Suricata 3.1

Victor Julien
Amsterdam 2016

Bio

- @inliniac
- blog.inliniac.net
- Open Source hippie
- Suricata creator and lead developer
- Vuurmuur

3.0

- First major release in 2 years
- Many new features, much better performance
- Released January 2016

3.0

- Multi-tenancy
  - Multiple detection engines with their own settings
- “xbits” - flowbits on steroids
  - Per host
  - Per ip-pair
- SMTP file extraction

3.0

- Much improved JSON output
  - Engine stats
  - Meta data added to alerts
  - Payload logging
  - Netflow(ish) logging
- NETMAP on Linux and FreeBSD
- Lua scripting extensions

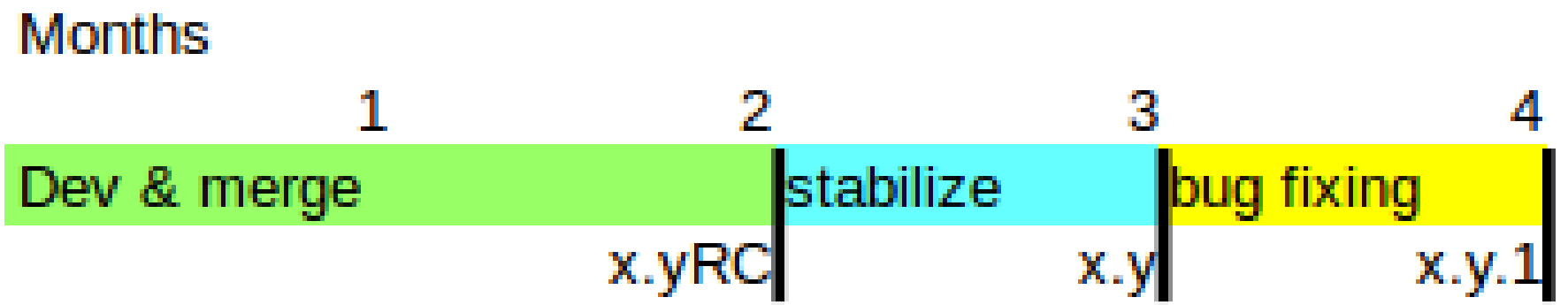
3.0 Lua improvements

- Output scripts
- Stats
- Netflow
- Protocols: SSH/TLS
- Stream payloads

```lua
-- simple fast-log to stdout lua module

function init (args)
    local needs = {}
    needs["type"] = "packet"
    needs["filter"] = "alerts"
    return needs
end

function setup (args)
    alerts = 0
end

function log(args)
    ts = SCPacketTimeString()
    sid, rev, gid = SCRuleIds()
    ipver, srcip, dstip, proto, sp, dp = SCPacketTuple()
    msg = SCRuleMsg()
    class, prio = SCRuleClass()
    if class == nil then
        class = "unknown"
    end

    print (ts .. "  [**] [" .. gid .. ":" .. sid .. ":" .. rev .. "] " ..
           msg .. " [**] [Classification: " .. class .. "] [Priority: " ..
           prio .. "] {" .. proto .. "} " ..
           srcip .. ":" .. sp .. " -> " .. dstip .. ":" .. dp)

    alerts = alerts + 1;
end

function deinit (args)
    print ("Alerted " .. alerts .. " times");
end
~
```

New release schedule

- In Barcelona we decided to go for time based “major” releases
- 3 per year, so ~4 month per release
- Maybe a little bit too aggressive, we’ll eval later this year


Months
1
2
3
4
Dev & merge
stabilize
bug fixing
x.yRC
x.y
x.y.1

3.1 TLS Updates

- Inspecting “raw” TLS is increasingly important
- Great work by Mats Klepsland of NorCERT
- Matching on tls_sni (mpm enabled)
- Improved logger
- Lots of “under the hood” improvements

3.1 performance improvements

- Hyperscan
  - Default for MPM and SPM matching
- Detection engine rewrite
  - Much simplified grouping code
  - Shorter load times
  - Better perf for most
- AF_PACKET: tpacket v3

3.1 performance improvements

- “StreamingBuffer” work
  - New low level data storing API for HTTP body tracking
  - File API moved over to it as well
- Threading / locking updates
  - Detection engine now runs entirely under flow lock
  - Much simpler for adding modules
- Lots of smaller things (e.g. shrink internal data structs)

3.1 Misc

- Usability
  - -i now uses --af-packet if available
  - Consistent thread naming
  - Improved NIC offloading detection
- QA
  - Lots of fuzz testing (AFL)
  - Entry points into the engine to assist there

3.1.1

- Planned for mid July
- Bug fix update for 3.1
- NETMAP fixes
- Offloading detection improvements
- (likely) SMTP Lua extensions

Something about QA

- Buildbot
- Address Sanitizer (asan)
- Fuzz testing
  - AFL+asan
  - pcap based
- Just started using Undefined Behavior Sanitizer (ubsan)

3.2 work and plans

- Performance
  - Deeper Hyperscan integration (libpcre acceleration)
- TLS
  - Logging of and matching on: cipher suites, more extensions, more cert info
  - Re-implement tls keywords to be more performant & expressive

3.2 work and plans

- Documentation
  - Move user docs to sphinx
  - Sphinx allows for nice pdf’s and readthedocs
- Improve ease of use
  - Disable NIC offloading, instead of just warning
  - Improve default settings
  - Shrink & split up default yaml file

3.2 work and plans

- TCP Stream reassembly rewrite, improving:
  - performance
  - code quality
  - Anomaly detection
    - e.g. improved man on the side (mots) detection
  - Detection engine integration
- File extraction/tracking:
  - SHA256 support

YARA

- "The pattern matching swiss knife for malware researchers (and everyone else)"
- Developed by VirusTotal (part of Google)
- Just relicensed to BSD license
- I have a PoC for inspecting files with YARA rules

Get involved

- There are things to do at every level
  - From hardcore coding, to designing swag
  - Docs, diagrams, video guides
  - User support, evangelizing
  - QA, testing, bug triaging
  - Etc etc

SuriCon 2.0

- November 9 to 11, Washington, D.C.
- 2 days of talks, 1 day of roadmap brainstorm
- http://suricon.net


See you at the 2nd Annual
Suricata User Conference in
WASHINGTON, DC
November 9–11, 2016