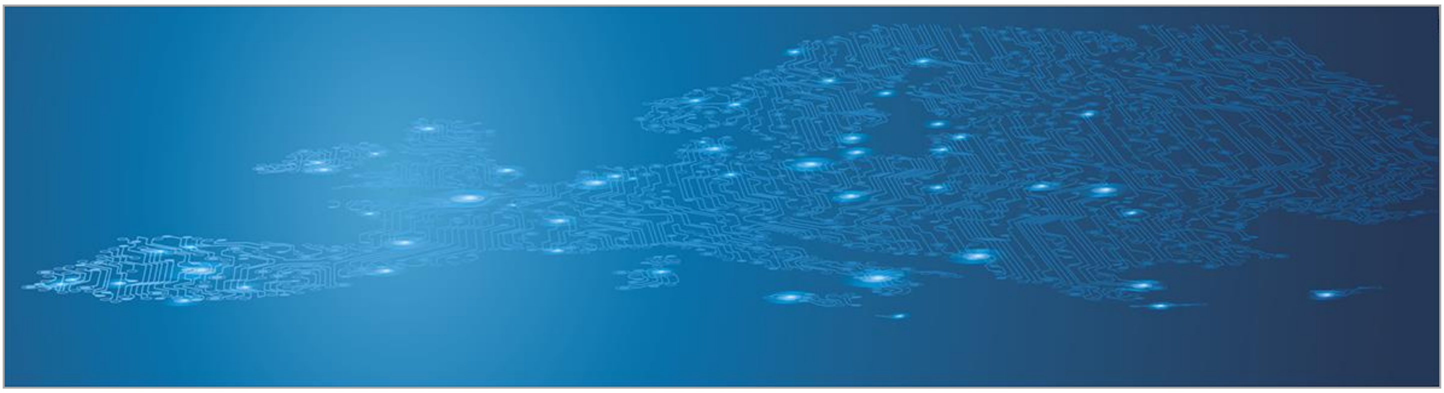

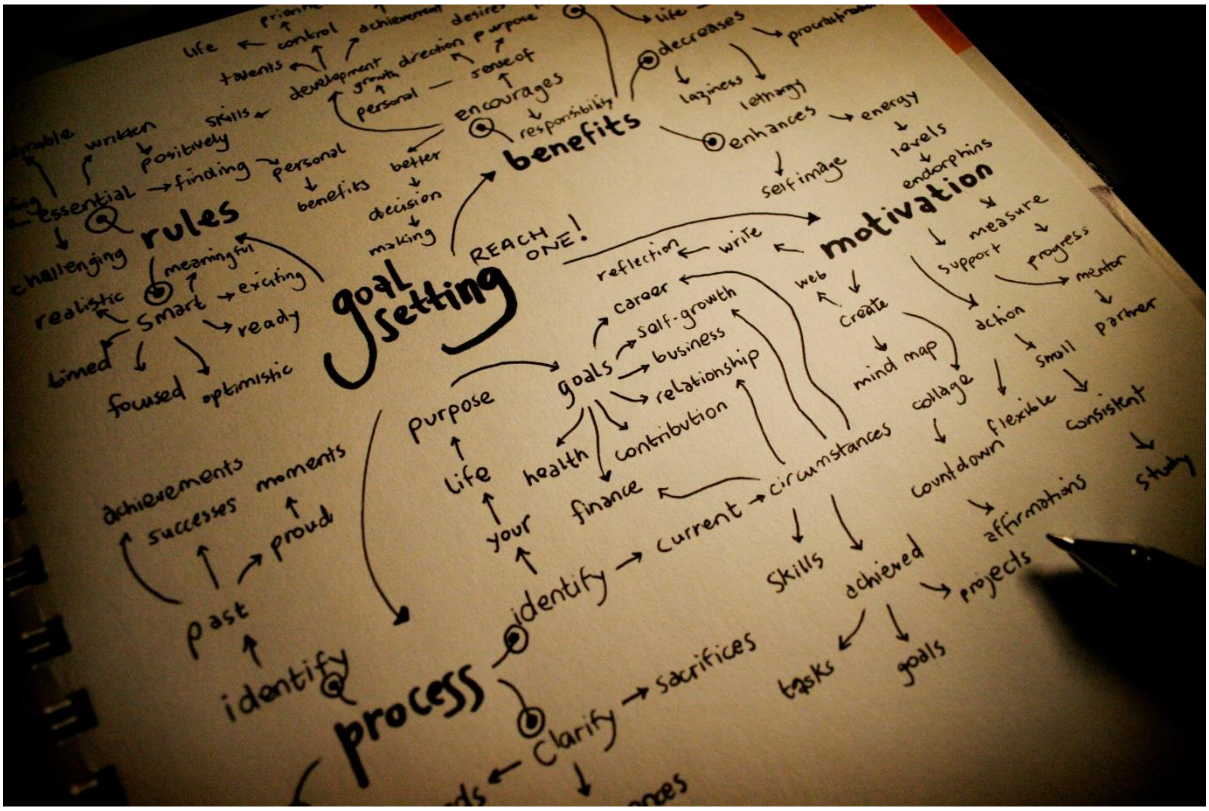

Incident Handling Procedure Testing

Toolset, Document for students

September 2014

enisa

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.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

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

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

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

Table of Contents

1 What Will You Learn

In this exercise you will learn how to build your own incident handling procedure – how to identify the most important players in this procedure, the critical points and the most suitable means of communication.

You will become familiar with the basic set of activities relating to the incident handling process.

You will learn the correct sequence of activities during the incident handling process.

You will gain knowledge about the most important parts of the IH procedure, those that have a critical influence on the successful process which will be provided to you.

You will become familiar with all possible players in the IH process.

You will learn the most effective methods for cooperation between a CSIRT and the key incident handling players.

2 Exercise Task

2.1 Task 1 Developing incident handling procedure

Using the incident handling procedure objects, form a complete incident handling procedure. Make the proper sequence of the activities, build relationships between them, and show the directions of the work flows. Additionally, extend the procedure with your proposals for activities using the blank objects.

After forming a procedure, identify the activities which require communication with external parties. For each of them, indicate the recommended means of communication (eg, a normal e-mail, a phone, an encrypted e-mail, etc).

Analyse your procedure. Point out the critical elements and identify the potential problems which could appear during execution of a procedure.

Use Appendix 1 for this task.

Appendix 1

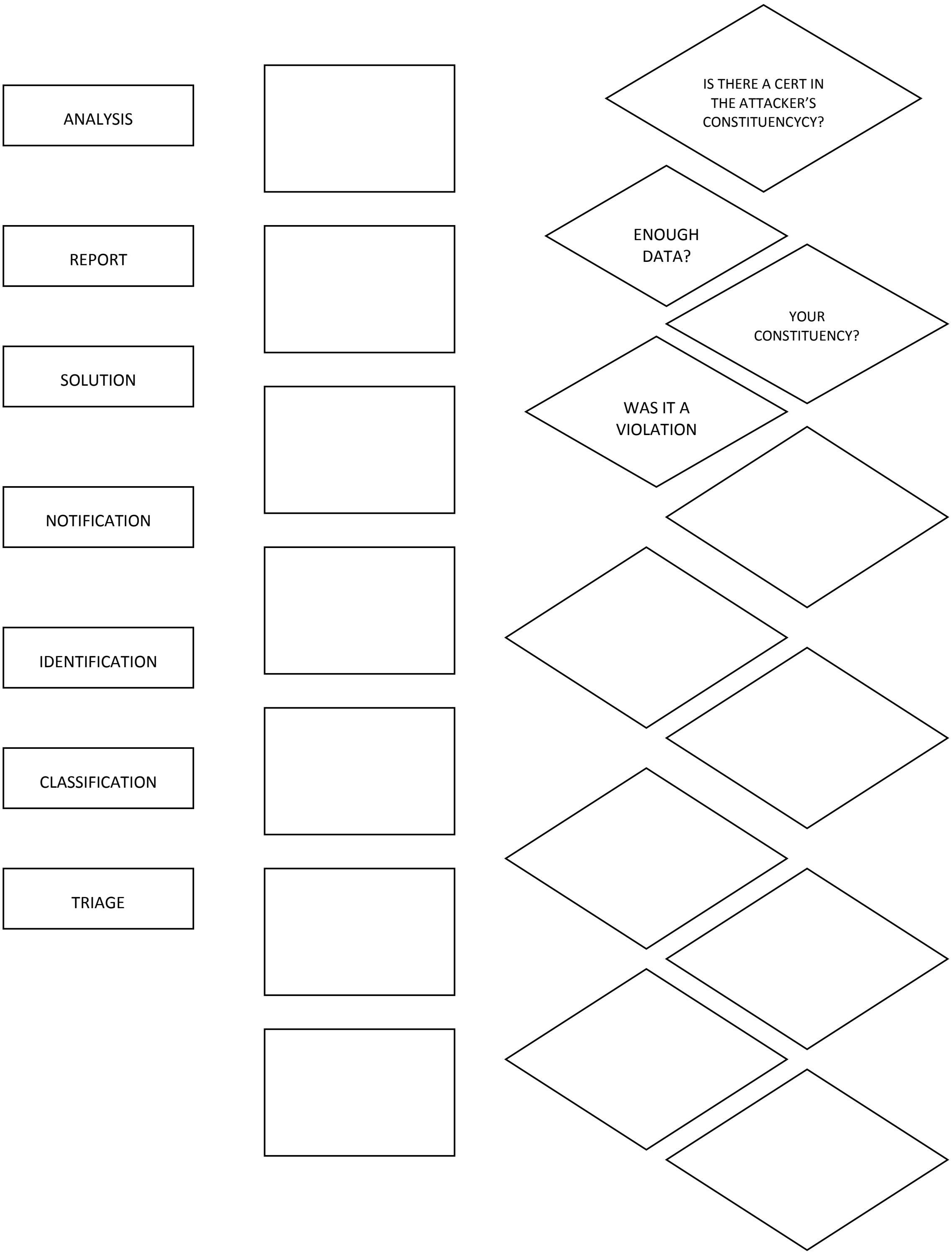

Figure 1 : Incident Handling Procedure

2.2 Task 2 Resolving critical problems in incident handling

2.3 Please write down the most critical parts of the procedure identified by the groups and the trainer. Provide your ideas on how to deal with them in order to mitigate the related risks and propose proactive activities for avoiding such problems.

Critical Part	Solution / Recommendation / Ideas

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