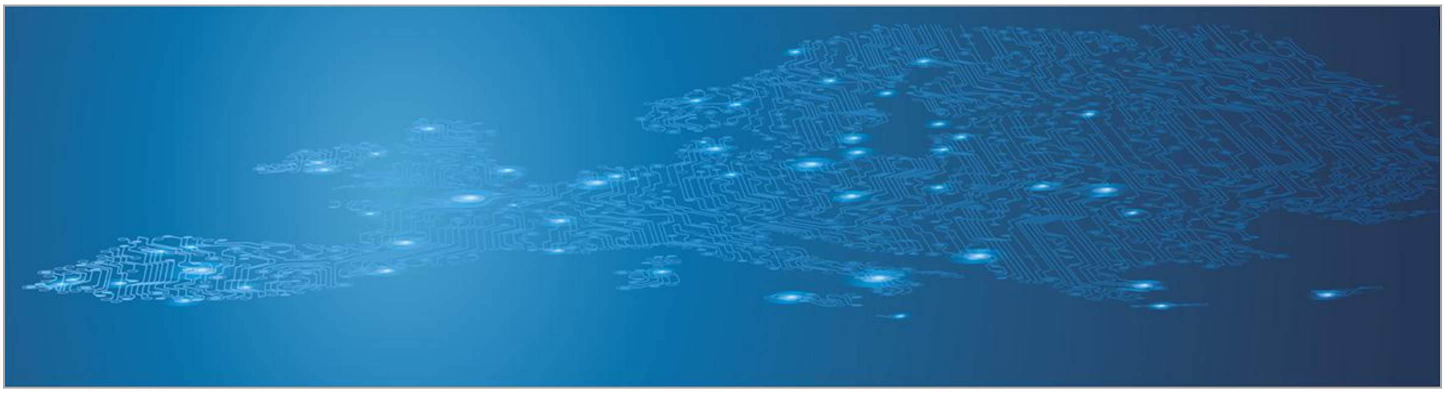
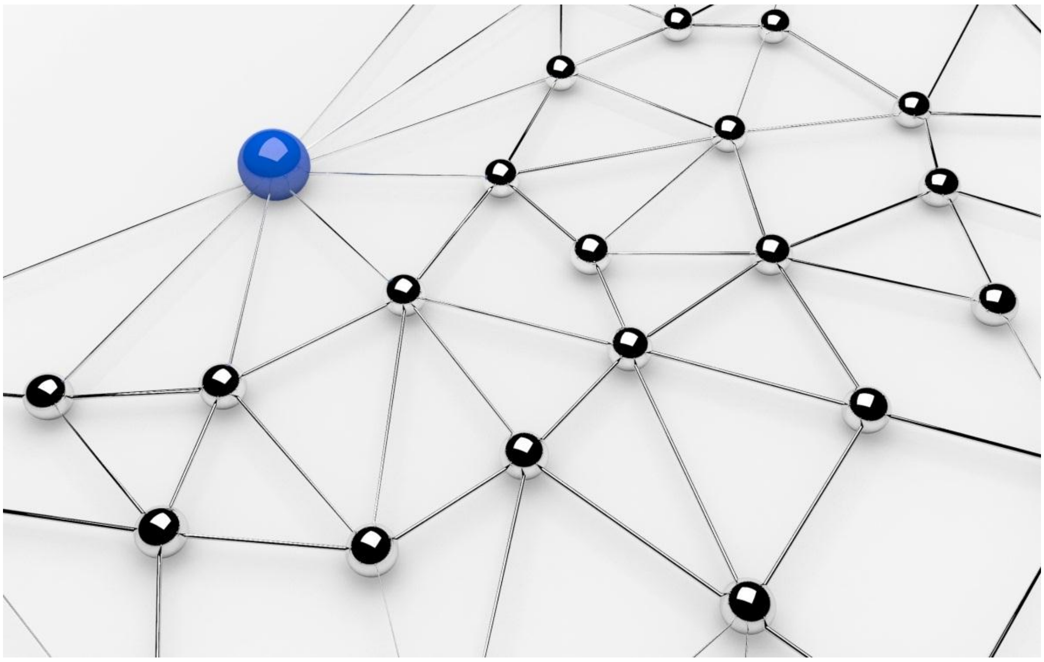




Presenting, correlating and filtering various feeds

Toolset, Document for students

September 2013

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This document was created by the CERT capability team at ENISA in consultation with:

Don Stikvoort and Alan Thomas Robinson from S-CURE, The Netherlands, Mirosław Maj, Tomasz Chlebowski, Paweł Weżgowiec from ComCERT, Poland, Przemysław Skowron from Poland, Roeland Reijers from Rubicon Projects, The Netherlands and Mirko Wollenberg from DFN-CERT Services, Germany.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this document, please use press@enisa.europa.eu.

Acknowledgements

- ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors:
- 1. Tomas Lima from CERT.PT
- 2. The countless people who reviewed this document.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-79-00077-5 doi:10.2788/14231

Table of Contents

2 Introduction 1

3 Exercise tasks 1

3.1 Setup 1
- 3.1.1 Task 1: Identifying data sources 1
- 3.1.2 Task 2: Using Kibana 1
- 3.1.3 Task 3: Tracing cybercrime activity 2

4 Conclusion 3

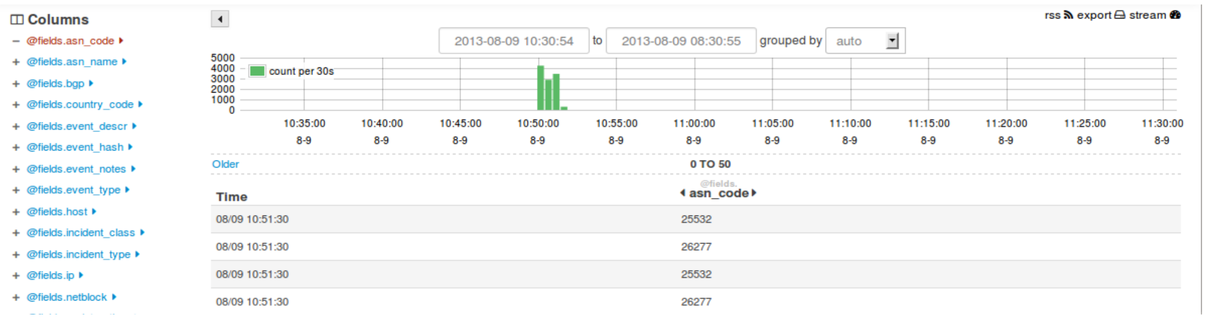
5 References 4

1 What you will learn

In this exercise you will gain an overview of data visualisation approaches. Based upon AbuseHelper (see also exercise 14 Proactive Incident Detection), the visualisation provided by Kibana (and related tools) will be introduced in more detail.

The necessary material for the exercise is located in the folder /usr/share/trainee/28_VCT of the ENISA virtual appliance.

The commands for setup are to be found in the file ‘Commands for VCT exercise.doc’ and will not be repeated in this document.



Columns
- − @fields.asn_code
- + @fields.asn_name
- + @fields.bgp
- + @fields.country_code
- + @fields.event_descr
- + @fields.event_hash
- + @fields.event_notes
- + @fields.event_type
- + @fields.host
- + @fields.incident_class
- + @fields.incident_type
- + @fields.ip
- + @fields.netblock

2013-08-09 10:30:54 to 2013-08-09 08:30:55 grouped by auto

0 TO 50

Time	@fields.asn_code
08/09 10:51:30	25532
08/09 10:51:30	26277
08/09 10:51:30	25532
08/09 10:51:30	26277

Figure 1: Kibana web interface

2 Introduction

During the introduction the trainer will familiarise you with the topic of data visualisation, different solutions and implementations of visualisation and the tools used in the main section of the exercise.

Your main tool will be Kibana, which provides a web interface implementing the Apache Lucene syntax.

3 Exercise tasks

3.1 Setup

Before you can start working on the tasks it is necessary to initialise the working environment properly. Follow the instructions given by the trainer (you will find the necessary commands in the ‘Commands for VCT exercise.doc’ file).

After the setup there will be three tasks to be processed.

3.1.1 Task 1: Identifying data sources

Use the spread sheet AH-data-feed-eval.xls in the main folder of the exercise. Fill out all the fields taking particular care in the reasoning with regard to the usability for cybercrime investigations.

3.1.2 Task 2: Using Kibana

Use the Kibana web frontend to answer the following questions:

- Which feeds are configured?
- Which ASN’s are in the incoming data fields?
- Which ASN’s are distributing malware?
- Which three ASN’s have the most phishing incidents?

Write your results down and document the steps you have taken to achieve the goals. Describe constraints of the visualisation approach and advantages of the approach. Give a rating regarding the use of Kibana in incident response teams.

3.1.3 Task 3: Tracing cybercrime activity

Although this is not meant to be a full-scale role-play exercise there is some background information which should help you understand the data to be analysed and the context of the incidents.

Background information regarding the context of the data:

You are the incident response team of a company providing e-commerce solutions. It hosts the business infrastructure (site, shop solution, payment) for its customers in software as a service (SaaS)[1] model. The sites it hosts generate daily revenue of approximately €10 million.

Technical details of the technical infrastructure of the company:

This information is necessary to analyse the incident data.

1. Domain: example.com
2. Network: 192.0.32.0/20
3. Autonomous System Number (ASN)[2]: AS26711
4. Apache Webserver
5. ModSecurity intrusion detection system (IDS)

Three data sets have been prepared containing incident related information. These reside in the folders event_1, event_2 and event_3 in /usr/share/trainee/28_VCT/add and are named event-log.csv. Inject them into the running visualisation installation as requested by the trainer (see the commands document for details).

• Answer the following questions:

The customers are based in the EU and logins from networks outside Europe are very unusual. Please check the logins and write down any anomalies.

Check the incident data for hints on the cause of the compromises.

For both parts develop and document the next steps during the incident response process.

• Answer the following:

In the data is evidence for the next steps the attackers have taken after the initial compromise. Identify the incidents and document the information and the necessary steps to contain and respond to them.

• Answer the following:

Customers are complaining about issues with webservers. Check the data for possible causes and document them with technical detail.

[1] *Software as a Service (SaaS) http://cloudtaxonomy.opencrowd.com/taxonomy/software-as-a-service/*
[2] *Autonomous System (AS) Numbers http://www.iana.org/assignments/as-numbers/as-numbers.xhtml*

4 Conclusion

The last part of the exercise reviews each task.

You will start with the exercises and each team of students will present its findings and the process of analysing the data in Kibana. Afterwards these presentations will be discussed by all participants and summarised by the trainer to document the learning effect.

In the second step Kibana and alternative visualisation approaches and implementations are the topic of the discussion. Use your notes as a base and try also to include background information from outside of the exercise experience.

Finally, the general approach of visualising data will be discussed. Develop criteria which helps to decide when and how to visualise.

5 References

1. The Honeynet Project – Know Your Tools use Picviz to find attacks, 2009 (*http://www.honeynet.org/files/KYT-Picviz_v1_0.pdf*)
2. logstash – open source log management (*http://logstash.net/*)
3. Kibana – Make sense of a mountain of logs (*http://kibana.org/*)
4. Elasticsearch – Real Time Data and Analysis (*http://www.elasticsearch.net/*)
5. certpt – GenericEvent-AbuseHelper (*https://bitbucket.org/certpt/genericevent-abusehelper/src*)
6. certpt – LogCollector-AbuseHelper-Extension (*https://bitbucket.org/certpt/logcollector-abusehelper-extension/overview*)
7. Wikipedia – Information visualization (*https://en.wikipedia.org/wiki/Information_visualization*)
8. Apache Lucene – Query Parser Syntax (*https://lucene.apache.org/core/3_5_0/queryparsersyntax.html*)
9. CERT.at – ProcDOT (*http://cert.at/downloads/software/procdot_en.html*)
10. Wikipedia – Netcat (*http://en.wikipedia.org/wiki/Netcat*)
11. ENISA – Exercise Material (*http://www.enisa.europa.eu/activities/cert/support/exercise*)
12. AbuseHelper – (*http://www.abusehelper.be/*)
13. Wikipedia – Graph (abstract data type) (*https://en.wikipedia.org/wiki/Graph_%28data_structure%29*)
14. Wikipedia – Parallel coordinates (*https://en.wikipedia.org/wiki/Parallel_coordinates*)
15. Wikipedia – Heatmap (*https://en.wikipedia.org/wiki/Heatmap)*
16. Team Cymru – Internet Malicious Activity Maps (*https://team-cymru.org/Monitoring/Malevolence/maps.html)*

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu