



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.**

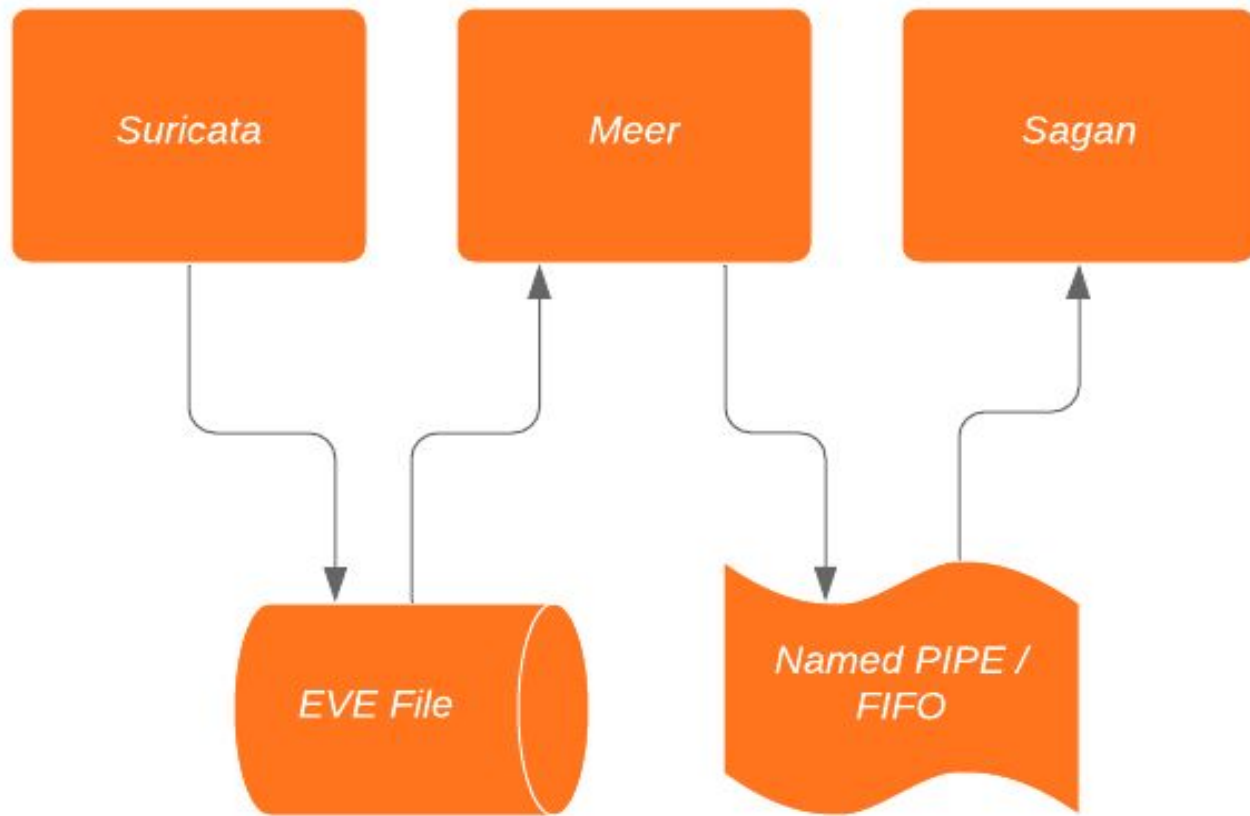
The Ultimate Goal:



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



Field	Type	Null	Key	Default	Extra
ip_address	varchar(46)	YES	MUL	NULL	
reputation	int(11)	YES		NULL	
fingerprint	varchar(100)	YES		NULL	
comments	varchar(1024)	YES		NULL	
rep_source	varchar(128)	YES		NULL	
rep_published	datetime	YES		NULL	
rep_last_status	datetime	YES		NULL	

MySQL/MariaDB linking table



id	name
1	Greylist/Neutral
2	Client IP
3	Malicious
4	Honeypot
7	Advisory
8	Scanner
9	Tor
10	Proxy IP

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
name	varchar(50)	NO		NULL	



Redis API keys

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

The keys contains something like:
"Champ Clark III"



Querying the threat intel

Sample HTTP GET request



<https://bluedot.gis.io/intel.php?apikey={APIKEY}&ip=104.152.187.66&pretty>

Sample API return



```
{
  "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_timestamp": "2019-10-24 13:27:07",
  "query": "104.152.187.66",
  "query_type": "ip_address"
}
```



Configuring Sagan.

Sample “sagan.yaml” Bluedot configuration



```
- 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.



```
{ "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_)   Received/Processed/Ignored : 17127907/15767113/0 (92.055%/0.000%)
[*]  /_  \//   Signatures matched      : 552814 (3.228%)
[*]  (||  ||)  Alerts                   : 552814 (3.228%)
[*]   oo-oo    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



```
[*]      -[ Sagan Bluedot Processor ]-
[*]
[*]      * IP Reputation *
[*]
[*]      IP addresses in cache           : 1522 (0.507%)
[*]      IP hits from cache             : 21997632 (100.000%)
[*]      IP/Bluedot hits in logs        : 26278
[*]      IP with date > mdate           : 0
[*]      IP with date > cdate           : 0
[*]      IP with date > mdate [cache]   : 0
[*]      IP with date > cdate [cache]   : 0
[*]      IP queries per/second          : 0 (0/1000)
```

Sagan "Bluedot" File hash statistics



```
[*]          * File Hash *
[*]
[*]          Hashes in cache                : 698 (0.233%)
[*]          Hash hits from cache           : 96261 (99.993%)
[*]          Hash/Bluedot hits in logs      : 0
[*]          Hash queries per/second        : 0 (0/1000)
```

Sagan “Bluedot” URL statistics



```
[*]          * URL Reputation *  
[*]  
[*]          URLs in cache           : 1898 (0.633%)  
[*]          URL hits from cache     : 222970 (99.991%)  
[*]          URL/Bluedot hits in logs : 0  
[*]          URL queries per/second  : 0 (0/1000)
```

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



```
[*]          * TLS/JA3 Reputation *  
[*]  
[*]      JA3 in cache                : 41 (0.410%)  
[*]      JA3 hits from cache         : 533804 (100.000%)  
[*]      JA3/Bluedot hits in logs   : 0  
[*]      JA3 queries per/second     : 0 (0/1000)
```




Sagan rules for detection.



IP address lookup:

```
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 both, none,
Malicious,Tor,Honeypot,Proxy; sid: 8900000;
rev:1;)
```

MD5/SHA1/SHA256 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;)
```

URL 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;)
```

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;)
```

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:
not-suspicious; bluedot: type ip_reputation,
track all, mdate_effective_period 2 months,
Malicious,Tor,Proxy; sid: 8900000; rev:1;)
```



IP address lookup with ctime

```
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;)
```

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