Mining Suricata for Threat Intel with Sagan.

Champ Clark III • CTO @ Quadrant Information Security
Twitter: @quadrantsec / @dabeave666
cclark@quadrantsec.com
What is Sagan?

https://sagan.io
What we heard at Suricon 2018 about Suricata & Threat Intel.
“We want Suricata to do ‘threat intel’ lookups.”
"We want Suricata to do ‘threat intel’ lookups."

- Suricata is really busy doing packet analysis.
- Threat intel “lookups” are expensive.
- Wasn’t built into Suricata.
- (This is prior to learning about Suricata “datasets”.)
“It needs to be dynamic.”
“It needs to be dynamic.”

- Static file with IP addresses is easy enough but not flexible for most.
- Need to be able to add / remove / modify threat intel on the fly.
“Data should be aged out / weighted”
“Data should be aged out / weighted”

- Older data becomes less valuable.
- If the data is past X date, then don’t bother alerting on it.
- Threat Intel “hits” in the field should be able to update the timestamp to show the threat is still active.
Threat Intel should be done “post” Suricata analysis.
The Ultimate Goal:

Parse IP address, hashes, JA3, filenames, URLs, etc & from Suricata and perform “Threat Intelligence” database queries.
Getting logs from Suricata to Sagan for analysis.
Suricata IDS/IPS

Sagan Server

Syslog via syslog-ng/rsyslog
Threat data storage.
### MySQL/MariaDB IP Schema

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>varchar(46)</td>
<td>YES</td>
<td>MUL</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>reputation</td>
<td>int(11)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>fingerprint</td>
<td>varchar(100)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>comments</td>
<td>varchar(1024)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>rep_source</td>
<td>varchar(128)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>rep_published</td>
<td>datetime</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>rep_last_status</td>
<td>datetime</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>
MySQL/MariaDB linking table

<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Greylist/Neutral</td>
</tr>
<tr>
<td>2</td>
<td>Client IP</td>
</tr>
<tr>
<td>3</td>
<td>Malicious</td>
</tr>
<tr>
<td>4</td>
<td>Honeypot</td>
</tr>
<tr>
<td>7</td>
<td>Advisory</td>
</tr>
<tr>
<td>8</td>
<td>Scanner</td>
</tr>
<tr>
<td>9</td>
<td>Tor</td>
</tr>
<tr>
<td>10</td>
<td>Proxy IP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>int(11)</td>
<td>NO</td>
<td>PRI</td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>varchar(50)</td>
<td>NO</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>
Redis API keys

GET {SHA HASH} # Read only
GET [SHA HASH]:write # Read and write.

The keys contain something like: “Champ Clark III”
Querying the threat intel
Sample HTTP GET request

{  
  "api_user": "Generic API User",
  "code": 3,
  "category": "Malicious",
  "comments": "Malicious: Associated with previous critical event.",
  "source": "Quadrant Systems",
  "ctime_epoch": 1429488000,
  "ctime": "2015-04-20 00:00:00",
  "mtime_epoch": 1429488000,
  "mtime": "2015-04-20 00:00:00",
  "query": "104.152.187.66",
  "query_type": "ip_address"
}
Configuring Sagan.
- bluedot:

  enabled: yes
  device-id: "Suricata_Threat_Intel"
  cache-timeout: 120
  categories: "$RULE_PATH/bluedot-categories.conf"

  max-ip-cache: 300000
  max-hash-cache: 10000
  max-url-cache: 20000
  max-filename-cache: 1000
  max-ja3-cache: 10000

  ip-queue: 100
  hash-queue: 100
  url-queue: 100
  filename-queue: 100
  ja3-queue: 100

  host: "bluedot.qis.io"
  ttl: 86400
  uri: "q.php?qipapikey=APIKEYHERE"

  skip_networks: "8.8.8.8/32, 8.8.4.4/32"
Sagan rules for Suricata!

- `$RULE_PATH/suricata-bluedot.rules`
- `$RULE_PATH/suricata-geoip.rules`
- `$RULE_PATH/suricate-aetas.rules`
Sagan.yaml - enable JSON Parsing

parse-json-message: enabled
parse-json-program: enabled
json-message-map: "${RULE_PATH}/json-message.map"
Sagan - Sample JSON input map.

```json
{ "software":"suricata", "event_type": "event_type", "src_ip": "src_ip", "dest_ip": "dest_ip", "src_port": "src_port", "dest_port": "dest_port", "message": "%JSON%", "proto": "proto", "flow_id": "flow_id", "md5": "md5", "sha1": "sha1", "sha256": "sha256", "filename": "filename", "hostname": "hostname", "url": "url", "ja3": "hash" }
```
Sagan startup screen (basic statistics).

```
[*,.-.-.,.-]  [-[ Sagan Version 1.2.2 - Engine Statistics ]-]
[*]        \/
[*]       (o_)
[*]       /  \
[*]     (|| ||)
[*]     00-00

Received/Processed/Ignored : 17127907/15767113/0 (92.055%/0.000%)
Signatures matched          : 552814 (3.228%)
Alerts                      : 552814 (3.228%)
After                       : 0 (0.000%)
Threshold                   : 0 (0.000%)
Dropped                     : 0 (0.000%)
Thread Exhaustion           : 1360794 (7.945%)
Thread Usage                : 0/600 (0.000%)
JSON Input                  : 15767074 (92.055%)
JSON Program/Message        : 15701466 (91.672%)
GeoIP Hits:                 : 17374 (0.101%)
GeoIP Lookups:              : 18412709
GeoIP Errors                : 363
Uptime                      : 2 days, 11 hours, 43 minutes, 22 seconds.
Avg. events per/second      : 79
```
Sagan “Bluedot” IP Rep statistics

```
* IP Reputation *

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses in cache</td>
<td>1522 (0.507%)</td>
</tr>
<tr>
<td>IP hits from cache</td>
<td>21997632 (100.000%)</td>
</tr>
<tr>
<td>IP/Bluedot hits in logs</td>
<td>26278</td>
</tr>
<tr>
<td>IP with date &gt; mdate</td>
<td>0</td>
</tr>
<tr>
<td>IP with date &gt; cdate</td>
<td>0</td>
</tr>
<tr>
<td>IP with date &gt; mdate [cache]</td>
<td>0</td>
</tr>
<tr>
<td>IP with date &gt; cdate [cache]</td>
<td>0</td>
</tr>
<tr>
<td>IP queries per/second</td>
<td>0 (0/1000)</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashes in cache</td>
<td>698 (0.233%)</td>
</tr>
<tr>
<td>Hash hits from cache</td>
<td>96261 (99.993%)</td>
</tr>
<tr>
<td>Hash/Bluedot hits in logs</td>
<td>0</td>
</tr>
<tr>
<td>Hash queries per/second</td>
<td>0 (0/1000)</td>
</tr>
<tr>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>URLs in cache</td>
<td>1898 (0.633%)</td>
</tr>
<tr>
<td>URL hits from cache</td>
<td>222970 (99.991%)</td>
</tr>
<tr>
<td>URL/Bluedot hits in logs</td>
<td>0</td>
</tr>
<tr>
<td>URL queries per second</td>
<td>0 (0/1000)</td>
</tr>
</tbody>
</table>
Sagan “Bluedot” Filename statistics

* Filename Reputation *

Filenames in cache : 25 (0.250%)
Filename hits from cache : 37825 (99.999%)
Filename/Bluedot hits in logs : 0
URL queries per/second : 0 (0/1000)
Sagan “Bluedot” JA3 statistics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLS/JA3 Reputation</strong></td>
<td></td>
</tr>
<tr>
<td>JA3 in cache</td>
<td>41 (0.410%)</td>
</tr>
<tr>
<td>JA3 hits from cache</td>
<td>533804 (100.000%)</td>
</tr>
<tr>
<td>JA3/Bluedot hits in logs</td>
<td>0</td>
</tr>
<tr>
<td>JA3 queries per/second</td>
<td>0 (0/1000)</td>
</tr>
</tbody>
</table>
Sagan rules for detection.
alert any $EXTERNAL_NET any -&gt; $HOME_NET any
(msg:"Bluedot from Suricata JSON flow";
event_type: suricata-flow|flow;
content:!"/intel.php"; classtype: suspicious-traffic; bluedot: type
ip_reputation, track both, none, Malicious,Tor,Honeypot,Proxy; sid: 8900000;
rev:1;)

IP address lookup:
alert any $EXTERNAL_NET any -> $HOME_NET any
(msg: "[BLUEDOT] Malicious hash detected via Bluedot"; event_type: files|fileinfo;
content:!"/intel.php"; bluedot: type file_hash,Malicious; classtype:
suspicious-traffic; sid:8900001; rev:1;)

MD5/SHA1/SHA256 lookup:
alert any $EXTERNAL_NET any -> $HOME_NET any
(msg: "[BLUEDOT] URL filename detected via Bluedot"; event_type: http;
content:!/intel.php"; bluedot: type url,Malicious; classtype: suspicious-traffic;
sid:8900003; rev:1;)

URL lookup
Filename lookup

alert any $EXTERNAL_NET any -> $HOME_NET any
(msg: "[BLUEDOT] Malicious filename detected via Bluedot"; event_type: files|fileinfo;
content:!/intel.php"; bluedot: type
filename,Malicious; classtype:
suspicious-traffic; sid:8900002; rev:1;)

alert any $EXTERNAL_NET any -> $HOME_NET any
(msg:"Bluedot from Suricata JSON flow";
event_type: suricata-flow|flow;
content:!/intel.php";
classtype: not-suspicious;
bluedot: type ip_reputation,
track all, mdate_effective_period 2 months,
Malicious,Tor,Proxy; sid: 8900000; rev:1;)

IP address lookup with mtime
alert any $EXTERNAL_NET any -> $HOME_NET any
(msg: "Bluedot from Suricata JSON flow";
event_type: suricata-flow|flow;
content:!/intel.php";
classtype: suspicious-traffic;
bluedot: type
ip_reputation, track all,
cdate_effective_period 6 months,
Malicious,Tor,Proxy;
sid: 8900000;
rev: 1;)

IP address lookup with ctime
SSH traffic by GeoIP destination.

alert any $EXTERNAL_NET any -> $HOME_NET any (msg:"GEOIP Suricata ssh by dst"; country_code: track by_dst, isnot $HOME_COUNTRY; classtype: successful-user; event_type: ssh; sid:8900022; rev:1;
SSH traffic by time destination.

alert any $EXTERNAL_NET any -> $HOME_NET any (msg:"Strange time for SSH traffic by dest"; alert_time: days 0123456, hours 0300-0500; classtype: suspicious-traffic; event_type: ssh; sid:8900022; rev:1;)

Bluedot source code.

https://github.com/beave/sagan/tree/master/extra/bluedot
Q/A
https://sagan.io

Champ Clark III • CTO @ Quadrant Information Security
Twitter: @quadrantsec / @dabeave666
cclark@quadrantsec.com