Integration Guide

Stamus Networks API – SOAR Integration Examples

Introduction

This document provides examples of the API endpoints and sample queries that might be used to integrate Stamus NDR (formerly Scirius Security Platform) with a Security Orchestration, Automation, and Response system. The functionality covered in this integration guide includes:

Accessing the HostID data
Retrieving information for a specific host
Queries for NTA/NSM fields (non-hunt/alert based)

Note, this is not an exhaustive set of examples. There are more than 4000 fields/keys available to the integrations.

Table of Contents

HostID Feature

The HostID feature is a Stamus Networks data construct that provides a 360-degree view of a specific host from a network forensics perspective. It tracks, updates, and aggregates the following items and their respective values, first seen, last seen, and when used by that host:

- Hostname
- Usernames (used by SMB/KRB5 for example)
- JA3/JA3S
- HTTP user agents
- SSH user agents
- Roles - server /proxy/printer etc
- Services - ldap/nginx/apache etc
- Alerts generated from the host

HostID RestAPI

There are 3 major RestAPI endpoints that can retrieve information on HostID. They are HostID, HostID Discovery, and HostID Activity. Each are described below:

HostID Endpoints

/rest/appliances/host_id/
/rest/appliances/host_id/<host_ip>/

This endpoint can be either used to retrieve data for all HostID IPs, or for a specific IP.

This is the standard HostID info display as shown in the Hunt section of the UI. Items are grouped exactly as displayed. It will return all findings **REGARDLESS** of the timespan selected.

Examples

Basic Query on HostID

Note: The query will return data for **ALL** HostID IPs on the relevant SSP

```
curl -k https://demo.stamus-networks.com/rest/appliances/host_id/?tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET | jq
```

Example Usage and Query Output

```
curl -k https://demo.stamus-networks.com/rest/appliances/host_id/?tenant\=63 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET | jq

{
  "count": 131129,
  "next": "https://demo.stamus-networks.com/rest/appliances/host_id/?page=2&tenant=63",
  "previous": null,
  "results": [
    {
      "ip": "181.129.140.140",
      "host_id": {
        "first_seen": "2021-12-04T03:44:38.633479+00:00",
        "last_seen": "2021-12-04T03:44:38.633479+00:00",
        "net_info": [
          {
            "agg": "bad_actor.wzywz.bad.bad-users",
            "first_seen": "2021-12-04T03:44:38.633479+00:00",
            "last_seen": "2021-12-04T03:44:38.633479+00:00"
          }
        ],
        "net_info_count": 1,
        "services": [
```

```
      {
        "proto": "tcp",
        "port": 449,
        "values": [
          {
            "first_seen": "2021-12-04T03:44:38.633479+00:00",
            "last_seen": "2021-12-04T03:44:38.633479+00:00",
            "app_proto": "tls",
            "tls": {
              "issuerdn": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd",
              "subject": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd",
              "fingerprint": "9a:03:4b:35:0f:51:73:22:a9:f8:e9:0d:57:74:51:91:08:c4:f2:99",
              "cn": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd"
            }
          }
        ]
      }
    ],
    "services_count": 1,
    "tenant": 63
  }
},
{
  "ip": "162.248.225.57",
  "host_id": {
    "first_seen": "2021-12-04T03:41:06.015676+00:00",
    "last_seen": "2021-12-04T03:41:06.015676+00:00",
    "tenant": 63
  }
},
{
  "ip": "216.58.194.142",
  "host_id": {
    "first_seen": "2021-12-04T04:00:43.710403+00:00",
    "last_seen": "2021-12-04T04:00:43.710403+00:00",
    "hostname": [
      {
        "host": "android.clients.google.com",
        "first_seen": "2021-12-04T04:00:43.710403+00:00",
        "last_seen": "2021-12-04T04:00:43.710403+00:00"
      }
    ],
    "hostname_count": 1,
    "tenant": 63
```

```
    }
   },
   {
    "ip": "172.217.9.161",
    "host_id": {
     "first_seen": "2021-12-04T04:00:43.018093+00:00",
     "last_seen": "2021-12-04T04:00:43.018093+00:00",
     "hostname": [
      {
       "host": "lh3.googleusercontent.com",
       "first_seen": "2021-12-04T04:00:43.018093+00:00",
       "last_seen": "2021-12-04T04:00:43.018093+00:00"
      }
     ],
     "hostname_count": 1,
     "tenant": 63
    }
   },
   {...}
  }
 ]
}
```

Example Response from UI

```
GET /rest/appliances/host_id/?tenant=63
```


```
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "count": 131129,
    "next": "https://demo.stamus-networks.com/rest/appliances/host_id/?page=2&tenant=63",
    "previous": null,
    "results": [
        {
            "ip": "181.129.140.140",
            "host_id": {
                "first_seen": "2021-12-04T03:44:38.633479+00:00",
                "last_seen": "2021-12-04T03:44:38.633479+00:00",
                "net_info": [
                    {
                        "agg": "bad_actor.wzywz.bad.bad-users",
                        "first_seen": "2021-12-04T03:44:38.633479+00:00",
                        "last_seen": "2021-12-04T03:44:38.633479+00:00"
                    }
                ],
                "net_info_count": 1,
                "services": [
                    {
                        "proto": "tcp",
                        "port": 449,
                        "values": [
                            {
                                "first_seen": "2021-12-04T03:44:38.633479+00:00",
                                "last_seen": "2021-12-04T03:44:38.633479+00:00",
                                "app_proto": "tls",
                                "tls": {
                                    "issuerdn": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd",
                                    "subject": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd",
                                    "fingerprint": "9a:03:4b:35:0f:51:73:22:a9:f8:e9:0d:57:74:51:91:08:c4:f2:99",
                                    "cn": "C=AU, ST=Some-State, O=Internet Widgits Pty Ltd"
                                }
                            }
                        ]
                    }
                ],
                "services_count": 1,
                "tenant": 63
            }
        },
        {
            "ip": "162.248.225.57",
            "host_id": {
                "first_seen": "2021-12-04T03:41:06.015676+00:00",
                "last_seen": "2021-12-04T03:41:06.015676+00:00",
                "tenant": 63
            }
        },
        {
            "ip": "216.58.194.142",
            "host_id": {
```


Basic query on HostID for a specific Host IP

Note: The query will return HostID data for a **specified** host IP ONLY

```
curl -k https://<stamus.security.platform.ip>/rest/appliances/host_id/<hostid_ip>?from_date=<timestamp>&to_date=<timestamp>&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k https://demo.stamus-networks.com/rest/appliances/host_id/10.7.5.5?tenant\=63 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET | jq

{
 "ip": "10.7.5.5",
 "host_id": {
  "first_seen": "2021-12-04T03:28:50.710412+00:00",
  "last_seen": "2021-12-04T04:28:56.000329+00:00",
  "net_info": [
   {
    "agg": "winfarm.vmzone.servers.zerotrust.clients",
    "first_seen": "2021-12-04T03:28:50.710412+00:00",
    "last_seen": "2021-12-04T04:28:56.171936+00:00"
   }
  ],
  "hostname": [
   {
    "host": "phantasmedia-dc.phantasmedia.com",
    "first_seen": "2021-12-04T03:28:50.941161+00:00",
    "last_seen": "2021-12-04T03:36:26.941173+00:00"
   }
  ],
  "tls.ja3": [
   {
    "agent": [
     "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.122
Safari/537.36 SE 2.X MetaSr 1.0"
    ],
    "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-10-11,23-24,0",
    "hash": "6734f37431670b3ab4292b8f60f29984",
    "first_seen": "2021-12-04T03:41:52.325784+00:00",
    "last_seen": "2021-12-04T04:16:23.479629+00:00"
   },
   {
    "agent": [
     "User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.0.3705"
    ],
    "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-0-10-11,23-24,0",
    "hash": "1d095e68489d3c535297cd8dffb06cb9",
    "first_seen": "2021-12-04T03:41:54.325784+00:00",
```

```
      "last_seen": "2021-12-04T03:41:54.325784+00:00"
    },
    {
      "agent": [
       "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/78.0.3904.108 Safari/537.36"
      ],
      "string": "771,4866-4867-4865-49199-49195-49200-49196-158-49191-103-49192-107-163-159-52393-
52392-52394-49327-49325-49315-49311-49245-49249-49239-49235-162-49326-49324-49314-49310-49244-
49248-49238-49234-49188-106-49187-64-49162-49172-57-56-49161-49171-51-50-157-49313-49309-49233-
156-49312-49308-49232-61-60-53-47-255,0-11-10-35-22-23-13-43-45-51,29-23-30-25-24,0-1-2",
      "hash": "398430069e0a8ecfbc8db0778d658d77",
      "first_seen": "2021-12-04T04:01:44.710397+00:00",
      "last_seen": "2021-12-04T04:27:10.325785+00:00"
    },
    {
      "agent": [
       "www.niraiya.com  |  Stolen Passwords Checker Bot  |  Macintosh; Intel Mac OS X 10_7_5 (compatible;
niraiya.com/2.0;)  |  We don't share data to 3rd parties : https://www.niraiya.com/privacyandsecurity  |  Report
Us : https://www.niraiya.com/contactus"
      ],
      "string": "771,49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,65281-0-23-35-13-
5-18-16-11-10-27,29-23-24,0",
      "hash": "5353c0796e25725adfdb93f35f5a18f7",
      "first_seen": "2021-12-04T04:28:55.710396+00:00",
      "last_seen": "2021-12-04T04:28:56.171936+00:00"
    },
    {
      "agent": [
       "visual studio code 1.37.0-insider electron 4.2.5 ubuntu 18.04"
      ],
      "string": "771,49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,65281-0-23-35-13-
5-18-16-30032-11-10-27,29-23-24,0",
      "hash": "717217c022d59183bfde190cd3ff072f",
      "first_seen": "2021-12-04T04:28:58.479667+00:00",
      "last_seen": "2021-12-04T04:28:58.479667+00:00"
    }
  ],
  "http.user_agent": [
    {
      "agent": "test",
      "first_seen": "2021-12-04T03:44:47.864245+00:00",
      "last_seen": "2021-12-04T03:47:03.402716+00:00"
    },
```

```
    {
      "agent": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727;
SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E)",
      "first_seen": "2021-12-04T03:44:55.402700+00:00",
      "last_seen": "2021-12-04T03:44:55.402700+00:00"
    },
    {
      "agent": "WinHTTP sender/1.0",
      "first_seen": "2021-12-04T03:46:39.556551+00:00",
      "last_seen": "2021-12-04T03:46:39.556551+00:00"
    },
    {
      "agent": "WinHTTP loader/1.0",
      "first_seen": "2021-12-04T03:47:28.095016+00:00",
      "last_seen": "2021-12-04T03:48:00.248866+00:00"
    },
    {
      "agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
      "first_seen": "2021-12-04T04:05:34.402698+00:00",
      "last_seen": "2021-12-04T04:28:46.710409+00:00"
    }
  ],
  "net_info_count": 1,
  "hostname_count": 1,
  "tls.ja3_count": 5,
  "http.user_agent_count": 5,
  "services": [
    {
      "proto": "tcp",
      "port": 88,
      "values": [
        {
          "first_seen": "2021-12-04T03:28:58.004561+0000",
          "last_seen": "2021-12-04T03:29:42.000623+0000",
          "app_proto": "krb5"
        }
      ]
    },
    {
      "proto": "tcp",
      "port": 135,
      "values": [
        {
          "first_seen": "2021-12-04T03:30:28.000129+0000",
```

```
      "last_seen": "2021-12-04T04:13:33.081058+0000",
      "app_proto": "dcerpc"
    }
   ]
  },
  {
   "proto": "tcp",
   "port": 389,
   "values": [
    {
     "first_seen": "2021-12-04T03:29:04.004295+0000",
     "last_seen": "2021-12-04T03:43:18.000515+0000",
     "app_proto": "unknown"
    }
   ]
  },
  {
   "proto": "tcp",
   "port": 445,
   "values": [
    {
     "first_seen": "2021-12-04T03:29:32.000175+0000",
     "last_seen": "2021-12-04T04:13:34.004197+0000",
     "app_proto": "smb"
    },
    {
     "first_seen": "2021-12-04T03:36:52.008238+0000",
     "last_seen": "2021-12-04T04:13:33.093365+0000",
     "app_proto": "unknown"
    }
   ]
  },
  {
   "proto": "tcp",
   "port": 3268,
   "values": [
    {
     "first_seen": "2021-12-04T03:36:13.001016+0000",
     "last_seen": "2021-12-04T04:13:33.094466+0000",
     "app_proto": "unknown"
    }
   ]
  },
  {
```

```
      "proto": "tcp",
      "port": 49155,
      "values": [
       {
        "first_seen": "2021-12-04T03:30:28.000269+0000",
        "last_seen": "2021-12-04T04:04:29.000426+0000",
        "app_proto": "dcerpc"
       }
      ]
     },
     {
      "proto": "tcp",
      "port": 49158,
      "values": [
       {
        "first_seen": "2021-12-04T03:29:44.001691+0000",
        "last_seen": "2021-12-04T03:37:00.000551+0000",
        "app_proto": "dcerpc"
       }
      ]
     }
    ],
    "services_count": 8,
    "tenant": 63
   }
}
```


Example Query from UI - HostID for a specific Host IP

```
https://stamus.security.platform.ip/rest/appliances/host_id/10.7.5.5?tenant=63
```

Example Response from UI - HostID for a specific Host IP

```
GET /rest/appliances/host_id/10.7.5.5?tenant=63
```

```
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "ip": "10.7.5.5",
    "host_id": {
        "first_seen": "2021-12-04T03:28:50.710412+00:00",
        "last_seen": "2021-12-04T04:28:56.000329+00:00",
        "net_info": [
            {
                "agg": "winfarm.vmzone.servers.zerotrust.clients",
                "first_seen": "2021-12-04T03:28:50.710412+00:00",
                "last_seen": "2021-12-04T04:28:56.171936+00:00"
            }
        ],
        "hostname": [
            {
                "host": "phantasmedia-dc.phantasmedia.com",
                "first_seen": "2021-12-04T03:28:50.941161+00:00",
                "last_seen": "2021-12-04T03:36:26.941173+00:00"
            }
        ],
        "tls.ja3": [
            {
                "agent": [
                    "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0"
                ],
                "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-10-11,23-24,0",
                "hash": "6734f37431670b3ab4292b8f60f29984",
                "first_seen": "2021-12-04T03:41:52.325784+00:00",
                "last_seen": "2021-12-04T04:16:23.479629+00:00"
            },
            {
                "agent": [
                    "User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.0.3705"
                ],
                "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-4,65281-0-10-11,23-24,0",
                "hash": "1d095e68489d3c535297cd8dffb06cb9",
                "first_seen": "2021-12-04T03:41:54.325784+00:00",
                "last_seen": "2021-12-04T03:41:54.325784+00:00"
            },
            {
                "agent": [
                    "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/78.0.3904.108 Safari/537.36"
                ],
                "string": "771,4866-4867-4865-49199-49195-49200-49196-158-49191-103-49192-107-163-159-52393-52392-52394-49327-49325-49315-49311-49245-49249-4
                "hash": "398430069e0a8ecfbc8db0778d658d77",
                "first_seen": "2021-12-04T04:01:44.710397+00:00",
                "last_seen": "2021-12-04T04:27:10.325785+00:00"
            },
            {
```

HostID Discovery Endpoints

/rest/appliances/host_id_extra_info/
/rest/appliances/host_id_extra_info/<host_ip>/

This returns a flat structure - not grouped - and presents the same data as in the HostID display page, sorted by timestamp (first seen). It is easier to pick out specific fields - such as user-agent or a TLS JA3 - making it very very useful for SEIMs/SOARs too. It will return all findings for the timespan selected.

Use case: find/list all newly discovered user agents (and/or hostnames/JA3/JA3S/SSH agents/Services/Usernames/Roles) seen on that IP for the last 24hrs.

This endpoint lists **additional information** for hosts **inside** the given range of time - for **IPs/key fields** (services/user agents, etc.)

Examples

Basic query on HostID Discovery

Note: The query will return discovery data for **ALL** HostID IPs on the relevant SSP

```
curl -k
https://<stamus.security.platform.ip>/rest/appliances/host_id_extra_info/
?from_date=<timestamp>&to_date=<timestamp>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl - k
https://stamus.security.platform.ip/rest/appliances/host_id_extra_info/\?from_dat
e\=1634380250255\&to_date\=1636972250255\&tenant\=63 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X
GET

{
   "count": 21,
   "next": null,
   "previous": null,
   "results": [
       {
           "host": "phantasmedia-dc.phantasmedia.com",
           "first_seen": "2021-11-22T06:56:54.405241+00:00",
```

```
            "last_seen": "2021-11-22T11:30:47.825058+00:00",
            "type": "hostname",
            "value": "phantasmedia-dc.phantasmedia.com",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:02.008034+0000",
            "last_seen": "2021-11-22T11:24:04.000077+0000",
            "app_proto": "krb5",
            "type": "services",
            "proto": "tcp",
            "port": 88,
            "value": "tcp:88",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:09.000075+0000",
            "last_seen": "2021-11-22T11:37:39.015577+0000",
            "app_proto": "unknown",
            "type": "services",
            "proto": "tcp",
            "port": 389,
            "value": "tcp:389",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:35.001790+0000",
            "last_seen": "2021-11-22T12:07:54.003827+0000",
            "app_proto": "smb",
            "type": "services",
            "proto": "tcp",
            "port": 445,
            "value": "tcp:445",
            "ip": "10.7.5.5"
        },
{
            ...
        }]
    }
```

Example Query from UI

```
https://stamus.security.platform.ip/rest/appliances/host_id_extra_info/?from_date=1634380250255&to_date=1636972250255&tenant=63
```

Example Response from UI

```
GET /rest/appliances/host_id_extra_info/?from_date=1637501738000&to_date=163758813800000&tenant=63

HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "count": 21,
    "next": null,
    "previous": null,
    "results": [
        {
            "host": "phantasmedia-dc.phantasmedia.com",
            "first_seen": "2021-11-22T06:56:54.405241+00:00",
            "last_seen": "2021-11-22T11:30:47.825058+00:00",
            "type": "hostname",
            "value": "phantasmedia-dc.phantasmedia.com",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:02.008034+0000",
            "last_seen": "2021-11-22T11:24:04.000077+0000",
            "app_proto": "krb5",
            "type": "services",
            "proto": "tcp",
            "port": 88,
            "value": "tcp:88",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:09.000075+0000",
            "last_seen": "2021-11-22T11:37:39.015577+0000",
            "app_proto": "unknown",
            "type": "services",
            "proto": "tcp",
            "port": 389,
            "value": "tcp:389",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:35.001790+0000",
            "last_seen": "2021-11-22T12:07:54.003827+0000",
            "app_proto": "smb",
            "type": "services",
            "proto": "tcp",
            "port": 445,
            "value": "tcp:445",
            "ip": "10.7.5.5"
        },
        {
```

Basic query on HostID Discovery for a specific Host IP

Note: The query will return discovery data for a **specified** HostID IP only

```
curl -k
https://stamus.security.platform.ip/rest/appliances/host_id_extra_info/<h
ost_id_ip>?from_date=<timestamp>&to_date=<timestamp>&tenant=<tenand_id> -
H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET
```

NOTE: *<tenant>* param should not be used if multi tenancy is not enabled (this is valid for all the examples described in this integration guide)

Example Usage and Query Output

```
curl - k
https://stamus.security.platform.ip/rest/appliances/host_id_extra_info/10.7.5.5\?
from_date\=1634380250255\&to_date\=1636972250255\&tenant\=63 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET
   [{
       "host": "phantasmedia-dc.phantasmedia.com",
       "first_seen": "2021-11-22T06:56:54.405241+00:00",
       "last_seen": "2021-11-22T11:30:47.825058+00:00",
       "type": "hostname",
       "value": "phantasmedia-dc.phantasmedia.com"
   },
   {
       "first_seen": "2021-11-22T06:57:02.008034+0000",
       "last_seen": "2021-11-22T11:24:04.000077+0000",
       "app_proto": "krb5",
       "type": "services",
       "proto": "tcp",
       "port": 88,
       "value": "tcp:88"
   },
   {
       "first_seen": "2021-11-22T06:57:09.000075+0000",
       "last_seen": "2021-11-22T11:37:39.015577+0000",
       "app_proto": "unknown",
       "type": "services",
       "proto": "tcp",
       "port": 389,
```

```
        "value": "tcp:389"
    },
    {
        "first_seen": "2021-11-22T06:57:35.001790+0000",
        "last_seen": "2021-11-22T12:07:54.003827+0000",
        "app_proto": "smb",
        "type": "services",
        "proto": "tcp",
        "port": 445,
        "value": "tcp:445"
    },
    {
        "first_seen": "2021-11-22T06:57:48.001138+0000",
        "last_seen": "2021-11-22T11:31:21.000258+0000",
        "app_proto": "dcerpc",
        "type": "services",
        "proto": "tcp",
        "port": 49158,
        "value": "tcp:49158"
    }, {
          ...
     }]
```


Example Query from UI - HostID Discovery for a specific Host IP

```
https://stamus.security.platform.ip/rest/appliances/host_id_extra_
info/<host_id_ip>?from_date=<timestamp>&to_date=<timestamp>&tenant
=<tenant_id>
```

Example Response from UI - HostID Discovery for a specific Host IP

```
GET /rest/appliances/host_id_extra_info/10.7.5.5?from_date=1637501738000&to_date=16375881380000&tenant=63
```

```
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept
```


```
[
    {
        "host": "phantasmedia-dc.phantasmedia.com",
        "first_seen": "2021-11-22T06:56:54.405241+00:00",
        "last_seen": "2021-11-22T11:30:47.825058+00:00",
        "type": "hostname",
        "value": "phantasmedia-dc.phantasmedia.com"
    },
    {
        "first_seen": "2021-11-22T06:57:02.008034+0000",
        "last_seen": "2021-11-22T11:24:04.000077+0000",
        "app_proto": "krb5",
        "type": "services",
        "proto": "tcp",
        "port": 88,
        "value": "tcp:88"
    },
    {
        "first_seen": "2021-11-22T06:57:09.000075+0000",
        "last_seen": "2021-11-22T11:37:39.015577+0000",
        "app_proto": "unknown",
        "type": "services",
        "proto": "tcp",
        "port": 389,
        "value": "tcp:389"
    },
    {
        "first_seen": "2021-11-22T06:57:35.001790+0000",
        "last_seen": "2021-11-22T12:07:54.003827+0000",
        "app_proto": "smb",
        "type": "services",
        "proto": "tcp",
        "port": 445,
        "value": "tcp:445"
    },
    {
        "first_seen": "2021-11-22T06:57:48.001138+0000",
        "last_seen": "2021-11-22T11:31:21.000258+0000",
        "app_proto": "dcerpc",
        "type": "services",
        "proto": "tcp",
        "port": 49158,
        "value": "tcp:49158"
    },
```

HostID Activity Endpoint

/rest/appliances/host_id_activity/

This returns the recently active HostID information - that was seen active during the timespan selected.

NOTE: Currently, the HostID Activity endpoint supports filtering only on *<start_date>*, *<end_date>* and *<tenant>*. However, */rest/appliances/host_id/<host_id_ip>* endpoint will return the information on the specified host's activity as well.

Use case: Find all active user agents (and/or hostnames/JA3/JA3S/SSH agents/Services/Usernames/Roles) seen for last 24hrs

This endpoint lists **all recently active IPs/key fields** that were seen active **during the timespan selected**.

Examples

Basic query with curl on HostID Activity

Note: The query will return activity data for **ALL** HostID IPs on the relevant SSP

```
curl -k
https://stamus.security.platform.ip/rest/appliances/host_id_activity//?from_date=<timestamp>&
to_date=<timestamp>&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl - k
https://stamus.security.platform.ip/rest/appliances/host_id_activity/\?from_date\
=1634380250255\&to_date\=1636972250255\&tenant\=63 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X
GET
 {
   "count": 21,
   "next": null,
   "previous": null,
   "results": [{
               "host": "phantasmedia-dc.phantasmedia.com",
               "first_seen": "2021-11-22T06:56:54.405241+00:00",
```

```
            "last_seen": "2021-11-22T11:30:47.825058+00:00",
            "type": "hostname",
            "value": "phantasmedia-dc.phantasmedia.com",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:02.008034+0000",
            "last_seen": "2021-11-22T11:24:04.000077+0000",
            "app_proto": "krb5",
            "type": "services",
            "proto": "tcp",
            "port": 88,
            "value": "tcp:88",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:09.000075+0000",
            "last_seen": "2021-11-22T11:37:39.015577+0000",
            "app_proto": "unknown",
            "type": "services",
            "proto": "tcp",
            "port": 389,
            "value": "tcp:389",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:35.001790+0000",
            "last_seen": "2021-11-22T12:07:54.003827+0000",
            "app_proto": "smb",
            "type": "services",
            "proto": "tcp",
            "port": 445,
            "value": "tcp:445",
            "ip": "10.7.5.5"
        },
        {

            ...
    }]
}
```

Example Query from UI

```
https://stamus.security.platform.ip/rest/appliances/host_id_activity/?from_date=<timestamp>&to_date=<timestamp>&tenant=<tenant_id>
```

Example Response from UI

```
GET /rest/appliances/host_id_activity/?from_date=1637501738000&to_date=16375881380000&tenant=63
```

```
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "count": 21,
    "next": null,
    "previous": null,
    "results": [
        {
            "host": "phantasmedia-dc.phantasmedia.com",
            "first_seen": "2021-11-22T06:56:54.405241+00:00",
            "last_seen": "2021-11-22T11:30:47.825058+00:00",
            "type": "hostname",
            "value": "phantasmedia-dc.phantasmedia.com",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:02.008034+0000",
            "last_seen": "2021-11-22T11:24:04.000077+0000",
            "app_proto": "krb5",
            "type": "services",
            "proto": "tcp",
            "port": 88,
            "value": "tcp:88",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:09.000075+0000",
            "last_seen": "2021-11-22T11:37:39.015577+0000",
            "app_proto": "unknown",
            "type": "services",
            "proto": "tcp",
            "port": 389,
            "value": "tcp:389",
            "ip": "10.7.5.5"
        },
        {
            "first_seen": "2021-11-22T06:57:35.001790+0000",
            "last_seen": "2021-11-22T12:07:54.003827+0000",
            "app_proto": "smb",
            "type": "services",
            "proto": "tcp",
            "port": 445,
            "value": "tcp:445",
            "ip": "10.7.5.5"
        },
        {
```

HostID Python

Examples

HostID Python Requests example code

```
# importing the requests and json libraries
import requests
import json
 # api-endpoint
URL =
"https://stamus.security.platform.ip/rest/appliances/host_id/1.2.163.123"
 # defining a params dict for the parameters to be sent to the API
TOKEN = "<token>"
PARAMS = {"tenant": 63} # parameter only needed when multi tenancy is enabled
AUTH = {"Content Type": "application/json", "Authorization": "Token " + TOKEN
}

# sending get request and saving the response as response object
r = requests.get(url = URL, headers=AUTH, params = PARAMS)
 # extracting data in json format
data = r.json()
 # printing the output of the 10th result
print(json.dumps(data, indent=2))
```

HostID Command line execution

```
$ python3 host.py
```

HostID Response body

```
{
   "ip": "1.2.163.123",
   "host_id": {
     "first_seen": "2021-12-06T06:42:12.002111+00:00",
     "last_seen": "2021-12-06T10:14:11.047509+00:00",
     "hostname": [
       {
```

```
      "host": "www.server-102a37b.cn",
      "first_seen": "2021-12-06T07:59:52.406486+00:00",
      "last_seen": "2021-12-06T07:59:52.406486+00:00"
    }
  ],
  "hostname_count": 1,
  "services": [
    {
      "proto": "tcp",
      "port": 80,
      "values": [
        {
          "first_seen": "2021-12-06T08:05:58.000509+0000",
          "last_seen": "2021-12-06T08:05:58.000509+0000",
          "app_proto": "unknown"
        }
      ]
    },
    {
      "proto": "tcp",
      "port": 443,
      "values": [
        {
          "app_proto": "unknown",
          "last_seen": "2021-12-06T06:42:12.002111+0000",
          "first_seen": "2021-12-06T06:42:12.002111+0000"
        }
      ]
    },
    {
      "proto": "tcp",
      "port": 6780,
      "values": [
        {
          "first_seen": "2021-12-06T08:40:36.001877+0000",
          "last_seen": "2021-12-06T08:40:36.001877+0000",
          "app_proto": "unknown"
        }
      ]
    },
```

```
      {
        "proto": "tcp",
        "port": 20000,
        "values": [
          {

            "first_seen": "2021-12-06T09:01:39.009940+0000",
            "last_seen": "2021-12-06T09:01:39.009940+0000",
            "app_proto": "dnp3"
          }
        ]
      },
      {
        "proto": "tcp",
        "port": 43750,
        "values": [
          {
            "first_seen": "2021-12-06T08:43:52.036962+0000",
            "last_seen": "2021-12-06T08:43:52.036962+0000",
            "app_proto": "unknown"
          }
        ]
      }
    ],
    "services_count": 5,
    "tenant": 63
  }
}
```


Examples

HostID Discovery Python Requests example code

```
# importing the requests and json libraries
import requests
import json
 # api-endpoint
```

```
URL =
"https://stamus.security.platform.ip/rest/appliances/host_id_extra_info/1.2.1
63.123"

# defining a params dict for the parameters to be sent to the API
TOKEN = "<token>"
PARAMS = {"tenant": 63} # parameter only needed when multi tenancy is enabled
AUTH = {"Content Type": "application/json", "Authorization": "Token " + TOKEN
}

# sending get request and saving the response as response object
r = requests.get(url = URL, headers=AUTH, params = PARAMS)
 # extracting data in json format
data = r.json()
 # printing the output of the 10th result
print(json.dumps(data, indent=2))
```

HostID Discovery Command line execution

```
$ python3 host_id_discovery.py
```

HostID Discovery Response body


```
[
 {
   "app_proto": "unknown",
   "last_seen": "2021-12-06T06:42:12.002111+0000",
   "first_seen": "2021-12-06T06:42:12.002111+0000",
   "type": "services",
   "proto": "tcp",
   "port": 443,
   "value": "tcp:443"
 },
 {
   "host": "www.server-102a37b.cn",
   "first_seen": "2021-12-06T07:59:52.406486+00:00",
   "last_seen": "2021-12-06T07:59:52.406486+00:00",
   "type": "hostname",
   "value": "www.server-102a37b.cn"
```

```
  },
  {
    "first_seen": "2021-12-06T08:05:58.000509+0000",
    "last_seen": "2021-12-06T08:05:58.000509+0000",
    "app_proto": "unknown",
    "type": "services",
    "proto": "tcp",
    "port": 80,
    "value": "tcp:80"
  },
  {
    "first_seen": "2021-12-06T08:40:36.001877+0000",
    "last_seen": "2021-12-06T08:40:36.001877+0000",
    "app_proto": "unknown",
    "type": "services",
    "proto": "tcp",
    "port": 6780,
    "value": "tcp:6780"
  },
  {
    "first_seen": "2021-12-06T08:43:52.036962+0000",
    "last_seen": "2021-12-06T08:43:52.036962+0000",
    "app_proto": "unknown",
    "type": "services",
    "proto": "tcp",
    "port": 43750,
    "value": "tcp:43750"
  },
  {
    "first_seen": "2021-12-06T09:01:39.009940+0000",
    "last_seen": "2021-12-06T09:01:39.009940+0000",
    "app_proto": "dnp3",
    "type": "services",
    "proto": "tcp",
    "port": 20000,
    "value": "tcp:20000"
  }
]
```

Examples

HostID Activity Python Requests example code

```
# importing the requests and json libraries
import requests
import json
 # api-endpoint
URL = "https://stamus.security.platform.ip/rest/appliances/host_id_activity/"
 # defining a params dict for the parameters to be sent to the API
TOKEN = "<token>"
PARAMS = {"tenant": 63} # parameter only needed when multi tenancy is enabled

AUTH = {"Content Type": "application/json", "Authorization": "Token " + TOKEN
}

# sending get request and saving the response as response object
r = requests.get(url = URL, headers=AUTH, params = PARAMS)
 # extracting data in json format
data = r.json()
 # printing the output of the 10th result
print(json.dumps(data, indent=2))
```

HostID Activity Command line execution

```
$ python3 host_id_discovery.py
```

HostID Activity Response body


```
{
   "count": 23,
   "next": null,
   "previous": null,
   "results": [
     {
       "user": "pfmfzzj",
       "first_seen": "2021-12-05T14:26:59.543344+00:00",
       "last_seen": "2021-12-06T06:49:26.063160+00:00",
       "type": "username",
```

```
    "value": "pfmfzzj",
    "ip": "1.1.182.9"
  },
  {
    "host": "bkruukxs3",
    "first_seen": "2021-12-05T14:26:59.543344+00:00",
    "last_seen": "2021-12-06T06:49:26.063160+00:00",
    "type": "hostname",
    "value": "bkruukxs3",
    "ip": "1.1.182.9"
  },
  {
    "host": "vistacli",
    "first_seen": "2021-12-05T14:27:21.100013+00:00",
    "last_seen": "2021-12-06T06:49:47.619818+00:00",
    "type": "hostname",
    "value": "vistacli",
    "ip": "1.1.107.177"
  },
  {
    "user": "winuser",
    "first_seen": "2021-12-05T14:27:21.100013+00:00",
    "last_seen": "2021-12-06T06:49:47.619818+00:00",
    "type": "username",
    "value": "winuser",
    "ip": "1.1.107.177"
  },
  {
    "user": "ybhemrocmvc",
    "first_seen": "2021-12-05T14:43:06.413347+00:00",
    "last_seen": "2021-12-06T07:05:32.933154+00:00",
    "type": "username",
    "value": "ybhemrocmvc",
    "ip": "1.1.160.67"
  },
  {
    "host": "uktic5",
    "first_seen": "2021-12-05T14:43:06.413347+00:00",
    "last_seen": "2021-12-06T07:05:32.933154+00:00",
    "type": "hostname",
    "value": "uktic5",
    "ip": "1.1.160.67"
```

```
    },
    {
      "user": "e9l0yuk",
      "first_seen": "2021-12-05T14:52:48.023348+00:00",
      "last_seen": "2021-12-06T07:15:14.543151+00:00",
      "type": "username",
      "value": "e9l0yuk",
      "ip": "1.1.48.141"
    },
    {
      "host": "ynt6nde4lko",
      "first_seen": "2021-12-05T14:52:48.023348+00:00",
      "last_seen": "2021-12-06T07:15:14.543151+00:00",
      "type": "hostname",
      "value": "ynt6nde4lko",
      "ip": "1.1.48.141"
    },
    {
      "agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2)
AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.6 Safari/537.11",
      "first_seen": "2021-12-05T15:24:55.970011+00:00",
      "last_seen": "2021-12-06T07:47:22.489818+00:00",
      "type": "http.user_agent",
      "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2)
AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.6 Safari/537.11",
      "ip": "1.1.20.25"
    },
    {
      "host": "client-1016bb1",
      "first_seen": "2021-12-05T16:03:52.093349+00:00",
      "last_seen": "2021-12-06T08:26:18.613153+00:00",
      "type": "hostname",
      "value": "client-1016bb1",
      "ip": "1.1.107.177"
    },
    {
      "agent": "Generic 1.x",
      "first_seen": "2021-12-05T16:11:46.008171+00:00",
      "last_seen": "2021-12-06T08:34:13.006673+00:00",
      "type": "http.user_agent",
      "value": "Generic 1.x",
      "ip": "1.1.107.177"
```

```
  },
  {
    "host": "vistacli",
    "first_seen": "2021-12-05T17:00:12.876682+00:00",
    "last_seen": "2021-12-06T09:22:39.396484+00:00",
    "type": "hostname",
    "value": "vistacli",
    "ip": "1.1.20.25"
  },
  {
    "user": "winuser",
    "first_seen": "2021-12-05T17:00:12.876682+00:00",
    "last_seen": "2021-12-06T09:22:39.396484+00:00",
    "type": "username",
    "value": "winuser",
    "ip": "1.1.20.25"
  },
  {
    "user": "winuser",
    "first_seen": "2021-12-05T17:06:08.013367+00:00",
    "last_seen": "2021-12-06T09:28:34.533159+00:00",
    "type": "username",
    "value": "winuser",
    "ip": "1.1.205.137"
  },
  {
    "host": "vistacli",
    "first_seen": "2021-12-05T17:06:08.013367+00:00",
    "last_seen": "2021-12-06T09:28:34.533159+00:00",
    "type": "hostname",
    "value": "vistacli",
    "ip": "1.1.205.137"
  },
  {
    "user": "winuser",
    "first_seen": "2021-12-05T17:06:12.273357+00:00",
    "last_seen": "2021-12-06T09:28:38.793162+00:00",
    "type": "username",
    "value": "winuser",
    "ip": "1.1.151.27"
  },
  {
```

```
    "host": "vistacli",
    "first_seen": "2021-12-05T17:06:12.273357+00:00",
    "last_seen": "2021-12-06T09:28:38.793162+00:00",
    "type": "hostname",
    "value": "vistacli",
    "ip": "1.1.151.27"
  },
  {
    "user": "winuser",
    "first_seen": "2021-12-05T17:13:24.580023+00:00",
    "last_seen": "2021-12-06T09:35:51.099831+00:00",
    "type": "username",
    "value": "winuser",
    "ip": "1.1.24.163"
  },
  {
    "host": "vistacli",
    "first_seen": "2021-12-05T17:13:24.580023+00:00",
    "last_seen": "2021-12-06T09:35:51.099831+00:00",
    "type": "hostname",
    "value": "vistacli",
    "ip": "1.1.24.163"
  },
  {
    "first_seen": "2021-12-05T17:32:59.606678+0000",
    "app_proto": "http",
    "last_seen": "2021-12-06T09:55:26.126483+0000",
    "type": "services",
    "proto": "tcp",
    "port": 80,
    "value": "tcp:80",
    "ip": "1.1.75.230"
  },
  {
    "host": "replica2.example.com",
    "first_seen": "2021-12-05T17:32:59.606678+00:00",
    "last_seen": "2021-12-06T09:55:26.126483+00:00",
    "type": "hostname",
    "value": "replica2.example.com",
    "ip": "1.1.75.230"
  },
  {
```

```
      "first_seen": "2021-12-05T17:45:41.720011+0000",
      "app_proto": "http",
      "last_seen": "2021-12-06T10:08:08.756485+0000",
      "type": "services",
      "proto": "tcp",
      "port": 80,
      "value": "tcp:80",
      "ip": "1.1.134.39"
    },
    {
      "host": "replica1.example.com",
      "first_seen": "2021-12-05T17:45:41.720011+00:00",
      "last_seen": "2021-12-06T10:08:08.756485+00:00",
      "type": "hostname",
      "value": "replica1.example.com",
      "ip": "1.1.134.39"
    }
  ]
}
```

Retrieve Information for a Specific Host

NOTE #1: *<tenant_id>* parameter should be used, only if multi-tenancy is enabled on the SSP. Listed below are examples with and without a tenant parameter.

NOTE #2: You can also optionally set ***<start_date>*** and ***<end_date>*** to specify a time range for your queries. Start/end dates are given in **unix timestamp format**.

Example

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=<f
ield>&from_date=1637662856188&to_date=1637749256188&tenant=<tenant_id>&qf
ilter=<src_ip>:<ip_value> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

The following list contains the basic Rest API query (under **Basic Query** section), as well as example queries with the optional parameters ***<start_date>***, ***<end_date>*** and ***<tenant_id>*** and their relevant console outputs. The **Basic Query** shows the api endpoint for field stats per field, as well as a qfilter - it could filter either per src_ip, dest_ip, alert.source_ip, alert.dest_ip or any other field, depending on the needed information.

The examples, under **Example Usage**, contain different fields, as well as the optional parameters like <start_date> and <end_date> to set a time range for the query and <tenant_id> - in case multi-tenancy is enabled on your SSP.

The queries are listed, according to the information they provide for the desired field/qfilter combination.

NOTE #3: A **<token>** is mandatory for each query. It can be found on your SSP, under Account Settings -> Edit token, or directly under: https://stamus.security.platform.ip/accounts/edit/token

Example Queries

Query Structure

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=<f
ield>&qfilter=<filter_field>:"<ip>" -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

alert.metadata.affected_product

Basic query on alert.metadata.affected_product for a particular alert.source.ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=al
ert.metadata.affected_product&qfilter=alert.source.ip:"<ip>" -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.metadata.affected_product\&from_date\=1637662856188\&to_date\=16377
49256188\&tenant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.metadata.affected_product": [{
     "key": "Windows_XP_Vista_7_8_10_Server_32_64_Bit",
     "doc_count": 964
   }, {
     "key": "Any",
     "doc_count": 4
   }]
}
```

alert.metadata.attack_target

Basic query on alert.metadata.attack_target for a particular src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=al
ert.metadata.attack_target&qfilter=src_ip:"<ip>" -H 'Authorization: Token
<token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.metadata.attack_target\&from_date\=1637662856188\&to_date\=16377492
56188\&tenant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.metadata.attack_target": [{
     "key": "Client_Endpoint",
     "doc_count": 954
   }, {
     "key": "Client_and_Server",
     "doc_count": 2
   }]
}
```

alert.metadata.malware_family

Basic query on alert.metadata.malware_family for a particular src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=al
ert.metadata.malware_family&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.metadata.malware_family\&from_date\=1637662856188\&to_date\=1637749
256188\&tenant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.metadata.malware_family": [{
     "key": "Cobalt_Strike",
     "doc_count": 928
   }, {
     "key": "AnchorTrickBot",
     "doc_count": 7
   }, {
     "key": "BazaLoader",
     "doc_count": 6
   }]
}
```

alert.metadata.mitre_tactic_id

Basic query on alert.metadata.mitre_tactic_id for src_ip or dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=al
ert.metadata.mitre_tactic_id&qfilter=(src_ip:<ip>ORdest_ip<ip>) -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.metadata.mitre_tactic_id\&qfilter\=\(src_ip%3A%22192.168.5.125%22%2
0OR%20dest_ip%3A%22192.168.5.125%22\) -H 'Authorization: Token
```

```
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.metadata.mitre_tactic_id": [{
     "key": "TA0011",
     "doc_count": 14
   }]
}
```

alert.metadata.mitre_tactic_name

Basic query on alert.metadata.mitre_tactic_name for src_ip or dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/?fields=al
ert.metadata.mitre_tactic_name&qfilter=(src_ip:<ip>ORdest_ip<ip>) -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.metadata.mitre_tactic_name\&qfilter\=\(src_ip%3A%22192.168.5.125%22
%20OR%20dest_ip%3A%22192.168.5.125%22\) -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET


{
   "alert.metadata.mitre_tactic_name": [{
       "key": "Command_And_Control",
       "doc_count": 14
   }]
}
```

alert.metadata.mitre_technique_name

Basic query on alert.metadata.mitre_technique_name for src_ip or dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.metadata.mitre_technique_name&qfilter=(src_ip:<ip>ORdest_ip<ip>) -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.metadata.mitre_technique_name\&qfilter\=\(src_ip%3A%22192.168.5.125
%22%20OR%20dest_ip%3A%22192.168.5.125%22\) -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.metadata.mitre_technique_id": [{
       "key": "T1071",
       "doc_count": 14
   }]
}
```

alert.metadata.mitre_tactic_name

Basic query on alert.metadata.mitre_tactic_name for a src_ip or dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.metadata.mitre_tactic_name&qfilter=(src_ip:<ip>ORdest_ip<ip>) -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
```

```
alert.metadata.mitre_tactic_name\&qfilter\=\(src_ip%3A%22192.168.5.125%22
%20OR%20dest_ip%3A%22192.168.5.125%22\) -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.metadata.mitre_technique_name": [{
       "key": "Application_Layer_Protocol",
       "doc_count": 14
   }]
}
```

alert.signature

Basic query on alert.signature for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.signature&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.signature\&from_date\=1637662856188\&to_date\=1637749256188\&tenant
\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.signature": [{
       "key": "ET MALWARE Cobalt Strike Malleable C2 (OneDrive)",
       "doc_count": 928
   }, {
       "key": "ET MALWARE Anchor_DNS stickseed Variant CnC Checkin",
       "doc_count": 14
   }, {
       "key": "ET MALWARE Win32/TrickBot Anchor Variant Style External IP
Check",
```

```
        "doc_count": 7
    }, {
        "key": "ETPRO HUNTING Suspicious User-Agent containing Loader
Observed",
        "doc_count": 7
    }, {
        "key": "ETPRO POLICY External IP Check (checkip.amazonaws.com)",
        "doc_count": 7
    }, {
        "key": "ETPRO MALWARE BazaLoader MalDoc CnC Checkin",
        "doc_count": 4
    }, {
        "key": "ET RPC DCERPC SVCCTL - Remote Service Control Manager
Access",
        "doc_count": 2
    }, {
        "key": "ET USER_AGENTS Suspicious User-Agent (contains loader)",
        "doc_count": 2
    }, {
        "key": "ETPRO HUNTING Suspicious POST to .exe Without Referer",
        "doc_count": 2
    }, {
        "key": "ETPRO MALWARE BazaLoader MalDoc Retrieving Payload",
        "doc_count": 2
    }]
}
```


alert.category

Basic query on alert.category for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.category&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.category\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\
=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.category": [{
       "key": "Malware Command and Control Activity Detected",
       "doc_count": 942
   }, {
       "key": "A Network Trojan was detected",
       "doc_count": 16
   }, {
       "key": "Potentially Bad Traffic",
       "doc_count": 9
   }, {
       "key": "Device Retrieving External IP Address Detected",
       "doc_count": 8
   }, {
       "key": "Attempted User Privilege Gain",
       "doc_count": 2
   }, {
       "key": "Not Suspicious Traffic",
       "doc_count": 1
   }]
}
```

alert.severity

Basic query on alert.severity for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.severity&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.severity\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\
=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.severity": [{
       "key": 1,
       "doc_count": 960
   }, {
       "key": 2,
       "doc_count": 17
   }, {
       "key": 3,
       "doc_count": 1
   }]
}
```

host

Basic query on host for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=hos
t&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
host\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\&qfil
ter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET
{
```

```
    "host": [{
        "key": "probe-1",
        "doc_count": 978
    }]
}
```

alert.target.ip

Basic query on alert.target.ip for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.target.ip&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.target.ip\&from_date\=1637662856188\&to_date\=1637749256188\&tenant
\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
    "alert.target.ip": [{
        "key": "192.168.5.125",
        "doc_count": 953
    }, {
        "key": "192.168.5.5",
        "doc_count": 2
    }]
}
```

alert.lateral

Basic query on alert.lateral for a src_ip or dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.lateral&qfilter=(src_ip:<ip>ORdest_ip<dest_ip>) -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.lateral\&qfilter\=\(src_ip%3A%2210.7.5.5%22%20OR%20dest_ip%3A%2210.
7.5.101%22\) -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.lateral": [{
     "key": "clients",
     "doc_count": 2
   }]
}
```

alert.source.net_info

Basic query on alert.source.net_info for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.source.net_info&qfilter=src_ip:<ip> -H 'Authorization: Token <token>'
-H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.source.net_info\&from_date\=1637662856188\&to_date\=1637749256188\&
```

```
tenant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.source.net_info": [{
       "key": "BAD USERS",
       "doc_count": 952
   }, {
       "key": "BAD_ACTOR.flanx.bad",
       "doc_count": 928
   }, {
       "key": "BAD_ACTOR.hzovb.bad",
       "doc_count": 8
   }, {
       "key": "BAD_ACTOR.moqcy.bad",
       "doc_count": 5
   }, {
       "key": "BAD_ACTOR.yoqem.bad",
       "doc_count": 3
   }, {
       "key": "AFFECTED USERS",
       "doc_count": 2
   }, {
       "key": "BAD_ACTOR.embba.bad",
       "doc_count": 2
   }, {
       "key": "BAD_ACTOR.exmji.bad",
       "doc_count": 2
   }, {
       "key": "BAD_ACTOR.goylc.bad",
       "doc_count": 2
   }, {
       "key": "BAD_ACTOR.hhjur.bad",
       "doc_count": 2
   }]
}
```

alert.target.net_info

Basic query on alert.target.net_info for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ale
rt.target.net_info&qfilter=src_ip:<ip> -H 'Authorization: Token <token>'
-H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
alert.target.net_info\&from_date\=1637662856188\&to_date\=1637749256188\&
tenant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "alert.target.net_info": [{
       "key": "AFFECTED USERS",
       "doc_count": 953
   }, {
       "key": "USER.fsbrp.org",
       "doc_count": 953
   }]
}
```

fqdn.src

Basic query on fqdn.src for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=fqd
n.src&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
fqdn.src\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\&
qfilter\=alert.source.ip:217.12.218.46 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "fqdn.src": [{
     "key": "wlmf4r449ubb.minedu.government.zz",
     "doc_count": 2
   }]
}
```

fqdn dest

Basic query on fqdn.dest for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=fqd
n.dest&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
fqdn.dest\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\
&qfilter\=alert.source.ip:217.12.218.46 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "fqdn.src": [{
       "key": "dc01.minedu.government.yy",
       "doc_count": 2
```

```
    }]
}
```

src_ip for a geoip.provider.autonomous_system_number

Basic query on src_ip for a geoip.provider.autonomous_system_number

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=src
_ip&qfilter=geoip.provider.autonomous_system_number:<number> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
src_ip\&from_date\=1637592693854\&to_date\=1637765493854\&tenant\=63\&qfi
lter\=geoip.provider.autonomous_system_number%3A23969 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "src_ip": [{
       "key": "1.1.129.63",
       "doc_count": 4
   }, {
       "key": "1.1.133.206",
       "doc_count": 4
   }, {
       "key": "1.1.141.132",
       "doc_count": 4
   }, {
       "key": "1.1.181.82",
       "doc_count": 4
   }, {
       "key": "1.1.218.199",
       "doc_count": 3
   }, {
```

```
        "key": "1.1.222.170",
        "doc_count": 3
    }, {
        "key": "1.1.128.145",
        "doc_count": 2
    }, {
        "key": "1.1.129.100",
        "doc_count": 2
    }, {
        "key": "1.1.129.252",
        "doc_count": 2
    }, {
        "key": "1.1.130.220",
        "doc_count": 2
    }]
}
```


geoip.provider.autonomous_system_organization for a src_ip

Basic query on geoip.provider.autonomous_system_organization for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=src
_ip&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output


```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
geoip.provider.autonomous_system_organization\&from_date\=1637662856188\&
to_date\=1637749256188\&tenant\=100\&qfilter\=src_ip:192.168.5.125 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

{
    "geoip.provider.autonomous_system_organization": [{
        "key": "ITL Company",
```

```
        "doc_count": 928
    }, {
        "key": "Amazon.com, Inc.",
        "doc_count": 20
    }, {
        "key": "Cloudflare, Inc.",
        "doc_count": 3
    }]
}
```

geoip.provider.autonomous_country_name for a src_ip

Basic query on geoip.provider.autonomous_country_name for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=geo
ip.country_name&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
geoip.country_name\&from_date\=1637662856188\&to_date\=1637749256188\&ten
ant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
    "geoip.country_name": [{
        "key": "Netherlands",
        "doc_count": 928
    }, {
        "key": "United States",
        "doc_count": 27
    }, {
        "key": "United Kingdom",
        "doc_count": 6
```

```
    }]
}
```

geopip.city_name

Basic query on geopip.city_name for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=geo
pip.city_name&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
geopip.city_name\&from_date\=1637662856188\&to_date\=1637749256188\&tenan
t\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
    "geoip.country_name": [{
        "key": "Amsterdam",
        "doc_count": 928
    }, {
        "key": "London",
        "doc_count": 27
    }, {
        "key": "Sheffield",
        "doc_count": 6
    }]
}
```

dest_ip

Basic query on dest_ip for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=des
t_ip&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
dest_ip\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\&q
filter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "dest_ip": [{
       "key": "217.12.218.46",
       "doc_count": 928
   }, {
       "key": "192.168.5.5",
       "doc_count": 17
   }, {
       "key": "107.21.162.206",
       "doc_count": 11
   }, {
       "key": "176.111.174.53",
       "doc_count": 6
   }, {
       "key": "104.21.74.174",
       "doc_count": 3
   }, {
       "key": "3.224.94.38",
       "doc_count": 3
   }, {
       "key": "34.193.115.2",
       "doc_count": 3
   }, {
       "key": "52.20.197.7",
       "doc_count": 3
   }, {
```

```
        "key": "52.204.109.97",
        "doc_count": 3
    }, {
        "key": "172.67.75.172",
        "doc_count": 1
    }]
}
```

src_port

Basic query on src_port for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=src
_port&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
src_port\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\&
qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
    "src_port": [{
        "key": 50344,
        "doc_count": 4
    }, {
        "key": 50334,
        "doc_count": 3
    }, {
        "key": 50989,
        "doc_count": 3
    }, {
        "key": 51391,
```

```
        "doc_count": 2
    }, {
        "key": 51486,
        "doc_count": 2
    }, {
        "key": 50329,
        "doc_count": 1
    }, {
        "key": 50343,
        "doc_count": 1
    }, {
        "key": 50376,
        "doc_count": 1
    }, {
        "key": 50408,
        "doc_count": 1
    }, {
        "key": 50409,
        "doc_count": 1
    }]
}
```


dest_port

Basic query on dest_port for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=des
t_port&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
dest_port\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\
&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
```

```
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "dest_port": [{
       "key": 80,
       "doc_count": 961
   }, {
       "key": 53,
       "doc_count": 15
   }, {
       "key": 135,
       "doc_count": 2
   }]
}
```

protocol

Basic query on proto for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=pro
to&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
proto\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\&qfi
lter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "proto": [{
       "key": "TCP",
       "doc_count": 963
```

```
    }, {
        "key": "UDP",
        "doc_count": 15
    }]
}
```

tunnel.src_ip

Basic query on tunnel.src_ip for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tun
nel.src_ip&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
tunnel.src_ip\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=
100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
  "tunnel.src_ip": [{
      "key": 147,
      "doc_count": 2
  }]
}
```

tunnel.dest_ip

Basic query on tunnel.dest_ip for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tun
nel.dest_ip&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
```

```
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
tunnel.dest_ip\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\
=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "tunnel.dest_ip": [{
       "key": "192.88.99.1",
       "doc_count": 2
   }]
}
```

tunnel.proto

Basic query on tunnel.proto for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tun
nel.proto&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
tunnel.proto\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=1
00\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
```

```
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "tunnel.proto": [{
       "key": "IPv6",
       "doc_count": 2
   }]
}
```

tunnel.depth

Basic query on tunnel.depth for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tun
nel.depth&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
tunnel.depth\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=1
00\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "tunnel.depth": [{
       "key": 1,
       "doc_count": 2
   }]
}
```

http.hostname

Basic query on http.hostname for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.hostname&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.hostname\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=
100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.hostname": [{
       "key": "onedrive.live.com",
       "doc_count": 928
   }, {
       "key": "checkip.amazonaws.com",
       "doc_count": 23
   }, {
       "key": "veso2.xyz",
       "doc_count": 6
   }, {
       "key": "admin.yougleeindia.in",
       "doc_count": 3
   }, {
       "key": "api.ip.sb",
       "doc_count": 1
   }]
}
```

http.url

Basic query on http.url for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=http.url&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=http.url\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET

{
   "http.url": [{
       "key": "/preload?manifest=wac",
       "doc_count": 928
   }, {
       "key": "/",
       "doc_count": 23
   }, {
       "key": "/uploads/files/rt3ret3.exe",
       "doc_count": 4
   }, {
       "key": "/theme/js/plugins/rt3ret3.exe",
       "doc_count": 3
   }, {
       "key": "/campo/r/r1",
       "doc_count": 2
   }, {
       "key": "/ip",
       "doc_count": 1
   }]
}
```

http.http_user_agent

Basic query on http.http_user_agent for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_user_agent&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -
H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_user_agent\&from_date\=1637662856188\&to_date\=1637749256188\&t
enant\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_user_agent": [{
       "key": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)
like Gecko",
       "doc_count": 928
   }, {
       "key": "WinHTTP loader/1.0",
       "doc_count": 23
   }, {
       "key": "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US)
WindowsPowerShell/5.1.19041.610",
       "doc_count": 1
   }]
}
```

http.status

Basic query on http.status for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
```

```
p.status&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=http.status\&from_date\=1637662856188\&to_date\=1637749256188\&tena
nt\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.status": [{
       "key": 200,
       "doc_count": 958
   }, {
       "key": 406,
       "doc_count": 3
   }]
}
```

http.http_refer

Basic query on http.http_refer for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
```

```
s\=http.http_refer\&from_date\=1637662856188\&to_date\=1637749256188\&
tenant\=95\&qfilter\=src_ip:10.1.21.102 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_refer": [{
       "key": "http://solovolonetwork.eu/plugins/smittybar4.php",
       "doc_count": 1
   }]
}
```

http.http_refer_info.domain

Basic query on http.http_refer_info.domain for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.domain&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_refer_info.domain\&from_date\=1637662856188\&to_date\=163774925
6188\&tenant\=95\&qfilter\=dest_ip:10.1.21.102 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_refer_info.domain": [{
       "key": "solovolonetwork.eu",
       "doc_count": 1
   }]
}
```

http.http_refer_info.host

Basic query on http.http_refer_info.host for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.host&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=http.http_refer_info.host\&from_date\=1637662856188\&to_date\=163774
9256188\&tenant\=95\&qfilter\=dest_ip:10.1.21.102 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_refer_info.host": [{
       "key": "solovolonetwork.eu",
       "doc_count": 1
   }]
}
```

http.http_refer_info.domain_without_tld

Basic query on http.http_refer_info.domain_without_tld for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.domain_without_tld&qfilter=src_ip:<ip> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_refer_info.domain_without_tld\&from_date\=1637662856188\&to_dat
e\=1637749256188\&tenant\=95\&qfilter\=dest_ip:10.1.21.102 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

{
   "http.http_refer_info.domain_without_tld": [{
       "key": "solovolonetwork",
       "doc_count": 1
   }]
}
```

http.http_refer_info.scheme

Basic query on http.http_refer_info.scheme for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.scheme&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_refer_info.scheme\&from_date\=1637662856188\&to_date\=163774925
6188\&tenant\=95\&qfilter\=dest_ip:10.1.21.102 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_refer_info.scheme": [{
       "key": "http",
       "doc_count": 1
   }]
}
```

http.http_refer_info.resource_path

Basic query on http.http_refer_info.resource_path for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.resource_path&qfilter=src_ip:<ip> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_refer_info.resource_path\&from_date\=1637662856188\&to_date\=16
37749256188\&tenant\=95\&qfilter\=dest_ip:10.1.21.102 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_refer_info.resource_path": [{
       "key": "/plugins/smittybar4.php",
       "doc_count": 1
   }]
}
```

http.http_refer_info.subdomain

Basic query on http.http_refer_info.subdomain for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.subdomain&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
url -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_refer_info.subdomain\&qfilter\=src_ip:109.236.87.40 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

{
   "http.http_refer_info.subdomain": [{
       "key": "awv",
       "doc_count": 1
   }]
}
```

http.http_refer_info.tld

Basic query on http.http_refer_info.tld for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=htt
p.http_refer_info.tld&qfilter=dest_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
http.http_refer_info.tld\&from_date\=1637662856188\&to_date\=163774925618
8\&tenant\=95\&qfilter\=dest_ip:10.1.21.102 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "http.http_refer_info.tld": [{
       "key": "eu",
       "doc_count": 1
   }]
```

```
}
```

dns.query.rrname

Basic query on dns.query.rrname for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=dns
.query.rrname&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
dns.query.rrname\&from_date\=1637662856188\&to_date\=1637749256188\&tenan
t\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "dns.query.rrname": [{
       "key": "api.ip.sb",
       "doc_count": 1
   }, {
       "key":
"efkezwpdxpsq3lsdvnnc.bprkmg4pueyf4gnc3mtq5v9d3udl3.gh4znchgys2kryddywlhf
s.f92chowrmjnsq2zph5pawzhd.hbvfhtjinhmjnzjrcbemscdcdddjdddddl94c.qhnnxbk
uhd5as4jank6hrd5iac.sluaknhbsoe.com",
       "doc_count": 1
   }, {
       "key":
"efkezwpdxpsq3lsdvnncbprkmg.4pueyf4gnc3mtq5v9d3u.dl3gh4znchgys2kryddywlhf
sf92chow.rmjnsq2zph5pawzhdhbvfhtjinhmjnzjrcbem.sszgdgdddygddddd4f9b.gmli2
huud3yisl25gy9xcax6rb.sluaknhbsoe.com",
       "doc_count": 1
   }, {
       "key":
"efkezwpdxpsq3lsdvnncbprkmg.4pueyf4gnc3mtq5v9d3udl.3gh4znchgys2kryddywlhf
```

```
sf9.2chowrmjnsq2zph5pawzhdhbvfhtjinhmjnzjr.cbemsszgfu2ahkwgdgdddygdddddd45
dg.9xjokgowqbn6sbhbrbi52bkzfh.sluaknhbsoe.com",
        "doc_count": 1
    }, {
        "key":
"efkezwpdxpsq3lsdvnncbprkmg.4pueyf4gnc3mtq5v9d3udl3gh4znch.gys2kryddywlhf
sf92chow.rmjnsq2zph5pawzhdhbvfhtjinhmjnzjrcbe.msszgfu2ahkdcddddjdddddlq3w
.ixvx2teotwppsfueypmxu4wheb.sluaknhbsoe.com",
        "doc_count": 1
    }, {
        "key":
"efkezwpdxpsq3lsdvnncbprkmg4p.ueyf4gnc3mtq5v9d3udl3gh4znchgy.s2kryddywlhf
sf92chowrmjnsq2zph5pawzhdhb.vfhtjinhmjnzjrcbemsszgfu2ahkw.gdgdddygdddddjl
lb.3s5ynywcd5mfcnergmltxeg9tj.sluaknhbsoe.com",
        "doc_count": 1
    }, {
        "key":
"efkezwpdxpsq3lsdvnncbprkmg4p.ueyf4gnc3mtq5v9d3udl3gh4znchgys2kryddyw.lhf
sf92chowrmjnsq2zph5pawzhdh.bvfhtjinhmjnzjrcbems.szgfuhdhddddbdddddqguc.nf
loozinho69cduwfiyvtc2enh.sluaknhbsoe.com",
        "doc_count": 1
    }, {
        "key":
"efkezwpdxpsq3lsdvnncbprkmg4pu.eyf4gnc3mtq5v9d3udl3gh4znchgys2kryddyw.lhf
sf92chowrmjnsq2zph5pawzhdhbvfhtjinhm.jnzjrcbemsszgfdlddddqddddddg2i.3fx6d
2yvcncxsvepmnxgjhnaeb.sluaknhbsoe.com",
        "doc_count": 1
    }, {
        "key":
"efkezwpdxpsq3lsdvnncbprkmg4pueyf4.gnc3mtq5v9d3udl3gh4znchgys2kr.yddywlhf
sf92chowrmjnsq2zph5pawz.hdhbvfhtjinhmjnzjrcbemsszgfdldddd.qddddddp92.e2uh
udvaqakxs9jltw36e2426j.sluaknhbsoe.com",
        "doc_count": 1
    }, {
        "key":
"efkezwpdxpsq3lsdvnncbprkmg4pueyf4.gnc3mtq5v9d3udl3gh4znchgys2kryddywlh.f
sf92chowrmjnsq2zph5pawzhdhbv.fhtjinhmjnzjrcbemscdcddddjddddddkgd.wvaakxug
ttossnhitfqvosww5g.sluaknhbsoe.com",
        "doc_count": 1
    }]
}
```

dns.query.rrtype

Basic query on dns.query.rrtype for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=dns
.query.rrtype&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
dns.query.rrtype\&from_date\=1637662856188\&to_date\=1637749256188\&tenan
t\=100\&qfilter\=src_ip:192.168.5.125 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "dns.query.rrtype": [{
       "key": "A",
       "doc_count": 15
   }]
}
```

tls.sni

Basic query on tls.sni for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
.sni&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=tls.sni\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=
63\&qfilter\=src_ip:185.251.38.235 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "tls.sni": [{
       "key": "c54rng3686.com",
       "doc_count": 23
   }]
}
```

tls.subject

Basic query on tls.subject for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
.subject&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=tls.subject\&from_date\=1637662856188\&to_date\=1637749256188\&tena
nt\=63\&qfilter\=src_ip:185.251.38.235 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "tls.subject": [{
       "key": "C=XX, ST=1, L=1, O=1, OU=1, CN=*",
```

```
        "doc_count": 23
    }]
}
```

tls.issuerdn

Basic query on tls.issuerdn for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
.issuerdn&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
tls.issuerdn\&from_date\=1637662856188\&to_date\=1637749256188\&tenant\=6
3\&qfilter\=src_ip:185.251.38.235 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
    "tls.issuerdn": [{
        "key": "C=XX, ST=1, L=1, O=1, OU=1, CN=*",
        "doc_count": 23
    }]
}
```

tls.fingerprint

Basic query on tls.fingerprint for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
.fingerprint&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=tls.fingerprint\&qfilter\=src_ip:77.247.181.163 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET


{
   "tls.fingerprint": [{
       "key":
"1c:61:ba:de:36:ac:49:33:af:59:d2:87:74:45:08:3d:46:e6:31:31",
       "doc_count": 1
   }]
}
```

tls.ja3.hash

Basic query on tls.ja3.hash for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
.ja3.hash&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=tls.ja3.hash\&from_date\=1637662856188\&to_date\=1637749256188\&ten
ant\=63\&qfilter\=src_ip:185.251.38.235 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET


{
   "tls.fingerprint": [{
```

```
        "key":
"5b:14:93:e9:8f:c8:e7:7a:2e:a9:69:34:b3:da:83:b3:21:83:b1:9c",
        "doc_count": 23
    }]
}
```

tls.ja3.agent

Basic query on tls.ja3.agent for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
.ja3.agent&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=tls.ja3.agent\&from_date\=1637662856188\&to_date\=1637749256188\&te
nant\=63\&qfilter\=src_ip:185.251.38.235 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
    "tls.ja3.agent": [{
        "key": "Tofsee  (from abuse.ch)",
        "doc_count": 23
    }]
}
```

tls.ja3s.hash

Basic query on tls.ja3s.hash for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=tls
```

```
.ja3s.hash&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=tls.ja3s.hash\&from_date\=1637662856188\&to_date\=1637749256188\&te
nant\=63\&qfilter\=src_ip:185.251.38.235 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "tls.ja3s.hash": [{
       "key": "f47b284bf7f61821a407e4f140a02686",
       "doc_count": 23
   }]
}
```

smtp.mail_from

Basic query on smtp.mail_from for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smt
p.mail_from&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=smtp.mail_from\&qfilter\=src_ip:49.68.159.2 -H 'Authorization:
```

```
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "smtp.mail_from": [{
       "key": "<mrikglck@rkts.com>",
       "doc_count": 1
   }]
}
```

smtp.rcpt_to

Basic query on smtp.rcpt_to for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smt
p.rcpt_to&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=smtp.rcpt_to\&qfilter\=src_ip:49.68.159.2 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "smtp.rcpt_to": [{
       "key": "<info@audioschematics.dk>",
       "doc_count": 1
   }]
}
```

smtp.helo

Basic query on smtp.helo for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smtp.helo&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=smtp.helo\&qfilter\=src_ip:49.68.159.2 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET

{
   "smtp.helo": [{
       "key": "rkts.com",
       "doc_count": 1
   }]
}
```

smb.command

Basic query on smb.command for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smb.command&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=smb.command\&qfilter\=src_ip:192.168.2.202 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "smb.command": [{
       "key": "SMB2_COMMAND_TREE_CONNECT",
       "doc_count": 1
   }]
}
```

smb.status

Basic query on smb.status for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smb
.status&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=smb.status\&qfilter\=src_ip:192.168.2.202 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "smb.status": [{
       "key": "STATUS_SUCCESS",
       "doc_count": 1
   }]
```

```
}
```

smb.filename

Basic query on smb.filename for a dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smb
.filename&qfilter=dest_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=smb.filename\&qfilter\=dest_ip:192.168.10.30 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "smb.filename": [{
       "key": "temp\\mimikatz.exe",
       "doc_count": 1
   }]
}
```

smb.share

Basic query on smb.share for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=smb
.share&qfilter=dest_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=smb.share\&qfilter\=src_ip:192.168.2.202 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "smb.share": [{
       "key": "\\\\10.230.33.21\\agerasfiles",
       "doc_count": 1
   }]
}
```

ssh.client.software_version

Basic query on ssh.client.software_version for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ssh
.client.software_version&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=ssh.client.software_version\&qfilter\=src_ip:140.143.77.85 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

{
   "ssh.client.software_version": [{
       "key": "libssh-0.1",
       "doc_count": 1
   }]
```

```
}
```

ssh.server.software_version

Basic query on ssh.server.software_version for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=ssh
.server.software_version&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?field
s\=ssh.server.software_version\&qfilter\=src_ip:140.143.77.85 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

{
   "ssh.server.software_version": [{
       "key": "OpenSSH_6.4",
       "doc_count": 1
   }]
}
```

hostname_info.subdomain

Basic query on hostname_info.subdomain for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=hos
tname_info.subdomain&qfilter=src_ip:<ip> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields
\=hostname_info.subdomain\&from_date\=1637662856188\&to_date\=16377492561
88\&tenant\=100\&qfilter\=src_ip:140.143.77.85 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET


{
   "hostname_info.subdomain": [{
       "key": "www",
       "doc_count": 2
   }]
}
```

hostname_info.domain

Basic query on hostname_info.domain for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=hos
tname_info.domain&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -
H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
hostname_info.domain\&from_date\=1637662856188\&to_date\=1637749256188\&t
enant\=100\&qfilter\=src_ip:217.12.218.46 -H 'Authorization: Token
```

```
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "hostname_info.domain": [{
       "key": "google.com",
       "doc_count": 2
   }]
}
```

hostname_info.tld

Basic query on hostname_info.tld for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=hos
tname_info.tld&qfilter=src_ip:<ip> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
hostname_info.tld\&from_date\=1637662856188\&to_date\=1637749256188\&tena
nt\=100\&qfilter\=src_ip:217.12.218.46 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "hostname_info.tld": [{
       "key": "com",
       "doc_count": 2
   }]
}
```

hostname_info.domain_without_tld

Basic query on hostname_info.domain_without_tld for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=hos
tname_info.domain_without_tld&qfilter=src_ip:<ip> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
hostname_info.domain_without_tld\&from_date\=1637662856188\&to_date\=1637
749256188\&tenant\=100\&qfilter\=src_ip:217.12.218.46 -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "hostname_info.domain_without_tld": [{
       "key": "google",
       "doc_count": 2
   }]
}
```

hostname_info.host

Basic query on hostname_info.host for a src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats?fields=hos
tname_info.domain_without_tld&qfilter=src_ip:<ip> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/fields_stats/\?fields\=
hostname_info.host\&from_date\=1637662856188\&to_date\=1637749256188\&ten
ant\=100\&qfilter\=src_ip:217.12.218.46 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "hostname_info.host": [{
       "key": "www.google.com",
       "doc_count": 2
   }]
}
```

Queries for NTA/NSM fields (non-hunt/alert)

Query Structure

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter=<filter_field>
:<field_value> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

NOTE #1: *<tenant_id>* parameter should be used, only if multi-tenancy is enabled on the SSP. Below are listed examples with and without a tenant parameter.

NOTE #2: You can also optionally set ***<start_date>*** and ***<end_date>*** to specify a time range for your queries. Start/end dates are given in **unix timestamp format**.

NOTE #3: Requires Upgrade38 (U38) and above

Example

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter=<f
ilter_field>:<field_value>&from_date=1637662856188&to_date=1637749256188
-H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET
```

The following list contains the basic Rest API query (under **Basic Query** section), as well as example queries with the optional parameters ***<start_date>***, ***<end_date>*** and ***<tenant_id>*** and their relevant console outputs. The **Basic Query** shows the api endpoint for field stats per field, as well as a qfilter - it could either per src_ip, dest_ip, alert.source_ip, alert.dest_ip or any other field, depending on the needed information.

The examples, under **Example Usage**, contain different fields, as well as the optional parameters like <start_date> and <end_date> to set a time range for the query and <tenant_id> - in case multi-tenancy is enabled on your SSP.

The queries are listed, according to the information they provide for the desired field/qfilter combination.

NOTE #4: A **<token>** is mandatory for each query. It can be found on your SSP, under Account Settings -> Edit token, or directly under:

https://stamus.security.platform.ip/accounts/edit/token

Example Queries

HTTP - http.hostname

Basic query on http.hostname

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=http.hostname:<hostname> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=http.hostname:www.internationalbankfund.com -H 'Authorization:
Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

{
   "count": 1,
   "next": null,
   "previous": null,
   "results": [{
       "@version": "1",
       "ether": {
           "src_mac": "00:08:02:1c:47:ae",
           "dest_mac": "20:e5:2a:b6:93:f1"
       },
       "in_iface": "tppdummy0",
       "beat": {
```

```
        "name": "SSProbe-1",
        "version": "6.3.2",
        "hostname": "SSProbe-1"
    },
    "flow_id": 1644478096315332,
    "host": "SSProbe-1",
    "@timestamp": "2021-11-29T11:04:53.805Z",
    "type": "json-log",
    "offset": 617104075,
    "dest_port": 49169,
    "app_proto": "http",
    "fileinfo": {
        "filename": "/",
        "sid": [],
        "tx_id": 0,
        "size": 16,
        "gaps": false,
        "type": "ASCII text",
        "state": "CLOSED",
        "magic": "ASCII text",
        "stored": false
    },
    "see_name": "scirius-enterprise",
    "timestamp": "2021-11-29T11:04:53.805021+0000",
    "see_id": "4ee461e6e5fb",
    "dest_ip": "10.1.8.101",
    "http": {
        "status": 200,
        "user_agent": {
            "os_major": "10",
            "os": "Mac OS X",
            "os_minor": "9",
            "name": "Firefox",
            "os_name": "Mac OS X",
            "build": "",
            "device": "Other",
            "minor": "0",
            "major": "25"
        },
```

```
            "http_user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X
10.9; rv:25.0) Gecko/20100101 Firefox/25.0",
            "url": "/",
            "hostname": "icanhazip.com",
            "http_content_type": "text/plain",
            "protocol": "HTTP/1.1",
            "length": 16,
            "http_method": "GET"
        },
        "src_ip": "147.75.40.2",
        "source": "/var/log/suricata/eve-0.json",
        "tags": ["beats_input_codec_json_applied"],
        "src_port": 80,
        "proto": "TCP",
        "hostname_info": {
            "domain": "icanhazip.com",
            "tld": "com",
            "domain_without_tld": "icanhazip",
            "url": "icanhazip.com",
            "host": "icanhazip.com"
        },
        "event_type": "fileinfo",
        "_id": "ESZea30BQfk1jLvDgmD5"
    }]
}
```


HTTP - http_user_agent

Basic query on http.http_user_agent

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=http.http_user_agent:<http_user_agent>&start_date=<start_date>&end_da
te=<end_date> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=http.http_user_agent:Windows\&start_date\=1638193893\&end_date\=16
38193894 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
 "count": 1,
 "next": null,
 "previous": null,
 "results": [
   {
     "@version": "1",
     "ether": {},
     "in_iface": "tppdummy0",
     "beat": {
       "name": "SSProbe-1",
       "version": "6.3.2",
       "hostname": "SSProbe-1"
     },
     "flow_id": 1031244477682551,
     "host": "SSProbe-1",
     "@timestamp": "2021-11-29T11:12:09.346Z",
     "type": "json-log",
     "offset": 624409505,
     "dest_port": 49170,
     "app_proto": "http",
     "fileinfo": {
       "filename": "/",
       "sid": [],
       "tx_id": 0,
       "size": 620544,
       "gaps": false,
       "type": "data",
```

```
      "state": "CLOSED",
      "magic": "data",
      "stored": false
    },
    "see_name": "scirius-enterprise",
    "timestamp": "2021-11-29T11:12:09.346679+0000",
    "see_id": "4ee461e6e5fb",
    "dest_ip": "10.1.10.101",
    "http": {
      "status": 200,
      "user_agent": {
        "name": "Other",
        "os_name": "Other",
        "build": "",
        "os": "Other",
        "device": "Other"
      },
      "http_user_agent": "\\xa4",
      "url":
"/?NTgxNTM4&xPPmZDFrSehlGee&ByHCbhyhLcL=blackmail&wchiumQhaCAV=detonat
or&puPFBsD=difference&DEBAiFkrVEg=heartfelt&fgdd3s=wHfQMvXcJwDJFYbGMvr
ERqNbNknQA06PxpH2_drYdZqxKGni1-
b5UUSk6FuCEh3h9vI&jmxzfYbewVI=vest&yddhzfp=known&CYxTETSmutZ=heartfelt
&VTofgMElKGpgC=everyone&ANheaHFkbsz=already&qSfyMreHMO=known&veVdeVp=c
ommunity&UJhUlFUvJfGgP=known&ajdklwKeGf=referred&UCdIyXWEd=golfer&tcfg
g4=keeABNVLohUyDfAI1yYldB11A8fqoiRWEmxOdicKH_ROOMw11-
ZuWF7Iz2VTFkvEXd_s&TTOkOtrpyQt=heartfelt&sGwhHmzJMTQ2MTc1",
      "hostname": "176.53.161.71",
      "http_content_type": "application/x-msdownload",
      "protocol": "HTTP/1.1",
      "length": 620544,
      "http_method": "GET"
    },
    "src_ip": "176.53.161.71",
    "source": "/var/log/suricata/eve-0.json",
    "tags": [
      "beats_input_codec_json_applied"
    ],
    "metadata": {
```

```
        "flowbits": [
          "ET.RIGEKExploit",
          "http.dottedquadhost"
        ]
      },
      "src_port": 80,
      "proto": "TCP",
      "hostname_info": {
        "domain": "176.53.161.71",
        "domain_without_tld": "176.53.161.71",
        "url": "176.53.161.71",
        "host": "176.53.161.71"
      },
      "event_type": "fileinfo",
      "_id": "HyZla30BQfk1jLvDKZiH"
    }
  ]
}
```


JA3 - tls.ja3s.hash

Basic query on tls.ja3s.hash

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=tls.ja3s.hash:<tls_ja3s_hash>&start_date=<start_date>&end_date=<end_d
ate> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET | jq -r
```

Example Usage and Query Output


```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=tls.ja3s.hash:e35df3e00ca4ef31d42b34bebaa2f86e\&start_date\=163818
8470\&end_date\=1638188472 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
```

```
application/json' -X GET | jq -r

{
   "count": 1,
   "next": null,
   "previous": null,
   "results": [
     {
       "@version": "1",
       "in_iface": "tppdummy0",
       "beat": {
         "name": "SSProbe-1",
         "version": "6.3.2",
         "hostname": "SSProbe-1"
       },
       "flow_id": 1847879503822356,
       "host": "SSProbe-1",
       "tls": {
         "serial":
"03:11:44:76:C8:20:04:10:7D:A4:2F:67:EC:A1:70:CF:EA:23",
         "ja3": {
           "hash": "37cdab6ff1bd1c195bacb776c5213bf2",
           "string": "771,49196-49200-159-52393-52392-52394-49195-
49199-158-49188-49192-107-49187-49191-103-49162-49172-57-49161-49171-
51-157-156-61-60-53-47-255,11-10-35-13-22-23,29-23-25-24,0-1-2"
         },
         "subject": "CN=mexcompany.net",
         "fingerprint":
"25:bd:7e:d5:39:b3:79:0b:b0:ee:9b:f3:dc:2a:1b:72:77:23:d3:10",
         "ja3s": {
           "hash": "e35df3e00ca4ef31d42b34bebaa2f86e",
           "string": "771,49200,65281-11-35"
         },
         "notbefore": "2018-12-26T17:37:06",
         "version": "TLS 1.2",
         "issuerdn": "C=US, O=Let's Encrypt, CN=Let's Encrypt
Authority X3",
         "notafter": "2019-03-26T17:37:06",
         "from_proto": "smtp"
```

```
    },
    "tcp": {
      "psh": true,
      "tcp_flags_ts": "1b",
      "tcp_flags_tc": "1b",
      "state": "last_ack",
      "ack": true,
      "fin": true,
      "syn": true,
      "tcp_flags": "1b"
    },
    "app_proto_orig": "smtp",
    "@timestamp": "2021-11-29T12:21:11.534Z",
    "type": "json-log",
    "offset": 635074097,
    "flow": {
      "age": 2,
      "reason": "timeout",
      "had_gap": null,
      "state": "closed",
      "start": "2021-11-29T12:20:54.626850+0000",
      "pkts_toclient": 13,
      "end": "2021-11-29T12:20:56.546826+0000",
      "pkts_toserver": 11,
      "bytes_toserver": 1115,
      "alerted": false,
      "bytes_toclient": 4423
    },
    "dest_port": 25,
    "app_proto": "tls",
    "see_name": "scirius-enterprise",
    "timestamp": "2021-11-29T12:21:11.534771+0000",
    "see_id": "4ee461e6e5fb",
    "dest_ip": "209.126.235.42",
    "source": "/var/log/suricata/eve-0.json",
    "src_ip": "10.1.24.101",
    "tags": [
      "beats_input_codec_json_applied"
    ],
```

```
        "src_port": 50025,
        "proto": "TCP",
        "event_type": "flow",
        "_id": "Kieka30BQfk1jLvDcAWx"
      }
    ]
  }
```

JA3S - tls.ja3.hash

Basic query on tls.ja3.hash

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=tls.ja3.hash:<tls_ja3_hash>&start_date=<start_date>&end_date=<end_dat
e> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=tls.ja3.hash:bafc6b01eae6f4350f5db6805ace208e\&start_date=16381906
83\&end_date\=1638190743 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
   "count": 1,
   "next": null,
   "previous": null,
   "results": [
     {
       "@version": "1",
       "in_iface": "tppdummy0",
       "beat": {
         "name": "SSProbe-1",
```

```
        "version": "6.3.2",
        "hostname": "SSProbe-1"
      },
      "flow_id": 912046469807376,
      "host": "SSProbe-1",
      "tls": {
        "serial":
"00:92:0F:D1:B7:FE:4B:88:AE:B6:ED:5A:B0:C3:6C:56:68",
        "ja3": {
          "hash": "bafc6b01eae6f4350f5db6805ace208e",
          "string": "769,49172-49171-49162-49161-53-47-56-50-10-19-5-
4,0-10-11-23-65281,25-23-24,0",
          "agent": [
            "Mozilla/5.0 (Windows NT 6.3) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/44.0.2446.21 Safari/537.36"
          ]
        },
        "subject": "OU=Domain Control Validated, OU=PositiveSSL
Wildcard, CN=*.ipify.org",
        "fingerprint":
"a8:ec:3c:8e:03:51:58:e5:a9:c0:b5:fe:8c:d1:b4:ec:ed:4c:09:a9",
        "ja3s": {
          "hash": "184d532a16876b78846ae6a03f654890",
          "string": "769,49171,65281-11"
        },
        "notbefore": "2018-01-24T00:00:00",
        "sni": "api.ipify.org",
        "issuerdn": "C=GB, ST=Greater Manchester, L=Salford, O=COMODO
CA Limited, CN=COMODO RSA Domain Validation Secure Server CA",
        "version": "TLSv1",
        "notafter": "2021-01-23T23:59:59"
      },
      "tcp": {
        "psh": true,
        "tcp_flags_ts": "1b",
        "tcp_flags_tc": "1b",
        "state": "closed",
        "ack": true,
        "fin": true,
```

```
      "syn": true,
      "tcp_flags": "1b"
    },
    "@timestamp": "2021-11-29T12:58:03.374Z",
    "type": "json-log",
    "offset": 643782118,
    "flow": {
      "age": 1,
      "reason": "timeout",
      "had_gap": null,
      "state": "closed",
      "start": "2021-11-29T12:57:47.343424+0000",
      "pkts_toclient": 14,
      "end": "2021-11-29T12:57:48.263420+0000",
      "pkts_toserver": 11,
      "bytes_toserver": 1166,
      "alerted": true,
      "bytes_toclient": 6919
    },
    "dest_port": 443,
    "app_proto": "tls",
    "see_name": "scirius-enterprise",
    "timestamp": "2021-11-29T12:58:03.374726+0000",
    "see_id": "4ee461e6e5fb",
    "dest_ip": "54.204.36.156",
    "source": "/var/log/suricata/eve-0.json",
    "src_ip": "10.0.90.129",
    "tags": [
      "beats_input_codec_json_applied"
    ],
    "src_port": 49163,
    "proto": "TCP",
    "hostname_info": {
      "domain": "ipify.org",
      "domain_without_tld": "ipify",
      "tld": "org",
      "url": "api.ipify.org",
      "host": "api.ipify.org",
      "subdomain": "api"
```

```
        },
        "event_type": "flow",
        "_id": "ECfGa30BQfk1jLvDQk0b"
      }
    ]
  }
```

TLS SNI - tls.sni

Basic query on tls.sni

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=tls.sni:<tls_sni>&start_date=<start_date>&end_date=<end_date> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=tls.sni:decretery.host\&start_date\=1638190352\&end_date\=16381903
53 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950'
-H 'Content-Type: application/json' -X GET | jq -r

{
 "count": 1,
 "next": null,
 "previous": null,
 "results": [
   {
     "@version": "1",
     "in_iface": "tppdummy0",
     "beat": {
       "name": "SSProbe-1",
       "version": "6.3.2",
```

```
      "hostname": "SSProbe-1"
    },
    "flow_id": 1077768638451658,
    "host": "SSProbe-1",
    "tls": {
      "serial": "00:AD:44:97:71:65:09:EE:00",
      "ja3": {
        "hash": "1d095e68489d3c535297cd8dffb06cb9",
        "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-
4,65281-0-10-11,23-24,0",
        "agent": [
          "User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.2; .NET CLR 1.0.3705"
        ]
      },
      "subject": "C=US, ST=AK, O=furled receptiveness, OU=pastoral's
pitchblende, CN=castles.info",
      "fingerprint":
"e0:2d:cd:bd:af:bd:c8:36:dc:b3:5f:d1:c6:1f:f7:db:f6:88:68:65",
      "ja3s": {
        "hash": "4192c0a946c5bd9b544b4656d9f624a4",
        "string": "769,47,65281"
      },
      "notbefore": "2019-02-17T05:00:01",
      "sni": "decretery.host",
      "issuerdn": "C=US, ST=AK, O=furled receptiveness, OU=pastoral's
pitchblende, CN=castles.info",
      "version": "TLSv1",
      "notafter": "2020-02-17T05:00:01"
    },
    "tcp": {
      "rst": true,
      "psh": true,
      "tcp_flags_ts": "1e",
      "tcp_flags_tc": "1a",
      "state": "closed",
      "ack": true,
      "syn": true,
      "tcp_flags": "1e"
```

```
  },
  "@timestamp": "2021-11-29T12:52:32.550Z",
  "type": "json-log",
  "offset": 642792889,
  "flow": {
    "age": 163,
    "reason": "timeout",
    "had_gap": null,
    "state": "closed",
    "start": "2021-11-29T12:49:31.578617+0000",
    "pkts_toclient": 727,
    "end": "2021-11-29T12:52:14.518642+0000",
    "pkts_toserver": 223,
    "bytes_toserver": 16677,
    "alerted": false,
    "bytes_toclient": 954645
  },
  "dest_port": 443,
  "app_proto": "tls",
  "see_name": "scirius-enterprise",
  "timestamp": "2021-11-29T12:52:32.550661+0000",
  "see_id": "4ee461e6e5fb",
  "dest_ip": "46.148.26.88",
  "source": "/var/log/suricata/eve-0.json",
  "src_ip": "10.2.20.101",
  "tags": [
    "beats_input_codec_json_applied"
  ],
  "src_port": 49582,
  "proto": "TCP",
  "hostname_info": {
    "domain": "decretery.host",
    "tld": "host",
    "domain_without_tld": "decretery",
    "url": "decretery.host",
    "host": "decretery.host"
  },
  "event_type": "flow",
  "_id": "yCfBa30BQfk1jLvDFUNj"
```

```
    }
  ]
}
```

TLS Issuer DN - tls.issuerdn

Basic query on tls.issuerdn

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=tls.issuerdn:<tls_issuerdn> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=tls.issuerdn:CN\=www.wehpsikted.com -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
   "count": 1,
   "next": null,
   "previous": null,
   "results": [
     {
       "@version": "1",
       "in_iface": "tppdummy0",
       "beat": {
         "name": "SSProbe-1",
         "version": "6.3.2",
         "hostname": "SSProbe-1"
       },
       "flow_id": 1430543006523562,
       "host": "SSProbe-1",
       "tls": {
```

```
        "serial": "6A:70:12:58:77:CD:86:D3",
        "ja3": {
          "hash": "e7d705a3286e19ea42f587b344ee6865",
          "string": "771,49195-49199-49162-49161-49171-49172-49170-
49159-49169-51-50-69-57-56-136-22-47-65-53-132-10-5-4-255,0-11-10-35-
13-15,23-25-28-27-24-26-22-14-13-11-12-9-10,0-1-2",
          "agent": [
            "Malware Test FP: malspam-traffic"
          ]
        },
        "subject": "CN=www.7unfq5xbo6pqf7.net",
        "fingerprint":
"48:96:b3:19:14:98:56:3e:1e:72:bf:e3:37:e1:72:b1:89:b0:aa:78",
        "ja3s": {
          "hash": "a95ca7eab4d47d051a5cd4fb7b6005dc",
          "string": "771,49199,65281-11-15"
        },
        "notbefore": "2018-12-16T00:00:00",
        "sni": "www.ekjw72.com",
        "issuerdn": "CN=www.wehpsikted.com",
        "version": "TLS 1.2",
        "notafter": "2019-05-24T00:00:00"
      },
      "tcp": {
        "psh": true,
        "tcp_flags_ts": "1a",
        "tcp_flags_tc": "1a",
        "state": "established",
        "ack": true,
        "syn": true,
        "tcp_flags": "1a"
      },
      "@timestamp": "2021-11-29T14:03:14.090Z",
      "type": "json-log",
      "offset": 656705508,
      "flow": {
        "age": 14,
        "reason": "timeout",
        "had_gap": null,
```

```
        "state": "established",
        "start": "2021-11-29T13:56:45.595218+0000",
        "pkts_toclient": 498,
        "end": "2021-11-29T13:56:59.175187+0000",
        "pkts_toserver": 182,
        "bytes_toserver": 31930,
        "alerted": true,
        "bytes_toclient": 675734
      },
      "dest_port": 9101,
      "app_proto": "tls",
      "see_name": "scirius-enterprise",
      "timestamp": "2021-11-29T14:03:14.090781+0000",
      "see_id": "4ee461e6e5fb",
      "dest_ip": "128.31.0.39",
      "source": "/var/log/suricata/eve-0.json",
      "src_ip": "10.3.20.101",
      "tags": [
        "beats_input_codec_json_applied"
      ],
      "src_port": 49252,
      "proto": "TCP",
      "hostname_info": {
        "domain": "ekjw72.com",
        "domain_without_tld": "ekjw72",
        "tld": "com",
        "url": "www.ekjw72.com",
        "host": "www.ekjw72.com",
        "subdomain": "www"
      },
      "event_type": "flow",
      "_id": "UicBbH0BQfk1jLvDzrnU"
    }
  ]
}
```

TLS Subject DN - tls.subject

Basic query on tls.subject

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=tls.subject:<tls_subject>&start_date=<start_date>&end_date=<end_date>
-H 'Authorization: Token <token>' -H 'Content-Type: application/json'
-X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=tls.subject:CN\=www.b2zhaqdqh2on.net\&start_date\=1638194632\&end_
date\=1638194633 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
 "count": 1,
 "next": null,
 "previous": null,
 "results": [
   {
     "@version": "1",
     "in_iface": "tppdummy0",
     "beat": {
       "name": "SSProbe-1",
       "version": "6.3.2",
       "hostname": "SSProbe-1"
     },
     "flow_id": 1339182605844783,
     "host": "SSProbe-1",
     "tls": {
       "serial": "00:E1:1E:CF:E1:48:D6:82:B1",
       "ja3": {
         "hash": "e7d705a3286e19ea42f587b344ee6865",
         "string": "771,49195-49199-49162-49161-49171-49172-49170-
```

```
49159-49169-51-50-69-57-56-136-22-47-65-53-132-10-5-4-255,0-11-10-35-
13-15,23-25-28-27-24-26-22-14-13-11-12-9-10,0-1-2",
        "agent": [
          "Malware Test FP: malspam-traffic"
        ]
      },
      "subject": "CN=www.b2zhaqdqh2on.net",
      "fingerprint":
"9c:b2:7b:0e:bf:9f:97:5d:fd:4c:bd:1a:e4:8d:df:79:14:88:21:dd",
      "ja3s": {
        "hash": "303951d4c50efb2e991652225a6f02b1",
        "string": "771,49199,65281-11"
      },
      "notbefore": "2019-02-06T00:00:00",
      "sni": "www.3zgkgore7qqua5poc.com",
      "issuerdn": "CN=www.ruv4ntpaszrlquyzebjd.com",
      "version": "TLS 1.2",
      "notafter": "2019-06-27T23:59:59"
    },
    "tcp": {
      "psh": true,
      "tcp_flags_ts": "1a",
      "tcp_flags_tc": "1a",
      "state": "established",
      "ack": true,
      "syn": true,
      "tcp_flags": "1a"
    },
    "@timestamp": "2021-11-29T14:03:52.114Z",
    "type": "json-log",
    "offset": 656955489,
    "flow": {
      "age": 46,
      "reason": "timeout",
      "had_gap": null,
      "state": "established",
      "start": "2021-11-29T13:57:00.115194+0000",
      "pkts_toclient": 492,
      "end": "2021-11-29T13:57:46.175208+0000",
```

```
        "pkts_toserver": 191,
        "bytes_toserver": 122667,
        "alerted": true,
        "bytes_toclient": 563083
      },
      "dest_port": 9001,
      "app_proto": "tls",
      "see_name": "scirius-enterprise",
      "timestamp": "2021-11-29T14:03:52.114704+0000",
      "see_id": "4ee461e6e5fb",
      "dest_ip": "51.15.52.16",
      "source": "/var/log/suricata/eve-0.json",
      "src_ip": "10.3.20.101",
      "tags": [
        "beats_input_codec_json_applied"
      ],
      "src_port": 49256,
      "proto": "TCP",
      "hostname_info": {
        "domain": "3zgkgore7qqua5poc.com",
        "domain_without_tld": "3zgkgore7qqua5poc",
        "tld": "com",
        "url": "www.3zgkgore7qqua5poc.com",
        "host": "www.3zgkgore7qqua5poc.com",
        "subdomain": "www"
      },
      "event_type": "flow",
      "_id": "rScCbH0BQfk1jLvDZrvf"
    }
  ]
}
```

TLS Fingerprint - tls.fingerprint

Basic query on tls.fingerprint

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilte
r=tls.fingerprint:<tls_fingerprint> -H 'Authorization: Token <token>'
-H 'Content-Type: application/json' -X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=tls.fingerprint%3A%2247%3A6c%3Add%3A3c%3A4d%3Af3%3A47%3A26%3A26%3A
ae%3A76%3Ab8%3Ade%3A1c%3Abe%3A59%3A56%3Ace%3A69%3A7b%22 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET | jq -r

{
   "count": 1,
   "next":
"https://stamus.security.platform.ip/rest/rules/es/events_tail/?page=2
&qfilter=tls.fingerprint%3A%2247%3A6c%3Add%3A3c%3A4d%3Af3%3A47%3A26%3A
26%3Aae%3A76%3Ab8%3Ade%3A1c%3Abe%3A59%3A56%3Ace%3A69%3A7b%22",
   "previous": null,
   "results": [
     {
       "@version": "1",
       "in_iface": "tppdummy0",
       "beat": {
         "name": "SSProbe-1",
         "version": "6.3.2",
         "hostname": "SSProbe-1"
       },
       "flow_id": 1052035311955231,
       "host": "SSProbe-1",
```

```
      "tls": {
        "serial": "00:B3:8D:6C:8E:CD:9B:13:3E",
        "ja3": {
          "hash": "6734f37431670b3ab4292b8f60f29984",
          "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-
4,65281-10-11,23-24,0",
          "agent": [
            "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0"
          ]
        },
        "subject": "C=GB, ST=London, L=London, O=Global Security,
OU=IT Department, CN=example.com",
        "fingerprint":
"47:6c:dd:3c:4d:f3:47:26:26:ae:76:b8:de:1c:be:59:56:ce:69:7b",
        "ja3s": {
          "hash": "623de93db17d313345d7ea481e7443cf",
          "string": "769,49172,65281-11"
        },
        "notbefore": "2019-04-30T18:40:36",
        "version": "TLSv1",
        "issuerdn": "C=GB, ST=London, L=London, O=Global Security,
OU=IT Department, CN=example.com",
        "notafter": "2020-04-29T18:40:36"
      },
      "tcp": {
        "psh": true,
        "tcp_flags_ts": "1b",
        "tcp_flags_tc": "1b",
        "state": "closed",
        "ack": true,
        "fin": true,
        "syn": true,
        "tcp_flags": "1b"
      },
      "@timestamp": "2021-11-29T14:35:46.458Z",
      "type": "json-log",
      "offset": 666030792,
      "flow": {
```

```
      "age": 0,
      "reason": "timeout",
      "had_gap": null,
      "state": "closed",
      "start": "2021-11-29T14:35:31.179410+0000",
      "pkts_toclient": 11,
      "end": "2021-11-29T14:35:31.539393+0000",
      "pkts_toserver": 8,
      "bytes_toserver": 1067,
      "alerted": true,
      "bytes_toclient": 2294
    },
    "dest_port": 443,
    "app_proto": "tls",
    "see_name": "scirius-enterprise",
    "timestamp": "2021-11-29T14:35:46.458794+0000",
    "see_id": "4ee461e6e5fb",
    "dest_ip": "185.222.202.43",
    "source": "/var/log/suricata/eve-0.json",
    "src_ip": "10.5.1.102",
    "tags": [
      "beats_input_codec_json_applied"
    ],
    "src_port": 49313,
    "proto": "TCP",
    "event_type": "flow",
    "_id": "PicfbH0BQfk1jLvDnfad"
  },
  {
    "@version": "1",
    "in_iface": "tppdummy0",
    "beat": {
      "name": "SSProbe-1",
      "version": "6.3.2",
      "hostname": "SSProbe-1"
    },
    "flow_id": 995354058510010,
    "host": "SSProbe-1",
    "tls": {
```

```
        "serial": "00:B3:8D:6C:8E:CD:9B:13:3E",
        "ja3": {
          "hash": "6734f37431670b3ab4292b8f60f29984",
          "string": "769,47-53-5-10-49171-49172-49161-49162-50-56-19-
4,65281-10-11,23-24,0",
          "agent": [
            "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0"
          ]
        },
        "subject": "C=GB, ST=London, L=London, O=Global Security,
OU=IT Department, CN=example.com",
        "fingerprint":
"47:6c:dd:3c:4d:f3:47:26:26:ae:76:b8:de:1c:be:59:56:ce:69:7b",
        "ja3s": {
          "hash": "623de93db17d313345d7ea481e7443cf",
          "string": "769,49172,65281-11"
        },
        "notbefore": "2019-04-30T18:40:36",
        "version": "TLSv1",
        "issuerdn": "C=GB, ST=London, L=London, O=Global Security,
OU=IT Department, CN=example.com",
        "notafter": "2020-04-29T18:40:36"
      },
      "tcp": {
        "psh": true,
        "tcp_flags_ts": "1b",
        "tcp_flags_tc": "1b",
        "state": "closed",
        "ack": true,
        "fin": true,
        "syn": true,
        "tcp_flags": "1b"
      },
      "@timestamp": "2021-11-29T14:35:44.439Z",
      "type": "json-log",
      "offset": 666029398,
      "flow": {
        "age": 0,
```

```
          "reason": "timeout",
          "had_gap": null,
          "state": "closed",
          "start": "2021-11-29T14:35:31.559428+0000",
          "pkts_toclient": 12,
          "end": "2021-11-29T14:35:31.959410+0000",
          "pkts_toserver": 9,
          "bytes_toserver": 1398,
          "alerted": true,
          "bytes_toclient": 2769
        },
        "dest_port": 443,
        "app_proto": "tls",
        "see_name": "scirius-enterprise",
        "timestamp": "2021-11-29T14:35:44.439347+0000",
        "see_id": "4ee461e6e5fb",
        "dest_ip": "185.222.202.43",
        "source": "/var/log/suricata/eve-0.json",
        "src_ip": "10.5.1.102",
        "tags": [
          "beats_input_codec_json_applied"
        ],
        "src_port": 49314,
        "proto": "TCP",
        "event_type": "flow",
        "_id": "PScfbH0BQfk1jLvDnfad"
    }
  ]
}
```


DNS - dns.query.rrname

This will return all IPs that have queried for the domain abc.xyz. (Not only the one that has triggered the alert)

Basic query on dnes.query.rrname

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=dns.query.rrname:<dnes_query_rrname> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=dns.query.rrname:t23bendarron.top -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
 "count": 1,
 "next": null,
 "previous": null,
 "results": [
   {
     "tx_id": 0,
     "packet_info": {
       "linktype": 1
     },
     "@version": "1",
     "ether": {
       "src_mac": "00:08:02:1c:47:ae",
       "dest_mac": "a4:1f:72:c2:09:6a"
     },
     "in_iface": "tppdummy0",
     "alert": {
       "category": "Potentially Bad Traffic",
       "source": {
         "ip": "10.5.1.5",
         "port": 53
       },
       "action": "allowed",
       "signature": "ET DNS Query to a *.top domain - Likely Hostile",
       "signature_id": 2023883,
       "target": {
```

```
        "ip": "10.5.1.103",
        "port": 49966
      },
      "rev": 4,
      "gid": 1,
      "metadata": {
        "attack_target": [
          "Client_Endpoint"
        ],
        "deployment": [
          "Perimeter"
        ],
        "signature_severity": [
          "Major"
        ],
        "updated_at": [
          "2020_09_15"
        ],
        "affected_product": [
          "Windows_XP_Vista_7_8_10_Server_32_64_Bit"
        ],
        "created_at": [
          "2017_02_07"
        ]
      },
      "severity": 2
    },
    "packet":
"pB9ywglqAAgCHEeuCABFAAA+Af4AAIARIjwKBQFnCgUBBcMuADUAKk/xnwYBAAABAAAAA
AAADHQyM2JlbmRhcnJvbgN0b3AAAAEAAQ==",
    "sig": {
      "source": "etpro",
      "created": "2017-02-07",
      "updated": "2020-09-15"
    },
    "beat": {
      "name": "SSProbe-1",
      "version": "6.3.2",
      "hostname": "SSProbe-1"
```

```
  },
  "flow_id": 588600226972007,
  "host": "SSProbe-1",
  "@timestamp": "2021-11-29T14:35:38.923Z",
  "dns": {
    "query": [
      {
        "type": "query",
        "rrname": "t23bendarron.top",
        "tx_id": 0,
        "id": 40710,
        "rrtype": "A"
      }
    ]
  },
  "type": "json-log",
  "offset": 1391973362,
  "flow": {
    "start": "2021-11-29T14:35:38.923476+0000",
    "src_ip": "10.5.1.103",
    "dest_ip": "10.5.1.5",
    "dest_port": 53,
    "pkts_toserver": 1,
    "bytes_toserver": 76,
    "src_port": 49966,
    "pkts_toclient": 0,
    "bytes_toclient": 0
  },
  "dest_port": 53,
  "app_proto": "dns",
  "stream": 0,
  "see_name": "scirius-enterprise",
  "timestamp": "2021-11-29T14:35:38.923476+0000",
  "see_id": "4ee461e6e5fb",
  "dest_ip": "10.5.1.5",
  "source": "/var/log/suricata/eve-alert.json",
  "src_ip": "10.5.1.103",
  "tags": [
    "beats_input_codec_json_applied"
```

```
      ],
      "src_port": 49966,
      "proto": "UDP",
      "payload_printable": ".............t23bendarron.top.....",
      "hostname_info": {
        "domain": "t23bendarron.top",
        "tld": "top",
        "domain_without_tld": "t23bendarron",
        "url": "t23bendarron.top",
        "host": "t23bendarron.top"
      },
      "event_type": "alert",
      "_id": "FCcfbH0BQfk1jLvDdvbo"
    }
  ]
}
```


KRB5 - krb5.cname

Basic query on krb5.cname

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=krb5.cname:<krb5_cname> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET | jq -r
```

Example Usage and Query Output


```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=krb5.cname:rudolph.wilkins -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
"count": 1,
```

```
"next": null,
"previous": null,
"results": [
 {
   "dest_port": 88,
   "@version": "1",
   "ether": {
     "src_mac": "00:08:02:1c:47:ae",
     "dest_mac": "a4:1f:72:c2:09:6a"
   },
   "in_iface": "tppdummy0",
   "see_name": "scirius-enterprise",
   "beat": {
     "name": "SSProbe-1",
     "version": "6.3.2",
     "hostname": "SSProbe-1"
   },
   "timestamp": "2021-11-29T14:44:35.987332+0000",
   "flow_id": 1020087339148367,
   "host": "SSProbe-1",
   "dest_ip": "10.5.10.5",
   "see_id": "4ee461e6e5fb",
   "source": "/var/log/suricata/eve-0.json",
   "src_ip": "10.5.10.103",
   "tags": [
     "beats_input_codec_json_applied"
   ],
   "@timestamp": "2021-11-29T14:44:35.987Z",
   "src_port": 49198,
   "proto": "TCP",
   "type": "json-log",
   "offset": 668335642,
   "event_type": "krb5",
   "krb5": {
     "cname": "rudolph.wilkins",
     "realm": "PIZZAJUKEBOX.COM",
     "encryption": "aes256-cts-hmac-sha1-96",
     "weak_encryption": false,
     "sname": "ldap/PizzaJukebox-DC.pizzajukebox.com",
```

```
      "msg_type": "KRB_TGS_REP"
    },
    "_id": "PCgnbH0BQfk1jLvDqAXP"
  }]
}
```

KRB5 - krb5.sname

Basic query on krb5.sname

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=krb5.sname:<krb5_sname> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=krb5.sname%3A%22cifs%2FPizzaJukebox-DC.pizzajukebox.com%22 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET | jq -r

{
  "count": 3,
  "next": null,
  "previous": null,
  "results": [
    {
      "dest_port": 88,
      "@version": "1",
      "ether": {
        "src_mac": "00:08:02:1c:47:ae",
        "dest_mac": "a4:1f:72:c2:09:6a"
      },
```

```
      "in_iface": "tppdummy0",
      "see_name": "scirius-enterprise",
      "beat": {
        "name": "SSProbe-1",
        "version": "6.3.2",
        "hostname": "SSProbe-1"
      },
      "timestamp": "2021-11-29T14:44:35.127316+0000",
      "flow_id": 776898956720522,
      "host": "SSProbe-1",
      "dest_ip": "10.5.10.5",
      "see_id": "4ee461e6e5fb",
      "source": "/var/log/suricata/eve-0.json",
      "src_ip": "10.5.10.103",
      "tags": [
        "beats_input_codec_json_applied"
      ],
      "@timestamp": "2021-11-29T14:44:35.127Z",
      "src_port": 49195,
      "proto": "TCP",
      "type": "json-log",
      "offset": 668328479,
      "event_type": "krb5",
      "krb5": {
        "cname": "rudolph.wilkins",
        "realm": "PIZZAJUKEBOX.COM",
        "encryption": "aes256-cts-hmac-sha1-96",
        "weak_encryption": false,
        "sname": "cifs/PizzaJukebox-DC.pizzajukebox.com",
        "msg_type": "KRB_TGS_REP"
      },
      "_id": "ICgnbH0BQfk1jLvDpAXm"
    }
  ]
}
```

SSH - ssh.client.software_version

Basic query on ssh.client.software_version

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=ssh.client.software_version:<ssh_client_software_version> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=ssh.client.software_version:libssh-0.1 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
 "count": 1,
 "next": null,
 "previous": null,
 "results": [
   {
     "timestamp": "2021-11-29T15:09:54.000000+0000",
     "flow_id": 610408626702955,
     "in_iface": "enp94s0np0",
     "event_type": "alert",
     "vlan": 147,
     "src_ip": "140.143.77.85",
     "src_port": 36734,
     "dest_ip": "138.245.204.2",
     "dest_port": 22,
     "proto": "TCP",
     "alert": {
       "action": "allowed",
       "gid": 1,
```

```
        "signature_id": 2006546,
        "rev": 9,
        "signature": "ET SCAN LibSSH Based Frequent SSH Connections
Likely BruteForce Attack",
        "category": "Attempted Administrator Privilege Gain",
        "severity": 1,
        "metadata": {
          "updated_at": [
            "2010_07_30"
          ],
          "created_at": [
            "2010_07_30"
          ]
        }
      },
      "ssh": {
        "client": {
          "proto_version": "2.0",
          "software_version": "libssh-0.1"
        },
        "server": {
          "proto_version": "2.0",
          "software_version": "OpenSSH_6.4"
        }
      },
      "app_proto": "ssh",
      "flow": {
        "pkts_toserver": 6,
        "pkts_toclient": 5,
        "bytes_toserver": 576,
        "bytes_toclient": 1735,
        "start": "2019-04-09T01:12:28.182891+0200"
      },
      "@timestamp": "2021-11-29T15:09:54.000Z",
      "host": "Probe",
      "_id": "QSh1bH0BQfk1jLvDHMbM"
    }
  ]
}
```

SSH - ssh.server.software_version

Basic query on ssh.server.software_version

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events_tail/?qfilter
=ssh.server.software_version:<server_software_version> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET | jq -r
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/events\_tail/\?qfilt
er\=ssh.server.software_version:OpenSSH_6.4 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET | jq -r

{
 "count": 1,
 "next": null,
 "previous": null,
 "results": [
   {
     "timestamp": "2021-11-29T15:09:54.000000+0000",
     "flow_id": 610408626702955,
     "in_iface": "enp94s0np0",
     "event_type": "alert",
     "vlan": 147,
     "src_ip": "140.143.77.85",
     "src_port": 36734,
     "dest_ip": "138.245.204.2",
     "dest_port": 22,
     "proto": "TCP",
     "alert": {
       "action": "allowed",
       "gid": 1,
       "signature_id": 2006546,
       "rev": 9,
```

```
        "signature": "ET SCAN LibSSH Based Frequent SSH Connections
Likely BruteForce Attack",
        "category": "Attempted Administrator Privilege Gain",
        "severity": 1,
        "metadata": {
          "updated_at": [
            "2010_07_30"
          ],
          "created_at": [
            "2010_07_30"
          ]
        }
      },
      "ssh": {
        "client": {
          "proto_version": "2.0",
          "software_version": "libssh-0.1"
        },
        "server": {
          "proto_version": "2.0",
          "software_version": "OpenSSH_6.4"
        }
      },
      "app_proto": "ssh",
      "flow": {
        "pkts_toserver": 6,
        "pkts_toclient": 5,
        "bytes_toserver": 576,
        "bytes_toclient": 1735,
        "start": "2019-04-09T01:12:28.182891+0200"
      },
      "@timestamp": "2021-11-29T15:09:54.000Z",
      "host": "Probe",
      "_id": "QSh1bH0BQfk1jLvDHMbM"
    }
  ]
}
```

General queries in Hunt, with all their subqueries, broken down into requests/ responses

NOTE #1: *<tenant_id>* parameter should be used, only if multi-tenancy is enabled on the SSP. Below are listed examples with and without tenant parameter.

NOTE #2: You can also optionally set *<start_date>* and *<end_date>* to specify a time range for your queries.

The following list contains the basic Rest API endpoint (under **Curl Query** section) , as well as example queries with the optional parameters (*<start_date>*, *<end_date>* and *<tenant_id>*) and the relevant console outputs.

The examples are divided into sections according to the information they provide and then further subdivided into query per field (for example **Alert Metadata** section -> **Affected Product** field).

Query Structure

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=<
field>&qfilter=<filter_value> -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

NOTE #1: *<tenant_id>* parameter should be used, only if multi-tenancy is enabled on the SSP. Below are listed examples with and without a tenant parameter.

NOTE #2: You can also optionally set *<start_date>* and *<end_date>* to specify a time range for your queries. Start/end dates are given in **unix timestamp format**.

Example

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=<
field>&qfilter=<filter_value>&from_date=1637662856188&to_date=1637749256
188 -H 'Authorization: Token <token>' -H 'Content-Type:
```

```
application/json' -X GET
```

Example Queries

alert.metadata.affected_product

Basic query on alert.metadata.affected_product

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.metadata.affected_product&qfilter=alert.source.ip:<ip> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.metadata.affected_product\&qfilter\=alert.source.ip:170.238.117.187 -
H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "Windows_XP_Vista_7_8_10_Server_32_64_Bit",
   "doc_count": 29
}]
```

alert.metadata.attack_target

Basic query on alert.metadata.attack_target for a relevant alert.source.ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.metadata.attack_target&qfilter=alert.source.ip:<ip> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k https:
//stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.me
tadata.attack_target\&qfilter\=alert.source.ip:170.238.117.187 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "Client_Endpoint",
   "doc_count": 29
}]
```

alert.metadata.maleware_family

Basic query on alert.metadata.maleware_family for an alert.source.ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.metadata.maleware_family&qfilter=alert.source.ip:<ip> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k https:
//stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.me
tadata.malware_family\&qfilter\=alert.source.ip:170.238.117.187 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "TrickBot",
   "doc_count": 15
}]
```

alert.metadata.signature_severity

Basic query on alert.metadata.signature_severity

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=alert.metadata.signature_severity&qfilter=alert.source.ip:<ip> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k https:
//stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.metadata.signature_severity\&qfilter\=alert.source.ip:170.238.117.187 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "Major",
   "doc_count": 21
}, {
   "key": "Informational",
   "doc_count": 4
}, {
   "key": "Minor",
   "doc_count": 4
}]
```

alert.metadata.mitre_tactic_id

Basic query on alert.metadata.signature_severity

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field\=alert.metadata.mitre_tactic_id&from_date=<start_date>&to_date=<end_date>&tenant=<tenand_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.metadata.mitre_tactic_id\&from_date\=1634657760979\&to_date\=16372497
60979\&tenant\=100 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "TA0011",
   "doc_count": 28
}]
```

alert.metadata.mitre_tactic_name

Basic query on alert.metadata.mitre_tactic_name

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.metadata.mitre_tactic_name&from_date=<start_date>&to_date=<end_date>&te
nant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.metadata.mitre_tactic_name\&from_date\=1634657760979\&to_date\=163724
9760979\&tenant\=100 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "Command_And_Control",
```

```
   "doc_count": 28
}]
```

alert.metadata.mitre_technique_name

Basic query on alert.metadata.mitre_technique_name

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.metadata.mitre_technique_name&from_date=<start_date>&to_date=<end_date>
&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.metadata.mitre_technique_name\&from_date\=1634657760979\&to_date\=163
7249760979\&tenant\=100 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "Application_Layer_Protocol",
   "doc_count": 28
}]
```

alert.signature

Basic query on alert.signature

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.signature&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <tokem>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.signature\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=
100 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "ET MALWARE Cobalt Strike Malleable C2 (OneDrive)",
   "doc_count": 928
}, {
   "key": "Anchor_DNS stickseed Variant CnC Checkin",
   "doc_count": 14
}, {
   "key": "ET MALWARE Anchor_DNS stickseed Variant CnC Checkin",
   "doc_count": 14
}, {
   "key": "ET MALWARE Observed Malicious SSL Cert (BazaLoader CnC)",
   "doc_count": 13
}, {
   "key": "ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)",
   "doc_count": 13
}, {
   "key": "ET MALWARE Win32/TrickBot Anchor Variant Style External IP
Check",
   "doc_count": 7
}, {
   "key": "ETPRO HUNTING Suspicious User-Agent containing Loader
Observed",
   "doc_count": 7
}, {
   "key": "ETPRO POLICY External IP Check (checkip.amazonaws.com)",
   "doc_count": 7
}, {
   "key": "ETPRO MALWARE BazaLoader MalDoc CnC Checkin",
   "doc_count": 4
}, {
```

```
   "key": "ET INFO Observed ZeroSSL Certificate for Suspicious TLD
(.xyz)",
   "doc_count": 2
}]
```

alert.category

Basic query on alert.category

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.category&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.category\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=1
00 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "Malware Command and Control Activity Detected",
   "doc_count": 956
}, {
   "key": "Domain Observed Used for C2 Detected",
   "doc_count": 26
}, {
   "key": "A Network Trojan was detected",
   "doc_count": 16
}, {
   "key": "Potentially Bad Traffic",
   "doc_count": 13
}, {
   "key": "Device Retrieving External IP Address Detected",
   "doc_count": 8
}, {
```

```
    "key": "Attempted User Privilege Gain",
    "doc_count": 2
}, {
    "key": "Misc Attack",
    "doc_count": 1
}, {
    "key": "Not Suspicious Traffic",
    "doc_count": 1
}, {
    "key": "Potential Corporate Privacy Violation",
    "doc_count": 1
}]
```


alert.severity

Basic query on alert.severity

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=alert.severity&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output


```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.severity\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=100 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET

[{
    "key": 1,
    "doc_count": 1001
}, {
    "key": 2,
```

```
    "doc_count": 22
}, {
    "key": 3,
    "doc_count": 1
}]
```

host

Basic query on host

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=host
&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token> -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ho
st\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=100 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
    "key": "sn-probe-aws-1",
    "doc_count": 1024
}]
```

alert.source.ip

Basic query on alert.source.ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
```

```
t.source.ip -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k https:
//stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.so
urce.ip\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=100 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "217.12.218.46",
   "doc_count": 928
}, {
   "key": "184.72.1.208",
   "doc_count": 24
}, {
   "key": "107.21.162.206",
   "doc_count": 8
}, {
   "key": "176.111.174.53",
   "doc_count": 6
}, {
   "key": "104.21.74.174",
   "doc_count": 3
}, {
   "key": "192.168.5.125",
   "doc_count": 2
}, {
   "key": "3.224.94.38",
   "doc_count": 2
}, {
   "key": "34.193.115.2",
   "doc_count": 2
}, {
   "key": "52.20.197.7",
   "doc_count": 2
}, {
   "key": "52.204.109.97",
```

```
    "doc_count": 2
}]
```

alert.target.ip

Basic query on alert.target.ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=alert.target.ip&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id>
-H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.target.ip\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=100 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
    "key": "192.168.5.125",
    "doc_count": 980
}, {
    "key": "192.168.5.5",
    "doc_count": 2
}]
```

alert.lateral

Basic query on alert.lateral

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.lateral -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.lateral\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

[{
   "key": "org.affected-users",
   "doc_count": 9
}]
```

alert.source.net_info_agg

Basic query on alert.source.net_info_agg

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=aler
t.source.net_info_agg -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=al
ert.source.net_info_agg\&from_date\=1634657760979\&to_date\=1637249760979
\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET
```

```
[{
   "key": "bad_actor.ffewr.bad.bad-users",
   "doc_count": 30
}, {
   "key": "bad_actor.atssl.bad.bad-users",
   "doc_count": 18
}, {
   "key": "bad_actor.jkupq.bad.bad-users",
   "doc_count": 15
}, {
   "key": "bad_actor.kdvdj.bad.bad-users",
   "doc_count": 15
}, {
   "key": "bad_actor.dgtwn.bad.bad-users",
   "doc_count": 9
}, {
   "key": "bad_actor.mcclr.bad.bad-users",
   "doc_count": 9
}, {
   "key": "bad_actor.xxxju.bad.bad-users",
   "doc_count": 9
}, {
   "key": "bad_actor.abjuj.bad.bad-users",
   "doc_count": 8
}, {
   "key": "bad_actor.zppjm.bad.bad-users",
   "doc_count": 4
}, {
   "key": "user.rergu.org.affected-users",
   "doc_count": 4
}]
```


alert.target.net_info_agg

Basic query on alert.target.net_info_agg

```
curl -k
```

```
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=alert.target.net_info_agg -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=alert.target.net_info_agg\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "user.rergu.org.affected-users",
   "doc_count": 92
}, {
   "key": "user.azclb.org.affected-users",
   "doc_count": 40
}]
```

fqdn.src

Basic query on fqdn.src

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=fqdn.src -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=fqdn.src\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
```

```
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "wlmf4r449ubb.minedu.government.zz",
   "doc_count": 2
}]
```

fqdn.dest

Basic query on fqdn.dest

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=fqdn
.dest&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=fq
dn.dest\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "dc01.minedu.government.zz",
   "doc_count": 2
}]
```

geoip.provider.autonomous_system_number

Basic query on geoip.provider.autonomous_system_number

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=geoip.provider.autonomous_system_number -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=geoip.provider.autonomous_system_number\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET

[{
   "key": 198610,
   "doc_count": 60
}, {
   "key": 50673,
   "doc_count": 45
}, {
   "key": 29182,
   "doc_count": 24
}, {
   "key": 16276,
   "doc_count": 20
}, {
   "key": 10620,
   "doc_count": 12
}, {
   "key": 48096,
   "doc_count": 12
}, {
   "key": 56851,
   "doc_count": 12
```

```
}, {
   "key": 22773,
   "doc_count": 8
}, {
   "key": 7684,
   "doc_count": 4
}, {
   "key": 26496,
   "doc_count": 3
}]
```

geoip.provider.autonomous_system_organization

Basic query on geoip.provider.autonomous_system_organization

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=geoi
p.provider.autonomous_system_organization -H 'Authorization: Token
<token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ge
oip.provider.autonomous_system_organization\&from_date\=1634657760979\&to
_date\=1637249760979\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json'  -X GET

[{
   "key": "Beget Ltd",
   "doc_count": 60
}, {
   "key": "Serverius Holding B.V.",
   "doc_count": 45
```

```
}, {
   "key": "JSC ISPsystem",
   "doc_count": 24
}, {
   "key": "OVH SAS",
   "doc_count": 20
}, {
   "key": "OOO IT-Grad",
   "doc_count": 12
}, {
   "key": "PE Skurykhin Mukola Volodumurovuch",
   "doc_count": 12
}, {
   "key": "Telmex Colombia S.A.",
   "doc_count": 12
}, {
   "key": "Cox Communications Inc.",
   "doc_count": 8
}, {
   "key": "SAKURA Internet Inc.",
   "doc_count": 4
}, {
   "key": "Alibaba (China) Technology Co., Ltd.",
   "doc_count": 3
}]
```


geoip.country_name

Basic query on geoip.country_name

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=geoi
p.country_name&from_date=<start_date>&to_date=<end_date> -H
'Authorization: Token <token>' -H 'Content-Type: application/json'  -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ge
oip.country_name\&from_date\=1634657760979\&to_date\=1637249760979\&tenan
t\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950'
-H 'Content-Type: application/json'  -X GET

[{
   "key": "Russia",
   "doc_count": 84
}, {
   "key": "Netherlands",
   "doc_count": 45
}, {
   "key": "France",
   "doc_count": 20
}, {
   "key": "United States",
   "doc_count": 18
}, {
   "key": "Belarus",
   "doc_count": 12
}, {
   "key": "Colombia",
   "doc_count": 12
}, {
   "key": "Ukraine",
   "doc_count": 12
}, {
   "key": "Japan",
   "doc_count": 4
}, {
   "key": "Hong Kong",
   "doc_count": 3
}, {
   "key": "Australia",
   "doc_count": 1
}]
```

geoip.city_name

Basic query on geoip.city_name

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=geoi
p.city_name -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ge
oip.city_name\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=
91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET
  [{
   "key": "Leiderdorp",
   "doc_count": 35
}, {
   "key": "Kyiv",
   "doc_count": 12
}, {
   "key": "Medellín",
   "doc_count": 12
}, {
   "key": "Enschede",
   "doc_count": 10
}, {
   "key": "Phoenix",
   "doc_count": 8
}, {
   "key": "Scottsdale",
   "doc_count": 3
}, {
   "key": "Center Conway",
   "doc_count": 2
```

```
}, {
   "key": "San Francisco",
   "doc_count": 2
}, {
   "key": "Sydney",
   "doc_count": 1
}]
```

src_ip

Basic query on src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=src_
ip -H 'Authorization: Token <token>' -H 'Content-Type: application/json'
-X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sr
c_ip\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "172.16.10.97",
   "doc_count": 81
}, {
   "key": "87.236.22.142",
   "doc_count": 30
}, {
   "key": "5.45.74.250",
   "doc_count": 20
}, {
   "key": "172.16.10.2",
```

```
    "doc_count": 19
}, {
    "key": "185.246.64.237",
    "doc_count": 18
}, {
    "key": "145.239.25.100",
    "doc_count": 15
}, {
    "key": "185.255.79.71",
    "doc_count": 9
}, {
    "key": "31.131.19.227",
    "doc_count": 9
}, {
    "key": "46.249.62.199",
    "doc_count": 8
}, {
    "key": "190.146.112.216",
    "doc_count": 6
}]
```


dest_ip

Basic query on dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=dest
_ip&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=de
st_ip\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
```

```
'Content-Type: application/json' -X GET

[{
   "key": "172.16.10.97",
   "doc_count": 85
}, {
   "key": "172.16.10.2",
   "doc_count": 44
}, {
   "key": "87.236.22.142",
   "doc_count": 30
}, {
   "key": "5.45.74.250",
   "doc_count": 15
}, {
   "key": "70.184.86.103",
   "doc_count": 8
}, {
   "key": "185.246.64.237",
   "doc_count": 6
}, {
   "key": "190.146.112.216",
   "doc_count": 6
}, {
   "key": "145.239.25.100",
   "doc_count": 5
}, {
   "key": "133.242.164.31",
   "doc_count": 4
}, {
   "key": "185.255.79.71",
   "doc_count": 3
}]
```

src_port

Basic query on src_port

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=src_
port -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sr
c_port\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": 443,
   "doc_count": 64
}, {
   "key": 80,
   "doc_count": 32
}, {
   "key": 447,
   "doc_count": 18
}, {
   "key": 8082,
   "doc_count": 6
}, {
   "key": 49321,
   "doc_count": 6
}, {
   "key": 49618,
   "doc_count": 6
}, {
   "key": 49213,
   "doc_count": 4
```

```
}, {
   "key": 49931,
   "doc_count": 4
}, {
   "key": 49557,
   "doc_count": 3
}, {
   "key": 445,
   "doc_count": 2
}]
```

dest_port

Basic query on dest_port

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=dest
_port&from_date=<start_date>&to_date=<end_date> -H 'Authorization: Token
<token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=de
st_port\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": 443,
   "doc_count": 45
}, {
   "key": 80,
   "doc_count": 20
}, {
```

```
    "key": 8080,
    "doc_count": 10
}, {
    "key": 447,
    "doc_count": 6
}, {
    "key": 8082,
    "doc_count": 6
}, {
    "key": 49616,
    "doc_count": 6
}, {
    "key": 53,
    "doc_count": 5
}, {
    "key": 7080,
    "doc_count": 4
}, {
    "key": 49216,
    "doc_count": 4
}, {
    "key": 49217,
    "doc_count": 4
}]
```


proto

Basic query on proto

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=prot
o -H 'Authorization: Token <token>' -H 'Content-Type: application/json'
-X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=pr
oto\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "TCP",
   "doc_count": 215
}, {
   "key": "UDP",
   "doc_count": 5
}]
```

vlan

Basic query on vlan

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=vlan
-H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=vl
an\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": 147,
   "doc_count": 2
}, {
   "key": 2996,
```

```
   "doc_count": 2
}]
```

tunnel.src_ip

Basic query on tunnel.src_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tunn
el.src_ip&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tu
nnel.src_ip\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "70.55.213.211",
   "doc_count": 2
}]
```

tunnel.dest_ip

Basic query on tunnel.dest_ip

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tunn
el.dest_ip&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tu
nnel.dest_ip\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=9
1 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

[{
   "key": "192.88.99.1",
   "doc_count": 2
}]
```

tunnel.proto

Basic query on tunnel.proto

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tunn
el.proto&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tu
nnel.proto\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "IPv6",
   "doc_count": 2
}]
```

tunnel.depth

Basic query on tunnel.depth

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tunnel.depth&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tunnel.depth\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json'  -X GET

[{
   "key": 1,
   "doc_count": 2
}]
```

http.hostname

Basic query on http.hostname

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http.hostname&from_date=<start_date>&to_date=<end_date> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
```

```
tp.hostname\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "5.45.74.250",
   "doc_count": 35
}, {
   "key": "190.146.112.216",
   "doc_count": 12
}, {
   "key": "46.249.62.199",
   "doc_count": 10
}, {
   "key": "70.184.86.103",
   "doc_count": 8
}, {
   "key": "133.242.164.31",
   "doc_count": 4
}, {
   "key": "aucklandluxuryrealestatelistings.com",
   "doc_count": 3
}, {
   "key": "104.228.227.210",
   "doc_count": 2
}, {
   "key": "198.199.96.164",
   "doc_count": 2
}, {
   "key": "47.224.42.17",
   "doc_count": 2
}, {
   "key": "54.153.245.124",
   "doc_count": 1
}]
```

http.url

Basic query on http.url

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.url&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.url\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "/",
   "doc_count": 19
}, {
   "key": "/sin.png",
   "doc_count": 19
}, {
   "key": "/tin.png",
   "doc_count": 10
}, {
   "key": "/win.png",
   "doc_count": 6
}, {
   "key": "/Sw9JKmXqaSj.exe",
   "doc_count": 5
}, {
   "key": "/Tinx86_14.exe",
   "doc_count": 5
}, {
   "key": "/win9/LOVELESS-
PC_W617601.2CA1E9F687FADECC78247C980B61536A/81/",
   "doc_count": 5
```

```
}, {
   "key": "/pHXewgm3qzll_3L/",
   "doc_count": 3
}, {
   "key": "/win9/LOVELESS-
PC_W617601.2CA1E9F687FADECC78247C980B61536A/83/",
   "doc_count": 3
}, {
   "key": "/win9/BOMBALICIOUS-
DC_W617601.E51E3A88424D7EC649CC8276EF9926D1/90",
   "doc_count": 2
}]
```


http.http_user_agent

Basic query on http.http_user_agent

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.http_user_agent&from_date=<start_date>&to_date=<end_date>&tenant=<tenant
_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_user_agent\&from_date\=1634657760979\&to_date\=1637249760979\&ten
ant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
```

```
    "key": "WinHTTP loader/1.0",
    "doc_count": 23
}, {
    "key": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)",
    "doc_count": 18
}, {
    "key": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64;
x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET
CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)",
    "doc_count": 7
}, {
    "key": "test",
    "doc_count": 4
}, {
    "key": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)
like Gecko",
    "doc_count": 1
}, {
    "key": "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.2228.0 Safari/537.36",
    "doc_count": 1
}, {
    "key": "WinHTTP sender/1.0",
    "doc_count": 1
}]
```


http.status

Basic query on http.status

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.status&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.status\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -
H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": 200,
   "doc_count": 80
}]
```

http.http_refer

Basic query on http.http_refer

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.http_refer&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=
91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

[{
   "key": "http://wasserman-digital-marketing.com/wp-login.php",
   "doc_count": 4
}, {
   "key":
"http://awv.283886.net/index.php?zVv9HUbyhfhYFWqU18c=uSfsMTr30qtTFXrfh
```

```
adMoVmAgJYyqRZg_VWrmgtmJl6oksThl79zFThM",
   "doc_count": 2
}]
```

http.http_refer_info.domain_without_tld

Basic query on http.http_refer_info.domain_without_tld

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.http_refer_info.domain_without_tld -H 'Authorization: Token <token>' -H
'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.domain_without_tld\&from_date\=1634657760979\&to_date\
=1637249760979\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "wasserman-digital-marketing.com",
   "doc_count": 4
},
{
   "key": "283886",
   "doc_count": 2
}]
```

http.http_refer_info.host

Basic query on http.http_refer_info.host

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.http_refer_info.host -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.host\&from_date\=1634657760979\&to_date\=1637249760979
\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "wasserman-digital-marketing.com",
   "doc_count": 4
},
{
   "key": "awv.283886.net",
   "doc_count": 2
}]
```

http.http_refer_info.domain

Basic query on http.http_refer_info.domain

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.domain -H 'Authorization: Token <token>' -H 'Content-
Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.domain\&from_date\=1634657760979\&to_date\=16372497609
```

```
79\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json'  -X GET

[{
   "key": "wasserman-digital-marketing.com",
   "doc_count": 4
}, {
   "key": "283886.net",
   "doc_count": 2
}]
```

http.http_refer_info.scheme

Basic query on http.http_refer_info.scheme

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.scheme -H 'Authorization: Token <token>' -H 'Content-
Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.scheme\&from_date\=1634657760979\&to_date\=16372497609
79\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "http",
   "doc_count": 6
}]
```

http.http_refer_info.resource_path

Basic query on http.http_refer_info.resource_path

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.resource_path&from_date=<start_date>&to_date=<end_date
>&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.resource_path\&from_date\=1634657760979\&to_date\=1637
249760979\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json'  -X GET

[{
        "key": "/wp-login.php",
        "doc_count": 4
    },
    {
        "key": "/index.php",
        "doc_count": 2
}]
```

http.http_refer_info.subdomain

Basic query on http.http_refer_info.subdomain

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
```

```
.http_refer_info.subdomain&from_date=<start_date>&to_date=<end_date>&tena
nt=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.subdomain\&from_date\=1634657760979\&to_date\=16372497
60979\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "awv",
   "doc_count": 2
}]
```

http.http_refer_info.tld

Basic query on http.http_refer_info.tld

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=http
.http_refer_info.tld&from_date=<start_date>&to_date=<end_date> -H
'Authorization: Token <token>' -H 'Content-Type: application/json'  -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ht
tp.http_refer_info.tld\&from_date\=1634657760979\&to_date\=1637249760979\
&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET
```

```
[{
   "key": "awv",
   "doc_count": 2
}]
```

dns.query.rrname

Basic query on dns.query.rrname

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=dns.
query.rrname -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=dn
s.query.rrname\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\
=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "scotiation.pw",
   "doc_count": 4
}, {
   "key": "api.ip.sb",
   "doc_count": 1
}]
```

dns.query.rrtype

Basic query on dns.query.rrtype

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=dns.
query.rrtype -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=dn
s.query.rrtype\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\
=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

 [{
     "key": "A",
     "doc_count": 5
 }]
```

tls.sni

Basic query on tls.sni

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
sni&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json'  -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.sni\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET
```

```
[{
   "key": "mediaterki.com",
   "doc_count": 32
}, {
   "key": "scotiation.pw",
   "doc_count": 28
}, {
   "key": "api.ip.sb",
   "doc_count": 3
}]
```


tls.subject

Basic query on tls.subject

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
subject&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output


```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.subject\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -
H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "C=US, ST=NC, O=detracting exploitation's, OU=really
preemption, CN=incision's.com",
   "doc_count": 60
}, {
   "key": "C=GB, ST=London, L=London, O=Global Security, OU=IT
Department, CN=example.com",
   "doc_count": 51
```

```
}, {
   "key": "OU=Domain Control Validated, OU=ShinoSaki DV,
CN=api.ip.sb",
   "doc_count": 3
}]
```

tls.issuerdn

Basic query on tls.issuerdn

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
issuerdn&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.issuerdn\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "C=US, ST=NC, O=detracting exploitation's, OU=really
preemption, CN=incision's.com",
   "doc_count": 60
}, {
   "key": "C=GB, ST=London, L=London, O=Global Security, OU=IT
Department, CN=example.com",
   "doc_count": 51
}, {
   "key": "C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA
Limited, CN=COMODO RSA Domain Validation Secure Server CA",
   "doc_count": 3
}]
```

tls.fingerprint

Basic query on tls.fingerprint

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
fingerprint&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id>
-H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.fingerprint\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=
91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key":
"a5:6a:f2:33:b0:c4:57:d0:bc:dc:a5:a5:ac:08:4b:67:d7:38:e3:ff",
   "doc_count": 60
}, {
   "key":
"b9:bb:88:11:da:eb:c4:84:05:c0:b7:65:83:f1:60:1d:90:d8:a7:2f",
   "doc_count": 18
}, {
   "key":
"33:a5:f9:37:f6:aa:47:39:52:9a:59:53:36:86:0c:1e:3b:8b:42:ca",
   "doc_count": 15
}, {
   "key":
"84:ca:90:98:e1:c7:f5:f2:a8:e2:33:b4:7d:fa:3f:1d:67:7c:64:72",
   "doc_count": 9
}, {
   "key":
"db:d9:25:71:83:0f:ae:ef:b4:5d:78:cc:42:ce:6b:13:06:23:ef:72",
   "doc_count": 9
```

```
}, {
   "key":
"3a:45:a5:f2:64:df:3a:8c:8a:22:f1:92:02:3a:c9:76:90:d2:13:16",
   "doc_count": 3
}]
```

tls.ja3.hash

Basic query on tls.ja3.hash

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
ja3.hash&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.ja3.hash\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

   [{
      "key": "6734f37431670b3ab4292b8f60f29984",
      "doc_count": 68
  }, {
      "key": "1d095e68489d3c535297cd8dffb06cb9",
      "doc_count": 63
  }]
```

tls.ja3.agent

Basic query on tls.ja3.agent

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
ja3.agent&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.ja3.agent\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

  [{
      "key": "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0",
      "doc_count": 68
  }, {
      "key": "User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.2; .NET CLR 1.0.3705",
      "doc_count": 63
  }]
```

tls.ja3s.hash

Basic query on tls.ja3s.hash

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=tls.
ja3s.hash&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json'  -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=tl
s.ja3s.hash\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
```

```
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

[{
   "key": "4192c0a946c5bd9b544b4656d9f624a4",
   "doc_count": 60
}, {
   "key": "623de93db17d313345d7ea481e7443cf",
   "doc_count": 51
}, {
   "key": "8ca430f840a9e4501ec08479c0bc714c",
   "doc_count": 3
}]
```

smtp.mail_from

Basic query on smtp.mail_from

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smtp
.mail_from&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -
H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
tp.mail_from\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=9
1 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

[{
   "key": "<mrikglck@rkts.com>",
   "doc_count": 2
}]
```

```
```

smtp.rcpt_to

Basic query on smtp.rcpt_to

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smtp
.rcpt_to&from_date=<start_date>&to_date=<end_date> -H 'Authorization:
Token <token>' -H 'Content-Type: application/json'  -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
tp.rcpt_to\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
-H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json'  -X GET

[{
   "key": "<info@audioschematics.dk>",
   "doc_count": 2
}]
```

smtp.helo

Basic query on smtp.helo

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smtp
.helo&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
tp.helo\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "rkts.com",
   "doc_count": 2
}]
```

smb.command

Basic query on smb.command

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smb.
command -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
b.command\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -
H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "SMB2_COMMAND_TREE_CONNECT",
   "doc_count": 2
},
{
   "key": "SMB2_COMMAND_WRITE",
   "doc_count": 2
}]
```

smb.status

Basic query on smb.status

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smb.
status&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
b.status\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
   "key": "STATUS_SUCCESS",
   "doc_count": 2
}]
```

smb.filename

Basic query on smb.filename

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smb.
filename&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
b.filename\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91
```

```
-H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X
GET

[{
   "key": "temp\\mimikatz.exe",
   "doc_count": 2
}]
```

smb.share

Basic query on smb.share

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=smb.
share&from_date=<start_date>&to_date=<end_date> -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=sm
b.share\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET

[{
   "key": "",
   "doc_count": 2
},
{
   "key": "\\\\10.230.33.21\\agerasfiles",
   "doc_count": 2
}]
```

ssh.client.software_version

Basic query on `ssh.client.software_version`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=ssh.
client.software_version&from_date=<start_date>&to_date=<end_date> -H
'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ss
h.client.software_version\&from_date\=1634657760979\&to_date\=16372497609
79\&tenant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "libssh-0.1",
   "doc_count": 2
}]
```

ssh.server.software_version

Basic query on `ssh.server.software_version`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=ssh.
server.software_version&from_date=<start_date>&to_date=<end_date>&tenant=
<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ssh.server.software_version\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET

[{
   "key": "OpenSSH_6.4",
   "doc_count": 2
}]
```

hostname_info.subdomain

Basic query on `hostname_info.subdomain`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=hostname_info.subdomain&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=hostname_info.subdomain\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type: application/json' -X GET

[{
   "key": "api",
   "doc_count": 4
}]
```

hostname_info.domain

Basic query on `hostname_info.domain`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=host
name_info.domain&from_date=<start_date>&to_date=<end_date>&tenant=<tenant
_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ho
stname_info.domain\&from_date\=1634657760979\&to_date\=1637249760979\&ten
ant\=91 -H 'Authorization: Token
a877cafd50dc434574aebd8d7385f0fa9925e950' -H 'Content-Type:
application/json' -X GET

[{
   "key": "5.45.74.250",
   "doc_count": 35
}, {
   "key": "mediaterki.com",
   "doc_count": 32
}, {
   "key": "scotiation.pw",
   "doc_count": 32
}, {
   "key": "190.146.112.216",
   "doc_count": 12
}, {
   "key": "46.249.62.199",
   "doc_count": 10
}, {
   "key": "70.184.86.103",
   "doc_count": 8
}, {
   "key": "133.242.164.31",
```

```
    "doc_count": 4
}, {
    "key": "ip.sb",
    "doc_count": 4
}, {
    "key": "aucklandluxuryrealestatelistings.com",
    "doc_count": 3
}, {
    "key": "104.228.227.210",
    "doc_count": 2
}]
```


hostname_info.tld

Basic query on `hostname_info.tld`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=host
name_info.tld&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_id
> -H 'Authorization: Token <token>' -H 'Content-Type: application/json' -
X GET
```

Example Usage and Query Output


```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ho
stname_info.tld\&from_date\=1634657760979\&to_date\=1637249760979\&tenant
\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -
H 'Content-Type: application/json' -X GET

[{
    "key": "com",
    "doc_count": 36
}, {
    "key": "pw",
    "doc_count": 32
}, {
```

```
    "key": "sb",
    "doc_count": 4
}]
```

hostname_info.domain_without_tld

Basic query on `hostname_info.domain_without_tld`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=host
name_info.domain_without_tld&from_date=<start_date>&to_date=<end_date>&te
nant=<tenant_id> -H 'Authorization: Token <token>' -H 'Content-Type:
application/json' -X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=hostname_i
nfo.domain_without_tld\&from_date\=1634657760979\&to_date\=1637249760979\&tenant\
=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950' -H
'Content-Type: application/json' -X GET

[{
    "key": "5.45.74.250",
    "doc_count": 35
}, {
    "key": "mediaterki",
    "doc_count": 32
}, {
    "key": "scotiation",
    "doc_count": 32
}, {
    "key": "190.146.112.216",
    "doc_count": 12
}, {
    "key": "46.249.62.199",
    "doc_count": 10
```

```
}, {
   "key": "70.184.86.103",
   "doc_count": 8
}, {
   "key": "133.242.164.31",
   "doc_count": 4
}, {
   "key": "ip",
   "doc_count": 4
}, {
   "key": "aucklandluxuryrealestatelistings",
   "doc_count": 3
}, {
   "key": "104.228.227.210",
   "doc_count": 2
}]
```

hostname_info.host

Basic query on `hostname_info.host`

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/?field=host
name_info.host&from_date=<start_date>&to_date=<end_date>&tenant=<tenant_i
d> -H 'Authorization: Token <token>' -H 'Content-Type: application/json'
-X GET
```

Example Usage and Query Output

```
curl -k
https://stamus.security.platform.ip/rest/rules/es/field_stats/\?field\=ho
stname_info.host\&from_date\=1634657760979\&to_date\=1637249760979\&tenan
t\=91 -H 'Authorization: Token a877cafd50dc434574aebd8d7385f0fa9925e950'
-H 'Content-Type: application/json' -X GET

[{
   "key": "198.12.71.157",
   "doc_count": 468
```

```
},
{
  "key": "c54rng3686.com",
  "doc_count": 46
},
{
  "key": "cclaudeq19.top",
  "doc_count": 34
},
{
  "key": "170.238.117.187",
  "doc_count": 33
},
{
  "key": "94.140.125.34",
  "doc_count": 30
},
{
  "key": "5.188.168.49",
  "doc_count": 18
},
{
  "key": "bh44meamelie.xyz",
  "doc_count": 6
},
{
  "key": "germakhya.xyz",
  "doc_count": 6
},
{
  "key": "api.ip.sb",
  "doc_count": 4
},
{
  "key": "myexternalip.com",
  "doc_count": 3
}]
```

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

