Incident Categories (Public)

Version 3.0 - 2016.01.19 (Final)

Procedures (PRO 303)

TLP: TLP:WHITE

Classification: PUBLIC

Department: GOVCERT.LU

Contents

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

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 timeframe.

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 timeframe 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. *PRO301 - Incident Reporting Guidelines for Constituents*
2. *PRS401 - Incident Management Process*
3. *CSIRT Case Classification - Example for Enterprise CSIRT*. URL: http://www.first.org/_assets/resources/guides/
4. *SP800-61: Computer Security Incident Handling Guide*. Aug. 2012. URL: http://csrc.nist.gov/publications/
5. *US CERT Incident categories*. URL: http://www.us-cert.gov/government-users/reporting-requirements

1.5 Definitions and Abbreviations

Abbreviation	Definition
NIST	National Institute of Standards and Technology
CAT	Incident category
AV	Antivirus

Table 1: Definitions and Abbreviations

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

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 timeframe* applies for the concerned constituent. The *reporting timeframe* is the timeframe within which the constituent should report the incident. Once this timeframe has exceeded, GOVCERT.LU cannot guarantee that the incident will be resolved efficiently.

The *reporting timeframe* 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.

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

Warning: When updating this table; please update also the table 2 in the *PRO301 - Incident Reporting Guidelines for Constituents*

Category	Name	Description	Reporting Timeframe	
			Critical system	Non critical system
CAT 1	Compromised information	Successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.	Within one (1) hour of discovery/detection.	Within four (4) hours of discovery/detection.
CAT 2	Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.	Within one (1) hour of discovery/detection.	Within one (1) hour of discovery/detection.
CAT 3	Unauthorised Access	In this category an individual (internal or external) gains logical or physical access without permission to a national or local network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.	Within four (4) hours of discovery/detection.
CAT 4	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Organisations are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.	Within one (1) hour of discovery/detection if widespread across organization otherwise one (1) day.	Within four (4) hours of discovery/detection if widespread across organisation otherwise one (1) day.
CAT 5	(Distributed) Denial of Service	An attack that successfully prevents or impairs the normal authorised functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.	Within four (4) hours of discovery/detection if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

Category	Name	Description	Reporting Timeframe	
			Critical system	Non critical system
CAT 6	Theft or Loss	Theft or loss of sensitive equipment (Laptop, hard disk, media etc.) of organisation.	Within one (1) day of discovery/detection.	Within one (1) week of discovery/detection.
CAT 7	Phishing	Use of fraudulent computer network technology to entice organisation's users to divulge important information, such as obtaining users' bank account details and credentials by deceptive emails or fraudulent web site	Within four (4) hours of discovery/detection.	Within one (1) day of discovery/detection.
CAT 8	Unlawful activity	Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.	Within six (6) hours of discovery/detection.	Within one (1) day of discovery/detection.
CAT 9	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify an organisation computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Within one (1) hour of discovery/detection.	Within two (2) weeks of discovery/detection.
CAT 10	Policy Violations	Deliberate violation of Infosec policy such as: - Inappropriate use of corporate asset such as computer, network, or application. - Unauthorised escalation of privileges or deliberate attempt to subvert access controls.	Within six (6) hours of discovery/detection.	Within one (1) week of discovery/detection.

Table 2: Information Security Incident Categories

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

The categories and attacks are based on a mix of categories proposed by NIST (*SP800-61: Computer Security Incident Handling Guide*), FIRST (*CSIRT Case Classification - Example for Enterprise CSIRT*) and US-CERT (*US CERT Incident categories*).

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:

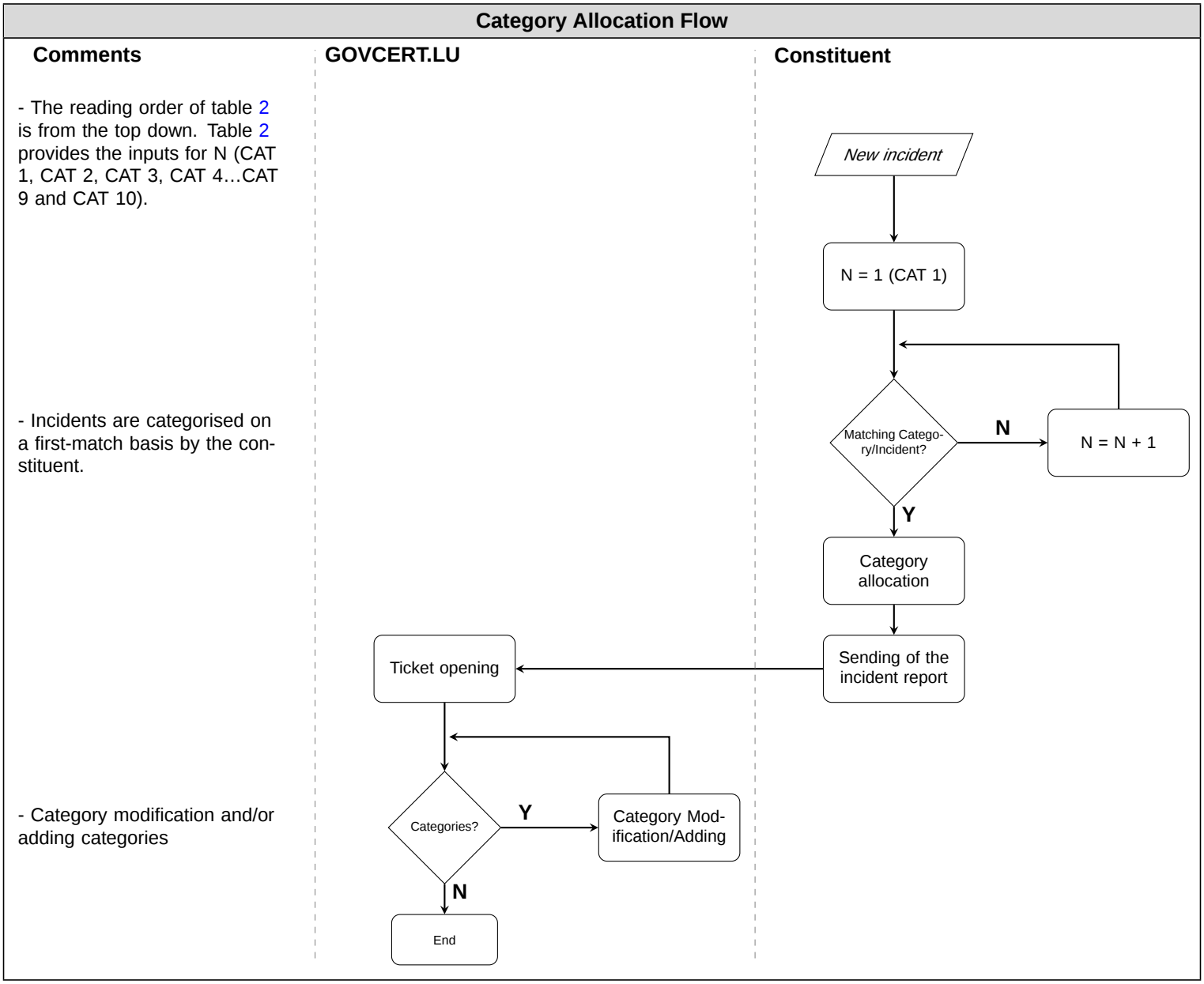

Figure 1: Category Allocation Flow

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu

The constituent choses the category that fits best such as described in figure 1. During the *identification phase*[1] GOVCERT.LU can (if judged necessary) change this category (false encoding by the constituent) and/or add others categories.

[1] See *PRS401 - Incident Management Process*

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.govcert.lu
info@govcert.etat.lu