CLOUDFLARE

API Documentation

Area 1 Email Security

v 1.34.4

January 2023

Introduction

The Cloudflare Area 1 email security service offers Application Programming Interfaces (APIs) to expose our phishing campaign rulesets. These APIs both aid research and provide a set of indicators to block using network security edge devices.

All API requests are initiated using normal HTTP requests (GET/POST/DELETE), and responses are returned in JSON. Authentication to the APIs uses HTTP Basic Authentication over HTTPS.

Table of Contents

API Authentication and Authorization

All API access is controlled with a service account/password pair. Service account creation is self-service through the Area 1 Portal at https://horizon.area1security.com/settings/service-accounts . For example, to use the Blockable Indicators API with service account "`Nouv9pFhzfCprgMq7ReEW8KQoDdsTgXI9129EzGjbhEZBQFs089SvghphEWxU1yru6I_OqO4yWNc1234`" and password "`Jwtx6J7wEYQ5mFvi2WUB9qVBj3TgPm6ZntIT0CLobbdAHOIqypjgewCvTSCUabcd`", make the following HTTPS request:

```
  curl -u
'Nouv9pFhzfCprgMq7ReEW8KQoDdsTgXI9129EzGjbhEZBQFs089SvghphEWxU1yru6I_OqO4yWNc1
234:Jwtx6J7wEYQ5mFvi2WUB9qVBj3TgPm6ZntIT0CLobbdAHOIqypjgewCvTSCUabcd'
https://api.area1security.com/indicators

or with a browser

  https://api.area1security.com/indicators

and the browser will popup a login window to request the service account and
password
```

Rate Limiting

Some API endpoints are rate limited, so that resources can be better shared across all customers using the API. The following endpoints and their limits apply:

/alerts	12 / hour
/indicators	10 / hour
/search	4 / minute

These limits are enforced per customer. If the limit is exceeded, an HTTP 429 (Too Many Requests) status will be returned. The full body and headers, as from a curl command, look like this:

```
HTTP/1.1 429 Too Many Requests
Date: Thu, 13 Jun 2019 17:12:01 GMT
Retry-After: Thu Jun 13 18:11:56 GMT 2019 (in 3595 seconds)
Content-Type: application/json;charset=utf-8
Content-Length: 261
Server: Jetty(9.4.15.v20190215)

{
  "message" : "rate limited, query limit exceeded. Retry after: Thu Jun 13 18:11:56 GMT 2019 (in 3595 seconds)",
  "documentation_url" : "https://cdn.area1security.com/api/html/rate_limited.html",
  "url" : "http://localhost:8080/papillon/indicators",
  "status" : 429
}
```

Indicators API

This service returns malicious indicators (file hashes, URLs, domains, and IP address) that we recommend you block at your network edge using proxy devices and firewalls. For each indicator, the service returns the available details listed below. The Indicators API can be polled hourly for new information.

API Endpoints

https://api.area1security.com/indicators

API Parameters

- *since* limits results to indicators that were discovered after the given epoch timestamp (seconds, default = 0)
- *end* limits results to indicators that were discovered before the given epoch timestamp (seconds, default = current time)

Any indicator that was active during since-end interval will be returned. Both parameters are optional.

- *actor* limit the indicators to only those that involve the given actor (e.g. CHN1, RUS2)
- *killchain* limit the indicators to only those that are of the given killchain
- *cat* can be a category (e.g. "targeted" or "universal"), a malware family (e.g. "sofacy" or "rocket kitten"), or a threat type (e.g. "Actor Tool" or "Webshell")
- *type* is one of "domain", "filehash", "address", or "url"

Multiple values can be provided for these last three items by separating the values with commas, like "killchain=1,3" or "actor=CHN1,CHN2". That usage acts like an OR, it will return items that have killchain = 1 OR killchain = 3, or actor = CHN1 OR actor = CHN3.

If more than one of those parameters are used, it will act like an AND on the items. So combining the above example, "actor=CHN1,CHN2&killchain=1,3" would return indicators with an actor value of CHN1 or CHN3 AND a killchain of 1 or 3. An indicator with actor = CHN1 but a killchain = 5 in that case would not be returned.

Example Request

https://api.area1security.com/indicators?since=1449121459&end=1451538000&actor=CHN1&killchain=1,3

Response

Returns a list of indicators that should be blocked. Each item in the list contains:

- **item_type** The indicator's type (ip, domain, filehash, url).
- **item_name** The name of the indicator (ip address, domain name, filehash, url)
- **threat_name** The Area 1 Security authored threat name
- **first_detected** The epoch timestamp of when the indicator was first identified as malicious
- **description** (optional) A URL at which textual content describing the threat is available.
- **threat_categories** threat context as key value pairs (only present when the value is not null). These items are returned as arrays, because there can be multiple values for some of the categories (e.g. a url may be both a *Malicious Web Server* and a *Credential Harvester*):
    - *actor*: associated actor code
    - *category*: targeted or universal (Universal indicators are non-targeted phishing or malicious indicators)
    - *delivery_vecto*r: how the threat is delivered. Ex: email,
    - *kill_chain*: Kill chain values in the range of 0 through 7 indicating what stages of an attack the indicator is seen or used in. Smaller numbers indicate early stages of attack, larger numbers are associated with late stages of an attack.
    - *malware*: the family of malware with which the indicator is associated. Ex: Derusbi, PoisonIvy, PlugX
    - *motive*: motive of the threat actors using the indicator. Ex: espionage
    - *threat_type*: the threat type associated with the indicator. Ex: credential harvester, ransomware etc.

Example Response

Note: The following indicators' *item_name*s are not legitimate.


```
[
    {
      "threat_name": "Actor Infrastructure",
      "item_type": "address",
      "item_name": "127.0.0.1",
      "first_detected": 1448604680
    },
    {
      "threat_name": "Google Credential Harvester",
      "item_type": "domain",
      "item_name": "example.com",
      "first_detected": 1430582823
    },
    {
      "threat_name": "TC.DROPPERS_winrar_sfx",
      "item_type": "filehash",
      "item_name": "ad5475019da8dc903d91e0229a9c236e02215538",
      "first_detected": 1449138024
    },
    {
      "threat_name": "Google Credential Harvester",
      "item_type": "url",
      "description": "https://api.area1.com/nirvana/
  google-credential-harvesting.html",
      "item_name": "www.example.com/a-bad-url/",
      "first_detected": 1449164991,
      "threat_categories": [
        {
```

```
        "threat_type": [
           "Credential Harvester",
           "Malicious Web Server"
        ],
        "category": [
           "Universal"
        ],
        "killchain": [
          "3"
        ],
        "actor": [
          "CHN1"
        ]
      }
    ]
  }
]
```

Indicator Search API

This service can be queried with a basic indicator (file hash (MD5/SHA-1/SHA-256), URL, domain, IP Address, or email address) and returns information about the indicator. The API queries multiple Area 1 Security backend services, so the response can vary slightly depending on which service responds to the query.

API Endpoints

https://api.area1security.com/search

API Parameter

- *query* the indicator of interest
- *historic* return data from Area 1's internal systems for items that are not currently active (default is false, so you must add &historic=true to get this result)

Example Request

https://api.area1security.com/search?query=0123456789abcdeffedcba9876543210

https://api.area1security.com/search?query=127.0.0.1

https://api.area1security.com/search?query=example.com&historic=true

https://api.area1security.com/search?query=http://www.example.com/index.html

Response

Returns information that we know about the indicator, including:

- **indicator** The query term, possibly normalized (lowercased hash values, etc)
- **disposition** The indicator's status (UNKNOWN, BENIGN, SUSPICIOUS, MALICIOUS).
- **first_seen** The epoch timestamp of when the indicator was first seen
- **last_seen** The epoch timestamp of when the indicator was last seen

- **first_detected** The epoch timestamp when Area 1 Security first considered this item to be malicious
- **associated_items** Lists (possibly empty) of other items associated with the indicator, such as urls, files, or an infections_map containing infection names and number of times seen

- **Hash_MD5, Hash_SHA1, Hash_SHA256, Hash_authentihash, Hash_imphash, Hash_ssdeep -** other hash values that can be shown if the query term is a hash (MD5, SHA1, SHA256 are supported as query terms)
- **detail -** WHOIS information if the query term is a domain name
- **threat_categories** additional available data regarding each threat, currently sets of the values *actor, category, delivery_vector, kill_chain, malware, motive, threat_type*
- **threat_status** only displayed if historic=true, value of *active* or *inactive* to denote whether the item is considered a threat at the time of the query
- **tlp** traffic light protocol (https://www.us-cert.gov/tlp)
- **tag_histories** show time intervals where an indicator belonged to specific categories
    - In the first example below, the indicator "127.0.0.1" had one interval where it was tagged with *Actor-ABC1* (2 distinct time ranges within that interval) and one interval tagged with *Actor-ABC41*. That tag is currently active (the *end* value is "current").
  - **confidence_rating** our confidence (0-100) that this tag does indeed apply to the indicator (not all tags will have this field)
  - **overall_confidence** our overall confidence (0-100) for our judgement on this indicator. The value is chosen from a prioritized list of the tag_histories in the order { Actor, Indicator Category, Malware, Target, any other tag }.

All fields may not be present for a given query.

Example Response

Note: The following items' "indicator" values are not legitimate.

```
{
  "indicator": "www.example.com",
  "tag_histories": [
    {
      "intervals": [
        {
          "start": 1402128060000,
          "end": 1417680060000
        },
        {
          "start": 1422128060000,
          "end": 1447680060000
        }
      ],
      "category": "Actor",
      "confidence_rating": 70,
      "value": "ABC1"
    },
    {
      "intervals": [
        {
          "start": 1469114747000,
          "end": "1534803500"
        }
      ],
      "category": "Indicator Category",
      "confidence_rating": 80,
      "value": "Targeted"
    }
  ],
  "threat_status": "inactive",
  "disposition": "MALICIOUS",
  "first_seen": 1419277223000,
  "last_seen": 1470847567000,
  "tlp": "white",
  "family": "domain",
  "type": "Domain_Name",
  "associated_items": {
    "urls": [
      "http://example.com/t76f3g",
      "http://www.example.com/t76f3g"
    ],
    "infections_map": {
      "Ransomware Locky Distribution Site": 34
    },
    "ips": [
      "192.168.1.1"
```

```
    ]
  },
  "threat_categories": [
    {
      "threat_type": "Credential Harvester",
      "category": "Universal"
    },
    {
      "kill_chain": "3",
      "threat_type": "Malicious Web Server",
      "category": "Universal"
    }
  ],
  "detail": {
    "country": "united states",
    "ui_name": "domains by proxy, llc",
    "org": "domains by proxy, llc",
    "city": "scottsdale",
    "created": 1415810080000,
    "domain": "www.example.com",
    "name": "registration private",
    "geo_state": "arizona",
    "ui_place": "Scottsdale, Arizona, United States",
    "email": "www.example.com@domainsbyproxy.com"
  },
  "overall_confidence": 70
}
```


Example Response

/search endpoint results for a malicious file hash


```
{
  "indicator": "7e2561eb67a6ead09f727d98b71c01f18985bbb0",
  "first_seen": 1433810886000,
  "last_seen": 1478200022000,
  "Hash_ImpHash": "8b64d3ea6711c7e0a4e57bd12b350e0e",
"Hash_authentihash":"0a90f9d921b3b645e2f3773583d0029bdc3c81ce9a421244ab0ed9b0a
8c42667",
  "type": "Hash_SHA1",
  "Hash_ssdeep":
```

```
"6144:n6H8ZGtTBG+snn8KwrgprThQZsSJ0/pi9:6H8ZGtT0+mn8KygPKsc0o9",
  "disposition": "MALICIOUS",
  "tlp": "white",
  "Hash_MD5": "d1c27ee7ce18675974edf42d4eea2506",
  "tag_histories": [
    {
      "intervals": [
        {
          "start": 1337347427000,
          "end": "current"
        }
      ],
      "category": "Actor",
      "value": "PRK1"
    },
    {
      "intervals": [
        {
          "start": 1337347427000,
          "end": "current"
        }
       ],
       "category": "ThreatType",
       "value": "Dropper"
    },
   ],
  "family": "file",
  "Hash_SHA256":
"4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f740a5ee2de74f447be39b9"
}
```

Actors API

This service returns overview and summary information of each indicator associated with a known malicious actor. This information is updated twice per hour.

API Endpoints

https://api.area1security.com/actors[?actor=<actor_name>]

https://api.area1security.com/actors?actor=list

API Parameters

- *actor_name* Limits the response to the Area 1 authored name of an actor
- *list* Returns a list of Area 1 authored actors names
- *since* show changes in actors since this time. The value can be in iso8601 format (2022-04-24T12:34:56), YYYYMMDD (20220424), epoch seconds (since 1970) or epoch milliseconds (since 1970). If not specified, defaults to the beginning of the current day.
- *end* end of period for showing changes. The value can be in iso8601 format (2022-04-24T12:34:56), YYYYMMDD (20220424), epoch seconds (since 1970) or epoch milliseconds (since 1970). If not specified, defaults to the end of the current day.

Example Request

https://api.area1security.com/actors

(equivalent to https://api.area1security.com/actors?actor=ALL_ACTORS)

https://api.area1security.com/actors?actor=RUS1

https://api.area1security.com/actors?actor=RUS1&since=20221201&end=20221219

https://api.area1security.com/actors?actor=list

List API Response

If the list parameter is set, this API returns a list of Area 1 Security authored actor names.

Example List API Response


```
{
  "data": [
    "CHN6",
    "CHN2",
    "CHN4",
    "CHN5",
    "CHN3",
    "CHN13",
    "CHN1",
    "CHN8",
    "CHN9",
    "CHN24",
    "CHN11",
    "CHN12",
    "RUS1",
    "ALL_ACTORS"
  ]
}
```


Actor API Response

Returns a list of dictionary items that includes the following key value pairs:

- **actor** The Area 1 Security authored actor name

- **data** an array of data, one entry per indicator (domain, hash, ip, url) The fields in each data object are similar to those described above under the **Indicator Search API** section and so the descriptions won't be duplicated here.

Example Actor API Response


```
[
{
  "actor": "XX01",
  "data": [
    {
      "indicator": "web-backend.website.net",
      "tag_histories": [
      {
        "intervals": [
          {
            "start": 1475229111000,
            "end": "current"
          }
        ],
        "category": "Actor",
        "confidence_rating": 60,
        "value": "XX01"
      },
      {
        "intervals": [
          {
            "start": 1475229111000,
            "end": "current"
          }
        ],
```

```
        "category": "Indicator Category",
        "confidence_rating": 60,
        "value": "Targeted"
      }
    ],
    "first_seen": 1475229111000,
    "last_seen": 1475229111000,
    "type": "Domain_Name",
    "overall_confidence": 60
    }
  ]
}
]
```

Anonymity Endpoint API

This service returns information of each indicator associated with known indicators used to try to hide the originator. These could be anonymous mailboxes, anonymous mailers, Tor exit nodes, or VPNs.This information is updated twice per hour.

API Endpoints

https://api.area1security.com/anonymity[/<mailbox|mailer|tor|vpn>][/<active|all>]

https://api.area1security.com/anonymity/tor (defaults to active)

API Parameters

- *mailbox|mailer|tor|vpn* indicates what specific type of Anonymity indicator is being requested. If no type is specified, then all types will be returned.
- *active|all* the endpoint *active* or *all* determines the return of only currently tagged anonymity indicators (the default) or anything that has ever been tagged with *Anonymity*

Example Request

https://api.area1security.com/anonymity/tor

(equivalent to https://api.area1security.com/anonymity/tor/active)

https://api.area1security.com/anonymity/tor/all

Anonymity API Response

Returns a dictionary that includes the following key value pairs:

- **data** an array of data, one entry per indicator (domain, hash, ip, url) The fields in each data object are similar to those described above under the **Indicator Search API** section and so the descriptions won't be duplicated here.

The example shown below would correspond to a */tor/active* endpoint, where the *end* value for the Tor Exit Node is *"current"*. If the */tor/all* endpoint was used, some of the *end* values could have a numeric timestamp value instead of *current*.

Example Anonymity API Response


```
{
  "data": [
    {
      "associations": [
        {
          "name": "Private Internet Access (PIA)",
          "type": "Exit Node"
        },
        {
          "name": "swiss.privateinternetaccess.com",
          "type": "Resolves"
        }
      ],
      "first_seen": 1443814655000,
      "item_name": "179.43.156.194",
      "item_type": "IPv4_Address",
      "last_seen": 1493814514000,
      "tag_histories": [
        {
           "category": "Indicator Rating",
           "intervals": [
              {
                  "end": "current",
                  "start": 1388527418000
```

```
            }
         ],
         "value": "Anonymity"
        },
        {
            "category": "ThreatType",
            "intervals": [
                {
                    "end": "current",
                    "start": 1388527418000
                }
            ],
            "value": "Tor Exit Node"
        }
    ],
    "tlp": "white"
}
```

Emailalert API

This service returns the content of an email given an alert_id from the detection message sent from Area1 (slack, hipchat, email). Users may only retrieve and view emails that are associated with their company (using the API security credentials, uuid and password).

API Endpoints

https://api.area1security.com/emailalert?alert=<alert_id>&password=<password>

API Parameters

- *alert_id* the alert_id from an Area1 detection message
- *password* if a password is provided, the message will be encrypted in a zip file. Note that you must encode and special characters that are part of the password using standard url encoding.

Example Request

https://api.area1security.com/emailalert?alert=3xc7qzabcdxxxx31VJ-2017-08-22T10:09:12

https://api.area1security.com/emailalert?

alert=3xc7qzabcdxxxx31VJ-2017-08-22T10:09:12&password=passwd%20has%20spaces

Emailalert API Response

If a matching email is found for the given alert, the full content of the email will be saved to the user's computer. If the user has the browser configured to automatically save downloads, it will be saved to that directory with the filename *SMTP-alert_id.eml, or SMTP-alert_id.zip, if a password was provided.* If downloads are not saved automatically, the "Save File" dialog will be displayed, with the default filename *SMTP-alert_id.eml*.(or .zip).

Quarantine Release API

This service allows a quarantined message to be released to one or more of its original recipient(s). The message is identified using its alert_id, which may have been received via webhook push or via the Alerts API.

API Endpoints

POST https://api.area1security.com/quarantine-release

JSON Request Body Properties

- *alert* (required) the alert_id from an Area1 detection message
- *recipient* (optional) deliver the message to one or more of the specified original recipients. If not provided, the message will be released to all original recipients

Example Requests

In addition to the required *Authorization* header, POST requests should include the header specifying the body content as JSON: *Content-Type: application/json*

Example providing both alert ID and recipients:

```
POST https://api.area1security.com/quarantine-release
Content-Type: application/json
{
    "alert": "4NXwLh1kdK-2023-01-03T14:57:16",
    "recipient": [
        "user001@example.com",
        "user002@example.com"
    ]
}
```

Example providing both alert ID without recipients, which will release to all of the original message recipients:

```
POST https://api.area1security.com/quarantine-release
Content-Type: application/json
{
    "alert": "4NXwLh1kdK-2023-01-03T14:57:16"
}
```

Alternative Request Method: GET

This API may also be accessed using the HTTP GET request method by using the two JSON request body properties, “alert” and “recipient” as request parameters.

Example GET request providing on alert ID:

```
GET
https://api.area1security.com/quarantine-release?alert=4NXwLh1kdK-2023-01-03T14
:57:16
```

Example GET request providing alert ID and target recipients:

```
GET
https://api.area1security.com/quarantine-release?alert=4NXwLh1kdK-2023-01-03T14
:57:16&recipient=user001@example.com&recipient=user002@example.com
```

Quarantine Release API Response

A successful quarantine release request will return an HTTP status 200 with JSON response body listing the email addresses for the release.

```
{
    "delivered": [
        "user001@example.com",
        "user002@example.com"
    ]
```

```
}
```

An unsuccessful response will return an HTTP status 4xx or 5xx with a JSON response body that includes an error message.

```
{
    "error": "No message found for provided alert"
}
```

Alerts API

This service returns information of each alert that is generated through the Area 1 Security email product. The same information is available through a push-to-SIEM feature in real time, but this endpoint is provided for users who don't have a SIEM or are unable to open it up to our pushes. All timestamps are in UTC. Items that have no value or are empty will not be displayed (e.g. an email with no attachments will have no attachments item rather than having an attachments item with an empty value).

This endpoint will return up to 5,000 alerts, depending on your email volume and the time range used. If the endpoint returns a 504 Gateway Timeout error, it's likely that it's trying to process and return too much data. In that case it's recommended to provide a limit parameter on the request and use a smaller value than the default of 5,000. Also, the since= and end= parameters may be used to limit the time range.

API Endpoints

https://api.area1security.com/alerts?[disposition=bulk,malicious,suspicious,spam,spoof,all]&[since=iso8601, seconds]&[end=iso8601, seconds]&[limit=]&[page=]

API Parameters

- *disposition=malicious,suspicious,spoof,spam,bulk,all* indicates what level of alert is being requested. If no type is specified, then only MALICIOUS alerts will be returned. Comma-separated values are accepted (e.g disposition=malicious,suspicious). The disposition *ALL* is equivalent to *disposition=malicious,suspicious,spoof,spam*.
- *since* the start of the alert time window. The value can be in iso8601 format (2022-04-24T12:34:56), YYYYMMDD (20220424), epoch seconds (since 1970). If not specified, defaults to the beginning of the current day.
- *end* the end of the alert time window. The value can be in iso8601 format (2022-04-24T12:34:56), YYYYMMDD (20220424), epoch seconds (since 1970). If not specified, defaults to the end of the current day.

- *limit* the maximum number of records to return in the response. The maximum allowed value, and also the default, is 5,000 records. See *page* parameter for more on paging through results.
- *page* return the next page of results using the token returned by the "Next-Page" response header from prior request. Note that alerts for messages are typically delayed between 5 and 10 minutes from the time the message was processed. When requesting the most recent alerts, using the *page* parameter on the same request may return new messages

Example Request

Retrieve the first 100 alerts since the start of the current day UTC:

https://api.area1security.com/alerts?limit=100

Retrieve the next 100 alerts received since the start of the current day UTC, using the “Next-Page” header value from the previous response:

https://api.area1security.com/alerts?limit=100&page=1auct-hp8d

Retrieve the first 5,000 malicious or suspicious messages since 01:00 UTC on 2022-04-24:

https://api.area1security.com/alerts?disposition=malicious,suspicious&since=2022-04-24T01:00:00

Alerts API Response

Returns a JSON array that includes the following data for each alert as JSON objects:

Example Alerts API Response

```
Headers:
  Next-Page: 1auct-hp8d
```

```
Body:
[
  {
    "source": "area1security",
    "time": 1524570920,
    "event": {
    "final_disposition": "MALICIOUS",
    "delivery_mode": "DIRECT",
    "attachments": [
     {
      "sha1": "9817e37aa1e615713e3049979542ca41e2abcb37",
      "sha256":
"e3baa939f091b712bd5d96d2a826c136d969bd9b1b57065febbb7492b1cbef69",
       "content_type_provided": "image/jpeg",
       "content_type_computed": "image/jpeg",
       "name": "image003.jpg",
       "ssdeep":

"48:lX6uERAL3EZ+XRjeG7tma95wp5RQf/gMo/SNXI38mfKDNVBLWrQg:l9EMg+jeG7TedQfI
MoqRxEfLsQg",

       "md5": "965364701f344f098ae913cb59b6aa1c",
       "extension": "jpg",
       "att_size": 123456
      }
     ],
     "smtp_helo_server_name": "mail.example.net",
     "envelope_to": [
      "user@example.com"
     ],
     "subject": "Potential Partnership",
```

```
    "smtp_helo_server_ip_as_name": "LIQUIDWEB - Liquid Web, L.L.C, US",
    "alert_reasons": [
      "Malicious previous hop domain server 'mail.example[dot]net'",
      "no really, it's a very mailicious domain 'example[dot]net'"
    ],
    "encrypted_feature_count": null,
    "message_id": "<002001d3db86$7bb1b220$73660$@example.com.ph>",
    "replyto_name": null,
    "from_name": "Christine",
    "smtp_helo_server_ip": "192.168.1.184",
    "smtp_helo_server_ip_geo": "US/-/-",
    "smtp_helo_server_ip_as_number": "3232235960",
    "envelope_from": "christine@example.com.ph",
    "alert_id": "40VVylabcbz7pJj-2022-04-24T04:41:19",
    "replyto": "christine@example.com.ph",
    "from": "CEO Christine <christine@example.com.ph>",
    "to": [
      "user@example.com"
    ],
    "links": [
     "http://uh-oh.thisisa.com/badlink",
     "http://another-malicious-link.xyz/"
     ],
   "ts": "2022-04-24T04:41:19Z"
  }
 }
... and possibly many more
]
```


One important value in the result is the ***alert_id*** field, which can be used with the /emailalerts endpoint to get back to the original email content.

Useractivity Endpoint API

This service returns the API activity data for the logged-in user (customer). It shows all activity against the various API endpoints and the Area 1 customer portal for the requested time range. Default is the current day's activity.

API Endpoints

https://api.area1security.com/useractivity?since=date&end=date

API Parameters

- *since* the start date for the activity request. The value can be in iso8601 format (2022-04-24T12:34:56), YYYYMMDD (20220424), epoch seconds (since 1970) or epoch milliseconds (since 1970). If not specified, defaults to the beginning of the current day.
- *end* the end date for the activity request. The value can be in iso8601 format (2022-04-24T12:34:56), YYYYMMDD (20220424), epoch seconds (since 1970) or epoch milliseconds (since 1970). If not specified, defaults to the end of the current day.

Example Request

https://api.area1security.com/useractivity (gets activity for today)

https://api.area1security.com/useractivity?since=20220901&end=20220930

Useractivity API Response


```
{
  "data": [
    {
      "created_at": 1538482202098,
      "source": "api",
      "action": "indicators",
      "attributes": {
```

```
        "since": 1537877401000
      },
      "customer_name": "A1S",
      "customer_id": "acdadd2e-c63e-11e8-9bd8-5b14f50beb85",
      "s0": "since=1537877401000"
    },
    {
      "created_at": 1538482011705,
      "source": "api",
      "action": "alerts",
      "attributes": {
        "disposition": "(MALICIOUS|SUSPICIOUS|SPOOF|SPAM)",
        "end": 1538480204000,
        "since": 1538479304000
      },
      "customer_name": "A1S",
      "customer_id": "acdadd2e-c63e-11e8-9bd8-5b14f50beb85"
    },
    {
      "created_at": 1538481112544,
      "source": "api",
      "action": "search",
      "query": "www.example.com",
      "customer_name": "A1S",
      "customer_id": "acdadd2e-c63e-11e8-9bd8-5b14f50beb85"
    }
  ]
}
```

Domainproximity Endpoint API

This service returns information on domains that are similar to domains registered with Area 1 Security for the logged-in user (customer). Several different algorithms are used to determine the similarity compared to newly registered domains in WHOIS data.

API Endpoints

https://api.area1security.com/domainproximity?distance=value

API Parameters

- *distance* show similar domains less than or equal to this value, according to the edit distance measure. Value is in the range 1-3, with a default of 3 if not specified.

Example Request

https://api.area1security.com/domainproximity (gets all similar domains)

https://api.area1security.com/domainproximity?distance=1

Response

Returns information that we know about the indicator, including:

- **domain -** the reference domain that's being compared
- **imp_domain -** the newly registered impostor domain to be compared to the reference domain.
- **reg_dt -** the registration date of the (potential impostor) domain.
- **edit_dist** - The (modified) Levenshtein distance (number of additions/subtractions/substitutions) between the reference domain and the potential impostor domain (the *distance* parameter).
- **norm_dist** - The Levenshtein distance normalized by the character length of the domain.

Domainproximity API Response


```
{
  "domain": "area1security.com",
  "data": [
      {
      "reg_dt": "2018-11-23T00:00:00Z",
      "norm_dist": 0.2,
      "edit_dist": 3,
      "imp_domain": "ar-security.com"
      },
      {
      "reg_dt": "2018-05-13T00:00:00Z",
      "norm_dist": 0.0666666666666667,
      "edit_dist": 1,
      "imp_domain": "areassecurity.com"
      },
      {
      "reg_dt": "2018-02-13T00:00:00Z",
      "norm_dist": 0.133333333333333,
      "edit_dist": 2,
      "imp_domain": "arsalsecurity.com"
      }
  ]
}
```

Detections Search Endpoint API

This service returns information for each email that matches the search parameter(s). Only emails that have a detection (final_disposition of SPOOF, SPAM, SUSPICIOUS, MALICIOUS-BEC or MALICIOUS) will be searched. The content of the following email metadata fields are searched:

- alert_id
- CC
- From (envelope_from)
- From Name
- final_disposition
- md5 hash (of any attachment)
- sha1 hash (of any attachment)
- sha256 hash (of any attachment)
- name (of any attachment)
- Reason
- Received DateTime (yyyy-mm-ddThh:mm:ss)
- Sent DateTime (yyyy-mm-ddThh:mm:ss)
- ReplyTo
- To (envelope_to)
- To Name
- Message-ID
- smtp_helo_server_ip
- smtp_previous_hop_ip
- x_originating_ip
- Subject

API Endpoints

https://api.area1security.com/detections-search

API Parameters

- *query* space delimited query term(s) [Required] case-insensitive, multiple words must be separated by spaces (spaces url-encoded as "%20" or "+")
- *days_back* how far back to begin the search (default is 7, max is 365)
- *limit* how many results to return (default is 100, max is 1000)

Example Request

https://api.area1security.com/detections-search?query=malicious

https://api.area1security.com/detections-search?query=malicious&days_back=3

https://api.area1security.com/detections-search?query=bob+jones

Response

Returns a JSON object containing metadata fields from emails that matched the query.

- **data** list containing each of the search results
- **query_time:** the time in epoch milliseconds UTC

Detections Search API Response


```
{
  "data": [
    {
      "cc": null,
      "tracking_value_sent": "",
      "final_disposition": "MALICIOUS",
      "x_originating_ip": null,
      "to_name": null,
      "subject": "listen, I highly recommend u to read that email, just to
ensure not a thing will take place ",
      "findings": [
```

```
            {
        "reason": "IP is a source of spam/uce :
Smtp-Helo-Server-Ip='127.0.0[dot]186'",
        "score": null,
        "detection": "SPAM",
        "field": "smtp_helo_server_ip",
        "attachment": null,
        "portion": "SMTP",
        "name": "blocklist",
        "action": "PROMOTE",
        "detail": null,
        "diagnostic": "",
        "value": "127.0.0.186",
        "version": null
            }
        ],
        "sent_date": "2019-11-21T00:22:01",
        "detectionReasons": [
            "IP is a source of spam/uce :
Smtp-Helo-Server-Ip=<b>127.0.0[dot]186</b>"
        ],
        "client_uuid": "abcdef12-3456-7890-abcd-ef1234567896",
        "from_name": null,
        "smtp_helo_server_ip": "127.0.0.186",
        "smtp_previous_hop_ip": "127.0.0.186",
        "envelope_from": "d1994@example.com",
        "replyto": "d1994@example.com",
        "from": "d1994@example.com",
        "to": [
            "email@area1security.com"
        ],
```

```
      "threat_cats_blocking": [
          "IdentityDeception",
          "BrandImpersonation",
          "CredentialHarvester",
          "Link"
      ],
      "client_name": "area1",
      "postfix_ident": "47JJcT1w6GztQV7",
      "ts": "2019-11-20T23:22:01"
      }
  ],
  "query_time": 1574294490485
}
```

Mailtrace Endpoint API

This service returns information for each email that matches the search parameter(s). All email can be searched, whether it registered a detection or not. Only certain fields from the email will be searched.

- **alert_id** (as parameter *alertId*)
- **from** (email from address as parameter *sender*)
- **message_id** (as parameter *messageId*)
- **subject** (any words, as parameter *subject*)
- **to** (email to address as parameter *recipient)*

API Endpoints

https://api.area1security.com/mailtrace

API Parameters

- *subject* space delimited word(s) from the email subject, case-insensitive, multiple words must be separated by spaces
- *alertId* the full alert_id field (only present for emails with a final_disposition of SPOOF, SPAM, SUSPICIOUS, MALICIOUS-BEC, or MALICIOUS)
- *messageId* the full messageid of the email
- *recipient* any "To" address of the email
- *sender* the "From" address of the email
- *since* the start time of the search window. The value can be in iso8601 format (2018-04-24T12:34:56), epoch seconds, epoch milliseconds, or YYYYMMDD (default is 7 days ago)
- *end* the end time of the search window. The value can be in iso8601 format (2018-04-24T12:34:56), epoch seconds, epoch milliseconds, or YYYYMMDD (default is the current time)
- *limit* how many results to return (default is 100, max is 1000)

Example Requests

https://api.area1security.com/mailtrace?alertid=43pVC02YH1zHQN4-2019-01-29T02:03:09

https://api.area1security.com/mailtrace?alertid=43pVC02YH1zHQN4-2019-01-29T02:03:09&since=20191101

https://api.area1security.com/mailtrace?subject=lost+found

Response

Returns a JSON object containing metadata fields from emails that matched the query.

- **data** list containing each of the search results
- **query_time:** the time in epoch milliseconds UTC

Detections Search API Response


```
{
  "data": [
      {
        "postfix_ident_outbound": "47Jjdp3WRsz11M1D",
        "final_disposition": "NONE",
        "envelope_to": [
          "rebecca@example.com"
        ],
        "subject": "[EXTERNAL] RE: Lost and found",
        "from": "kelsey@example.com",
        "message_id": "<DM3P159M258D4E0@DM3P159MB001.PROD.OUTLOOK.COM>",
        "postfix_ident": "47Jjcz1H88z11M4F",
        "client_name": "mr. client",
        "ts": "2019-11-21T15:09:33"
      }
    ]
```

```
  "query_time": 1574294490485
}
```

Preview Endpoint API

This service returns the content of an email rendered as a PNG image given an alert_id from the detection message sent from Area1 (slack, email). Users may only retrieve and view emails that are associated with their company (using the API security credentials, uuid and password).

API Endpoints

https://api.area1security.com/preview?alert=<alert_id>

API Parameters

- *alert_id* the alert_id from an Area1 detection message

Example Request

https://api.area1security.com/preview?alert=3xc7qzabcdxxxx31VJ-2017-08-22T10:09:12

Preview API Response

If a matching email is found for the given alert, the body of the email will be converted to a PNG image, which will be displayed directly in the browser, or can be redirected to a file (if accessing the API with a script or curl).

Analyze SPF Endpoint API

This endpoint analyzes the SPF record for the given domain and returns the results.

Note: This is a public endpoint (no authorization credentials needed to use it).

API Endpoints

https://api.area1security.com/pub/analyzespf/<domain><?ip=ipaddress>

API Parameters

- *domain* the domain name to be analyzed (required)
- *ip* analyze the SPF policy record for the provided domain given this originating IP address

Example Request

https://api.area1security.com/pub/analyzespf/area1security.com

Analyze SPF API Response

This shows the result for a valid SPF record.


```
{
  "data": [
    {
      "result": "valid",
      "reason": null,
      "policy_record": "v=spf1 include:spf.mandrillapp.com
include:et._spf.pardot.com include:mail.zendesk.com include:es._spf.adp.com
include:_spf.salesforce.com include:spf.protection.outlook.com
a:rpc.boldchat.com -all",
      "spf_records": [
        {
```

```
          "hostname": "example.com",
          "record": "v=spf1 include:spf.mandrillapp.com
include:et._spf.pardot.com include:mail.zendesk.com include:es._spf.adp.com
include:_spf.salesforce.com include:spf.protection.outlook.com
a:rpc.boldchat.com -all"
        },
        {
          "hostname": "spf.mandrillapp.com",
          "record": "v=spf1 ip4:198.2.128.0/24 ip4:198.2.132.0/22
ip4:198.2.136.0/23 ip4:198.2.145.0/24 ip4:198.2.186.0/23
ip4:205.201.131.128/25 ip4:205.201.134.128/25 ip4:205.201.136.0/23
ip4:205.201.139.0/24 ip4:198.2.177.0/24 ip4:198.2.178.0/23 ip4:198.2.180.0/24
~all"
        },
        {
          "hostname": "et._spf.pardot.com",
          "record": "v=spf1 ip4:198.245.81.0/24 ip4:136.147.176.0/24
ip4:13.111.0.0/22 ip4:13.111.52.0/22 ip4:13.111.63.0/24 ip4:13.111.68.0/24
ip4:13.111.72.0/22 ip4:13.111.92.0/24 ip4:13.111.111.0/24 ip4:136.147.182.0/24
ip4:136.147.135.0/24 ip4:199.122.123.0/24 -all"
        },
        {
          "hostname": "mail.zendesk.com",
          "record": "v=spf1 ip4:103.151.192.0/23 ip4:185.12.80.0/22
ip4:188.172.128.0/20 ip4:192.161.144.0/20 ip4:216.198.0.0/18 ~all"
        },
        {
          "hostname": "es._spf.adp.com",
          "record": "v=spf1 ip4:170.146.220.0/24 ip4:170.146.221.0/24
ip4:170.146.224.15 ip4:170.146.224.16/31 ip4:170.146.226.15
ip4:170.146.226.16/31 -all"
```

```
        },
        {
          "hostname": "_spf.salesforce.com",
          "record": "v=spf1 exists:%{i}._spf.mta.salesforce.com -all"
        },
        {
          "hostname": "spf.protection.outlook.com",
          "record": "v=spf1 ip4:40.92.0.0/15 ip4:40.107.0.0/16
ip4:52.100.0.0/14 ip4:104.47.0.0/17 ip6:2a01:111:f400::/48
ip6:2a01:111:f403::/48 include:spfd.protection.outlook.com -all"
        },
        {
          "hostname": "spfd.protection.outlook.com",
          "record": "v=spf1 ip4:51.4.72.0/24 ip4:51.5.72.0/24 ip4:51.5.80.0/27
ip4:20.47.149.138/32 ip4:51.4.80.0/27 ip6:2a01:4180:4051:0800::/64
ip6:2a01:4180:4050:0800::/64 ip6:2a01:4180:4051:0400::/64
ip6:2a01:4180:4050:0400::/64 -all"
        }
      ],
      "domain": "example.com",
      "dns_lookups": [
        {
          "primary_spf_include": false,
          "hostname": "example.com",
          "record_type": "TXT"
        },
        {
          "primary_spf_include": true,
          "hostname": "spf.mandrillapp.com",
          "record_type": "TXT"
        },
```

```
      {
        "primary_spf_include": true,
        "hostname": "et._spf.pardot.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": true,
        "hostname": "mail.zendesk.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": true,
        "hostname": "es._spf.adp.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": true,
        "hostname": "_spf.salesforce.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": false,
        "hostname": "0.0.0.0._spf.mta.salesforce.com",
        "record_type": "A"
      },
      {
        "primary_spf_include": true,
        "hostname": "spf.protection.outlook.com",
        "record_type": "TXT"
      },
      {
```

```
          "primary_spf_include": false,
          "hostname": "spfd.protection.outlook.com",
          "record_type": "TXT"
        },
        {
          "primary_spf_include": false,
          "hostname": "rpc.boldchat.com",
          "record_type": "A"
        }
      ]
    }
  ],
  "ts": 1631729275
}
```

And this is the result for an invalid SPF record.


```
{
  "data": [
    {
      "result": "permerror",
      "reason": "Maximum (10) mechanism/modifiers calls done: 12",
      "policy_record": "v=spf1 include:_spf.google.com
include:_spfprod.badexample2.com include:servers.mcsv.net
include:bounce.badexample3.com include:_spf.intacct.com
include:helpscoutemail.com ~all",
      "spf_records": [
        {
          "hostname": "badexample.com",
          "record": "v=spf1 include:_spf.google.com
include:_spfprod.badexample2.com include:servers.mcsv.net
include:bounce.badexample3.com include:_spf.intacct.com
include:helpscoutemail.com ~all"
        },
        {
          "hostname": "_spf.google.com",
          "record": "v=spf1 include:_netblocks.google.com
include:_netblocks2.google.com include:_netblocks3.google.com ~all"
        },
        {
          "hostname": "_netblocks.google.com",
          "record": "v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19
ip4:66.102.0.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0.0/16
ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19
ip4:216.239.32.0/19 ~all"
        },
```

```
        {
          "hostname": "_netblocks2.google.com",
          "record": "v=spf1 ip6:2001:4860:4000::/36 ip6:2404:6800:4000::/36
ip6:2607:f8b0:4000::/36 ip6:2800:3f0:4000::/36 ip6:2a00:1450:4000::/36
ip6:2c0f:fb50:4000::/36 ~all"
        },
        {
          "hostname": "_netblocks3.google.com",
          "record": "v=spf1 ip4:172.217.0.0/19 ip4:172.217.32.0/20
ip4:172.217.128.0/19 ip4:172.217.160.0/20 ip4:172.217.192.0/19
ip4:172.253.56.0/21 ip4:172.253.112.0/20 ip4:108.177.96.0/19 ip4:35.191.0.0/16
ip4:130.211.0.0/22 ~all"
        },
        {
          "hostname": "_spfprod.badexample3.com",
          "record": "v=spf1 ip4:161.199.13.0/24 ip4:192.133.16.0/24
ip4:192.82.209.0/24 ip4:161.199.112.0/24 ip4:74.121.196.224/27
ip4:162.249.108.96/28 ip4:38.111.1.0/24 ip4:65.144.119.0/24 ip4:146.20.113.101
ip4:146.20.113.144 ip4:146.20.113.217 ip4:156.70.24.139 ip4:156.70.25.163
~all"
        },
        {
          "hostname": "servers.mcsv.net",
          "record": "v=spf1 ip4:205.201.128.0/20 ip4:198.2.128.0/18
ip4:148.105.8.0/21 -all"
        },
        {
          "hostname": "bounce.badexample2.com",
          "record": "v=spf1 a ip4:64.94.250.0/25 ip4:66.151.182.16/28
ip4:66.151.230.128/25 ip4:69.25.74.128/26 ip4:69.25.201.128/25
ip4:69.25.202.64/26 ip4:69.25.243.160/27 ip4:70.42.50.128/26 ip4:70.42.57.0/25
```

```
ip4:63.251.142.0/24 ip4:38.97.115.0/24 ip4:161.199.13.0/24
include:sp.actionkit.com -all"
        },
        {
          "hostname": "sp.actionkit.com",
          "record": "v=spf1 exists:%{i}._spf.sparkpostmail.com ~all"
        },
        {
          "hostname": "_spf.intacct.com",
          "record": "v=spf1 ip4:4.7.16.128/26 ip4:38.108.186.0/24
ip4:199.87.209.0/24 ip4:4.53.200.128/26 ip4:52.62.199.66 ip4:52.19.0.156
ip4:3.97.56.230 ip4:18.233.211.170 ?all"
        },
        {
          "hostname": "helpscoutemail.com",
          "record": "v=spf1 ip4:54.173.229.38 ip4:52.0.20.102
ip4:54.174.116.32 ip4:52.2.238.96 ip4:52.20.146.34 ip4:34.198.122.65 ~all"
        }
      ],
      "domain": "badexample.com",
      "dns_lookups": [
        {
          "primary_spf_include": false,
          "hostname": "badexample.com",
          "record_type": "TXT"
        },
        {
          "primary_spf_include": true,
          "hostname": "_spf.google.com",
          "record_type": "TXT"
        },
```

```
      {
        "primary_spf_include": false,
        "hostname": "_netblocks.google.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": false,
        "hostname": "_netblocks2.google.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": false,
        "hostname": "_netblocks3.google.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": true,
        "hostname": "_spfprod.ngpvan.com",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": true,
        "hostname": "servers.mcsv.net",
        "record_type": "TXT"
      },
      {
        "primary_spf_include": true,
        "hostname": "bounce.badexample2.com",
        "record_type": "TXT"
      },
      {
```

```
          "primary_spf_include": false,
          "hostname": "bounce.badexample2.com",
          "record_type": "A"
        },
        {
          "primary_spf_include": false,
          "hostname": "sp.actionkit.com",
          "record_type": "TXT"
        },
        {
          "primary_spf_include": false,
          "hostname": "<ip>._spf.sparkpostmail.com",
          "record_type": "A"
        },
        {
          "primary_spf_include": true,
          "hostname": "_spf.intacct.com",
          "record_type": "TXT"
        },
        {
          "primary_spf_include": true,
          "hostname": "helpscoutemail.com",
          "record_type": "TXT"
        }
      ]
    }
  ],
  "ts": 1631729251
}
```

System Status Endpoint API

This endpoint returns the status of many Area 1 systems. The results are updated every 5 minutes, so there's no need to access the endpoints any more often than that.

API Endpoints

https://api.area1security.com/status</service>

API Parameters

- *service* if present, the Area 1 system to check the status of. If not specified, then the status of all systems will be returned.
- Valid values for "service" are "api", "dns", "email", "portal".

Example Request

https://api.area1security.com/status - returns status of all systems

https://api.area1security.com/status/email - returns the status of the email system

System Status API Response

This shows the result for a request for ALL systems. Subsystem requests show only the respective part of the ALL result.

"last_updated" indicates when our system last checked the status of the others

"status_last_changed" is the timestamp of the last system update (usually indicating the time an outage began or ended)

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
 "last_updated": "2021-09-29T18:35:01Z",
 "data": [
```

```
    {
      "name": "Email Protection Service",
      "description": "Cloud Anti-Phishing MTA",
      "status": "operational",
      "status_last_changed": "2021-08-31T21:27:36.207Z"
    },
    {
      "name": "Recursive DNS Service",
      "description": "Cloud Anti-Phishing DNS Resolver",
      "status": "operational",
      "status_last_changed": "2021-09-27T17:00:51.990Z"
    },
    {
      "name": "API",
      "description": "API service accessing Area 1 data",
      "status": "operational",
      "status_last_changed": "2020-11-21T06:00:36.101Z"
    },
    {
      "name": "Customer Portal",
      "description": "Management Portal",
      "status": "operational",
      "status_last_changed": "2021-05-20T20:54:37.949Z"
    }
  ],
  "ts": 1632940553
}
```

Customer Reports Endpoint API

This endpoint returns customer-specific reports saved and maintained in one of our internal security system.

API Endpoints

https://api.area1security.com/customerreports

API Parameters

- *since:* Returns reports created after this date/time. Format supports “YYYY-MM-DD” format, as well as “YYYY-MM-DDTHH:MM:SS”. Timestamp values are assumed to be UTC.
- *disposition:* one of MALICIOUS, SUSPICIOUS, SPOOF, SPAM or BULK

Example Request

https://api.area1security.com/customerreports - returns all reports for this customer

System Status API Response

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
  "data": [
      {
      "created": "2020-12-02T01:23:56.925569Z",
      "message_id": "<20201118155306.7ECCB27C5E@localhost>",
      "title": "Domain Impersonation of Vendor example[.]com",
      "priority": "Low",
      "content": "## Overview\nSometime prior to 2020-11-18T15:53:08Z an
unknown attack group specializing in BEC Type 3 attacks registered the
malicious domain name examp1e[.]com in order to facilitate a near perfect
impersonation of the vendor domain name example[.]com.  Following
registration, the attacker created the malicious email address
```

```
badguy@example[.]com.  The attacker initiated a malicious email on
2020-11-18T15:53:08Z to Area 1 user goat@area1security.com with a subject of
This is a BEC Type 4 Test Email and attempted to get the user
goat@area1security.com to take action on their request.  Area 1 Security was
unable to verify if the legitimate vendor example[.]com was or was not
compromised at this time.\n\n## Targets and Victimology\n* Area 1 Target:
goat@area1security.com\n\n## Details\n* Delivery Disposition: SPAM\n* Current
Disposition: MALICIOUS\n* Area 1 - Alert ID:
4CbnQX52XTztQVB-2020-11-18T15:53:08\n* Message-ID:
<20201118155306[.]7ECCB27C5E@localhost>\n* Timestamp: 2020-11-18T15:53:08Z\n*
Subject: This is a BEC Type 4 Test Email\n* Attempted Fraudulent Amount:
N/A\n\n### Indicators of Compromise (IOC)\n* badguy@example[.]com - MALICIOUS
Email Account - This account has been automatically marked by Area 1 Security
as MALICIOUS for a period of 2 years.\n* example[.]com - MALICIOUS Domain Name
- This account has been automatically marked by Area 1 Security as MALICIOUS
for a period of 2 years.\n\n## References\n### Follow Up Actions\nNOTE: In
order to further train our models to detect these attacks faster, please
locate all original emails from this attack and send them as EML files to our
automated Phish Submission System area1@area1reports.com.",
      "tags": [
      {
      "category": "ThreatType",
      "value": "BEC Type 3"
      },
      {
      "category": "ThreatType",
      "value": "BEC"
      },
      {
      "category": "ThreatType",
      "value": "Identity Deception"
```

```
      },
      {
      "category": "ThreatType",
      "value": "Domain Impersonation"
      }
      ],
      "disposition": "MALICIOUS",
      "content_fields": {},
      "recipients": [
          "goat@area1security.com"
      ],
      "client_name": "area1",
      "postfix_ident": "4CbnQX52XTztQVB",
      "updated": "2021-01-26T03:41:28.199802Z",
      "status": "Pending",
      "ts": "2020-11-18T15:53:08"
    }
  ],
  "ts": 1639054136
}
```

MailConfig Allowlist Endpoint API

This endpoint returns the various Allowlist items that can be configured for the Area 1 Email Protection Service through the Area 1 Portal (Settings|Allow List|Allowed Patterns). Trusted Senders, Exempt Recipients, and Acceptable Senders will be exempted from normal detection scanning.

API Endpoints

https://api.area1security.com/allowlists<|(acceptablesenders|exemptrecipients|trustedsenders)

API Parameters

- *acceptablesenders/exemptrecipients/trustedsenders* if present, only that subset of the Allowlists will be returned.

Example Request

https://api.area1security.com/allowlists - returns all configured allowlists

https://api.area1security.com/allowlists/trustedsenders - returns only the trustedsenders data

MailConfig Allowlist API Response

This shows the result for a request for ALL allowlists. Some entries may show up in multiple sub-lists (e.g. trustedsenders and exemptrecipients)

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
  "data": {
      "ts": 1638453455,
      "acceptable_senders": [
        {
          "is_sender": true,
```

```
        "comments": "email with whitespace",
        "is_regex": true,
        "pattern": "fred\\ bloggs@example.com",
        "created_at": "Thu, 06 Aug 2020 21:52:02 GMT",
        "is_spoof": true,
        "id": 27352,
        "last_modified": "Fri, 04 Dec 2020 18:56:55 GMT",
        "sender verification": true,
        "is_recipient": true
      }
    ],
    "exempt_recipients": [
      {
        "is_sender": true,
        "comments": "email with whitespace",
        "is_regex": true,
        "pattern": "fred\\ bloggs@example.com",
        "created_at": "Thu, 06 Aug 2020 21:52:02 GMT",
        "is_spoof": true,
        "id": 27352,
        "last_modified": "Fri, 04 Dec 2020 18:56:55 GMT",
        "sender verification": true,
        "is_recipient": true
      }
    ],
    "trusted_senders": [
      {
        "is_sender": true,
        "comments": "IP regex",
        "is_regex": true,
        "pattern": "147\\.160\\.167\\.([0-9]|[1-5][0-9]|6[0-3])",
```

```
            "created_at": "Tue, 27 Oct 2020 23:20:59 GMT",
            "is_spoof": false,
            "id": 27401,
            "last_modified": "Mon, 30 Nov 2020 19:06:43 GMT",
            "sender verification": true,
            "is_recipient": false
          }
        ]
    }
}
```

The data returned for one of the sub-items looks similar to the above, but it only contains the data for the specific request (e.g. */allowlists/trustedsenders* returns only the *trusted_senders* array).

Creating New Allowlist Items

New Allowlist items can be created by sending a properly-formatted JSON body as a POST request to these same endpoints.

curl -u service_account_id:private_key -X POST --data-binary '@/tmp/post.json' https://api.area1security.com/allowlists</acceptablesenders|exemptrecipients|trustedsenders>

Where the file */tmp/post.json* contains json in this format (*pattern* represents an email address or a domain and can be a fixed string or a regular expression).

```
{
    "data": [
      {
            "pattern": "required[0-9]{3}@example.com",
            "comments": "optional, but helpful"
      },
      {
            "pattern": "required-with-default-comments@example.com"
```

```
      }
    ]
}
```

The API return data from that POST, assuming success, will look like this

```
{
  "blackbox": {
    "data": {
      "failures": [],
      "whitelists": {
      "num_pages": 10,
      "rows": [
      {
              "is_sender": true,
              "comments": "added by API",
              "is_similarity": false,
              "is_regex": false,
              "pattern": "required-with-default-comments@example.com",
              "created_at": "Thu, 10 Feb 2022 14:50:22 GMT",
              "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
              "verify_sender": true,
              "is_spoof": true,
              "id": 27571,
              "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
              "last_modified": "Thu, 10 Feb 2022 14:50:22 GMT",
              "is_recent": false,
              "is_recipient": true
      },
      {
```

```
            "is_sender": true,
            "comments": "optional, but helpful",
            "is_similarity": false,
            "is_regex": true,
            "pattern": "required[0-9]{3}@example.com",
            "created_at": "Thu, 10 Feb 2022 14:50:22 GMT",
            "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
            "verify_sender": true,
            "is_spoof": true,
            "id": 27570,
            "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
            "last_modified": "Thu, 10 Feb 2022 14:50:22 GMT",
            "is_recent": false,
            "is_recipient": true
        }
            ]
          }
        },
        "success": true
    },
    "status": 200
}
```


Deleting Allowlist Items

Allowlist items can be deleted by using the DELETE endpoint with the id that is to be deleted. The id can be obtained from either a GET request or the original POST return that created the item.

curl -u service_account_id:private_key -X DELETE https://api.area1security.com/allowlists/<id>

MailConfig Blocklist Endpoint API

This endpoint returns the various Blocklist items that can be configured for the Area 1 Email Protection Service through the Area 1 Portal (*Settings|Block List|Blocked Senders)*.

API Endpoints

https://api.area1security.com/blocklists

Example Request

https://api.area1security.com/blocklists - returns all configured blocklists

MailConfig Blocklist API Response

This shows the result for a request for all blocklists.

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
  "ts": 1638453455,
  "data": [
    {
      "comments": "email",
      "is_regex": false,
      "pattern": "email@example.com",
      "created_at": "Fri, 23 Oct 2020 15:16:35 GMT",
      "id": 20389747904,
      "last_modified": "Mon, 30 Nov 2020 19:15:07 GMT"
    },
    {
      "comments": "regex IPv4",
      "is_regex": true,
      "pattern": "^(192\\.168\\.1\\.[0-9]{1,3})$",
```

```
      "created_at": "Wed, 07 Oct 2020 17:29:39 GMT",
      "id": 47620930942,
      "last_modified": "Wed, 07 Oct 2020 22:59:03 GMT"
    }
  }
}
```

Creating New Blocklist Items

New Blocklist items can be created by sending a properly-formatted JSON body as a POST request to the blocklists endpoint.

curl -u service_account_id:private_key -X POST --data-binary '@/tmp/post.json' https://api.area1security.com/blocklists

Where the file */tmp/post.json* contains json in this format (*pattern* represents an email address and can be a fixed string or a regular expression):

```
{
    "data": [
      {
            "pattern": "required.{0,10}@example.com",
            "comments": "optional, but helpful"
      },
      {
            "pattern": "blockme@example.com"
      }
    ]
}
```

The API return data from that POST, assuming success, will look like this


```
{
  "blackbox": {
      "data": {
          "failures": [],
          "blacklists": [
              {
          "comments": "added by API",
          "is_regex": false,
          "pattern": "blockme@example.com",
          "created_at": "Fri, 11 Feb 2022 18:06:40 GMT",
          "id": 15330,
          "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
          "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
          "last_modified": "Fri, 11 Feb 2022 18:06:40 GMT"
              },
              {
          "comments": "optional, but helpful",
          "is_regex": true,
          "pattern": "required.{0,10}@example.com",
          "created_at": "Fri, 11 Feb 2022 18:06:40 GMT",
          "id": 15329,
          "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
          "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
          "last_modified": "Fri, 11 Feb 2022 18:06:40 GMT"
              }
          ]
      },
      "success": true
  },
  "status": 200
```

```
}
```

Deleting Blocklist Items

Blocklist items can be deleted by using the DELETE endpoint with the id that is to be deleted. The id can be obtained from either a GET request or the original POST return that created the item.

curl -u service_account_id:private_key -X DELETE https://api.area1security.com/blocklists/<id>

MailConfig Domains Endpoint API

This endpoint returns information about customer domains that are configured for the Area 1 Email Protection Service through the Area 1 Portal (Config|Domains & Routing|Domains).

API Endpoints

https://api.area1security.com/domains

Example Request

https://api.area1security.com/domains - returns all configured domain information

MailConfig Domains API Response

This shows the result for a request for all configured domains.

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
  "data": [
      {
      "require_tls_outbound": true,
      "require_tls_inbound": false,
      "drop_dispositions": "{MALICIOUS,MALICIOUS-BEC,SPAM}",
      "domain": "a1s5example.com",
      "id": 1560,
      "lookback_hops": 1,
      "transport": "example.com"
      },
      {
      "require_tls_outbound": true,
      "require_tls_inbound": false,
      "drop_dispositions": "{MALICIOUS,MALICIOUS-BEC,SPAM}",
```

```
      "domain": "a1s4example.com",
      "id": 1559,
      "lookback_hops": 1,
      "transport": "example.com"
      }
  ],
  "success": true,
  "ts": 1639515997
}
```


Creating New Domain Items

New Domains can be created by sending a properly-formatted JSON body as a POST request to the domains endpoint.

curl -u service_account_id:private_key -X POST --data-binary '@/tmp/post.json' https://api.area1security.com/domains

Where the file */tmp/post.json* contains json in this format (using all defaults):


```
{
    "data": [
      {
        "domain": "example.com"
      }
    ]
}
```


The API return data from that POST, assuming success, will look like this

```
{
  "blackbox": {
      "data": {
          "failures": [],
          "blacklists": [
              {
          "proxy_port": -1,
                "require_tls_inbound": false,
                "comments": null,
                "require_tls": false,
                "is_primary": false,
                "drop_dispositions": "{MALICIOUS,MALICIOUS-BEC,SPAM}",
                "created_at": "Fri, 25 Feb 2022 20:59:18 GMT",
                "transport": null,
                "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
                "reject_type": "HARD",
                "require_tls_outbound": false,
                "dmarc_enforcement": "PROMOTE",
                "domain": "example.com",
                "id": 1576,
                "lookback_hops": 1,
                "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
                "o365_tenant_id": null,
                "dmarc_report_enabled": true,
                "last_modified": "Fri, 25 Feb 2022 20:59:18 GMT"
              }
          ]
      },
      "success": true
```

```
  },
  "status": 200
}
```

POST json file overriding default values:

```
{
  "require_tls_outbound": true,
  "require_tls_inbound": true,
  "drop_dispositions": "{MALICIOUS,SPAM}",
  "domain": "example.com",
  "lookback_hops": 1,
  "transport": "google.com"
}
```

Deleting Domain Items

Domain items can be deleted by using the DELETE endpoint with the id that is to be deleted. The id can be obtained from either a GET request or the original POST return that created the item.

curl -u service_account_id:private_key -X DELETE https://api.area1security.com/domains/<id>

MailConfig Domain Restrictions Endpoint API

This endpoint returns information about customer domain restrictions that are configured for the Area 1 Email Protection Service through the Area 1 Portal.

API Endpoints

https://api.area1security.com/domainrestrictions

Example Request

https://api.area1security.com/domainrestrictions - returns all configured domain restriction information

MailConfig Domain Restrictions API Response

This shows the result for a request for all configured domain restrictions.

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
  "data": [
      {
          "domain_id": 1560,
          "domain": "a1s5example.com",
          "restrictions": [
              {
            "comments": "added by API",
            "range": "192.168.51.3/32",
            "created_at": "Mon, 15 Nov 2021 14:39:12 GMT",
            "id": 7634,
            "last_modified": "Mon, 15 Nov 2021 14:39:12 GMT"
              }
          ]
```

```
      },
      {
          "domain_id": 1559,
          "domain": "a1s4example.com",
          "restrictions": [
              {
            "comments": "testing",
            "range": "192.168.61.3/32",
            "created_at": "Tue, 09 Nov 2021 21:15:26 GMT",
            "id": 7631,
            "last_modified": "Thu, 18 Nov 2021 16:19:18 GMT"
            },
            {
          "comments": "added by API",
          "range": "192.168.51.3/32",
          "created_at": "Tue, 09 Nov 2021 20:54:36 GMT",
          "id": 7630,
          "last_modified": "Tue, 09 Nov 2021 20:54:36 GMT"
            }
        ]
      }
  ],
  "ts": 1639517839
}
```


Note that the domain restrictions are associated with the customer's configured domains, and that there can be multiple restrictions on any domain.

Creating New Domain Restrictions

New Blocklist items can be created by sending a properly-formatted JSON body as a POST request to the domainrestrictions endpoint.

curl -u service_account_id:private_key -X POST --data-binary '@/tmp/post.json' https://api.area1security.com/domainrestrictions

Where the file */tmp/post.json* contains json in this format. *domain_id* can be obtained from the */domains* endpoint, and is the domain that you want to apply the restriction to. *range* is a CIDR addresses indicating the IP(s) that should not be allowed to connect to that domain. The POST can contain multiple entries as shown here:

```
{
  "data": [
      {
          "domain_id": 999999,
          "range": "192.168.9.9/32"
      },
      {
          "domain_id": 1560,
          "range": "192.168.5.5/32"
      },
      {
          "domain_id": 1560,
          "range": "192.168.6.6/32",
          "comments": "not required, but helpful"
      }
  ]
}
```

The API return data from that POST, consisting of success and failure for each entry, will look like this, with two successes and one failure (non-existent *domain_id*):

```
{
```

```
  "fail": [],
  "data": [
      {
          "error": "insert or update on table \"customer_domain_restrictions\"
violates foreign key constraint
\"customer_domain_restrictions_domain_id_fkey\"\nDETAIL:  Key
(domain_id)=(999999) is not present in table \"customer_domains\".\n"
      },
      {
          "domain_id": 1560,
          "comments": "added by API",
          "created_at": "Fri, 25 Mar 2022 18:52:47 GMT",
          "range": "192.168.5.5/32",
          "id": 7656,
          "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
          "last_modified": "Fri, 25 Mar 2022 18:52:47 GMT"
      },
      {
          "domain_id": 1560,
          "comments": "not required, but helpful",
          "created_at": "Fri, 25 Mar 2022 18:52:47 GMT",
          "range": "192.168.6.6/32",
          "id": 7657,
          "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
          "last_modified": "Fri, 25 Mar 2022 18:52:47 GMT"
      }
  ],
  "success": [
      "http://localhost:8080/domainrestrictions/7656",
      "http://localhost:8080/domainrestrictions/7657"
  ],
```

```
  "status": 201
}
```

Deleting Domain Restriction

Domain Restrictions can be deleted by using the DELETE endpoint with the id that is to be deleted. The id can be obtained from either a GET request or the original POST return that created the item.

curl -u service_account_id:private_key -X DELETE https://api.area1security.com/domain_restrictions/<id>

MailConfig BEC Endpoint API

This endpoint can return or update information about BEC (Business Email Compromise) that is configured for the Area 1 Email Protection Service through the Area 1 Portal.

API Endpoints

https://api.area1security.com/bec

Example Request

https://api.area1security.com/bec - returns all configured BEC information

MailConfig BEC API Response

This shows the result for a request for all configured BEC entries.

"ts" is the timestamp in epoch seconds of when this api request was made (UTC)


```
{
  "data": [
      "display_names": [
          {
              "comments": null,
              "is_email_regex": false,
              "name": "Robert Smith",
              "created_at": "Thu, 03 Jun 2021 19:56:41 GMT",
              "id": 3350135,
              "last_modified": "Fri, 10 Dec 2021 23:11:09 GMT",
              "email": "bobsmith@example.com"
          },
          {
              "comments": null,
              "is_email_regex": false,
```

```
            "name": "Robert Smith",
            "created_at": "Wed, 02 Jun 2021 16:18:15 GMT",
            "id": 3337861,
            "last_modified": "Wed, 02 Jun 2021 16:18:15 GMT",
            "email": "robert.smith@example.com"
        }
  ],
  "ts": 1639517839
}
```

Creating New BEC Items

New BEC items can be created by sending a properly-formatted JSON body as a POST request to the BEC endpoint.

curl -u service_account_id:private_key -X POST --data-binary '@/tmp/post.json' https://api.area1security.com/bec

Where the file */tmp/post.json* contains json in this format (*pattern* represents an email address and can be a fixed string or a regular expression):

```
{
    "data": [
      {
            "email": "required@example.com",
            "name": "Tim Required",
            "comments": "optional, but helpful"
      },
      {
            "email": "tim.required@example.com",
            "name": "Tim Required"
```

```
        }
    ]
}
```

The API return data from that POST, assuming success, will look like this


```
{
  "blackbox": {
      "data": {
          "failures": [],
          "display_names": {
              "num_pages": null,
              "rows": [
                 {
                     "levenshtein_distance": 1,
                     "comments": "optional, but helpful",
                     "is_email_regex": false,
                     "provenance": "A1S_INTERNAL",
                     "name": "Tim Required",
                     "created_at": "Fri, 11 Mar 2022 14:54:52 GMT",
                     "jarowinkler_distance": 0.98,
                     "id": 6979393,
                     "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
                     "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
                     "last_modified": "Fri, 11 Mar 2022 14:54:52 GMT",
                     "email": "required@example.com"
          },
          {
                     "levenshtein_distance": 1,
                     "comments": "added by API",
```

```
                    "is_email_regex": false,
                    "provenance": "A1S_INTERNAL",
                    "name": "Tim Required",
                    "created_at": "Fri, 11 Mar 2022 14:54:52 GMT",
                    "jarowinkler_distance": 0.98,
                    "id": 6979394,
                    "customer_id": "1b8183fa-15cd-471b-90bb-68fffb575d6f",
                    "deleted_at": "Thu, 01 Jan 1970 00:00:00 GMT",
                    "last_modified": "Fri, 11 Mar 2022 14:54:52 GMT",
                    "email": "tim.required@example.com"
            }
            ]
        },
        "success": true
    },
    "status": 200
}
```


Deleting BEC Items

BEC items can be deleted by using the DELETE endpoint with the id that is to be deleted. The id can be obtained from either a GET request or the original POST return that created the item.

curl -u service_account_id:private_key -X DELETE https://api.area1security.com/bec/<id>