# Introduction to Network Threat Detection with Suricata

With Support from:


# $ whoami

**Lukáš Šišmiš** is a core Suricata developer by day and a Ph.D. student and researcher at CESNET by night where he focuses on Suricata acceleration through DPDK.

**Socials:** I'm on LinkedIn (Lukas Sismis) and Discord (lukas#1869)

Watch this presentation locally at:
https://1url.cz/@suricata-intro-slides

# Open Information Security Foundation (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.

# Agenda

- Suricata 101
  - What is it
  - Install, config and run
  - What is suricata-update
  - Suricata logs - eve.json, jq
  - Very basic rule intro
- EveBox 101
  - Event exploration
- Hands-on
  - Alert generation check
  - Alerts and events exploration in IDS/NSM mode

# Suricata is

- An **open-source cybersecurity** tool that helps protect **computer networks** from harmful activities;
- **Monitoring network traffic**, constantly checking for any signs of attacks or threats;
- Detecting when something suspicious happens (**IDS/IPS/NSM**);
- Preventing attacks by blocking or stopping harmful network activities before they cause damage (IPS);
- Generating important forensics data for threat hunters and analyzers;
- Developed by a community of experts who constantly improve and update it for everyone to use.

# Suricata is:

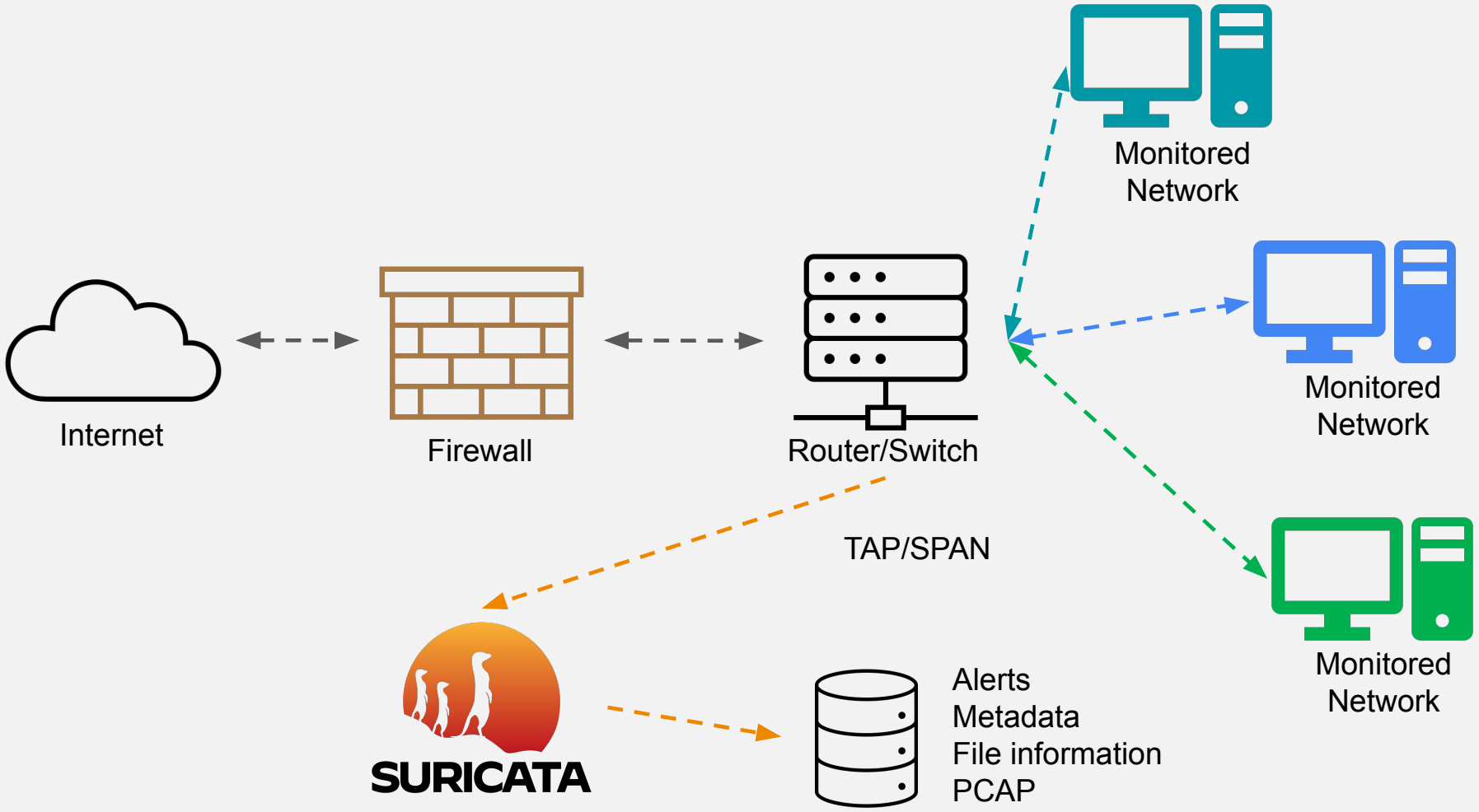
Suricata is far more than an IDS/IPS

Network Traffic
Cloud & On-premise

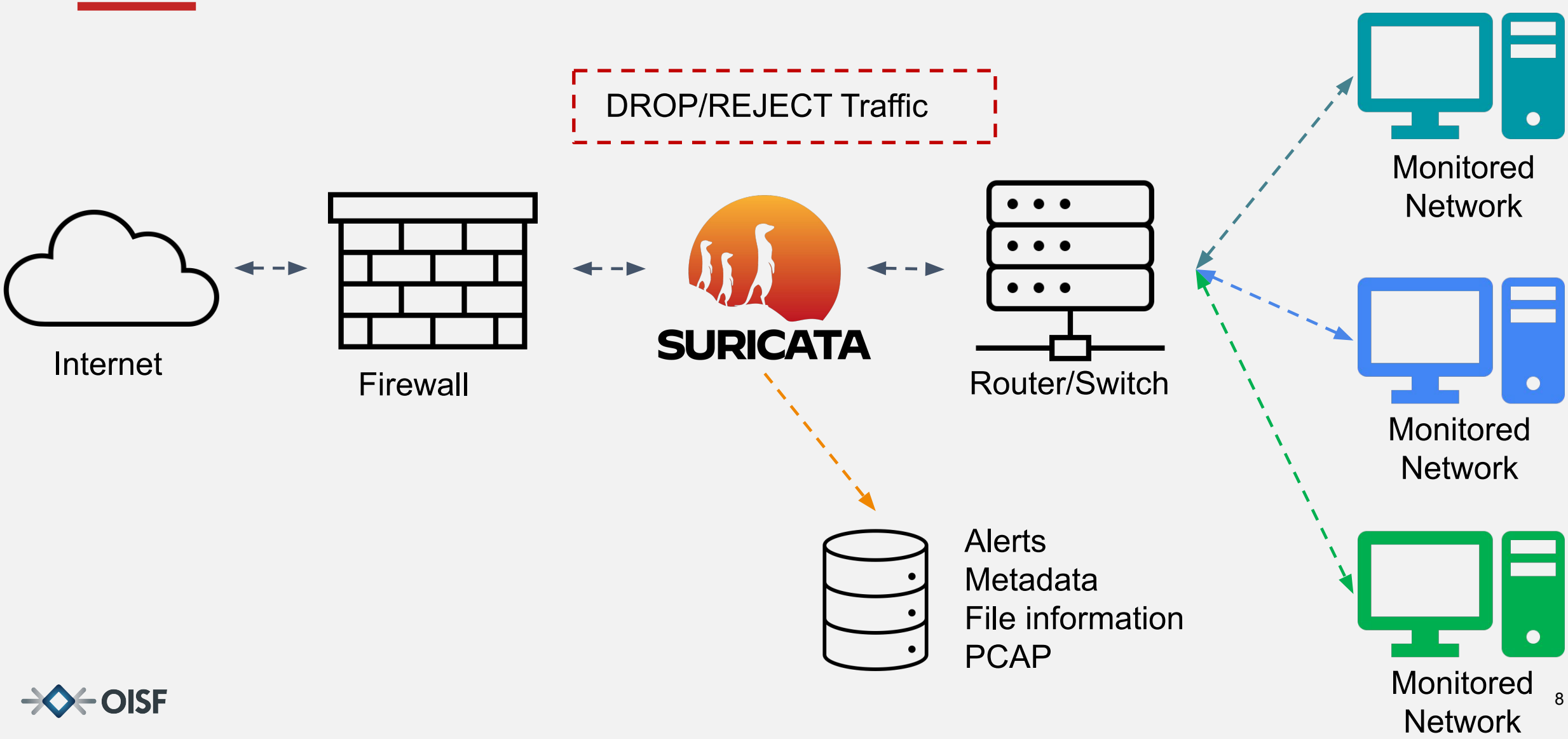

- IDS Alerts
- Protocol Transactions
- Network Flows
- PCAP Recordings
- Extracted Files

Source: Stamus Networks

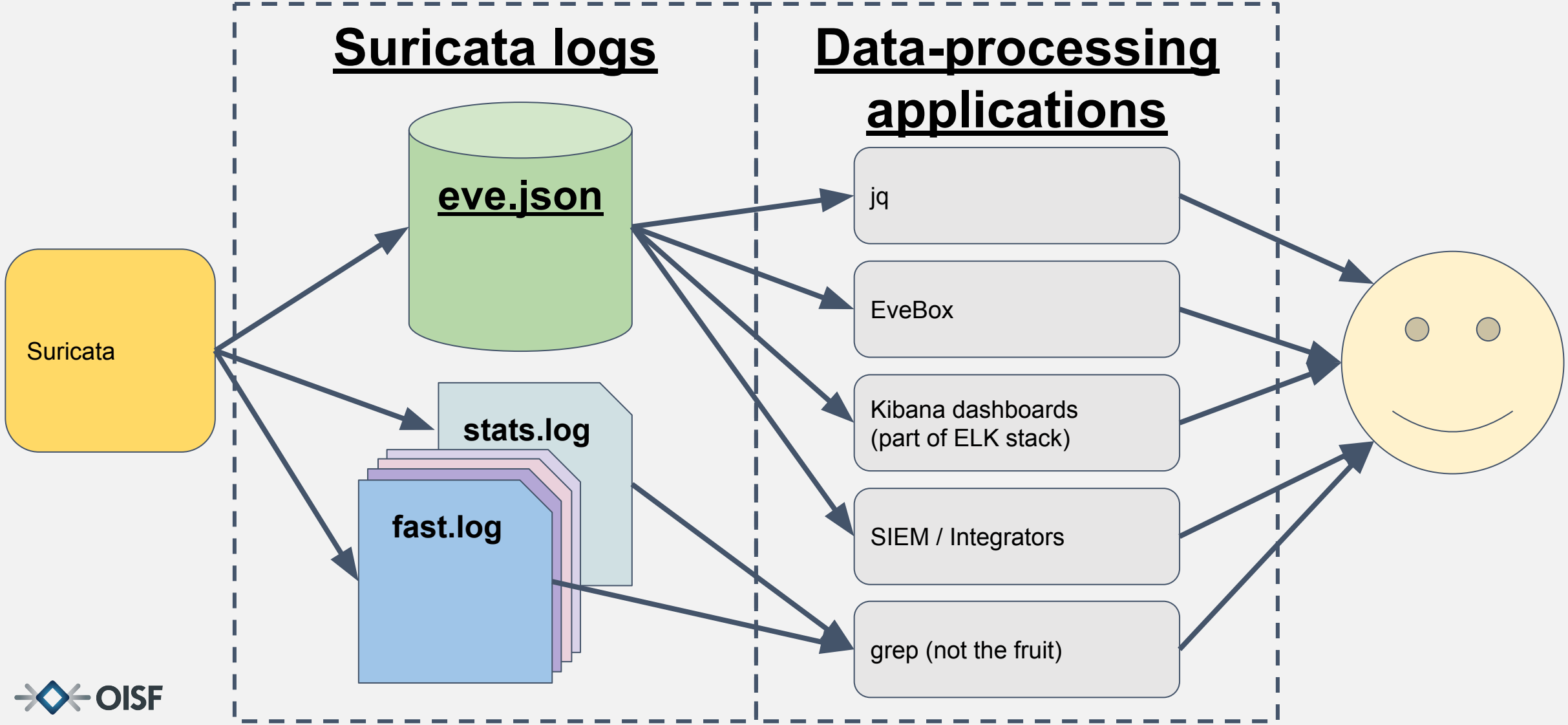
# Network monitoring



# Active Monitoring (IPS)



# Interpreting Suricata outputs



# Warm up

- Suricata... rules!
  - alert http any any -> any any (http.user_agent; content:"python"; sid: 1;)

    Action - what happens when the rule matches

    Header - protocol, IP addresses and ports, and traffic direction

    Options - rule specifics - traffic content, flow state, buffer size…

- Important config step:
  - Rule variables: EXTERNAL_NET and HOME_NET IP
    - suricata.yaml -> vars
  - Useful setting: alert.printable-payload:yes
  - Tricky configuration options: -k none

# Warm up - explore malware

- Email attachment verification
  - https://app.any.run/tasks/4d78bf9f-8df9-446a-8935-4d14526ee3bf

- FTP Data Exfiltration
  - https://app.any.run/tasks/aa36e5bf-1b36-4287-bd4c-a6cd32e010fb
  - Virustotal
  - Suricata + Evebox exploration
- More PCAP sources:
  - https://www.youtube.com/watch?v=4n8B9NxbWAE

# Hands-on time

Or - what cybersecurity exercises / SOC analyst life can look like.

# Get ready...

You can get Suricata as:

- Binary from the package archives together with
  Evebox: https://evebox.org/ <- (very lightweight, anyone can run it)
  or
  ELK stack <- (scales well, suitable for larger production environments)
- Pre-packaged environment e.g. SELKS (Docker/virtual machine)
  https://github.com/StamusNetworks/SELKS/wiki
- Compile (and customize) it yourself

# Steady...

Running natively (Ubuntu 22.04)

- sudo apt-get install curl
- curl -fsSL https://evebox.org/files/GPG-KEY-evebox -o /etc/apt/keyrings/evebox.asc
- echo "deb [signed-by=/etc/apt/keyrings/evebox.asc] https://evebox.org/files/debian stable main" | sudo tee /etc/apt/sources.list.d/evebox.list
- sudo apt-get update
- sudo apt-get install evebox

- sudo add-apt-repository ppa:oisf/suricata-stable
- sudo apt-get update
- sudo apt-get install suricata
- sudo suricata-update

# Commands overview

- `suricata-update`
- `rm -f /var/log/suricata/eve.json && \`
  `suricata \`
  `-k none \`
  `-c /etc/suricata/suricata.yaml \`
  `-S /var/lib/suricata/rules/suricata.rules \`
  `-l /var/log/suricata/ \`
  `-r path/and/name-of-your-file.pcap`

→ Let's clean up a bit

→ Disable checksum checks
→ Suricata configuration file
→ Use this rules file (remember suricata-update?)
→ Logging directory (eve.json, etc.)
→ Examined PCAP

- `evebox oneshot /var/log/suricata/eve.json`

→ Run Evebox as process (not as a daemon) and read that JSON file from Suricata's logging directory

# GO!

- Goal 1: Run Suricata with the PCAP and rules
- Goal 2: Explore different Suricata events such as
  - Alerts,
  - Application layer protocol records,
  - Flow records, Per-IP events,
  - Anomalies
- Goal 3: Try to answer
  - Summary of Pcap Activities (what steps is malware doing, how it is acting on the network, etc.)
  - Details (of the infected Windows host)
  - Indicators of Compromise (IOCs)
  - Tactics, Techniques, Procedures (TTPs)

# Spoonwatch - Malware Traffic Analysis Quiz

- You've got a reported incident and you only have a short captured session
- To help fill out an incident report, answer these questions:
  - When did the malicious traffic start in UTC?
  - What is the victim's IP address?
  - What is the victim's Windows host name?
  - What is the victim's Windows user account name?
  - What type of attack was this, what happened?

https://www.malware-traffic-analysis.net/2022/01/07/index.html

SpoonWatch ZIP in (password: **infected** )
https://drive.google.com/drive/folders/1s9EziaImQ7dGu9V1bocLtSo1MwD6JNpT?usp=drive_link

# Exercises

- PCAPs and files stored in:
  - https://drive.google.com/drive/folders/1s9EziaImQ7dGu9V1bocLtSo1MwD6JNpT?usp=drive_link

- Short URL: https://1url.cz/@suricata-intro-materials

# Exercises - running natively

- Elevate to sudo and run Suricata-update
  - `sudo su`
  - `suricata-update`
- You let Suricata inspect the PCAP:
  - 
```
rm -f /var/log/suricata/eve.json && \
suricata \
-k none \
-c /etc/suricata/suricata.yaml \
-S /var/lib/suricata/rules/suricata.rules \
-l /var/log/suricata/ \
-r 2022-01-07-traffic-analysis-exercise.pcap
```
- You view the results in the Evebox
  - `evebox oneshot /var/log/suricata/eve.json`

only touch this part

# Exercises running on DOCKER

- You let Suricata inspect the PCAP:
  - 
```
PCAP_PATH=~/Downloads/HTTP.pcap && \
rm -f $(pwd)/{pcap,logs}/* && \
cp "$PCAP_PATH" "$(pwd)/pcap/" && \
sudo docker run --rm -v "$(pwd)/pcap:/pcap:ro" \
-v "$(pwd)/rules:/rules:ro" -v "$(pwd)/etc:/etc/suricata:ro" \
-v "$(pwd)/logs:/var/log/suricata" \
jasonish/suricata:latest suricata -r /pcap/* -l /var/log/suricata
\
-S /rules/suricata.rules -c /etc/suricata/suricata.yaml && \
sudo docker run --rm -v "$(pwd)/logs:/var/log/suricata:ro" -p
5636:5636 \
jasonish/evebox:latest evebox oneshot --host 0.0.0.0 \
/var/log/suricata/eve.json
```

only touch this part

# Something you want to see (Evebox is running)

```
2025-06-13T19:48:48Z  INFO evebox::sqlite::connection: Removing obsolete index events_src_ip_index
2025-06-13T19:48:48Z  INFO evebox::sqlite::connection: Removing obsolete index events_dest_ip_index
2025-06-13T19:48:48Z  INFO evebox::sqlite::connection: Removing obsolete index events_event_type_archived
2025-06-13T19:48:48Z  INFO evebox::sqlite::connection: Removing obsolete index events_escalated_view_index
2025-06-13T19:48:48Z  INFO evebox::sqlite::connection: Updating SQLite indexes
2025-06-13T19:48:48Z  INFO evebox::sqlite::connection: Enabling FTS
2025-06-13T19:48:49Z  INFO evebox::sqlite::connection: Rusqlite connection: journal_mode=wal
2025-06-13T19:48:49Z  INFO evebox::sqlite::connection: Rusqlite connection: synchronous=1
2025-06-13T19:48:49Z  INFO evebox::sqlite::connection: Rusqlite connection: auto_vacuum=1
2025-06-13T19:48:49Z  INFO evebox::cli::oneshot: Reading /var/log/suricata/eve.json (7653 bytes)
2025-06-13T19:48:49Z  INFO evebox::cli::oneshot: /var/log/suricata/eve.json: 1 events (100%)
2025-06-13T19:48:49Z  INFO evebox::cli::oneshot: Read 1 events in 0.003747583s
2025-06-13T19:48:49Z  INFO evebox::sqlite::configdb: Opening configuration database :memory:
2025-06-13T19:48:49Z  INFO evebox::cli::oneshot: Server started at http://0.0.0.0:5636
2025-06-13T19:48:49Z ERROR evebox::cli::oneshot: Failed to open http://0.0.0.0:5636 in browser: No valid browsers detect
ed. You can specify one in BROWSER environment variable
2025-06-13T19:48:49Z  INFO evebox::cli::oneshot: If your browser didn't open, try connecting to http://127.0.0.1:5636
```

# Spoonwatch - Malware Traffic Analysis Quiz

- You've got a reported incident and you only have a short captured session
- To help fill out an incident report, answer these questions:
  - When did the malicious traffic start in UTC? -> 2022-01-07 at approximately 16:07
  - What is the victim's IP address? -> 192.168.1.216
  - What is the victim's Windows host name? -> DESKTOP-GXMYNO2
  - What is the victim's Windows user account name? -> steve.smith
  - What type of attack was this, what happened?
  - File executables download

# For the next exercises, edit suricata.yaml

```
types:
  - alert:
      payload: yes              # enable dumping payload in Base64
      payload-buffer-size: 100kb # max size of payload buffer to output in eve-log
      payload-printable: yes    # enable dumping payload in printable (lossy) format
      # packet: yes               # enable dumping of packet (without stream segments)
```

# Exercise - Agent Tesla

- PCAP:
  - 2023-09-21-AgentTesla-traffic-expertsconsultgh.co.pcap
- Your task is to answer the following report:
  - What are the victim's and attacker's IP addresses?
  - Determine what is happening in the PCAP
  - What alerts/events did you consider the most revealing?
  - List your found Indicators of Compromise and Tactics, Techniques, Procedures
    - what is easily changeable is IoC only (e.g. domain name), what is a more algorithmic approach and can be used in the future detections (possibly an IP lookup)

# Exercise - Agent Tesla

- What are the victim's and attacker's IP addresses?
  - Victim: 10.10.25.101
  - Attacker: 173.254.28.237
- Determine what is happening in the PCAP
  - Getting the public IP - to know what I infiltrated and where I am.
  - Sending the email
  - Email contains credentials and machine info
- What alerts/events did you consider the most revealing?
  - ALERT: ET MALWARE AgentTesla Exfil Via SMTP

# Exercise - Agent Tesla

- List your found Indicators of Compromise and Tactics, Techniques, Procedures
  - IoCs:
    - ledcenter.by
  - TTPs:
    - ALERT: ET INFO External IP Address Lookup Domain (ipify .org) in TLS SNI
    - ALERT: ET INFO External IP Lookup Domain (ipify .org) in DNS Lookup
    - Email
    - Agent Tesla Alert

# Exercise - Powershell in da house

- PCAP:
  - 1cbca783-8323-474e-aa6a-ca655ed6637e.pcap
- Your task is to answer the following report:
  - What are the victim's and attacker's IP addresses?
  - Determine what is happening in the PCAP
  - What alerts/events did you consider the most revealing?
  - List your found Indicators of Compromise (IoCs) and Tactics, Techniques, Procedures (TTPs).

Hint what to also use:

CyberChef - From Base64

https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)

# Exercise - Powershell in da house

- What are the victim's and attacker's IP addresses?
  - Victim: 192.168.100.126
  - Attacker: 154.30.255.3
- Determine what is happening in the PCAP
  - Download from sites which have deployed known TLS certs
  - Powershell code infiltration
- What alerts/events did you consider the most revealing?
  - ALERT: ET ATTACK_RESPONSE PowerShell Base64 Encoded Content Command Common In Powershell Stagers M2

# Exercise - Powershell in da house

- List your found Indicators of Compromise and Tactics, Techniques, Procedures
  - IoCs:
    - certificates
    - domain name
  - TTPs:
    - powershell download from an unknown site

# Exercise - Powershell in da house - extra

- What is hidden deep behind layers of encoding:
  - Cyberchef
- Enable file-store to capture the full-length original file
  - https://docs.suricata.io/en/latest/file-extraction/file-extraction.html
  - file-store section - enable and set size to 0 (unlimited)
  - `grep -R  "Obfuscated using" logs/filestore/ # find file`
  - Happy deobfuscation!
- Detonator at:
  - https://app.any.run/tasks/1cbca783-8323-474e-aa6a-ca655ed6637e/

# Exercise - Powershell in da house - extra

- Various level of obfuscation including base64 variants - base64:
  - directly in the string
  - in the variables
  - in two variables
  - in two concatenated strings
- 10+ layers of various obfuscation

# Exercises & other good stuff

- Malware exercises - https://www.malware-traffic-analysis.net/training-exercises.html
- Unit42 exercises - https://unit42.paloaltonetworks.com/category/tutorial/
- Suricata YT channel: https://www.youtube.com/@OISFSuricata/
- Google CyberSecurity Certificate: https://grow.google/certificates/cybersecurity/
- Josh Stroschein YT channel - https://www.youtube.com/@jstrosch
- SuriCons - https://suricon.net/archives-2/
- Awesome lists:
  - PCAP tools - https://github.com/caesar0301/awesome-pcaptools
  - Suricata list - https://github.com/satta/awesome-suricata
- Contact info@oisf.net to get your custom training!

# Come meet us at SuriCon 2025!

- Montreal, Canada
- November 19 - 21
- Pre-conference trainings @ https://suricon.net/trainings/
  - Rule Writing for Suricata (new)
  - Advanced threat hunting
  - Advanced deployment


https://suricon.net/

# Conclusion

- Understanding Suricata
  - You know what is Suricata and where to deploy it
- Data and Event Analysis
  - You gained insights into the different types of data Suricata produces
- Hands-on Experience
  - Updated rules,
  - Investigated incidents, IoCs, TTPs,

- We are excited to see you at Suricon in Montreal!

OISF

SURICATA

# Thank you for watching our presentation!

Website

**suricata.io**

Forum

**forum.suricata.io**

E-mail

**info@oisf.net**

Discord

**discord.gg/t3rV2x7MrG**

OISF