Infoblox Dossier Calls Reference

Dossier API Guide

06/16/2021

Table of Contents

Dossier API Services

GET tide/api/services/intel/lookup/targets

Returns a list of indicator types.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/targets'
\ --header 'Authorization: Token <key>'
```

Response:

```
[
        "ip",
        "host",
        "url",
        "hash",
        "email"
]
```

GET tide/api/services/intel/lookup/sources

Returns a list of Dossier sources.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/sources'
\ --header 'Authorization: Token <key>'
```

Response:


```
{
        "alexa": true,
        "atp": true,
        "ccb": true,
        "dns": true,
        "gcs": true,
        "geo": true,
        "gsb": true,
        "isight": true,
        "malware_analysis": true,
        "pdns": true,
        "ptr": true,
        "rlabs": false,
        "rwhois": false,
        "sdf": false,
        "whois": true,
        "inforank": true,
        "malware_analysis_v3": true,
        "activity": true,
        "rpz_feeds": true,
        "custom_lists": true,
        "whitelist": true,
        "infoblox_web_cat": true
}
```

GET tide/api/services/intel/lookup/sources/target/{target_type}

Returns sources that support queries for an indicator type.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/
sources/target/ip' \ --header 'Authorization: Token <key>'
```

Response:


```
{
        "activity": true,
        "atp": true,
        "ccb": true,
        "custom_lists": true,
        "gcs": true,
        "geo": true,
        "isight": true,
        "malware_analysis": true,
        "malware_analysis_v3": true,
        "pdns": true,
        "ptr": true,
        "rpz_feeds": true,
        "whitelist": true,
        "whois": true
}
```

GET tide/api/services/intel/lookup/source/{source}/targets

Return a list of indicator types supported by a given source.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/source/at
p/targets' \ --header 'Authorization: Token <key>'
```

Response:

```
[
    "email",
    "hash",
    "host",
    "ip",
    "url"
]
```

GET tide/api/services/intel/lookup/sources/target/{target_type}

Required parameters:
Value: The indicator to search for.
Source: The source to search.
Multiple sources can be specified. If no source is specified, the call will search on all sources.

Optional parameters:
Wait: whether to wait for the lookup to complete – true or false [defaults to false].

Start a new Dossier lookup job for a specified indicator and source(s).

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/
indicator/host?value=google.com&source=alexa&source=dns&wait=f
alse' \ --header 'Authorization: Token <key>'
```

Response:


```
{
       "status": "pending",
       "job_id": "aef7e05a-42c6-45f2-9be4-02139caf31a4",
       "job": {
           "id": "aef7e05a-42c6-45f2-9be4-02139caf31a4",
           "state": "created",
           "status":"pending",
           "create_ts":1501802999664,
           "create_time": "2017-08-03T23:29:59.664186262Z",
           "pending_tasks": [
               "8e4d8ac5-9772-42f6-8644-0a23fb509870",
               "6c19c40f-c5c6-4d89-b099-e92b036e92d5"
           ],
           "org": "org",
           "user": "user@test.com"
      },
      "tasks": {
          "6c19c40f-c5c6-4d89-b099-e92b036e92d5": {
             "id": "6c19c40f-c5c6-4d89-b099-e92b036e92d5",
             "state": "created",
             "status": "pending",
             "create_ts": 1501802999664,
             "create_time": "2017-08-03T23:29:59.664186262Z",
             "params": {
                "type":
                "host",
```

```
                "target": "google.com",
                "source": "dns"
            }
        },
        "8e4d8ac5-9772-42f6-8644-0a23fb509870": {
            <status>
        }
    }
}
```

GET tide/api/services/intel/lookup/jobs/{job_id}

Returns status of a Dossier lookup job.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/jobs/aef7e05
a-42c6-45f2-9be4-02139caf31a4' \ --header 'Authorization: Token
<key>'
```

Response:

```
{
      "status": "success",
      "job_id": "aef7e05a-42c6-45f2-9be4-02139caf31a4",
      "job": {
           "id": "aef7e05a-42c6-45f2-9be4-02139caf31a4",
           "state": "completed",
           "status": "success",
           "create_ts": 1501802999664,
           "create_time": "2017-08-03T23:29:59.664Z",
           "completed_tasks": [
              "8e4d8ac5-9772-42f6-8644-0a23fb509870",
              "6c19c40f-c5c6-4d89-b099-e92b036e92d5"
           ],
           "org": "org",
           "user": "user@test.com"
      },
      "tasks": {
           "6c19c40f-c5c6-4d89-b099-e92b036e92d5": {
           "id": "6c19c40f-c5c6-4d89-b099-e92b036e92d5",
           "state":"completed",
           "status": "success",
           "create_ts": 1501802999664,
           "create_time": "2017-08-03T23:29:59.664Z",
           "start_ts": 1501802999908,
           "start_time": "2017-08-03T23:29:59.908Z",
           "end_ts": 1501802999960,
           "end_time": "2017-08-03T23:29:59.96Z",
           "params": {
                "type":"host",
                "target": "google.com",
                "source": "dns"
           }
      },
      "8e4d8ac5-9772-42f6-8644-0a23fb509870": {
           <status>
        }
    }
}
```

GET tide/api/services/intel/lookup/jobs/{job_id}/results

Returns results of a Dossier lookup job.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/jobs/aef7
e05a-42c6-45f2-9be4-02139caf31a4/results' \ --header
'Authorization: Token <key>'
```

Response:

```
{
        "state": "completed",
        "status": "success",
        "job_id": "aef7e05a-42c6-45f2-9be4-02139caf31a4",
        "results": [
             {
                  "task_id": "8e4d8ac5-9772-42f6-8644-0a23fb509870",
                  "params": {
                       "type": "host",
                       "target": "google.com",
                       "source": "alexa"
                  },
                  "v": "3.0.0",
                  "status": "success",
                  "data": {
                      <data>
                  }
    },
    {
        "task_id": "6c19c40f-c5c6-4d89-b099-e92b036e92d5",
        "params": {
        "type": "host",
        "target": "google.com",
        "source": "dns"
     },
     "v": "2.0.0",
     "status": "success",
     "time": 25,
     "data": {
          <data>
     }
    }
  ]
}
```

GET tide/api/services/intel/lookup/jobs/{job_id}/tasks/{task_id}

Returns status of a single task in a Dossier lookup job.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/jobs/aef
7e05a-42c6-45f2-9be4-02139caf31a4/tasks/6c19c40f-c5c6-4d89-b099-
e92b036e92d5' \ --header 'Authorization: Token <key>'
```

Response:


```
{
      "state":
      "completed",
      "status": "success",
      "task": {
          "id": "6c19c40f-c5c6-4d89-b099-e92b036e92d5",
          "state":  "completed",
          "status": "success",
          "create_ts": 1501802999664,
          "create_time": "2017-08-03T23:29:59.664Z",
          "start_ts": 1501802999908,
          "start_time": "2017-08-03T23:29:59.908Z",
          "end_ts": 1501802999960,
          "end_time": "2017-08-03T23:29:59.96Z",
          "params": {
              "type": "host",
              "target": "google.com",
              "source": "dns"
           }
     }
}
```

GET tide/api/services/intel/lookup/jobs/{job_id}/tasks/{task_id}/result

Returns results of a single task in a Dossier lookup job.

Example:

```
curl --location --request GET
'https://csp.infoblox.com/tide/api/services/intel/lookup/jobs/aef
7e05a-42c6-45f2-9be4-02139caf31a4/tasks/6c19c40f-c5c6-4d89-b099-
e92b036e92d5/results' \ --header 'Authorization: Token <key>'
```

Response:

```
{
    "state":
    "completed",
    "status":
    "success",
    "results": {
        "task_id": "6c19c40f-c5c6-4d89-b099-e92b036e92d5",
        "params": {
           "type": "host",
           "target": "google.com",
           "source": "dns"
     },
     "v": "3.0.0",
     "status":
     "success", "time": 25,
     "data": {
     <data>
     }
   }
}
```

Dossier Data Provider Services

Dossier aggregates threat data from multiple partners in order to generate a full report. The following sections will provide a brief description of what information is retrieved and display the expected return data from each Dossier provider in JSON format. Key names are what can be expected in request response, and the key's value is the data type that can be expected.

Activity

The Activity worker provides information regarding security events on a customer's network for either hosts or IPs. This includes hits against customer custom lists and policies.

Data Structure:

```
{
    "results": {
        "dns": [
            {
                "type": string
                "timestamp": string
                "qname": string
                "opcode": string
                "rcode": string
                "response": string
                "qip": string
                "policy_id": string
                "device_name": string
                "user": string
                "network": string
                "query_type: string
            },...
        ],
        "security: [
            {
                "type": string
                "timestamp": string
                "qname": string
                "opcode": string
                "qip": string
                "policy_id": string
                "severity": string
                "tclass": string
                "tproperty": string
                "confidence": string
                "feed_name": string
                "feed_type": string
                "device_name": string
                "user": string
                "network": string
                "country": string
                "policy_name": string
```

```
                        "policy_action": string
                        "query_type: string
                    },...
                ]
            }
        }
```

Example:
Given an indicator of "google.com", Activity will return the following:

```
{
    "results": {
        "dns": [
            {
                "type": "1",
                "timestamp": "1595868534"
                "qname": "google.com,
                "opcode": "0",
                "rcode": "0",
                "response": "172.253.63.139",
                "qip": "22.123.32.33"
                "policy_id": "288337"
                "device_name": "22.123.32.33",
                "user": "unknown",
                "network": "test_net",
                "query_type: "A"
            },...
        ],
        "security: [
            {
                "type": "2",
                "timestamp": "1595868603",
                "qname": "google.com.",
                "opcode": "0",
                "qip": "22.123.32.33"
                "policy_id": "288337",
                "severity": "Low",
                "tclass": "Low",
                "tproperty": "dummy",
                "confidence": "High",
                "feed_name": "dummy",
                "feed_type": "FQDN",
                "device_name": "22.123.32.33",
                "user": "unknown",
                "network": "test_net",
                "country": "unknown",
                "policy_name": "test_pol",
                "policy_action": "Block",
                "query_type: "A"
            },...
        ]
    }
}
```

Alexa

Alexa provides a ranking for a domain name based on traffic. Alexa can currently provide rankings for the top 100,000 hostnames.

Data Structure:

```
{
    "details": {
        "adult_content": string,
        "description": string
        "links_in_count": integer,
        "owned_domains": [string],
        "rank": integer
    },
    "match": bool
}
```

Example:

Given an indicator of “google.com”, Alexa returns the following:

```
{
    "details": {
          "adult_content": “no”,
          "description": "Enables users to search the world's
information, including webpages, images, and videos. Offers unique
features and search technology.",
          "links_in_count": 1300441,
          "owned_domains": ["google.com"],
          "rank": 1
    },
    "match": true
}
```

ATP (Active Trust Platform)

ATP provides a list of reported threats associated with the indicator from the Active Trust Platform.

Data Structure:

```
{
      "record_count": integer,
      "threat": [
            {
                "batch_id": string,
                "class": string,
                "detected": string,
                "domain": string,
                "host": string,
                "id": string,
                "imported": string,
                "ip": string,
                "origin": string,
                "profile": string,
                "property": string,
                "received": string,
                "target": string,
                "threat_level": integer,
                "tld": string,
                "tlp": string,
                "type": string,
                "up": string,
                "url": string,
                "extended": {
                      "url_hash": string ...
                      ...
                 ],
           },...
       ],
        "threat_actor": {
             "name": string,
             "references": [string],
             "region": string,
             "targets": string
       }
 }
```

Example:
Given an indicator of “eicar.co”, ATP returns the following:


```
{
      “record_count”: 19,
      “threat”: [
            {
                “batch_id”: "88ab7b07-2b66-11eb-b7eb-fbf8622dd134",
                “class”: "Spambot",
                “"detected": "2013-05-05T10:36:44.000Z",
                "dga": "false",
                "domain": "eicar.co"
                "extended": {
                     "threat_actor": "APT38"
                }
                "host": "eicar.co",
                "id": "88ac6568-2b66-11eb-b7eb-fbf8622dd134",
                "imported": "2020-11-20T19:28:14.458Z",
                "profile": "IID",
                "property": "Spambot_Cutwail",
                "received": "2020-11-20T19:28:14.458Z",
                "threat_level": 100,
                "tld": "co",
                "type": "HOST",
                "up": "true"
           },...
        ],
         “threat_actor”: {
               "name": "APT38",
               "references": [
                     "https://www.fireeye.com/blog/threat-
                    research/2018/10/apt38-details-on-new-north-korean-
                    regime-backed-threat-group.html"
                ],
                “region”: “North Korea”
                “targets”: "Media, government, but mainly financial
               institutions in order to raise money for the North
               Korean regime: Russia, Turkey, US, Poland, Mexico,
               Brazil, Uruguay, Taiwan, Malaysia, Chile, Vietnam,
               Philippines"
         }
}
```

CCB (Cyber Campaign Briefs)

The Infoblox Cyber Intelligence team ATP produces weekly Cyber Campaign Briefs (CCBs), a short write-up that a watch desk analyst writes about an interesting or notable threat campaign. This source returns a list of reports that a given indicator appears in.

Data Structure:

```
{
  "reports": [
     {
              "document_id": string,
              "id": string,
              "indicators": [
                   {
                          "description": string,
                          "id": string,
                          "indicator": string,
                          "indicator_type": string,
                   },
          ],
          "keyword": [string],
          "overview": string,
          "publish_date": string,
          "title": string
        }
    ]
}
```

Example:

Given an indicator of "185.117.89.145", CCB returns the following:

```
{
  "reports": [
     {
              "document_id": "CCB-2019-50",
              "id": "1a8f258a-0df9-43ec-918d-a7927a83b630",
              "indicators": [
                   {
                          "description": "FlawedAmmyy C2 IP",
                          "id": "27d08fe5-fe62-4824-9a29-
                            47addedb77f4",
                          "indicator": "185.117.89.145",
                          "indicator_type": "ip",
                   },
                   {
                          "description": "FlawedAmmyy C2 IP",
                          "id": "8689c812-aa6e-4b02-bb0f-
                            388c931d8796",
                          "indicator": "185.117.89.145",
```

```
                        "indicator_type": "ip",
                    },
            ],
            "keyword": [
                   "AndroMut",
                   "FlawedAmmyy",
                   "RAT",
                    "TA50",
                   "South Korea",
                   "U.A.E.",
                   "U.S.",
                   "Andromeda",
                   "Gamarue",
                   "mutshellmy777",
                   "Ammyy Admin",
                   "Invoice",
                   "financial quote"
            ],
            "overview": "From 22 to 24 July, we observed a malicious email
            campaign distributing the new AndroMut downloader, which in
            turn dropped the FlawedAmmyy remote access trojan
            (RAT).Proofpoint attributed the campaign to threat actor
            TA505, which they assess is also linked to other
            Prevalent malware such as the Dridex banking trojan, Locky
            ransomware, and Jaff ransomware.",
           "publish_date": "2019-08-07T00:00:00Z",
           "title": "Cyber Campaign Brief: AndroMut Drops FlawedAmmyy"
           }
    ]
}
```

Custom Lists

The Custom Lists Dossier Worker returns matching customer custom lists for a given indicator

Data Structure

```
{
      "results": {
            "indicator": [
                  {
                        "confidence_level": string,
                        "created_time": string,
                        "description": string,
                        "id": int,
                        "item_count": int,
                        "name": string,
                        "policies": [string],
                        "threat_level": string,
                        "type": string,
                        "updated_time": string
                  }
            ]
      }
}
```

Example:
Given "moiparks.in" is used as an indicator, Custom Lists returns the following:

```
{
      "results": {
            "moiparks.in": [
                  {
                        "confidence_level": "HIGH",
                        "created_time": "2020-01-09T05:23:56Z",
                        "description": "",
                        "id": 634638,
                        "item_count": 2,
                        "name": "Henry's List",
                        "policies": [],
                        "threat_level": "LOW",
                        "type": "custom_list",
                        "updated_time": "2020-05-19T21:11:16Z"
                        }
                  ]
      }
}
```

DNS

The DNS API call returns DNS information for a hostname.

Data Structure:

```
{
    “A”: [
          {
             “ip”: string,
             “reverse”: string,
             “ttl”: integer
          },...
    ],
    “AAAA”: [string],
    “CERT”: [string],
    “CNAME”: [string],
    “HTTPS”: [string],
    “MX”: [string],
    “NS”: [string],
    “SOA”: [string],
    “SVCB”: [string],
    “TSIG”: [string],
    “TXT”: [string],
    “rcode”: string
}
```

Example:

Given an indicator of “eicor.co”, DNS returns the following:

```
{
    “A”: [
          {
             "ip": "72.52.178.23",
              "reverse": "lb01.parklogic.com.",
              "ttl": 14399
          },...
    ],
    “AAAA”: [],
    “CERT”: [],
    “CNAME”: [],
    “HTTPS”: [],
    “MX”: [
          "10 mx156.hostedmxserver.com."
    ],
    “NS”: [
          "ns2.parklogic.com.",
          "ns1.parklogic.com."
    ]
    “SOA”:
       "ns1.parklogic.com. hostmaster.eicar.co. 2021052101
    3600 7200 1209600 3600"
    “SVCB”: [],
    “TSIG”: [],
```

```
    "TXT": [
         "\"v=spf1"],
    "rcode": "NOERROR"
}
```

GCS (Global Custom Search)

The GCS API call returns the results of a customized Bing search on the indicator.

Data Structure:

```
{
        “items”: [
              {
                    “displayURL”: string,
                    “link”: string,
                    “snippet”: string,
                    “title”: string
              },...
        ]
}
```

Example:
Given an indicator of “op.ggmoiparks.in”, GCS will return the following:

```
{
        "items": [
              {
                     "displayURL":
              "https://www.hybrid-
              analysis.com/sample/8a0163a269a7c
              c64547e471c6668ae10f2903340d3bf5a
              801cd71ef9e2ef20e0/5fddd83ceaeabd
              3be759eb53",
                     "link": "https://www.hybrid-
              analysis.com/sample/8a0163a269a7cc
              64547e471c6668ae10f2903340d3bf5a80
              1cd71ef9e2ef20e0/5fddd83ceaeabd3be
              759eb53",
                     "snippet": "Submit malware
                     for free analysis with Falcon
                     Sandbox and Hybrid Analysis
                     technology. Hybrid Analysis
                     develops and licenses analysis
                     tools to fight malware.",
                     "title": "Free Automated Malware
                     Analysis Service - powered by ..."
                     },...
              ]
}
```

GeoIP

The GeoIP API call returns information about the geographical location of an IP address.

Data Structure:

```
{
     “as_num”: string,
     “city”: string,
     “country_code”: string,
     “country_name”: string,
     “isp”: string,
     “latitude”: number,
     “longitude”: number,
     “org”: string,
     “postal_code”: string,
     “region”: string
    }
```

Example:

Given an indicator of “45.63.119.161”, GeoIP returns the following:

```
{
     "asn_num": "(20473,
     "city": "Frankfurt am Main",
     "country_code": "DE",
     "country_name": "Germany",
     "isp": "AS-CHOOPA",
     "latitude": 50.0971,
     "longitude": 8.5952,
      "org": "Choopa, LLC",
      "postal_code": "65933",
      "region": "Hesse"
}
```

GSB (Google Safe Browsing)

The GSB API call provides threat information for a given indicator from Google's Web Risk API.

Data Structure:

```
{
        "threat": {
            "threatTypes": [string],
            "expireTime": string
        }
}
```

Example:

```
{
        "threat": {
            "threatTypes": [
              "MALWARE"
            ],
            "expireTime": "2019-07-17T15:01:23.045123456Z"
        }
}
```

iSight

The iSight API call provides threat information for a given indicator.

Data Structure:

```
{
  "match": bool,
  "response": [
   {
    "summary": { "ThreatScape": [string],
    "publishDate": integer,
    "reportId": string,
     "title": string
     },
    "details": {
    "abstract": string,
    "analysis": string,
    "copyright": string,
    "execSummary": string,
    "publishDate": string,
    "reportId": string,
    "riskRating": string,
    "title": string,
       "version": string,
       "tagSection": {
          "networks": {
          "network": [
           {
           "domain": string,
           "identifier": string,
           "ip": string,
           "networkType": string
          },
          …
         ],
          "main": {
            "affectedIndustry": [string],
            "affectedSystems": {
            "affectedSystem": [string]
            },
            "impacts": {
             "impact": [string]
            },
            "intendedAudiences": {
            "intendedAudience": [string]
            },
            "ttps": {
            "ttp": [string]
            }
      }
    }
```

```
    }
}
```


Example:
Given an indicator like “"http://moiparks.in/bubu/file.exe” is used, iSight will return the following:


```
{
  “match”: true,
  “response”: [
   {
    “details”: {
     “ThreatScape”: {
       "product": [
        "ThreatScape Cyber Crime"
     ]
    },
    "abstract": "\u003cp\u003eThe Pony (aka Fareit) tool
    is a generic platfor…", "copyright": "©
    Copyright  2017 FireEye, Inc. All rights
    reserved.",
    "execSummary": "\u003cp\u003eThe Pony (aka
     Fareit)  tool is a generic …", "publishDate": "June
     15, 2016  08:36:00 AM",
    "reportId": "16-00009344",
    "riskRating": "LOW", "tagSection": {
       "files": {
       "file": [
    {
     "fileName": "UNAVAILABLE",
     "identifier": "Attacker",
      "md5": "f53631c1641461cbffbd3ca598f3aee7",
      "sha1":
       "3e207d750f0761631db2027dba778e411069c1f2",
       "sha256":
       "c89da29e589f8680486e10ef8ed81b7d3150b0df
        acbc8de4ac90fcf43f06d00a"
    }],
    "title": "Indicator Report: Pony Activity Report
    (June 8 to 15, 2016)",
    "version": "1"
    },
    "summary": {
    "ThreatScape": [
    "Cyber Crime"
    ],
    "publishDate": 1465997760,
    "reportId": "16-00009344",
```

```
        "title": "Indicator Report: Pony Activity Report
        (June 8 to 15, 2016)"
        }
}
```

Infoblox Web Category

The Infoblox Web Category Dossier worker provides categorization for a given indicator.

Data Structure:

```
{
    "results": [
            {
                    "description": string,
                    "id": string,
                    "name": string
            },
      ]
 }
```

Example:
Given “op.gg” is used as an indicator, Infoblox Web Category returns the following:

```
{
    "results": [
            {
                "description": "Covers cheat codes, tips,
             tricks and information on roleplaying games
             (RPG). Can be combined with any other Hobbies
             and Interests categories. Examples are MMORPG,
             live action RPG, multi-user Dungeon etc.",
                    "id": "10260",
                    "name": "Roleplaying Games"
            },
            {
                "description": "Web sites that provide
             guide, cheats, tricks, walkthroughs and other
             related fields of video and computer games.
             Can be paired with a specific Sports category
             Relating to Sports Fantasy Games. If gambling
             with money, pair it with Gambling category.
             Can be combined with any other Hobbies and
             Interests categories. Examples are arcade
             game, video games, nintendo etc.",
                     "id": "10266",
                     "name": "Video and Computer
             Games"
            }
     ]
 }
```

InfoRank

The InfoRank worker returns the ranking of a host indicator in the Infoblox curated InfoRank list. The InfoRank list provides the most popular second-level domains (SLDs) updated each day from an aggregated dataset based on DNS records from various data sources. The process to determine the rank for each domain uses count information in combination with statistical inference techniques to accurately estimate the SLDs' true ranks over time. The api reports top and bottom bracket of where this indicator historically will fall. For example, cbsnews.com will normally fall between 687 and 813. If a site suddenly became number 100 and its normally 10,000, then this should be considered an anomaly and investigated further.

Data Structure:

```
{
    "domain": string,
    "interval":
    string, "rank":
    integer
}
```

Example:
Given an indicator of "google.com", InfoRank will return the following:

```
{    "domain":
     "google.com",
     "interval":       "[39,
     40]", "rank": 39
}
```

Malware Analysis

The Malware Analysis API call provides threat reports on an indicator generated by Malware Analysis.

Data Structure:

```
{
      "match": bool,
      "details": {
       "as_owner": string,
       "asn": string,
       "country": string,
       "response_code":
       integer, "verbose_msg":
       string, "detected_urls":
       [
        {
         "scan_date":
         string, "url":
         string,
         "positives":
         integer,
         "total": integer
        },
        …
       ],
       "resolutions": [
        {
         "hostname": string,
         "last_resolved": string
        },
        …
       ],
       "resolutions": [
        {
         "hostname": string,
         "last_resolved": string
        },
        …
       ],
       "detected_communicating_samples": [
        {
         "date": string,
         "positives":
         integer,
         "sha256": string,
         "total": integer
        },
        …
       ],
       "undetected_communicating_samples: [
        {
```

```
            "date": string,
            "positives": integer,
            "sha256": string,
            "total": integer
           },
           …
          ],
          "detected_download_samples: [
           {
            "date": string,
            "positives": integer,
            "sha256": string,
            "total": integer
           },
           …
          ],
          "undetected_download_samples: [
           {
            "date": string,
            "positives": integer,
            "sha256": string,
            "total": integer
           },
           …
          ],
          "undetected_referrer_samples: [
           {
            "positives": integer,
            "sha256": string,
            "total": integer
           },
           …
          ],
         }
        }
```


Example:
Given “moiparks.in” is used as an indicator, Malware Analysis will return the following:


```
{
 "details": {
       "BitDefender domain info": "This URL domain/host was
  seen to host badware at some point in time",
       "alphaMountain.ai category": "Malicious",
       "detected_communicating_samples": [
           {
               "date": "2019-10-06 23:27:39",
               "positives": 42,
               "sha256":
           "6cd6abeccf5e7f8507d209eafb8a1a77f2bd4fe679dd633725759f
           0a7385500c",
               "total": 73
           }
       ],
```

```
        "detected_downloaded_samples": [],
        "detected_urls": [
             {
                   "positives": 1,
                   "scan_date": "2021-04-08 01:27:26",
                   "total": 85,
                   "url": "https://moiparks.in/jack/admin.php"
              },...
        ],
        "domain_siblings": [],
        "resolutions": [
             {
                  "ip_address": "198.54.117.200",
                  "last_resolved": "2018-09-26 17:02:16"
             },...
        ],
        "response_code": 1,
        "subdomains": [
             "www.moiparks.in"
        ],
        "undetected_communicating_samples": [],
        "undetected_downloaded_samples": [
              {
                  "date": "2018-09-14 02:52:35",
                  "positives": 0,
                  "sha256":
        "21f2049d5b7a94430621acbc5f6c467c134d368a2c69a8283cc08b1f61
        83962c",
                  "total": 57
              },...
                  ],
              "undetected_urls": [],
              "verbose_msg": "Domain found in dataset",
              "whois": "",
              "whois_timestamp": 1600070810
        },
        "match": true
}
```

Malware Analysis v3

The Malware Analysis v3 API call provides threat reports on an indicator generated by Malware Analysis.

Data Structure:

```
{
      "data": {
            "attributes": {},
            "communicating_files": [],
            "downloaded_files": [],
            "id": string,
            "links": {},
            "referrer_files": [],
            "resolutions": [],
            "siblings": [],
            "subdomains": [],
            "type": string,
            "urls": []
      }
}
```

Example:
Given an indicator of “moiparks.in”, Malware Analysis v3 will return the following:

```
{
      "data": {
            "attributes": {
                  "categories": {
                        "alphaMountain.ai": "Malicious"
                        },
                        "last_analysis_results": {
                        "ADMINUSLabs": {
                              "category": "harmless",
                              "engine_name": "ADMINUSLabs",
                              "method": "blacklist",
                              "result": "clean"
                              },...
                        },
                        "last_analysis_stats": {
                        "harmless": 71,
                        "malicious": 4,
                        "suspicious": 1,
                        "timeout": 0,
                        "undetected": 9
                        },
                        "last_dns_records": [],
                        "last_modification_date": 1617845258,
                        "popularity_ranks": {},
                        "reputation": 0,
                        "tags": [],
                        "total_votes": {
                        "harmless": 0,
                        "malicious": 0
                        },
                        "whois": "",
                        "whois_date": 1600070810
```

```
},
"communicating_files": [
{
      "attributes": {
      "capabilities_tags": [],
      "downloadable": true,
      "exiftool": {
            "FileType": "RTF",
            "FileTypeExtension": "rtf",
            "MIMEType": "text/rtf"
            },
            "first_seen_itw_date":
      1465386294,
            "first_submission_date":
      1465386468,
            "last_analysis_date":
      1620122891,
            "last_analysis_results": {
            "ALYac": {
                  "category": "malicious",
                  "engine_name": "ALYac",
                  "engine_update":
            "20210504",
                  "engine_version":
            "1.1.3.1",
                  "method": "blacklist",
                  "result": "Trojan.RTF-COM-
            Dropper.Gen"
                  },...
            },
            "last_analysis_stats": {
            "confirmed-timeout": 0,
            "failure": 0,
            "harmless": 0,
            "malicious": 37,
            "suspicious": 0,
            "timeout": 0,
            "type-unsupported": 15,
            "undetected": 23
            },
            "last_modification_date":
      1620130159,
            "last_submission_date":
      1526341830,
            "magic": "Rich Text Format data,
      version 1, unknown character set",
            "md5":
      "11c4c7cc2bbab51f6353ecbab4a34d68",
            "meaningful_name": "SOA \u0026
      payment copy.doc",
            "names": [
            "SOA \u0026 payment copy.doc",
            "SOA",
            "sourcedoc1$"
            ],
            "packers": {
```

```
      "F-PROT": "appended"
      },
      "popular_threat_classification":
{
      "popular_threat_category": [
            {
                  "count": 16,
                  "value": "trojan"
                  },
                  {
                  "count": 8,
                  "value": "dropper"
                  }
            ],
            "popular_threat_name": [
            {
                  "count": 3,
                  "value":
               "cve20151641"
                  },
                  {
                  "count": 2,
                  "value": "expl"
                  },
                  {
                  "count": 2,
                  "value": "mo97"
                  }
            ],
            "suggested_threat_label":
"trojan.cve20151641/expl"
      },
      "reputation": -4,
      "rtf_info": {
      "document_properties": {
            "custom_xml_data_propertie
s": 0,
            "default_character_set":
"ANSI (default)",
            "dos_stubs": 0,
            "embedded_drawings": 0,
            "embedded_pictures": 0,
            "longest_hex_string":
86779,
            "non_ascii_characters":
293846,
            "objects": [
                  {
                        "class":
                  "otkloadr WRAssembly
                  1",
                        "type": "OLE
                  control"
                        },
                        {
```

```
                        "class":
                    "otkloadr WRAssembly
                    1",
                        "type": "OLE
                    embedded"
                        },
                     {
                        "class":
                    "otkloadr WRAssembly
                    1",
                        "type": "OLE
                    embedded"
                        }
                     ],
                     "read_only_protection
                ": false,
                     "rtf_header": "rtf1",
                     "user_protection":
                false
                 }
            },
            "sandbox_verdicts": {
            "Lastline": {
                 "category": "malicious",
                 "malware_classification":
            [
                     "MALWARE"
                     ],
                     "sandbox_name":
                "Lastline"
                 }
            },
            "sha1":
"609a4c511be0e6042c94ff88c26b0acf19f7d
a8c",
            "sha256":
"6cd6abeccf5e7f8507d209eafb8a1a77f2bd4
fe679dd633725759f0a7385500c",
            "size": 761563,
            "ssdeep":
"12288:9v4VZv95bR7embfqQOK6wbVvqSGNImo
dL48JkibF0eYGhpv6g:9yx9lRtnt5lpZF0rGd"
,
            "tags": [
            "ole-embedded",
            "exploit",
            "rtf",
            "cve-2015-1641",
            "ole-control"
            ],
            "times_submitted": 14,
            "tlsh":
"T1CDF4CFA7034937C1DE9B5D71EF99B407490
5F0A3E6C90B24DBEFE0709BE612938B2A45",
            "total_votes": {
            "harmless": 0,
```

```
                    "malicious": 1
                    },
                    "trid": [
                    {
                          "file_type": "Rich Text
                    Format",
                          "probability": 100
                          }
                    ],
                    "type_description": "Rich Text
              Format",
                    "type_extension": "rtf",
                    "type_tag": "rtf",
                    "unique_sources": 12,
                    "vhash":
              "8c37320968a225c52fb8344bd0bed6dc9"
                    },
                    "id":
          "6cd6abeccf5e7f8507d209eafb8a1a77f2bd4fe679
          dd633725759f0a7385500c",
                    "links": {
                    "self":
          "https://www.virustotal.com/api/v3/files/6c
          d6abeccf5e7f8507d209eafb8a1a77f2bd4fe679dd6
          33725759f0a7385500c"
                    },
                    "type": "file"
               },...
     ],
     "downloaded_files": [
     {
          "attributes": {
               "autostart_locations": [
                    {
                          "entry":
                    "C:\\WINDOWS\\winmain64.exe",
                          "location": "Task
                    Scheduler"
                          },
                          {
                          "entry":
                    "C:\\Windows\\winmain64.exe",
                          "location": "Task
                    Scheduler"
                          }
                    ],
                    "downloadable": true,
                    "exiftool": {
                    "FileType": "TXT",
                    "FileTypeExtension": "txt",
                    "LineCount": 1,
                    "MIMEEncoding": "us-ascii",
                    "MIMEType": "text/plain",
                    "Newlines": "(none)",
                    "WordCount": 6
                    },
```

```
      "first_submission_date":
1473369233,
      "last_analysis_date":
1574853432,
      "last_analysis_results": {
      "ALYac": {
            "category": "undetected",
            "engine_name": "ALYac",
            "engine_update":
     "20191127",
            "engine_version":
     "1.1.1.5",
            "method": "blacklist",
            "result": null
            },...
      },
      "last_analysis_stats": {
      "confirmed-timeout": 0,
      "failure": 0,
      "harmless": 0,
      "malicious": 0,
      "suspicious": 0,
      "timeout": 0,
      "type-unsupported": 13,
      "undetected": 57
      },
      "last_modification_date":
1620640787,
      "last_submission_date":
1560296158,
      "magic": "ASCII text, with no
line terminators",
      "md5":
"43b31a333c9b78f0c53d0f392c233581",
      "meaningful_name": "gate.php",
      "names": [
      "gate.php",...
      ],
      "reputation": 0,
      "sha1":
"5a6c92842517f32fc654fa90d1bb7aff59779
39e",
      "sha256":
"21f2049d5b7a94430621acbc5f6c467c134d3
68a2c69a8283cc08b1f6183962c",
      "size": 15,
      "ssdeep": "3:eXCRXn:e0n",
      "tags": [
      "text"
      ],
      "times_submitted": 90,
      "total_votes": {
      "harmless": 0,
      "malicious": 0
      },
      "trid": [
```

```
                              {
                                    "file_type": "file seems
                                   to be plain text/ASCII",
                                    "probability": 0
                                    }
                              ],
                              "type_description": "Text",
                              "type_extension": "txt",
                              "type_tag": "text",
                              "unique_sources": 11
                        },
                        "id":
                    "21f2049d5b7a94430621acbc5f6c467c134d368a2c
                    69a8283cc08b1f6183962c",
                        "links": {
                        "self":
                    "https://www.virustotal.com/api/v3/files/21
                    f2049d5b7a94430621acbc5f6c467c134d368a2c69a
                    8283cc08b1f6183962c"
                        },
                    "type": "file"
                    },..
              ],
              "id": "moiparks.in",
              "links": {
              "self":
        "https://www.virustotal.com/api/v3/domains/moiparks.in
        "
              },
              "referrer_files": [],
              "resolutions": [
              {
                    "attributes": {
                        "date": 1538837772,
                        "host_name": "moiparks.in",
                        "ip_address": "69.64.147.10",
                        "resolver": "VirusTotal"
                        },
                        "id": "69.64.147.10moiparks.in",
                        "links": {
                        "self":
                    "https://www.virustotal.com/api/v3/resoluti
                    ons/69.64.147.10moiparks.in"
                        },
                        "type": "resolution"
                    },...
              ],
              "siblings": [],
              "subdomains": [
              {
                    "attributes": {
                        "categories": {
                              "Comodo Valkyrie Verdict":
                         "media sharing",
                              "sophos": "malware callhome,
                         command and control"
```

```
                    },
                    "last_analysis_results": {
                    "ADMINUSLabs": {
                          "category": "harmless",
                          "engine_name":
                    "ADMINUSLabs",
                          "method": "blacklist",
                          "result": "clean"
                          },...
                    },
                    "last_analysis_stats": {
                    "harmless": 74,
                    "malicious": 2,
                    "suspicious": 1,
                    "timeout": 0,
                    "undetected": 8
                    },
                    "last_dns_records": [],
                    "last_modification_date":
              1610393131,
                          "popularity_ranks": {},
                          "reputation": 0,
                          "tags": [],
                          "total_votes": {
                          "harmless": 0,
                          "malicious": 0
                          },
                          "whois": ""
                    },
                    "id": "www.moiparks.in",
                    "links": {
                    "self":
             "https://www.virustotal.com/api/v3/domains/
             www.moiparks.in"
                          },
                               "type": "domain"
               },...
          ],
          "type": "domain",
          "urls": [
               {
                    "attributes": {
                         "categories": {
                              "sophos": "malware callhome,
                         command and control"
                          },
                          "first_submission_date":
                     1617845246,
                          "has_content": false,
                          "html_meta": {},
                          "last_analysis_date": 1617845246,
                          "last_analysis_results": {
                               "ADMINUSLabs": {
                                    "category":
                               "harmless",
```

```
                                    "engine_name":
                                "ADMINUSLabs",
                                    "method": "blacklist",
                                    "result": "clean"
                                },...
                            },
                            "last_analysis_stats": {
                                "harmless": 75,
                                "malicious": 1,
                                "suspicious": 0,
                                "timeout": 0,
                                "undetected": 9
                        },
                        "last_final_url":
                    "https://moiparks.in/jack/admin.php",
                        "last_modification_date": 1617845256,
                        "last_submission_date": 1617845246,
                        "reputation": 0,
                        "tags": [],
                        "targeted_brand": {},
                        "threat_names": [
                            "C2/Generic-A"
                            ],
                            "times_submitted": 1,
                            "total_votes": {
                            "harmless": 0,
                            "malicious": 0
                            },
                            "trackers": {},
                            "url":
                        "https://moiparks.in/jack/admin.php"
                        },
                        "context_attributes": {
                        "url":
                    "https://moiparks.in/jack/admin.php"
                        },
                        "id":
                    "fc9079b288905dab4db77984c4f8d78feacf015f99
                    26e0baeb0cfefc061693f1",
                        "links": {
                        "self":
                    "https://www.virustotal.com/api/v3/urls/fc9
                    079b288905dab4db77984c4f8d78feacf015f9926e0
                    baeb0cfefc061693f1"
                        },
                        "type": "url"
                    },...
            ]
    }
```

PDNS

The PDNS API call provides passive DNS data for a domain or IP address.

Data Structure:

```
{
      "duration": integer,
      "items": [
            {
                  "Domain": string,
                  "Hostname": string,
                  "IP": string,
                  "Last_Seen": integer,
                  "NameServer": string,
                 "Record_Type": string
            },...
      ],
      "status": integer,
      "total_results": integer
}
```

Example:
Given “45.63.119.161” is used as the indicator, PDNS will return the following:

```
{
      "duration": integer,
      "items": [
            {
                  "Domain": "",
                  "Hostname": "amd450.in",
                  "IP": "45.63.119.161",
                  "Last_Seen": 1598972832,
                  "NameServer": "",
                  "Record_Type": "A"
            },
            {
                  "Domain": "",
                  "Hostname": "asdjkl123.in",
                  "IP": "45.63.119.161",
                  "Last_Seen": 1616943872,
                  "NameServer": "",
                  "Record_Type": "A"
            }
            {
                  "Domain": "",
                  "Hostname": "jetsetflysystems.asia",
                  "IP": "45.63.119.161",
                  "Last_Seen": 1615889982,
                  "NameServer": "",
                  "Record_Type": "A"
             }
```

```
        ],
                    "status": 200,
                    "total_results": 3
}
```

PTR (Reverse DNS)

The PTR API call provides the domain associated with an IP address.

Data Structure:

```
{
 “ptr_record”: string
}
```

Example:

Given “45.63.119.161” is used as the indicator, PDNS will return the following:

```
{
 "ptr_record": "45.63.119.161.vultr.com"
}
```

RPZ Feeds

The RPZ Feeds worker returns matching host or IP records in Infoblox generated RPZ feeds which consist of active threat records matching certain classes, properties, or other characteristics.

Data Structure:

Data Structure:

```
{
        "records": [
        {
        "class": string,
        "detected": string,
        "expiration": string,
        "feed_name": string,
        "indicator": string,
        "property": string,
        "threat_level": integer
        },...
        ]
}
```

Example:
Given an indicator of "eicar.co", RPZ Feeds will return the following:

```
{
        "records": [
                {
                        "class": string,
                        "detected": string,
                        "expiration": string,
                        "feed_name": string,
                        "indicator": string,
                        "property": string,
                        "threat_level": integer
                },...
        ]
}
```

Example:
Given an indicator of "eicar.co", RPZ Feeds will return the following:

```
{
        "records": [
                {
                        "class": "MaliciousNameserver",
```

```
                        "detected": "2016-11-09T22:55:27Z",
                        "expiration": "2038-01-19T22:55:27Z",
                        "feed_name": "base",
                "indicator": "eicar.co",
        "property": "MaliciousNameserver_Generic",
        "threat_level": 100
        }
        ]
}
```

WHOIS Report

The WHOIS Report API call provides the WHOIS report on a domain or IP address.

Data Structure:

```
 {
"domain_name": string,
"emails": [string],
"name_servers": [string],
"record_source": string,
"registrant": string,
"registration": {
  "created":string,
 "expires": string,
 "registrar": string,
 "statuses": [string],
 "updated": string
},
"whois": {
 "date": string,
 "record": string
},
"parsed_whois": {
  "domain": string,
  "created_date": string,
  "expired_date": string,
  "updated_date": string,
  "name_servers": [string],
   "statuses": [string],
   "registrar": {
  "abuse_contanct_email":
  string, "abuse_contact_phone":
  string, "iana_id": string,
  "name": string,
  "url": string,
  "whois_server": string
 },
 "contacts": {
  "admin": {
  "city": string,
  "country": string,
  "email": string,
  "fax": string,
  "name": string,
  "org": string,
   "phone": string,
   "postal": string,
   "state": string,
```

```
        "street":
        [string]
       },
       "billing": {
        "city":string
        ,
       "country": string,
       "email": string,
       "fax": string,
       "name": string,
       "org": string,
       "phone": string,
       "postal":
string,
       "state": string,

"street":[string]
       },
      "registrant": {
       "city": string,
       "country":
       string, "email":
       string, "fax":
       string, "name":
       string, "org":
       string, "phone":
       string,
       "postal":
       string, "state":
       string,
       "street":
       [string]
       },
       "tech": {
       "city": string,
       "country": string,
       "email": string,
       "fax": string,
       "name": string,
       "org": string,
       "phone": string,
       "postal": string,
       "state": string,
       "street": [string]
       },
      "other_properties": {
       "dnssec": string,
       "registry_id": string
      }
     }
    }
```

Example:
Given “moiparks.in” is used as the indicator, WHOIS returns the following:


```
    {
     "response": {
      "domain_name": "moiparks.in",
      "emails": [
       "admin@blueliv.com"
      ],
      "parsed_whois": {
       "contacts": {
        "admin": {
         "city": "Barcelona",
         "country": "ES",
         "email":
         "admin@blueliv.com",
         "fax": "",
         "name": "Dns Admin",
         "org": "FOR SINKHOLING PURPOSES",
         "phone": "34933096100",
         "postal": "08018",
         "state": "Barcelona",
         "street": [
          "Pallars 99, office 17"
]
},
        "registrant": {
         "city": "Barcelona",
         "country": "ES",
         "email":
         "admin@blueliv.com",
         "fax": "",
         "name": "Dns Admin",
         "org": "FOR SINKHOLING PURPOSES",
         "phone": "34933096100",
         "postal": "08018",
         "state": "Barcelona",
         "street": [
          "Pallars 99, office 17"
]
},
        "tech": {
         "city": "Barcelona",
         "country": "ES",
         "email":
         "admin@blueliv.com",
         "fax": "",
         "name": "Dns Admin",
         "org": "FOR SINKHOLING PURPOSES",
```

```
        "phone": "34933096100",
        "postal": "08018",
        "state": "Barcelona",
        "street": [
         "Pallars 99, office 17"
        ]
}
},
      "created_date": "2017-09-18T08:20:24+00:00",
      "domain": "moiparks.in",
      "expired_date": "2018-09-18T08:20:24+00:00",
      "name_servers": [ "dns1.registrar-
       servers.com", "dns2.registrar-
       servers.com"
      ],
      "other_properties": {
       "admin_id": "db6386c3df9e2db4",
       "dnssec": "Unsigned",
       "domain_id": "D414400000005073264-AFIN",
       "last_updated_on": "18-Sep-2017 08:20:26
       UTC", "reg_id": "db6386c3df9e2db4",
       "status": [
        "CLIENT TRANSFER PROHIBITED",
        "TRANSFER PROHIBITED",
        "ADDPERIOD"
       ],
       "tech_id": "db6386c3df9e2db4"
      },
      "registrar": {
       "abuse_contact_email":
       "",
       "abuse_contact_phone":
       "", "iana_id": "",
       "name": "eNom, Inc. (R46-
       AFIN)", "url": "",
       "whois_server": ""
      },
      "statuses": [],
      "updated_date":
      ""
     },
     "record_source": "moiparks.in",
     "registrant": "FOR SINKHOLING PURPOSES",
     "whois": {
      "date": "2017-09-20",
      "record": "Domain ID:D414400000005073264-AFIN\nDomain…"
     }
    }
   }
```