IDMEF V2

(Incident Detection Message Exchange Format)

pour la Défense Nationale et Européenne

Executive summary:

Le format de détection d'incidents IDMEFv2 (Incident Detection Message Exchange Format) a été conçu pour répondre aux besoins de protection des infrastructures critiques, y compris mobiles, contre les attaques hybrides et complexes. Ainsi il répond aux besoins de supervisions de sécurité des armées au sens large c'est-à-dire couvrant la confidentialité, l'intégrité et la disponibilité physique et cybernétique. Le format IDMEFv2 s'appuie sur les concepts de son prédécesseurs IDMEFv1 (RFC 4765) défini il y a près de 20 ans en le complétant avec les nouveaux concepts d'aujourd'hui et en particulier l'utilisation massive et croissante d'objets connectés en mouvement sous l'influence éventuelle de phénomènes naturels. Non seulement ce format répond aux besoins internes de l'armée française mais également pour la supervision (ou Hypervision) conjointe de systèmes de défense interalliés. Les premières ébauches du format ont été publiées auprès de l'IETF en 2022. Actuellement le format est en phase de test et validation dans plusieurs projets de recherche européens. La version définitive est prévue pour le début de l'année 2027. Compte-tenu des sujets géopolitiques qui secouent l'Europe en ce début d'année 2025, il est urgent que le ministère et les industriels de la défense s'impliquent pour soutenir cette phase de réglage et adoption au côté des équipes de recherche.

Le format IDMEFv2 : historique

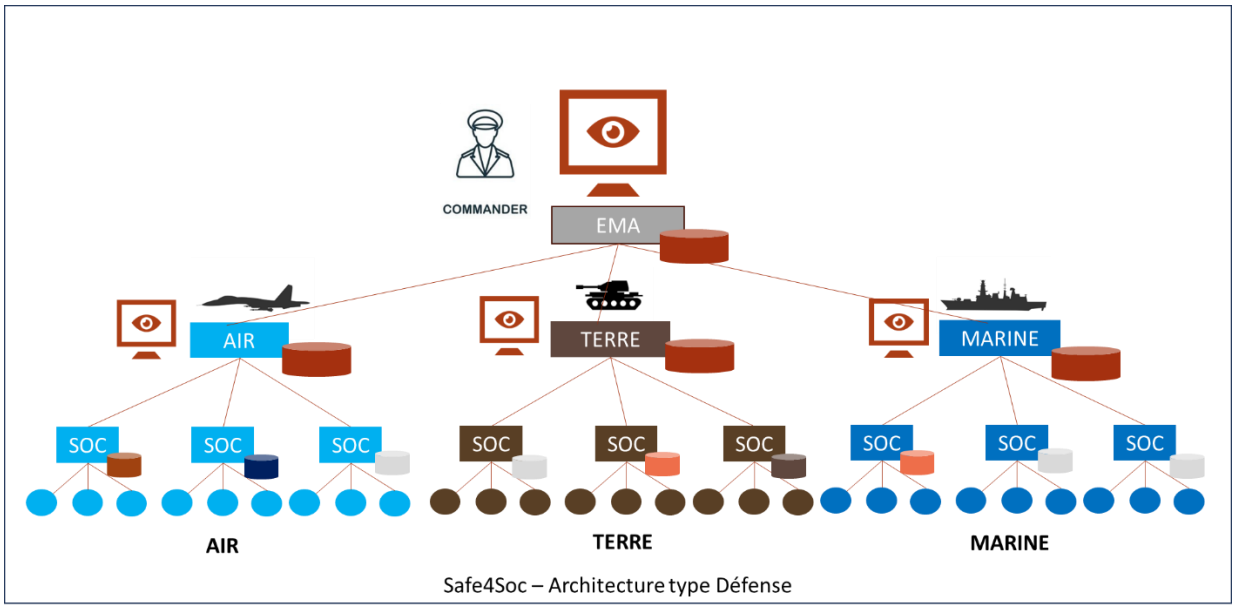
Le format IDMEFv2 (Incident Detection) s'appuie sur certains concepts de son prédécesseur IDMEFv1 (Intrusion Detection) en l'élargissant à tous types d'incidents (Cyber et Physique), en y associant la dimension disponibilité et en y rajoutant l'interférence possible des éléments naturels sur la sécurité des systèmes. En particulier, lorsque ces systèmes sont embarqués au sein d'architectures mobiles hors des datacenters protégés, sécurisés et réfrigérés. La définition de ce format est le résultat d'une suite de projets de recherche dont le premier SECEF1 (SECurity Exchange Format) a été financé par un RAPID DGA et sponsorisé par l'ANSSI en 2015. L'objectif de ce premier projet était la promotion du format IDMEFv1 au sein des administrations et de l'armée et ses conclusions ont mis en évidence la nécessité de faire évoluer le format. En 2020, la collaboration entre le projet FUI SECEF2 et un projet H2020 (7Shield.eu) de protection d'infrastructures critiques contre des attaques hybrides et complexes a mis en avant la nécessité d'élargir le format à tous les types d'incidents physiques et naturels. L'initiative IDMEFv2 (www.idmefv2.org) de standardisation auprès de l'IETF d'une nouvelle version du format est alors lancée. Aujourd'hui, c'est au sein d'un projet de recherche Européen Safe4SOC (Standard Alert Format Exchange for SOCs) que les travaux se poursuivent pour encore deux ans sous la responsabilité des équipes de recherches de Telecom SudParis.

IDMEFv2 : implémentation technique

Pour faciliter son adoption, IDMEFv2 s'appuie sur des concepts simples et universels. Techniquement, les drafts définissent une implémentation de message JSON transporté sur HTTPs. Conceptuellement, le format privilégie la simplicité à l'exhaustivité avec des mécanismes simples d'extension. C'est à ce jour la seule initiative de format d'incident qui combine l'espace numérique avec l'espace physique ainsi que la possibilité de traiter des incidents naturels.

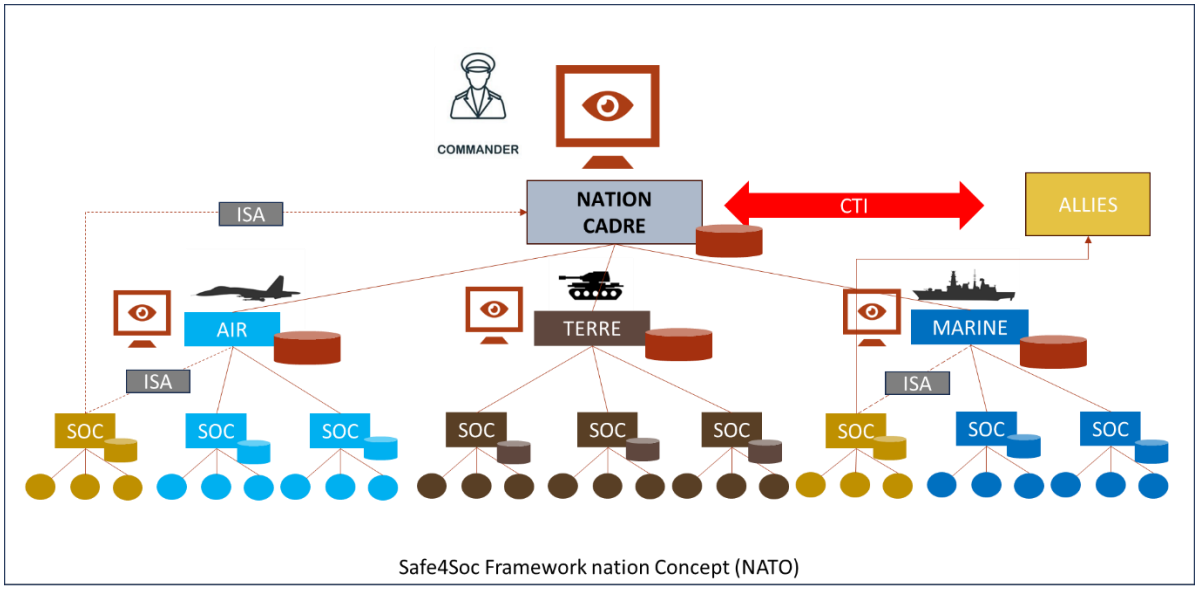
IDMEFv2 et le monde de la Défense

IDMEFv2 a initialement été conçu par des équipes expertes en détection d'incidents issues de l'industrie de l'intégration de systèmes critiques dans le domaine de la Défense. IDMEFv2 est conçu pour répondre aux problèmes de supervision NOC-SOC, et aujourd'hui PSIM, de nombreux programmes tels que *RIFAN2, *RDIP, *SIA et autre Intraced/Intradef ainsi que sur des problématiques d'interconnexion de nos forces avec l'OTAN. Dans sa conception, le format IDMEFv2 répond ainsi à ces problématiques de consolidation standard et sécurisée de supervision multisites hétérogènes. Le projet Safe4Soc vient renforcer ces aspects en travaillant spécifiquement sur la connexion de plusieurs SOCs dotés de systèmes de supervision (SIEM) propriétaires à un SOC IDMEFv2 de supervision central, un SOC de SOCs. Les systèmes des armées sont très hétérogènes et le format IDMEFv2 permet d'en assurer la supervision. Ainsi ce format peut être utilisé au sein des différents corps d'armée mais également dans une optique de consolidation interarmées.



Safe4Soc – Architecture type Défense

Le projet Safe4Soc développe d'autre part la notion de « Information Sharing Agreement » à l'aide d'une passerelle de filtrage et sécurisation des données. L'objectif et de s'assurer, pour chaque SOC/NOC/PSIM connectés au système central, de ne partager que les informations nécessaires à la mutualisation de la supervision sans dévoiler d'informations sensibles. Ce filtrage se fait au sein d'une passerelle qui supprime, anonymise ou chiffre les informations en fonction des accords entre les deux parties. Cette fonctionnalité répond entre autres aux nécessités de cloisonnement et de besoin d'en connaître que connaissent les armées en particulier lors d'opération conjointes.



Safe4Soc Framework nation Concept (NATO)

Sur le schéma ci-dessus les modules ISA représentent le filtrage éventuel des informations partagées par des SOCs « alliés » vers le SOC de la nation cadre dans le cadre d'une opération OTAN ou de Défense Européenne.

Pour plus d'information

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

https://github.com/IDMEFv2 : Outils open-source de manipulation du format

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

CONTACT

Gilles.Lehmann@telecom-sudparis.eu

Coordinateur des projets IDMEFv2 et Safe4Soc

**SOC: Security Operation Center, NOC : Network Operation Center, PSIM: Physical Security Information Management, SIEM: Security Information & Event Management, RIFAN: Réseau IP de la force Aéronavale, RDIP : Réseau de Déserte IP, Système d'Information des Armées*