Review Open Call F4Fp-SME

LEONIDAS KALLIPOLITIS

ZELUS P.C.

Forensics Visualisation Toolkit - FVT

FEC7

Remote review, 1 APRIL 2020

Outline

- The Company
- The Experiment
- Project Results
- Business Impact
- Feedback

ZELUS

Zelus

ZELUS

THE COMPANY

Zelus Profile

WHAT WE DO

Solutions for all

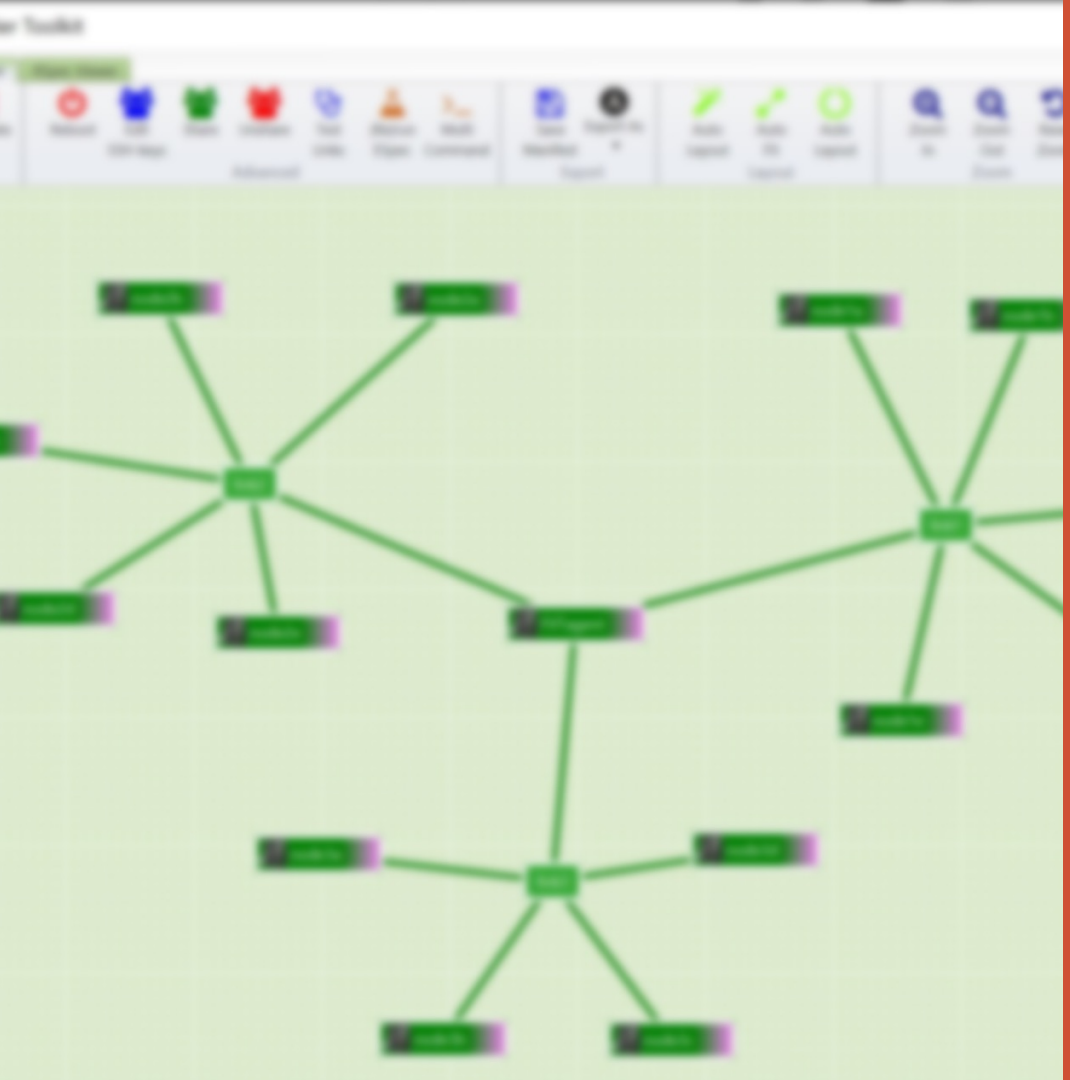
We offer secure, innovative solutions for business of every size, from micro SMEs to large industries.

Digital Forensics

Focused on innovation and cyber security, we support an innovative toolset for Digital Forensics analysis and threat hunting.

Complete Software Lifecycle

We offer management and implementation services for IT projects supporting the complete Software Development LifeCycle



The Experiment

Experiment Description 1/3

CONCEPT

- Enhance *Digital Forensics* process by focusing on visualisation
- Fast situational awareness
- Elimination of false positives
- Act complementary to existing cyber security systems (SIEM, IDS, etc.)

OBJECTIVES

- Validation of our tool's usability
- Assessment of data volume that must be handled
- Measurement of efficiency and applicability to the needs of target customers
- Testing of implementation strategy and flexibility

Experiment Description 2/3

BACKGROUND

- Collection, processing & analysis of security-related data has become exremely challenging due to data volume, complexity and increasing sophistication of attacks
- Organisations have to
    - protect their assets
    - comply to regulations
    - manage budget

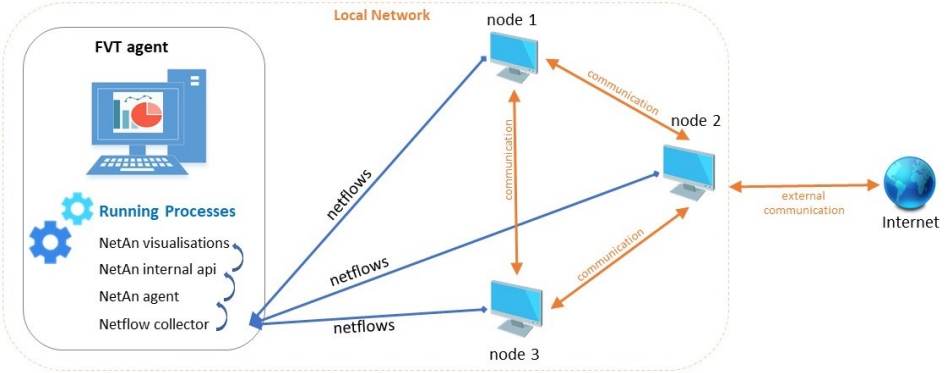
MOTIVATION

- Leverage visualisations to foster digital forensics
- Help operators quickly discover the root cause of incidents on a post-mortem analysis
- Enable real-time analysis and threat hunting capabilities
- Cost-effective solution for SMEs

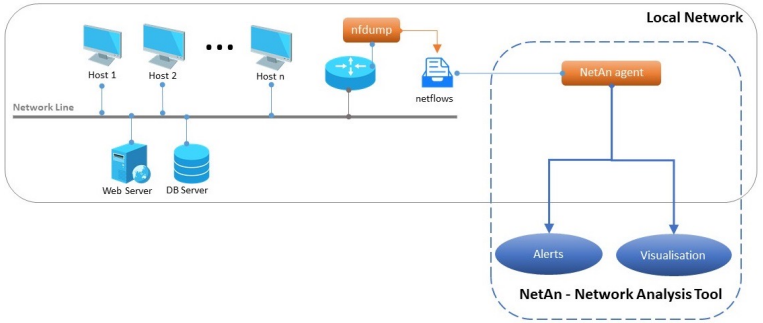
Experiment Description 3/3

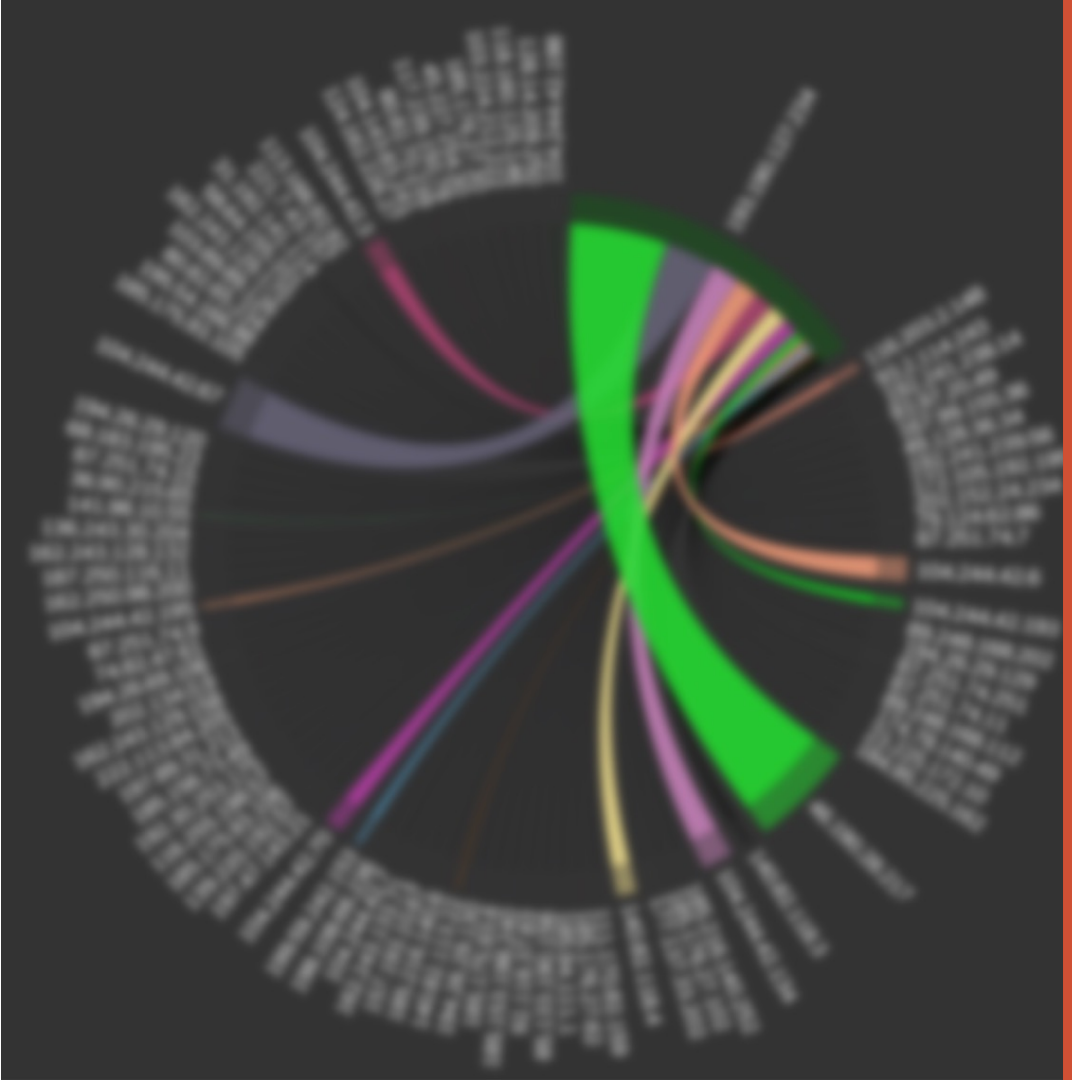
SET-UP

- Testbed: Virtual Wall 2
- Management & Resource Provision:jFED
- 3 -15 physical nodes, 1 address pool
- FVTagent
  - Netflow collector
  - Visualisation app hosting
- All nodes
  - Probes sending netflows to FVTagent



FVT- Network Analysis Deployment





Project Results

Experiment Results

TECHNICAL RESULTS

- Complex visualisation when number of nodes increased
- More advanced filtering and grouping needed
- Process to install, setup and run in all nodes of a network must be easier and less-time consuming
- Data size (#netflows) can be handled adequately by our internal processing API

Experiment Results

LESSONS LEARNED

- The tool seems fit-for-purpose for basic forensic investigation scenarios
- Installation and deployment need to be streamlined to support bigger networks – Dockerisation seems a fit-for-purpose option
- Visualisation elements require constant updates and new functionalities to keep up with emerging needs – unforeseen problems as monitored assets increase
- Netflow processing internal API performs satisfactory for 1-day traffic loads of the examined networks but more processing is needed to support new functionalities

Business Impact

Business Impact 1/4

VALUE PERCEIVED

- Acceleration of time-to-market process:
    - better estimation of resources and timeline for a production deployment
    - Saved effort of searching of other testbeds to match our needs for testing
    - Reduced cost to test various setups and topologies
    - Minimised setup, admin and running times allowed us to save time that could be utilised for core business tasks, e.g. Enhancing tool features

Business Impact 2/4

VALUE PERCEIVED

- Better definition of target customer groups
    - Assessment of the needs and network topologies of potential customers
    - Definition of forensic analysis scenarios that the tool can support in its first release
- Decrease in business risk:
    - early identification of weaknesses and mitigation before going to market
    - Allready added new fetures while executing the experiment

Business Impact 3/4

DIRECT VALUE

- New features already incorporated
- Demos on near real-world setups

- First contacts with potential customers
    - Professional associations (doctors)
    - Insurance companies

Business Impact 4/4

FUNDING & FURTHER DEVELOPMENT

- Participation to confirmed for funding H2020 proposal (currently in preparation)
- Participation in upcoming H2020 calls
- Pursuing scientific publications

Feedback

Feedback 1/5

RESOURCES USED

- Virtual Wall 2
    - Physical nodes
    - Adress Pool
- jFed (GUI)

SUPPORT USED

- VW Documentation
- jFed Documentation
- jFed feedback
- F4F Online google group

Feedback 2/5

EXPERIENCE

- Easy setup of the experiment via very well received features
    - OS image selection
    - Root ssh access
    - Duration extension
- Superfast responses to reported issues (all of them sorted out)
    - Resource allocation not working (temporal problem)
    - Ssh access impossible (putty related)

Feedback 3/5

ADMINISTRATION

- Easy and time-effective proposal template for the Open Call
- Guidelines and procedures easy to follow
- Given budget covers entirely resources allocated for the experiment
- FEC events present great opportunity to disseminate results and meet new contacts
    - Maybe participate to the next one, whenever it takes place

Feedback 4/5

ADDED VALUE

1. Easy application procedure for the fund
2. Easy setup of the experiments
3. Extensive documentation
4. Functionalities tailored to real-world needs, e.g. root access
5. Quick response team in providing support
6. Amount of available resources (many nodes to allocate in our case)
7. Diversity of resources

Feedback 5/5

USEFULLENESS TO ZELUS

- Funding came in at perfect timing for our start-up (founded in May 2019)
- Assistance in testing/validation of our tool and formulation of our value proposition without requiring capital expenditures
- Big boost on our road to commercialisation


Co-funded by the
European Union


Co-funded by the
Swiss Confederation

This project has received funding from the European Union's Horizon 2020 research and innovation programme, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation, under grant agreement No 732638.

WWW.FED4FIRE.EU