

IDMEF V2

(Incident Detection Message Exchange Format)

nacionalinei ir Europos gynybai

Santrauka (Executive Summary):

Incident Detection Message Exchange Format (IDMEFv2) buvo sukurtas siekiant patenkinti poreikius apsaugoti kritinę infrastruktūrą, įskaitant mobiliąją, nuo hibridinių ir sudėtingų atakų. Taigi, jis atitinka nacionalinių gyvybinių interesų saugumo priežiūros poreikius tiek pačioje teritorijoje, tiek ir vykdant esminių paslaugų operatoriaus (OES) hiperviziją. IDMEFv2 formatas remiasi beveik prieš 20 metų apibrėžto jo pirmtako IDMEFv1 (RFC 4765) koncepcijomis, papildant jas šiuolaikinėmis naujomis koncepcijomis, visų pirma susijusiomis su intensyviu ir augančiu mobilių sujungtų objektų naudojimu esant gamtos reiškinių apribojimams. Šis formatas ne tik atitinka kritinės infrastruktūros vidaus poreikius, bet ir leidžia konsoliduoti šios infrastruktūros hiperviziją centrinėje platformoje, taip pat bendradarbiauti ir keistis saugia informacija apie grėsmes tarp Europos Sąjungos valstybių. Pirmosios šio formato versijos buvo publikuotos IETF 2022 metais. Šis formatas šiuo metu yra testuojamas ir validuojamas keliuose Europos mokslinių tyrimų projektuose. Galutinę versiją planuojama pristatyti 2027 metų pradžioje. Atsižvelgiant į geopolitines problemas, kurios 2025 m. pradžioje sukrėtė Europą, Europos saugumo agentūros ir kiti suinteresuoti veikėjai, įskaitant ir mokslinių tyrimų komandas, turėtų įsitraukti į šio parengiamąjo etapo veiklas.

IDMEFv2 formatas: istorija

IDMEFv2 formatas (incidentų aptikimas) remiasi kai kuriomis savo pirmtako IDMEFv1 (įsibrovimo aptikimas) koncepcijomis, jas išplečia, kad apimtų visų tipų incidentus (kibernetinius ir fizinius), integruoja prieinamumo (availability) dimensiją ir prideda galimą gamtos veiksnių poveikį sistemos saugumui. Tai ypač svarbu, kai šios sistemos yra įdiegtos mobiliuose architektūrose, esančiose už apsaugotų, saugių ir vėsiamų duomenų centrų ribų. Šio formato kūrimas yra eilės mokslinių tyrimų projektų rezultatas, iš kurių pirmasis, SECEF1 (SECurity Exchange Format), buvo finansuotas Prancūzijos gynybos ministerijos ir remiamas Prancūzijos nacionalinės saugumo agentūros 2015 metais. Šio pirminio projekto tikslas buvo skatinti IDMEFv1 formato naudojimą administracinėse struktūrose ir kariuomenėje, o jo išvados išryškino būtinybę tobulinti šį formatą. 2020 metais Prancūzijos SECEF2 projekto ir Europos H2020 projekto (7Shield.eu) bendradarbiavimas kritinės infrastruktūros apsaugos nuo hibridinių ir sudėtingų atakų srityje atskleidė poreikį išplėsti formatą, kad jis apimtų visų rūšių fizinius ir gamtinius incidentus. Tai paskatino IDMEFv2 formato (www.idmefv2.org) IETF standartizavimo iniciatyvą. Šiandien tyrimai tęsiasi Europiniame Safe4SOC projekte (Standard Alert Format Exchange for SOCs), vadovaujant Telecom SudParis tyrėjų komandai, ir darbas bus tęsiamas ateinančius dvejus metus.

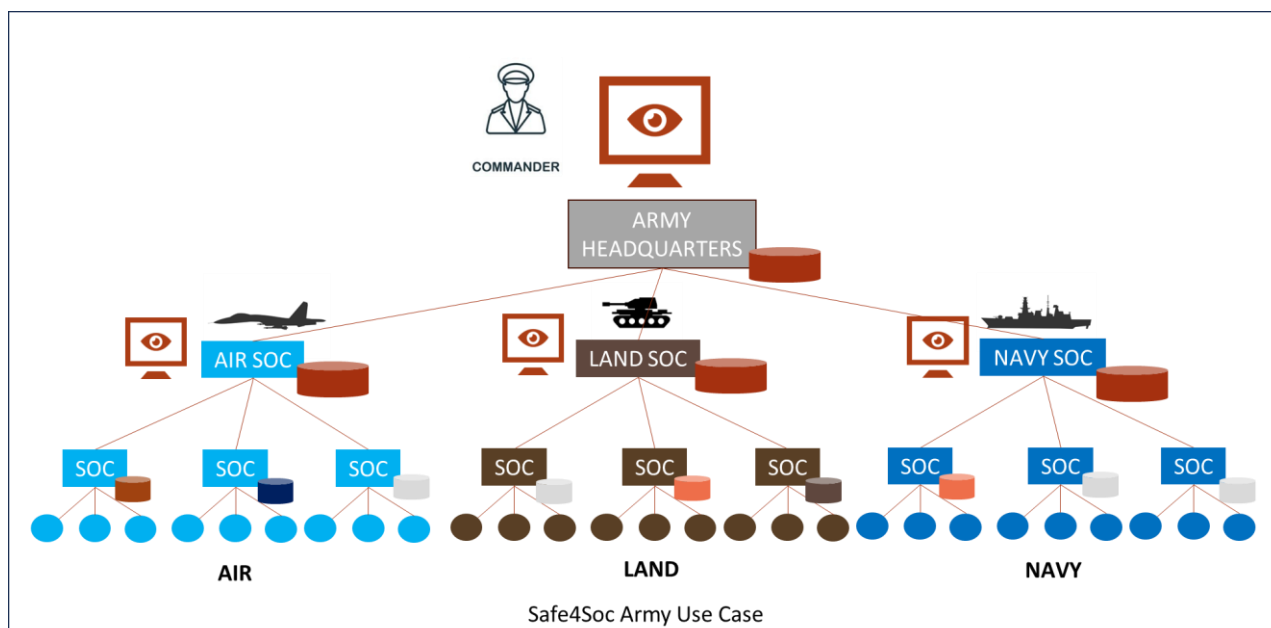
IDMEFv2: techninis įgyvendinimas

Siekiant palengvinti formato priėmimą, IDMEFv2 remiasi paprastomis ir universaliomis sąvokomis. Techniniu požiūriu, formatas įgyvendinamas naudojant JSON pranešimų transportavimą per HTTPS. Konceptualiai, šis formatas teikia pirmenybę paprastumui, o ne išsamumui, numatant paprastus išplėtimo mechanizmus. Šiuo metu tai yra vienintelė informavimo apie incidentus formato iniciatyva, kuri apima skaitmeninę ir fizinę erdves, ir taip pat sprendžia gamtinių incidentų valdymo klausimus.

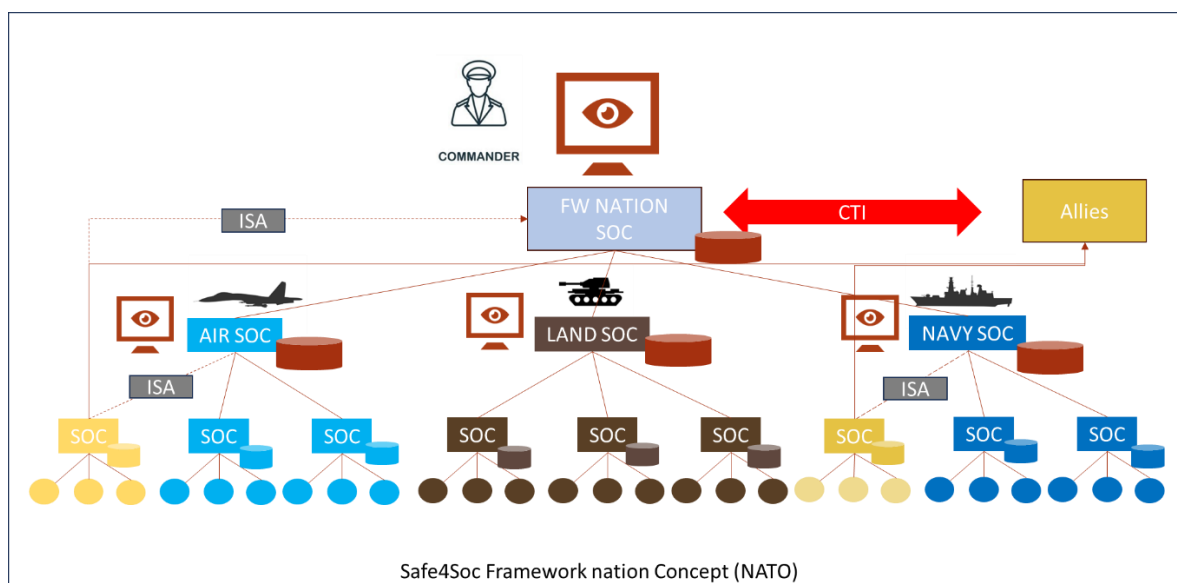
IDMEFv2 ir Gynybos sektorius

IDMEFv2 pradinę versiją kūrė ekspertų komandos, kurios specializuojasi incidentų aptikimo srityje integruojant kritines sistemas gynybos sektoriuje. Šis formatas sukurtas siekiant spręsti NOC-SOC ir PSIM monitoringo uždavinius įvairiose karinėse sistemose, o taip pat NATO operacijų pajėgų tarpusavio komunikavimo problemas. Savo sandara IDMEFv2 atitinka standartizuoto ir saugaus daugiašalio heterogeninio monitoringo konsolidavimo reikalavimus. Safe4SOC projektas stiprina šiuos aspektus, konkrečiai nagrinėdamas kelių Saugumo Operacijų Centrų (SOC), aprūpintų nuosavybinėmis monitoringo sistemomis (SIEM), prijungimo prie centrinio IDMEFv2 monitoringo SOC klausimus. Atsižvelgiant į didelę

karinių sistemų įvairovę, IDMEFv2 užtikrina jų monitoringo poreikius ir gali būti naudojamas įvairiose karinėse veiklose bei jungtinių pajėgų konsolidacijai.



Safe4SOC projekte taip pat plėtojamas „informacijos dalijimosi susitarimo“ principas, naudojant duomenų filtravimo ir saugumo vartus (gateway). Šio susitarimo tikslas – užtikrinti, kad kiekvienas prie centrinės sistemos prijungtas SOC/NOC/PSIM dalytųsi tik ta informacija, kuri būtina monitoringo bendrinimui, neatskleidžiant konfidencialios informacijos. Šis filtravimas atliekamas per vartus (gateway), kurie pagal abiejų šalių susitarimus panaikina, anonimizuoja arba šifruoja informaciją. Ši savybė atitinka segmentavimo ir „būtinybės žinoti“ principą, kuris yra ypač svarbus jungtinėms karinėms operacijoms.



Aukščiau pateiktame paveiksle pavaizduoti ISA moduliai atspindi galimą „sąjungininkų“ SOC bendrinamos informacijos filtravimą, kai ji perduodama vadovaujančios šalies SOC NATO arba Europos gynybos operacijų kontekste.

Daugiau informacijos

<http://www.idmefv2.org>: IDMEFv2 darbo grupės

<https://github.com/IDMEFv2>: atvirojo kodo manipuliavimo įrankia

<https://safe4soc.eu/>: Security Alert Format Exchange for SOC's projektas

KONTAKTAI

Gilles.Lehmann@telecom-sudparis.eu

IDMEFv2 ir Safe4SOC projektų koordinatorius

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