerId": "1111111111",
  "attackDescription": "Attack seen in less than 5 emails or customers",
  "cluster": "341277"
  }
 ],
 "reportWindowStartTime": 1563004843,
 "reportWindowEndTime": 1565596221,
 "topAttacked": [{
  "key": "dummy@customer.domain",
  "value": 16106,
  "type": "count"
  }, {
  "key": "another@customer.domain",
  "value": 7935,
  "type": "count"
  }, {
  "key": "test@customer.domain",
  "value": 550,
  "type": "count"
  }
 ],
 "internalCustomerId": "1111111111"
}
```


Sample9.json: Clean URLs

In the following sample code, the clean URL names are shown in **bold**.


```
{
  "emailInfo": {
    "xMsgRef": "156218225900000000001040001056002",
    "longMsgRef": "server-2.tower-56.messagelabs.com!1562182259!104!1",
```

```
    "messageId": "",
    "isOutbound": true,
    "messageSize": 8529,
    "mailProcessingStartTime": 1562182261,
    "subject": "SSFeedBuilderCleanEmailURLE2E-0009",
    "envFrom": "envfrom1@pi-dmas-auto001-d001.test",
    "headerFrom": "envfrom1@pi-dmas-auto001-d001.test",
    "rawHeaderFrom": "",
    "headerReplyTo": "",
    "envTo": [
      "user5@nosuchdomain1.test",
      "user1@tnt1.test",
      "user2@tnt2.test",
      "user3@tnt1.test",
      "user6@nosuchdomain2.test",
      "user4@tnt-auto002-d001.test"
    ],
    "headerTo": [
      "user5@nosuchdomain1.test",
      "user1@tnt1.test",
      "user2@tnt2.test",
      "user3@tnt1.test",
      "user6@nosuchdomain2.test",
      "user4@tnt-auto002-d001.test"
    ],
    "senderIp": "25.16.1.69",
    "senderMailserver": "unknown",
    "country": "",
    "HELOString": "robot-host.stream16",
    "avQuarantinePenId": "10023_1562182261",
    "authResults": {
      "raw_header": "Authentication-Results: mx.messagelabs.com; spf=none (spf record not found)
 smtp.mailfrom=pi-dmas-auto001-d001.test; dkim=none (message not signed); dmarc=none header.from=pi-dmas-
auto001-d001.test\n",
      "dkim": "DKIM_NONE",
      "dkim_signing_domain": "",
      "spf": "SPF_NONE",
      "dmarc": "DMARC_NONE",
      "dmarc_policy": "DMARC_POLICY_NONE",
      "dmarc_override_action": ""
    },
    "filesAndLinks": [
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "SMTP Envelope (1)",
        "fileSize": 45,
        "fileType": "Email/HeaderPart",
        "md5": "b0025273674d7cb7688c8681c165d732",
        "sha256": "20278bedc0255b1a93f3453444b3a94ab36beea771f61f0d0c13edab68b1d312",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 2,
        "parentIndex": 1,
```

```
  "linkSource": "BASIC_EMAIL_INFO"
},
{
  "nodeType": "FILE_INCLUDED",
  "fileNameOrURL": "message.txt",
  "fileSize": 28,
  "fileType": "text/plain",
  "md5": "df76142276e354b558fe486c878a51e3",
  "sha256": "74f7fd3b1c262b7824396be68f5a7595bfc9d65a7c528e85a0eba8d7a1e23e96",
  "urlCategories": null,
  "urlRiskScore": null,
  "index": 4,
  "parentIndex": 3,
  "linkSource": "BASIC_EMAIL_INFO"
},
{
  "nodeType": "FILE_INCLUDED",
  "fileNameOrURL": "SMTP Envelope (2)",
  "fileSize": 128,
  "fileType": "Email/HeaderPart",
  "md5": "b43166aa8c7621885ef040e9a4b79049",
  "sha256": "e4f88b0f509be5ea90385205ab3e3aee4494131cce2a1f54d62a1f90ca4fb9ad",
  "urlCategories": null,
  "urlRiskScore": null,
  "index": 3,
  "parentIndex": 1,
  "linkSource": "BASIC_EMAIL_INFO"
},
{
  "nodeType": "FILE_INCLUDED",
  "fileNameOrURL": "file_attachment.txt",
  "fileSize": 5645,
  "fileType": "text/plain",
  "md5": "0d9c06c9e475b007c73200b8d7215d46",
  "sha256": "c927dddcaecbb21f0d4d7e7e8b67e205cbacd26eceb5faf345bf48735a7903fd",
  "urlCategories": null,
  "urlRiskScore": null,
  "index": 6,
  "parentIndex": 5,
  "linkSource": "BASIC_EMAIL_INFO"
},
{
  "nodeType": "LINK_INCLUDED",
  "fileNameOrURL": "http://scanningthesky.org/risk1.html?98",
  "fileSize": 0,
  "fileType": "",
  "md5": null,
  "sha256": null,
  "urlCategories": null,
  "urlRiskScore": null,
  "index": 7,
  "parentIndex": 6,
  "linkSource": "BASIC_EMAIL_INFO"
```

```
      },
      {
        "nodeType": "LINK_INCLUDED",
        "fileNameOrURL": "http://scanningthesky.org/risk1.html?96",
        "fileSize": 0,
        "fileType": "",
        "md5": null,
        "sha256": null,
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 8,
        "parentIndex": 6,
        "linkSource": "BASIC_EMAIL_INFO"
      },
      {
        "nodeType": "LINK_INCLUDED",
        "fileNameOrURL": "http://scanningthesky.org/risk1.html?95",
        "fileSize": 0,
        "fileType": "",
        "md5": null,
        "sha256": null,
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 9,
        "parentIndex": 6,
        "linkSource": "BASIC_EMAIL_INFO"
      },
      {
        "nodeType": "FILE_INCLUDED",
        "fileNameOrURL": "SMTP Envelope (0)",
        "fileSize": 518,
        "fileType": "Email/Header",
        "md5": "15f0f640200bf0b513a5b55d1e66c6d4",
        "sha256": "50cb6bac63b867e61d3bcd05d7cfd41856ac226dcf6aebab7c4ff41eb8a5c5a9",
        "urlCategories": null,
        "urlRiskScore": null,
        "index": 1,
        "parentIndex": 0,
        "linkSource": "BASIC_EMAIL_INFO"
      }
    ],
    "tlsInfo": null
  },
  "incidents": null
}
```


Sample10.json: Email Delivery Data


```
{
  "isOutbound": false,
  "xMsgRef": "00000000000000000000000000000000",
```

```
  "senderDomain": "sender.org",
  "senderName": "someone.withLongName",
  "rcptDomain": "symantec.com",
  "rcptName": "tester",
  "deliveryStatus": "DELIVERED",
  "binding": "REINJECT",
  "attempt": 1,
  "timestampZms": 1579202990011,
  "connectionIP": "123.32.11.128",
  "connectionHostname": "mail.symantec.com",
  "privacyUser": false,
  "banner": "This is the banner, a not so short banner",
  "smtpResponseCode": 250,
  "smtpResponseMessage": "Request action taken and completed.",
  "tlsAdvertised": true,
  "tlsUsed": true,
  "tlsPolicy": "OPPORTUNISTIC",
  "tlsProtocol": "some Protocol",
  "tlsCipher": "some cipher",
  "tlsKeyLength": 256,
  "tlsFallbackReason": "",
  "tlsForwardSecrecy": false,
  "tlsNegotiationFailed": false,
  "dkimSignature": "DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane; c=relaxed/
simple; q=dns/txt; t=1117574938; x=1118006938; h=from:to:subject:date:keywords:keywords;
 bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=; b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav
+yuU4zGeeruD00lszZVoG4ZHRNiYzR"
}
```


Symantec
by Broadcom Software