ThreatQuotient

CrowdStrike Falcon X Sandbox CDF Guide

Version 1.0.0

January 19, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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

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.

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.43.0`

Introduction

The CrowdStrike Falcon X Sandbox CDF ingests Reports, Indicators, Signatures, Malware and Attack Pattern objects based on submissions via the **CrowdStrike Falcon X Sandbox Operation**.

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 feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the integration.

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 **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client ID	The Falcon X Client Id used for authentication.
Secret	The Falcon X Secret used for authentication.

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

ThreatQ Mapping

Falcon X Sandbox

Main feed used to retrieve report ids which will further on be used in the Falcon X Details supplemental feed.

```
GET https://api.crowdstrike.com/falconx/queries/reports/v1
```


```
{
    "meta": {
        "query_time": 0.008275485,
        "pagination": {
            "offset": 0,
            "limit": 10,
            "total": 86
        },
        "powered_by": "falconx-api",
        "trace_id": "02ac753f-e7a5-4d39-a339-ca9080d94860",
        "quota": {
            "total": 100,
            "used": 0,
            "in_progress": 0
        }
    },
    "resources": [
        "ace79a13936f4ec8ad4de36606814bfc_e332f0252af143b89ad44b973c05124b",
        "ace79a13936f4ec8ad4de36606814bfc_43d809df175f4ff9aa4fe47b2e1d3759",
        "ace79a13936f4ec8ad4de36606814bfc_f0f165f79cb4486f8ee0013a82221de5",
        "ace79a13936f4ec8ad4de36606814bfc_0b8a0f0ea902457ca8902afa26c0fa8d",
        "ace79a13936f4ec8ad4de36606814bfc_8815c0c3180d42b18dd202fe5182e757",
        "ace79a13936f4ec8ad4de36606814bfc_133535ec09784a7ea19b155aa1092b77",
        "ace79a13936f4ec8ad4de36606814bfc_cca86b85a5804038826880ac749d3274",
        "ace79a13936f4ec8ad4de36606814bfc_f325aac08bb1415ea0e5fbd35b7dbb39",
        "ace79a13936f4ec8ad4de36606814bfc_bcd04c21f18a44a39a4c44c1cca4a830",
        "ace79a13936f4ec8ad4de36606814bfc_eebc849ccc8646fba61f1580eeb384ec"
    ],
    "errors": []
}
```

Falcon X Details (Supplemental):

Supplemental feed called once per each report id returned by the Falcon X Sandbox feed.

```
GET https://api.crowdstrike.com/falconx/entities/reports/v1?ids={resources}
```


```
{
    "meta": {
        "query_time": 0.016763999,
        "powered_by": "falconx-api",
        "trace_id": "b3242eef-8a82-4a70-b66f-6c33a27ef30a",
        "quota": {
            "total": 100,
            "used": 0,
            "in_progress": 0
        }
    },
    "resources": [
        {
            "id": "ace79a13936f4ec8ad4de36606814bfc_f0f165f79cb4486f8ee0013a82221de5",
            "cid": "ace79a13936f4ec8ad4de36606814bfc",
            "created_timestamp": "2020-09-25T17:12:55Z",
            "origin": "apigateway",
            "verdict": "PUP",
            "ioc_report_strict_csv_artifact_id": "75375e10d727841534a6a790eb9cc618221029fb69dd10b435f256af77d7b20c",
            "ioc_report_broad_csv_artifact_id": "314c916e99a07f43b4f5720edabb3593a57134bdb6c922c549a487433cedb4bc",
            "ioc_report_strict_json_artifact_id": "3f5e8c8325919a4c4c04cc00059728563f0847e8d3af0b220feafb7bd8b9437a",
            "ioc_report_broad_json_artifact_id": "bfe90e91f5cc8bfbb9e6e9c1d99a7c22ea22b5fb8961eab68e10948dc2619b45",
            "ioc_report_strict_stix_artifact_id": "b980b6f1f1bc7e3d4b6b30f0ebbb89329691a85a8510c761e2c6c41fbaf77f8f",
            "ioc_report_broad_stix_artifact_id": "6e601826bfc72529358823d3a1768fb23a5d1b5aa4454f80097635a37ca3a956",
            "ioc_report_strict_maec_artifact_id": "63fbf10af2e88a1ce190e047e79c50316a98f78f5a09c54a6d7854bdd8ebc8e6",
            "ioc_report_broad_maec_artifact_id": "53acc18ad1e6f266eaa395ce0be2b4461815b4588c913db0289bd1b668a80bcd",
            "sandbox": [
                {
                    "sha256": "b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66",
                    "environment_id": 110,
                    "environment_description": "Windows 7 64 bit",
                    "file_size": 218112,
                    "file_type": "PE32 executable (GUI) Intel 80386, for MS Windows",
                    "file_type_short": [
                        "peexe",
                        "executable"
                    ],
                    "submit_name": "malware-ransom-cerber",
                    "submission_type": "file",
                    "verdict": "malicious",
                    "threat_score": 61,
                    "windows_version_name": "Windows 7",
                    "windows_version_edition": "Professional",
                    "windows_version_service_pack": "Service Pack 1",
                    "windows_version_version": "6.1 (build 7601)",
                    "windows_version_bitness": 64,
                    "incidents": [
                        {
                            "name": "Fingerprint",
                            "details": [
                                "Reads the active computer name"
                            ]
```

```
                    }
                ],
                "file_metadata": {
                    "file_compositions": [
                        "1 .OBJ Files (COFF) linked with LINK.EXE 10.10 (Visual Studio 2010) (build: 30319)",
                        "6 .CPP Files (with LTCG) compiled with CL.EXE 16.00 (Visual Studio 2010) (build:
30319)",
                        "152   .C Files compiled with CL.EXE 16.00 (Visual Studio 2010) (build: 30319)",
                        "68 .CPP Files compiled with CL.EXE 16.00 (Visual Studio 2010) (build: 30319)",
                        "2   .C Files compiled with CL.EXE 15.00 (Visual Studio 2008) (build: 30729)"
                    ],
                    "imported_objects": [
                        "23 .LIB Files generated with LIB.EXE 9.00 (Visual Studio 2008) (build: 30729)",
                        "23 .ASM Files assembled with MASM 10.00 (Visual Studio 2010) (build: 30319)",
                        "1 .CPP Files compiled with CL.EXE 15.00 (Visual Studio 2008) (build: 30729)"
                    ],
                    "file_analysis": [
                        "File contains C++ code",
                        "File appears to contain raw COFF/OMF content",
                        "File was optimized using LTCG and/or POGO",
                        "File is the product of a large codebase (228 files)"
                    ]
                },
                "classification": [
                    "61.7% (.EXE) Win64 Executable (generic)",
                    "14.7% (.DLL) Win32 Dynamic Link Library (generic)",
                    "10.0% (.EXE) Win32 Executable (generic)",
                    "4.5% (.EXE) OS/2 Executable (generic)",
                    "4.4% (.EXE) Generic Win/DOS Executable"
                ],
                "contacted_hosts": [
                    {
                        "address": "54.214.246.97",
                        "port": 80,
                        "protocol": "TCP",
                        "associated_runtime": [
                            {
                                "name": "malware-ransom-cerber.exe",
                                "pid": 2908
                            }
                        ],
                        "country": "United States"
                    }
                ],
                "extracted_interesting_strings": [
                    {
                        "value": ".?AV?$ctype@_W@std@@",
                        "type": "Ansi",
                        "source": "Memory/File Scan",
                        "filename": "b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66.bin"
                    },
                    {
                        "value": "\\Sessions\\1\\Windows\\ApiPort",
                        "type": "Unicode",
                        "source": "Runtime Data",
                        "process": "malware-ransom-cerber.exe"
                    }
                ],
                "signatures": [
                    {
                        "threat_level_human": "informative",
                        "category": "General",
                        "identifier": "mutant-0",
```

```
                            "type": 4,
                            "relevance": 3,
                            "name": "Creates mutants",
                            "description": "\"\\Sessions\\1\\BaseNamedObjects\\DBWinMutex\"\n \"DBWinMutex\"",
                            "origin": "Created Mutant"
                        },
                        {
                            "threat_level_human": "informative",
                            "category": "General",
                            "identifier": "network-1",
                            "type": 7,
                            "relevance": 1,
                            "name": "Contacts server",
                            "description": "\"54.214.246.97:80\"",
                            "origin": "Network Traffic"
                        }
                    ],
                    "processes": [
                        {
                            "uid": "00064797-00002908",
                            "name": "malware-ransom-cerber.exe",
                            "normalized_path": "C:\\malware-ransom-cerber.exe",
                            "sha256": "b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66",
                            "pid": 2908,
                            "icon_artifact_id": "6fc9590b42ff8dcbd51c4cddf7ec83bad13f08dcfc882dfbfae326a4c4d68e8d",
                            "process_flags": [
                                {
                                    "name": "Network Activity"
                                }
                            ],
                            "registry": [
                                {
                                    "operation": "Query",
                                    "path": "HKLM\\SYSTEM\\CONTROLSET001\\CONTROL\\MUI\\UILANGUAGES\\EN-US\\TYPE",
                                    "key": "TYPE",
                                    "value": "0000000004000000040000091000000"
                                },
                                {
                                    "operation": "Open",
                                    "path": "HKLM\\SYSTEM\\CURRENTCONTROLSET\\CONTROL\\MUI\\UILANGUAGES\
\PENDINGDELETE\\"
                                }
                            ],
                            "mutants": [
                                "\\Sessions\\1\\BaseNamedObjects\\DBWinMutex",
                                "DBWinMutex"
                            ],
                            "handles": [
                                {
                                    "id": 4,
                                    "type": "KeyHandle",
                                    "path": "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File
Execution Options"
                                },
                                {
                                    "id": 8,
                                    "type": "KeyHandle",
                                    "path": "HKLM\\SYSTEM\\ControlSet001\\Control\\SESSION MANAGER"
                                }
                            ],
                            "file_accesses": [
                                {
                                    "type": "CREATE",
```

```
                        "path": "\\DEVICE\\NETBT_TCPIP_{C3450F58-7060-4AEA-B0A0-C245927D78D0}",
                        "mask": "FILE_READ_DATA"
                    }
                ]
            }
        ],
        "screenshots_artifact_ids": [
            "90efed5c7f1ab7d4e7c1c7218ffdc3b97337fb56c7f385f4db6bea97ff1c6971"
        ],
        "file_imports": [
            {
                "module": "ADVAPI32.dll",
                "functions": [
                    "ChangeServiceConfigW",
                    "CloseServiceHandle",
                    "OpenSCManagerW"
                ]
            },
            {
                "module": "KERNEL32.dll",
                "functions": [
                    "CloseHandle",
                    "CompareStringW",
                    "CreateDirectoryW",
                    "CreateFileW"
                ]
            }
        ],
        "architecture": "32 Bit",
        "packer": "VC8 -> Microsoft Corporation",
        "sample_flags": [
            "Network Traffic"
        ],
        "mitre_attacks": [
            {
                "tactic": "Persistence",
                "technique": "Kernel Modules and Extensions",
                "attack_id": "T1215",
                "informative_identifiers": [
                    "Opens the Kernel Security Device Driver (KsecDD) of Windows"
                ]
            },
            {
                "tactic": "Persistence",
                "technique": "Hooking",
                "attack_id": "T1179",
                "suspicious_identifiers": [
                    "Installs hooks/patches the running process"
                ]
            }
        ],
        "pcap_report_artifact_id": "9c4e58f37151e40b7ffc262fa21c94c90cfdaaf92605a2eae155ae12ff5103a8",
        "memory_strings_artifact_id": "39d08bfb8a113aca310b617922aa68024eaeb730f3248d0f5ddf0af983c4b2b6"
    }
],
"malquery": [
    {
        "verdict": "pua",
        "input": "b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66",
        "type": "sha256",
        "resources": [
            {
                "sha256": "89fd45344d44ebf2062a5c7052f1293a0d1ae148818528cd64ab63914c3d8e71",
```

```
                        "md5": "054973ed2d69bdc969ff018e3bb3d610",
                        "sha1": "5583c5c0435dae9807966294ac8809d32c3a9fbb",
                        "family": "Adload",
                        "label": "malware",
                        "file_size": 245248,
                        "file_type": "PE32",
                        "first_seen_timestamp": "2019-11-01T00:00:00Z"
                    },
                    {
                        "sha256": "49ef703699d7ebcdff63c2108c0b9ab3b4ff8cc18c53d4acd50345ca1a6f1207",
                        "md5": "a5a58df030caf79ed2a476a7c5586d04",
                        "sha1": "b4d9d9b38b3d417bc2174d73bd5c9d38dc95cf4f",
                        "family": "Adload",
                        "label": "malware",
                        "file_size": 245248,
                        "file_type": "PE32",
                        "first_seen_timestamp": "2019-10-25T00:00:00Z"
                    }
                ]
            }
        ],
        "threat_graph": {
            "indicators": [
                {
                    "type": "sha256",
                    "value": "b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66",
                    "global_prevalence": "common"
                }
            ]
        },
        "tags": [
            "adload"
        ]
    }
],
"errors": []
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
resources[].sandbox[].submit_name	Report.Name	N/A	'malware-ransom-cerber'	To create the Report Name we add 'Falcon X Report' before the key ('Falcon X Report malware-ransom-cerber').
resources[].created_timestamp	Report.published_at	N/A	'2020-09-25T17:12:55Z'	
resources[].sandbox[].sha256	Related.Indicator	SHA-256	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66'	
resources[].sandbox[].environment_description	Report.Attribute	Environment Description	'Windows 7 64 bit'	
resources[].sandbox[].file_size	Report.Attribute	File Size	'218112'	
resources[].sandbox[].file_type	Report.Attribute	File Type	'PE32 executable (GUI) Intel 80386, for MS Windows'	
resources[].sandbox[].file_type_short[]	Report.Attribute	File Type Short	'peexe'	
resources[].sandbox[].submission_type	Report.Attribute	Submission Type	'file'	
resources[].sandbox[].verdict	Report.Attribute	Verdict	'malicious'	
resources[].sandbox[].threat_score	Report.Attribute	Threat Score	'61'	
resources[].sandbox[].incidents[].name	Report.Attribute	Incident Name	'Fingerprint'	
resources[].sandbox[].incidents[].details	Report.Attribute	Incident Detail	'Reads the active computer name'	
resources[].sandbox[].classification[]	Report.Attribute	Classification	'"61.7% (.EXE) Win64 Executable (generic)"'	
resources[].sandbox[].contacted_hosts[].country	Report.Attribute and Related Indicator.Attribute	Host Country	'United States'	
resources[].sandbox[].contacted_hosts[].address	Related Indicator	IP Address	'54.214.246.97'	
resources[].sandbox[].contacted_hosts[].port	Related Indicator.Attribute	Port	'80'	
resources[].sandbox[].contacted_hosts[].protocol	Related Indicator.Attribute	Protocol	'TCP'	
resources[].sandbox[].contacted_hosts.associated_runtime.name	Related Indicator.Indicator	Filename	'malware-ransom-cerber.exe'	
resources[].sandbox[].extracted_interesting_strings[].filename	Related Indicator	Filename	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66.bin'	
resources[].sandbox[].extracted_interesting_strings[].process	Related Indicator	Filename	'malware-ransom-cerber.exe'	
resources[].sandbox[].signatures.name	Related Signature.Name	Custom	'Creates mutants'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
resources[].sandbox[].signatures.description	Related Signature.Value and Related Signature.Description	N/A	'"\Sessions\1\BaseNamedObjects\ DBWinMutex"\n "DBWinMutex"'	
resources[].sandbox[].signatures.category	Related Signature.Attribute	Category	'General'	
resources[].sandbox[].signatures.identifier	Related Signature.Attribute	Identifier	'mutant-0'	
resources[].sandbox[].signatures.type	Related Signature.Attribute	Type	'4'	
resources[].sandbox[].signatures.relevance	Related Signature.Attribute	Relevance	'3'	
resources[].sandbox[].signatures.origin	Related Signature.Attribute	Origin	'Created Mutant'	
resources[].sandbox[].processes.name	Related Indicator	Filename	'malware-ransom-cerber.exe'	
resources[].sandbox[].processes.process_flags[].name	Related Indicator.Attribute	Name	'Network Activity'	
resources[].sandbox[].processes.sha256	Related Indicator.Indicator	SHA-256	'b9079fb0fff9f40d7b5544f29 d260b1659d8fcf019deadc72 ec2c12882203a66'	
resources[].sandbox[].processes.registry[].path	Related Indicator.Registry	Registry Key	'HKLM\SYSTEM\CONTROLSET 001\CONTROL\MUI\UILANGU AGES\EN-US\TYPE'	
resources[].sandbox[].processes.registry[].key	Related Indicator.Registry.Attribute	Key	'TYPE'	
resources[].sandbox[].processes.registry[].value	Related Indicator.Registry.Attribute	Value	'0000000004000000040000000 91000000'	
resources[].sandbox[].processes.file_accesses[].path	Related Indicator.Indicator	File Path	'\DEVICE\NETBT_TCPIP_{C3450F 58-7060-4AEA-B0A0-C245927D7 8D0}'	
resources[].sandbox[].mitre_attacks[].attack_id	Related Attack_pattern	Attack Pattern	'T1179'	
resources[].malquery[].resources[].family	Related Malware	Malware	'Adload'	
resources[].malquery[].resources[].file_size	Related Malware.Attribute	File Size	'245248'	
resources[].malquery[].resources[].file_type	Related Malware.Attribute	File Type	'PE32'	
resources[].malquery[].input	Related Malware.Indicator	SHA-256 or URL	'b9079fb0fff9f40d7b5544f29d26 0b1659d8fcf019deadc72ec2c12 882203a66'	Type determined based on '.type'.
resources[].malquery[].resources[].sha256	Related Malware.Indicator	SHA-256	'89fd45344d44ebf2062a5c7052f 1293a0d1ae148818528cd64ab6 3914c3d8e71'	
resources[].malquery[].resources[].md5	Related Malware.Indicator	MD5	'054973ed2d69bdc969ff018e3b b3d610'	
resources[].malquery[].resources[].sha1	Related Malware.Indicator	SHA-1	'5583c5c0435dae9807966294a c8809d32c3a9fbb'	
resources[].threat_graph.indicators[].value	Related Indicator	SHA-256	'b9079fb0fff9f40d7b5544f29d26 0b1659d8fcf019deadc72ec2c128 82203a66'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
resources[].tags[]	Report.Tags	N/A	'adload'	

Average Feed Run

Average Feed Run results for Falcon X Sandbox:

METRIC	RESULT
Run Time	6 minutes
Reports	41
Report Attributes	530
Indicators	2,104
Indicator Attributes	1,261
Attack Patterns	15
Malwares	15
Malware Attributes	91
Signatures	329
Signature Attributes	1,597

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Change Log

- **Version 1.0.0**
  - Initial release