AEGIS
IT RESEARCH

Friend or Foe?
Incident Characterization Techniques

iOSEC 2019
Luxemburg, 26/9/2019

Vassilis Prevelakis
AEGIS IT RESEARCH LTD

HORIZON 2020

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 833828.

Break In !!

Questions to ask

- How long has it been going on?
- Who did it?
- What was taken
- Which machines were compromised
- Credentials lost
- Backdoors installed
- …

So what to do?

- Time is of the essence
  - The sooner an attack is discovered the better
- Proper record keeping
  - If the attackers are found, it'll help in court
  - Also helps identify what happened and when
    - E.g. Bob's credentials were used to access a file, but Bob was on holiday!
- Vigilance

But …

- Security is an overhead
  - It does not make money, on the contrary!
- Tighter security, means more false alarms
- Staff get tired of responding
  - Stop being vigilant

- So we need a way to quickly determine whether an alert is for real

Digital Forensics

- The digital analogy to classical forensics (Sherlock Holmes)
- Traditional application was “after the fact”
- Nowadays DF also deal with “live” attacks and help in
    - Determining what is happening
    - Collecting data
    - If its an attack, coordinate response

- Our strategy is to leverage visualization tools to:
    - augment automated detection mechanisms with human intervention.
        - Minimize false positives
        - Eliminate false negatives

Characterizing an event

- So how do we tell whether a strange event signals an attack?
- Complex task requiring expert human operator
  - Combine readings from different sources to understand the event
    - also to increase confidence
  - Establish context
    - Even external factors
  - Compare and contrast with previous events
  - Match behavior with known attack vectors
- *Who you gonna call?*

Why visualization?

- Emphasis on visualization
  - Silver bullet for live forensics?

- Pros:
  - Provides good overview (situational awareness)
  - Allows combining data from different sources
  - Accommodates different views

- Cons:
  - Clutter may confuse operator
  - Creating the views may cause delays
  - Worse, may lead the operator into wrong conclusions.

AEGIS
IT RESEARCH

AEGIS Forensics Visualization Toolkit

- *Lets look at an existing Forensics Tool that emphasizes visualization*

- The AEGIS FVT aims to increase the situational awareness of operators when dealing with an event via
  - Ability to zoom in on details at the time of an event
  - Revealing possible relationships with other events or special indicators
  - Helping to identify past similar situations and discover re-occurring patterns

FVT (part 2)

- Timeline visualization
  - Temporal inspection of events and special indicators
- Timeline Comparison
  - Operator can compare two different time periods and relevant indicators on the same screen
- Disk Analysis
  - Disk related indicators
  - Signature search in disk images
- Preconfigured Views …

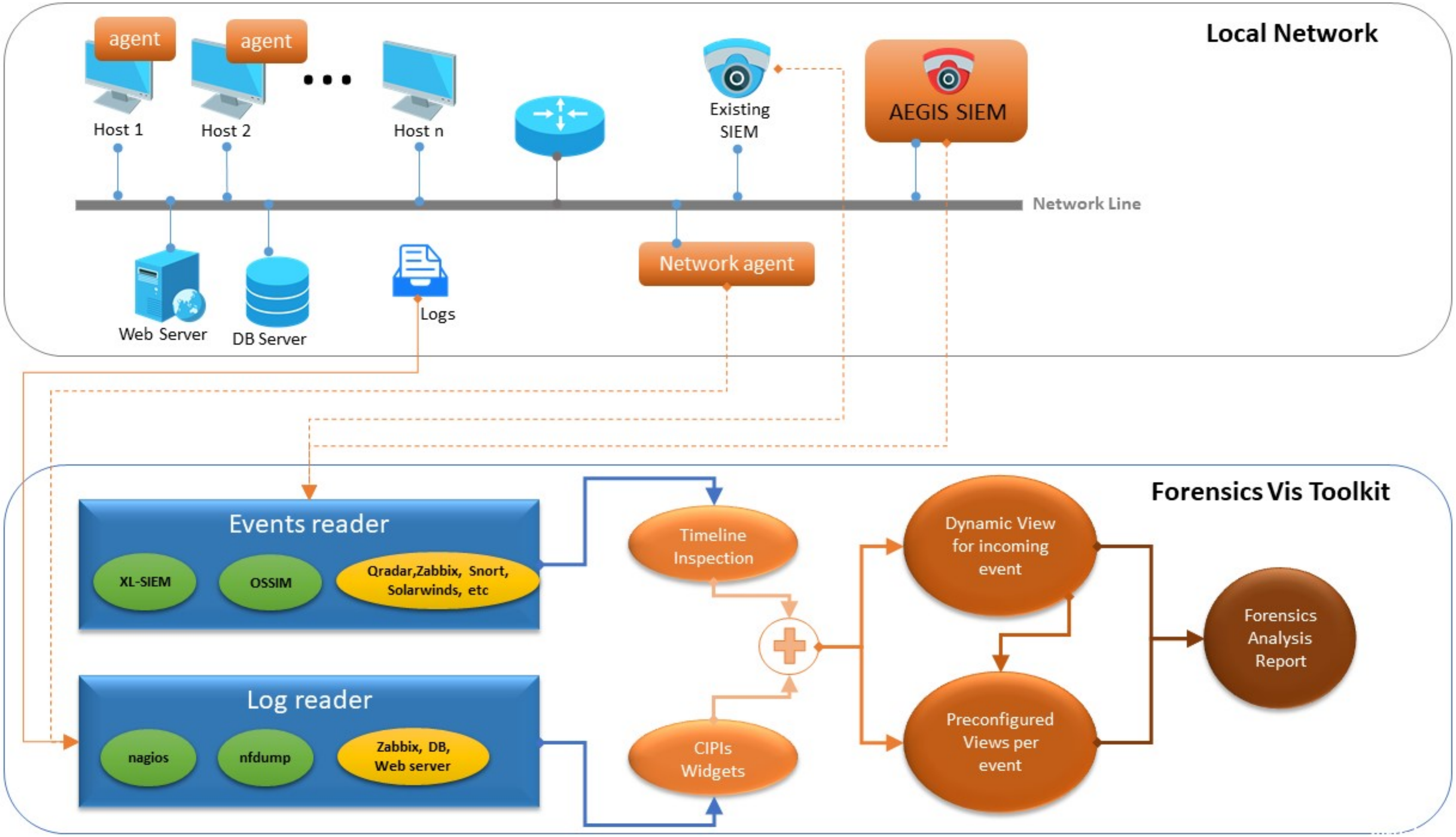
Preconfigured views

- Benefit of AEGIS forensic toolkit is that “knowledge” gained during an analysis can be utilised in future similar incidents
  - Event characterised by affected indicators
  - Operator response is stored in the event file
    - Specific views brought up
    - Events selected – highlighted during analysis
    - Etc.
  - Actions can be collected in a “script” to be run when similar event is observed.
  - Benefits:
    - Speeds up incident response
    - Makes event reporting faster – easier
    - Allows operator to concentrate on the analysis rather than bringing up the required views.
  - Should be used only by experienced personnel
    - May lead operator to wrong analysis (fight the last battle).

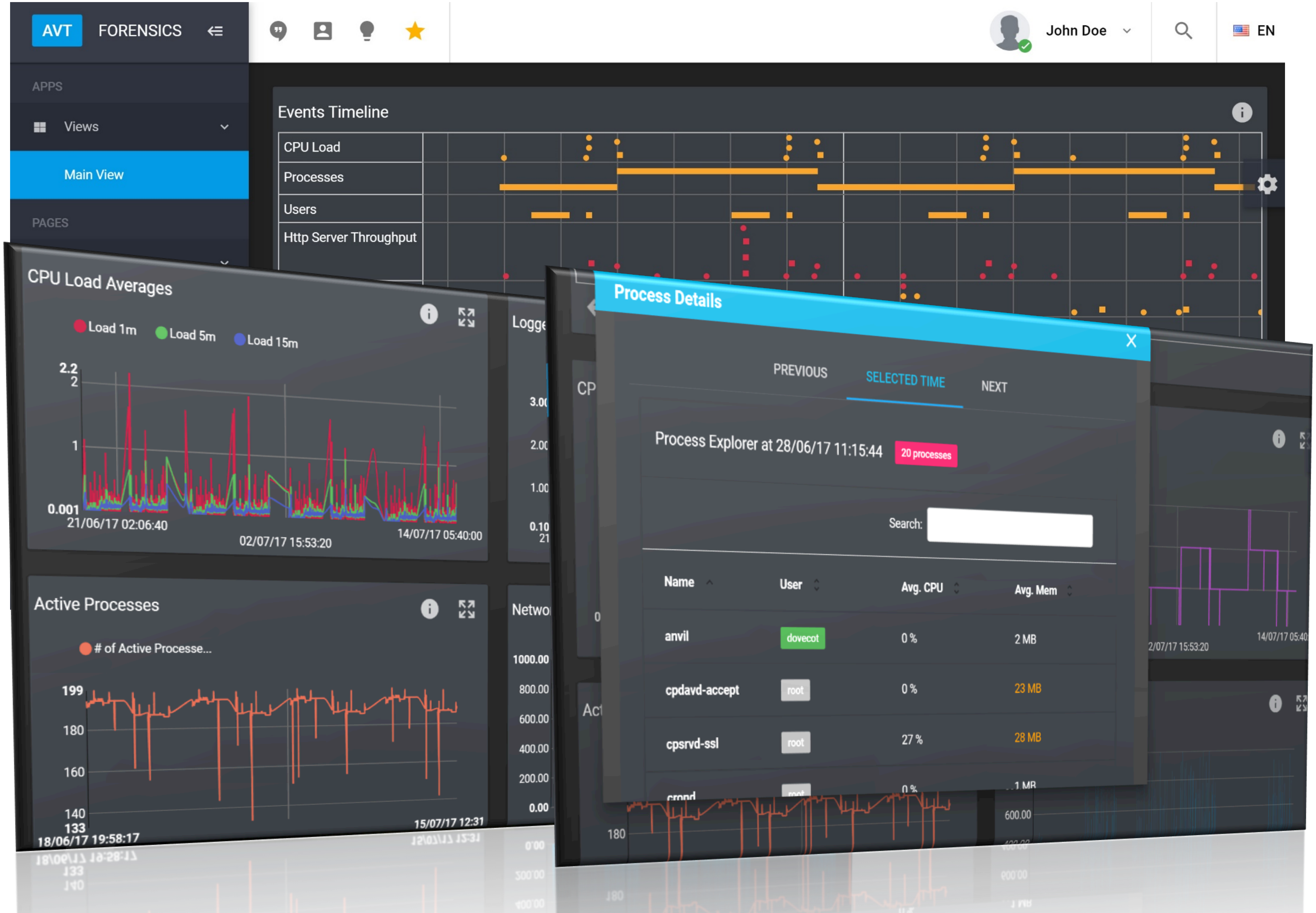
FVT (part 4)

- Where do we get the data?
- We draw data from agents that run on various platforms throughout the network: eg.
  - Nagios
  - Zabbix
  - Nfdump
  - Plus proprietary agents to collect richer information

Architecture Overview



FVT



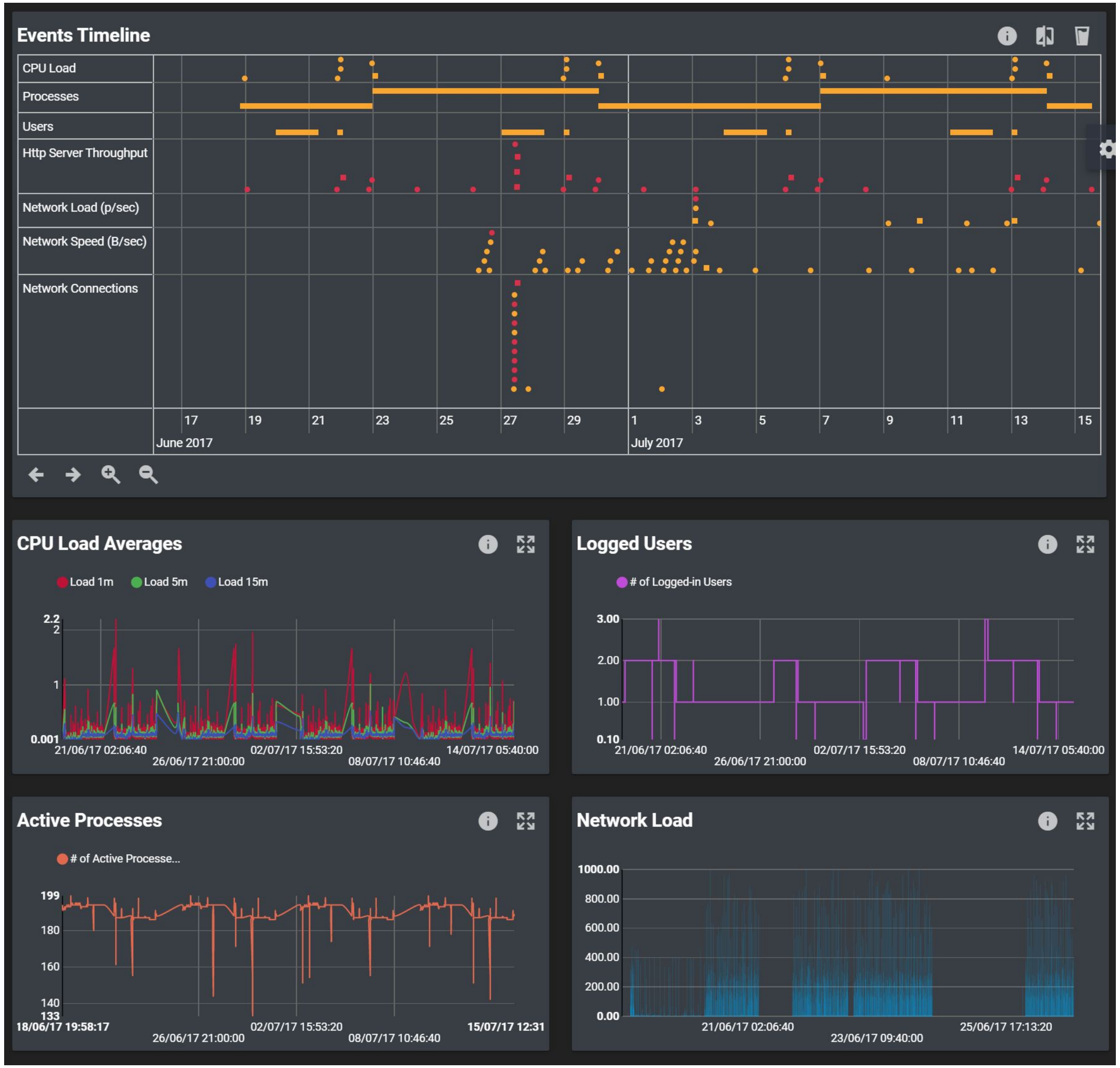
Process Details

Process Explorer at 28/06/17 11:15:44 20 processes

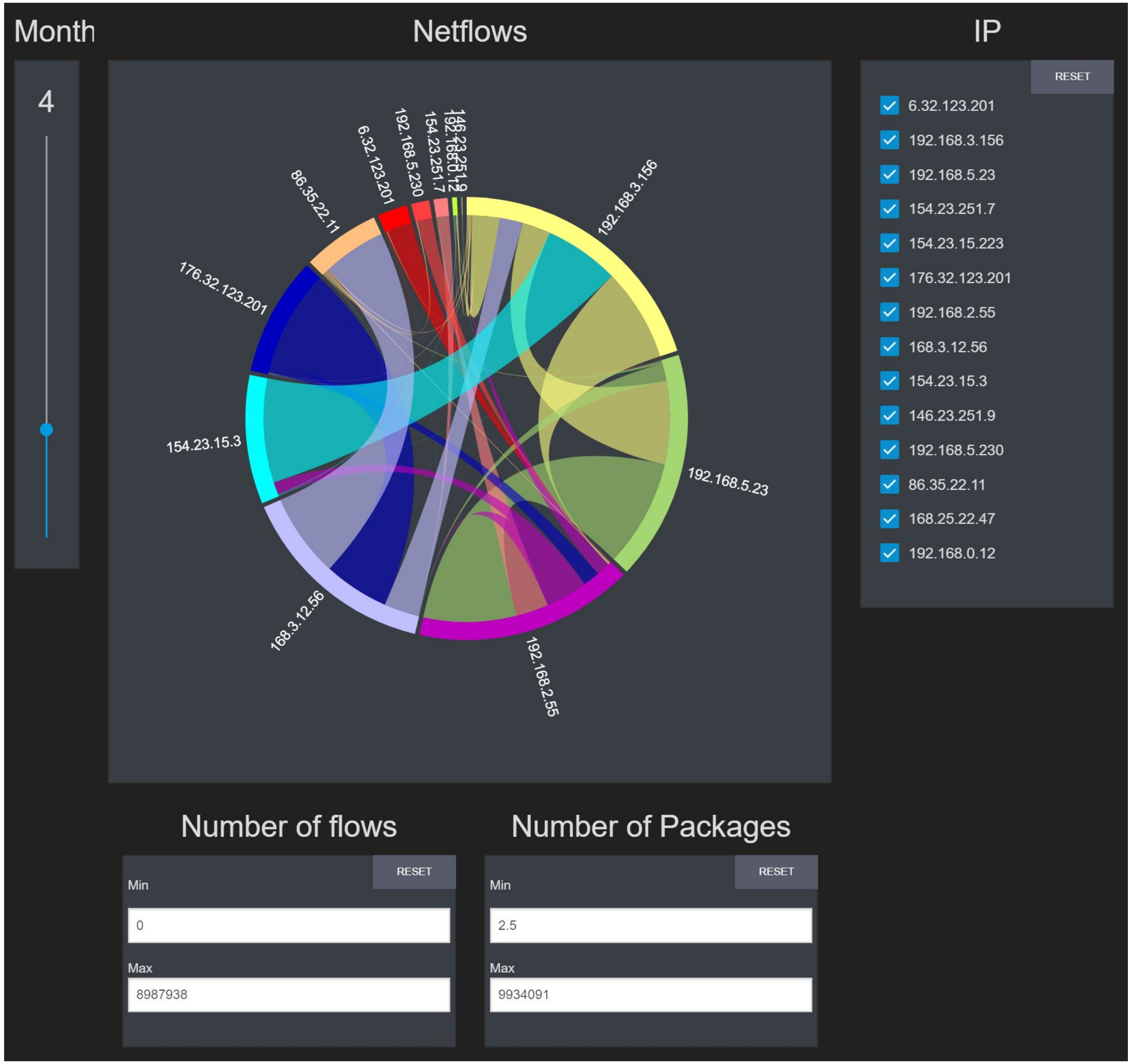
Search:

Name	User	Avg. CPU	Avg. Mem
anvil	dovecot	0 %	2 MB
cpdavd-accept	root	0 %	23 MB
cpsrvd-ssl	root	27 %	28 MB
crond	root	0 %	1 MB

FVT


Events Timeline
CPU Load
Processes
Users
Http Server Throughput
Network Load (p/sec)
Network Speed (B/sec)
Network Connections
17
19
21
23
25
27
29
1
3
5
7
9
11
13
15
June 2017
July 2017
CPU Load Averages
● Load 1m
● Load 5m
● Load 15m
2.2
2
1
0.001
21/06/17 02:06:40
26/06/17 21:00:00
02/07/17 15:53:20
08/07/17 10:46:40
14/07/17 05:40:00
Logged Users
● # of Logged-in Users
3.00
2.00
1.00
0.10
21/06/17 02:06:40
26/06/17 21:00:00
02/07/17 15:53:20
08/07/17 10:46:40
14/07/17 05:40:00
Active Processes
● # of Active Processe...
199
180
160
140
133
18/06/17 19:58:17
26/06/17 21:00:00
02/07/17 15:53:20
08/07/17 10:46:40
15/07/17 12:31
Network Load
1000.00
800.00
600.00
400.00
200.00
0.00
21/06/17 02:06:40
23/06/17 09:40:00
25/06/17 17:13:20

FVT – Netflow analysis



☑ 6.32.123.201
☑ 192.168.3.156
☑ 192.168.5.23
☑ 154.23.251.7
☑ 154.23.15.223
☑ 176.32.123.201
☑ 192.168.2.55
☑ 168.3.12.56
☑ 154.23.15.3
☑ 146.23.251.9
☑ 192.168.5.230
☑ 86.35.22.11
☑ 168.25.22.47
☑ 192.168.0.12

Number of flows

Min: 0

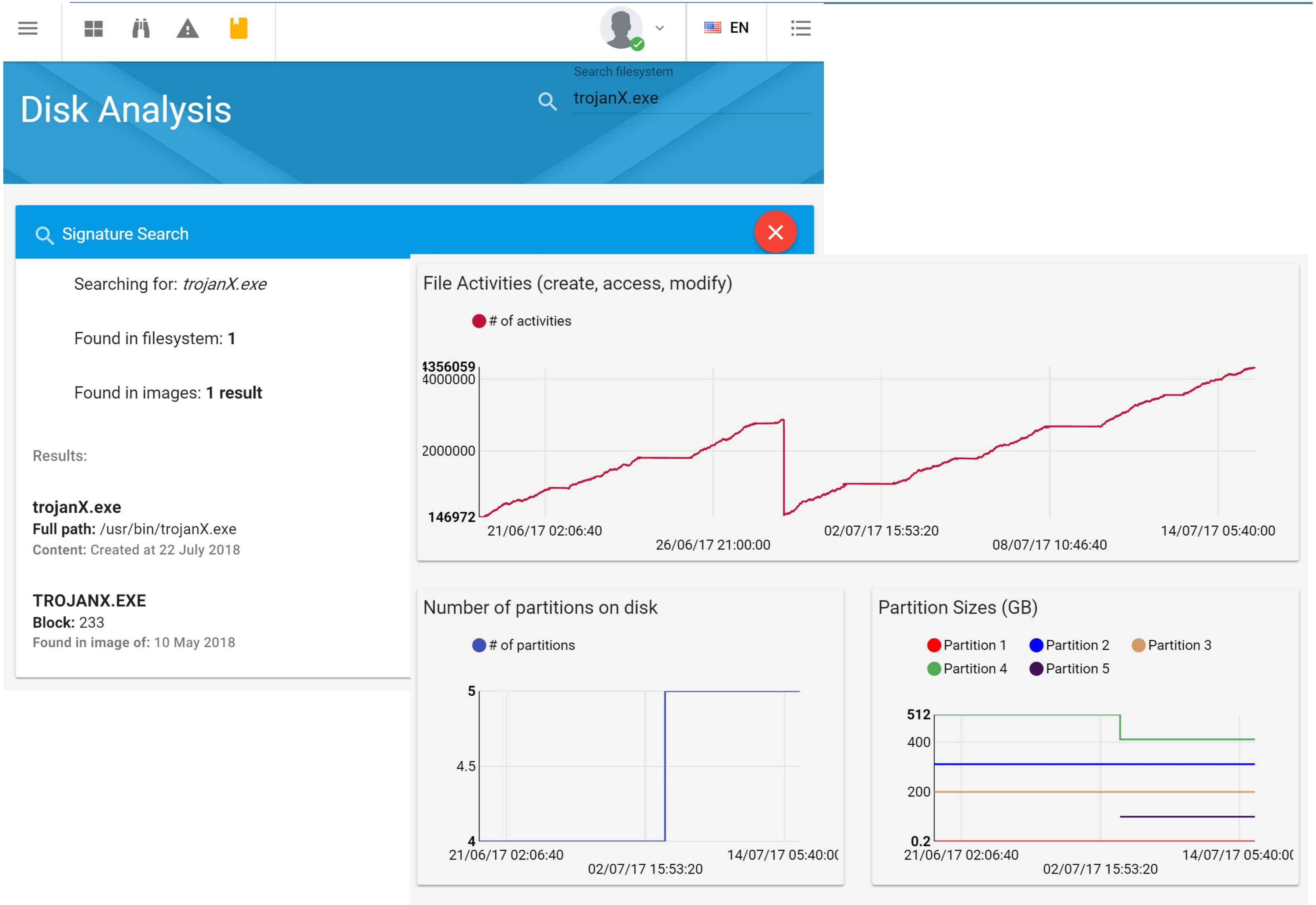
Max: 8987938

Number of Packages

Min: 2.5

Max: 9934091

FVT – Disk Analysis Summary



Disk Analysis

Search filesystem

trojanX.exe

Signature Search

Searching for: *trojanX.exe*

Found in filesystem: **1**

Found in images: **1 result**

Results:

trojanX.exe
Full path: /usr/bin/trojanX.exe
Content: Created at 22 July 2018

TROJANX.EXE
Block: 233
Found in image of: 10 May 2018

Summary

- Is visualization the answer?
- Not a silver bullet!
- But …
  - It’s a tool, if used properly it improves the performance of the operator
  - If not, it can confuse and disrupt the work of the operator.
  - Combined with machine learning techniques visualization can become the primary means for digital forensics analysis

AEGIS
IT RESEARCH

Friend or Foe?
Incident Characterization Techniques

iOSEC 2019
Luxemburg, 26/9/2019

QUESTIONS?

Vassilis Prevelakis
AEGIS IT RESEARCH LTD

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 833828.