IDMEF V2

(Incident Detection Message Exchange Format)

for National and European Defense

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. It thus meets the security supervision needs of the armed forces in the broad sense, i.e. covering confidentiality, integrity and physical and cyber availability. The IDMEFv2 format is based on the concepts of its predecessor IDMEFv1 (RFC 4765) defined nearly 20 years ago, supplementing it with today's new concepts, in particular the massive and growing use of connected objects in motion under the possible influence of natural phenomena. This format not only meets the internal needs of the French army but also for the joint supervision (or Hypervision) of inter-allied defense systems. The first drafts of the format were published to the IETF in 2022. The format is currently in the testing and validation phase in several European research projects. The final version is planned for the beginning of 2027. Given the geopolitical issues shaking Europe at the beginning of 2025, it is urgent that the Ministry and the defense industry get involved to support this adjustment and adoption phase alongside the research teams.

IDMEFv2 Format: History

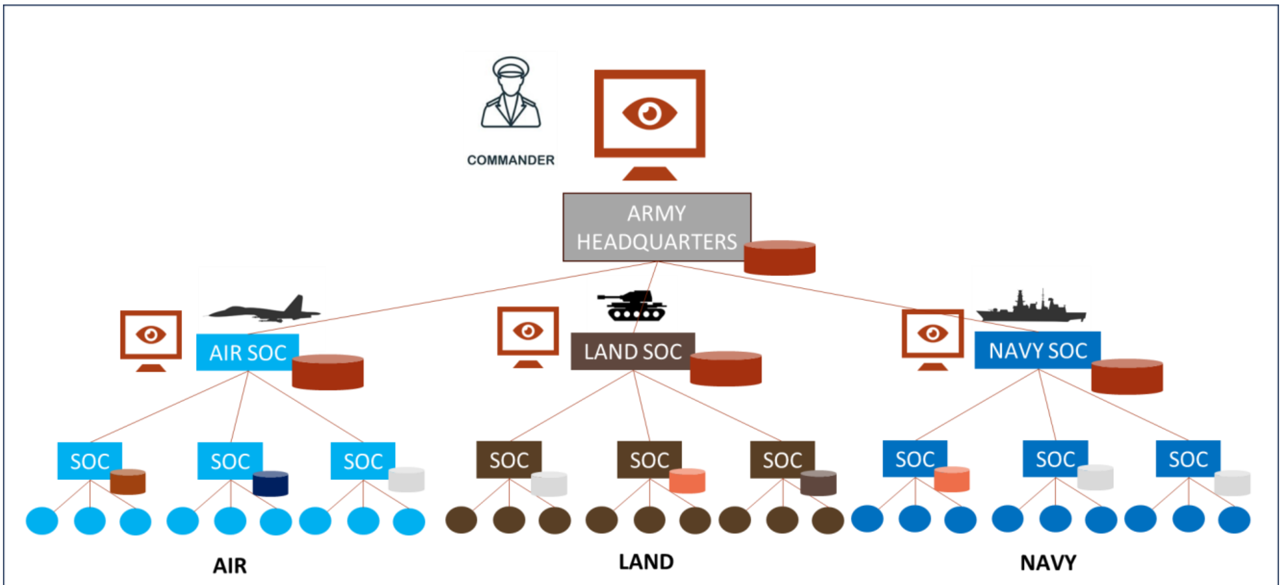
The IDMEFv2 format (Incident Detection) builds on some of the concepts of its predecessor, IDMEFv1 (Intrusion Detection), expanding it to cover all types of incidents (cyber and physical), integrating the dimension of availability, and adding the potential interference of natural elements on system security. 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.

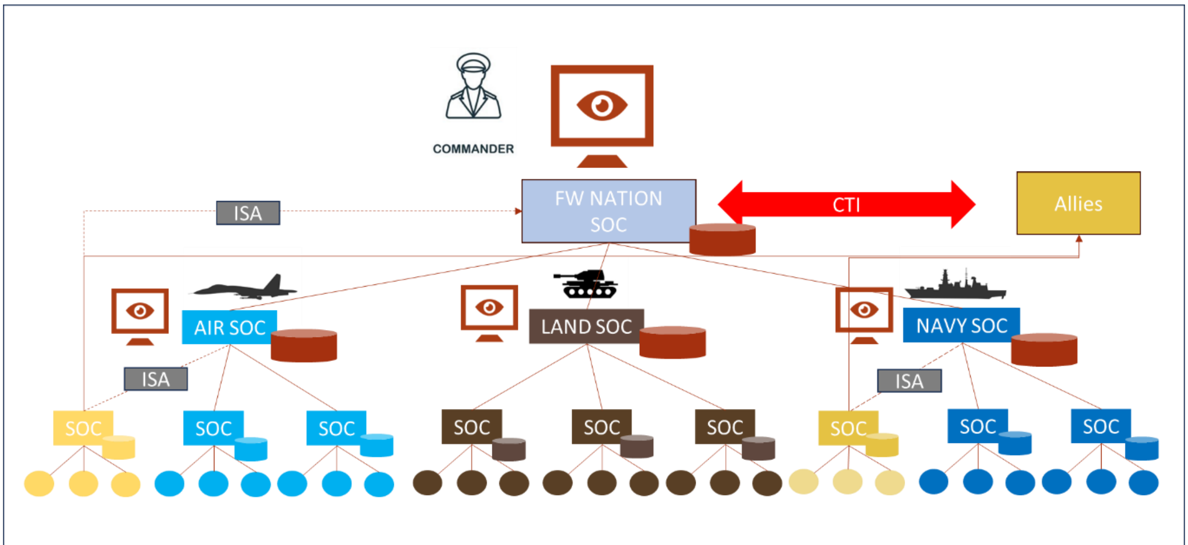
IDMEFv2 and the Defense Sector

IDMEFv2 was initially designed by expert teams in incident detection from the critical systems integration industry in the defense sector. It is designed to address the NOC-SOC and now PSIM monitoring challenges of numerous military systems, as well as the interconnection issues of forces within NATO operations. In its design, IDMEFv2 meets the challenges of standard and secure multisite heterogeneous monitoring consolidation. The Safe4SOC project strengthens these aspects by working specifically on connecting multiple SOCs equipped with proprietary supervision systems (SIEM) to a central IDMEFv2 supervision SOC, a SOC of SOCs. Given the high heterogeneity of military systems, IDMEFv2 ensures their monitoring and can be used across different military branches and for joint force consolidation.



Safe4Soc Army Use Case

Moreover, the Safe4SOC project is developing the concept of an "Information Sharing Agreement" through a data filtering and security gateway. The goal is to ensure that each SOC/NOC/PSIM connected to the central system shares only the information necessary for mutual monitoring without revealing sensitive data. This filtering is performed by a gateway that removes, anonymizes, or encrypts information based on agreements between the two parties. This feature addresses the need for compartmentalization and the "need-to-know" principle, which is particularly vital for joint military operations.



Safe4Soc Framework nation Concept (NATO)

In the diagram above, the ISA modules represent the potential filtering of information shared by "allied" SOCs toward the lead nation SOC in the context of NATO or European Defense operations.

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*