GOVCERT
.lu

Incident Categories (Public)

Version 4.0 - 2020-07-21 (Final)

Procedures (PRO 303)

TLP:	TLP:WHITE	**Department:**	GOVCERT.LU
Classification:	PUBLIC		

Contents

1 Introduction

1.1 Overview

Once an incident report has been received, it should be treated efficiently and rapidly in order to help the constituent solve the problem. The categorisation of incidents helps GOVCERT.LU to plan actions to resolve the incident and helps the constituent respect the reporting time frame.

The categorisation of incidents also supports the definition of standard incident response procedures for each type of incident.

1.2 Purpose

The aim of this procedure is to define:

- the incident categories used by GOVCERT.LU
- how a category is allocated to an incident
- the reporting time frame for constituents for each type of incident

1.3 Scope

This procedure concerns the GOVCERT.LU ticketing tool, its members and its constituents.

1.4 References

1. *PRS401 - Incident Management Process*

1.5 Abbreviations

Abbreviation	Definition
CERT	Computer Emergency Response Team
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
ENISA	European Union Agency for Cybersecurity
GOVCERT.LU	Governmental CERT of Luxembourg
ICMP	Internet Control Message Protocol
IDS	Intrusion detection system
IP	Internet protocol
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
VNC	Virtual Network Computing
WPAD	Web Proxy Auto-Discovery Protocol

Table 1: Definitions and Abbreviations

2 Information Security Incident Definition

An information security incident (or incident) is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and preservation of confidentiality, integrity and availability of information.

Event: An Event is an occurrence or change in a particular set of circumstances:

NOTE 1: An event can be one or more occurrences, and can have several causes.

NOTE 2: An event can consist of something that does not happen.

NOTE 3: An event can sometimes be referred to as an “incident” or an “accident”.

Information security event: An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be relevant to security.

3 Incident Categories

For each category of incident, a *reporting time frame* applies for the concerned constituent. The *reporting time frame* is the time frame within which the constituent should report the incident. Once this time frame has exceeded, GOVCERT.LU cannot guarantee that the incident will be resolved efficiently.

The *reporting time frame* is defined according to the sensitivity of the targeted system(s) as follows:

- Critical system: a critical system is a system, application, data, or other resources that is essential to the survival of an organisation. When a critical system fails or is interrupted, core operations are significantly impacted.
- Non critical system: system, application, data, or other resources which do not have strong impact on the good operation of the constituency if compromised.

Name & Description	Reporting Time Frame After Discovery	
	Critical system	Non critical system
1 - Information Content Security Unauthorised access to information, modification of information or loss of data: - by abusing stolen login credentials for a system or application - intercepting traffic - gaining access to physical documents - a ransomware encrypting data - loss of data caused by hard disk failure or physical theft	Within 1 hour.	Within 4 hours.
2 - Intrusions Compromise of a system or an application where the attacker: - gained administrative privileges - using an unprivileged (user/service) account - by exploiting (un-)known software vulnerabilities, e.g. SQL[1] injection Physical intrusion, e.g. into corporate building or data-centre.	Within 1 hour.	Within 1 hour.
3 - Malicious Code System infected with malware, e.g. PC, smartphone or server infected with a rootkit or which contacted a command-and-control (C2) server. URI used for malware distribution or malware configuration, e.g. a URL included in fake invoice or web-injects for a banking trojan.	Within 1 hour if widespread across organisation otherwise 1 day.	Within 4 hours if widespread across organisation otherwise 1 day.
4 - Availability Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down, SYN-Floods or UDP-based reflection attacks. Physical sabotage or outage, e.g cutting wires or malicious arson or caused by air condition failure or natural disaster.	Within 2 hours if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.	Within 4 hours if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.
5 - Fraud - Using resources for unauthorised purposes including profit-making ventures. - Offering or installing copies of unlicensed commercial software or other copyright protected materials (Warez). - Impersonation of the identity of another in order to benefit from it. - Masquerading as another entity in order to persuade the user to reveal private credentials (phishing).	Within 4 hours.	Within 1 day.
6 - Abusive Content - SPAM, IoC's referring to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc. - Discrimination of somebody - Child Sexual Exploitation, Sexual content, glorification of violence, etc.	Within 4 hours.	Within 1 day.

[1] Structured Query Language

Name & Description	Reporting Time Frame After Discovery	
	Critical system	Non critical system
7 - Information Gathering - Attacks that send requests to a system to discover weaknesses. e.g. fingerd, DNS[2] querying, ICMP[3], SMTP[4], port scanning. - Observing and recording of network traffic (wiretapping). - Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).	Within 1 hour.	Within 2 weeks.
8 - Intrusion Attempts - An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE[5] name (e.g. buffer overflow, backdoor, cross site scripting, etc.) - Multiple login attempts (Guessing / cracking of passwords, brute force). - An attack using an unknown exploit.	Within 1 hour.	Within 2 weeks.
9 - Vulnerable - Publicly accessible services offering weak crypto (e.g. web servers susceptible to POODLE/FREAK attacks). - Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks (e.g. open DNS resolvers). - Potentially unwanted publicly accessible services (e.g. Telnet, RDP[6] or VNC[7]). - Publicly accessible services potentially disclosing sensitive information (e.g. SNMP[8] or Redis). - A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (e.g. WPAD[9], outdated operating system version, etc.).	Within 6 hours.	Within 1 week.
10 - Other All incidents which do not fit in one of the given categories should be put into this class or the incident is not categorised.	Within 6 hours.	Within 1 day.
11 - Test Meant for testing.	Not applicable.	Not applicable.

Table 2: Information Security Incident Categories

The categories and attacks are based on the categories proposed by ENISA[10] in https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

[2] Domain Name System

[3] Internet Control Message Protocol

[4] Simple Mail Transfer Protocol

[5] Common Vulnerabilities and Exposures

[6] Remote Desktop Protocol

[7] Virtual Network Computing

[8] Simple Network Management Protocol

[9] Web Proxy Auto-Discovery Protocol

[10] European Union Agency for Cybersecurity

3.1 Category Allocation

Table 2 describes all the categories of incidents. A category is allocated by constituent and GOVCERT.LU to an incident according to the following flow chart:

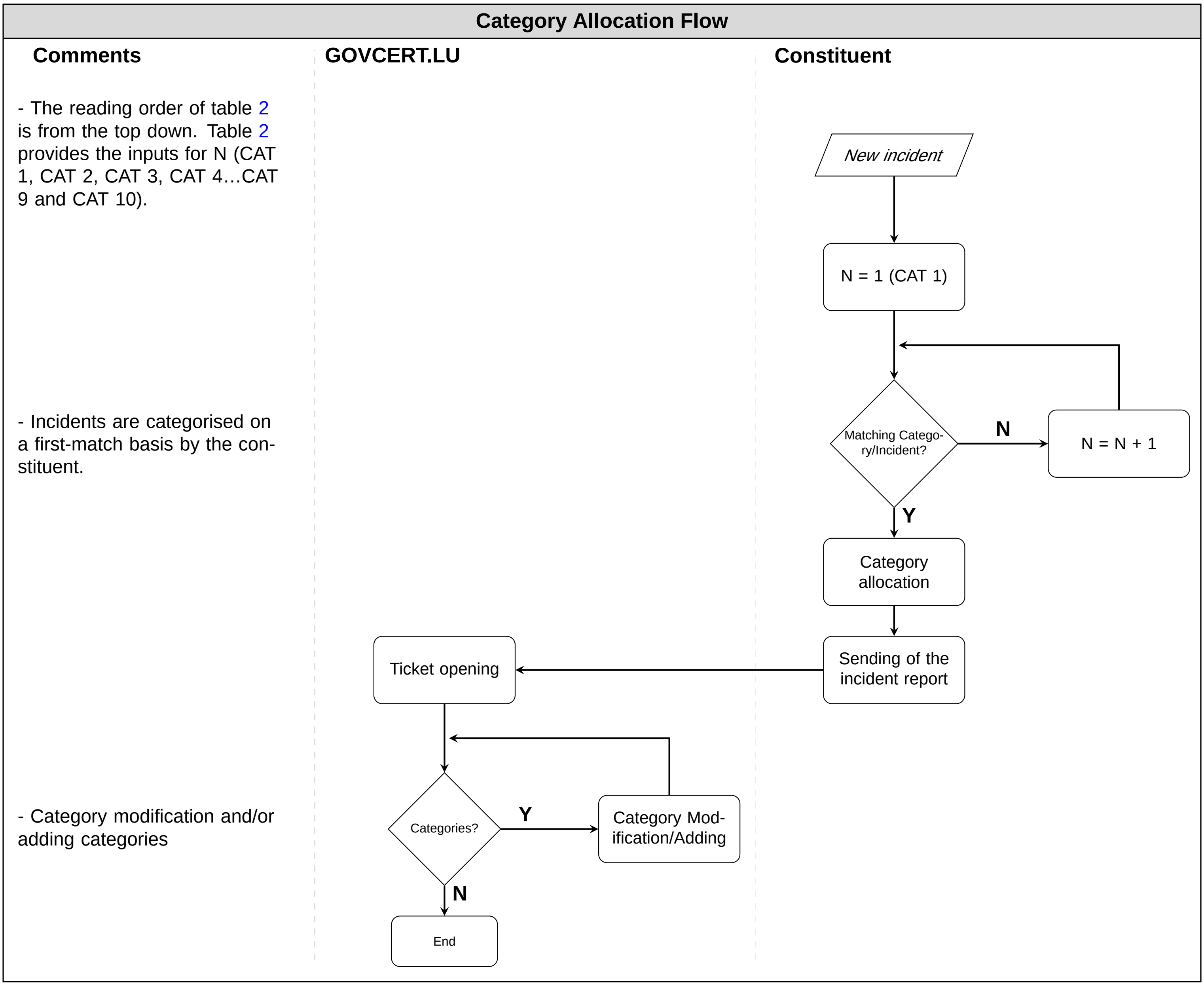
Category Allocation Flow
Comments
GOVCERT.LU
Constituent
- The reading order of table 2 is from the top down. Table 2 provides the inputs for N (CAT 1, CAT 2, CAT 3, CAT 4…CAT 9 and CAT 10).
- Incidents are categorised on a first-match basis by the constituent.
- Category modification and/or adding categories
New incident
N = 1 (CAT 1)
Matching Category/Incident?
N
N = N + 1
Y
Category allocation
Sending of the incident report
Ticket opening
Categories?
Y
Category Modification/Adding
N
End

Figure 1: Category Allocation Flow

The constituent choses the category that fits best such as described in figure 1. During the *identification phase*[11]

[11] See *PRS401 - Incident Management Process*

GOVCERT.LU can (if judged necessary) change this category (false encoding by the constituent) and/or add others categories.