CSNOG 2024

Securing networks with Suricata 7

cesnet

OISF

SURICATA

Introduction

Lukáš Šišmiš

Roles:

- Core Suricata team member
- Researcher @ CESNET
- Ph.D. student @ Brno University of Technology

in linkedin.com/in/sismis

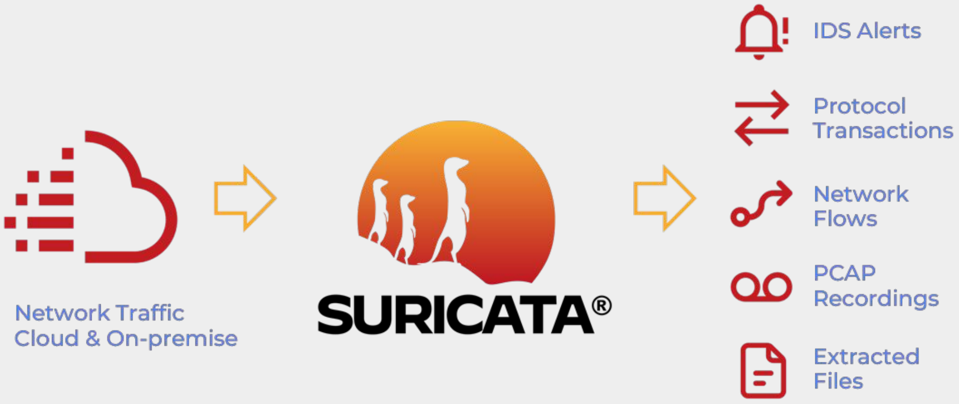
lukashino

Agenda

- Suricata overview
- What is new in 7.0

What is Suricata?

- An open-source high-performance network monitoring and security engine with active/passive monitoring, metadata logging and real-time file identification and extraction
- Produces a high-level of situational awareness and detailed application layer transaction records from network traffic.



Network Traffic
Cloud & On-premise

SURICATA®

IDS Alerts

Protocol
Transactions

Network
Flows

PCAP
Recordings

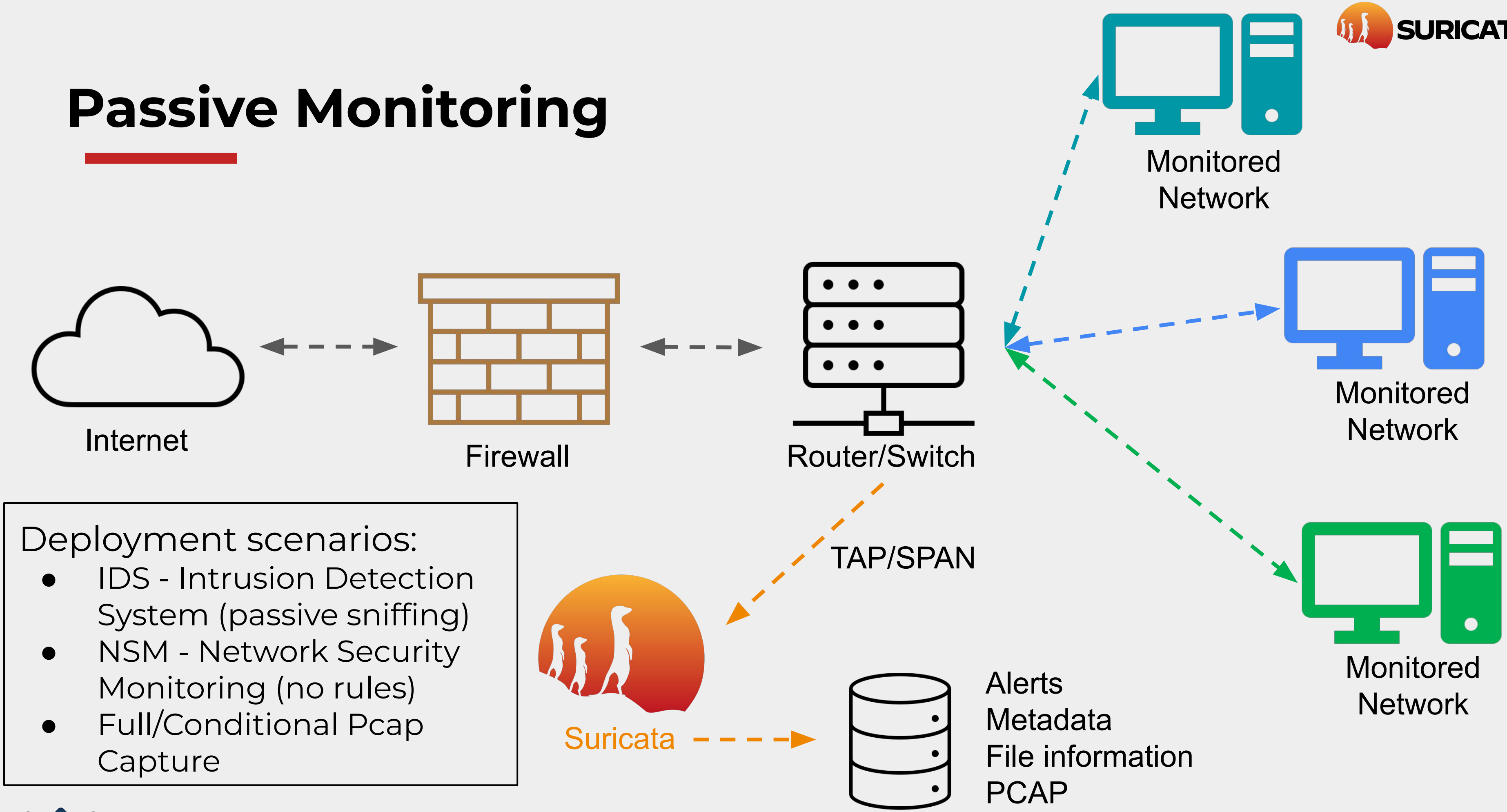
Extracted
Files

Source: Stamus Networks

What is OISF?

- US 501(c)3 non-profit organization that ensures Suricata remains world-class.
- Dedicated to preserving the integrity of open source security technologies and the communities that keep them thriving. Our team and our community includes world-class security and non-profit experts, programmers, and industry leaders dedicated to open source security technologies.
- Funding for Suricata comes from donations from world-class security organizations committed to our mission. A list of these organizations is available on our Consortium Members page.

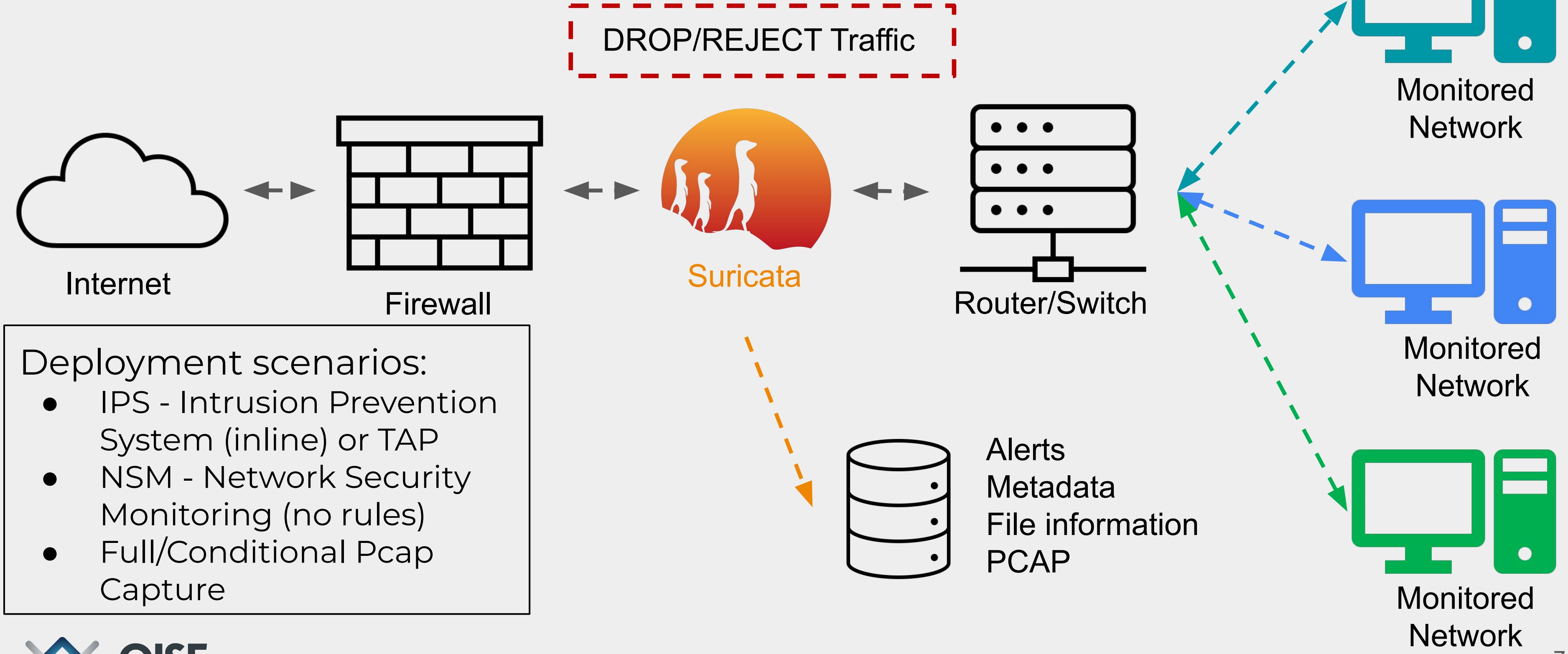
Passive Monitoring



Deployment scenarios:

- IDS - Intrusion Detection System (passive sniffing)
- NSM - Network Security Monitoring (no rules)
- Full/Conditional Pcap Capture

Active Monitoring

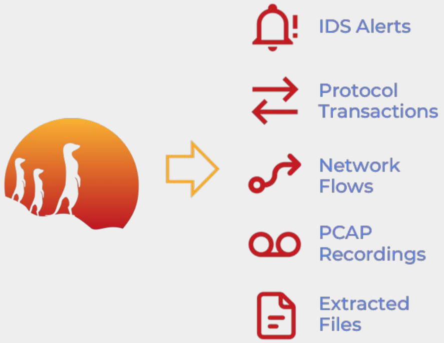


Deployment scenarios:

- IPS - Intrusion Prevention System (inline) or TAP
- NSM - Network Security Monitoring (no rules)
- Full/Conditional Pcap Capture

Suricata - Major Features

- Standards-based formats (YAML, JSON) ease integrations with SIEM tools such as Elastic and Splunk
- Multithreaded, hardware acceleration available. 100Gb+ deployments
- Network metadata and protocol logging, PCAP recording
- Advanced HTTP/2, DNS, SMTP, SMB and TLS support
- File identification and extraction - FTP/SMTP/HTTP/HTTP2/NFS/SMBv1-3
- Support for SCADA protocols - DNP3, ENIP, and CIP

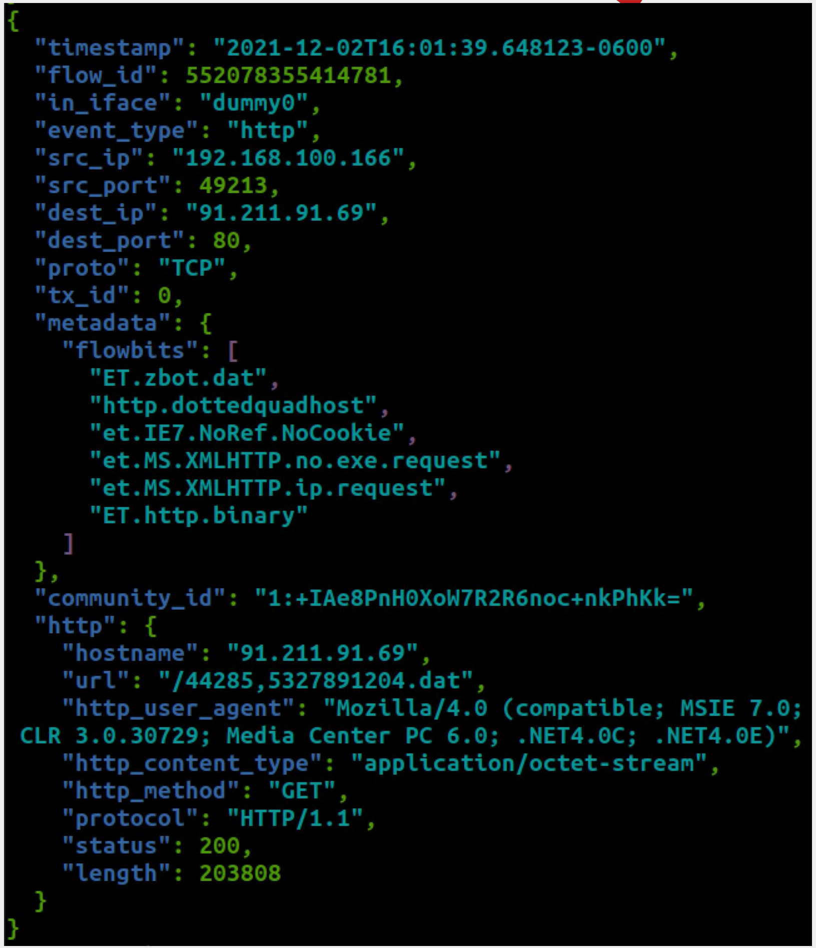


Network Metadata Logging

- Provides extensive logging of protocol and other network data

- Data logged in event records: HTTP/HTTP2, DNS, FTP, TLS, SMB, SSH, RDP, KRB5…

- Default output format in **J**ava**S**cript **O**bject **N**otation (JSON)

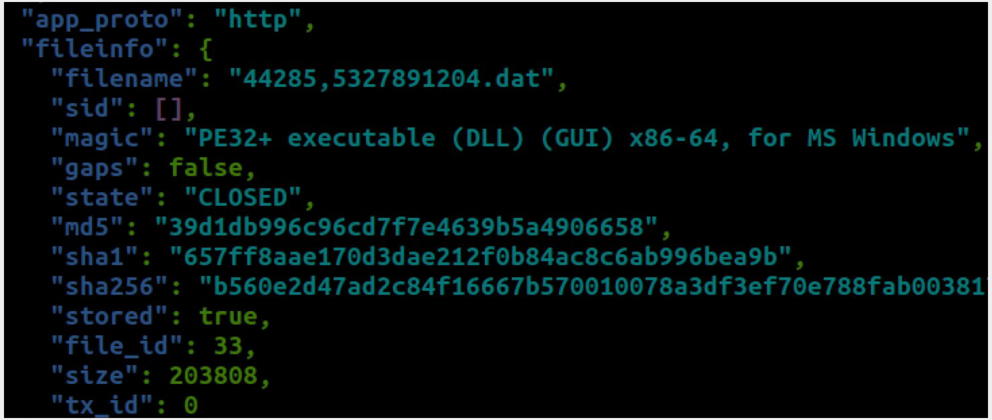


```
{
  "timestamp": "2021-12-02T16:01:39.648123-0600",
  "flow_id": 552078355414781,
  "in_iface": "dummy0",
  "event_type": "http",
  "src_ip": "192.168.100.166",
  "src_port": 49213,
  "dest_ip": "91.211.91.69",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "metadata": {
    "flowbits": [
      "ET.zbot.dat",
      "http.dottedquadhost",
      "et.IE7.NoRef.NoCookie",
      "et.MS.XMLHTTP.no.exe.request",
      "et.MS.XMLHTTP.ip.request",
      "ET.http.binary"
    ]
  },
  "community_id": "1:+IAe8PnH0XoW7R2R6noc+nkPhKk=",
  "http": {
    "hostname": "91.211.91.69",
    "url": "/44285,5327891204.dat",
    "http_user_agent": "Mozilla/4.0 (compatible; MSIE 7.0;
 CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)",
    "http_content_type": "application/octet-stream",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 203808
  }
}
```

File Identification and Extraction

- Can perform file identification and extraction in real-time

- File information includes:
    - Content type/libmagic
    - File hashes (MD5/SHA1/SHA2)
    - File size
- Files can also be extracted and stored to the file system



```
"app_proto": "http",
"fileinfo": {
  "filename": "44285,5327891204.dat",
  "sid": [],
  "magic": "PE32+ executable (DLL) (GUI) x86-64, for MS Windows",
  "gaps": false,
  "state": "CLOSED",
  "md5": "39d1db996c96cd7f7e4639b5a4906658",
  "sha1": "657ff8aae170d3dae212f0b84ac8c6ab996bea9b",
  "sha256": "b560e2d47ad2c84f16667b570010078a3df3ef70e788fab00381
  "stored": true,
  "file_id": 33,
  "size": 203808,
  "tx_id": 0
```

What's new in 7.0

- 2+ years of development
  - Total: 1375 **files changed**, 130027 insertions(+), 127626 deletions(-)
    - ⬆ **Rust**: 173 files changed, 39279 insertions(+), 13830 deletions(-)
    - ⬇ **C**: 978 files changed, 73882 insertions(+), 109446 deletions(-)
  - ⬆ **Docs**: 142 files changed, 6636 insertions(+), 1890 deletions(-)
- Community and consortium help
  - **75** contributors, non Suricata team members, donated/added code/reported and fixed bugs
- **Contribution leaderboard** - https://inliniac.net/leaderboard/7/

Organizations

- **stamus-networks.com**: 76 commits, code +8078 -2245. Tickets 19. Score 4234
- **cyber.gc.ca**: 10 commits, code +4170 -4295. Tickets 3. Score 1296
- **corelight.com**: 14 commits, code +254 -337. Tickets 6. Score 794
- **dcso.de**: 7 commits, code +1667 -1244. Tickets 0. Score 473

Top 11 individuals

1. 🥇**Eric Leblond**🥇: 119 commits, code +9035 -2496. Tickets 28. Score 6069
2. 🥈**Pierre Chifflier**🥈: 40 commits, code +5247 -5460. Tickets 0. Score 2099
3. 🥉**Modupe Falodun**🥉: 25 commits, code +540 -6775. Tickets 8. Score 1849
4. **jason taylor**: 58 commits, code +653 -349. Tickets 1. Score 1757

What's new in 7.0 - Main features

- **DPDK** IDS/IPS support for primary mode was added
- **AF_XDP** IDS support
- **NETMAP** API 14
- **Conditional PCAP** logging (can massively reduce the captured traffic size)

- **HTTP/HTTP2** new keywords for header inspection
- **TLS** client certificate logging and detection
- **Bittorrent** parser
- **EVE** documented and validated with a json schema
- **HTTP/2** support is no longer considered experimental
- **VLAN** support extended from 2 to 3 layers

- Initial **libsuricata** support

What's new in 7.0 - Performance improvements

- **file.data** MPM split per app protocol
- New lighter **rule profiling** mode
- **SMB** many fixes and optimizations
- **Hash** calculation using Rust crypto library
- **Flow manager** tuning
- Improved observability - many more performance-related **counters**
- Stream buffer, which is used by stream engine, file tracking, and more, is more **memory efficient**

What's new in 7.0 - Security/Deployment

- **Linux Landlock** support added
- Use of **setrlimit** to prevent Suricata from creating another process
- **Lock** cargo crates
- Default to **secure settings** for Datasets and Lua
- New **Security Policies**
  - https://github.com/OISF/suricata/blob/master/SECURITY.md

What's new in 7.0 - IPS

- Exception **Policies** added to better control packet handling in such conditions as memory caps being hit
- **DPDK** support

What's new in 7.0 - Rules/Detection/Protocols

- Added **new** rule **keywords** for DHCP, Kerberos, SNMP, TLS, QUIC
    - To list them : ***suricata --list-keywords=all***
- JA3(s) support for **QUIC**
- New (**experimental**) class of keywords through “frames API”: NFS, SMB, DNS, telnet, SSL/TLS
- **Lua scripting**: access to more rule info
- **QUICv1**, **GQUIC** support added.
    - GQUIC contributed
- **PostgreSQL, VN-Tag, IKEv1, ESP, Telnet** support added
- Active flow and TCP **counters**
- **flow.age** keyword was added
- **Multiple Buffer** Matching

More Resources

- Read the **Docs**: https://docs.suricata.io/en/latest/
- More Suricata **trainings/webinars**: https://suricata.io/learn/
- **Youtube**: https://www.youtube.com/@OISFSuricata/videos
- **Forums**: https://forum.suricata.io/
- **Awesome Suricata** links: https://github.com/satta/awesome-suricata
- Suricon 2024 - annual Suricata conference is happening in Madrid! https://suricon.net/

Call for Proposals Opening soon!

SURICATA

Thank you
and
visit the booth!

Website
suricata.io

Forum
forum.suricata.io

E-mail
info@oisf.net

Discord
discord.gg/t3rV2x7MrG

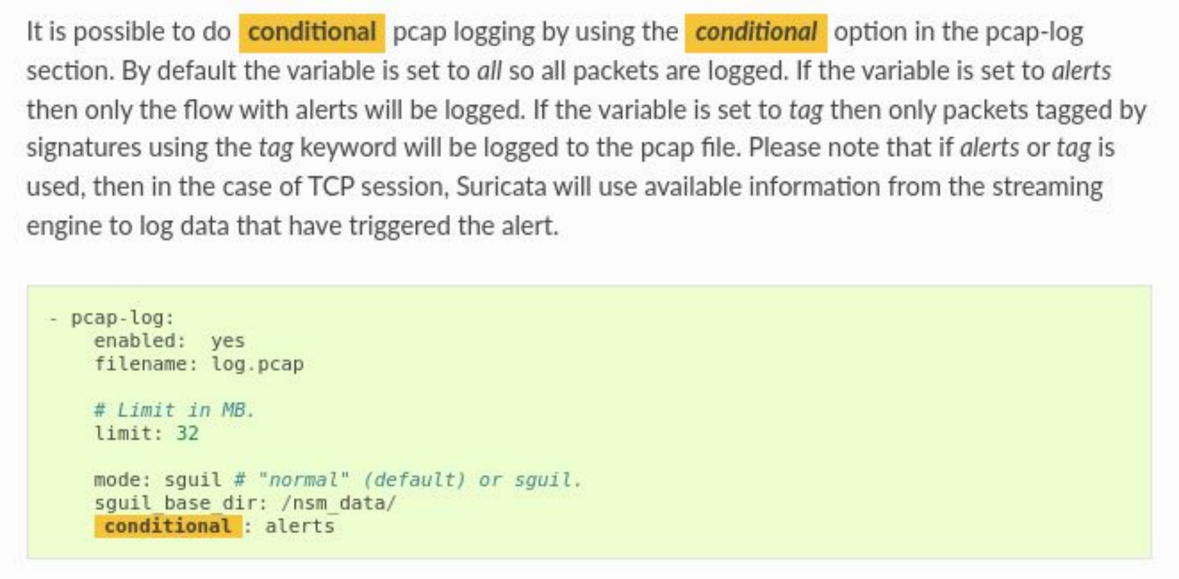
OISF cesnet

Extra slides

What's new in 7.0 - Usefulness in Deployment

Conditional pcap - record only flows that e.g. generate alerts/are tagged

- Deduplicated
  - same alert generating 100k times has the same / one pcap
    - Not 100k pcaps
- Full session pcap
- Of any alert event >
  - ***“event_type”:”alert”***



It is possible to do conditional pcap logging by using the *conditional* option in the pcap-log section. By default the variable is set to *all* so all packets are logged. If the variable is set to *alerts* then only the flow with alerts will be logged. If the variable is set to *tag* then only packets tagged by signatures using the *tag* keyword will be logged to the pcap file. Please note that if *alerts* or *tag* is used, then in the case of TCP session, Suricata will use available information from the streaming engine to log data that have triggered the alert.

```
- pcap-log:
    enabled:  yes
    filename: log.pcap

    # Limit in MB.
    limit: 32

    mode: sguil # "normal" (default) or sguil.
    sguil_base_dir: /nsm_data/
    conditional: alerts
```

©

What's new in 7.0 - Usefulness in Deployment

Conditional pcap storage savings explained
Example:

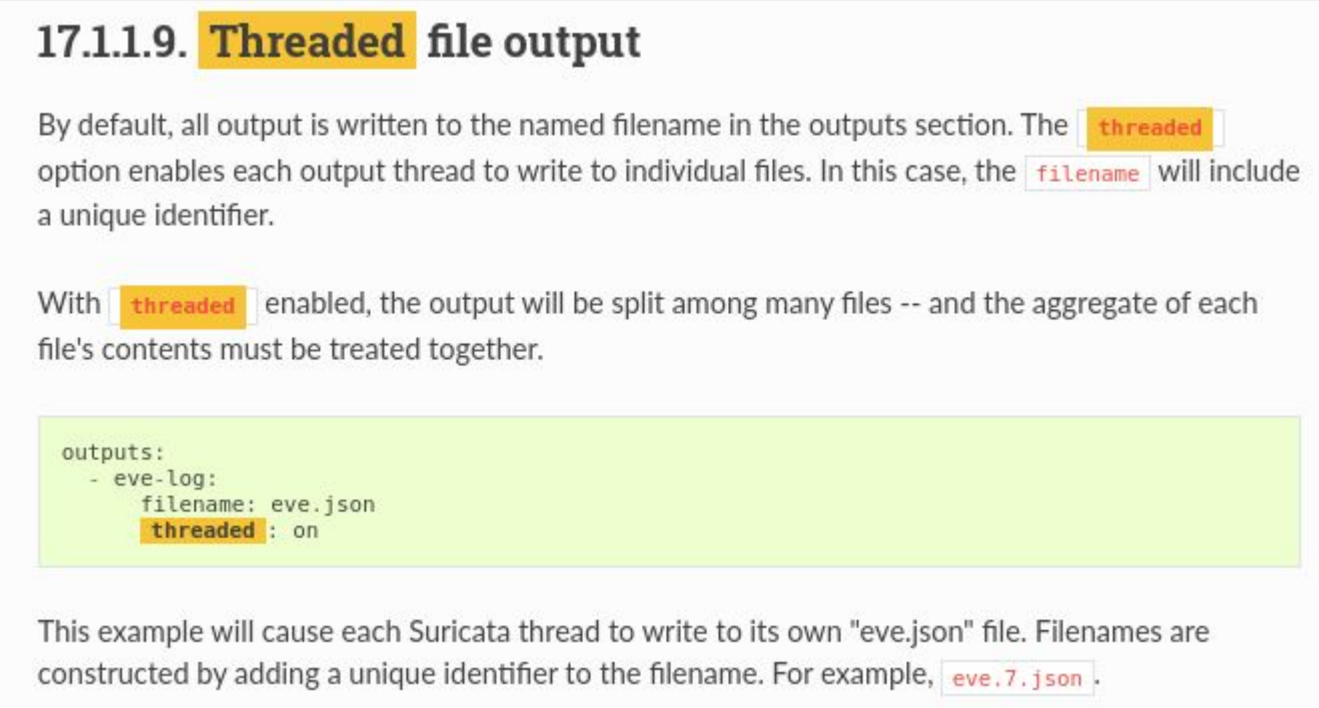
- Suricata sniffing **5Gbps traffic**
- Generating 16 million **alerts** & 500 million Suricata **protocol & flow** events
- **7 day** period
- Full packet capture **calculates** at ~369TB of space needed (not in RAID)

Conditional pcap results from an actual deployment:

- **87GB** disk usage of **deduplicated** storage
- ~0.023 % of 369TB

What's new in 7.0 - Usefulness in Deployment

- Threaded eve logging
- Improve writelock bottle neck



17.1.1.9. Threaded file output

By default, all output is written to the named filename in the outputs section. The `threaded` option enables each output thread to write to individual files. In this case, the `filename` will include a unique identifier.

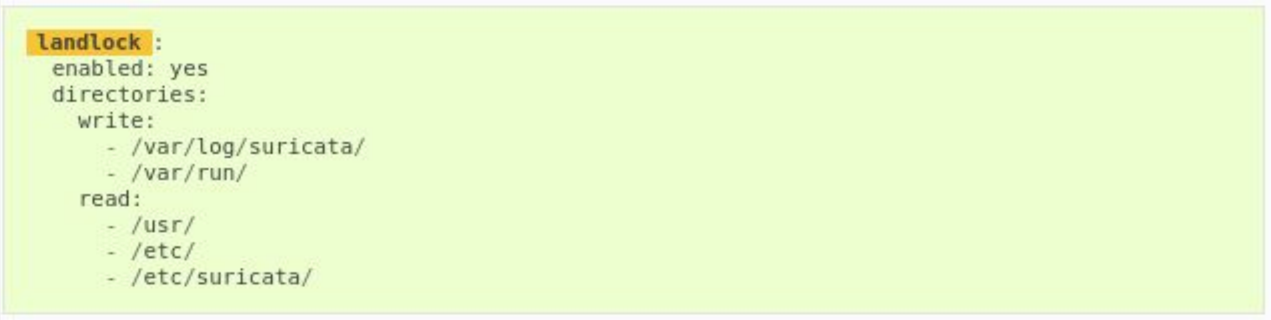
With `threaded` enabled, the output will be split among many files -- and the aggregate of each file's contents must be treated together.

```
outputs:
  - eve-log:
      filename: eve.json
      threaded: on
```

This example will cause each Suricata thread to write to its own "eve.json" file. Filenames are constructed by adding a unique identifier to the filename. For example, `eve.7.json`.

What's new in 7.0 - Supply chain protection

Landlock is a Linux **Security** Module that has been introduced in Linux 5.13. It allows an application to ***sandbox itself*** by selecting access right to directories using a **deny by default** approach.

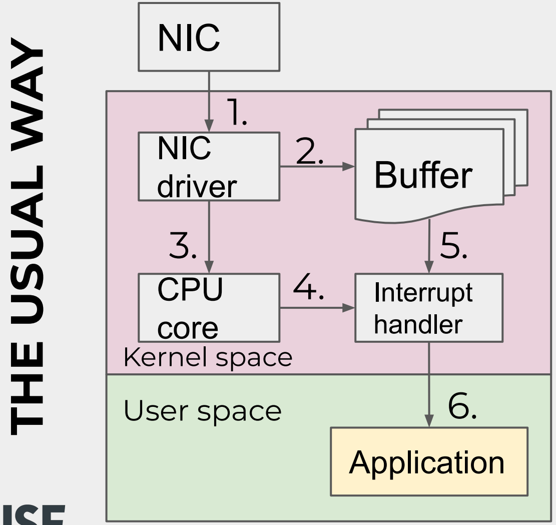


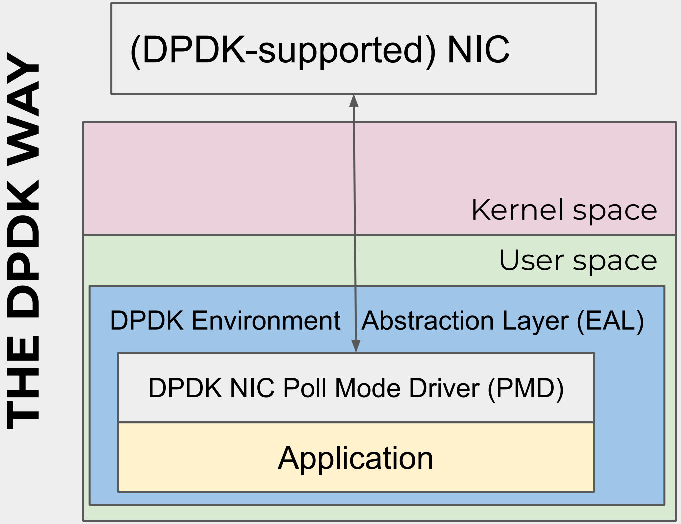
```
landlock:
  enabled: yes
  directories:
    write:
      - /var/log/suricata/
      - /var/run/
    read:
      - /usr/
      - /etc/
      - /etc/suricata/
```

https://docs.suricata.io/en/latest/configuration/landlock.html

What's new in 7.0 - Packet capture modules

- Existing AF_PACKET eBPF/XDP implementation was extended with:
  - DPDK,
  - AF_XDP (purely community contribution!).
- High-performance zero-copy capture modules **accelerate Suricata by ~15%**




THE DPDK WAY
(DPDK-supported) NIC
Kernel space
User space
DPDK Environment Abstraction Layer (EAL)
DPDK NIC Poll Mode Driver (PMD)
Application

What's new in 7.0 - Usefulness in detection

Multi buffer matching

For matching multiple headers in e.g. ***HTTP2*** traffic a rule using the new functionality would look like:

```
alert http2 any any -> any any (msg:"HTTP2 Multiple Header Buffer Example";
flow:established,to_server; http.request_header; content:"method|3a 20|GET";
http.request_header; content:"authority|3a 20|example.com"; classtype:misc-activity; sid:1;
rev:1;)
```

With HTTP2 there are **multiple** headers seen in the **same** flow record. We now have a way to write a rule in a more efficient way using the multiple buffer capability.

MBM is supported in: HTTP(2), DNS, file, TLS, IKE, KRB, MQTT, QUIC

Hint: ***suricata --list-keywords=all***

What's new in 7.0 - New keywords

(Some) new rule keywords are:

- flow.age

- tls.random_time
- tls.random_bytes
- tls.random
- tls.cert_chain_len

- dhcp.leasetime
- dhcp.rebinding_time
- dhcp.renewal_time

- quic.version
- quic.sni
- quic.ua
- quic.cyu.hash
- quic.cyu.string

- snmp.usm

- krb5.ticket_encryption

Hint: ***suricata --list-keywords=all***