The state of Meer

Champ Clark III [CTO]
Quadrant Information Security
cclark@quadrantsec.com

October 20 - 22, 2021

What is Meer.

* A data spooling system.
* Adds data to existing Suricata EVE JSON.
* An EVE data router.

What is Meer.

* System resource friendly.
* Fast.
* Simple (via the “KISS” motto)

The “meer.yaml”

* “core”
* “output”

```yaml
core:

  hostname: "mysensor"  # Unique name for this sensor (no spaces)
  interface: "eth0"     # Can be anything, but probably should be your interfaces.
  description: "My Awesome Sensor"
  runas: "suricata"     # User to "drop privileges" too.
  classification: "/etc/suricata/classification.config"
  meer_log: "/var/log/meer/meer.log"           # Meer log file
  waldo_file: "/var/log/meer/meer.waldo"       # Where to store the last record
  lock_file: "/var/log/meer/meer.lck"          # To prevent dueling processes.
  follow_eve: "/var/log/suricata/alert.json"  # The Suricata EVE file to monitor
```

meer.yaml (“core”)

The “meer.yaml”

Data enrichment.

```
fingerprint: disabled
fingerprint_log: "/tmp/fingerprint.eve"
fingerprint_networks: "10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12"
```

meer.yaml (“core”)

```
oui_lookup: disabled
oui_filename: "/usr/local/etc/manuf"
```

meer.yaml (“core”)

```
dns: enabled
dns_cache: 900          # Time in seconds.
```

meer.yaml (“core”)

The “meer.yaml” (“output”).

Where & how to send data.

The “meer.yaml” (“output”).

* SQL (MySQL/MariaDB/PostgreSQL)
* File
* Named pipe (FIFO)
* External
* Redis
* Elasticsearch

The “meer.yaml” - output event_types

alert, files, flow, dns, http, tls, ssh, smtp, email, fileinfo, dhcp, stats, rdp, sip, ftp, Ikev2, nfs, tftp, smb, dcerpc, mqtt, netflow, metadata, dnp3, anomaly.

```
output-plugins:

  sql:

    enabled: yes
    driver: mysql        # "mysql" or "postgresql"
    debug: no
    server: 127.0.0.1
    port: 3306           # Change to 5432 for PostgreSQL
    username: "XXXX"
    password: "XXXXXX"
    database: "snort_test"

    reconnect: enabled
    reconnect_time: 10

    extra_data: enabled         # Things like, xff, etc.

    reference_system: disabled                  # Legacy Barnyard2 support
    sid_file: "/etc/suricata/rules/sid-msg.map"   # Created with "create-sidmap"
    reference: "/etc/suricata/reference.config"
```

meer.yaml (“output”)

```
file:

  enabled: no
  file_location: "/path/to/output/file"

  alert: enabled
  files: enabled
  flow: enabled
  dns: enabled
  .....
```

meer.yaml (“output”)

```
pipe:

  enabled: no
  pipe_location: /var/sagan/fifo/sagan.fifo
  pipe_size: 1048576

  alert: enabled
  files: enabled
  flow: enabled
  dns: enabled
  http: enabled
  ....
```

meer.yaml (“output”)

```
external:

  enabled: no
  debug: no

  program: "/usr/local/bin/external_program"

  meer_metadata: enabled # metadata: meer external
  cisco_policies: "none" # policy-security-ips,policy-max-detect-ips,etc.
  et_signature_severity: "critical" # Critical,Major,Minor,Informational

  alert: enabled
  files: disabled
  flow: disabled
  ....
```

meer.yaml (“output”)

```
redis:

  enabled: no
  debug: no
  server: 127.0.0.1
  #password: "mypassword"
  port: 6379
  batch: 1                    # Batching (pipelining) data.
  key: "suricata"             # Default 'channel' to use.  If none is specified, the
                              # channel name will become the "event_type".
  mode: lpush                 # lpush, rpush, channel, set.
  append_id: disabled         # When enabled, the key becomes "event_type|hostname|waldo".
                              # For example, "alert|myhostname|1234".


  alert: enabled
  files: enabled
  flow: enabled
  ....
```

meer.yaml (“output”)

```yaml
elasticsearch:

  enabled: no
  debug: no
  url: "http://127.0.0.1:9200/_bulk"
  index: "suricata_$EVENTTYPE_$YEAR$MONTH$DAY"
  insecure: true
  batch: 100
  threads: 10
  #username: "myusername"
  #password: "mypassword"

  alert: enabled
  files: enabled
  ...
```

meer.yaml (“output”)

Future “core” support?

Continue to enrich Suricata data.

Automatic unification of “alert” data via “flow_id”?

Future output support?

Suricata feature request #120

"It would be great to have the capability to capture an entire session."

Suricata feature request #120

EVE JSON -> PCAP ?

HTTP (TLS) output?

IDK: You tell me :)

Meer: https://gitub.com/quadrantsec/meer
https://meer.readthedocs.io

Sagan: https://github.com/quadrantsec/sagan
https://sagan.readthedocs.io

Q & A

Champ Clark III (CTO) @ Quadrant Information Security

Twitter @dabeave666
E-Mail: cclark@quadrantsec.com