ALLDISPATCH
@IETF121

Update IDMEFv1

Incident Detection Message Exchange Format

Gilles Lehmann & Herve Debar , Telecom SudParis

Motivation

The Incident Detection Message Exchange Format version 2 (IDMEFv2) defines a data representation for security incidents detected in cyber and/or physical infrastructures.

The format is application-domain-agnostic so it can be used in standalone or combined cyber (SIEM), physical (PSIM) and availability (NMS) monitoring systems. IDMEFv2 can also be used to represent man-made or natural hazards threats.

IDMEFv2 improves situational awareness by facilitating correlation of multiple types of events using the same base format thus enabling efficient detection of complex and combined cyber and physical attacks and incidents.

Background

IDMEFv2 is inspired of IDMEFv1 RFCs 4765 (2007 - H. Debar):

- *https://www.rfc-editor.org/rfc/rfc4765.html*

IDMEFv2 Drafts (2024 – G. Lehmann)

- *https://datatracker.ietf.org/doc/draft-lehmann-idmefv2/*
- *https://datatracker.ietf.org/doc/draft-lehmann-idmefv2-https-transport/*

IDMEFv2 Website (Since 2023 ~ 200 visits/month)
https://idmefv2.org

IDMEFv2 mailing list (Approx. 60 members, not sufficiently active yet)
https://www.freelists.org/list/idmefv2

Background: Implementation

Complete SIEM prototype implementing IDMEFv2.
(security probes and SIEM connectors coming soon)
https://github.com/IDMEFv2/IDMEFv2-prototype

Python and Java librairies
https://github.com/IDMEFv2/python-idmefv2
https://github.com/IDMEFv2/java-idmef-library

IDMEFv2 JSON Validator
https://idmefv2.github.io/val/idmefv2_validator.html

Research project implementation 2020-2023
https://idmefv2.ovh/index.php/use-case-7shield/

IDMEFv2 research projects ongoing : SAFE4SOC (2024-2026)
https://safe4soc.eu/ (https://www.atlantis-horizon.eu/)

IETF

What needs to be done

Format and transport are defined and have been tested on real scale

We are entering the « tuning » phase, focusing on format attributes

It needs testing in real-world settings, with the code provided and retex from incident detection experts/researcher.

Expertise needed:

- *Cybersecurity Incident Detection*
- *Physical Incident Detection*
- *Combine Cyber and Physical Incident Detection*

Deadline: We need to finish the job by end of 2026 (end of the SAFE4SOC project)

Hoped-for dispatching outcome

Possible options

1. *Propose a new focused WG: Reactivate IDGW (only if IETF members are interested)*
2. *Publish as AD-sponsored (assuming AD is willing): IETF members who are interested can join external IDMEfv2 list*
3. *Additional discussion or community development required (e.g., with a new non-WG mailing list) if needed*

- ~~*Direct the work to an existing WG*~~
- ~~*Recommendation to hold a full BOF*~~