DSO ENTITY
DSOs FOR EUROPE

European Network of Transmission System Operators for Electricity
entsoe

Supporting document

for the Cyber-attack classification scale Methodology

1 Introduction

Under Article 37 of the Network Code for Cybersecurity (NCCS), the European Network of Transmission System Operators for Electricity (ENTSO-E) in cooperation with the EU DSO entity (DSO Entity) has developed a proposal for a methodology for a cyber-attack classification scale. This supporting document has been developed jointly by ENTSO-E and DSO Entity to accompany this methodology. It provides all interested parties with information about the rationale for the cyber-attack classification scale methodology, outlining why certain standards have been selected.

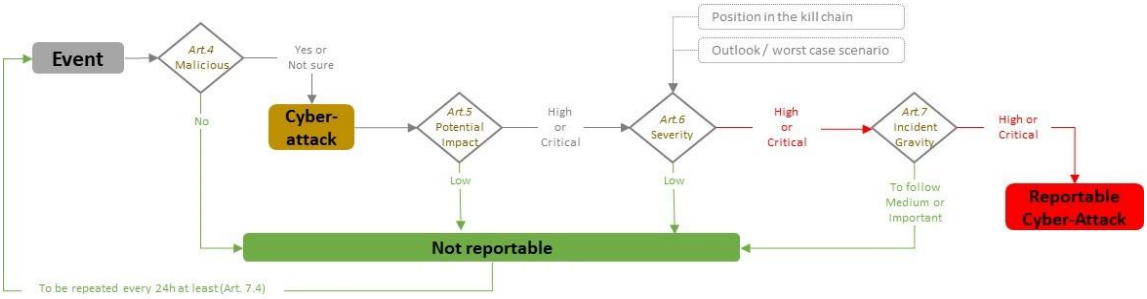
1.1 Legal status of this document

This document accompanies the cyber-attack classification scale methodology and is provided for information purposes only. Consequently, this document is not legally binding.

2 Cyber-attacks Classification Scale Methodology

The document contains the cyber-attack classification scale methodology to determine whether an incident is identified as a reportable cyber-attack according to the NCCS (see Figure 1). The classification of an event as a reportable cyber-attack is done according to the following criteria: potential impact, root cause, severity, and gravity.

The determination of the potential impact, severity, and gravity of a cyber-attack are defined in Article 37(8) of the NCCS. The root cause estimation has been included to enable the entities to decide whether an event is a cyber-attack, which is a pre-requisite of estimating the severity of the cyber-attack.



Tactics / Trying to	Severity of the Attack		Potential Impact: Low PI	Potential Impact: High PI	Potential Impact: Critical PI
Reconnaissance Ressource Development Initial acces	Low Severity	the attackers are trying to get access to one or more asset.	To follow gravity	Medium gravity	Important gravity
Execution Persistence Privilege escalation Defense Evasion Credential access Discovery	High Severity	the attackers have at least limited access to one or more assets	Medium gravity	High gravity	High gravity
Lateral Movement Collection Command and control Exfiltration Inhibit Response Function Impair Process Control Impact	Critical Severity	more than one assets are impacted by lateral movement, or [the attackers] appear to be able to interrupt the process or perpetuate actions on one or multiple assets to destabilize the entity	Important gravity	High gravity	Critical gravity

Figure 1 Process to determine if an event is a cyber-attack according to the NCCS.

Article 4: Estimation of the root cause

Article 4 describes the determination of the root cause of the detected incident. The objective is to determine if the event is malicious or not.

When an anomalous event is detected by an entity, the root cause should be estimated. The outcome can be one of the three possibilities: not malicious, malicious, or uncertain. Events with a not malicious root cause should not be considered in the NCCS scope.

Some examples of not malicious events are:

- Anomalies caused by authorised changes to the software, hardware, or configuration.
- Software bugs after they are verified by the vendor.
- Incidents with a clear natural cause, like fire or water in the data centre.

Some examples of malicious events are:

- Ransomware, viruses, or intrusions into the system.
- Anomalies caused by unauthorised changes to the software, hardware, or configuration.
- Software backdoors are considered malicious if their malicious intent has been verified by the

vendor, since it can be an indication of a successful supply chain attack.

Some examples of uncertain events are:

- Anomalies where it is unclear if they are caused by unauthorised changes to the software, hardware, or configuration.
- Software vulnerabilities not addressed by the vendor yet.

Events classified as malicious or as uncertain, will be treated as if they are cyber-attacks.

If an entity reports a cyber-attack that has been initially classified as "uncertain root cause", but at a later stage it becomes clear that the root cause is "not malicious", the entity may inform the CSIRTs and NCAs of the updated classification and the reporting for that event will, therefore, end.

Article 5: Determination of the potential impact of the cyber-attack

Article 5 describes the methodology for the determination of the potential impact of the cyber-attack (see Article 37(8)(a) of the NCCS). Potential impact refers to the potential operational consequences of a cyber-attack. The potential impact is determined by the impact classification of assets in a perimeter, which in turn depends on the processes they support. The potential impact scale is derived from ENTSO-E's Incident Classification Scale.

Assets are classified in the high-impact or critical-impact perimeters following Article 26(4)(c) of the NCCS during the entity risk assessment based on the high-impact or critical-impact processes identified during the Union-wide Risk Assessment. By doing so, the entities also determine the impact on the cross-border electricity flows that their assets can have. Only the assets that support the high-impact and critical-impact businesses processes will be classified in the high-impact or critical-impact perimeters.

To be able to timely determine the impact of an incident, all operational high- or critical-impact assets and all perimeters that have high or critical potential impact have to be documented in an asset register or inventory (see also Article 26(7) of the NCCS) and kept up to date. The entity's CSIRT/CERT should always have access to this register to react promptly in case of any event.

Assets are organised in perimeters. The high-impact perimeter contains high-impact assets, and the critical-impact perimeter contains critical-impact assets. There is a risk that an attacker will move from one asset to another laterally within this perimeter and eventually to other perimeters.

That an asset can directly reach another asset means that they are logically connected to each other. This means, for example, that communication between both assets is allowed because they are in the same network or because a firewall allows that traffic.

Article 6: Estimation of the severity of the cyber-attack

Article 6 describes the estimation of the severity of the cyber-attack (see Article 37(8)(b) of the NCCS). The objective is to estimate the stage of the cyber-attack in order to assess how far the attackers are in the entity's environment.

Article 6 defines the steps to estimate the severity of this cyber-attack. The determination of the severity is done according to the MITRE ATT&CK Enterprise and ICS tactics [1] [2]. Depending on the objective of the attacker at the time of the assessment, a severity will be given. The severity can be low, medium, or high.

The estimation of the severity will later be used to derive the overall gravity of the cyber-attack by combining it with its potential impact.

This estimation can be done based on the knowledge of the experts in the entity or through a more analytical approach that uses a set of pre-defined criteria to assess the severity of the incident. These

criteria can comprise metrics like the number of systems that are compromised, the speed of the attack, and the evidence of crucial data exfiltration or the execution of malicious commands.

- **Low Severity**

  During the initial reconnaissance the attackers are gathering intelligence about the target entity's infrastructure, assets, and operations. This includes researching their IT systems, identifying vulnerabilities, and understanding their security posture. This can be done, for instance by performing scanning activities. The probable goal of the attackers at this stage is to plan and prepare their malicious activities.

- **Medium Severity**

  The attackers have successfully penetrated the target entity's systems, gaining access to at least one asset. They may attempt to establish a persistent presence in the compromised system, obtain elevated privileges, expand their control over the system, evade discovery and maintain their anonymity, collect credentials to gain further access, or use malicious tools to gather information about the compromised system and the entity's network infrastructure.

- **High severity**

  The attackers show activities across boundaries bypassing security controls. They have successfully compromised multiple systems within the entity's network and/or obtained access to sensitive information about the entity's system, network, or operation to pursue their malicious intentions. Particularly targeting information that can be used to disrupt, steal, or damage the entity. They may use compromised systems to execute commands and exfiltrate data. The attackers may demonstrate clear intent to disrupt, disable, or modify the entity's critical systems, processes, or data.

Article 7: Cyber-attack gravity classification

Article 7 describes the assessment of the gravity of the cyber-attack by considering the results of the determination of the potential impact described in article 5 and the estimation of the severity described in article 6 (see Figure 2).

As defined by the NCCS, there are five possible gravity levels. Cyber-attacks with high or critical gravity shall be reported according to the NCCS.

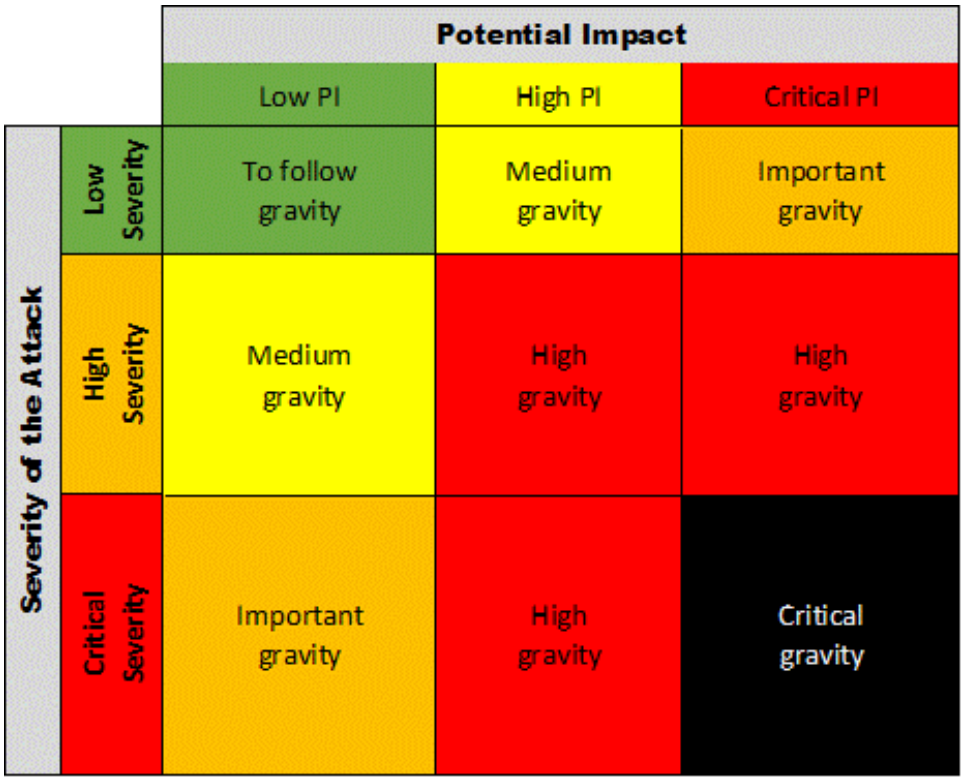


Figure 2 Matrix to determine the gravity of a cyber-attack

3 Annex I: Gravity matrix and process flow

Annex I of the cyber-attack classification scale methodology illustrates the steps to follow to determine if an event is a reportable incident. Annex I also includes an illustration of the gravity matrix and the steps of the kill chain (see Figure 1 and Figure 2).