ThreatQuotient

Proofpoint ET Signatures CDF User Guide

Version 1.0.0

February 20, 2024

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	1.0.0
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

The Proofpoint Emerging Threats Signatures CDF for ThreatQuotient enables a ThreatQ user to import Snort rules from Emerging Threats.

The integration provides the following feed:

- **Proofpoint Emerging Threats Signatures** - ingests Snort Signatures Adversary objects.

The integration ingests the following system objects:

- Signatures
- Indicators
- Malware

Prerequisites

If you are a Proofpoint Pro user, you will need your Oinkcode to use access the Pro version.

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.

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

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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Version	Select your version of Proofpoint. Options include **Open** and **Pro**.
ET Pro Oinkcode	Enter your Oinkcode if you selected the **Pro** version above.
Which Rules Do You Want to Import	Select which rules to import. Options include: ◦ Snort 2.9.0 ◦ Snort Edge ◦ Suricata 4.0 ◦ Suricata 5.0
Block Rules Snort 2.9.0	If you selected to import Snort 2.9.0, select which Block Rules Snort 2.9.0 rules to import. Options include: ◦ 3coresec.rules ◦ emerging-botcc.portgrouped.rules ◦ emerging-botcc.rules ◦ emerging-ciarmy.rules ◦ emerging-compromised.rules ◦ emerging-drop.rules ◦ emerging-dshield.rules ◦ emerging-tor.rules ◦ threatview_CS_c2.rules

PARAMETER	DESCRIPTION
Block Rules Snort Edge	If you selected to import Snort Edge, select which Block Rules Snort Edge rules to import. Options include: ◦ 3coresec.rules ◦ emerging-botcc.portgrouped.rules ◦ emerging-botcc.rules ◦ emerging-ciarmy.rules ◦ emerging-compromised.rules ◦ emerging-drop.rules ◦ emerging-dshield.rules ◦ emerging-tor.rules ◦ threatview_CS_c2.rules
Block Rules Suricata 4.0	If you selected to import Suricata 4.0 , select which Block Rules Sucricata rules to import. Options include: ◦ 3coresec.suricata.rules ◦ emerging-botcc.portgrouped.suricata.rules ◦ emerging-botcc.suricata.rules ◦ emerging-ciarmy.suricata.rules ◦ emerging-compromised.suricata.rules ◦ emerging-drop.suricata.rules ◦ emerging-dshield.suricata.rules ◦ emerging-tor.suricata.rules ◦ threatview_CS_c2.suricata.rules
Block Rules Suricata 5.0	If you selected to import Sucricata 5.0, select which Block Rules Scuricata 5.0 rules to import. Options include: ◦ 3coresec.suricata.rules ◦ emerging-botcc.portgrouped.suricata.rules ◦ emerging-botcc.suricata.rules ◦ emerging-ciarmy.suricata.rules ◦ emerging-compromised.suricata.rules ◦ emerging-drop.suricata.rules ◦ emerging-dshield.suricata.rules ◦ emerging-tor.suricata.rules ◦ threatview_CS_c2.suricata.rules
ET Snort 2.9.0 Rules	If you selected to import Snort 2.9.0, select which Snort 2.9.0 rules to import. Options include:

PARAMETER	DESCRIPTION
	◦ All Rules ◦ 3coresec.rules ◦ activex.rules ◦ attack_response.rules ◦ botcc.portgrouped.rules ◦ botcc.rules ◦ chat.rules ◦ ciarmy.rules ◦ compromised.rules ◦ current_events.rules ◦ deleted.rules ◦ dns.rules ◦ dos.rules ◦ drop.rules ◦ dshield.rules ◦ exploit.rules ◦ ftp.rules ◦ games.rules ◦ icmp.rules ◦ icmp_info.rules ◦ imap.rules ◦ inappropriate.rules ◦ info.rules ◦ malware.rules ◦ misc.rules ◦ mobile_malware.rules ◦ netbios.rules ◦ p2p.rules ◦ policy.rules ◦ pop3.rules ◦ rpc.rules ◦ scada.rules ◦ scada_special.rules (Pro Only) ◦ scan.rules ◦ shellcode.rules ◦ smtp.rules ◦ snmp.rules ◦ sql.rules ◦ telnet.rules ◦ tftp.rules ◦ threatview_CS_c2.rules ◦ tor.rules ◦ trojan.rules ◦ user_agents.rules ◦ voip.rules ◦ web_client.rules ◦ web_server.rules ◦ web_specific_apps.rules ◦ worm.rules
ET Snort Edge Rules	If you selected to import SnortEdge, select which Snort Edge rules to import. Options include: ◦ All Rules ◦ 3coresec.rules ◦ activex.rules ◦ attack_response.rules ◦ botcc.portgrouped.rules ◦ botcc.rules ◦ chat.rules ◦ ciarmy.rules ◦ compromised.rules ◦ current_events.rules ◦ deleted.rules ◦ mobile_malware.rules ◦ netbios.rules ◦ p2p.rules ◦ policy.rules ◦ pop3.rules ◦ rpc.rules ◦ scada.rules ◦ scada_special.rules (Pro Only) ◦ scan.rules ◦ shellcode.rules ◦ smtp.rules

PARAMETER	DESCRIPTION
	◦ dns.rules ◦ dos.rules ◦ drop.rules ◦ dshield.rules ◦ exploit.rules ◦ ftp.rules ◦ games.rules ◦ icmp.rules ◦ icmp_info.rules ◦ imap.rules ◦ inappropriate.rules ◦ info.rules ◦ malware.rules ◦ misc.rules ◦ snmp.rules ◦ sql.rules ◦ telnet.rules ◦ tftp.rules ◦ threatview_CS_c2.rules ◦ tor.rules ◦ trojan.rules ◦ user_agents.rules ◦ voip.rules ◦ web_client.rules ◦ web_server.rules ◦ web_specific_apps.rules ◦ worm.rules
ET Suricata 4.0 Rules	If you selected to import Suricata 4.0, select which Suricata 4.0 rules to import. Options include: ◦ All Rules ◦ 3coresec.rules ◦ activex.rules ◦ attack_response.rules ◦ botcc.portgrouped.rules ◦ botcc.rules ◦ chat.rules ◦ ciarmy.rules ◦ compromised.rules ◦ current_events.rules ◦ deleted.rules ◦ dns.rules ◦ dos.rules ◦ drop.rules ◦ dshield.rules ◦ exploit.rules ◦ ftp.rules ◦ games.rules ◦ icmp.rules ◦ icmp_info.rules ◦ imap.rules ◦ inappropriate.rules ◦ mobile_malware.rules ◦ netbios.rules ◦ p2p.rules ◦ policy.rules ◦ pop3.rules ◦ rpc.rules ◦ scada.rules ◦ scada_special.rules (Pro Only) ◦ scan.rules ◦ shellcode.rules ◦ smtp.rules ◦ snmp.rules ◦ sql.rules ◦ telnet.rules ◦ tftp.rules ◦ threatview_CS_c2.rules ◦ tor.rules ◦ trojan.rules ◦ user_agents.rules ◦ voip.rules ◦ web_client.rules ◦ web_server.rules

PARAMETER	DESCRIPTION
	◦ info.rules ◦ malware.rules ◦ misc.rules ◦ web_specific_apps.rules ◦ worm.rules
ET Suricata 5.0 Rules	If you selected to import Suricata 5.0, select which Suricata 5.0 rules to import. Options include: ◦ All Rules ◦ 3coresec.rules ◦ activex.rules ◦ attack_response.rules ◦ botcc.portgrouped.rules ◦ botcc.rules ◦ chat.rules ◦ ciarmy.rules ◦ compromised.rules ◦ current_events.rules ◦ deleted.rules ◦ dns.rules ◦ dos.rules ◦ drop.rules ◦ dshield.rules ◦ exploit.rules ◦ ftp.rules ◦ games.rules ◦ icmp.rules ◦ icmp_info.rules ◦ imap.rules ◦ inappropriate.rules ◦ info.rules ◦ malware.rules ◦ misc.rules ◦ mobile_malware.rules ◦ netbios.rules ◦ p2p.rules ◦ policy.rules ◦ pop3.rules ◦ rpc.rules ◦ scada.rules ◦ scada_special.rules (Pro Only) ◦ scan.rules ◦ shellcode.rules ◦ smtp.rules ◦ snmp.rules ◦ sql.rules ◦ telnet.rules ◦ tftp.rules ◦ threatview_CS_c2.rules ◦ tor.rules ◦ trojan.rules ◦ user_agents.rules ◦ voip.rules ◦ web_client.rules ◦ web_server.rules ◦ web_specific_apps.rules ◦ worm.rules

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.

ThreatQ Mapping

Proofpoint Emerging Threats Signatures

The Proofpoint Emerging Threats Signatures feed ingests Snort Signature Adversary objects.

```
GET https://rules.emergingthreats.net/open/snort-2.9.0/rules/emerging-botcc.rules
```

Sample Response:

```
alert tcp $HOME_NET any -> [104.129.55.103] any (msg:"ET CNC Feodo Tracker
Reported CnC Server TCP group 1"; flags:S;
reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,feodotracker.abuse.ch; threshold: type limit, track by_src,
seconds 3600, count 1; classtype:trojan-activity; flowbits:set,ET.Evil;
flowbits:set,ET.BotccIP; sid:2404300; rev:7100; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
deployment Perimeter, tag Banking_Trojan, signature_severity Major, created_at
2014_11_04, updated_at 2024_02_12;)
alert udp $HOME_NET any -> [104.129.55.103] any (msg:"ET CNC Feodo Tracker
Reported CnC Server UDP group 1"; reference:url,doc.emergingthreats.net/bin/
view/Main/BotCC; reference:url,feodotracker.abuse.ch; threshold: type limit,
track by_src, seconds 3600, count 1; classtype:trojan-activity;
flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2404301; rev:7100;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, tag Banking_Trojan,
signature_severity Major, created_at 2014_11_04, updated_at 2024_02_12;)
alert tcp $HOME_NET any -> [104.129.55.104] any (msg:"ET CNC Feodo Tracker
Reported CnC Server TCP group 2"; flags:S;
reference:url,doc.emergingthreats.net/bin/view/Main/BotCC;
reference:url,feodotracker.abuse.ch; threshold: type limit, track by_src,
seconds 3600, count 1; classtype:trojan-activity; flowbits:set,ET.Evil;
flowbits:set,ET.BotccIP; sid:2404302; rev:7100; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
deployment Perimeter, tag Banking_Trojan, signature_severity Major, created_at
2014_11_04, updated_at 2024_02_12;)
alert udp $HOME_NET any -> [104.129.55.104] any (msg:"ET CNC Feodo Tracker
Reported CnC Server UDP group 2"; reference:url,doc.emergingthreats.net/bin/
view/Main/BotCC; reference:url,feodotracker.abuse.ch; threshold: type limit,
track by_src, seconds 3600, count 1; classtype:trojan-activity;
flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2404303; rev:7100;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, tag Banking_Trojan,
signature_severity Major, created_at 2014_11_04, updated_at 2024_02_12;)
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE
Win32.LoadMoney User Agent"; flow:established,to_server; content:"User-Agent|3a
```

```
20|Downloader "; http_header; fast_pattern:12,11; pcre:"/^User-Agent\x3a
Downloader \d\.\d\r?$/Hm"; reference:url,www.microsoft.com/security/portal/
threat/encyclopedia/Entry.aspx?Name=PUA:Win32/LoadMoney; classtype:trojan-
activity; sid:2024260; rev:4; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2017_04_27, deployment Perimeter, former_category ADWARE_PUP,
malware_family Loadmoney, performance_impact Low, signature_severity Minor, tag
Loadmoney, updated_at 2017_04_27;)
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Data
Dynamics ActiveBar ActiveX Control (Actbar3.ocx 3.2) Multiple Insecure
Methods"; flow:to_client,established; file_data;
content:"5407153D-022F-4CD2-8BFF-465569BC5DB8"; distance:0; content:"Save";
distance:0; nocase; pcre:"/.*\.(ini|exe|dll|bat|com|cab|txt)/i"; pcre:"/(Save|
SaveLayoutChanges|SaveMenuUsageData)/i"; reference:bugtraq,24959;
reference:cve,CVE-2007-3883; reference:url,www.exploit-db.com/exploits/5395/;
reference:url,doc.emergingthreats.net/2008127; classtype:web-application-
attack; sid:2008127; rev:15; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
ActiveX, updated_at 2010_10_15;)
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data	Signature.Name	N/A	N/A	ET CNC Feodo Tracker Reported CnC Server TCP group 1	N/A
.data	Signature.Value	N/A	N/A	alert tcp $HOME_NET any -> [104.129.55.103] any (msg:"ET CNC Feodo Tracker Reported CnC Server TCP group 1"; flags:S; reference:url,doc.emergingthreats.net/bin/view/Main/BotCC; reference:url,feodotracker.abuse.ch; threshold: type limit, track by_src, seconds 3600, count 1; classtype:trojan-activity; flowbits:set,ET.Evil; flowbits:set,ET.BotccIP; sid:2404300; rev:7100; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag Banking_Trojan, signature_severity Major, created_at 2014_11_04, updated_at 2024_02_12;)	N/A
.data	Signature.Attribute	Signature Severity	N/A	Major	N/A
.data	Signature.Attribute	Created At	N/A	2014_11_04	N/A
.data	Signature.Attribute	Tag	N/A	Banking_Trojan	N/A
.data	Signature.Attribute	Deployment	N/A	Perimeter	N/A
.data	Signature.Attribute	Attack Target	N/A	Client_Endpoint	N/A
.data	Signature.Attribute	Affected Product	N/A	Windows_XP_Vista_7_8_10_Server_32_64_Bit	N/A
.data	Signature.Attribute	Classtype	N/A	trojan-activity	N/A
.data	Signature.Attribute	Threshold	N/A	type limit, track by_src, seconds 3600, count 1	N/A
.data	Signature.Attribute	SID	N/A	2404300	N/A
.data	Signature.Attribute	REV	N/A	7100	N/A
.data	Related.Malware.Value	N/A	N/A	Loadmoney	N/A
.data	Related.Indicator.Value	CVE	N/A	CVE-2007-3883	N/A

Average Feed Run

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.

METRIC	RESULT
Run Time	3 minutes
Signature	123
Signature Attributes	1,230

Known Issues / Limitations

- Several rule collections may contain a substantial number of signatures. Selecting multiple rule collections to run simultaneously can result in timeout error.

Change Log

- **Version 1.0.0**
  - Initial release