



Developing CSIRT Infrastructure

Toolset, Document for students

1.0
DECEMBER 2016



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.

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 ENISA, 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), 2016

Reproduction is authorised provided the source is acknowledged.

Table of Contents

| | |
|---------------------------------|----------|
| 1. What Will You Learn? | 4 |
| 1.1 CSIRT Infrastructure | 4 |
| 2. Introduction | 5 |

1. What Will You Learn?

1.1 CSIRT Infrastructure

To learn what kind of software and hardware solutions could be used to provide a particular CSIRT service for a constituency.

2. Introduction

The teacher will give a presentation introducing and describing the CSIRT services defined by CERT/CC (see Table 1).

| Reactive Services | Proactive Services | Security Quality Management Services |
|---|--|---|
| <ul style="list-style-type: none"> - Alerts and Warnings - Incident Handling <ul style="list-style-type: none"> - Incident analysis - Incident response on site - Incident response support - Incident response coordination - Vulnerability Handling <ul style="list-style-type: none"> - Vulnerability analysis - Vulnerability response - Vulnerability response coordination - Artifact Handling <ul style="list-style-type: none"> - Artifact analysis - Artifact response - Artifact response coordination | <ul style="list-style-type: none"> - Announcements - Technology Watch - Security Audits or Assessments - Configuration and Maintenance of Security Tools, Applications, and Infrastructures - Development of Security Tools - Intrusion Detection Services - Security-Related Information Dissemination | <ul style="list-style-type: none"> - Risk Analysis - Business Continuity and Disaster Recovery Planning - Security Consulting - Awareness Building - Education/Training - Product Evaluation or Certification |

Table 1 CSIRT services by CERT/CC

The introduction will also explain the various diagrams below which are part of the tasks section of the exercise.

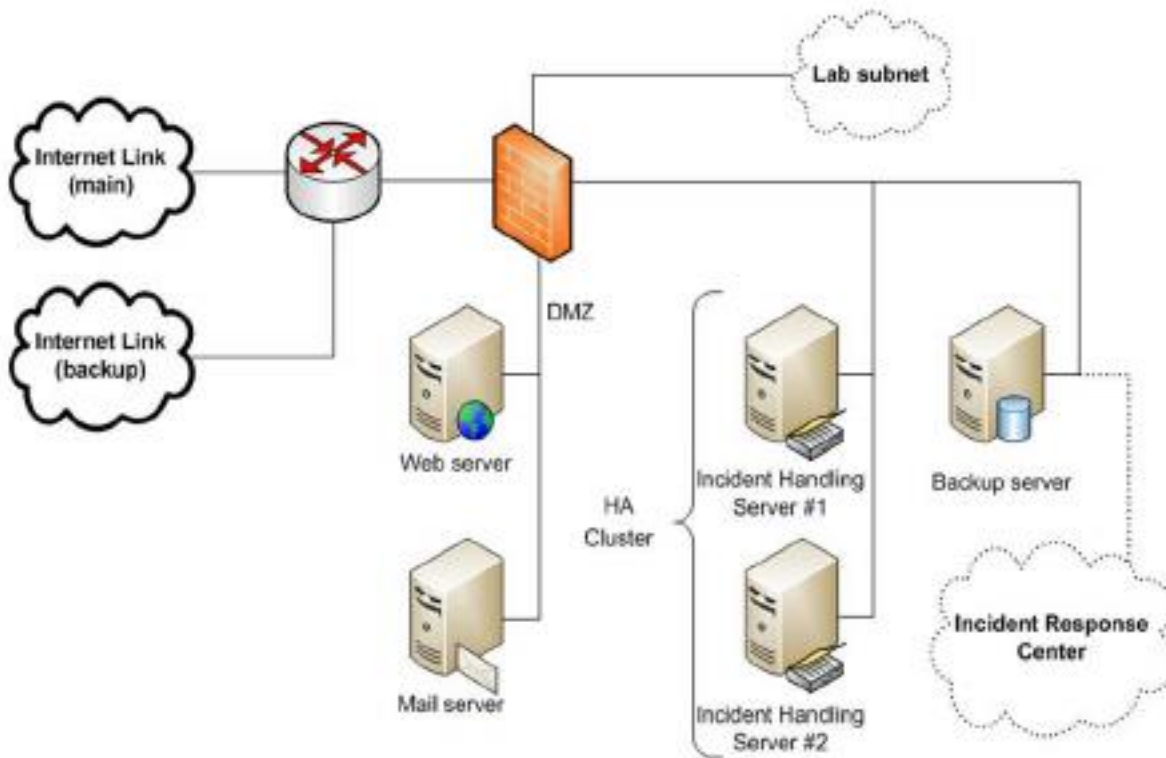


Figure 1 Simple (legacy) CSIRT network infrastructure

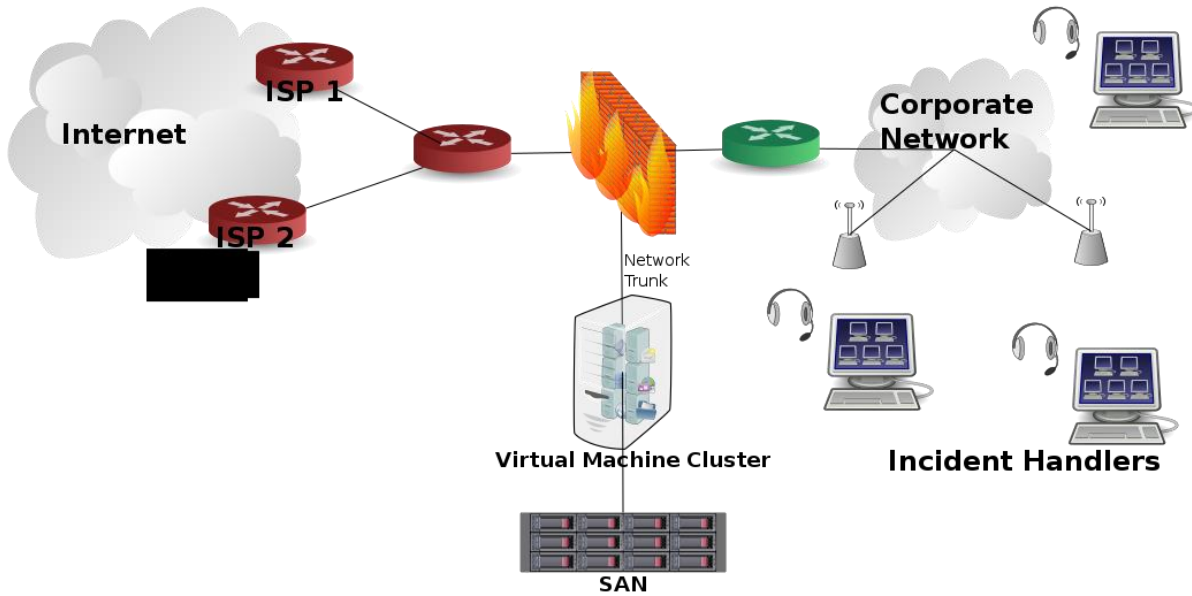


Figure 2 CSIRT infrastructure including virtualisation technologies

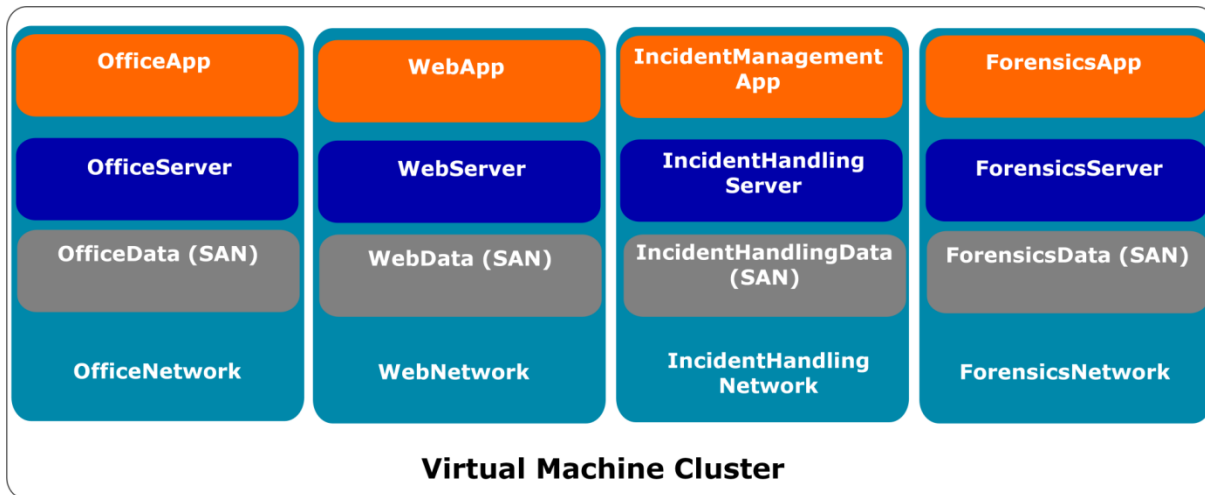


Figure 3 CSIRT infrastructure VM layers

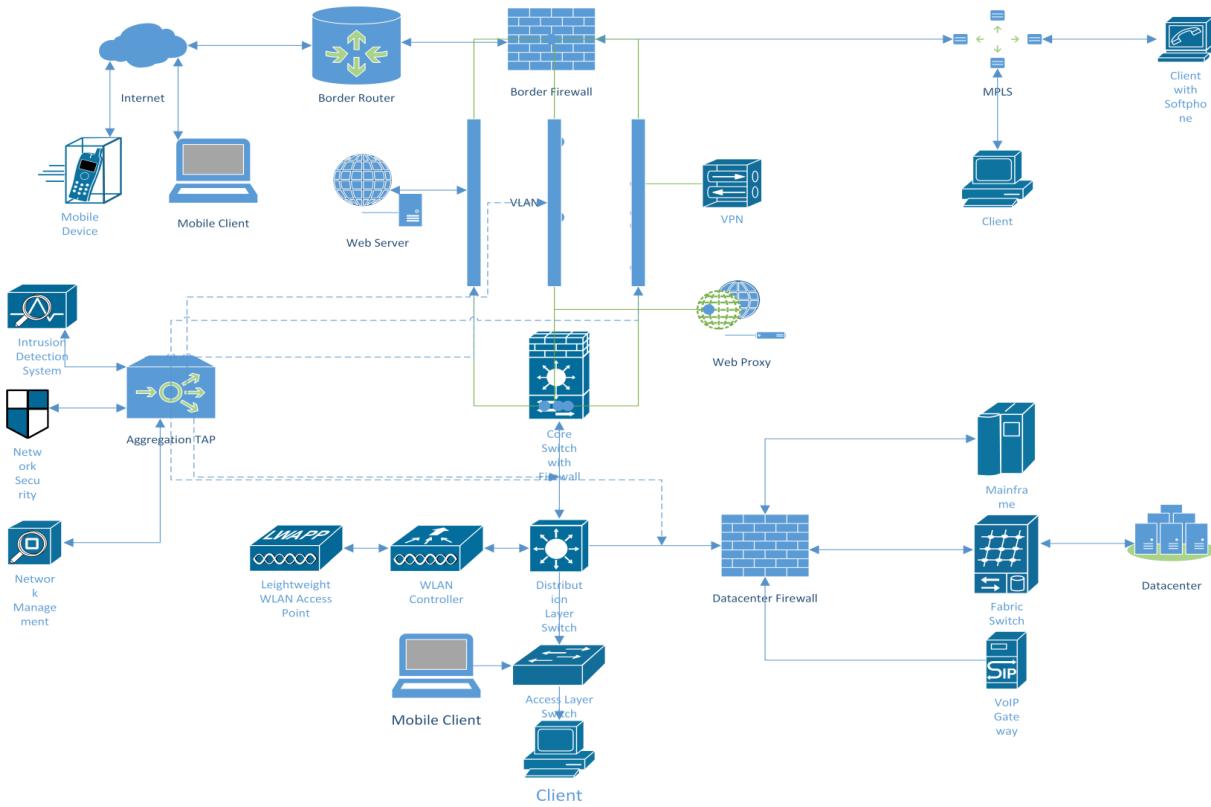


Figure 4 Enterprise scale network

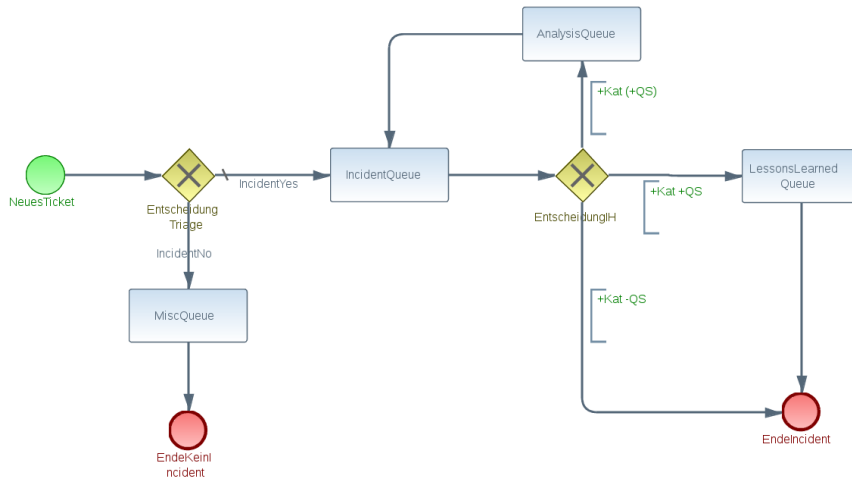


Figure 5 Incident response workflow

3. Exercise Tasks

3.1 **Task 1: Discuss the proposed infrastructures for the incident handling – incident analysis service**

The teacher will lead you through the task by providing questions focusing on certain core topics leading to a complete perspective of designing an infrastructure to support a CSIRT incident handling – incident analysis service.

3.2 **Task 2: Discuss the proposed infrastructure for 3-5 additional CSIRT services**

Use the table from the introduction to decide on further services and discuss/develop the required technical infrastructure and processes as done for the incident handling – incident analysis service in task 1.



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

