IDMEF V2

(Incident Detection Message Exchange Format)

for Critical Infrastructures and OES

Executive Summary:

The Incident Detection Message Exchange Format (IDMEFv2) was designed to meet the needs of protecting critical infrastructures, including mobile ones, against hybrid and complex attacks. Thus, it meets the security supervision needs of the nation's vital interests both intra-site and for the hypervision of Operator of Essential Services (OES). The IDMEFv2 format is based on the concepts of its predecessor IDMEFv1 (RFC 4765) defined nearly 20 years ago, complementing it with today's new concepts, in particular the massive and growing use of connected objects in motion under the constraint of natural phenomena. Not only does this format meet the internal needs of critical infrastructures, but it also allows for the consolidation of the hypervision of these infrastructures within a central platform as well as collaboration and the exchange of secure information on threats between states of the European Union. The first drafts of the format were published to the IETF in 2022. The format is currently being tested and validated in several European research projects. The final version is planned for early 2027. Given the geopolitical issues shaking Europe at the beginning of 2025, it is urgent that European security agencies and actors get involved to support this adjustment and adoption phase alongside research teams.

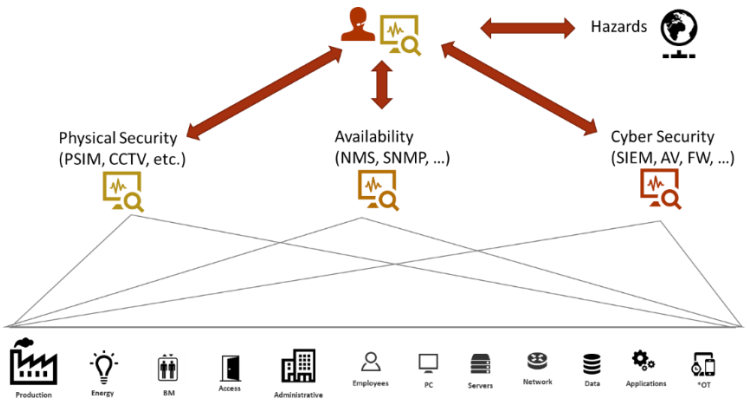
IDMEFv2 Format: History

The IDMEFv2 format (Incident Detection) builds on some of the concepts of its predecessor, IDMEFv1 (Intrusion Detection), expanding it to cover all types of incidents (cyber and physical), integrating the dimension of availability, and adding the potential interference of natural elements on system security. This is especially crucial when these systems are embedded in mobile architecture outside protected, secure, and cooled data centers. The development of this format results from a series of research projects, the first of which, SECEF1 (SECurity Exchange Format), was funded by French ministry of defense and sponsored by French national security agency in 2015. The goal of this initial project was to promote the IDMEFv1 format within administrations and the military, and its conclusions highlighted the need to evolve the format. In 2020, collaboration between the French SECEF2 project and the European H2020 project (7Shield.eu) on protecting critical infrastructure against hybrid and complex attacks underscored the need to broaden the format to include all types of physical and natural incidents. This led to the IDMEFv2 standardization initiative (www.idmefv2.org) with the IETF. Today, research continues within the European Safe4SOC project (Standard Alert Format Exchange for SOCs) under the leadership of the research teams at Telecom SudParis, with work set to continue for another two years.

IDMEFv2: Technical Implementation

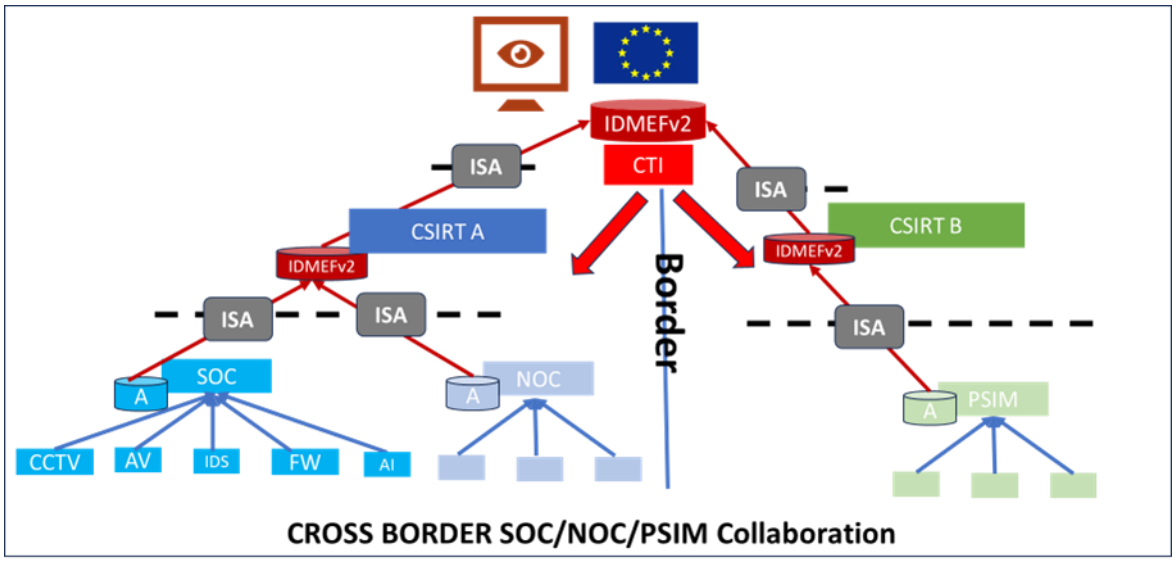
To facilitate its adoption, IDMEFv2 relies on simple and universal concepts. Technically, the drafts define a JSON message implementation transported over HTTPS. Conceptually, the format prioritizes simplicity over exhaustiveness with simple extension mechanisms. To date, it is the only incident format initiative that combines digital and physical spaces while also addressing natural incident management.

IDMEFv2 and critical infrastructures



The first official drafts of the IDMEFv2 format were specified within a European project for the protection of critical infrastructures with pilot sites deployed on ground segments. These infrastructures face cyber risks (viruses, intrusions, etc.), physical risks (intrusions, thefts, drones, etc.) and are sometimes also exposed to climatic hazards (snowstorms for a ground segment in Finland, forest fires for a ground segment in Greece, etc.). As a result, the format is now capable of describing all types of cyber, physical and natural incidents that impact the security but also the availability, too often treated separately, of platforms.

The Safe4Soc project reinforces the hypervision aspects by working specifically on the connection of several SOCs equipped with proprietary monitoring systems (SIEM) to a central IDMEFv2 monitoring SOC, a SOC of SOCs. IDMEFv2 thus makes it possible to envisage the hypervision of national infrastructures within a centralized platform, thus offering a global vision but also possibilities for analyzing global data with a view to creating new "Threat Intelligence". The Safe4Soc project also develops the notion of "Information Sharing Agreement" using a data filtering and security gateway. The objective is to ensure that each SOC/NOC/PSIM connected to the central system only shares the information necessary for the mutualization of monitoring without revealing sensitive information. This filtering is done within a gateway that deletes, anonymizes or encrypts the information according to the agreements between the two parties. This functionality responds, among other things, to the needs for partitioning and the need to know that centralized hypervision systems for our vital systems could require, particularly in the case of multi-nation systems.



In the diagram above, the ISA modules represent the possible filtering of information shared by SOCs from national SOCs to a European SOC, making it possible to detect combined attacks on several operators at national and European level, as well as the sharing of new “Threat Intelligence”.

For More Information

http://www.idmefv2.org: IDMEFv2 Task Forces

https://github.com/IDMEFv2: Open-source format manipulation tools

https://safe4soc.eu/: Security Alert Format Exchange for SOCs

CONTACT

Gilles.Lehmann@telecom-sudparis.eu

Coordinator of the IDMEFv2 and Safe4SOC projects

**SOC: Security Operation Center, NOC: Network Operation Center, PSIM: Physical Security Information Management, SIEM: Security Information & Event Management*