Exploring Suricata, an available ntopng integration

proofpoint.

Genina Po
Isaac Shaughnessy
Collin Caves

Goal of this session

proofpoint.

- Promote ntopng's Suricata Integration
- Introduce ntop community to Emerging Threats community
- Provide Suricata Rule Development Training
- Guidance on how to submit rules and feedback to Emerging Threats

Should leave with a …

- Curiosity to use ntopng's Suricata Integration
- Familiarity with Emerging Threats community
- Ability to see intent behind Suricata rules
- Yearn to submit rules and feedback to Emerging Threats

Did You Know?

- ntopng 3.9+ is capable of ingesting Suricata flow metadata and alerts.

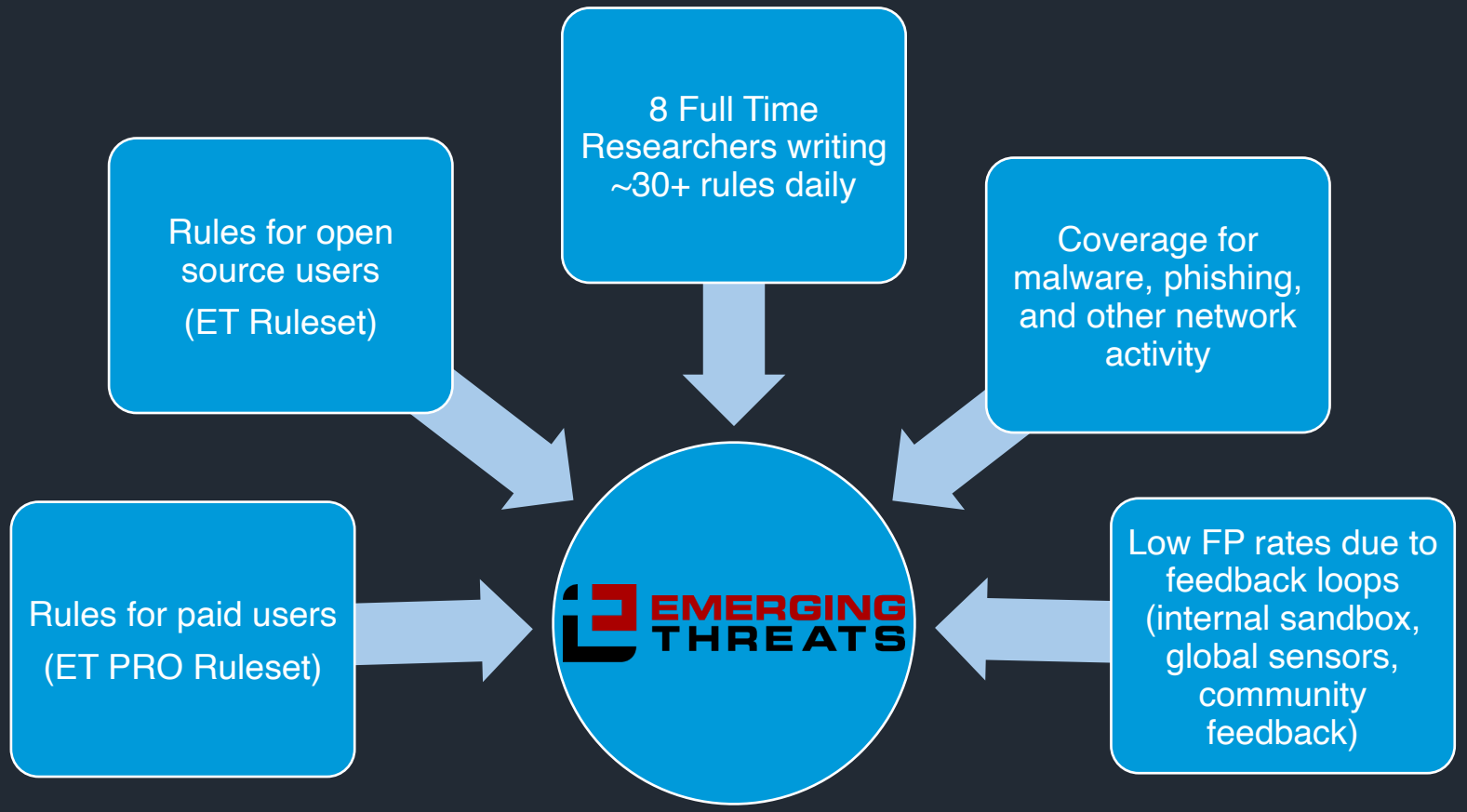
Application	Alert	Flow	Information
TCP:TLS DPI	External Alert	desktop-ys6fz2g:54805 ⇄ 207.246.77.75 :2222	Detected JA3 alert: Hash - [Abuse.ch] Possible Dridex [Emerging Threats]
TCP:TLS DPI	External Alert	desktop-ys6fz2g:54818 ⇄ 207.246.77.75 :2222	Detected JA3 alert: Hash - [Abuse.ch] Possible Dridex [Emerging Threats]
TCP:TLS DPI	App. on Non-Std Port	desktop-ys6fz2g:54805 ⇄ 207.246.77.75 :2222	App. on Non-Std Port
TCP:TLS DPI	App. on Non-Std Port	desktop-ys6fz2g:54818 ⇄ 207.246.77.75 :2222	App. on Non-Std Port
	External Alert	desktop-niee9lp:54695 ⇄ hadevatjulps.com :80	Detected MALWARE alert: Tordal/Hancitor/Chanitor Checkin [Emerging Threats]
	HTTP Suspicious User-Agent	desktop-niee9lp:59664 ⇄ hadevatjulps.com :80	HTTP Suspicious User-Agent [Empty or missing User-Agent]

proofpoint.

Who Creates Suricata Rules?

- Suricata alerts are generated from Suricata rules.
- Suricata rules are created by individuals and threat researcher groups.

About Proofpoint's Emerging Threats



Genina Po

- Threat Researcher at Emerging Threats
- Developing Internal Python Tools to Network Detection Research
- Interested in Malware, Phishing, and Martial Arts
- Contact on Keybase >> @bingohotdog

Isaac Shaughnessy

- Threat Detection Engineer at Emerging Threats
- IDS Signature Development
- Honeypot Development

Collin Caves

- Independent Security Researcher
- ET OPEN Community submitter for about 2 years
- 7 years of Cyber Security
- Loves dogs


SURICATA

What is Suricata?

- Three Operational modes (IDS/IPS/NSM)
- Rules detect and profile anomalous traffic.
- Sensor sits at network perimeter (usually)
- Used in security vendors use it (e.g. Corelight)

Detection Tools Similar to Suricata

How Do We Create Rules?

Rule Development Life Cycle

HUNTING

WRITING SIGNATURES

PERFORMANCE TESTING

FEEDBACK FROM COMMUNITY

RULE DEVELOPMENT LIFECYCLE

HUNTING

“Over 80,000 exploitable Hikvision cameras exposed online” - BleepingComputer

CVE PUBLISHED: September 9, 2021

CVE-2021-36260

RULE DEVELOPMENT LIFECYCLE

WRITING SIGNATURES

“Get Started” Pack

- Traffic PCAP and Wireshark
- Text Editor
- Suricata
- Dalton

Suricata MALWARE Rule, First Glance

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Win32/Shuckworm CnC Exfil M1";
flow:established,to_server; http.uri; content:"/baby.php"; startswith; content:"/baby";
endswith; http.user_agent; content:"Mozilla/5.0 (Windows NT 10.0)"; startswith; content:"
::/.beagle/."; endswith; fast_pattern; reference:url,symantec-enterprise-blogs.security.com/
blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine; classtype:trojan-activity; sid
:2036291; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, created_at 2022_04_21, deployment Perimeter, former_category
MALWARE, malware_family Gamaredon, signature_severity Major, updated_at 2022_04_21;)
```

Suricata MALWARE Rule, Break Down

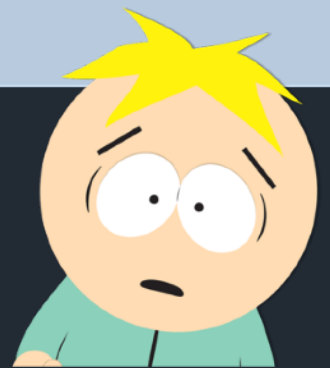
```
#Rule Action
alert

# Rule Header - defines the protocol, IP addresses, source, and destination
http $HOME_NET any -> $EXTERNAL_NET any

# Rule Options - rule specifics!
(msg:"ET MALWARE Win32/Shuckworm CnC Exfil M1";
flow:established,to_server;
http.uri; content:"/baby.php"; startswith; content:"/baby"; endswith;
http.user_agent; content:"Mozilla/5.0 (Windows NT 10.0)"; startswith;
content:"::/.beagle/."; endswith; fast_pattern;
reference:url,symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine;
classtype:trojan-activity;
sid:2036291;
rev:3;)
```

Sticky Buffers

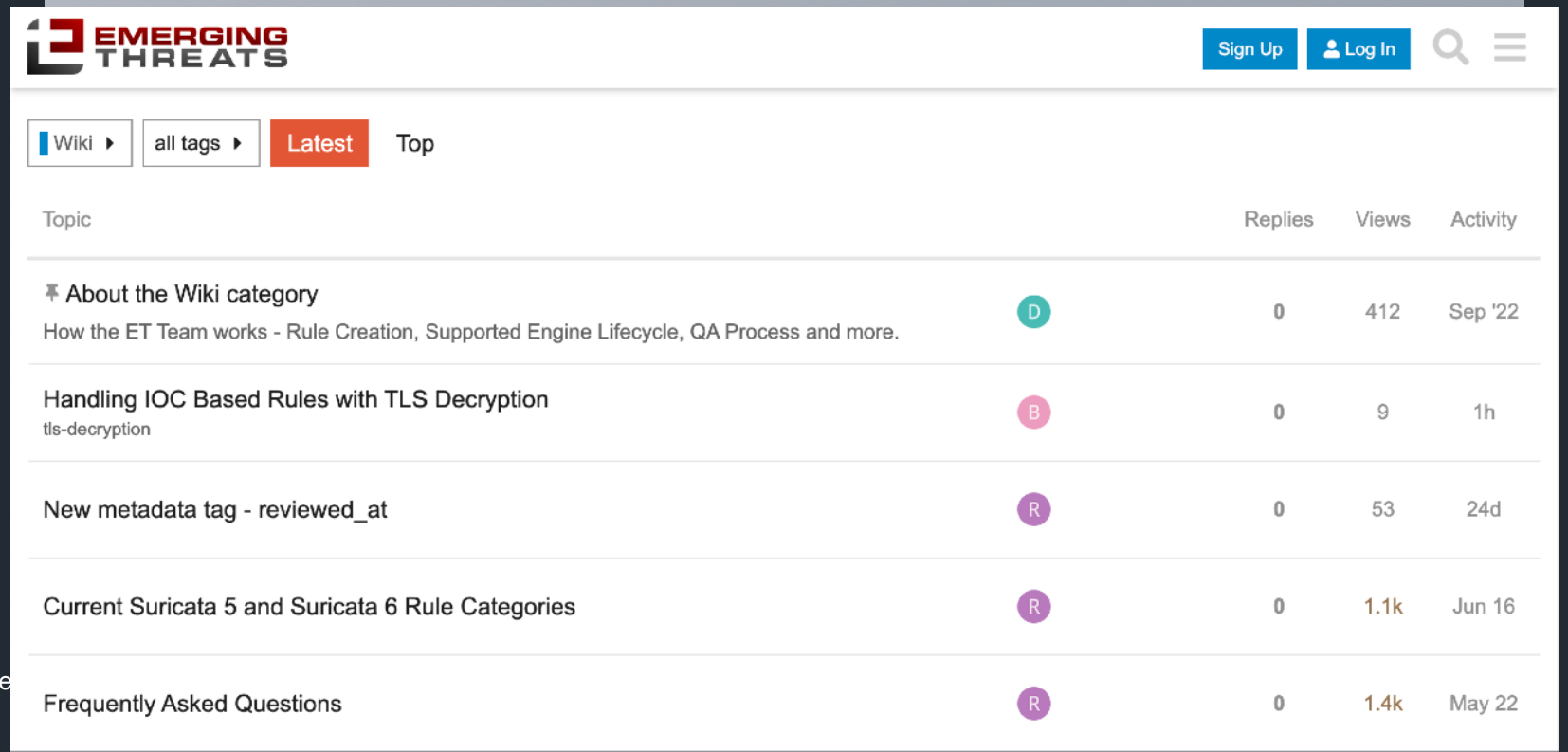
http.method;	content:"GET";
http.uri;	content:"malware.ps1"
http.user_agent;	content:"WindowsPowerShell/”



Metadata

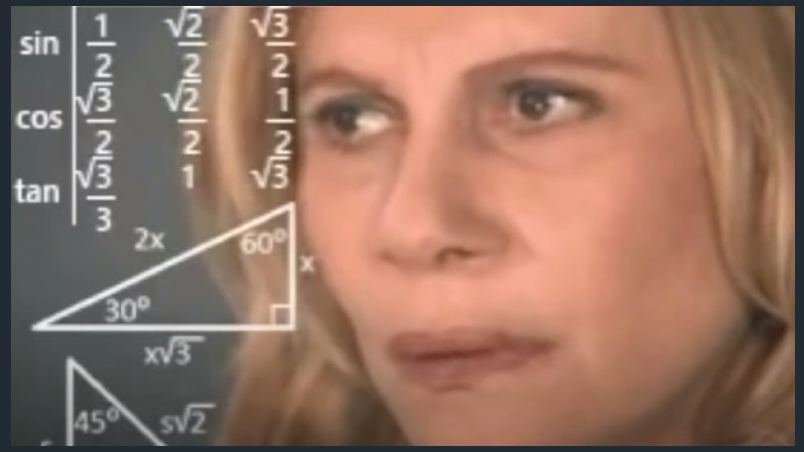
- Metadata provides user friendly into about rule's intent.
- Need more info on metadata, categories, classtypes, and etc? [Go to Emerging Threats Discourse and Wiki]

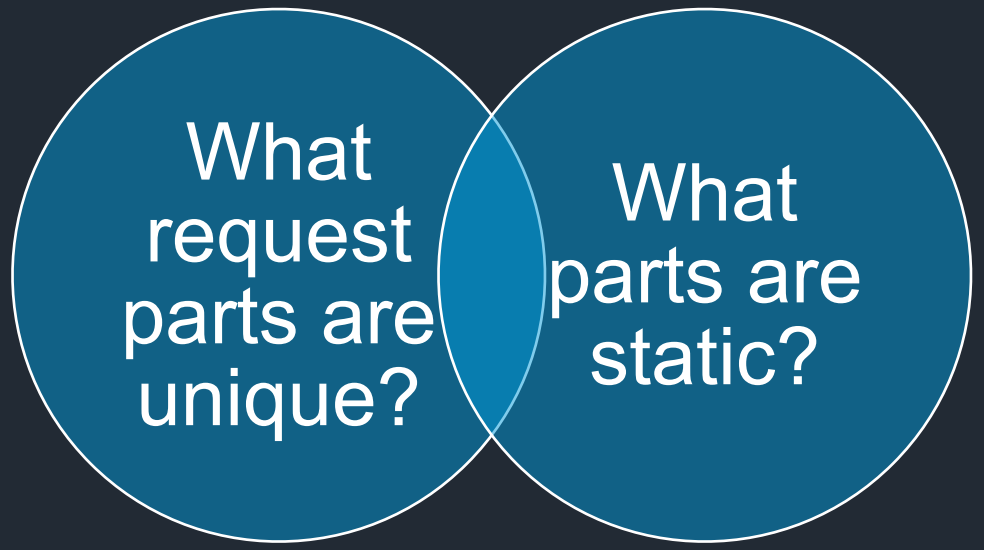
```
classtype:trojan-activity;
reference:url,symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint,
created_at 2022_04_21,
deployment Perimeter,
malware_family Gamaredon
signature_severity Major
updated_at 2022_04_21;)
```



Exercise: Thinking Like a Rule Writer

```
1 2 3
POST / HTTP/1.0
4 Host: zochao.com:2351
5 Keep-Alive: 300
6 Connection: keep-alive
7 User-Agent: Mozilla/4.0 (compatible; Synapse)
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 51
10 11                                          12 13   14 15
id=cGFGDBCDahEHAAEHHehDcaHDAacFACCF&data=_&act=1344
```





MALWARE Rule for DarkGate Activity

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Darkgate Stealer CnC Checkin"; flow:established,to_server;
    http.start; content:"POST / HTTP/1.0|0d 0a|Host|3a 20|"; startswith; fast_pattern; http.user_agent; bsize:33; content:
    "Mozilla/4.0 (compatible|3b 20|Synapse)"; http.request_body; content:"id="; startswith; content:"&data="; distance
    :32; within:6; content:"&act="; isdataat:!5,relative; reference:md5,23a45a5658dc1989c54f5bd9139c007a; reference
    :url,www.aon.com/cyber-solutions/aon_cyber_labs/darkgate-keylogger-analysis-masterofnone/; reference
    :md5,793c0217717b0a37794f7c3adbeda577; classtype:command-and-control; sid:2048089; rev:2; metadata:affected_product
    Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_05_28, deployment Perimeter,
    former_category MALWARE, malware_family DarkGate, performance_impact Low, confidence High, signature_severity Major,
    updated_at 2023_09_14, reviewed_at 2023_09_14, former_sid 2842772; target:src_ip;)
```

RULE DEVELOPMENT LIFECYCLE

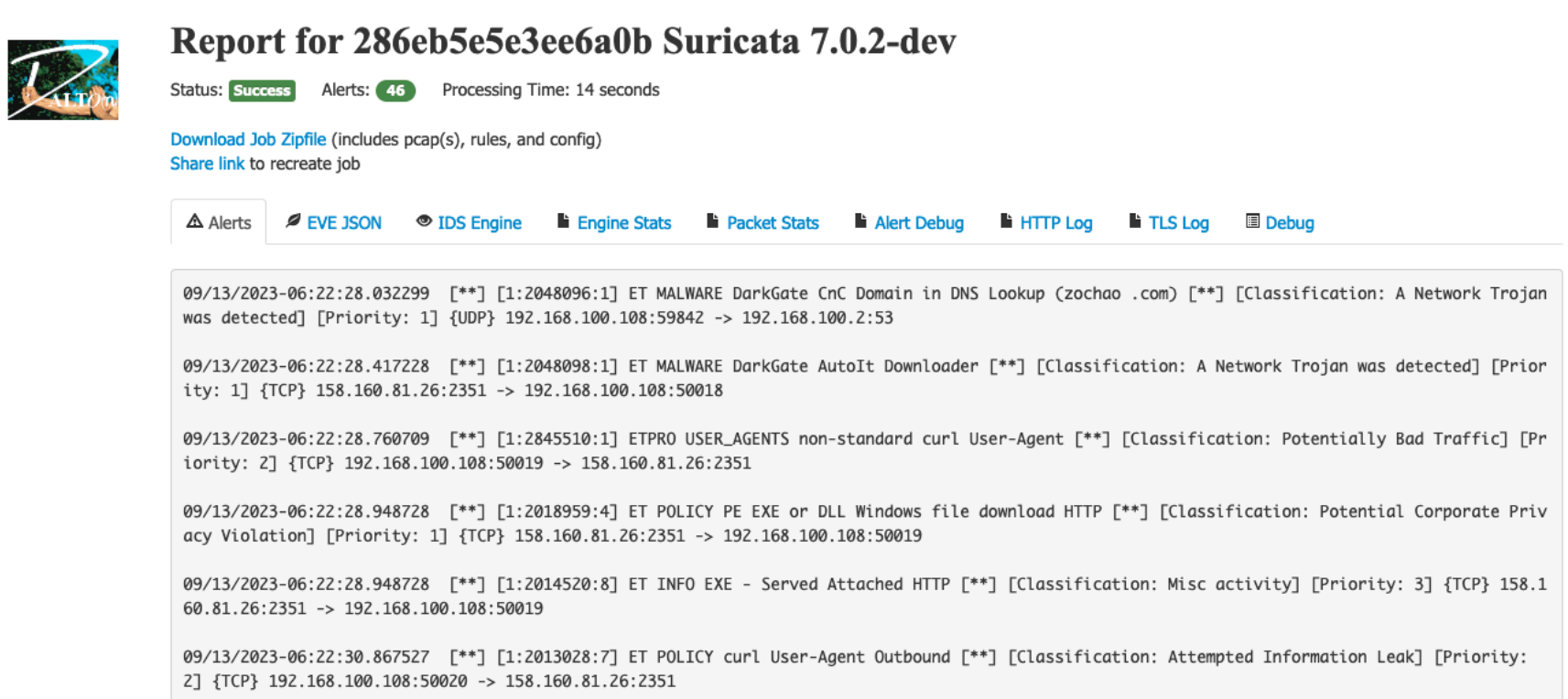
PERFORMANCE TESTING

DALTON – SURICATA PERFORMANCE TESTING TOOL

- What is Dalton?
  - Easily run PCAPs against IDS sensors of your choice for quick feedback
- More in depth presentation of Dalton
  - Detection Engineering with Dalton
- How to get it via Secureworks' Dalton?
  - Dalton - Suricata and Snort IDS rule and Pcap Testing System

Why Use Dalton?

- Simple and responsive
- Web Service though Docker
- Made open source by Dell SecureWorks
- Supports Snort, Zeek, and Suricata



...Wait, why is it called Dalton?

Frequently Asked Questions

1. **Why is it named 'Dalton'?**
   Dalton is the name of Patrick Swayze's character in the movie "Road House".

Demo –

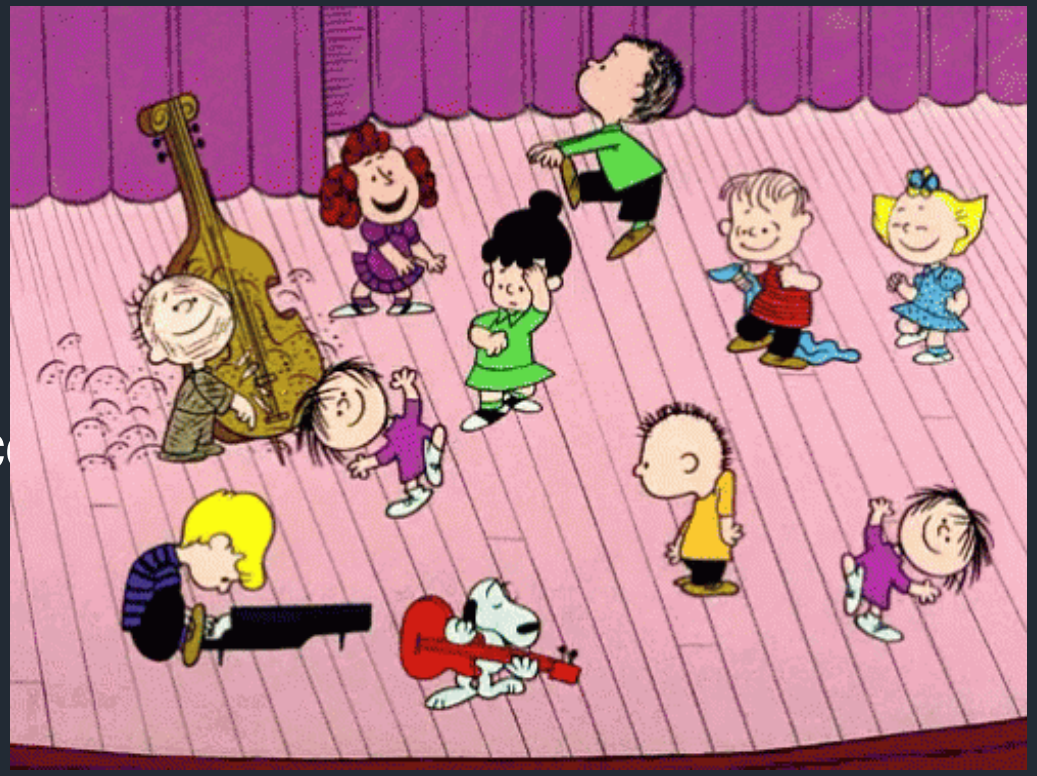
Using Dalton to Check if Rule's Syntax and Matching Behavior

RULE DEVELOPMENT LIFECYCLE

FEEDBACK FROM COMMUNITY

Working with ET Community

- Send feedback to Emerging Threats about …
  - False Positive activity
  - False Negative activity
- Submit signatures
- Send tips and leads to Emerging Threats Disc
- Share samples and PCAPs



Summary

- Need Explainability ?
  - ntopng's Suricata integration exists
- Need rules?
  - Use Emerging Threats rulesets, or other existing rulesets
- Need a deeper understandin g?
  - Learn about Suricata and creating rules
- Need feedback?
  - Chat with Emerging Threats on Discourse!

Questions?