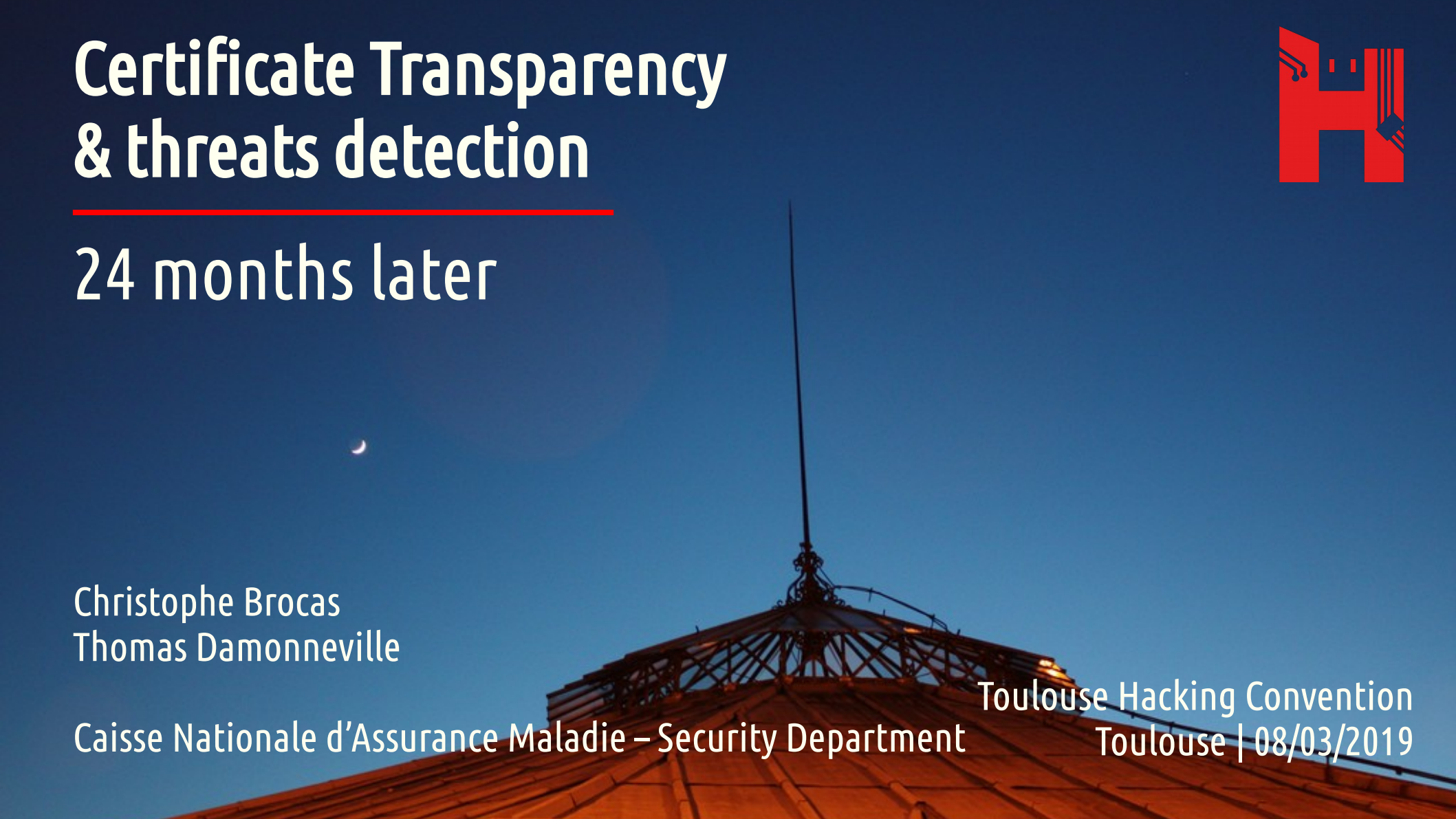
Certificate Transparency & threats detection

24 months later



Christophe Brocas
Thomas Damonneville

Caisse Nationale d'Assurance Maladie – Security Department

Toulouse Hacking Convention
Toulouse | 08/03/2019

Agenda

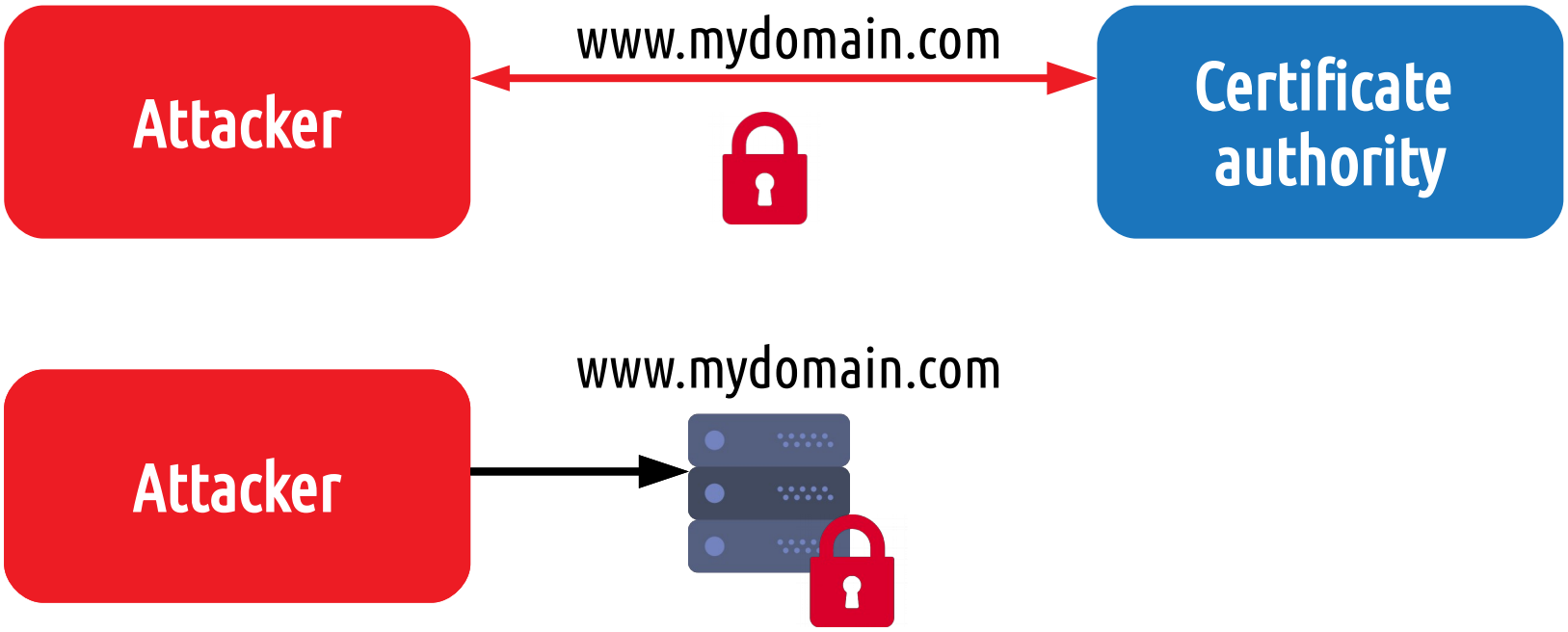
1) Certificate Transparency
    - Risk / Answer
    - How Certificate Transparency works

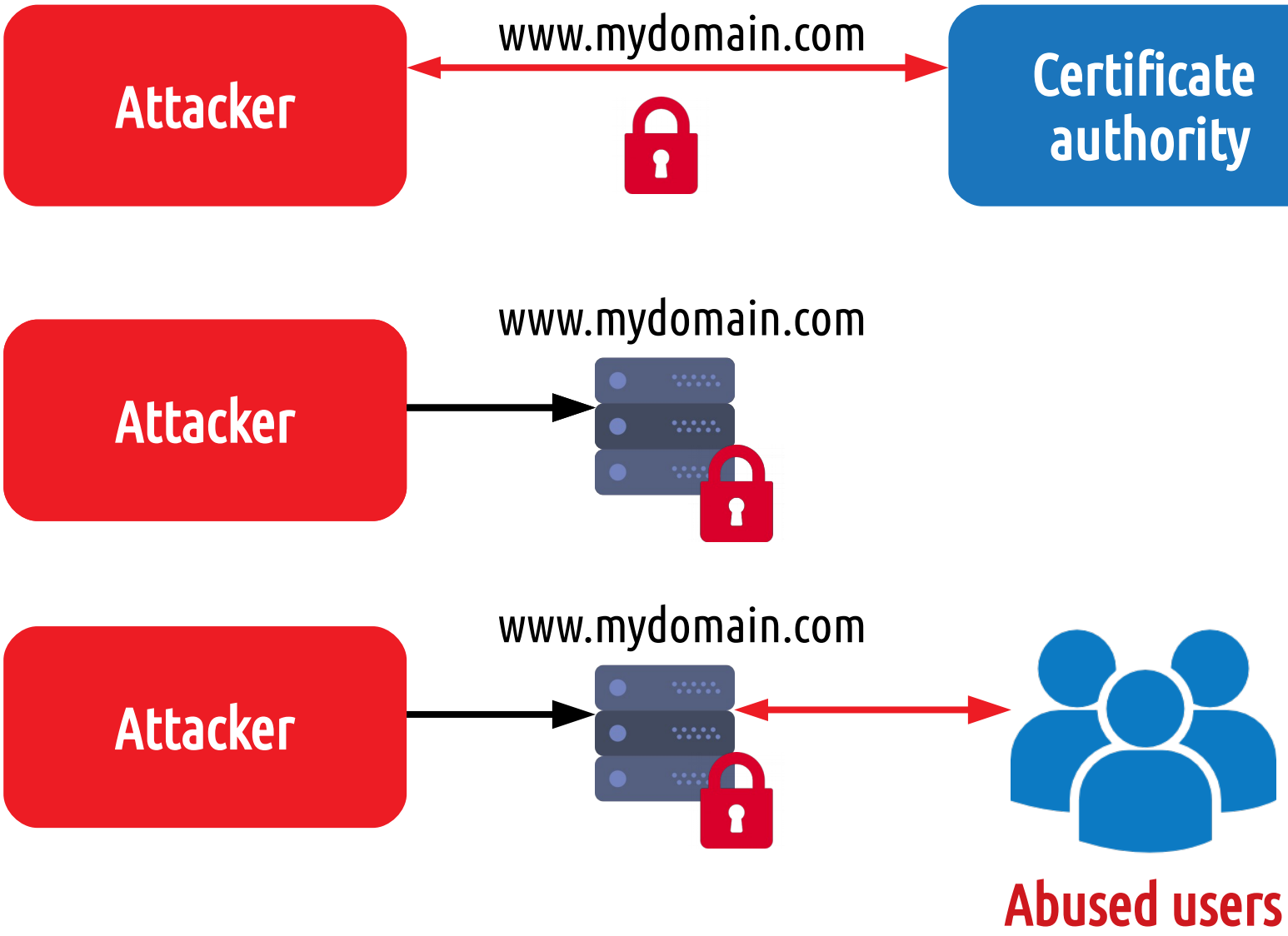
2) Benefits for threats monitoring
    - Usages for blue teams
    - CertStreamMonitor

3) CT & threats monitoring: a 24 months story


Risk & Answer


Attacker
www.mydomain.com
Certificate authority


Attacker
www.mydomain.com
Certificate authority
Attacker
www.mydomain.com

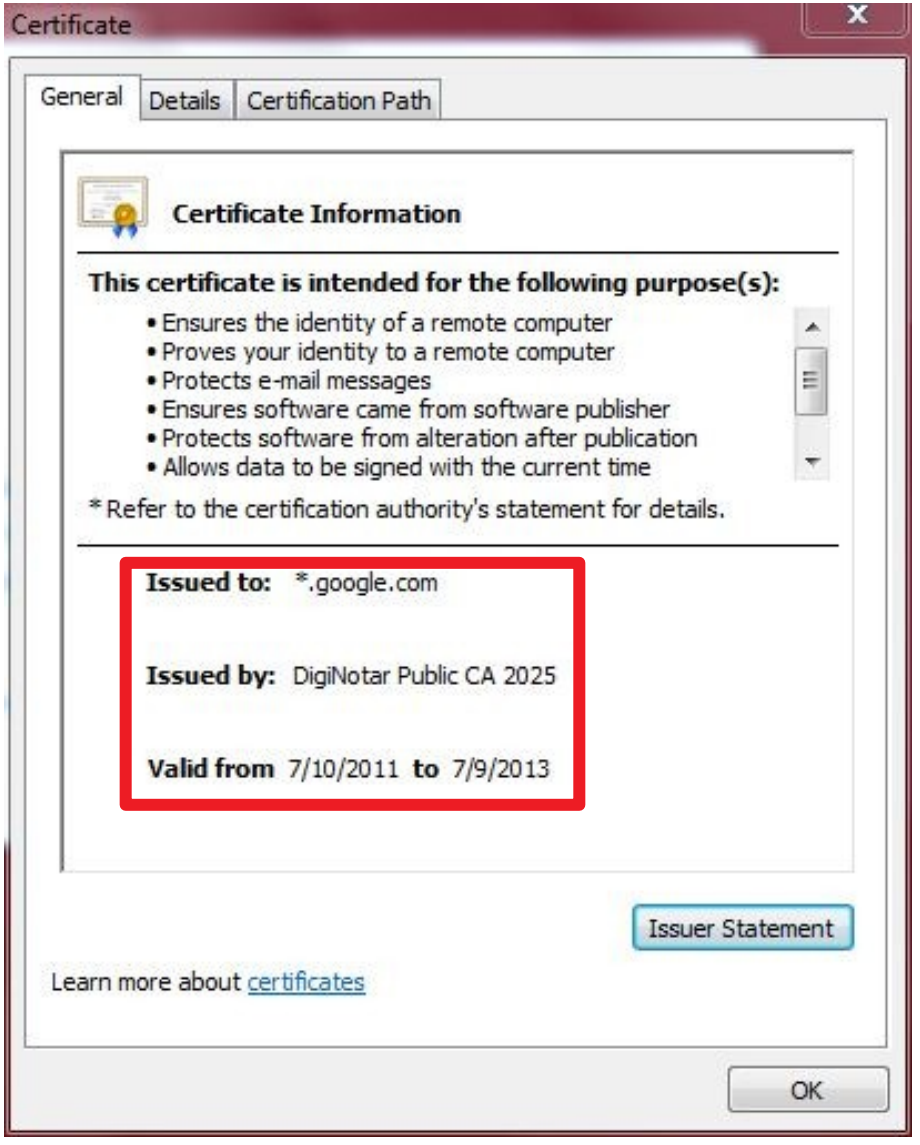

Attacker
www.mydomain.com
Certificate authority
Attacker
www.mydomain.com
Attacker
www.mydomain.com
Abused users

And « www.mydomain.com » owner?

And « www.mydomain.com » owner?

And « www.mydomain.com » owner?

Example


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• Protects e-mail messages
• Ensures software came from software publisher
• Protects software from alteration after publication
• Allows data to be signed with the current time
* Refer to the certification authority's statement for details.
Issued to: *.google.com
Issued by: DigiNotar Public CA 2025
Valid from 7/10/2011 to 7/9/2013
Issuer Statement
Learn more about certificates
OK

Certificate Transparency

Public CA have to submit all certificates they signed to publicly auditable and accessible, append-only, cryptographically signed logs.

Certificate Transparency

Public CA have to submit all certificates they signed to publicly auditable and accessible, append-only, cryptographically signed logs.

Timeline :

→ 2013 : Google (RFC 6962) then IETF (RFC 6962bis)
→ 2015 : CT mandatory for EV certificates
→ 30/04/2018 : CT for all certificates
→ 24/07/2018 : interstitial blocking page Chrome 68
→ 15/10/2018 : CT mandatory for Apple products

Votre connexion n'est pas privée

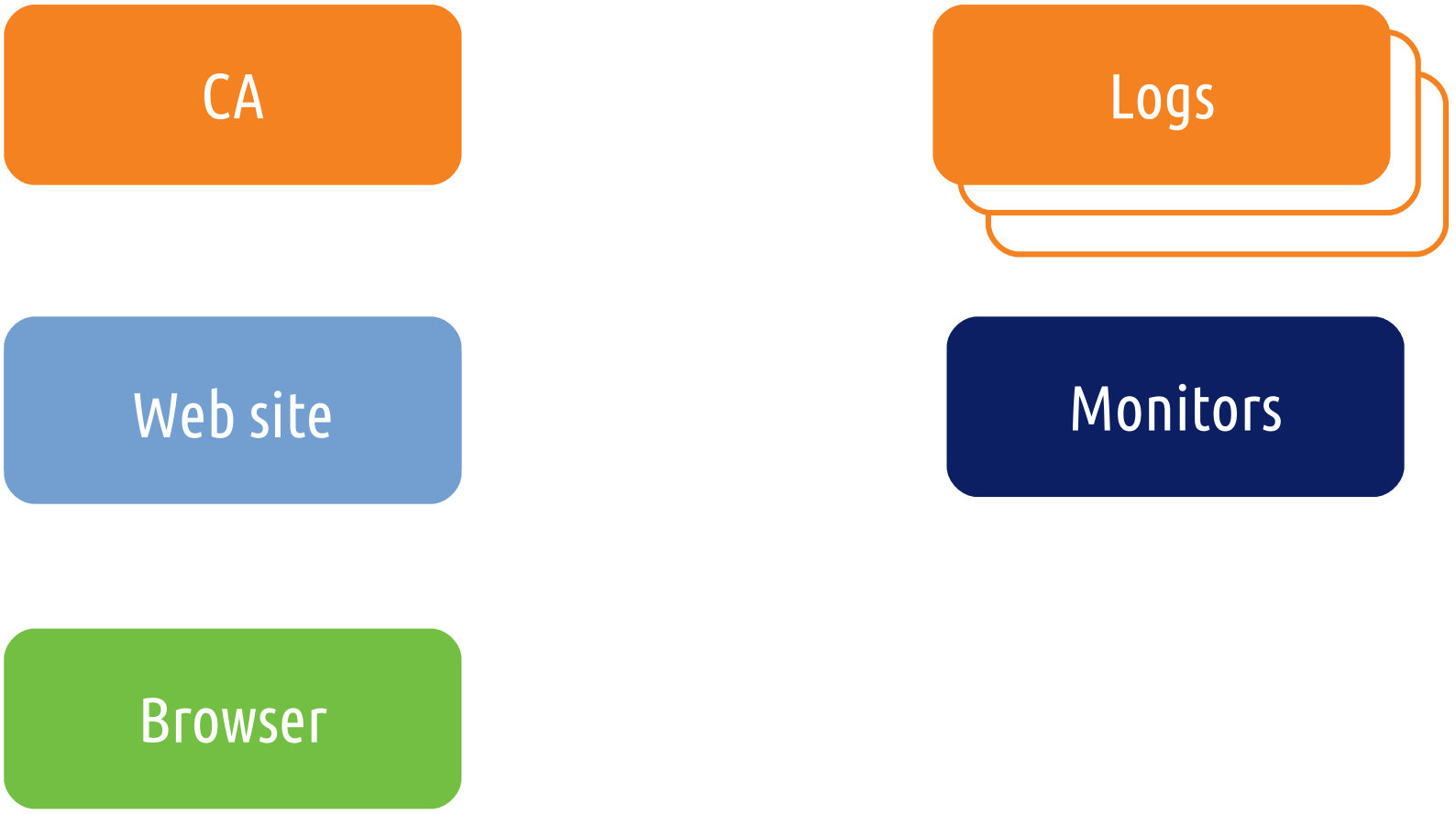
Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site **example.com** (mots de passe, messages ou numéros de carte de crédit, par exemple). En savoir plus

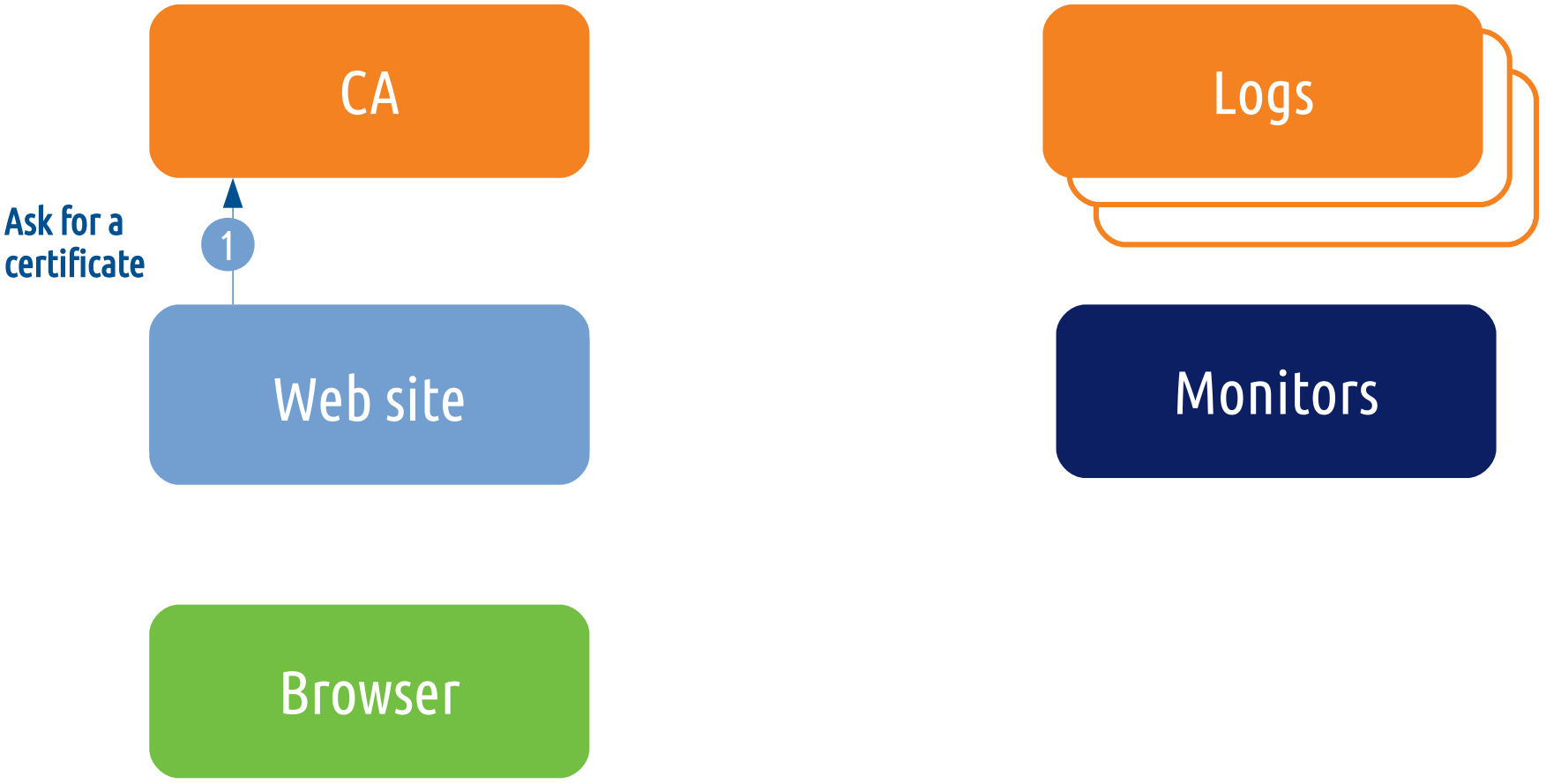
NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

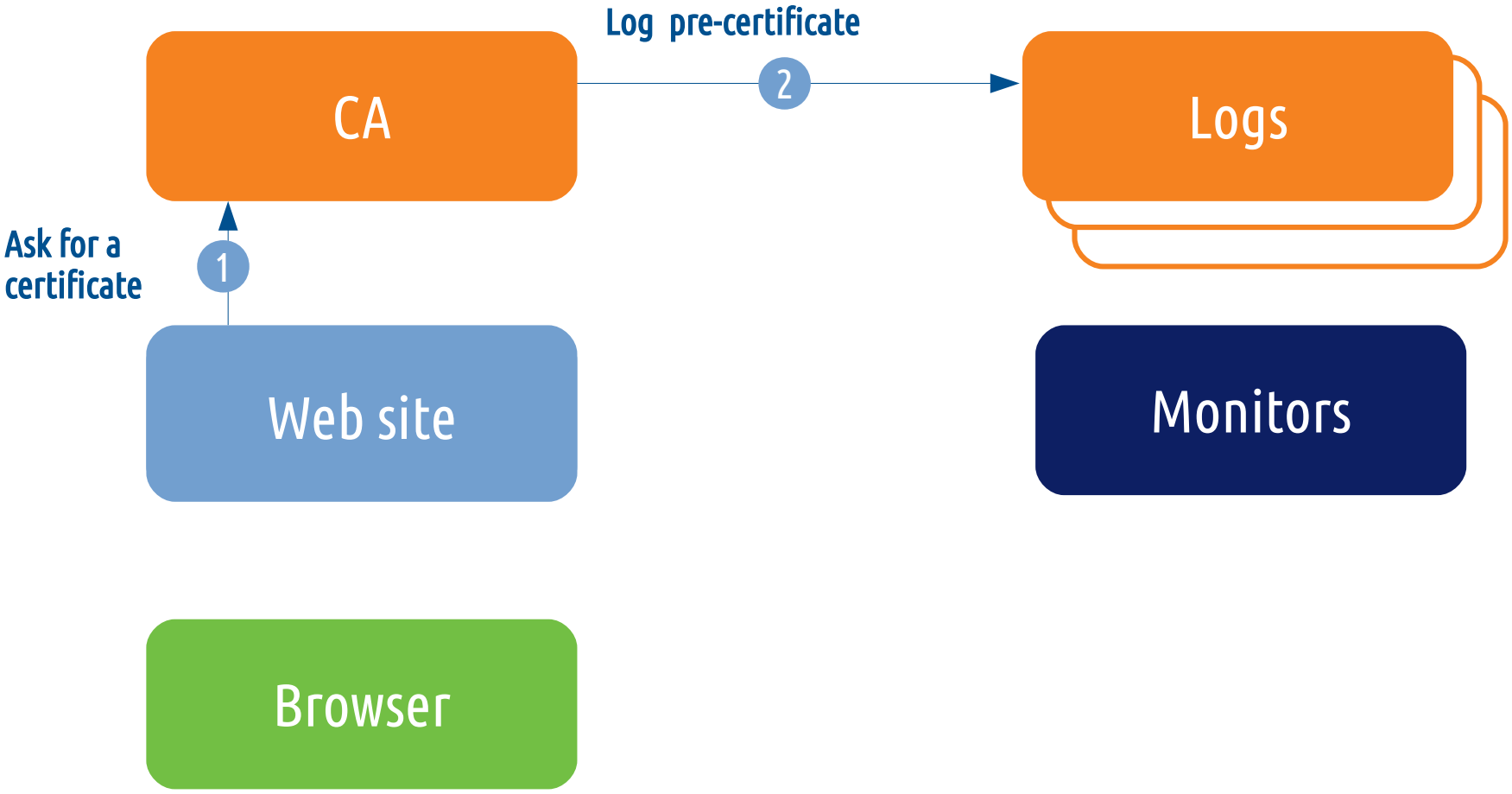
PARAMÈTRES AVANCÉS

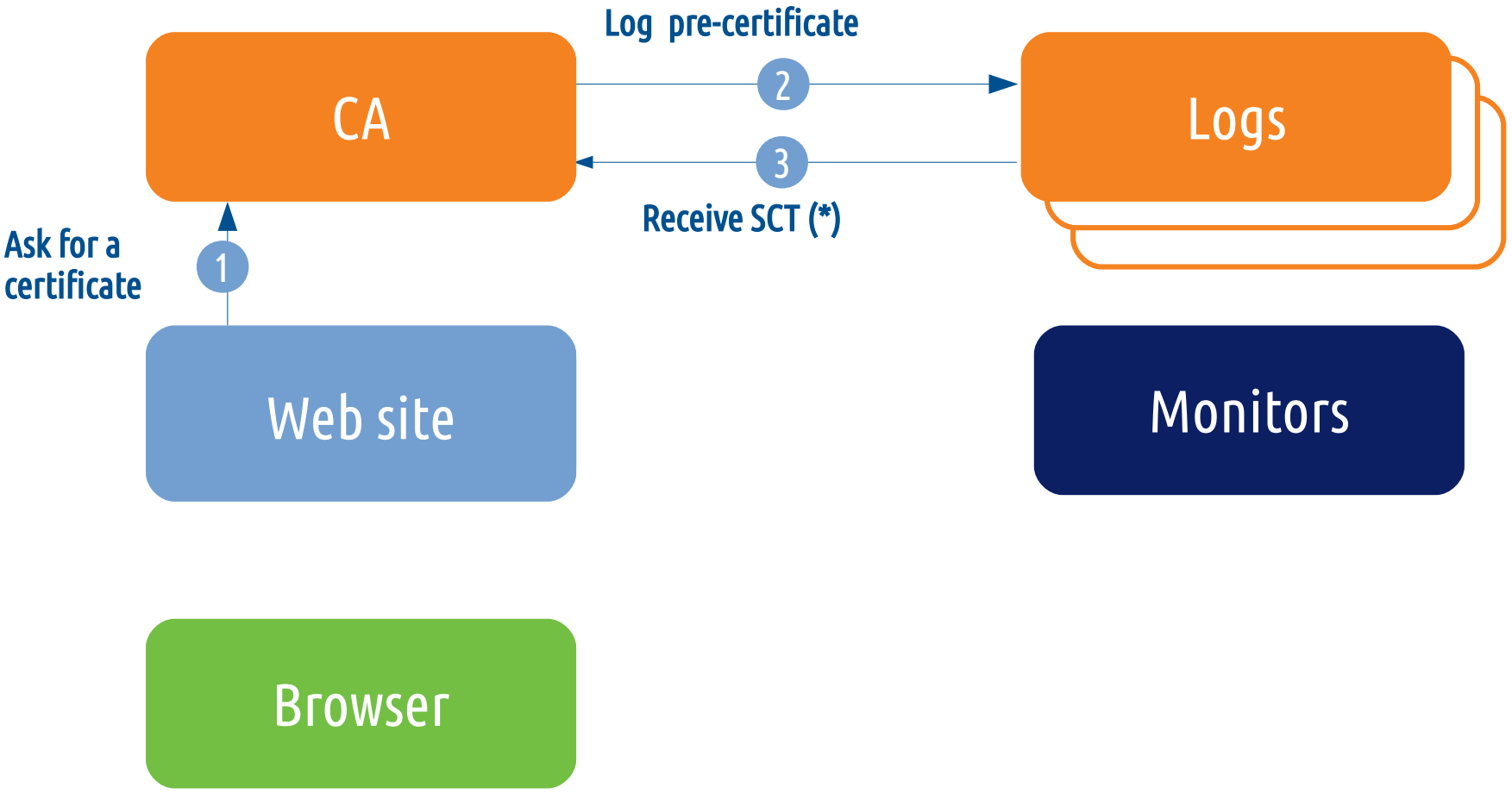
Retour à la sécurité

How CT works

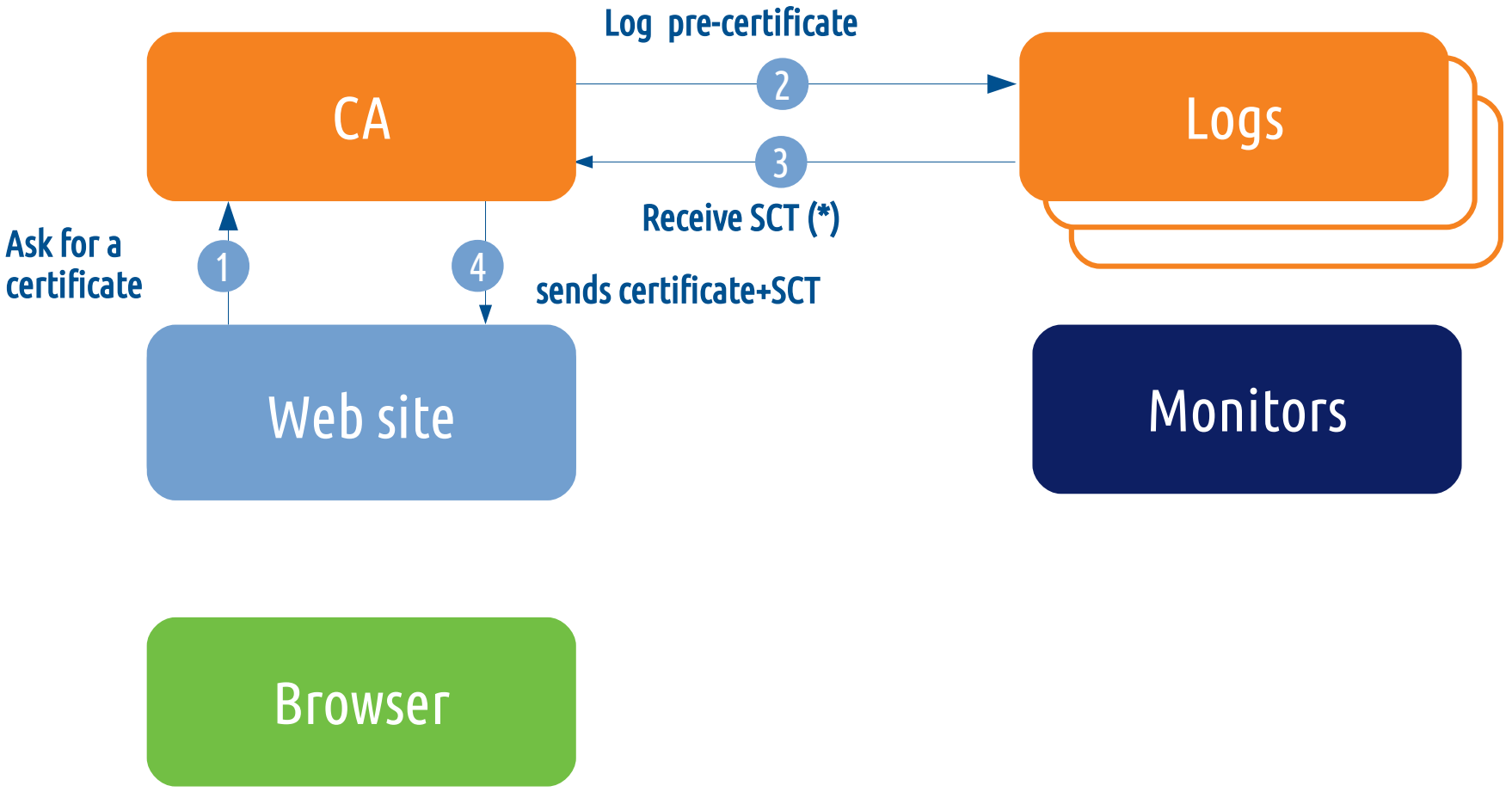

CA
Logs
Web site
Monitors
Browser


CA
Logs
Ask for a certificate
1
Web site
Monitors
Browser

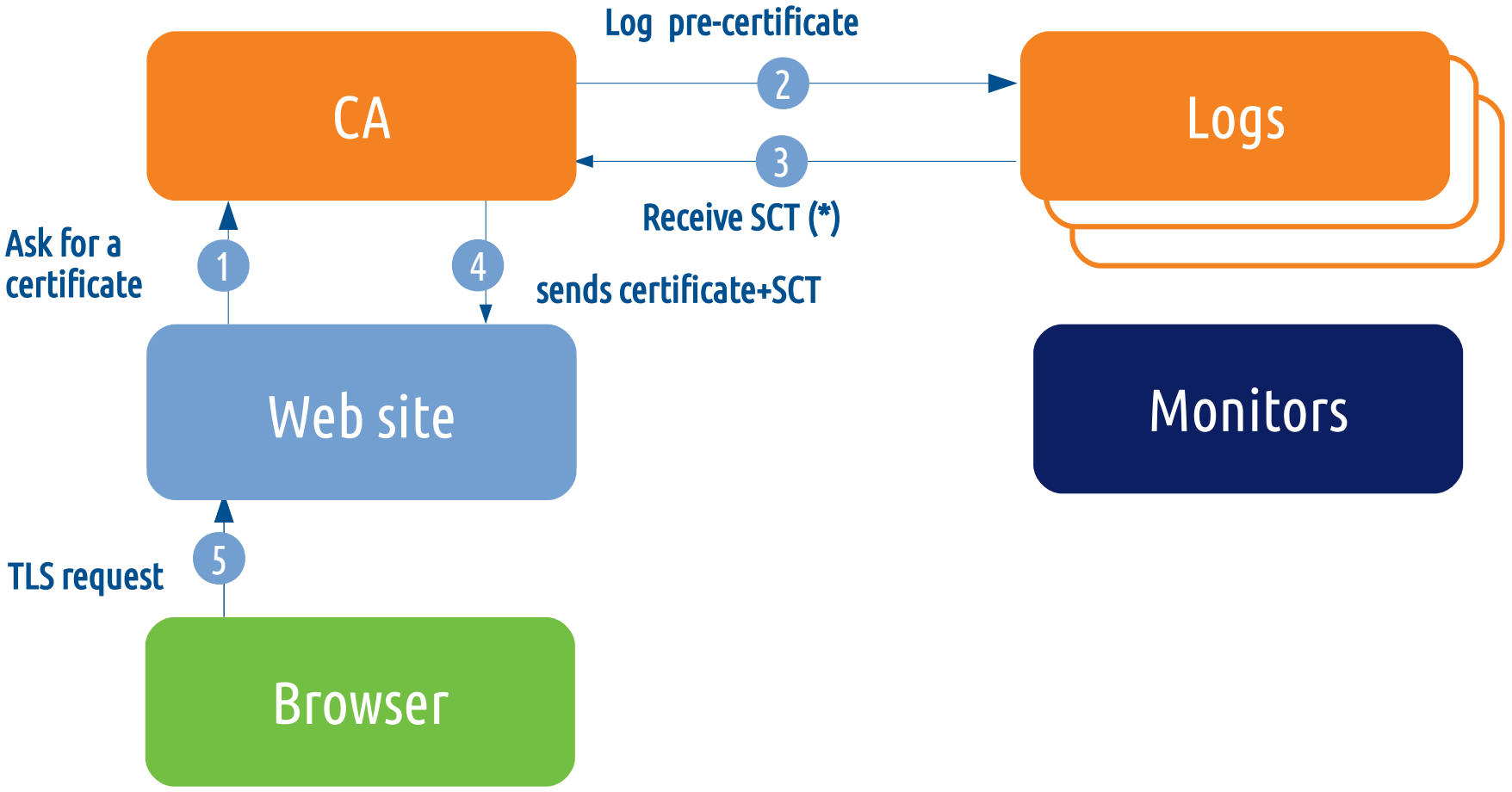

Log pre-certificate
2
CA
Logs
Ask for a certificate
1
Web site
Monitors
Browser



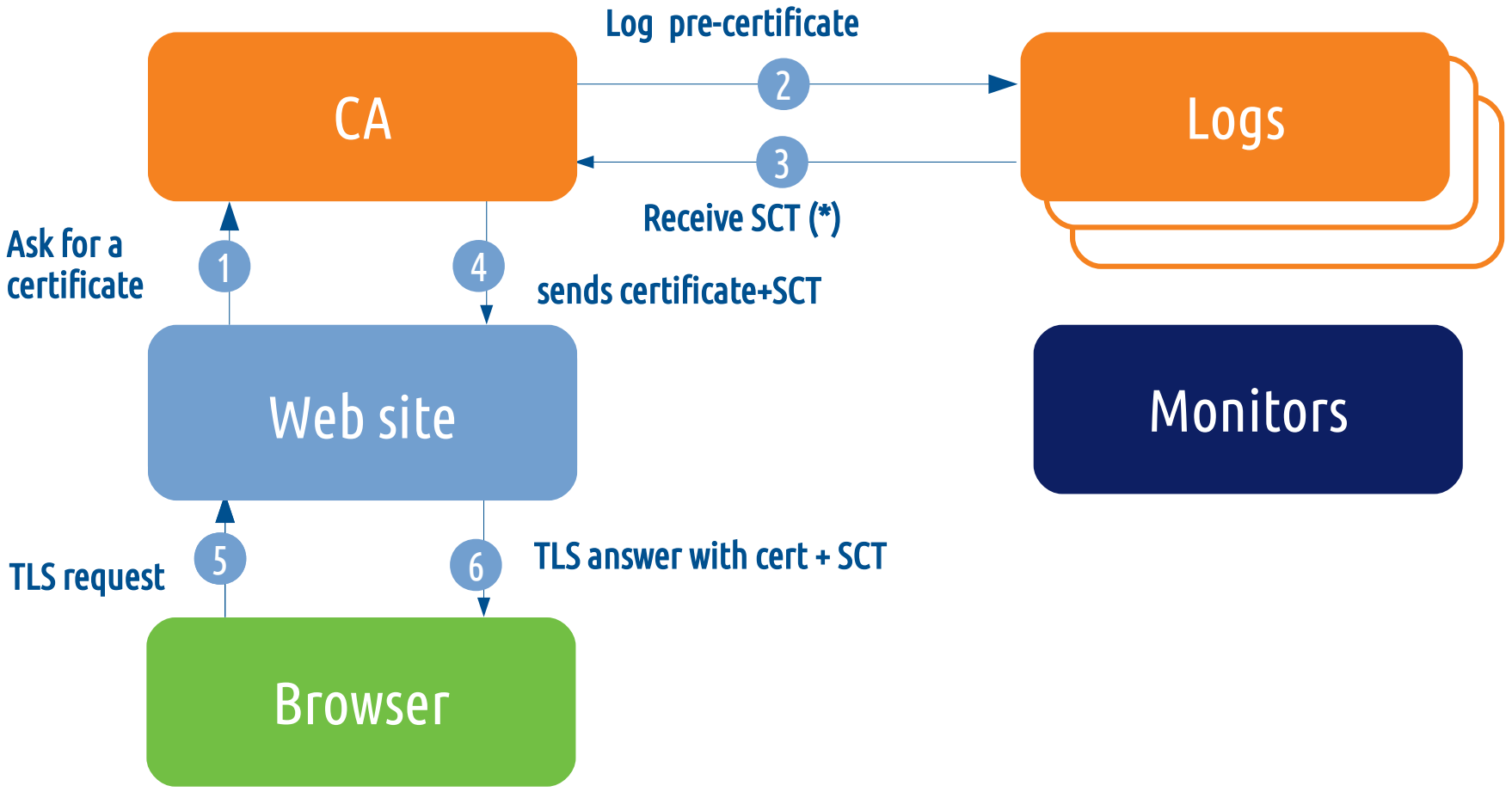
(*) Signed Certificate Timestamp



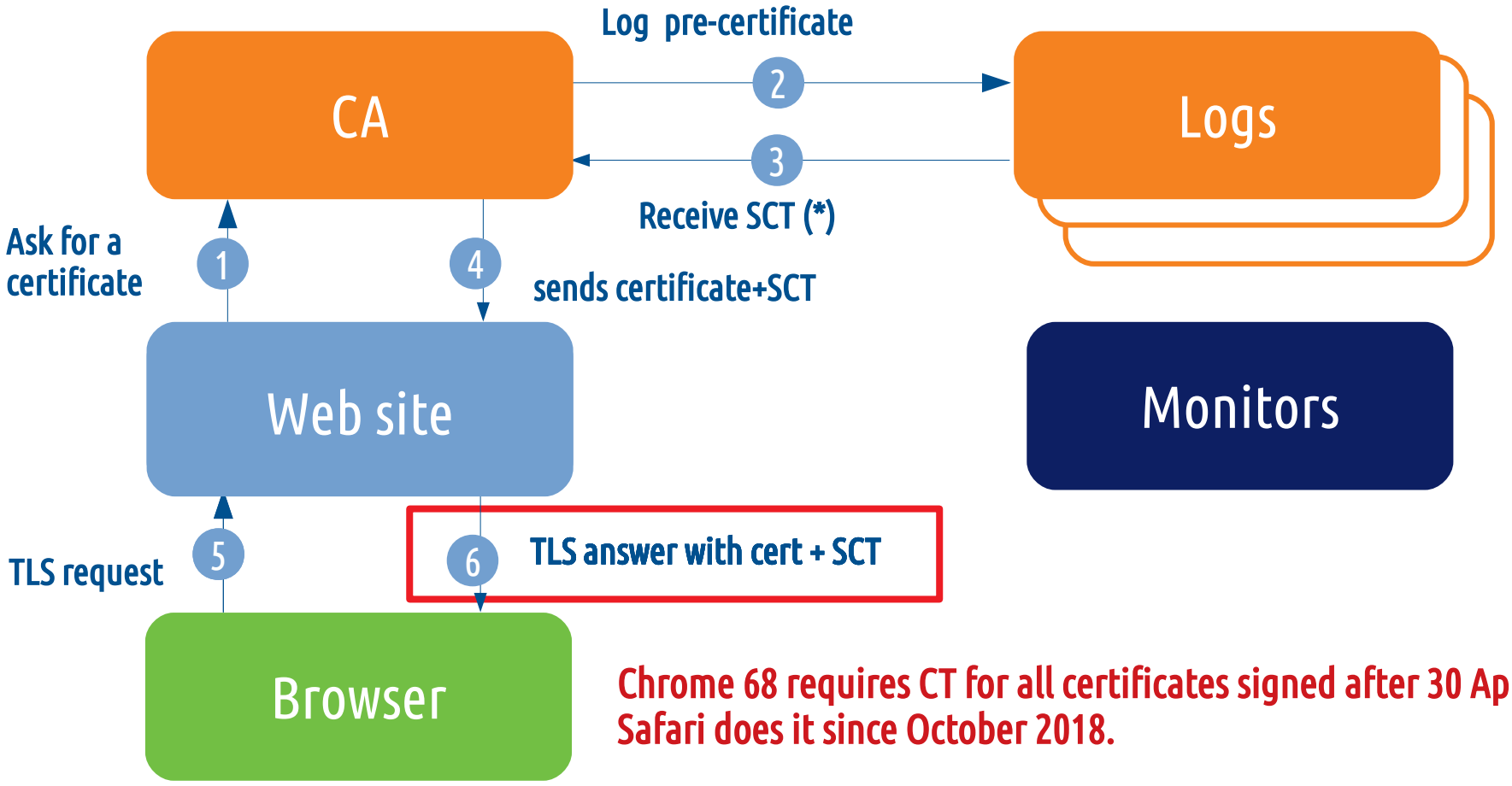
(*) Signed Certificate Timestamp



(*) Signed Certificate Timestamp

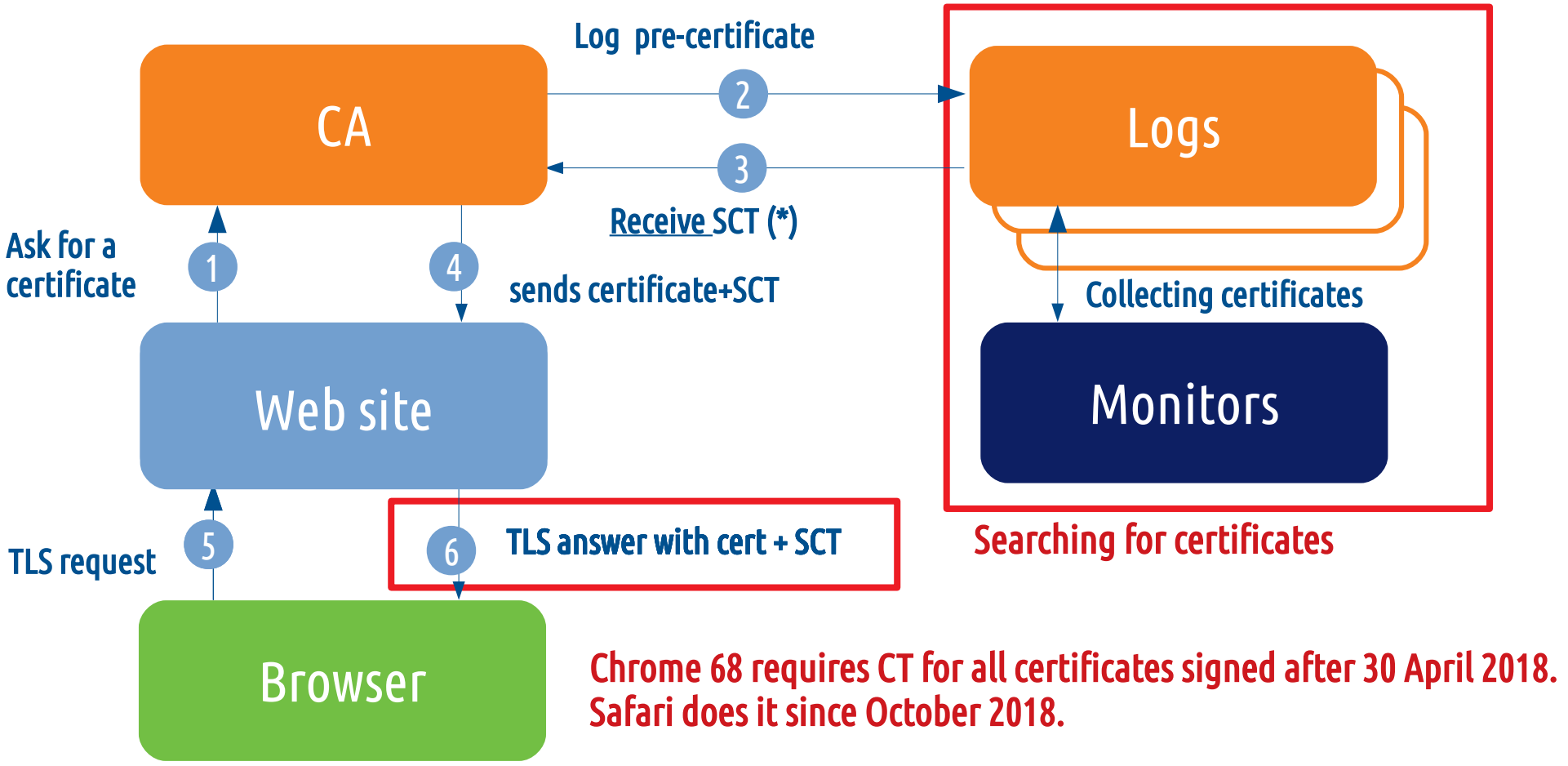


(*) Signed Certificate Timestamp



Chrome 68 requires CT for all certificates signed after 30 April 2018.
Safari does it since October 2018.

(*) Signed Certificate Timestamp



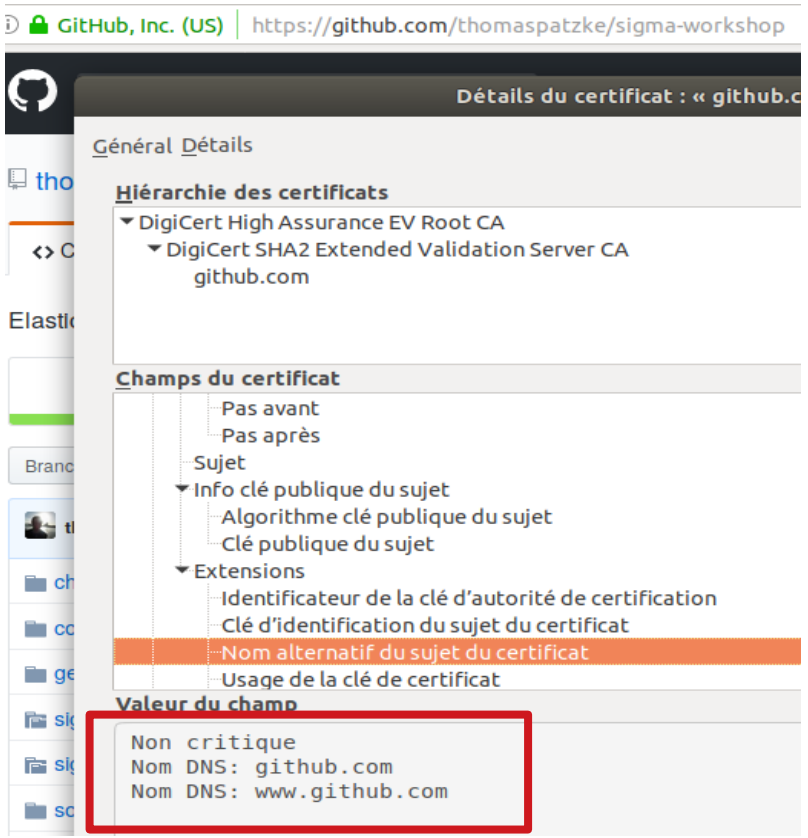
Chrome 68 requires CT for all certificates signed after 30 April 2018.
Safari does it since October 2018.

(*) Signed Certificate Timestamp

GAIN

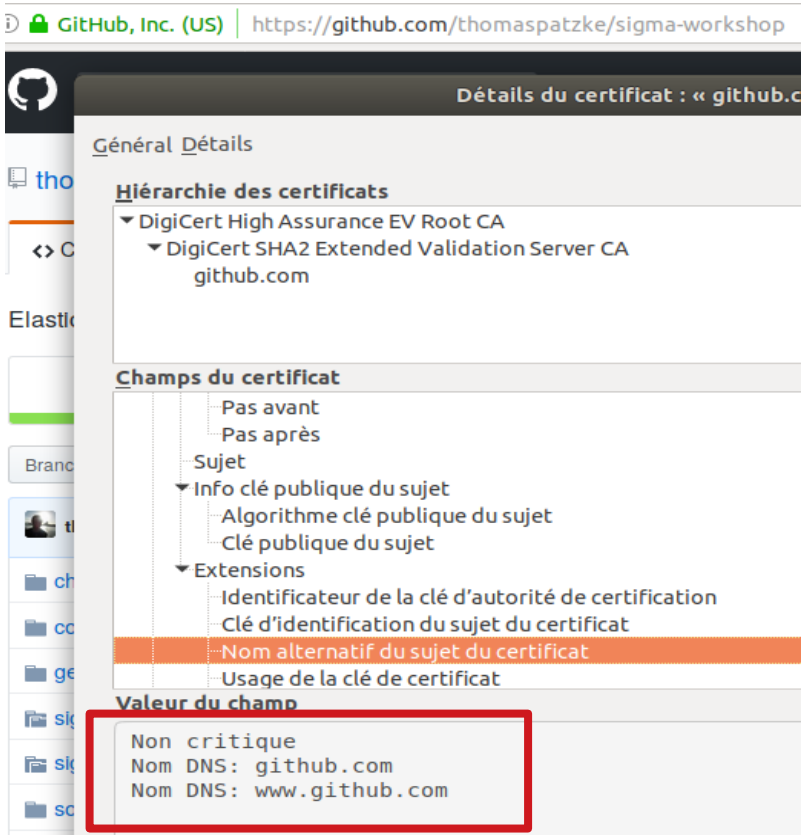
… for Blue Teams

CT : benefits for Blue Teams

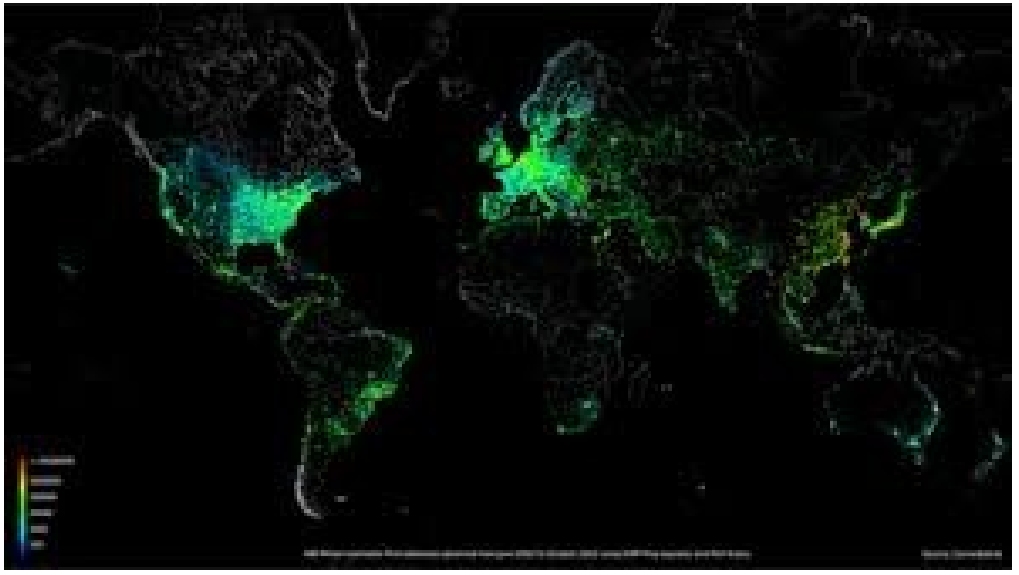


FQDN (!= DNS)

CT : benefits for Blue Teams



FQDN (!= DNS)



Internet wide logging

+

Open access to the data

CT: 2 useful usages (for us)

#1 Find certificates for our domains

→ hacked / malicious CA
→ hacked DNS server (*)
→ legit web site but not using corporate security best practices (hosting, certificate, DNS etc)

* : https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

CT: 2 useful usages (for us)

#2 Find certificates for « near » domains

→ phishing campaigns
→ image damage

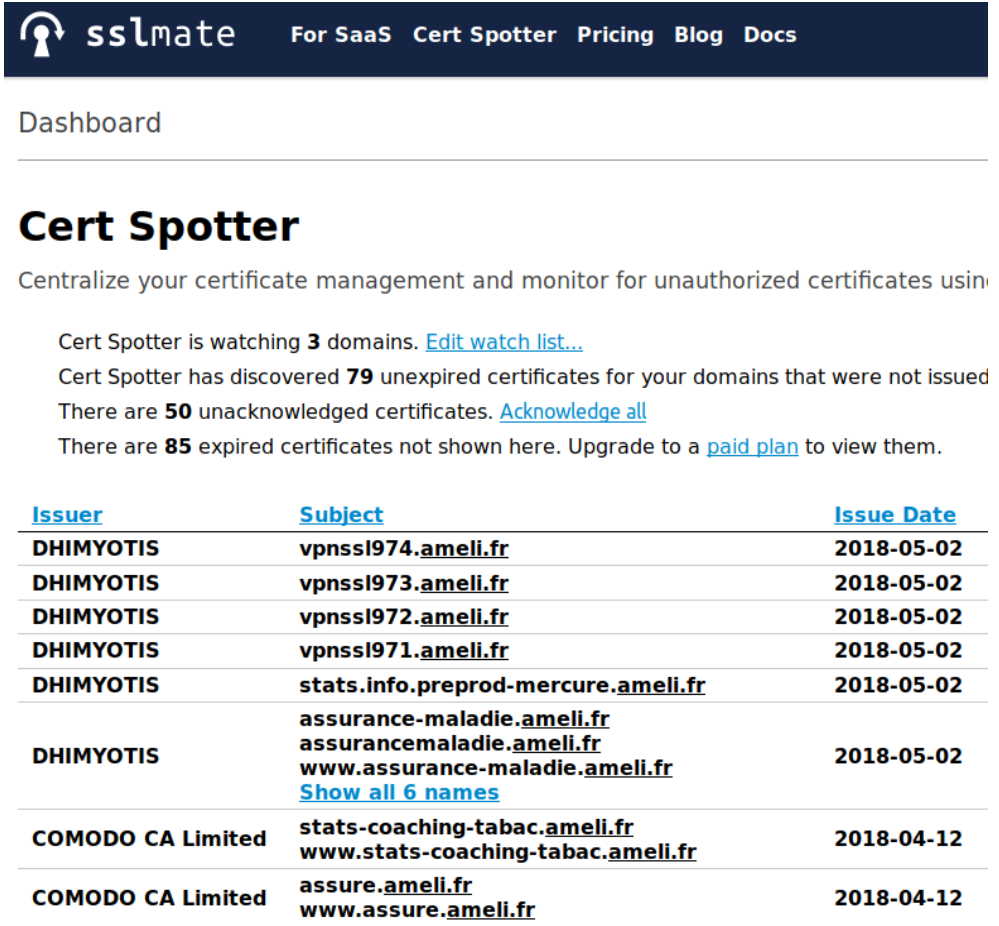
Usage #1: our domains monitoring

Current choice:

→ hosted service

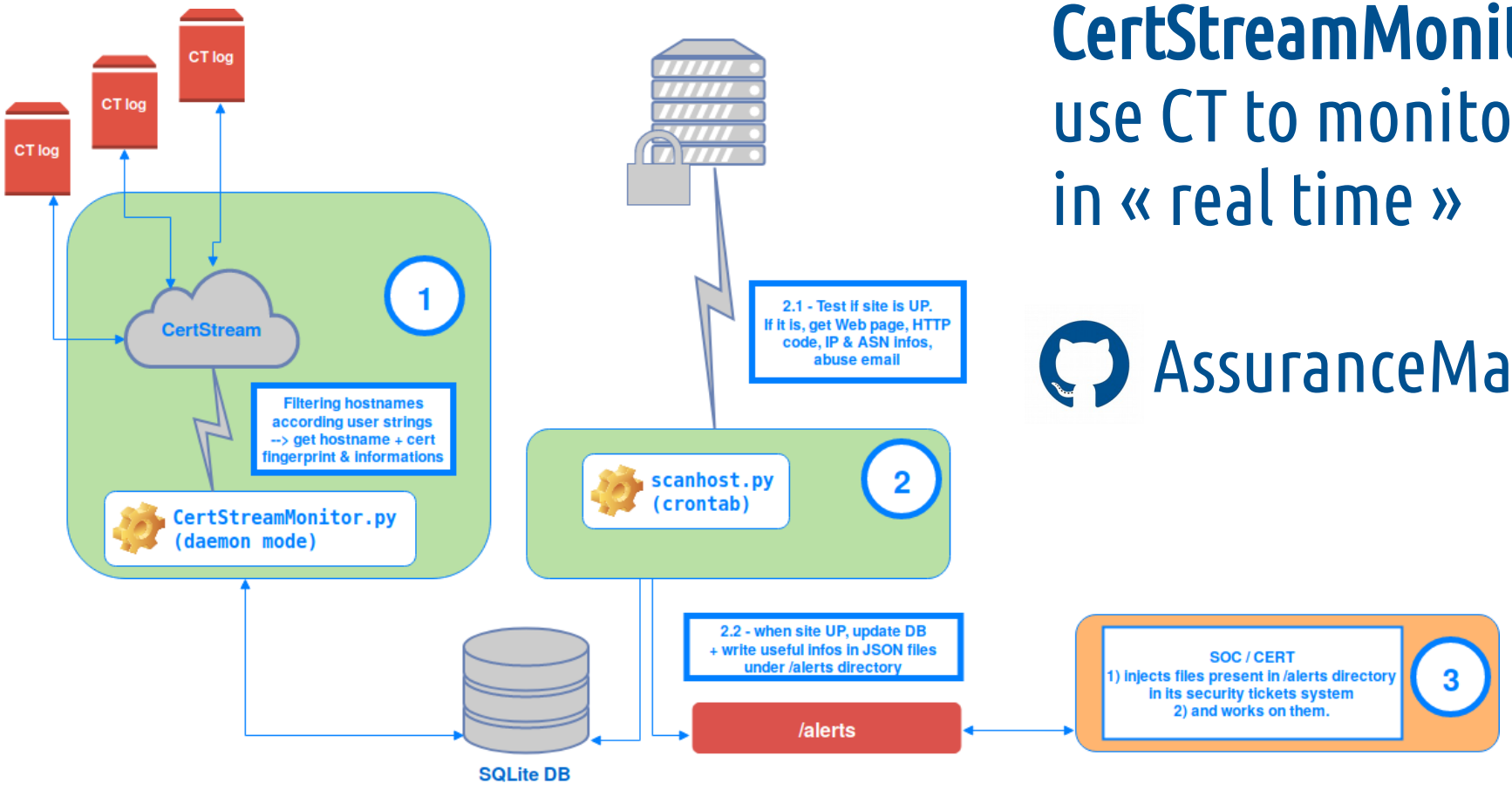
→ daily notification

→ managed by our team dealing with certificates (efficiency)



Code: CertStreamMonitor

Usage #2: « near » domains monitoring



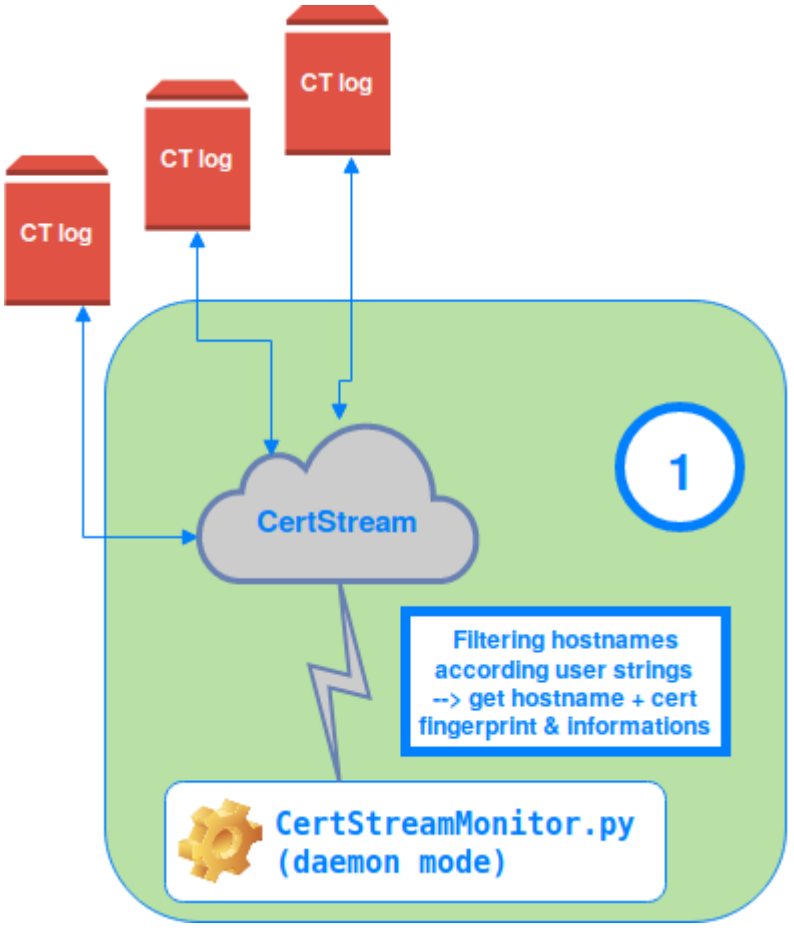
CertStreamMonitor :
use CT to monitor threats in « real time »

AssuranceMaladieSec

CertStreamMonitor

CertStreamMonitor.py

. works on multi CT logs flow
. keywords detection with threshold
. real time
. runs in daemon mode



CertStreamMonitor.py: how it works

Tailor your configuration file (conf/filename.conf)

→ Choose your keywords : ex: apple|account|login

→ Set your threshold: ex: 2 (defaut value)

CertStreamMonitor.py: how it works

Tailor your configuration file (conf/filename.conf)
→ Choose your keywords : ex: apple|account|login
→ Set your threshold: ex: 2 (defaut value)

hostnames with a number of keywords ≥ threshold
→ insert in DB (ex : login.apple-connect.com)

CertStreamMonitor.py: how it works

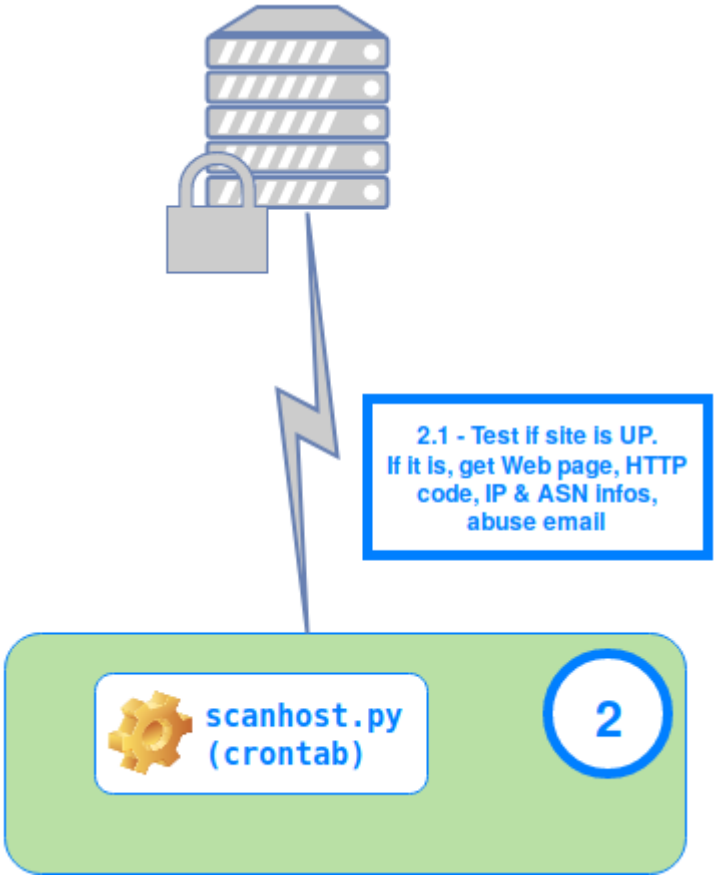
Tailor your configuration file (conf/filename.conf)
→ Choose your keywords : ex: apple|account|login
→ Set your threshold: ex: 2 (defaut value)

hostnames with a number of keywords ≥ threshold
→ insert in DB (ex : login.apple-connect.com)

hostnames with a number of keywords < threshold but >0
→ write to log file (ex : webmail.apple-mail.com)

scanhost.py: how it works

→ run on demand (ex. : 1/day)
→ test all hostnames not already logged as up
→ if hostname is up:
    * update DB
    * JSON report file
      (ip, AS, abuse email...)



scanhost.py: how it works

JSON report file


```
{
    "hostname": "assure.ameli.fr.eskandiromagic.info",
    "http_code": 200,
    "cert_serial_number": "53:F6:23:A0:16:11:5D:47:39:1D:C1:07:54:0C:4F:01:02:D8:C3:DD",
    "webpage_title": "Compte ameli - mon espace personnel - Connexion &agrave; mon compte",
    "ip_addr": "162.213.123.155",
    "asn": "40244",
    "asn_cidr": "162.213.120.0/22",
    "asn_country_code": "US",
    "asn_description": "TURNKEY-INTERNET - Turnkey Internet Inc., US",
    "asn_abuse_email": "abuse@turnkeyinternet.net"
}
```

Screenshots are not a demo <shame/>

```
cb@D375:~/tools/CertStreamMonitor$ python3 CertStreamMonitor.py -c conf/example.conf
Looking for these strings: paypal|apple|account|secure|login, detection threshold: 2
Connection established to CertStream! Listening for events...
[2018-11-28T17:26:03] mail.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certifi
:1C:85:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:26:03] secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certificatio
5:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:26:03] www.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certifio
1C:85:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:28:07] bbt-login-my-account.com (SAN: ) (Issuer: /C=GB/CN=COMODO ECC Domain Validation
gerprint: 85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC) (StartTime: 2018-11-28T00:00:0
[2018-11-28T17:28:08] *.bbt-login-my-account.com (SAN: ) (Issuer: /C=GB/CN=COMODO ECC Domain Validati
ingerprint: 85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC) (StartTime: 2018-11-28T00:00
[2018-11-28T17:28:13] paypai.com.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=Let's Encrypt
C3:A2:3C:C0:A3:D5:89:04:AA) (StartTime: 2018-11-28T15:23:11)
[2018-11-28T17:28:13] www.paypai.com.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=Let's Encr
:B8:C3:A2:3C:C0:A3:D5:89:04:AA) (StartTime: 2018-11-28T15:23:11)
Error connecting to CertStream - Connection is already closed. - Sleeping for a few seconds and tryin
Connection established to CertStream! Listening for events...
Error connecting to CertStream - Connection is already closed. - Sleeping for a few seconds and tryin
Connection established to CertStream! Listening for events...
[2018-11-28T17:42:38] appleid.apple.com.secure-informations.dynv6.net (SAN: ) (Issuer: /C=US/CN=Let's
92:44:82:95:49:21:DD:C9:47:58:1A:F4) (StartTime: 2018-11-28T12:32:52)
```

```
cb@D375:~/tools/CertStreamMonitor$ python3 CertStreamMonitor.py -c conf/example.conf
Looking for these strings: paypal|apple|account|secure|login, detection threshold: 2
Connection established to CertStream! Listening for events...
[2018-11-28T17:26:03] mail.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certif
:1C:85:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:26:03] secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certificatio
5:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:26:03] www.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certifi
1C:85:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:28:07] bbt-login-my-account.com (SAN: ) (Issuer: /C=GB/CN=COMODO ECC Domain Validation
gerprint: 85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC) (StartTime: 2018-11-28T00:00:0
[2018-11-28T17:28:08] *.bbt-login-my-account.com (SAN: ) (Issuer: /C=GB/CN=COMODO ECC Domain Validati
ingerprint: 85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC) (StartTime: 2018-11-28T00:0
[2018-11-28T17:28:13] paypai.com.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=Let's Encrypt
C3:A2:3C:C0:A3:D5:89:04:AA) (StartTime: 2018-11-28T15:23:11)
[2018-11-28T17:28:13] www.paypai.com.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=Let's Encr
:B8:C3:A2:3C:C0:A3:D5:89:04:AA) (StartTime: 2018-11-28T15:23:11)
Error connecting to CertStream - Connection is already closed. - Sleeping for a few seconds and tryin
Connection established to CertStream! Listening for events...
Error connecting to CertStream - Connection is already closed. - Sleeping for a few seconds and tryin
Connection established to CertStream! Listening for events...
[2018-11-28T17:42:38] appleid.apple.com.secure-informations.dynv6.net (SAN: ) (Issuer: /C=US/CN=Let's
92:44:82:95:49:21:DD:C9:47:58:1A:F4) (StartTime: 2018-11-28T12:32:52)
```

```
cb@D375:~/tools/CertStreamMonitor$ python3 CertStreamMonitor.py -c conf/example.conf
Looking for these strings: paypal|apple|account|secure|login, detection threshold: 2
Connection established to CertStream! Listening for events...
[2018-11-28T17:26:03] mail.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certifi
:1C:85:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:26:03] secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certificatio
5:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:26:03] www.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=cPanel, Inc. Certifi
1C:85:D9:99:7F:58:D3:50:F3:26:5F:4C:62:A0:0D) (StartTime: 2018-11-28T00:00:00)
[2018-11-28T17:28:07] bbt-login-my-account.com (SAN: ) (Issuer: /C=GB/CN=COMODO ECC Domain Validation
gerprint: 85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC) (StartTime: 2018-11-28T00:00:0
[2018-11-28T17:28:08] *.bbt-login-my-account.com (SAN: ) (Issuer: /C=GB/CN=COMODO ECC Domain Validati
ingerprint: 85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC) (StartTime: 2018-11-28T00:0
[2018-11-28T17:28:13] paypai.com.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=Let's Encrypt
C3:A2:3C:C0:A3:D5:89:04:AA) (StartTime: 2018-11-28T15:23:11)
[2018-11-28T17:28:13] www.paypai.com.secure-verifiedaccounts.com (SAN: ) (Issuer: /C=US/CN=Let's Encr
:B8:C3:A2:3C:C0:A3:D5:89:04:AA) (StartTime: 2018-11-28T15:23:11)
Error connecting to CertStream - Connection is already closed. - Sleeping for a few seconds and tryin
Connection established to CertStream! Listening for events...
Error connecting to CertStream - Connection is already closed. - Sleeping for a few seconds and tryin
Connection established to CertStream! Listening for events...
[2018-11-28T17:42:38] appleid.apple.com.secure-informations.dynv6.net (SAN: ) (Issuer: /C=US/CN=Let's
92:44:82:95:49:21:DD:C9:47:58:1A:F4) (StartTime: 2018-11-28T12:32:52)
```

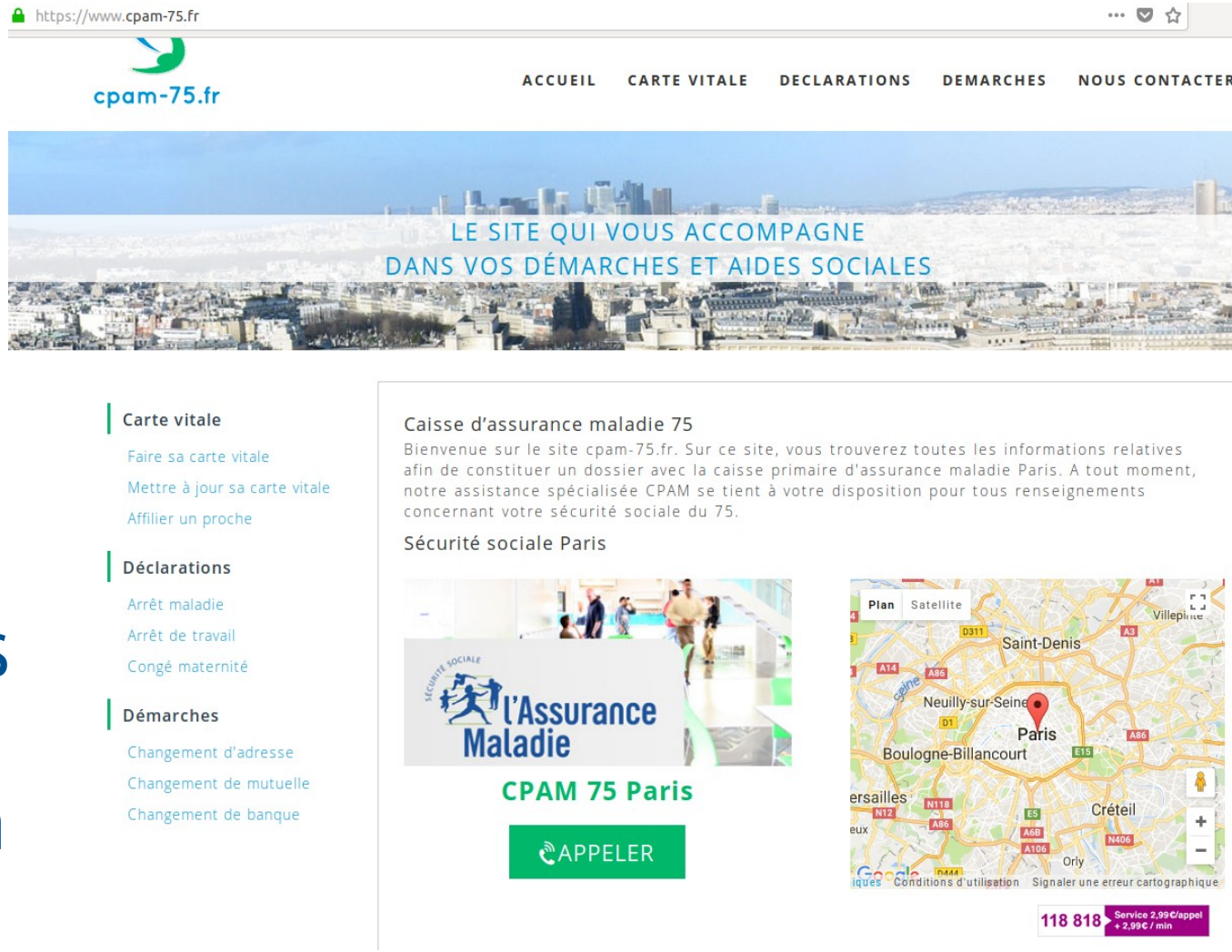
```
cb@D375:~/tools/CertStreamMonitor$ python3 ./scanhost.py -c conf/example.conf
Test all domains in DB for Internet Presence:
*****************************************
17:53:25 - ERROR -   https://mail.secure-verifiedaccounts.com - SSL error
17:53:25 - ERROR -   https://secure-verifiedaccounts.com - SSL error
17:53:25 - ERROR -   https://www.secure-verifiedaccounts.com - SSL error
17:53:27 - SUCCESS - HTTP 200 - bbt-login-my-account.com
Creating ./alerts/2018/11/28/bbt-login-my-account.com.json : {'hostname': 'bbt-login-my-account.com', 'we
': '104.31.64.0/20', 'asn_description': 'CLOUDFLARENET - Cloudflare, Inc., US', 'asn_abuse_email': 'abuse
: 200, 'cert_serial_number': '85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC'}
17:53:28 - WARNING - wildcard certificate: no request for *.bbt-login-my-account.com
17:53:29 - ERROR -   https://paypai.com.secure-verifiedaccounts.com - SSL error
17:53:29 - ERROR -   https://www.paypai.com.secure-verifiedaccounts.com - SSL error
17:53:30 - SUCCESS - HTTP 404 - appleid.apple.com.secure-informations.dynv6.net
Creating ./alerts/2018/11/28/appleid.apple.com.secure-informations.dynv6.net.json : {'hostname': 'appleid
try_code': 'US', 'asn_cidr': '68.183.96.0/20', 'asn_description': 'DIGITALOCEAN-ASN - DigitalOcean, LLC,
r': '68.183.96.151', 'http_code': 404, 'cert_serial_number': 'AF:76:7D:60:34:08:C1:0F:92:44:82:95:49:21:D
```

```
cb@D375:~/tools/CertStreamMonitor$ python3 ./scanhost.py -c conf/example.conf
Test all domains in DB for Internet Presence:
*****************************************
17:53:25 - ERROR -   https://mail.secure-verifiedaccounts.com - SSL error
17:53:25 - ERROR -   https://secure-verifiedaccounts.com - SSL error
17:53:25 - ERROR -   https://www.secure-verifiedaccounts.com - SSL error
17:53:27 - SUCCESS - HTTP 200 - bbt-login-my-account.com
Creating ./alerts/2018/11/28/bbt-login-my-account.com.json : {'hostname': 'bbt-login-my-account.com', 'we
': '104.31.64.0/20', 'asn_description': 'CLOUDFLARENET - Cloudflare, Inc., US', 'asn_abuse_email': 'abuse
: 200, 'cert_serial_number': '85:99:8F:C4:76:CC:86:3F:80:5F:51:C7:9A:E7:6A:4B:66:9B:70:AC'}
17:53:28 - WARNING - wildcard certificate: no request for *.bbt-login-my-account.com
17:53:29 - ERROR -   https://paypai.com.secure-verifiedaccounts.com - SSL error
17:53:29 - ERROR -   https://www.paypai.com.secure-verifiedaccounts.com - SSL error
17:53:30 - SUCCESS - HTTP 404 - appleid.apple.com.secure-informations.dynv6.net
Creating ./alerts/2018/11/28/appleid.apple.com.secure-informations.dynv6.net.json : {'hostname': 'appleid
try_code': 'US', 'asn_cidr': '68.183.96.0/20', 'asn_description': 'DIGITALOCEAN-ASN - DigitalOcean, LLC,
': '68.183.96.151', 'http_code': 404, 'cert_serial_number': 'AF:76:7D:60:34:08:C1:0F:92:44:82:95:49:21:D
```

Results

Example #1 : customers abuse

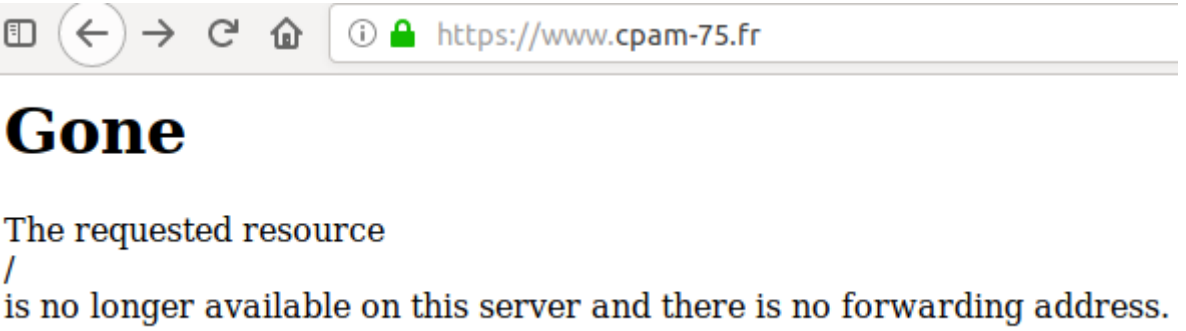
cpam-{78,75,13,...}.fr
→ service potentially abusing our customers (over priced phone number, personal data theft)



Results

Example #1 : customers abuse

cpam-{78,75,13,...}.fr
→ service potentially abusing our customers (over priced phone number, personal data theft)
→ service inactivation



Results

Example #2 : IT management

[redacted].fr

. Legit website
. Best practices not applied : (domainname, hosting etc)

Limits

TLS, not HTTP – only detect hostnames accessed through TLS

RegExp – relying on regexp to find hostnames can lead to miss some of them. Wildcard certificates also beat us.

Trust- we use tier service to get CT certificates (Calidog Security in our case). Can we trust it?

Limits

TLS, not HTTP – only detect hostnames accessed through TLS

RegExp – relying on regexp to find hostnames can lead to miss some of them. Wildcard certificates also beat us.

~~Trust - we use tier service to get CT certificates (Calidog Security in our case). Can we trust it?~~

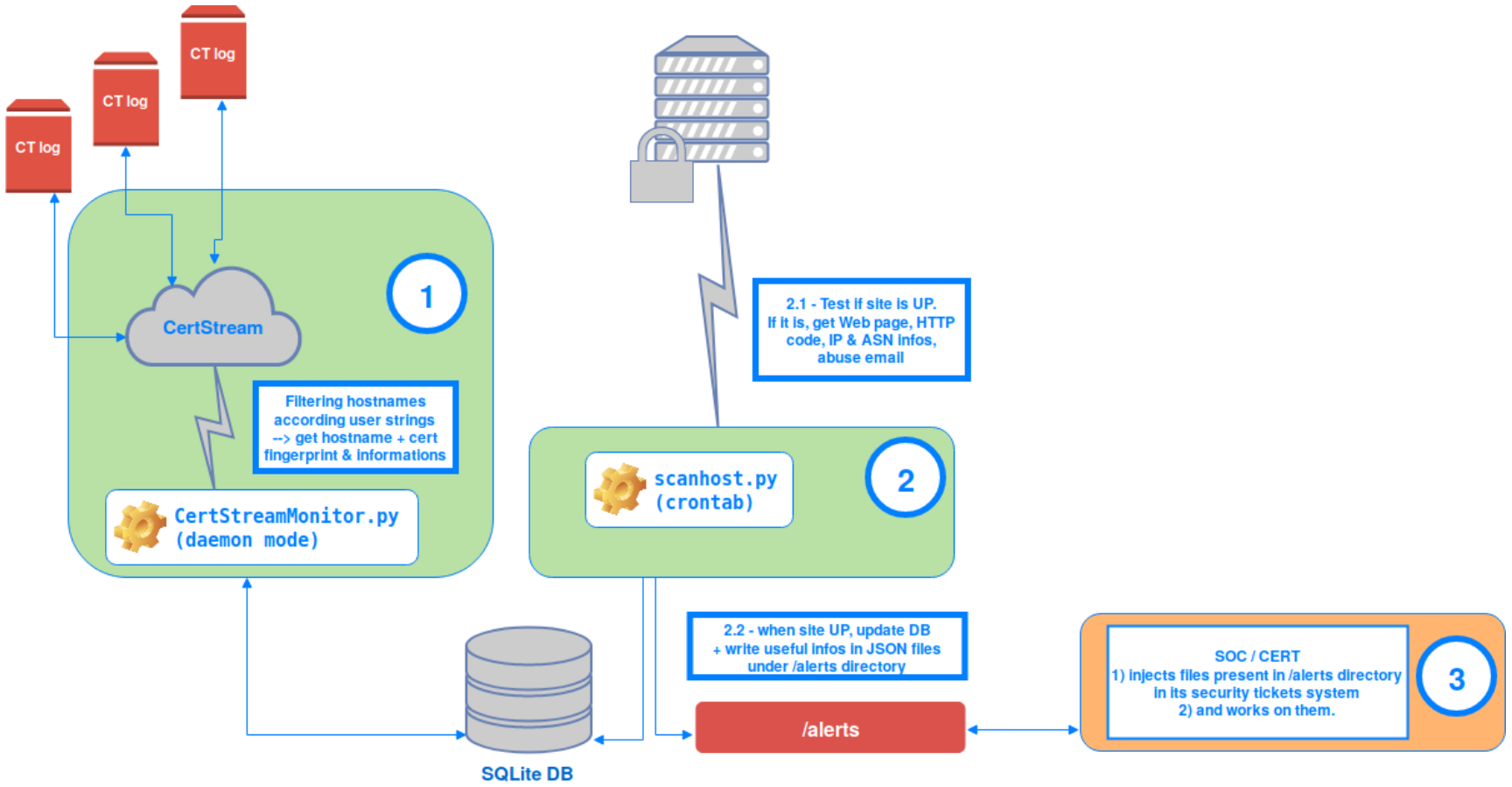
Limits

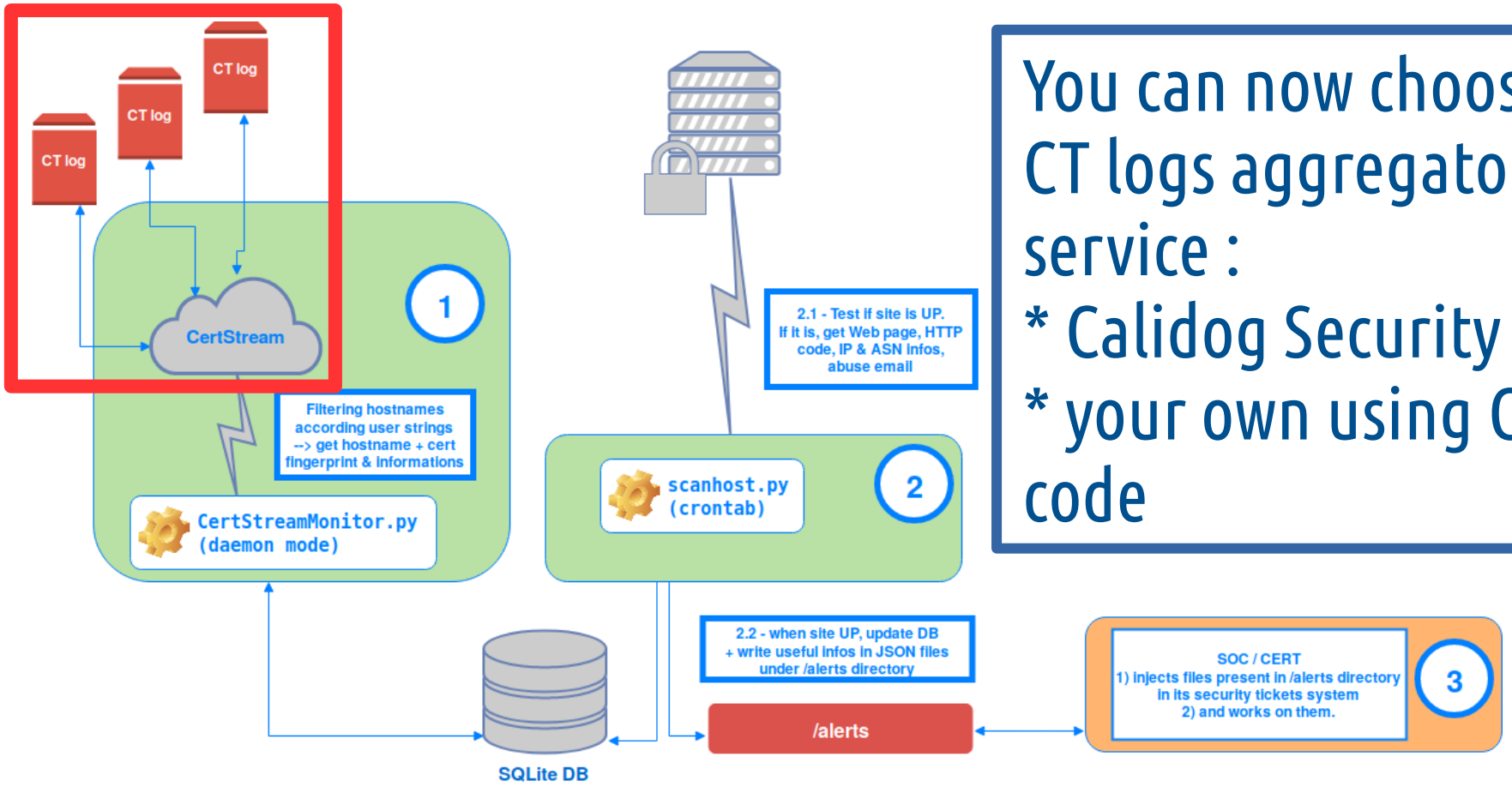
TLS, not HTTP – only detect hostnames accessed through TLS

RegExp – relying on regexp to find hostnames can lead to miss some of them. Wildcard certificates also beat us.

~~Trust - we use tier service to get CT certificates (Calidog Security in our case). Can we trust it?~~
But we rely on their code, a potential single point of failure.
→ it is a call for action to the Infosec community

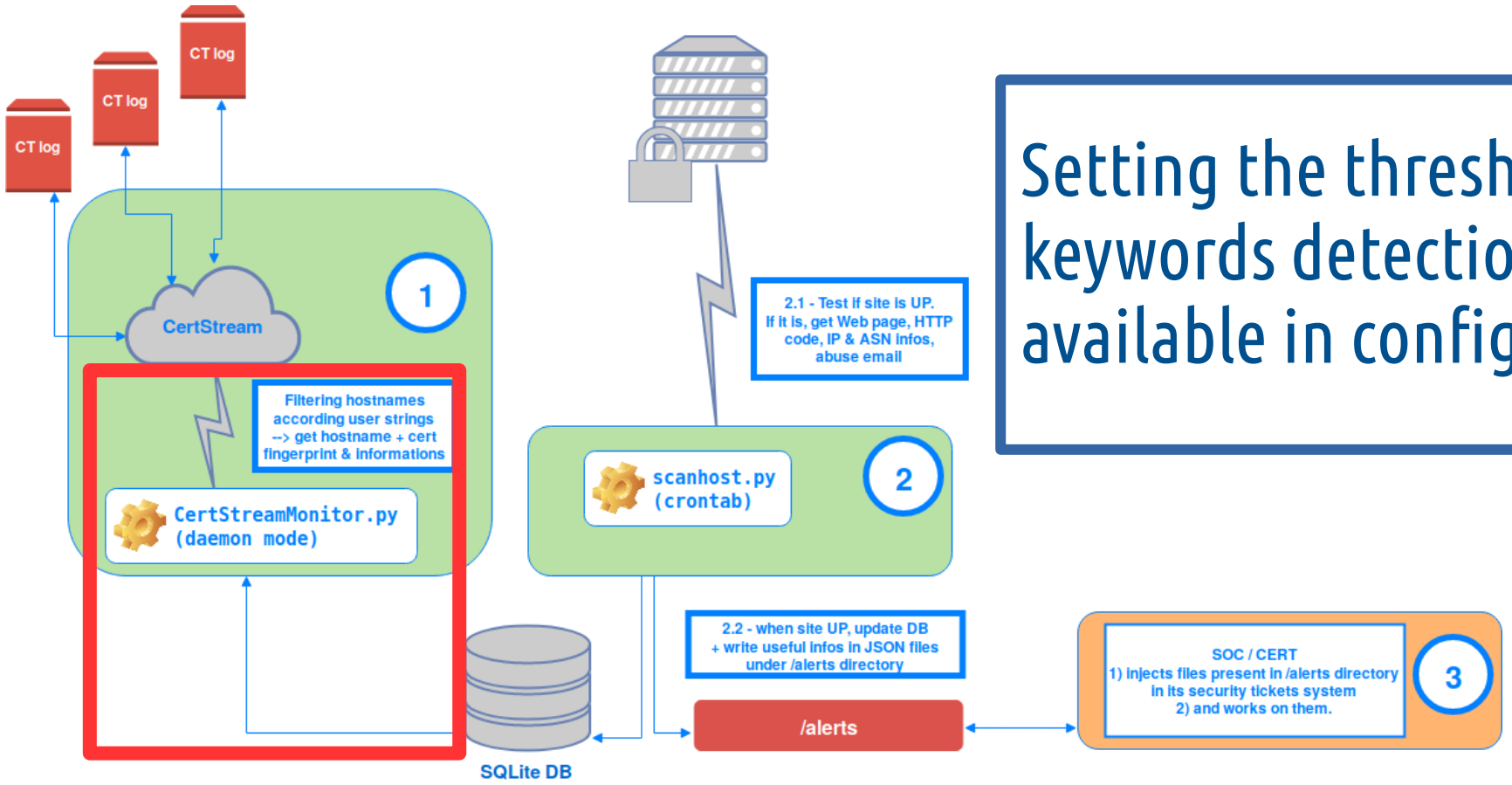
CertStreamMonitor evolution in 9 months


CT log
CT log
CT log
CertStream
1
Filtering hostnames
according user strings
--> get hostname + cert
fingerprint & informations
CertStreamMonitor.py
(daemon mode)
2.1 - Test if site is UP.
If it is, get Web page, HTTP
code, IP & ASN infos,
abuse email
scanhost.py
(crontab)
2
2.2 - when site UP, update DB
+ write useful infos in JSON files
under /alerts directory
SQLite DB
/alerts
SOC / CERT
1) injects files present in /alerts directory
in its security tickets system
2) and works on them.
3



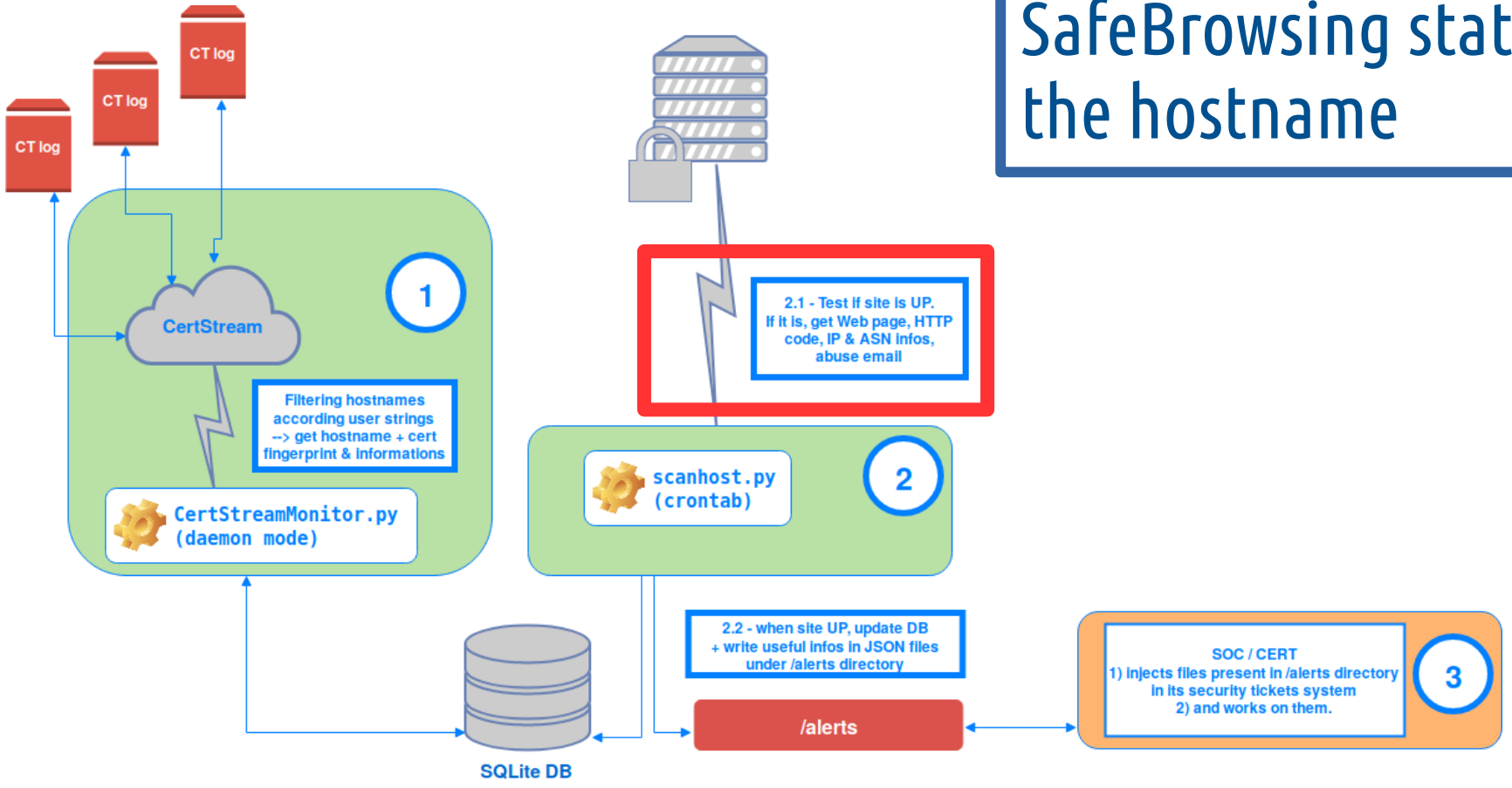
You can now choose your CT logs aggregator service :

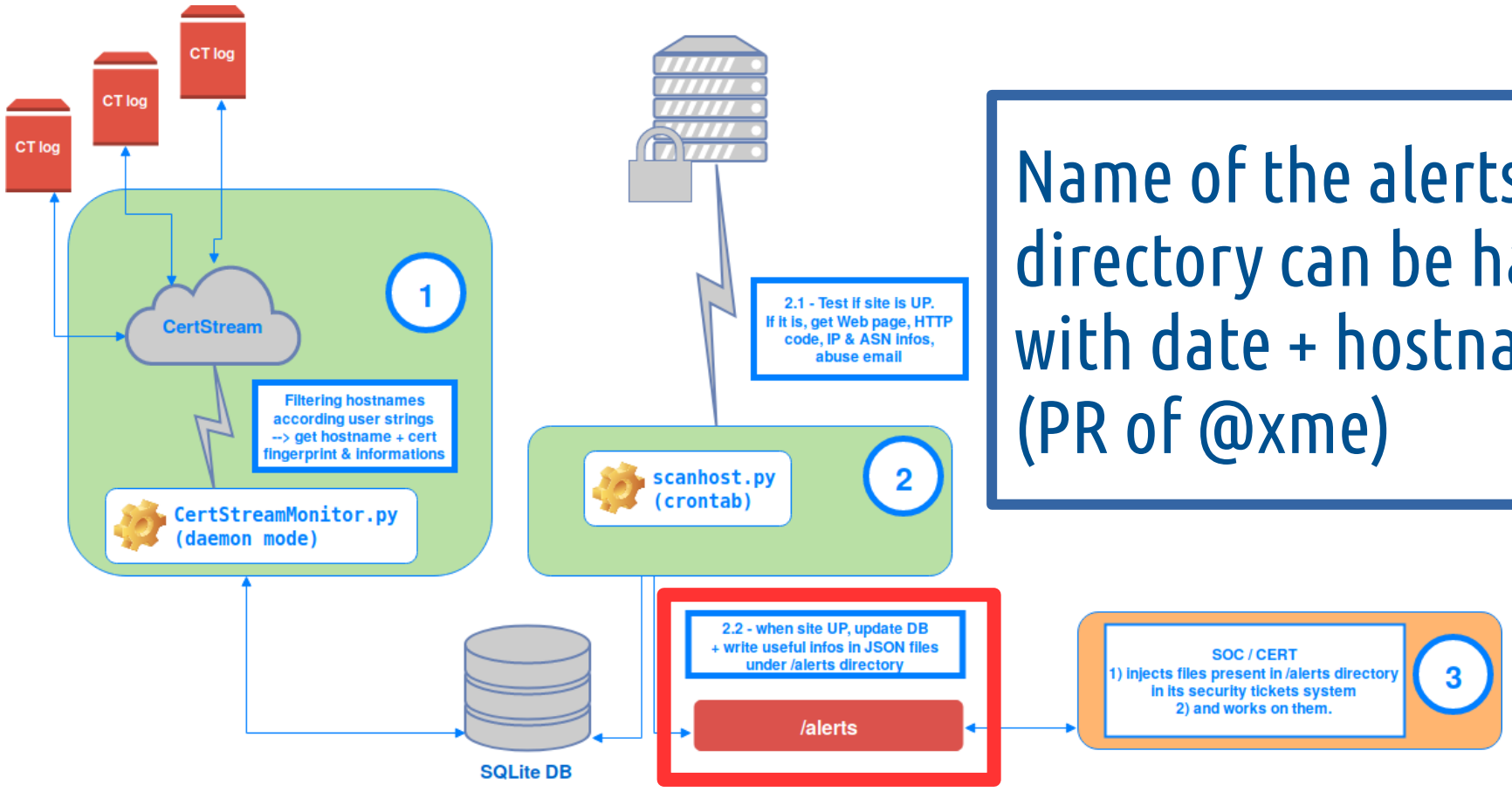
* Calidog Security one
* your own using Calidog code



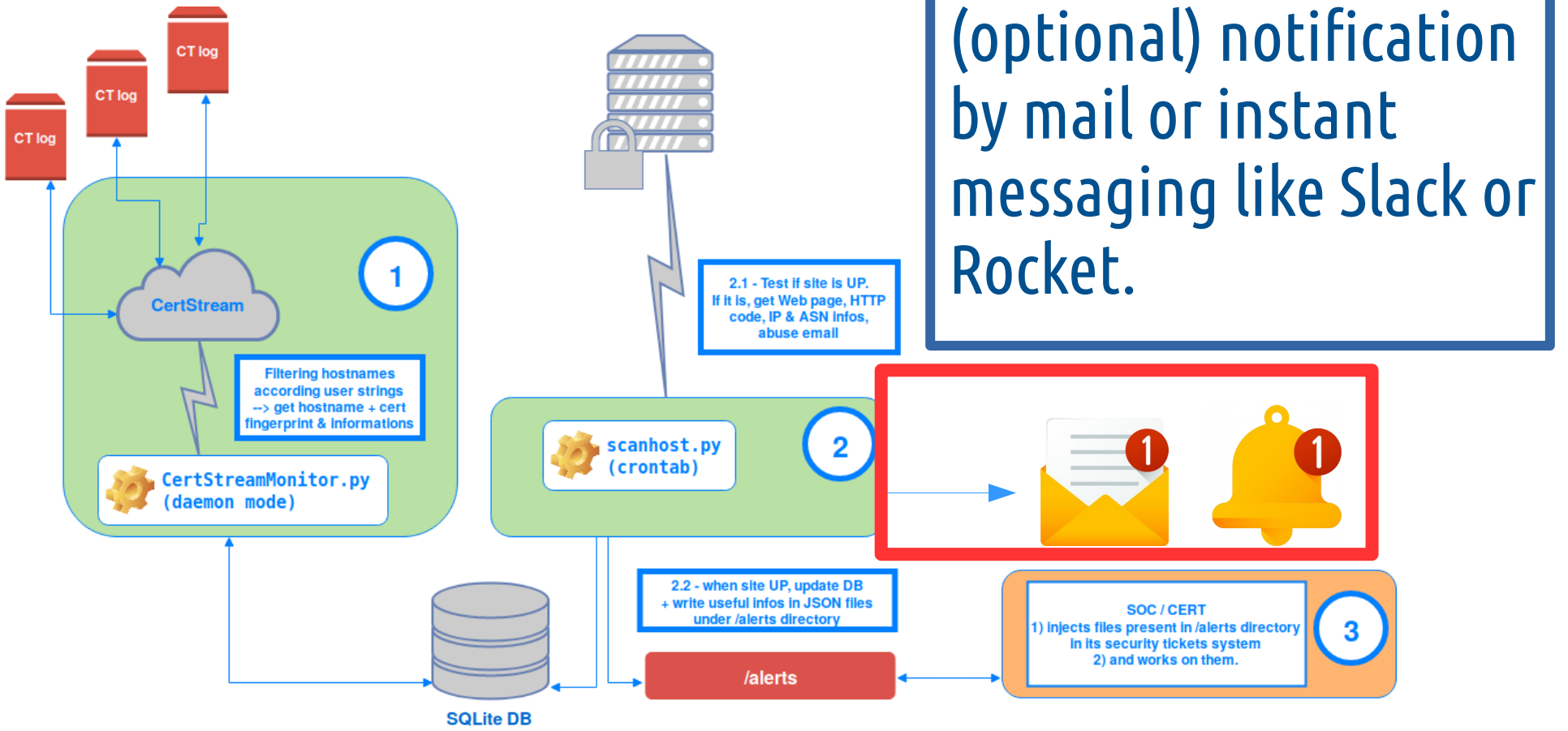
Setting the threshold for keywords detection is available in config file

(optional) check Google SafeBrowsing status of the hostname





Name of the alerts directory can be hashed with date + hostname (PR of @xme)



(optional) notification by mail or instant messaging like Slack or Rocket.

CT & Threats Monitoring: a 24 months story

Certificate Transparency Deadline Moved to April 2018

The announcement

April 2017

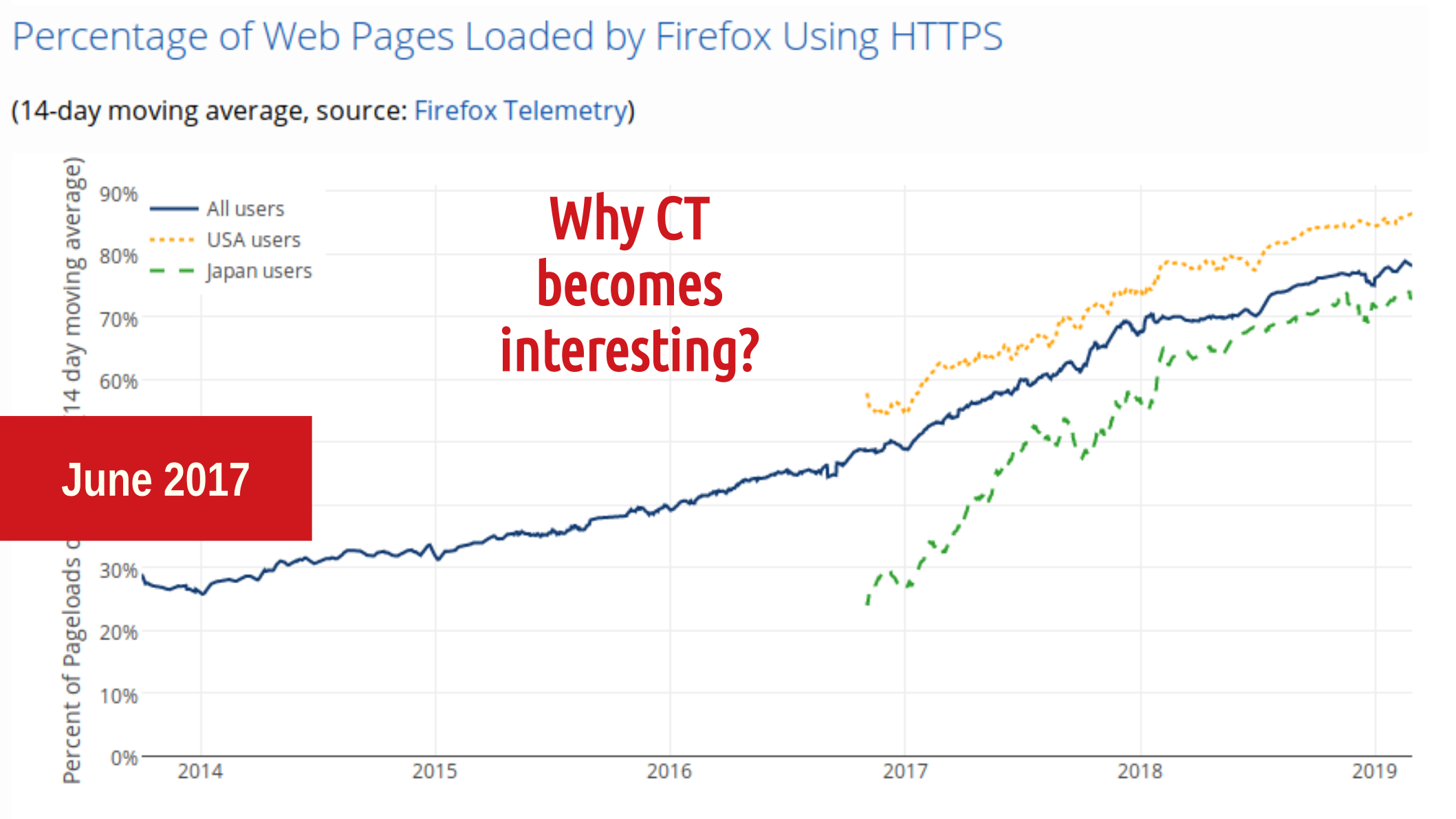
Bruce Morton *(Director, Certificate Technology & Standards; Entrust Datacard)* May 3, 2017 0 Comments

Google just announced they will not be enforcing certificate transparency (CT) logging for all new TLS certificates until April 2018. In a previous blog post, we advised that Google provided a new policy, which required new TLS certificates to be published to the CT logs in order for the domain to be trusted by Chrome.

The reason for the delay was not clear, but Google needs to consider the following:

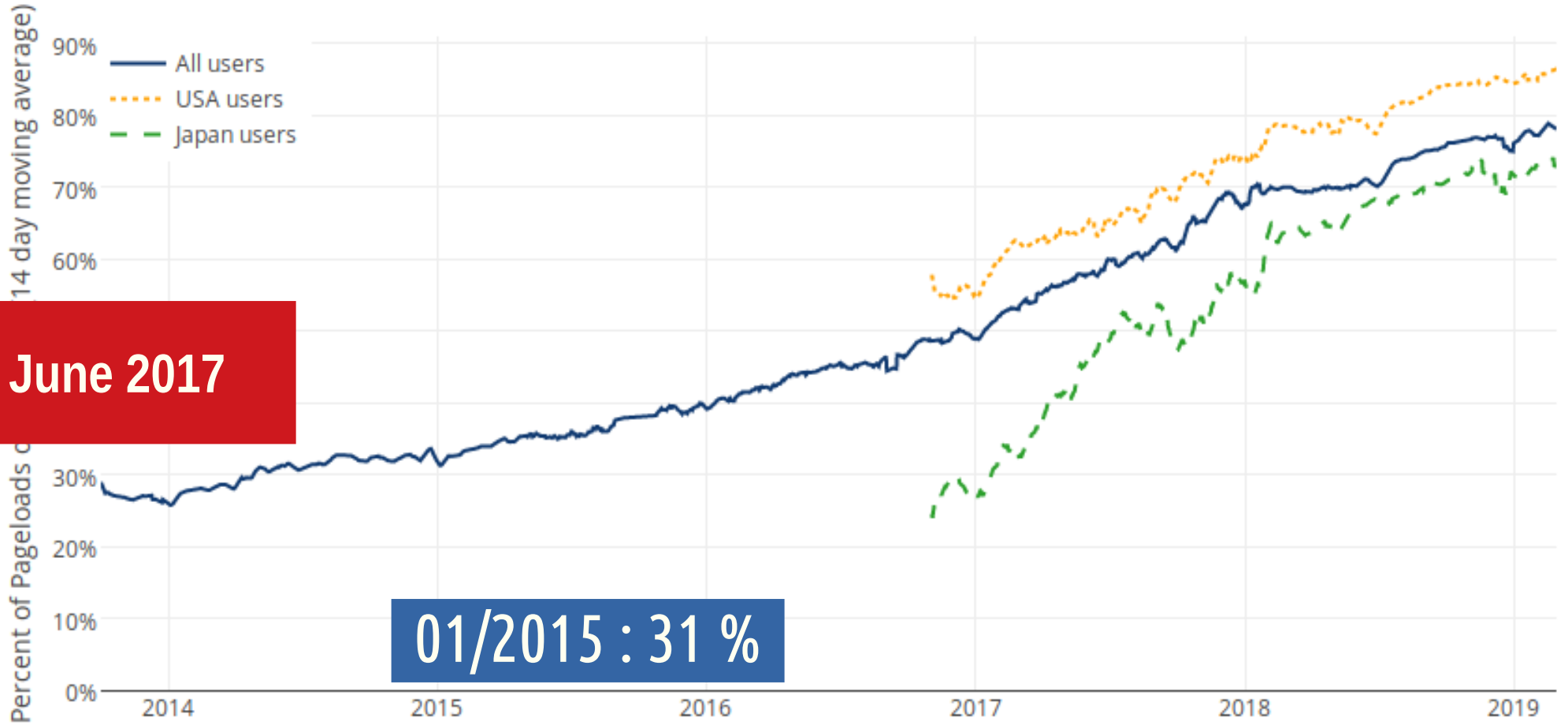
- Overall CT policy discussions with the major stakeholders are underway, but we are still far away from a conclusion.
- Other browsers appear to be supporting CT, but have yet to determine their policies or advance their browser code.
- The CT deployment document, RFC 6962-bis, tracked by IETF standards has not been released.
- The proposed document for CT Domain Label Redaction that addresses privacy has started, but has not been adopted or completed by the IETF.
- Sufficient, scalable, and reliable CT logs have not been deployed by the ecosystem to address the increase in requirements.

Certification authorities (CAs) as well as TLS certificate subscribers will welcome the extra time to help ensure that deployment of CT logging is efficient and seamless.


Percentage of Web Pages Loaded by Firefox Using HTTPS
(14-day moving average, source: Firefox Telemetry)
Why CT becomes interesting?
June 2017
All users
USA users
Japan users
90%
80%
70%
60%
30%
20%
10%
0%
2014
2015
2016
2017
2018
2019

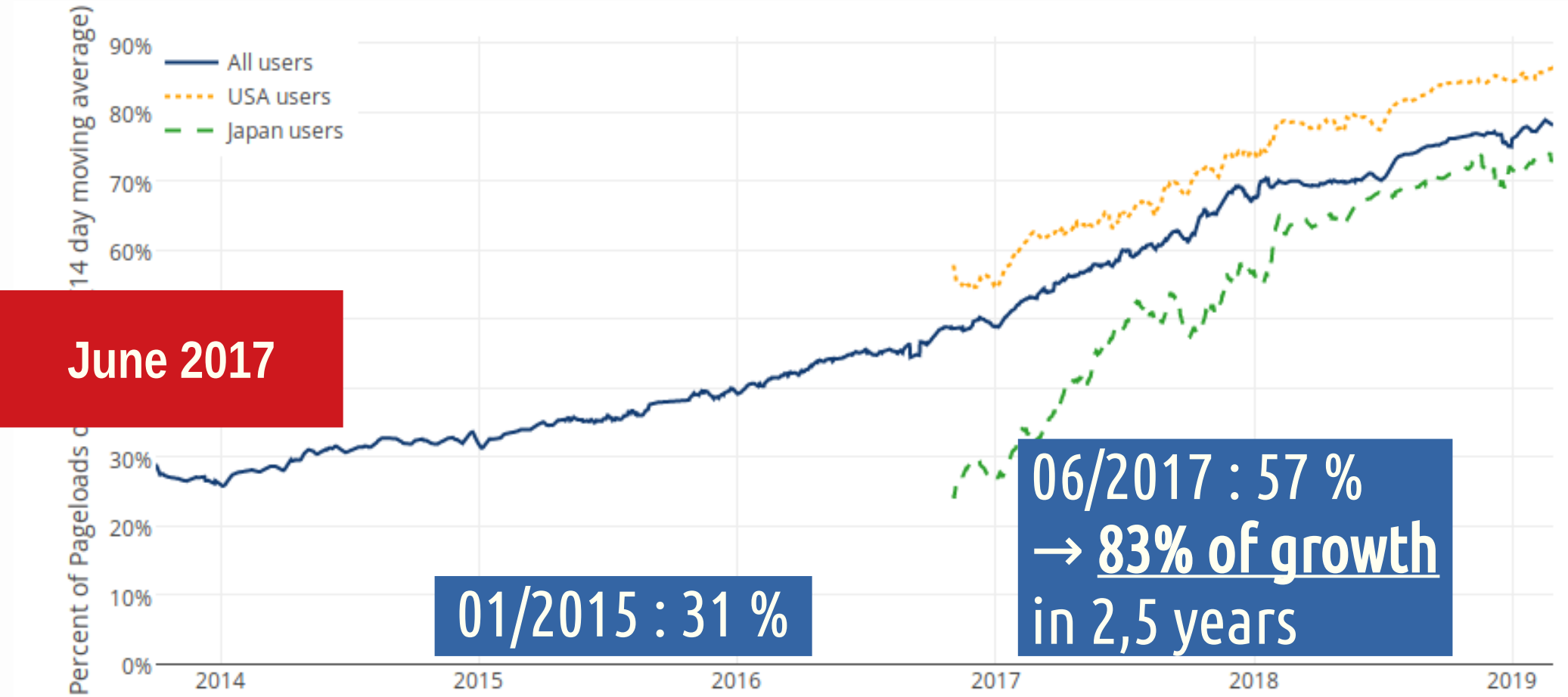
Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)



Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)



Catching phishing before they catch you

Paypal phishing, paypal phishing everywhere

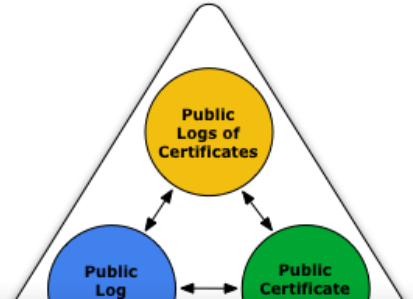
x0rz Follow

Nov 7, 2017 · 2 min read

Let's catch some phishing domain names using CertStream!

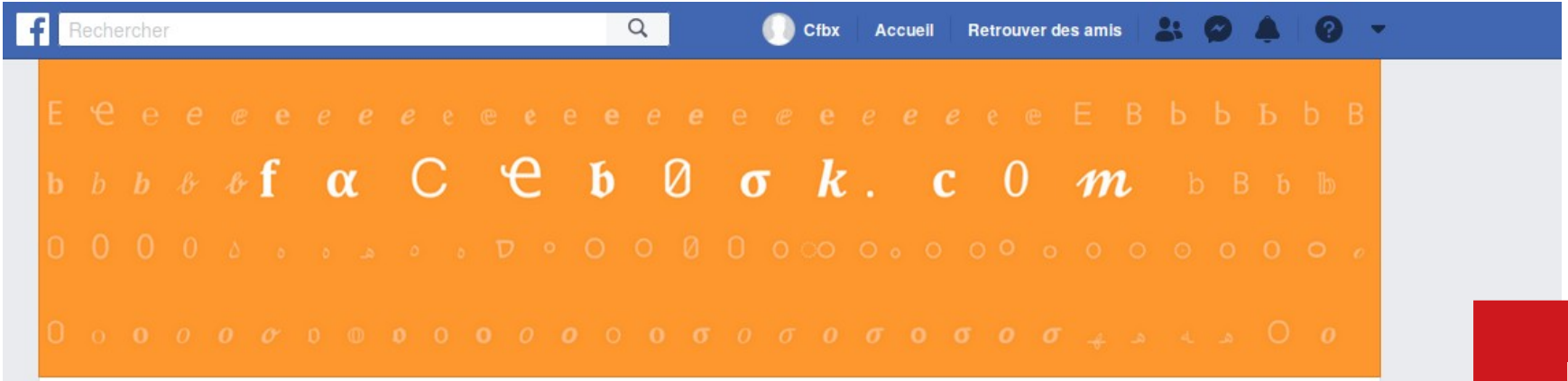
What is Certificate Transparency?

Certificate authorities (CA) get hacked (it already happened), and sometimes they mistakenly issue rogue certificates… That is why Google's Certificate Transparency project try to fix several structural flaws in the SSL certificate system by providing an open framework for monitoring and auditing SSL certificates in nearly real time, as they are being issued!



Nov. 2017

First tools show up



Detecting phishing domains using Certificate Transparency

April 30, 2018 0

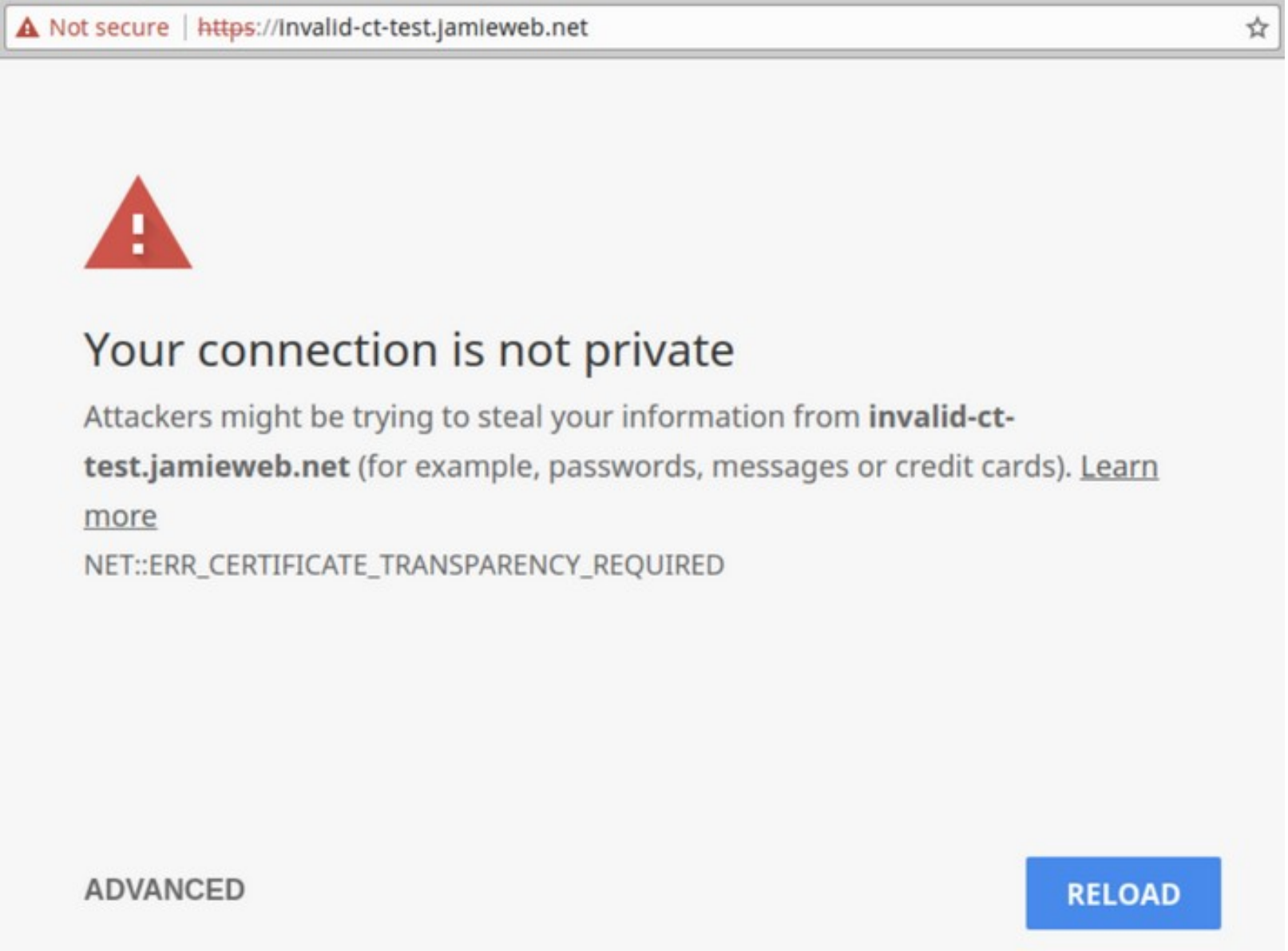
Certificate Transparency: Starting today, all SSL certificates must be logged

Certificate Transparency is now mandatory as of April 30, 2018

Today is the first day that Google is requiring all Certificate Authorities to log the SSL certificates they issue in certificate transparency logs. Failure to do so will result in a browser warning that tells users your website's certificate isn't CT compliant.

May 2018

More complex tools
+ CT required for all certificates



July 2018

Chrome implements CT as a strict requirement

cisco | TALOS

Software | Vulnerability Information | Reputation Center | Library | Support

TUESDAY, NOVEMBER 27, 2018

DNSpionage Campaign Targets Middle East

This blog post was authored by Warren Mercer and Paul Rascagneres.

Update 2018-11-27 15:30:00 EDT: A Russian-language document has been removed. Subsequent analysis leads us to believe it is unrelated to this investigation.

EXECUTIVE SUMMARY

Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it's clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks.

Nov. 2018

When CT becomes a DNS hacks detection tool

Threat Research

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

January 09, 2019 | by Muks Hirani, Sarah Jones, Ben Read

DNS IRAN

Introduction

FireEye's Mandiant Incident Response and Intelligence teams have identified a wave of DNS hijacking that has affected dozens of domains belonging to government, telecommunications and internet infrastructure entities across the Middle East and North Africa, Europe and North America. While we do not currently link this activity to any tracked group, initial research suggests the actor or actors responsible have a nexus to Iran. This campaign has targeted victims across the globe on an almost unprecedented scale, with a high degree of success. We have been tracking this activity for several months, mapping and understanding the innovative tactics, techniques and procedures (TTPs) deployed by the attacker. We have also worked closely with victims, security organizations, and law enforcement agencies where possible to reduce the impact of the attacks and/or prevent further compromises.

Nov. 2018

When CT becomes a DNS hacks detection tool

Emergency Directive 19-01

January 22, 2019

Mitigate DNS Infrastructure Tampering

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 1 "*Mitigate DNS Infrastructure Tampering*". Additionally, see the Director's blog post.

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." 44 U.S.C. § 3553(h)(1)–(2)

Action Four: Monitor Certificate Transparency Logs

- Within 10 business days, CISA will begin regular delivery of newly added certificates to Certificate Transparency (CT) logs for agency domains, via the Cyber Hygiene service.
- Upon receipt, agencies shall immediately begin monitoring CT log data for certificates issued that they did not request. If an agency confirms that a certificate was unauthorized, it must report the certificate to the issuing certificate authority and to CISA.

CT appears in Blue Teams best practices

Jan. 2019

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Tak

CT is point out as one of the tools able to control TLS grey/dark activities

Feb. 2019

Cyber-Mercenary Groups Shouldn't be Trusted in Your Browser or Anywhere Else

BY COOPER QUINTIN | FEBRUARY 22, 2019

Kevin Beaumont
@GossiTheDog

Suivre

I should point out - there's no problem with DarkMatter and UAE being a CA, optics aside. It does highlight InfoSec is trapped in this bubble of large trust; all browsers and devices that do SSL interception are going to need to do certificate transparency lookups, kinda now.

Traduire le Tweet

14:33 - 20 févr. 2019

~~blind~~
vision at Internet scale

efficiency
notified before or soon after the the attacks comes online

low cost
tools and services are there, just use them

+ bonus track: compliance
CT monitoring is now part of best practices requirements

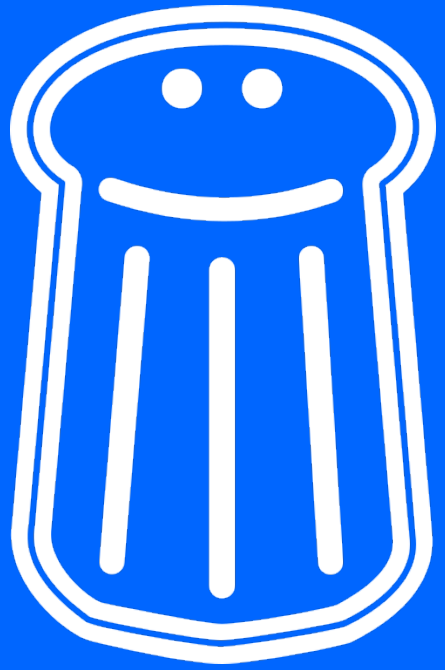
Thanks!

Some questions?

https://github.com/AssuranceMaladieSec

christophe.brocas@assurance-maladie.fr
thomas.damonneville@assurance-maladie.fr

@cbrocas | @o0tAd0o



Pass the SALT 2019

A conference dedicated to Free Software and Security | July, 1-3 2019 | Lille, France

The Call for Papers is OPEN until March, 31 2019

https://cfp.pass-the-salt.org/

Photos credits :

Images under Creative Commons licence:

Clair de lune : https://www.flickr.com/photos/cbrocas/4200102493/
danger : https://www.flickr.com/photos/adulau/26003405317/
complexity : https://www.flickr.com/photos/70023venus2009/6032939635
gain : https://www.flickr.com/photos/143106192@N03/29307455407/
book : https://www.flickr.com/photos/thesoulofhope/14545003924/
evolution : https://www.flickr.com/photos/elle_florio/26750479006/
Flaticons : Freepik from https://www.flaticon.com/