CERT Australia CTI Toolkit Documentation

Release v1.0

CERT Australia, Australian Government

Nov 14, 2017

Contents

This package contains cyber threat intelligence (CTI) tools created by CERT Australia.

Contents:

CHAPTER 1

About the CTI-Toolkit

Few systems can utilise indicators and observables when stored in STIX packages. CERT Australia has developed a utility (`stixtransclient.py`) that allows the atomic observables contained within a STIX package to be extracted and presented in either a text delimited format, in the Bro Intel Framework format, or in a Snort or Suricata rule format . The utility can also communicate with a MISP server and insert observables from a STIX package into a new MISP event.

CHAPTER 2

Installation

This document describes how to install the CERT Australia CTI Toolkit.

Installation is streamlined using Python's setuptools. The following installation process has been tested on clean install of Ubuntu Server 16.04.

1. Install prerequisites required by setuptools and libtaxii:

```
$ sudo apt-get install python-pip python-dev libxml2-dev libxslt1-dev libz-dev
```

2. Install the cti-toolkit:

```
$ sudo pip install cti-toolkit
```

That's it. You should now be able to run utilities, such as `stixtransclient.py`:

```
$ stixtransclient.py -h
```

2.1 Documentation

Online documentation is available at http://cti-toolkit.readthedocs.org/.

To build the documentation you need Sphinx:

```
$ sudo pip install Sphinx sphinxcontrib-napoleon sphinx_rtd_theme
$ cd docs
$ make html
```

This will create an HTML version of the documentation in `docs/_build/html`.

2.2 Tests

Requires tox:

```
$ sudo pip install tox
```

Then run the tests from the repository root using:

```
$ tox
```

CHAPTER 3

Command line options

The command line (and configuration) options for `stixtransclient.py` are displayed below. For a more detailed explanation, including examples, please see the *Configuration examples* page:

```
$ stixtransclient.py -h

usage: stixtransclient.py [-h] [-c CONFIG] [-v] [-d] [-V]
                          (--file FILE [FILE ...] | --taxii)
                          (-s | -t | -b | -m | --snort | -x XML_OUTPUT) [-r]
                          [--poll-url POLL_URL] [--hostname HOSTNAME]
                          [--port PORT] [--ca_file CA_FILE]
                          [--username USERNAME] [--password PASSWORD] [--ssl]
                          [--key KEY] [--cert CERT] [--path PATH]
                          [--collection COLLECTION]
                          [--begin-timestamp BEGIN_TIMESTAMP]
                          [--end-timestamp END_TIMESTAMP]
                          [--subscription-id SUBSCRIPTION_ID]
                          [--state-file STATE_FILE] [-f FIELD_SEPARATOR]
                          [--header] [--default-title DEFAULT_TITLE]
                          [--default-description DEFAULT_DESCRIPTION]
                          [--default-tlp {WHITE,GREEN,AMBER,RED}]
                          [--source SOURCE] [--bro-no-notice]
                          [--base-url BASE_URL]
                          [--snort-initial-sid SNORT_INITIAL_SID]
                          [--snort-rule-revision SNORT_RULE_REVISION]
                          [--snort-rule-action {alert,log,pass,activate,dynamic,drop,
↪reject,sdrop}]
                          [--misp-url MISP_URL] [--misp-key MISP_KEY]
                          [--misp-ssl [MISP_SSL]]
                          [--misp-client-cert MISP_CLIENT_CERT]
                          [--misp-client-key MISP_CLIENT_KEY]
                          [--misp-distribution MISP_DISTRIBUTION]
                          [--misp-threat MISP_THREAT]
                          [--misp-analysis MISP_ANALYSIS]
                          [--misp-info MISP_INFO] [--misp-published]
                          [--ais-marking] [--ais-proprietary]
```

```
                          [--ais-consent {EVERYONE,NONE,USG}]
                          [--ais-default-tlp {WHITE,GREEN,AMBER,RED}]
                          [--ais-country AIS_COUNTRY]
                          [--ais-administrative-area AIS_ADMINISTRATIVE_AREA]
                          [--ais-organisation AIS_ORGANISATION]
                          [--ais-industry-type {Chemical Sector,Commercial Facilities␣
↪Sector,Communications Sector,Critical Manufacturing Sector,Dams Sector,Defense␣
↪Industrial Base Sector,Emergency Services Sector,Energy Sector,Financial Services␣
↪Sector,Food and Agriculture Sector,Government Facilities Sector,Healthcare and␣
↪Public Health Sector,Information Technology Sector,Nuclear Reactors, Materials, and␣
↪Waste Sector,Other,Transportation Systems Sector,Water and Wastewater Systems␣
↪Sector}]

Utility to extract observables from local STIX files or a TAXII server. Args
that start with '--' (eg. -v) can also be set in a config file
(/etc/ctitoolkit.conf or ~/.ctitoolkit or specified via -c). Config file
syntax allows: key=value, flag=true, stuff=[a,b,c] (for details, see syntax at
https://goo.gl/R74nmi). If an arg is specified in more than one place, then
commandline values override config file values which override defaults.

optional arguments:
  -h, --help            show this help message and exit

global arguments:
  -c CONFIG, --config CONFIG
                        configuration file to use
  -v, --verbose         verbose output
  -d, --debug           enable debug output
  -V, --version         show program's version number and exit

input (source) options:
  --file FILE [FILE ...]
                        obtain STIX packages from supplied files or
                        directories
  --taxii               poll TAXII server to obtain STIX packages

output (transform) options:
  -s, --stats           display summary statistics for each STIX package
  -t, --text            output observables in delimited text
  -b, --bro             output observables in Bro intel framework format
  -m, --misp            feed output to a MISP server
  --snort               output observables in Snort rule format
  -x XML_OUTPUT, --xml_output XML_OUTPUT
                        output XML STIX packages to the given directory (use
                        with --taxii)

file input arguments (use with --file):
  -r, --recurse         recurse subdirectories when processing files.

taxii input arguments (use with --taxii):
  --poll-url POLL_URL   TAXII server's poll URL
  --hostname HOSTNAME   hostname of TAXII server (deprecated - use --poll-url)
  --port PORT           port of TAXII server (deprecated - use --poll-url)
  --ca_file CA_FILE     File containing CA certs of TAXII server
  --username USERNAME   username for TAXII authentication
  --password PASSWORD   password for TAXII authentication
  --ssl                 use SSL to connect to TAXII server (deprecated - use
                        --poll-url)
```

```
  --key KEY             file containing PEM key for TAXII SSL authentication
  --cert CERT           file containing PEM certificate for TAXII SSL
                        authentication
  --path PATH           path on TAXII server for polling (deprecated - use
                        --poll-url)
  --collection COLLECTION
                        TAXII collection to poll
  --begin-timestamp BEGIN_TIMESTAMP
                        the begin timestamp (format: YYYY-MM-
                        DDTHH:MM:SS.ssssss+/-hh:mm) for the poll request
  --end-timestamp END_TIMESTAMP
                        the end timestamp (format: YYYY-MM-
                        DDTHH:MM:SS.ssssss+/-hh:mm) for the poll request
  --subscription-id SUBSCRIPTION_ID
                        a subscription ID for the poll request
  --state-file STATE_FILE
                        file used to maintain latest poll times

other output options:
  -f FIELD_SEPARATOR, --field-separator FIELD_SEPARATOR
                        field delimiter character/string to use in text output
  --header              include header row for text output
  --default-title DEFAULT_TITLE
                        title for package (if not included in STIX file)
  --default-description DEFAULT_DESCRIPTION
                        description for package (if not included in STIX file)
  --default-tlp {WHITE,GREEN,AMBER,RED}
                        TLP colour for package (if not included in STIX file)
  --source SOURCE       source of indicators - e.g. Hailataxii, CERT-AU (use
                        with --bro)
  --bro-no-notice       suppress Bro intel notice framework messages (use with
                        --bro)
  --base-url BASE_URL   base URL for indicator source (use with --bro)

snort output arguments (use with --snort):
  --snort-initial-sid SNORT_INITIAL_SID
                        initial Snort IDs to begin from - default: 5500000
  --snort-rule-revision SNORT_RULE_REVISION
                        revision of the Snort rule - default: 1
  --snort-rule-action {alert,log,pass,activate,dynamic,drop,reject,sdrop}
                        action used for Snort rules generated - default:
                        'alert'

misp output arguments (use with --misp):
  --misp-url MISP_URL   URL of MISP server
  --misp-key MISP_KEY   token for accessing MISP instance
  --misp-ssl [MISP_SSL]
                        validate SSL certificate of the MISP server (takes an
                        optional CA certificate file)
  --misp-client-cert MISP_CLIENT_CERT
                        Client certificate for authenticating to MISP instance
  --misp-client-key MISP_CLIENT_KEY
                        Private key associated with client certificate
  --misp-distribution MISP_DISTRIBUTION
                        MISP distribution group - default: 0 (your
                        organisation only)
  --misp-threat MISP_THREAT
                        MISP threat level - default: 4 (undefined)
```

```
  --misp-analysis MISP_ANALYSIS
                        MISP analysis phase - default: 0 (initial)
  --misp-info MISP_INFO
                        MISP event description
  --misp-published      set MISP published state to True

XML (STIX) output arguments (use with --xml-output):
  --ais-marking         add the AIS Marking structure to the STIX package
  --ais-proprietary     set IsProprietary to True (otherwise False) in AIS
                        Marking
  --ais-consent {EVERYONE,NONE,USG}
                        consent level for submitter attribution in AIS Marking
  --ais-default-tlp {WHITE,GREEN,AMBER,RED}
                        TLP used in AIS Marking when none found in package
                        header
  --ais-country AIS_COUNTRY
                        ISO-3661-1 alpha2 submitter country for AIS Marking
  --ais-administrative-area AIS_ADMINISTRATIVE_AREA
                        ISO-3661-2 submitter administrative area for AIS
                        Marking
  --ais-organisation AIS_ORGANISATION
                        ISO-3661-2 submitter organisation for AIS Marking
  --ais-industry-type {Chemical Sector,Commercial Facilities Sector,Communications␣
↪Sector,Critical Manufacturing Sector,Dams Sector,Defense Industrial Base Sector,
↪Emergency Services Sector,Energy Sector,Financial Services Sector,Food and␣
↪Agriculture Sector,Government Facilities Sector,Healthcare and Public Health Sector,
↪Information Technology Sector,Nuclear Reactors, Materials, and Waste Sector,Other,
↪Transportation Systems Sector,Water and Wastewater Systems Sector}
                        submitter industry type for AIS Marking
```

CHAPTER 4

Configuration examples

The `stixtransclient.py` utility can read its configuration parameters from the following locations:

- /etc/ctitoolkit.conf
- ~/.ctitoolkit
- a configuration file specified using the `--config` command line option
- as explicit command line parameters

If a configuration option is specified in more than one of the above locations the last one processed will take precedence. Options are processed in the order listed above.

Any options that can be specified on the command line can be specified in a configuration file.

Examples explaining which options to use for various *sources* and *transforms* are provided below. It is possible to cut and paste the relevant options into a configuration file and then run `stixtransclient.py` with that configuration file using the `--config` command line option. Currently `stixtransclient.py` can only read STIX packages from a single source and output using a single transform.

4.1 STIX packages from a TAXII server

```
# Poll a collection on TAXII server
--taxii
--poll-url https://taxii.cert.gov.au/services/poll/
--collection advisories

# Provide credentials for authenticating to the TAXII server
# Credentials are optional (depending on server requirements)
--username alice
--password alice_password
--key /home/alice/keys/alice_key_file.pem
--cert /home/alice/keys/alice_cert_file.pem

# Save the poll state in a file so that subsequent polls will
```

```
# only obtain STIX packages that have not yet been downloaded
--state-file /home/alice/.taxii_poll_state

# Alternatively, specify a begin and/or end timestamp for the poll
# --begin-timestamp 2016-07-13T12:11:10+00:00
# --end-timestamp   2016-08-27T05:17:55+00:00
```

4.2 STIX packages from files

STIX packages can be read from a single file or from a directory and, optionally, subdirectories. Any files encountered that do not contain a valid STIX package will cause an error to be displayed, but processing will continue:

```
# Read a package from a single file
--file some_stix_file.xml

# Alternatively, read all the files in a directory
# --file some_directory_containing_stix_files

# Alternatively, read all the files in a directory and its subdirectories
# --file some_directory
# --recurse
```

4.3 Output statistics

```
# Display statistics (per STIX package)
--stats
```

4.4 Output text (CSV)

```
# Text (CSV) output - default separator is '|'
--text

# Optionally, specify a separator
# --field-separator ','
```

4.5 Output XML files (STIX)

Output STIX packages in files. This is useful for saving the results of polling a TAXII server. `stixtransclient.py` also allows the addition of the US DHS AIS Handling Structure to a package, prior to saving it to a file (see: https://www.us-cert.gov/ais for more details about the AIS program).

See `stixtransclient.py -h` for the full list of legal values for the AIS settings below:

```
# XML (STIX) output - specify a directory for the output
--xml-output output_directory

# Optionally, include an AIS Marking in the STIX packages
```

```
# --ais-marking
# Set the 'IsProprietary' flag in the AIS Marking
# --ais-proprietary
# Set the consent level for submitter attribution (EVERYONE, NONE, USG)
# --ais-consent USG
# Set the TLP to use if the source package does not contain one
# --ais-default-tlp AMBER
# Set the submitter country (ISO-3661-1)
# --ais-country AU
# Set the submitter administrative area (ISO-3661-2)
# --ais-administrative-area AU-ACT
# Set the submitter organisation
# --ais-organisation 'CERT Australia'
# Set the submitter industry type
# --ais-industry-type 'Other'
```

4.6 Output to a MISP server

A new MISP event will be created for each STIX package:

```
# MISP output - specify the URL and an API key
--misp
--misp-url https://misp.example.com/
--misp-key rnNB3NdKE5D0LzdKyxjzQsJ0nhys9a3NXHniLAKq

# Authentication options (optional)
# A client TLS key and certificate
# --misp-key alice_misp_key.pem
# --misp-cert alice_misp_cert.pem
# Verify the server certificate
# --misp-ssl
# Provide a file containing the CA's certificate
# --misp-ssl ca_certificate.pem

# Set MISP event values (optional)
# Distribution (default 0 - your organisation only)
# --misp-distribution 1
# Threat (default 4 - undefined)
# --misp-threat 3
# Analysis (default 0 - initial)
# --misp-analysis 2
# Information (taken from package title and description if available)
# --misp-info 'This is the event description'
# Published (default False)
# --misp-published
```

4.7 Output Bro Intel Framework rules

```
# BIF output
--bro

# Suppress Bro notices for matches (optional)
# --bro-no-notice
```

```
# Provide source and/or url fields for Bro output (optional)
# --source Hailataxii
# --base-url http://hailataxii.com/
```

4.8 Output Snort or Suricata rules

```
# Snort output
--snort

# Other snort options (optional)
# SID of first rule (incremented in subsequent rules)
# --snort-initial-sid 6600000
# A revision number for the rules (default 1)
# --snort-rule-revision 3
# The snort action on a match (default 'alert')
# --snort-action drop
```

4.9 General output options

The following options can be used with all output transforms:

```
# Specify a default title, description, or TLP to be used
# when the STIX package does not contain these values
# --default-title 'Some package title'
# --default-description 'A package description'
# --default-tlp 'WHITE'
```

CHAPTER 5

Output samples

Below you will find samples of output from the various transforms.

5.1 Statistics output

Display summary statistics about the object types (observables) contained in a STIX package (file):

```
$ stixtransclient.py --file CA-TEST-STIX.xml --stats

++++++++++++++++++++++++++++++++++++++
Summary statistics: CA-TEST-STIX (WHITE)
++++++++++++++++++++++++++++++++++++++
Address observables:                  2
DomainName observables:               3
EmailMessage observables:             2
File observables:                     6
HTTPSession observables:              1
Mutex observables:                    3
SocketAddress observables:            1
URI observables:                      1
WinRegistryKey observables:           1
```

5.2 Text (CSV) output

Display observable details in text (delimited) format:

```
$ stixtransclient.py --file CA-TEST-STIX.xml --text

# CA-TEST-STIX (TLP:WHITE)

# Address observables
```

```
# id|category|address
cert_au:Observable-fe5ddeac-f9b0-4488-9f89-bfbd9351efd4|ipv4-addr|158.164.39.51
cert_au:Observable-ccccceac-f9b0-4488-9f89-bfbd9351efd4|ipv4-addr|111.222.33.44

# DomainName observables
# id|domain|domain_condition
cert_au:Observable-6517027e-2cdb-47e8-b5c8-50c6044e42de|bad.domain.org|None
cert_au:Observable-c97cc016-24b6-4d02-afc2-308742c722dc|dnsupdate.dyn.net|None
cert_au:Observable-138a5be6-56b2-4d2d-af73-2d4865d6ff71|free.stuff.com|None

# EmailMessage observables
# id|fromaddr|fromaddr_condition|toaddr|toaddr_condition|subject|subject_
↪condition|attachment_ref
cert_au:Observable-b6770e76-7f05-48cb-a3de-7ba5fece8751|sender@domain.
↪tld|Equals|None|None|None|None|None
cert_au:Observable-31e5af27-2f71-4922-b49c-cfd3ddee2963|None|None|None|None|Important␣
↪project details|Equals|cert_au:Observable-5d647351-f8cf-442f-9e5a-ba6967c16301

# File observables
# id|file_name|file_name_condition|hash_type|hashes
cert_au:Observable-5d647351-f8cf-442f-9e5a-ba6967cccccc|filenameonly.
↪doc|None|None|None
cert_au:Observable-5d647351-f8cf-442f-9e5a-ba6967c16301|project.
↪doc|Equals|MD5|1111111111b42b57f518197d930471d9
cert_au:Observable-cccccd51-a524-483f-8f17-
↪2e8ff8474d80|None|None|MD5|ccccccccccccccc33574c79829dc1ccf
cert_au:Observable-84060d51-a524-483f-8f17-2e8ff8474d80|Execute_this.
↪jar|Equals|MD5|11111111111111133574c79829dc1ccf
cert_au:Observable-3ad6c684-80aa-4d92-9fef-7a9f70ccba95|malware.
↪exe|Equals|MD5|1111111111111111f2601b4d21660fb
cert_au:Observable-7cb2ac9f-4cae-443f-905d-0b01cb1faedc|VPN.
↪exe|Equals|SHA256|11111111111111119f167683e164e795896be3be94de7f7103f67c6fde667bdf
cert_au:Observable-7cb2ac9f-4cae-443f-905d-0b01cb1faedc|VPN.
↪exe|Equals|SHA1|893fb19ac24eabf9b1fe1ddd1111111111111111
cert_au:Observable-7cb2ac9f-4cae-443f-905d-0b01cb1faedc|VPN.
↪exe|Equals|MD5|11111111111111112977fa0588bd504a

# HTTPSession observables
# id|user_agent|user_agent_condition
cert_au:Observable-6a733d83-5d19-4d17-a51f-5bcb4ebc860a|Mozilla/5.0 (Windows NT 5.1)␣
↪AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.372 Safari/537.36|None

# Mutex observables
# id|mutex|mutex_condition
NCCIC:Observable-01234567-6868-4ffd-babc-ba2ad0e34f43|WIN_ABCDEF|None
NCCIC:Observable-abcdef01-3363-4533-a77c-10d71c371282|MUTEX_0001|None
CCIRC-CCRIC:Observable-01234567-e44c-473a-85c6-fc6c2e781114|iurlkjashdk|Equals

# SocketAddress observables
# id|category|address|port_value|port_protocol
CCIRC-CCRIC:Observable-01234567-2823-4d6d-8d77-bae10ca5bd97|ipv4-addr|183.82.180.
↪95|2665|TCP

# URI observables
# id|uri|uri_condition
cert_au:Observable-1a919136-ba69-4a28-9615-ad6ee37e88a5|http://host.domain.tld/path/
↪file|None
```

```
# WinRegistryKey observables
# id|hive|hive_condition|key|key_condition|name|name_condition|data|data_condition
cert_au:Observable-d0f4708e-4f2b-49c9-bc31-29e7119844e5|HKEY_CURRENT_
↪USER\Software|Equals|\Microsoft\Windows\CurrentVersion\Run|Equals|hotkey|Equals|
↪%APPDATA%\malware.exe -st|Equals
```

5.3 Bro Intel Framework output

Display observables in the format used by the Bro Intelligence Framework (with a header row explaining columns):

```
$ stixtransclient.py --file CA-TEST-STIX.xml --bro --header

# indicator indicator_type  meta.source     meta.url        meta.do_notice  meta.if_
↪in      meta.whitelist
158.164.39.51       Intel::ADDR     CERT-AU https://www.cert.gov.au/        T       -␣
↪       -
111.222.33.44       Intel::ADDR     CERT-AU https://www.cert.gov.au/        T       -␣
↪       -
bad.domain.org      Intel::DOMAIN   CERT-AU https://www.cert.gov.au/        T       -␣
↪       -
dnsupdate.dyn.net   Intel::DOMAIN   CERT-AU https://www.cert.gov.au/        T       -␣
↪       -
free.stuff.com      Intel::DOMAIN   CERT-AU https://www.cert.gov.au/        T       -␣
↪       -
sender@domain.tld   Intel::EMAIL    CERT-AU https://www.cert.gov.au/        T       -␣
↪       -
1111111111b42b57f518197d930471d9    Intel::FILE_HASH        CERT-AU https://www.cert.
↪gov.au/        T       -       -
ccccccccccccccc33574c79829dc1ccf    Intel::FILE_HASH        CERT-AU https://www.cert.
↪gov.au/        T       -       -
11111111111111133574c79829dc1ccf    Intel::FILE_HASH        CERT-AU https://www.cert.
↪gov.au/        T       -       -
111111111111111f2601b4d21660fb    Intel::FILE_HASH        CERT-AU https://www.cert.
↪gov.au/        T       -       -
1111111111111119f167683e164e795896be3be94de7f7103f67c6fde667bdf    Intel::FILE_HASH ␣
↪      CERT-AU https://www.cert.gov.au/        T       -       -
893fb19ac24eabf9b1fe1ddd1111111111111111    Intel::FILE_HASH        CERT-AU https://
↪www.cert.gov.au/        T       -       -
11111111111111112977fa0588bd504a    Intel::FILE_HASH        CERT-AU https://www.cert.
↪gov.au/        T       -       -
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2309.
↪372 Safari/537.36      Intel::SOFTWARE CERT-AU https://www.cert.gov.au/        T   ␣
↪   -       -
183.82.180.95       Intel::ADDR     CCIRC   https://www.publicsafety.gc.ca/cnt/ntnl-
↪scrt/cbr-scrt/ccirc-ccric-eng.aspx      T       -       -
host.domain.tld/path/file   Intel::URL      CERT-AU https://www.cert.gov.au/        T␣
↪       -       -
```

5.4 Snort/Suricata output

Display IP observables in the format used by Snort IDS starting with a snort rule id of 5590000 (Note - each run of `stixtransclient.py` will need a different initial sid):

```
$ stixtransclient.py --file CA-TEST-STIX.xml --snort --snort-initial-sid 5590000

alert ip any any -> 188.115.196.39 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 188.115.196.39 (ID cert_au:Observable-
↪6a47b9da-ee08-413e-81ca-a3bb2ad46db4)", sid:5590000; rev:1; classtype:bad-unknown;)
alert ip any any -> 59.210.83.95 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 59.210.83.95 (ID cert_au:Observable-
↪0e1f6465-e9c2-4409-9e2b-29189bbd6ca0)", sid:5590001; rev:1; classtype:bad-unknown;)
alert ip any any -> 217.105.97.215 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 217.105.97.215 (ID cert_au:Observable-
↪f19853c3-4ce9-465f-9d5a-b194f85016ee)", sid:5590002; rev:1; classtype:bad-unknown;)
alert ip any any -> 147.93.7.4 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 147.93.7.4 (ID cert_au:Observable-
↪15404e6d-6c09-4c5c-8024-14b55d8dee66)", sid:5590003; rev:1; classtype:bad-unknown;)
alert ip any any -> 203.95.198.169 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 203.95.198.169 (ID cert_au:Observable-
↪f5832d9a-894c-4667-a1c7-2b37f5048740)", sid:5590004; rev:1; classtype:bad-unknown;)
alert ip any any -> 110.244.163.122 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 110.244.163.122 (ID cert_au:Observable-
↪f7b8c56b-1a69-4d02-99ee-30e9bdd59452)", sid:5590005; rev:1; classtype:bad-unknown;)
alert ip any any -> 248.206.70.230 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 248.206.70.230 (ID cert_au:Observable-
↪5ad9e361-f32f-4174-b854-27bb73d77645)", sid:5590006; rev:1; classtype:bad-unknown;)
alert ip any any -> 99.253.98.57 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 99.253.98.57 (ID cert_au:Observable-
↪1526c98f-950e-46da-931a-3749524c519f)", sid:5590007; rev:1; classtype:bad-unknown;)
alert ip any any -> 3.46.87.116 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 3.46.87.116 (ID cert_au:Observable-
↪62fb38b3-fc53-48cb-ad7d-6a9762ee87c4)", sid:5590008; rev:1; classtype:bad-unknown;)
alert ip any any -> 28.13.163.200 any (flow:established,to_server; msg:"CTI-TOOLKIT␣
↪Connection to potentially malicious server 28.13.163.200 (ID cert_au:Observable-
↪091354ba-6db5-42a6-8db0-1041b148ba28)", sid:5590009; rev:1; classtype:bad-unknown;)
```

CHAPTER 6

API reference

Contents:

6.1 `certau.source` Module

6.2 `certau.transform` Module

CHAPTER 7

Indices and tables

- genindex
- modindex
- search