IDMEF V2

(Incident Detection Message Exchange Format)

pour la protection des infrastructures critiques et des OIVs.

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 intérêts vitaux de la nation tant intra-sites que pour l'hypervision de ces OIVs et autres OSE. 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 la contrainte des phénomènes naturels. Non seulement ce format répond aux besoins internes des infrastructures critiques, mais il permet également de consolider l'hypervision de ces infrastructures au sein d'une plateforme centrale ainsi que la collaboration et l'échange d'information sécurisée sur les menaces entre états de l'union européenne. 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 les agences de sécurité européennes s'impliquent pour soutenir cette phase de réglage et d'adoption au côté des équipes de recherche.

Le format IDMEFv2 : historique

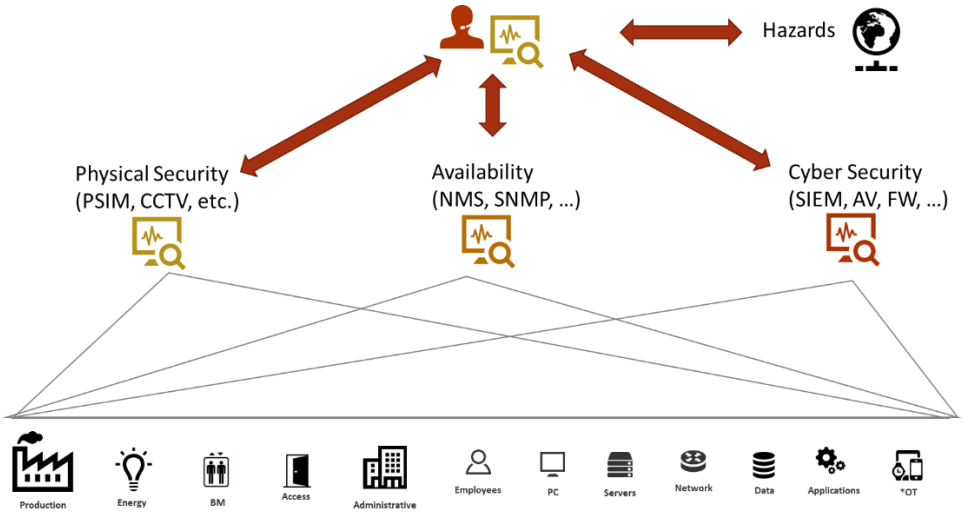
Le format IDMEFv2 (Incident Detection) s'appuie sur certains concepts de son prédécesseur IDMEFv1 (Intrusion Detection) en l'élargissant à tous types d'incidents (Cyber et Physique), en y associant la dimension disponibilité et en y rajoutant enfin l'interférence possible des éléments naturels sur la 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, format qui à l'époque était déjà utilisé au sein de certaines sondes souveraines. En 2020, la collaboration entre le projet FUI SECEF2 et le 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 du projet de recherche Européen Safe4SOC.eu (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

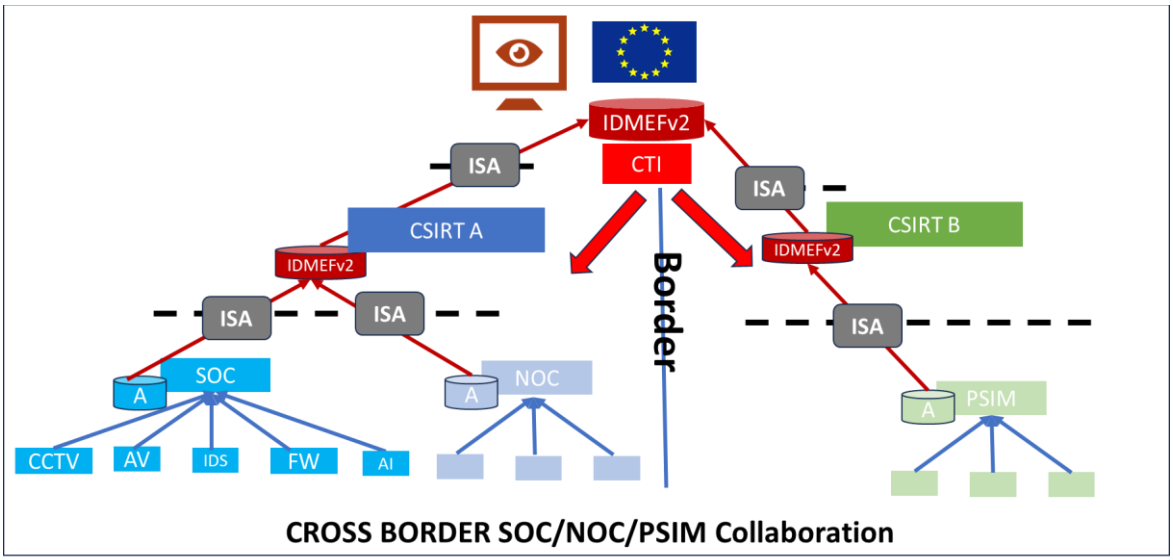
Pour faciliter son adoption IDMEFv2 s'appuie sur des concepts simples et universels. Techniquement, les drafts définissent une implémentation de message JSON transporté sur HTTPs. Conceptuellement, le format privilégie la simplicité à l'exhaustivité avec des mécanismes simples d'extension. C'est à ce 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 les infrastructures critiques

Les premiers drafts officiels du format IDMEFv2 ont été spécifiés au sein d'un projet européen de protection d'infrastructures critiques avec des sites pilotes déployés sur des segments sols. Ces infrastructures font face à des risques cyber (virus, intrusions, ...), des risques physiques (intrusions, vols, drones, ..) et sont parfois également exposées au aléas climatiques (tempêtes de neige pour un segment sol en Finlande, feu de forêt pour un segment sol en Grèce, ...). C'est ainsi que le format est aujourd'hui capable de décrire tout type d'incidents cyber, physique et naturels qui impactent la sécurité mais également la disponibilité, trop souvent traitée séparément, des plateformes.



Le projet Safe4Soc vient renforcer les aspects hypervision 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. IDMEFv2 permet ainsi d'envisager l'hypervision des infrastructures nationales au sein d'une plateforme centralisée offrant ainsi une vision globale mais également des possibilités d'analyse de données globales en vue de création de nouvelles « Threat Intelligence ». 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 pourrait nécessiter des systèmes d'hypervision centralisée de nos systèmes vitaux et en particulier dans le cas de système multi-nations.



Sur le schéma ci-dessus les modules ISA représentent le filtrage éventuel des informations partagées par des SOCs de SOCs nationaux vers un SOC européen permettant de détecter des attaques combinées sur plusieurs opérateurs au niveau national et européens ainsi que le partage de nouvelle « Threat Intelligence »

Pour plus d'information

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

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, OIV:Opérateurs d'Importance Vitale, OSE : Opérateurs de Service Essentiels*