ThreatQuotient

DomainTools Operation Guide

Version 3.0.0

August 29, 2022

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	3.0.0
Compatible with ThreatQ Versions	>= 4.47.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/domaintools

Introduction

The DomainTools operation provides context in the form of attributes and indicators of compromise from the DomainTools API.

The operation provides the following action:

- **Enrich** - provides actionable insights-at-scale with enterprise-scale ingestion of DomainTools data.

  > Different endpoints are utilized based on the indicator type selected for the operation.

The operation is compatible with Email Address, FQDN, and IP Address Indicator types.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Username	Your DomainTools API Username.
API Key	Your DomainTools API Key.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich	Provides actionable insights-at-scale with enterprise-scale ingestion of DomainTools data.	Indicator	FQDN, Email Address, IP Address

Enrich

The Enrich action provides actionable insights-at-scale with enterprise-scale ingestion of DomainTools data.

Each indicator type uses multiple enriching endpoints to retrieve data.

Parameters

The following operation parameters are available for the operation.

> Some configuration parameters are only available for specific indicator types.

PARAMETER	DESCRIPTION	INDICATOR TYPE
IRIS Investigate	The Iris is `DomainTools` flagship threat intelligence and investigation platform that combines enterprise-grade domain and DNS-based intelligence.	Email Address, IP Address, FQDN
Reverse Whois	Reverse Whois allows search for domains by the name, address, telephone number, email address or physical address of the Registrant listed	Email Address
Hosting History	Hosting History provides a list of changes that have occurred in a Domain Name's registrar, IP address, and name servers.	IP Address, FQDN
Reverse IP Whois	The Reverse IP Whois API provides a list of IP ranges that are owned by an Organization.	IP Address, FQDN
IRIS Enrich	Provides actionable insights-at-scale with enterprise-scale ingestion of DomainTools data.	FQDN

IRIS Investigate

Iris is DomainTools' flagship threat intelligence and investigation platform that combines enterprise-grade domain and DNS-based intelligence.

Based on the indicator type,the URL can be:

```
GET https://api.domaintools.com/v1/iris-investigate/?ip={}
```

```
GET https://api.domaintools.com/v1/iris-investigate/?domain={}
```

Sample Response:


```
{
"response": {
    "limit_exceeded": false,
    "message": "Enjoy your data.",
    "results_count": 1,
    "results": [
        {
            "domain": "protonmail.com",
            "whois_url": "https://whois.domaintools.com/protonmail.com",
            "admin_contact": "",
            "adsense": {
                "value": ""
            },
            "alexa": 3361,
            "popularity_rank": 243,
            "active": true,
            "google_analytics": {
                "value": ""
            },
            "registrant_contact": {
              "name": {
                "value": ""
              },
              "org": {
                "value": "Proton AG"
              },
              "street": {
                "value": ""
              },
              "city": {
                "value": ""
              },
              "state": {
                "value": ""
              },
              "postal": {
                "value": ""
              },
              "country": {
                "value": ""
              },
```

```
      "phone": {
        "value": ""
      },
      "fax": {
        "value": ""
      },
      "email": [
        {
          "value": "select request email form at https://domains.markmonitor.com/whois/protonmail.com"
        }
      ]
    },
    "create_date": {
        "value": "2010-08-21"
    },
    "expiration_date": {
        "value": "2024-08-21"
    },
    "email_domain": [
        {
            "value": "protonmail.ch"
        }
    ],
    "soa_email": [
        {
            "value": "support@protonmail.ch"
        }
    ],
    "ssl_email": [],
    "additional_whois_email": [
        {
            "value": "abusecomplaints@markmonitor.com"
        }
    ],
    "ip": [
        {
            "address": {
                "value": "185.70.42.12"
            },
            "asn": [
                {
                    "value": 62371
                }
            ],
            "country_code": {
                "value": "ch"
            },
            "isp": {
                "value": "Proton Technologies AG"
            }
        }
    ],
    "name_server": [
        {
            "host": {
                "value": "ns1.protonmail.com"
            },
            "domain": {
                "value": "protonmail.com"
            },
            "ip": [
```

```
                    {
                        "value": "185.70.42.150"
                    }
                ]
            }
        ],
        "domain_risk": {
            "risk_score": 0,
            "components": [
                {
                    "name": "zerolist",
                    "risk_score": 0
                }
            ]
        },
        "redirect": {
            "value": ""
        },
        "redirect_domain": {
            "value": ""
        },
        "registrant_name": {
            "value": ""
        },
        "billing_contact": "",
        "registrant_org": {
            "value": "Proton AG"
        },
        "registrar": {
            "value": "MarkMonitor, Inc."
        },
        "registrar_status": [
            "clientdeleteprohibited"
        ]
    }
]}
}
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response.results[].whois_url	Indicator.Attribute	WHOIS URL	N/A	https://whois.domaintools.com/desitales.com	N/A
.response.results[].admin_contact.name.value	Indicator.Attribute	Admin Name	N/A	N/A	N/A
.response.results[].admin_contact.org.value	Indicator.Attribute	Admin Organization	N/A	N/A	N/A
.response.results[].admin_contact.street.value	Indicator.Attribute	Admin Address Street	N/A	N/A	N/A
.response.results[].admin_contact.city.value	Indicator.Attribute	Admin Address City	N/A	N/A	N/A
.response.results[].admin_contact.state.value	Indicator.Attribute	Admin Address State	N/A	N/A	N/A
.response.results[].admin_contact.postal.value	Indicator.Attribute	Admin Address Postal	N/A	N/A	N/A
.response.results[].admin_contact.country.value	Indicator.Attribute	Admin Address Country	N/A	N/A	N/A
.response.results[].admin_contact.phone.value	Indicator.Attribute	Admin Phone	N/A	N/A	N/A
.response.results[].admin_contact.fax.value	Indicator.Attribute	Admin Fax	N/A	N/A	N/A
.response.results[].email_domain[].value	Indicator.Value	Email Domain	N/A	protonmail.ch	N/A
.response.results[].registrant_contact.name.value	Indicator.Attribute	Registrant Name	N/A	N/A	N/A
.response.results[].registrant_contact.org.value	Indicator.Attribute	Registrant Organization	N/A	Proton AG	N/A
.response.results[].registrant_contact.street.value	Indicator.Attribute	Registrant Address Street	N/A	N/A	N/A
.response.results[].registrant_contact.city.value	Indicator.Attribute	Registrant Address City	N/A	N/A	N/A
.response.results[].registrant_contact.state.value	Indicator.Attribute	Registrant Address State	N/A	N/A	N/A
.response.results[].registrant_contact.postal.value	Indicator.Attribute	Registrant Address Postal	N/A	N/A	N/A
.response.results[].registrant_contact.country.value	Indicator.Attribute	Registrant Address Country	N/A	N/A	N/A
.response.results[].registrant_contact.phone.value	Indicator.Attribute	Registrant Phone	N/A	N/A	N/A
.response.results[].registrant_contact.fax.value	Indicator.Attribute	Registrant Fax	N/A	N/A	N/A
.response.results[].billing_contact.name.value	Indicator.Attribute	Billing Name	N/A	N/A	N/A
.response.results[].billing_contact.org.value	Indicator.Attribute	Billing Organization	N/A	N/A	N/A
.response.results[].billing_contact.street.value	Indicator.Attribute	Billing Address Street	N/A	N/A	N/A
.response.results[].billing_contact.city.value	Indicator.Attribute	Billing Address City	N/A	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response.results[].billing_contact.state.value	Indicator.Attribute	Billing Address State	N/A	N/A	N/A
.response.results[].billing_contact.postal.value	Indicator.Attribute	Billing Address Postal	N/A	N/A	N/A
.response.results[].billing_contact.country.value	Indicator.Attribute	Billing Address Country	N/A	N/A	N/A
.response.results[].billing_contact.phone.value	Indicator.Attribute	Billing Phone	N/A	N/A	N/A
.response.results[].billing_contact.fax.value	Indicator.Attribute	Billing Fax	N/A	N/A	N/A
.response.results[].create_date	Indicator.Attribute	Created At	N/A	2010-08-21	N/A
.response.results[].expiration_date	Indicator.Attribute	Expiration Date	N/A	2024-08-21	N/A
.response.results[].ssl_email	Indicator.Attribute	SSL email	N/A	N/A	N/A
.response.results[].ip[]	Indicator.Value	IP Address	N/A	185.70.42.12	N/A
.response.results[].domain_risk.component[].name /.risk_score	Indicator.Attribute	Domain Risk Name and Score	N/A	zerolist/0	N/A

Reverse Whois

Reverse Whois allows search for domains by the name, address, telephone number, email address or physical address of the Registrant listed.

```
GET http://api.domaintools.com/v1/reverse-whois/?terms={email}&mode=purchase
```

Sample Response


```
{
    "response": {
        "domain_count": {
            "current": 0,
            "historic": 0
        },
        "domains": [
            "bulkcheck.com"
        ],
        "report_price": {
            "current": 0,
            "historic": 0
        }
    }
}
```


ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
response.domains[]	Indicator.Value	FQDN	N/A	bulkcheck.com	N/A

Hosting History

Hosting History provides a list of changes that have occurred in a Domain Name's registrar, IP address, and name servers. `GET https://api.domaintools.com/v1/{}/hosting-history/`

Sample Response:


```
{
    "response": {
        "domain_name": "cloudflare.com",
        "ip_history": [
            {
                "domain": "CLOUDFLARE.COM",
                "post_ip": "68.178.232.100",
                "pre_ip": null,
                "action": "N",
                "actiondate": "2009-02-23",
                "action_in_words": "New"
            }
        ],
        "registrar_history": [
            {
                "domain": "CLOUDFLARE.COM",
                "date_updated": "2009-02-17",
                "date_created": "2009-02-17",
                "date_expires": "2010-02-17",
                "date_lastchecked": "2009-02-20",
                "registrar": "GoDaddy.com",
                "registrartag": "Go Daddy Software Inc"
            }
        ],
        "nameserver_history": [
            {
                "domain": "CLOUDFLARE.COM",
                "action": "N",
                "actiondate": "2009-02-19",
                "action_in_words": "New",
                "post_mns": "Domaincontrol.com",
                "pre_mns": ""
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response.registrar_history[].registrar	Indicator.Attribute	WHOIS Registrar	N/A	GoDaddy.com	N/A
.response.registrar_history[].date_updated	Indicator.Attribute	Updated At	N/A	2009-02-17	N/A
.response.nameserver_history[].pre_mns	Indicator.Value	FQDN	N/A	N/A	N/A
.response.nameserver_history[].post_mns	Indicator.Value	FQDN	N/A	Domaincontrol.com	N/A
.response.nameserver_history[].action_in_words	Indicator.Attribute	WHOIS Action	N/A	New	N/A
.response.nameserver_history[].actiondate	Indicator.Attribute	WHOIS Action Date	N/A	2009-02-19	N/A
.response.ip_history[].post_ip	Indicator.Value	IP Address	N/A	68.178.232.100	N/A
.response.ip_history[].pre_ip	Indicator.Value	IP Address	N/A	N/A	N/A
.response.ip_history[].action_in_words	Indicator.Attribute	WHOIS Action	N/A	New	N/A
.response.ip_history[].actiondate	Indicator.Attribute	WHOIS ActionDate	N/A	2009-02-23	N/A

Reverse IP Whois (IP Address)

Reverse IP Whois allows search of IP ranges owned by an organization by an IP address, domain, email, or other query.

```
GET https://api.domaintools.com/v1/reverse-ip-whois/?ip={}
```

Sample Response:


```
{
    "response": {
        "whois_record": "NetRange:       172.64.0.0 - 172.71.255.255\nCIDR:           172.64.0.0/13\nNetName:
CLOUDFLARENET\nNetHandle:      NET-172-64-0-0-1\nParent:         NET172 (NET-172-0-0-0-0)\nNetType:        Direct
Allocation\nOriginAS:       AS13335\nOrganization:   Cloudflare, Inc. (CLOUD14)\nRegDate:        2015-02-25\nUpdated:
2021-05-26\nComment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse\nRef:
https://rdap.arin.net/registry/ip/172.64.0.0\n\nOrgName:        Cloudflare, Inc.\nOrgId:          CLOUD14\nAddress:
101 Townsend Street\nCity:           San Francisco\nStateProv:      CA\nPostalCode:     94107\nCountry:
US\nRegDate:        2010-07-09\nUpdated:        2021-07-01\nRef:            https://rdap.arin.net/registry/entity/
CLOUD14\n\nOrgNOCHandle: CLOUD146-ARIN\nOrgNOCName:   Cloudflare-NOC\nOrgNOCPhone:  +1-650-319-8930 \nOrgNOCEmail:
noc@cloudflare.com\nOrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN\n\nOrgTechHandle: ADMIN2521-
ARIN\nOrgTechName:   Admin\nOrgTechPhone:  +1-650-319-8930 \nOrgTechEmail:  rir@cloudflare.com\nOrgTechRef:
https://rdap.arin.net/registry/entity/ADMIN2521-ARIN\n\nOrgAbuseHandle: ABUSE2916-ARIN\nOrgAbuseName:
Abuse\nOrgAbusePhone:  +1-650-319-8930 \nOrgAbuseEmail:  abuse@cloudflare.com\nOrgAbuseRef:    https://rdap.arin.net/
registry/entity/ABUSE2916-ARIN\n\nOrgRoutingHandle: CLOUD146-ARIN\nOrgRoutingName:   Cloudflare-NOC\nOrgRoutingPhone:
+1-650-319-8930 \nOrgRoutingEmail:  noc@cloudflare.com\nOrgRoutingRef:    https://rdap.arin.net/registry/entity/
CLOUD146-ARIN\n\nRAbuseHandle: ABUSE2916-ARIN\nRAbuseName:   Abuse\nRAbusePhone:  +1-650-319-8930 \nRAbuseEmail:
abuse@cloudflare.com\nRAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN\n\nRNOCHandle: NOC11962-
ARIN\nRNOCName:   NOC\nRNOCPhone:  +1-650-319-8930 \nRNOCEmail:  noc@cloudflare.com\nRNOCRef:    https://
rdap.arin.net/registry/entity/NOC11962-ARIN\n\nRTechHandle: ADMIN2521-ARIN\nRTechName:   Admin\nRTechPhone:
+1-650-319-8930 \nRTechEmail:  rir@cloudflare.com\nRTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-
ARIN\n",
        "ip_from": "172.64.0.0",
        "ip_to": "172.71.255.255",
        "record_ip": "172.67.209.126",
        "short_record_ip": "172.67.209.126",
        "ip_from_alloc": "172.64.0.0",
        "ip_to_alloc": "172.71.255.255",
        "organization": "Cloudflare, Inc.",
        "server": "whois.arin.net",
        "country": "US",
        "record_date": "2022-08-10",
        "range": "172.64.0.0/13"
    }
}
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response.organization	Indicator.Attribute	WHOIS Organization	N/A	Cloudflare, Inc.	N/A
.response.country	Indicator.Attribute	WHOIS Country	N/A	US	N/A
.response.server	Indicator.Attribute	WHOIS Server	N/A	whois.arin.net	N/A
.response.range	Indicator.Attribute	IP Range	N/A	172.64.0.0/13	N/A
.response.record_date	Indicator.Attribute	Record Date	N/A	2022-08-10	N/A

Reverse IP Whois (FQDN)

Reverse IP Whois allows search of IP ranges owned by an organization by an IP address, domain, email, or other query.

```
GET https://api.domaintools.com/v1/reverse-ip-whois/?query={}
```

Sample Response:


```
{
    "response": {
        "records": [
            {
                "ip_from": "168.253.114.148",
                "ip_to": "168.253.114.148",
                "record_ip": "168.253.114.148",
                "record_date": "2022-07-13",
                "country": "NG",
                "range": "168.253.114.148/32",
                "organization": "Rotimi Alex (rotimialex@protonmail.com)",
                "server": "whois.afrinic.net",
                "short_record_ip": "168.253.114.148"
            }
        ],
        "record_count": 1,
        "page": 1,
        "has_more_pages": false
    }
}
```


ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response.organization	Indicator.Attribute	Organization	N/A	Rotimi Alex (rotimialex@protonmail.com)	N/A
.response.range	Indicator.Attribute	IP Address/IP Range	N/A	168.253.114.148/32	N/A

IRIS Enrich

Designed to support high query volumes with batch processing and fast response times, the Iris Enrich API provides actionable insights-at-scale with enterprise-scale ingestion of DomainTools data.

```
GET https://api.domaintools.com/v1/iris-enrich/?domain={}
```

Sample Response:


```
{
    "response": {
        "limit_exceeded": false,
        "message": "Enjoy your data.",
        "results_count": 1,
        "results": [
            {
                "domain": "protonmail.com",
                "whois_url": "https://whois.domaintools.com/protonmail.com",
                "adsense": {
                    "value": ""
                },
                "alexa": 3361,
                "popularity_rank": 243,
                "active": true,
                "google_analytics": {
                    "value": ""
                },
                "registrant_contact": {
                    "name": {
                      "value": ""
                    },
                    "org": {
                      "value": "Proton AG"
                    },
                    "street": {
                      "value": ""
                    },
                    "city": {
                      "value": ""
                    },
                    "state": {
                      "value": ""
                    },
                    "postal": {
                      "value": ""
                    },
                    "country": {
                      "value": ""
                    },
                    "phone": {
                      "value": ""
                    },
                    "fax": {
                      "value": ""
```

```
                    },
                    "email": [
                        {
                            "value": "select request email form at https://domains.markmonitor.com/whois/
protonmail.com"
                        }
                    ]
                },
                "create_date": {
                    "value": "2010-08-21"
                },
                "expiration_date": {
                    "value": "2024-08-21"
                },
                "email_domain": [
                    {
                        "value": "protonmail.ch"
                    }
                ],
                "soa_email": [
                    {
                        "value": "support@protonmail.ch"
                    }
                ],
                "ssl_email": [],
                "additional_whois_email": [
                    {
                        "value": "abusecomplaints@markmonitor.com"
                    }
                ],
                "ip": [
                    {
                        "address": {
                            "value": "185.70.42.12"
                        },
                        "asn": [
                            {
                                "value": 62371
                            }
                        ],
                        "country_code": {
                            "value": "ch"
                        },
                        "isp": {
                            "value": "Proton Technologies AG"
                        }
                    }
                ],
                "name_server": [
                    {
                        "host": {
                            "value": "ns1.protonmail.com"
                        },
                        "domain": {
                            "value": "protonmail.com"
                        },
                        "ip": [
                            {
                                "value": "185.70.42.150"
                            }
                        ]
```

```
                }
            ],
            "domain_risk": {
                "risk_score": 0,
                "components": [
                    {
                        "name": "zerolist",
                        "risk_score": 0
                    }
                ]
            },
            "redirect": {
                "value": ""
            },
            "redirect_domain": {
                "value": ""
            },
            "registrant_name": {
                "value": ""
            },
            "registrant_org": {
                "value": "Proton AG"
            },
            "registrar": {
                "value": "MarkMonitor, Inc."
            },
            "registrar_status": [
                "clientdeleteprohibited"
            ],
            "data_updated_timestamp": "2022-08-10T21:41:00.043000"
    }]}
}
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.response.results[].registrant_contact.name.value	Indicator.Attribute	Registrant	N/A	NA	N/A
.response.results[].registrant_contact.create_date.value	Indicator.Attribute	Created At	N/A	2010-08-21	N/A
.response.results[].registrant_contact.expiration_date.value	Indicator.Attribute	Expires At	N/A	2024-08-21	N/A
.response.results[].data_updated_timestamp	Indicator.Attribute	Updated At	N/A	2022-08-10T21:41:00.043000	N/A
.response.results[].domain_risk.risk_score	Indicator.Attribute	Risk Score	N/A	0	N/A
.response.results[].domain_risk.components[].name/.risk_score	Indicator.Attribute	Domain Risk Name and Score	N/A	zerolist/0	N/A
.response.results[].ip[].address.value	Indicator.Attribute	Record Source	N/A	185.70.42.12	N/A
.response.results[].registrar_status[]	Indicator.Attribute	Status	N/A	clientdeleteprohibited	N/A
.response.results[].registrar.value	Indicator.Attribute	Registrar	N/A	MarkMonitor, Inc.	N/A
.response.results[].registrant_contact.phone.value	Indicator.Attribute	Registrant Contact Phone	N/A	N/A	N/A
.response.results[].name_server[].host.value	Indicator.Value	Name Servers	N/A	ns1.protonmail.com	N/A
.response.results[].additional_whois_email[].value	Indicator.Value	Email Address	N/A	abusecomplaints@markmonitor.com	N/A
.response.results[]..email_domain[].value	Indicator.Value	FQDN	N/A	protonmail.ch	N/A

Change Log

- **Version 3.0.0**
  - Replaced Domain Reputation and Parsed Whois with new **Iris Enrich** endpoint
  - Removed Reverse IP enrichment endpoint.
  - Fixed a bug with Enrich Email - Reverse Whois.
- **Version 2.1.0**
  - N/A
- **Version 2.0.0**
  - N/A
- **Version 1.0.0**
  - Initial release