Network Working Group
Internet-Draft
Obsoletes: 4765 (if approved)
Intended status: Standards Track
Expires: 28 September 2026

G. Lehmann
Telecom SudParis

27 March 2026

The Incident Detection Message Exchange Format version 2 (IDMEFv2) draft-lehmann-idmefv2-07

Abstract

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

The format is 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.

This draft is maintained by the IDMEFv2 Task Force. Please consult our website for more information: https://www.idmefv2.org.

If approved this draft will obsolete RFC4765.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 September 2026.

Table of Contents

1. Introduction

The Incident Detection Message Exchange Format (IDMEF) is intended to solve the problem of security monitoring compartmentalization by proposing a single format to represent any type of incident, whether cyber or physical, intentional or accidental, natural or man-made.

Indeed security is often associated to the Confidentiality-Integrity-Availability triad, performance and availability management systems are still run independently from security management systems.

Additionally, with the adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices, and the exponential emergence of smart systems (transport, cities, buildings, etc), an increasingly interconnected mesh of cyber-physical systems (CPS) has emerged. This expansion of the attack and incident surfaces blurs the once-clear functions of cybersecurity and physical security.

Finally, as IT infrastructure moves out of data centers it becomes more exposed to external threats, including natural and man-made hazards.

Incident detection systems have traditionally focused on detecting cyber incidents or physical incident or availability incidents. There is an increasing need nowadays to have a unified view and management of all those incidents and their interconnection.

To achieve this goal the Incident Detection Message Exchange Format offers a unique data representation for multiple types of events:

* Cyber-security events (e.g. authentication failure/success, virus/malware detection, bruteforce/scan detection, etc.)

* Physical security events (e.g. intrusion detection, object detection, face or activity recognition, fire/smoke/noise/rain detection, etc.)

* Availability/observability/performance events (e.g. system failure, service malfunction, performance decrease, etc.)

* Natural and man made hazards events (e.g. wildfires, avalanches, droughts, earthquakes, pollution, fire, explosion, etc.)

1.1. IDMEFv2 deployment architecture

IDMEFv2 can be used to exchange incident detection information between specialized managers (SIEM, PSIM, NMS) and a universal "Cyber & Physical SIEM" (CPSIEM) or directly from specialized analyzers and a CPSIEM.

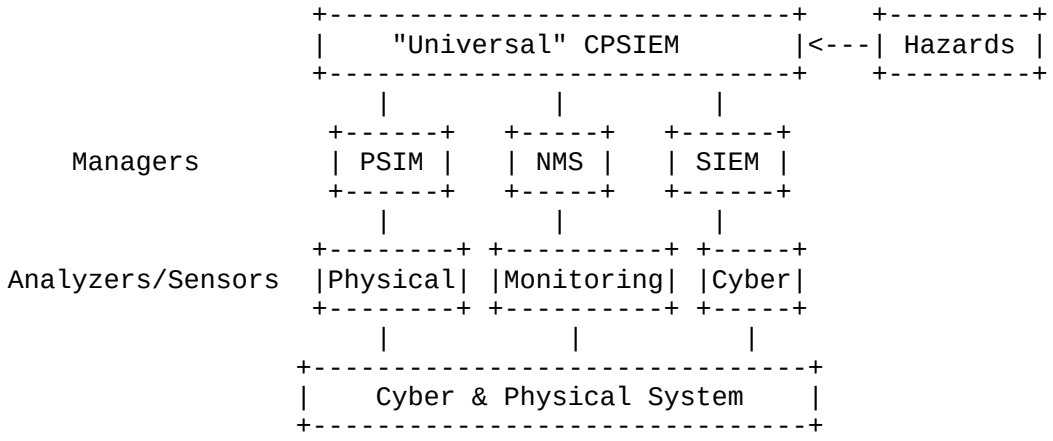

Figure 1: IDMEF Use Architecture

Thanks to its universality IDMEFv2 improves situational awareness by enabling correlation of multiple types of events using the same base format.

This document defines a model serialization methods for the purpose of describing and sharing these events.

1.2. IDMEFv1 (Intrusion Detection Message Exchange Format) - RFC 4765 - Legacy

IDMEFv2 (Incident Detection Message Exchange Format) is based on IDMEFv1 (Intrusion Detection Message Exchange Format) concepts. But IDMEFv1 was cyber intrusion focused as IDMEFv2 perimeter is much larger. Thus retro-compatibility although partly possible has not been a priority.

1.3. Relationship between IDMEFv2 and other event/incident formats

IDMEFv2 focuses essentialy on high level event/incident correlation and detection.There are many standard and proprietary formats on the incident detection market and in particular on the cybersecurity market. IDMEFv2 is complementary to most of these formats.

IDMEFv1 (Intrusion Detection Message Exchange Format - RFC 4765) : IDMEFv2 (Incident Detection) replaces and obsoletes IDMEFv1 (Intrusion Detection) by covering a wider spectrum.

IODEFv2 (Incident Object Definition Exchange Format - RFC 5070) : IDMEFv2 helps detect incident. When an incident is detected it will be analysed and eventually fully described and shared with other

security teams through IODEFv2. IODEFv2. IDMEF is used upstream IODEFv2. IDMEfv2 aLerts can be “attached” to IODEFv2 object to provide technical details about incidents.

Syslog (System Logging) : Syslog is a lossy format with no formal structuration. Syslog can be used by sensors to send information to analyzers. Out of those multi-format syslogs the analyzer might detect an incident or an event of interest. The analyzer will then use IDMEFv2 to notify the manager which might correlate this information with other datas to confirm the incident.

SNMP (Simple Network Management Protocol) : SNMP polls information from devices which is then compared to thresholds to detect incident. IDMEFv2 can be used when incident is detected downstream of SNMP to communicate the incident to the manager. IDMEFv2 can have a similar role as SNMP Traps.

STIX (Structured Threat Information Expression) : is a language and serialization format used to exchange cyber threat intelligence (CTI). IDMEFv2 can help detect incidents which might lead to the creation and sharing of STIX information. Cyber analyzer can also rely on STIX information to detect incidents that will be notified in IDMEFv2 format.

OCSF (The Open Cybersecurity Schema Framework) is an open-source, vendor-agnostic standard designed to normalize security telemetry from diverse tools. It provides a common language and consistent structure for security event data, simplifying data ingestion, correlation, and analysis. OCSF can be seen as a “super” syslog to describe events before IDMEFv2 extract “incidents” . OCSF is limited to cyber security.

SIEM proprietory formats (CEF, LEEF, ECS, CIM, ...) : By covering cyber, physical and monitoring incidents type, IDMEFv2 offers a wider spectrum than those formats. Gateways between IDMEFv2 and those formats can be developped to connect legacy cyber detection systems to an IDMEFv2 architecture.

1.4. Existing Deployments and Adoption

IDMEFv2 is not a theoretical proposal. It has been developed, validated, and deployed within the framework of eight large-scale European research projects, funded by the Horizon 2020 and Digital Europe programmes. These projects — namely 7SHIELD, PRECINCT, CyberSEAS, ATLANTIS, ENDURANCE, KINAITICS, TESTUDO, and SAFE4SOC — address critical sectors such as space systems, energy grids, transportation, and government infrastructure. These implementations span multiple domains, including Security Operations Centers (SOCs),

Physical Security Information Management (PSIM) systems, and critical infrastructure protection pilots.

This document aims to formalize this existing practice as an IETF Experimental RFC, to ensure interoperability, gather broader community feedback, and provide a stable foundation for future developments.

2. Terminology

2.1. Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Normative sections

Implementations of IDMEFv2 are REQUIRED to fully implement:

* The data types defined in Section 3

* The data model defined in Section 5

* The JavaScript Object Notation (JSON) serialization method Section 5.8.

2.3. Concepts related to event processing

2.3.1. Event

An event is something that triggered a notice. Any incident starts off as an event or a combination of events, but not all events result in an incident. An event need not be an indication of wrongdoing. E.g. someone successfully logging in or entering a building is an event.

2.3.2. Incident

An incident is an event that compromises or has a significant probability of compromising at least one of the organization’s security criteria such as Confidentiality, Integrity or Availability. An incident may affect a production tool, personnel, etc. It may be logical, physical or organizational in nature. Last but not least, an incident may be caused on purpose or by accident.

2.3.3. Alert

An alert is a notification/message that a particular event/incident (or series of events/incidents) has occurred.

2.3.4. Manager

The manager is the central console toward which all analyzers send their alerts. The manager collects, correlates, stores and displays the alerts to the operators.

Example : - A SIEM (Security Information & Event Management) or a Log Manager) - A PSIM (Physical Security Information Management) - A NMS (Network Management System) - A CPSIEM (Cyber & Physical Security Information Management System)

2.3.5. Operator

The level 1 operator is in charge of receiving manager notifications and identify or confirm when an event should be considered as an incident. The operator must also decide if there is a known resolution for this incident or if it needs a deeper analysys.

2.3.6. Analyst

The analyst will be contacted by the operator to analyze complex incidents that can’ t be easily resolved. The investigation starts with the IDMEFv2 information but the analyst might need more information like raw logs for a deeper forensics.

2.3.7. Attack

An attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of a cyber or physical asset. An attack is one or many kinds of incidents.

2.3.8. Correlation

Correlation is the identification of relationships between two or more events.

2.3.9. Aggregation

Aggregation is the consolidation of similar events into a single event.

3. The IDMEF Data Types

Each object inside the IDMEF data model has an associated data type. This type may be used to validate the content of incoming IDMEF messages.

3.1. Classes

The classes are meant to group related attributes together. Some of the classes may be instanciated multiple times (e.g. Source, Target, etc.) while others may only appear once in an IDMEF message (e.g. Analyzer).

3.2. Numbers

3.2.1. Integers

Integers inside the IDMEF data model are expressed using the following ABNF [RFC5234] grammar:

```
integer         =  *1minus int
int             =  zero / ( digit1-9 *DIGIT )
minus           =  %x2D                          ; -
zero            =  %0x30                         ; 0
digit1-9        =  %x31-39                       ; 1-9
```

E.g. 123.

Such values are indicated with the "INT" type annotation in the model.

3.2.2. Floating-point values

Floating-point values inside the IDMEF data model are expressed using the following ABNF grammar:

```
float           =  integer *1frac
frac            =  decimal-point 1*DIGIT
decimal-point   =  %x2E                           ; .
```

This grammar reuses some of the production rules listed in Section 3.2.1.

E.g. 12.34.

Such values are indicated with the "FLOAT" type annotation in the model.

3.3. Strings

Strings are series of characters from the [UNICODE] standard and are used to represent a text.

For readability, this document uses quotes (") to delimit strings, but please note that these quotes are not syntactically part of the actual strings.

E.g. "Hello world".

Some of the strings used in the IDMEFv2 data model follow a stricter syntax. These are included below for completeness.

Such values are indicated with the "STRING" type annotation in the model.

3.3.1. Enumerations

Enumerations are special strings used when valid values for an IDMEF attribute are restricted to those present in a predefined list.

Such values are indicated with the "ENUM" type annotation in the model.

3.3.2. Timestamps

Timestamps are used to indicate a specific moment in time. The timestamps used in the IDMEF data model follow the syntax defined by the "date-time" production rule of the grammar in [RFC3339] ch 5.6.

E.g. "1985-04-12T23:59:59.52Z" represents a moment just before April 5th, 1985 in Coordinated Universal Time (UTC).

Such values are indicated with the "TIMESTAMP" type annotation in the model.

3.3.3. Geographical Locations

Some attributes inside the IDMEF data model may refer to geographical locations using a set of coordinates. The reference system for all geographical coordinates is a geographic coordinate reference system, using the World Geodetic System 1984 [WGS84]. The reference system used is the same as for the Global Positioning System (GPS).

The format for such values can be either "latitude,longitude" or "latitude,longitude,altitude". Each of these coordinates is represented as a floating-point value. The latitude and longitude are expressed in degrees while the altitude is expressed in meters.

E.g. "48.8584,2.2945,276.13" matches the (3-dimensional) geographical location for the top floor or the Eiffel Tower located in Paris, France, while "48.8584,2.2945" matches the same location in two dimensions (with the altitude removed).

Such values are indicated with the "GEOLOC" type annotation in the model.

3.3.4. UNECE Location Codes (UN/LOCODE)

Some attributes inside the IDMEF data model may refer to geographical locations using Locations Codes. These codes can be assimilated to an enumeration, where the list of possible values is defined in the United Nations Economic Commission for Europe (UNECE) Codes for Trade [UN-LOCODE].

E.g. "FR PAR" is the Location Code for the city of Paris, France.

Such values are indicated with the "UNLOCODE" type annotation in the model.

3.3.5. Uniform Resource Identifiers (URIs)

The IDMEF data model uses Uniform Resource Identifiers (URIs), as defined in [RFC3986], when referring to external resources. Unless otherwise specified, either a Uniform Resource Location (URL) or a Uniform Resource Name (URN) may be used where a URI is expected.

E.g. both "https://example.com/resource" and "urn:myapp:resource" are valid Uniform Resource Identifiers.

Such values are indicated with the "URI" type annotation in the model.

3.3.6. IP Addresses

IP addresses inside the IDMEF data model are expressed as strings using the traditional dotted-decimal notation for IPv4 addresses (defined by the "dotnum" production rule in the grammar in [RFC5321]), while IPv6 addresses are expressed using the text representation defined in [RFC4291] ch 2.2.

E.g. "192.0.2.1" represents a valid IPv4 address, while "::1/128" represents a valid IPv6 address.

It is RECOMMENDED that implementations follow the recommendations for IPv6 text representation stated in [RFC5952].

Such values are indicated with the "IP" type annotation in the model.

3.3.7. E-mail addresses

E-mail addresses inside the IDMEF data model are expressed as strings using the address specification syntax defined in [RFC5322] ch 3.4.1.

E.g. "root@example.com".

Such values are indicated with the "EMAIL" type annotation in the model.

3.3.8. Attachment names

Attachments inside the IDMEF data model are identified using a unique name, composed of a string whose character set is limited to the ASCII letters (A-Z a-z) and digits (0-9).

E.g. "state" is a valid name for an attachment.

The constraint on name unicity is enforced per class. That is, but it is not possible for two attachments to share the same name inside the same alert.

Such values are indicated with the "ID" type annotation in the model.

3.3.9. Media types

Media types are used in the IDMEF data model to describe an attachment’s content. The syntax for such values is defined in [RFC2046].

IANA keeps a list of all currently registered media types in the Media Types registry .

E.g. "application/xml" or "text/plain; charset=utf-8".

Such values are indicated with the "MEDIATYPE" type annotation in the model.

3.3.10. Universally Unique IDentifiers (UUIDs)

Universally Unique Identifiers (UUIDs) are used to uniquely identify IDMEF messages. It is also possible for an IDMEF message to reference other IDMEF messages using their UUIDs. The syntax for UUIDs is defined in [RFC4122].

To limit the risk of UUID collisions, implementors SHOULD NOT generate version 4 UUIDs (randomly or pseudo-randomly generated UUIDs).

E.g. "ba2e4ef4-8719-42bb-a712-d6e8871c5c5a".

UUIDs are case-insensitive when used in comparisons.

Such values are indicated with the "UUID" type annotation in the model.

3.3.11. Protocol Names

Such values are indicated with the "PROTOCOL" type annotation in the model.

3.3.12. IDMEF Paths

This document defines a way to represent the path to every possible attribute inside an IDMEF message. For conciseness, the top-level "Alert" class is omitted from the path.

This representation can be used in contexts where the path to an IDMEF attribute is expected. An example of such usage can be seen in the definition of the "AggrCondition" attribute inside the Alert class (Section 5.2).

The syntax for these IDMEF paths is expressed in the following ABNF grammar:

```
class-name      =  "Analyzer" / "Sensor" / "Source" / "Target" /
                   "Attachment"
attribute-name  =  1*ALPHA
class-reference =  class-name "."
num             =  *1"-" 1*DIGIT
list-index      =  "(" num ")"
path            =  *1class-reference attribute-name *1list-index
```

Valid attribute names are limited to those defined for the specified class-reference (or in the top-level "Alert" class if class-reference is omitted).

For example, the following path refers to the "CeaseTime" attribute of the top-level "Alert" class: "CeaseTime".

Likewise, the following path refers to the "Name" attribute of the "Analyzer" class: "Analyzer.Name".

For attributes defined as lists (see Section 3.4), the path may include the (0-based) index for an entry inside the list. The index defaults to 0 if omitted. This means that several (valid) representations may be used to reference the same IDMEF attribute when list attributes are involved.

For example, both of the following paths refer to the IP address of the first source associated with an IDMEF message:

Source.IP
Source(0).IP

Compatible implementations MUST reject paths that reference an unknown class, an unknown attribute, or use a list-index for an IDMEF field which is not defined as a list.

A compatible implementation MUST also normalize paths before comparing them (e.g. by stripping the text "(0)" from paths referring to list attributes).

3.3.13. Hashes

Hashes are sometimes used inside the data model to protect the integrity (and optionally, authenticity) of attachments.

The syntax for these values is "function:hash_result", where "function" refers to one of the hashing function names listed in and "hash_result" contains the hexadecimal notation for the hash result obtained by calling the specified hash function on the input value.

In the context of IDMEF, either a keyless or keyed hash function may be used to process the raw input value.

E.g.
"sha256:a02735ed8b10ad432d557bd4849c0dac3b23d64706e0618716d6df2def338374"

Hashes are case-insensitive when used in comparisons.

Such values are indicated with the "HASH" type annotation in the model.

3.4. Lists

Some attributes of the IDMEF data model accept ordered lists of values.

Such ordered lists are indicated with the "X[]" type annotation in the model. where "X" refers to one of the data types defined in Section 3. For example, "ENUM[]" refers to an ordered list of enumeration values.

4. The IDMEF extension

In order to support the dynamic nature of security operations and to adapt to specific needs, the IDMEFv2 data model will need to continue to evolve. This section discusses how new data elements can be incorporated into the IDMEFv2. There is support to add additional enumerated values and new attributes.

These extension mechanisms are designed so that adding new data elements is possible without requiring modifications to this document. Extensions can be implemented publicly or privately. With proven value, well-documented extensions can be incorporated into future versions of the specification.

4.1. Extending the Enumerated Values of Attributes

Additional enumerated values can be added to select attributes either through the use of specially marked attributes with the "ext-" prefix or through a set of corresponding IANA registries. The former approach allows for the extension to remain private. The latter approach is public.

4.1.1. Private Extension of Enumerated Values

The data model supports adding new enumerated values to an attribute without public registration. For each attribute that supports this extension technique, there is a corresponding attribute in the same element whose name is identical but with a prefix of "ext-". This special attribute is referred to as the extension attribute. The attribute being extended is referred to as an extensible attribute. For example, an extensible attribute named "foo" will have a corresponding extension attribute named "ext-foo". An element may have many extensible attributes.

In addition to a corresponding extension attribute, each extensible attribute has "ext-value" as one its possible enumerated values. Selection of this particular value in an extensible attribute signals that the extension attribute contains data. Otherwise, this "ext-value" value has no meaning.

In order to add a new enumerated value to an extensible attribute, the value of this attribute MUST be set to "ext-value", and the new desired value MUST be set in the corresponding extension attribute. For example, extending the Category attribute of the Analyzer class would look as follows:

```
Analyzer: {
    ...
    "Category":["ext-value"],
    "ext-Category": "my-new-analyzer-category",
    ....
}
```

A given extension attribute MUST NOT be set unless the corresponding extensible attribute has been set to "ext-value".

4.1.2. Public Extension of Enumerated Values

The data model also supports publicly extending select enumerated attributes. A new entry can be added by registering a new entry in the appropriate IANA registry. Section (Table 10) provides a mapping between the extensible attributes and their corresponding registry.

4.2. Private Extension of Attributes

Use of new attributes is possible through the use of the attachment class. New attributes and their corresponding values should be stored in the Content attribute of an Attachment and the ContentEncoding must be set to JSON. For example creating a new attribute to store the email of the operator (in charge of solving the incident) will look as follows:

```
"Attachment" : [
    {
    "Name": "Operator",
    "ContentEnconding": "JSON",
    "Content": "{\"OperatorMail\":\"John.Does@acme.com\"}",
    }
[
```

5. The IDMEF Data Model

In this section, the individual components of the IDMEF data model will be discussed in detail. For each class, the semantics will be described.

5.1. Overview

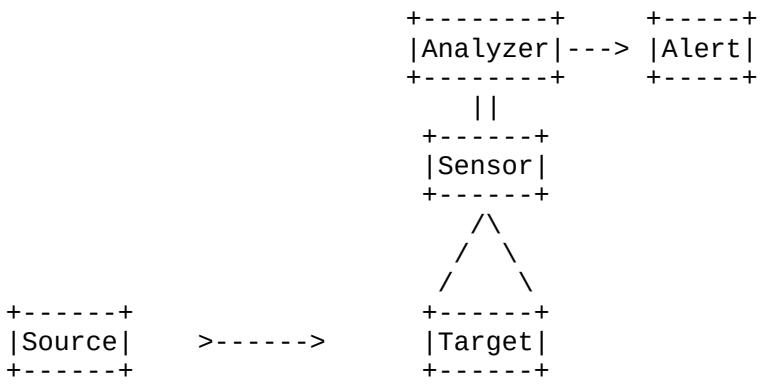

Figure 2: IDMEFv2 Overview Classes

An IDMEF message is composed of an instance of the Alert class (Section 5.2) representing the overall properties of the message. It also contains exactly one instance of the Analyzer class (Section 5.3) and zero or more instances of the Sensor class (Section 5.4). The message may also describe various aspects of an event using the Source (Section 5.5) and Target (Section 5.6) classes.

Last but not least, it may also include zero or more instances of the Attachment class (Section 5.7), e.g. captured files or network packets related to the event for example.

The relationship between the main Alert class and other classes of the data model is shown in Figure 3 (attributes are omitted for clarity).

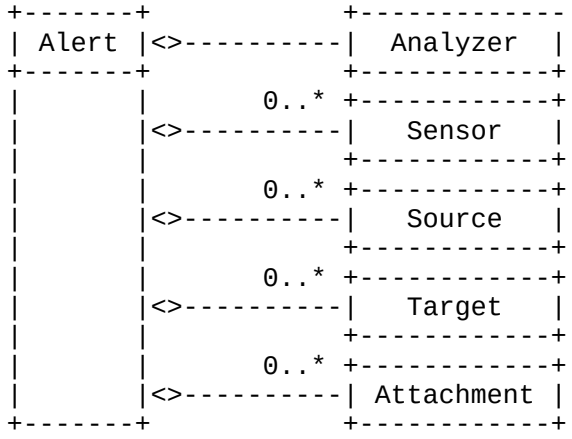

Figure 3: IDMEFv2 Classes

It is important to note that the data model does not specify how an incident should be categorized or identified. For example, an attacker scanning a network for machines listening on a specific port may be identified by one analyzer as a single attack against multiple targets, while another analyzer may identify it as multiple attacks from a single source. However, once an analyzer has determined the type of alert it plans on sending, the data model dictates how that alert should be formatted.

5.2. The Alert Class

The Alert class contains high level information about the event that triggered the alert.

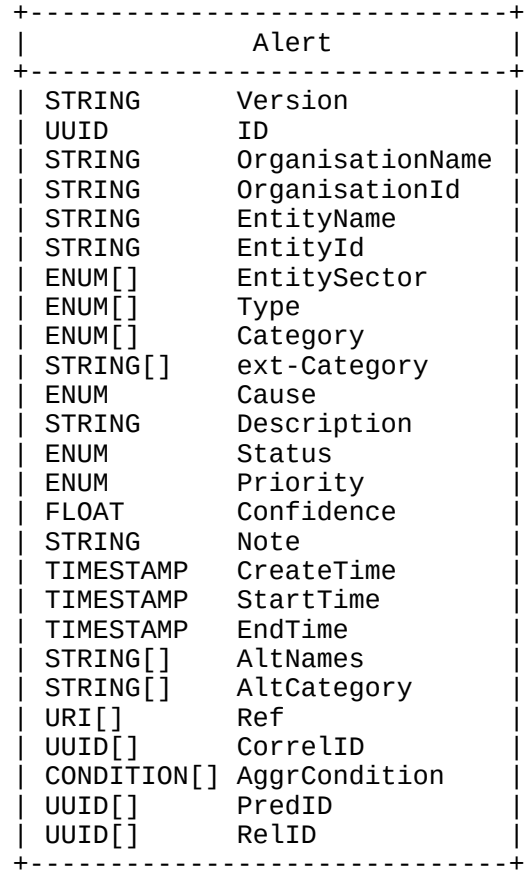

Figure 4: The Alert class

The aggregate classes that make up Alert are:

Analyzer
: Exactly one. An instance of the Analyzer class (Section 5.3) that describes the tool/device responsible for the analysis that resulted in the alert being created and sent.

Sensor
: Zero or more. Instances of the Sensor class (Section 5.4) used to describe the sensor(s) that captured the information used during the analysis.

  Depending on the tools/devices used to detect incidents, an Analyzer may rely on the output from a single sensor or from multiple sensors to generate alerts. In addition, the Analyzer

and Sensor may actually be part of the same physical device and may share some of their attributes (e.g. IP, Hostname, Model, etc.).

Source
: Zero or more. Instances of the Source class (Section 5.5) used to describe the source(s) of the incident (e.g. attackers, faulty device, etc.).

Target
: Zero or more. Instances of the Target class (Section 5.6) used to describe the target(s) of the incident, i.e. the impacted devices/users/services/locations.

Attachment
: Zero or more. Instances of the Attachment class (Section 5.7) used to describe the electronic artifacts captured in relation with the event.

  The intent of the Attachment class is to keep track of the electronic files left as a trail during the event. This may include things like on-disk files (e.g. malware samples), network packet captures, videos or still images from a camera feed, voice recording, etc.

The Alert class has the following attributes:

Version
: Mandatory. The version of the IDMEF format in use by this alert.

  During the drafts tuning period the version is equal to the draft version. Therefore it is "2.D.V0X" for Draft V0X.

ID
: Mandatory. Unique identifier for the alert.

OrganisationName
: Optional. Corporate/Main Office Organisation Name

  Useful if alerts are sent to a multi-organisation central incident detection manager.

  Example: ACME Corporation

OrganisationId
: Optional. Corporate/Main Office Organisation ID. Where possible official organisation ID manage by national authority.

Useful if alerts are sent to a multi-organisation central incident detection manager.

This ID has to be chosen depending on the overall detection perimeter and the nature of the monitored organisation (Private/ Public, Commercial, International, etc.)

Examples: OrganisationId in France could be SIREN, in England could be CR, Germany could be Handelsregisternummer, Spain could be CIF, Italia could be Partita IVA, USA could be EIN, etc. Commercial OrganisationId in Europe could be V.A.T ID

EntityName
Optional. Entity Name, monitored by the organisation, where the incident occurred.

Could be a town, region or country name or an internal name. Could also be the name of a client for a MSSP centralizing it’s client incidents in a single system.

Do not repeat the organisation name in the EntityName

Example:

- ACME HeadQuaters is located in Paris France and has a local office in India

- If the incident occurred in the local office: "OrganisationName": "ACME" , "EntityName": "India"

- If the incident occurred in the headquaters: "OrganisationName": "ACME", "EntityName": "Headquaters" (or "Paris")

EntityId
Optional. Entity ID, monitored by the organisation, where the incident occurred.

Useful if organisation and entity are not directly linked, like a client and a MSSP.

EntitySector
Optional. The economic sector(s) and sub-sector(s) in which the entity operates. Values follow the dot notation sector.subsector based on the critical infrastructure taxonomy defined in the NIS2 Directive and CER (Critical Entities Resilience) Directive.

This attribute enables sector-based correlation, regulatory compliance reporting, and risk context for incident detection.

Rank	Keyword	Description
0	Undefined	Sector undefined
1	Banking.Banking	Banking institutions and credit activities
2	Banking.Other	Other banking and financial entities critical for the stability of the financial system
3	Cemeteries.Crematoria	Crematoria operations
4	Cemeteries.PublicCemeteries	Public cemetery and crematorium facilities
5	Cemeteries.Other	Other cemetery and funeral service entities critical for public health and social continuity
6	Chemical.ChemicalProduction	Production of hazardous and high-consequence chemicals
7	Chemical.Storage	Chemical storage and distribution facilities
8	Chemical.Other	Other chemical sector entities critical for safety and security
9	CivilSociety.ElectionMonitoring	Election observation and monitoring entities

10	CivilSociety.HumanitarianAid	Humanitarian aid organizations
11	CivilSociety.NGOs	Non-governmental organizations with critical functions
12	CivilSociety.Other	Other civil society entities critical for democratic processes and social stability
13	CulturalHeritage.Archives	National and regional archives
14	CulturalHeritage.HistoricalSites	Historical monuments and archaeological sites
15	CulturalHeritage.Libraries	National and public libraries
16	CulturalHeritage.Museums	Museums and exhibition spaces
17	CulturalHeritage.Other	Other cultural heritage entities critical for national identity and continuity
18	Defense.CommandControl	Military C4ISR systems (command, control, communications, computers, intelligence, surveillance, reconnaissance)
19	Defense.CyberDefense	Military cyber defense and security operations centers

20	Defense.DefenseIndustrialBase	Defense manufacturing, weapons systems, munitions production
21	Defense.Logistics	Military supply chains, fuel depots, ammunition storage
22	Defense.MilitaryInstallations	Military bases, headquarters, and operational facilities
23	Defense.Research	Defense laboratories and R&D facilities
24	Defense.Other	Other defense and military entities critical for national security
25	Digital.CloudServices	Cloud computing and critical digital services
26	Digital.DataCenters	Data center hosting and infrastructure services
27	Digital.DigitalProviders	Online marketplaces, search engines and social media platforms
28	Digital.DomainNameSystems	DNS service providers and TLD registries
29	Digital.ICTServiceManagement	ICT service management B2B services

30	Digital.SatelliteCommunications	Satellite communication networks and ground stations
31	Digital.TelecomNetworks	Fixed and mobile telecommunications networks
32	Digital.UnderseaCables	Submarine communications cable infrastructure
33	Digital.Other	Other digital and telecommunications entities critical for the continuity of digital services
34	Education.PrimarySecondary	Primary and secondary schools
35	Education.ResearchSchools	Research-focused educational institutions
36	Education.Universities	Universities and higher education institutions
37	Education.Other	Other educational entities critical for societal continuity
38	EmergencyServices.CivilProtection	Civil protection and disaster management agencies
39	EmergencyServices.EmergencyMedical	Ambulance services and emergency medical response
40	EmergencyServices.FireAndRescue	Firefighting and

		rescue services
41	EmergencyServices.Police	Law enforcement agencies and operations
42	EmergencyServices.Other	Other emergency response entities critical for public safety
43	Energy.DistrictHeating	Operation of district heating networks
44	Energy.Electricity	Generation, transmission and distribution of electrical power
45	Energy.Gas	Transport, storage and distribution of natural gas
46	Energy.Hydrogen	Production, transport and storage of hydrogen
47	Energy.Nuclear	Nuclear power generation and fuel cycle facilities
48	Energy.Oil	Refining, transport and storage of petroleum products
49	Energy.Other	Other energy entities critical for the continuity of energy supply
50	Finance.FinancialMarketInfrastructures	Stock exchanges and clearing houses

51	Finance.Insurance	Systemically important insurance entities
52	Finance.PaymentSystems	Card schemes, transfers and instant payment systems
53	Finance.Other	Other financial entities critical for the stability of the financial system
54	Food.AgriculturalProduction	Strategic agricultural and livestock production
55	Food.FoodDistribution	Retail and logistics for food supply chains
56	Food.FoodProcessing	Industrial food processing and manufacturing
57	Food.FoodSafety	Food safety inspection and control authorities
58	Food.Other	Other food sector entities critical for the continuity of the food supply chain
59	Health.BloodAndTissue	Blood banks, tissue banks, and transplantation services
60	Health.HealthcareProviders	Hospitals and clinics providing essential care

61	Health.Laboratories	Medical analysis and diagnostic laboratories
62	Health.MedicalDevices	Manufacture and maintenance of critical medical devices
63	Health.PharmaceuticalSupplyChain	Manufacturing, wholesale and distribution of pharmaceuticals
64	Health.PublicHealth	Public health agencies and epidemiological surveillance
65	Health.Other	Other health entities critical for the continuity of healthcare services
66	Logistics.FreightForwarding	Freight forwarding and cargo management
67	Logistics.LastMileDelivery	Last-mile delivery services
68	Logistics.ThirdPartyLogistics	Third-party logistics providers
69	Logistics.Warehousing	Strategic warehousing and storage facilities
70	Logistics.Other	Other logistics entities critical for supply chain continuity
71	Manufacturing.Aerospace	Aerospace and aviation manufacturing

72	Manufacturing.Batteries	Battery manufacturing and energy storage production
73	Manufacturing.Chemical	Chemical manufacturing and industrial processes
74	Manufacturing.ComputerElectronicOptical	Manufacture of computer, electronic and optical products
75	Manufacturing.Defense	Defense manufacturing and strategic military supply chains
76	Manufacturing.MedicalDevices	Manufacture of medical devices and equipment
77	Manufacturing.MotorVehicles	Manufacture of motor vehicles and transport equipment
78	Manufacturing.Pharmaceutical	Pharmaceutical manufacturing and active pharmaceutical ingredients
79	Manufacturing.Semiconductors	Semiconductor fabrication and microelectronics manufacturing
80	Manufacturing.StrategicManufacturing	Critical manufacturing such as metallurgy and components
81	Manufacturing.Other	Other manufacturing

		entities critical for industrial resilience and strategic supply chains
82	MediaAndBroadcasting.BroadcastInfrastructure	Transmitters, towers, and broadcast distribution infrastructure
83	MediaAndBroadcasting.OnlineMedia	Digital news platforms and content providers
84	MediaAndBroadcasting.Press	Newspapers, publishing houses, and press agencies
85	MediaAndBroadcasting.Radio	Radio broadcasting networks and studios
86	MediaAndBroadcasting.Television	Television broadcasting networks and studios
87	MediaAndBroadcasting.Other	Other media entities critical for information integrity and public communication
88	Mining.CriticalRawMaterials	Extraction and processing of critical raw materials
89	Mining.EnergyMinerals	Coal, uranium, and other energy mineral mining
90	Mining.Other	Other mining entities critical for resource

			security
91	Nuclear.FuelCycle		Nuclear fuel production, enrichment, reprocessing, and waste management
92	Nuclear.Medical		Nuclear medical facilities and radioisotope production
93	Nuclear.PowerGeneration		Civil nuclear power plants and associated facilities
94	Nuclear.Research		Nuclear research reactors and laboratories
95	Nuclear.Other		Other nuclear entities critical for safety and security
96	Postal.PostalCourierServices		Postal and courier services
97	Postal.Other		Other postal and courier entities critical for the continuity of mail and parcel services
98	PublicAdministration.CentralGovernment		Central government ministries and agencies
99	PublicAdministration.Diplomatic		Embassies, consulates, and diplomatic missions
100	PublicAdministration.EmergencyServices		Police, fire, rescue, and

		emergency medical services
101	PublicAdministration.Judiciary	Courts, judicial systems, and correctional facilities
102	PublicAdministration.LocalGovernment	Regional and municipal public services
103	PublicAdministration.Other	Other public administration entities critical for the continuity of public services
104	ReligiousSites.PilgrimageSites	Major pilgrimage destinations
105	ReligiousSites.PlacesOfWorship	Churches, mosques, synagogues, temples, and other religious buildings
106	ReligiousSites.Other	Other religious sites critical for community continuity
107	Research.BiologicalSafety	BSL-3 and BSL-4 high-containment laboratories
108	Research.ChemicalSafety	High-containment chemical research facilities
109	Research.Research	Key research laboratories with strategic importance
110	Research.Other	Other research entities critical for strategic

			research continuity and innovation
111	Space.GroundStations		Satellite ground control and telemetry stations
112	Space.LaunchFacilities		Space launch sites and associated infrastructure
113	Space.SpaceActivities		Space industry and satellite operations
114	Space.Other		Other space entities critical for the continuity of space-based services and infrastructure
115	Transport.Aviation		Airports, air traffic control and airline operations
116	Transport.Maritime		Ports, terminals and maritime traffic management
117	Transport.Pipeline		Oil, gas, and hydrogen pipeline infrastructure
118	Transport.PublicTransport		Urban and regional public transportation systems
119	Transport.Rail		Railway infrastructure and train operations
120	Transport.Road		Traffic management and strategic road logistics

121	Transport.Other	Other transport entities critical for the continuity of passenger and freight mobility
122	Waste.HazardousWaste	Collection, treatment and disposal of hazardous waste
123	Waste.NonHazardousWaste	Management of non-hazardous solid waste
124	Waste.NuclearWaste	Nuclear waste management and storage facilities
125	Waste.Recycling	Waste processing and recycling operations
126	Waste.Other	Other waste management entities critical for the continuity of waste services
127	Water.DamsAndReservoirs	Dam and reservoir infrastructure for water management
128	Water.DrinkingWater	Capture, treatment and distribution of potable water
129	Water.Irrigation	Large-scale agricultural irrigation systems
130	Water.Wastewater	Collection and treatment of sewage and wastewater
131	Water.Other	Other water

			entities critical for the continuity of water supply and sanitation. (see Section 4.1.1)

Table 1: EntitySector

Type
Optional. Incident type.

Rank	Keyword	Description
0	Cyber	Cyber incident
1	Physical	Physical incident
2	Availability	Availability incident
3	Combined	Combined incident

Table 2: Incident types

Category
Optional. Incident category.

Rank	Keyword	Description
0	Abuse.Grooming	The process of deliberately building an emotional connection with a person to lower their inhibitions for the purpose of sexual abuse, exploitation, or trafficking.
1	Abuse.Harassment	A pattern of unwanted, intrusive behavior (physical, verbal, or online) directed at a specific person that

		causes fear, distress, or emotional harm.
2	Abuse.Coercion	The practice of compelling an individual to act against their will by using force, threats, intimidation, or extreme dependency, often for personal or financial gain.
3	Abuse.Trafficking	The act of recruiting, transporting, transferring, harboring, or receiving a person through force, fraud, or coercion for the purpose of exploitation, such as forced labor or sexual servitude.
4	Abuse.Extermism	The process of socializing an individual, often through psychological manipulation, to adopt the beliefs and goals of a violent extremist group and become willing to engage in activities that support the group.
5	Abuse.Other	Any other incident involving manipulation or coercion of people for harmful purposes that does not fit into the specific abuse subcategories.
6	Access.Compromise	An incident where a legitimate user’s credentials (e.g.,

			username/password) are stolen or guessed and used by an unauthorized individual to gain access to systems or data.
7	Access.Escalation	An incident where a user or process gains access rights, permissions, or capabilities that exceed those normally assigned, often to bypass security restrictions.
8	Access.Backdoor	The installation or discovery of a concealed method of bypassing normal authentication or encryption in a computer system, product, or embedded device.
9	Access.Unauthorized	An incident involving physical entry into a restricted building, room, or area without proper authorization.This includes physical entry into a restricted building, room, or area, as well as digital access to systems, applications, networks, or data by an individual or process lacking valid credentials or authorization.
10	Access.Tailgating	A physical security breach where an

		unauthorized person follows an authorized individual through a secured entry point, circumventing access control mechanisms.
11	Access.Forced	An incident involving the use of physical force to breach a barrier (e.g., lock, door, window) or the repeated systematic guessing of passwords to gain unauthorized access.
12	Access.Lost	An incident where physical or digital access credentials (e.g., keys, ID badges, login details) are misplaced, stolen, or used by an unauthorized person.
13	Access.Clonned	The act of creating an unauthorized copy of a physical or digital security credential, such as an access card, to gain illicit entry to a facility or system.
14	Access.Authorized	An incident involving legitimate, approved access to resources that may be relevant for auditing, monitoring, or establishing a baseline of normal activity.
15	Access.Other	Any other incident related to physical or digital access that

		does not fit into the specific access subcategories.
16	Availability.DoS	An incident where a single machine or network attempts to make a system, service, or network resource unavailable by overwhelming it with malicious requests or traffic.
17	Availability.DDoS	An incident where multiple compromised systems (a botnet) are used to target a single system with a flood of traffic, causing a denial of service.
18	Availability.Outage	An incident where essential utilities or services (such as electricity, water, or network connectivity) become unavailable, disrupting normal operations.
19	Availability.Failure	An incident caused by the unintentional malfunction of hardware or software due to errors, bugs, wear and tear, or other faults, leading to service degradation or unavailability.
20	Availability.Misconfiguration	An incident where incorrect configuration of systems, software, or networks leads to service disruptions,

		outages, or security vulnerabilities.
21	Availability.Overload	An incident where a system or component is subjected to a load beyond its designed capacity, leading to performance degradation or failure, even if the load is not malicious.
22	Availability.HeartBeat	A periodic signal generated by hardware or software to indicate normal operation, often used for monitoring system health, connectivity, or location tracking.
23	Availability.Other	Any other incident that impacts the availability of resources or services, not covered by the specific subcategories.
24	Fraud.Usage	The use of an organization’s assets (e.g., computing power, network, email) for non-work-related, often illegal, activities without authorization.
25	Fraud.Copyright	The act of reproducing, distributing, or installing software, media, or other materials in violation of their copyright, often for personal gain or distribution

		(piracy).
26	Fraud.Masquerade	A type of attack where an attacker illegitimately assumes the identity of another user, process, or system to gain unauthorized access, privileges, or benefits.
27	Fraud.Phishing	A cyber attack where an attacker disguises themselves as a trustworthy entity (e.g., via email or fake website) to trick a victim into revealing sensitive information like usernames, passwords, or credit card details.
28	Fraud.Corruption	A fraudulent scheme that is made possible by the abuse of power or position by a trusted individual (e.g., employee, official) who acts for personal gain.
29	Fraud.Espionnage	The use of illegal or unethical means, such as hacking, bribery, or theft, to acquire a competitor’s trade secrets, intellectual property, or other confidential business information.
30	Fraud.Other	Any other incident involving deception for financial or reputational gain that

		does not fit into the specific fraud subcategories.
31	Insider.Malicious	A security incident caused by a current or former employee, contractor, or other trusted insider who intentionally acts to harm the organization, its data, or its people.
32	Insider.Negligent	A security incident caused unintentionally by an insider, such as through carelessness, lack of awareness, or simple human error, leading to data exposure or system compromise.
33	Insider.Other	Any other security incident involving an insider (trusted individual) that does not fit into the specific insider threat subcategories.
34	Sabotage.Vandalism	The deliberate and malicious act of damaging, destroying, or obstructing an organization’s physical assets, operations, or systems.
35	Sabotage.Graffiti	The act of willfully defacing, damaging, or marking public or private property with inscriptions, drawings, or tags without permission.

36	Sabotage.Destruction	The intentional and malicious act of destroying or severely damaging physical assets, such as windows, equipment, or buildings.
37	Sabotage.Tampering	The act of deliberately meddling with or disabling security controls (e.g., locks, alarms, cameras) to compromise their effectiveness.
38	Sabotage.Equipment	The intentional act of causing damage to operational equipment, machinery, or vehicles, often to disrupt production or operations.
39	Sabotage.Disruption	The intentional disruption of essential services or utilities, such as electricity, water, or network connectivity, to cause operational downtime.
40	Sabotage.Data	The intentional act of deleting, altering, or corrupting digital or physical data to cause harm, disrupt operations, or cover tracks.
41	Sabotage.Other	Any other incident involving the intentional damage to property or assets not covered by the specific sabotage

		subcategories.
42	Safety.Explosion	A sudden, violent release of energy (e.g., from gas, chemicals, or explosives) that causes a blast, fire, and potential structural damage, injury, or loss of life.
43	Safety.Fire	An incident involving uncontrolled burning (e.g., structural, wildland, or chemical fire) that threatens human safety, property, or the environment.
44	Safety.Agression	An incident where an individual uses physical force against another person, causing bodily harm, pain, or the fear of immediate harm.
45	Safety.Sexual	An incident involving any unwanted sexual act, contact, or behavior directed against an individual without their consent.
46	Safety.Accident	An unplanned, unforeseen event (e.g., vehicle crash, industrial mishap, chemical spill) that results in injury, loss of life, or damage to health.
47	Safety.Hostage	An incident where a person or group is

		held against their will by a captor, often to compel a third party to meet certain demands.
48	Safety.Other	Any other incident that causes or has the potential to cause injury, loss of life, or endanger citizens, not covered by specific safety subcategories.
49	SupplyChain.Disruption	An event that disrupts the normal flow of products, services, or information within a supply chain, often impacting operations and delivery.
50	SupplyChain.Compromise	A security incident where an attacker exploits a vulnerability in a third-party vendor’s system to gain access to or compromise the primary target’s network or data.
51	SupplyChain.Other	Any other incident affecting the supply chain that does not fit into the specific supply chain subcategories.
52	Theft.Equiment	The unlawful taking of physical hardware, such as computers, mobile phones, or servers, resulting in loss of assets and potentially the data they contain.

53	Theft.Data	The unauthorized taking or copying of sensitive or confidential documents, whether in physical or digital form.
54	Theft.Machinery	The unlawful taking of heavy equipment, vehicles, or specialized machinery, often resulting in significant operational and financial loss.
55	Theft.PII	The unauthorized acquisition of Personally Identifiable Information (PII) that can be used to identify, contact, or impersonate an individual.
56	Theft.IP	The unlawful acquisition of a company’s intellectual property, including trade secrets, patents, formulas, or proprietary processes.
57	Theft.FinInfo	The theft of financial information, such as credit card numbers or bank account details, often for the purpose of fraudulent transactions.
58	Theft.Breaches	A security incident involving the unauthorized access, acquisition, or

		disclosure of sensitive, protected, or confidential data.
59	Theft.Other	Any other incident involving the intentional stealing of physical property or digital data not covered by specific theft subcategories.
60	Operational.Misuse	The use of an organization’s assets (e.g., computers, network, time) for purposes that are not officially authorized, which may violate policy but not be malicious.
61	Operational.Policy Violation	An incident where an individual fails to comply with established organizational policies, procedures, or security rules, whether intentionally or accidentally.
62	Operational.Process Failure	An incident where a designed process, procedure, or workflow fails to achieve its intended outcome, leading to operational or security gaps.
63	Operational.Other	Any other operational issue that does not fit into the specific operational incident subcategories.
64	Recon.Netword	The practice of probing a network to

			discover active hosts, open ports, and services, often as a precursor to an attack or unauthorized monitoring.
65	Recon.Landscape		The act of physically observing a location to gather information about security measures, layouts, or potential vulnerabilities.
66	Recon.Aerial		The act of using aerial platforms, such as drones or satellites, to conduct surveillance or gather intelligence about a target area.
67	Recon.OSINT		The practice of collecting and analyzing information from publicly available sources (e.g., social media, public records) for intelligence purposes.
68	Recon.Other		Any other incident involving scanning, spying, or monitoring to identify resources that does not fit into specific recon subcategories.
69	National.Terrorism		An incident involving the use of violence, intimidation, or threats by non-state actors against civilians or property to achieve political, religious, or

		ideological objectives.
70	National.Conflict	A state of armed conflict between two or more nations, involving organized military forces and impacting national security.
71	National.Cyber	Large-scale cyber operations, including attacks, espionage, and disinformation campaigns, conducted by state-sponsored or state-affiliated groups against national interests.
72	National.Crime	Large-scale illegal activities, such as trafficking in drugs, weapons, or people, conducted by sophisticated criminal networks that pose a threat to national and international security.
73	National.Environemental	Incidents related to large-scale environmental shifts, such as climate change, resource scarcity, or global pandemics, that have significant national security implications.
74	National.Economical	An incident involving significant disruption to a nation’s economy, such as market crashes, hyperinflation, or

		trade wars, affecting national stability.
75	National.Societal	An incident involving large-scale public disorder, such as strikes, riots, or civil unrest, that challenges social order and may require national-level response.
76	National.Other	Any other incident that has a significant impact at the national scale, not covered by specific national security subcategories.
77	SocialEng.Phishing	A type of social engineering where attackers send fraudulent emails, appearing to be from a legitimate source, to trick recipients into revealing sensitive information or installing malware.
78	SocialEng.Spear Phishing	A highly targeted phishing attack directed at a specific individual, organization, or role, often using personalized information to increase credibility.
79	SocialEng.Vishing	A social engineering attack conducted over the phone, where the attacker impersonates a legitimate entity to trick the victim into

			revealing sensitive information or performing actions.
80	SocialEng.Smishing		A social engineering attack conducted via SMS (text message), where the attacker sends a fraudulent message to trick the recipient into clicking a malicious link or providing information.
81	SocialEng.Pretexting		A social engineering tactic where the attacker creates a fabricated scenario or pretends to be someone they are not to engage a victim and extract information or access.
82	SocialEng.Baiting		A social engineering attack that lures victims by offering something desirable (e.g., free music, a prize) in exchange for information or by tricking them into downloading malware.
83	SocialEng.QuidProQuo		A social engineering tactic where the attacker offers a service or benefit (e.g., technical support) in exchange for information or access, often expecting something in return later.
84	SocialEng.Other		Any other incident involving psychological

		manipulation of people to divulge information or perform actions, not covered by specific social engineering subcategories.
85	Malware.Virus	A type of malicious software that attaches itself to a legitimate program or file and replicates itself to spread to other programs, often requiring human action to propagate.
86	Malware.Worm	A type of standalone malicious software that replicates itself to spread across networks, often exploiting vulnerabilities without requiring human interaction.
87	Malware.Trojan	A type of malware that disguises itself as legitimate or desirable software to trick users into installing it, after which it can perform malicious actions.
88	Malware.Ransomware	A type of malware that encrypts a victim’s files or systems, rendering them inaccessible, and demands a ransom payment, often in cryptocurrency, for the decryption key.
89	Malware.Spyware	A type of software

		that secretly monitors and collects information about a user’s activities, such as keystrokes, browsing habits, and personal data, without their consent.
90	Malware.Adware	A type of software that automatically displays or downloads unwanted advertisements, often in a disruptive manner, and may track user behavior.
91	Malware.Rootkit	A type of malware designed to hide its presence and grant an attacker persistent, privileged access to a compromised system while evading detection.
92	Malware.Other	Any other incident involving malicious software that does not fit into the specific malware subcategories.
93	Geophysical.Earthquake	An incident caused by a sudden, rapid shaking of the earth resulting from the movement of tectonic plates, which can cause ground shaking, surface rupture, and tsunamis.
94	Geophysical.MassMovement	An incident involving the downslope movement of rock, soil, or snow under the force of gravity, such as

		landslides, avalanches, or rockfalls.
95	Geophysical.Volcanic	An incident caused by the eruption of magma and volcanic gases from a volcano, which can produce lava flows, pyroclastic flows, ashfall, and lahars.
96	Geophysical.Other	Any other incident caused by solid-earth processes not covered by specific geophysical subcategories.
97	Meteo.Heat	A meteorological incident involving a prolonged period of excessively hot weather, which can cause health impacts, infrastructure stress, and environmental damage.
98	Meteo.Cold	A meteorological incident involving a rapid fall in temperature over a short period, or a prolonged period of extreme cold, posing risks to health and infrastructure.
99	Meteo.Fog	A meteorological incident where dense fog reduces visibility, potentially disrupting transportation and causing accidents.

100	Meteo.Rain	A meteorological incident involving excessive or prolonged rainfall that can lead to flooding, landslides, and transportation disruptions.
101	Meteo.Snow	A meteorological incident involving heavy snowfall and blizzard conditions, which can disrupt transportation, damage infrastructure, and pose risks to safety.
102	Meteo.Wind	A meteorological incident involving damaging or dangerous winds, such as from storms, tornadoes, or hurricanes, that can cause structural damage and power outages.
104	Meteo.Other	Any other incident caused by atmospheric processes not covered by specific meteorological subcategories.
105	Hydro.Flood	An incident where water submerges land that is normally dry, often caused by heavy rain, storm surge, or dam failure, leading to property damage and risk to life.
106	Hydro.Landslide	An incident involving the downward movement of slope materials (soil, rock) triggered

		by water saturation from heavy rain or snowmelt.
107	Hydro.Wave	An incident involving destructive waves, such as tsunamis or storm surges, that can cause coastal flooding, erosion, and damage.
108	Hydro.Other	Any other incident caused by the movement, distribution, and quality of water, not covered by specific hydrological subcategories.
109	Climat.Drought	A prolonged period of below-average precipitation leading to a water shortage, which can impact agriculture, ecosystems, and water supplies.
110	Climat.LakeOutburst	An incident where a glacial lake dam (often moraine or ice) fails, rapidly releasing a large volume of water and causing devastating floods downstream.
111	Climat.Wildfire	An unplanned and uncontrolled fire burning in natural or rural areas, often exacerbated by climatic conditions like drought, wind, and heat.

112	Climat.Other	Any other incident caused by long-lived atmospheric processes (climatological) not covered by specific subcategories.
113	Biological.Epidemic	The rapid and widespread occurrence of an infectious disease in a specific population or region, exceeding what is normally expected.
114	Biological.Insect	An incident involving a harmful outbreak or infestation of insects that threatens public health, agriculture, livestock, or property.
115	Biological.Animal	An incident where animals pose a direct threat to human safety, public health (e.g., zoonotic diseases), or economic stability (e.g., livestock diseases).
116	Biological.Zombies	A fictional or hypothetical scenario involving a pathogen that causes a pandemic of aggressive, infectious behavior, often used as a metaphor for worst-case outbreak scenarios in planning.
117	Biological.Other	Any other incident caused bybiological not covered by specific subcategories.

118	Extraterrestrial.Impact	An incident involving a celestial object (asteroid, meteoroid, comet) colliding with Earth, potentially causing localized or global damage.
119	Extraterrestrial.Aliens	A hypothetical incident involving the discovery of or interaction with extraterrestrial intelligent life, a theoretical scenario in scientific and security planning.
120	Extraterrestrial.SpaceWeather	An event caused by solar or cosmic activity, such as solar flares or geomagnetic storms, that can disrupt Earth’s technological infrastructure.
121	Extraterrestrial.Other	Any other incident caused extraterrestrial process not covered by specific subcategories.
122	Other.Uncategorised	Any incident that does not fit into one of the predefined categories in this taxonomy.
123	Other.Undetermined	An incident whose category is currently unknown, under investigation, or cannot be determined.
124	Other.Test	An incident generated

			solely for the purpose of testing systems, processes, or training personnel.
125	Other.ext-value		A value used to indicate that this attribute is extended and the actual value is provided using the corresponding ext-* attribute. (see Section 4.1.1)

Table 3: Incident categories

ext-Category
: Optional. A means by which to extend the Category attribute. (see Section 4.1.1)

Cause
: Optional. Incident cause. The cause can be modified by any analyzer on the way of the alert and later by the operator and/or the analyst if new investigation reveals and confirms a different cause of the event.

Rank	Keyword	Description
0	Normal	The event is related to an expected phenomenon or to a phenomenon that does not qualify as out of the ordinary.
1	Error	The event is related to a human error.
2	Malicious	The event is related to malicious code or malicious actions.
3	Malfunction	The event is related to a device or service malfunction.
4	Hazard	The event is related to a hazard phenomenon.
5	Unknown	The cause of the event is unknown.

Table 4: Incident causes

Description
Optional. Short free text human-readable description of the event. The description can add detail to the event category for easiest/faster comprehension by the operator. Example : * Cryptoware WannaCry blocked on pegasus server * Unknown person entering through east doorway

Status
Optional. Event state in the overall event lifecycle.

Rank	Keyword	Description
0	Event	The event is still considered as an harmless event and should not be treated.
1	Incident	The event is considered as an incident and should be taken care of.
2	Open	The incident is confirmed and actively being investigated.
3	Closed	Investigation is finished and the issue is handled.
4	FalsePositive	Investigation is finished, incident was a false positive.

Table 5: Incident statuses

Priority

Optional. Priority of the alert. Priority is defined by conbining impact and urgency. It indicates how fast the incident should be taken care of.

Rank	Keyword	Description
0	Unknown	Priority unknow
1	Info	No priority, the alert is informational
2	Low	Low priority
3	Medium	Medium priority
4	High	High priority

Table 6: Incident priorities

Confidence

Optional. A floating-point value between 0 and 1 indicating the analyzer's confidence in its own reliability of this particular detection, where 0 means that the detection is surely incorrect while 1 means there is no doubt about the detection made.

Note
Optional. Free text human-readable additional note, possibly a longer description of the incident if is not already obvious.

The Note attribute can be used to store any additional information. It can be additional information about the event and/or about the incident resolution, although the incident resolution information should in principle be stored elsewhere (with a link with the external tool in AltNames)

CreateTime
Mandatory. Timestamp indicating when the alert was created.

StartTime
Optional. Timestamp indicating the deduced start of the event.

StartTime can be later than CreateTime in case or Alerts created from forecast information (e.g. Snow Storm expected in two days staring at 10h00)

EndTime
Optional. Timestamp indicating the deduced end of the event.

AltNames
Optional. Alternative identifiers; strings which help pair the event to internal systems' information (for example ticket IDs inside a request tracking systems).

AltCategory
Optional. Alternate categories from a reference other than IDMEFv2 categories (e.g. MISP, MITRE ATT@CK or another proprietary/internal reference).

Ref
Optional. References to sources of information related to the incident and/or vulnerability, and specific to this incident.

This MAY be a URL to additional info, or a URN in a registered or unregistered ad-hoc namespace bearing reasonable information value and uniqueness, such as "urn:cve:CVE-2013-2266".

CorrelID

Optional. Identifiers for the messages which were used as information sources to create this message, in case the message has been created based on correlation/analysis/deduction from other messages.

AggrCondition
Optional. A list of IDMEF fields used to aggregate events. The values for these fields will be the same in all aggregated events.

This attribute should mostly be set by intermediary nodes, which detect duplicates, or aggregate events, spanning multiple detection windows, into a longer one.

The "StartTime" and "EndTime" attributes are used in conjunction with this attribute to describe the aggregation window.

PredID
Optional. A list containing the identifiers of previous messages which are obsoleted by this message.

The obsoleted alerts SHOULD NOT be used anymore. This field can be used to "update" an alert.

RelID
Optional. A list containing the identifiers of other messages related to this message.

5.3. The Analyzer Class

The Analyzer class describes the module that has analyzed the data captured by the sensors, identified an event of interest and decided to create an alert.

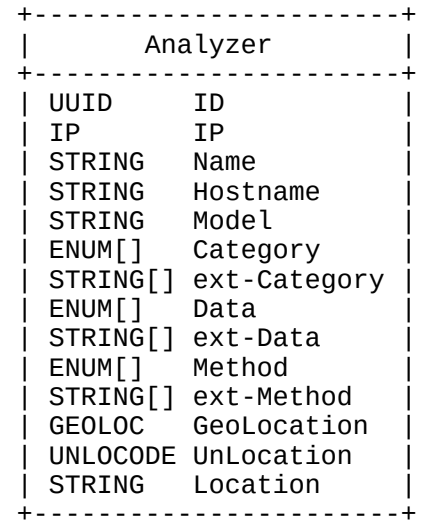

Figure 5: The Analyzer class

The Analyzer class has the following attributes:

ID
: Mandatory. Unique identifier for the analyzer.

IP
: Optional. Analyzer IP address.

Name
: Mandatory. Name of the analyzer, which must be reasonably unique, however still bear some meaningful sense.

  This attribute usually denotes the hierarchy of organizational units the detector belongs to and its own name. It MAY also be used to distinguish multiple analyzers running with the same IP address.

Hostname
: Optional. Hostname of this analyzer.

  SHOULD be a fully-qualified domain name.

Model
: Optional. Analyzer model description (usually its generic name, brand and version).

Category

Optional. Analyzer categories.

Rank	Keyword	Description
0	Undetermined	Analyzer category is undetermined
1	APP.BAST	Bastion Host - Secure remote access gateway
2	APP.DAST	Dynamic Application Security Testing - Runtime application testing
3	APP.IAST	Interactive Application Security Testing - Hybrid application testing
4	APP.RASP	Runtime Application Self-Protection - Self-protecting applications
5	APP.SAST	Static Application Security Testing - Source code analysis
6	CLD.CASB	Cloud Access Security Broker - Cloud service security mediation
7	CLD.CIEM	Cloud Infrastructure Entitlement Management - Cloud permission management
8	CLD.CSPM	Cloud Security Posture Management - Cloud configuration monitoring
9	CLD.CWPP	Cloud Workload Protection Platform - Cloud workload security
10	DDoS.ANTI-DDOS	Distributed Denial of Service Protection - DDoS mitigation system
11	DDoS.SCRUB	Scrubber/Scrubbing Center - Traffic cleaning for DDoS

12	DDoS.WAF-DDOS	Web Application Firewall with DDoS - Integrated DDoS protection
13	EMAIL.ANTI-PHISH	Anti-Phishing - Phishing attempt detection
14	EMAIL.DMARC	Domain-based Message Authentication - Email authentication monitoring
15	EMAIL.SEG	Secure Email Gateway - Comprehensive email security
16	EMAIL.SPAM-FILTER	Spam Filter - Unsolicited email detection
17	END.AM	Application Allowlisting - Application execution control
18	END.AV	Antivirus - Signature-based malware detection
19	END.DLP-EP	Endpoint Data Loss Prevention - Endpoint data leakage prevention
20	END.EDR	Endpoint Detection and Response - Advanced endpoint threat hunting
21	END.EPP	Endpoint Protection Platform - Comprehensive endpoint security
22	END.HIDS	Host Intrusion Detection System - Host-based threat monitoring
23	END.HIPS	Host Intrusion Prevention System - Host-based threat prevention
24	END.HPT	Honeypot - Deception-based threat detection
25	END.RASP	Runtime Application Self-

			Protection - In-app runtime protection
26	ID.DCAP		Data-Centric Audit and Protection - Data-centric security monitoring
27	ID.DLP		Data Loss Prevention - Data leakage prevention across channels
28	ID.IAM		Identity and Access Management - Identity governance and access control
29	ID.IRM		Identity Risk Management - Identity-based risk analysis
30	ID.PAM		Privileged Access Management - Privileged access management
31	ID.PIM		Privileged Identity Management - Privileged account security
32	ID.UEBA		User and Entity Behavior Analytics - Behavioral threat detection
33	NET.DNS-FW		DNS Firewall - Malicious domain filtering
34	NET.DPI		Deep Packet Inspection - Advanced packet analysis
35	NET.FW		Firewall - Network traffic filtering and policy enforcement
36	NET.NAC		Network Access Control - Endpoint compliance and access enforcement
37	NET.NBAD		Network Behavior Anomaly Detection - Anomaly detection in network behavior
38	NET.NDR		Network Detection and Response - Advanced network threat

		hunting
39	NET.NGFW	Next-Generation Firewall - Advanced firewall with app awareness
40	NET.NIDS	Network Intrusion Detection System - Network traffic analysis for threats
41	NET.NIPS	Network Intrusion Prevention System - Inline threat prevention
42	NET.PROXY	Proxy Server - ACL and TLS session monitoring
43	NET.WAF	Web Application Firewall - HTTP/HTTPS traffic filtering
44	NET.WIDS	Wireless Intrusion Detection System - WiFi threat detection
45	NET.WIPS	Wireless Intrusion Prevention System - WiFi threat prevention
46	OT.IoT-IDS	IoT Intrusion Detection System - IoT device threat detection
47	OT.OT-IDS	Operational Technology IDS - Industrial control system monitoring
48	OT.PLC-SCAN	PLC Scanner - PLC/SCADA vulnerability detection
49	PHY.1D-LAS	1D Laser Sensor - Basic laser presence/distance detection
50	PHY.1D-LiDAR	1D Light Detection and Ranging Sensor - Single-beam laser for distance measurement
51	PHY.2D-LAS	2D Laser Sensor - Planar laser scanning
52	PHY.2D-LiDAR	2D Light Detection and Ranging

		Sensor - Planar laser scanning for 2D mapping
53	PHY.3D-LAS	3D Laser Sensor - 3D laser scanning
54	PHY.3D-LiDAR	3D Light Detection and Ranging Sensor - 3D environmental scanning and mapping
55	PHY.ACCESS-CTRL	Access Control System - Physical entry/exit control monitoring
56	PHY.ADS	Anti-Drone System - Drone detection and countermeasure system
57	PHY.FR-CAM	Face Recognition Camera - Biometric facial recognition system
58	PHY.GLASS-BRK	Glass Break Detector - Acoustic glass breakage detection
59	PHY.HAR	Human Activity Recognition - AI-based human behavior and motion analysis
60	PHY.LWIR	Long-Wave Infrared - Long-wave thermal imaging
61	PHY.MOT-SEN	Motion Sensor - PIR/microwave motion detection
62	PHY.MWIR	Mid-Wave Infrared - Mid-wave thermal imaging
63	PHY.OBJ-DET	Object Detection Camera - General object detection and classification
64	PHY.SWIR	Short-Wave Infrared - Short-wave infrared imaging
65	PHY.VAD	Voice Activity Detection - Audio analysis for voice/

		speech detection
66	PHY.VNIR	Visible and Near-Infrared - Multi-spectral imaging sensor
67	SIEM.ETL	Extract, Transform, Load - Data pipeline tools (Logstash, Fluentd, Vector)
68	SIEM.LOG	Log Analyzer - Log aggregation and analysis (e.g., ELK Stack, Splunk)
69	SIEM.NMS	Network Management System - Network monitoring and management
70	SIEM.SIEM	Security Information and Event Management - Centralized security logging and alerting
71	SIEM.SOAR	Security Orchestration and Response - Automated incident response
72	TI.CTI	Cyber Threat Intelligence - Strategic threat intelligence
73	TI.TI-FEED	Threat Intelligence Feed - External threat data streams
74	TI.TIP	Threat Intelligence Platform - Threat data aggregation and analysis
75	VM.ASM	Attack Surface Management - External attack surface monitoring
76	VM.PENTEST	Penetration Testing Tools - Manual/automated security testing
77	VM.VULN-SCANNER	Vulnerability Scanner - Automated vulnerability assessment
78	VM.ASM	Attack Surface Management -

			External attack surface monitoring
79	ext-value		A value used to indicate that this attribute is extended and the actual value is provided using the corresponding ext-* attribute. (see Section 4.1.1)

Table 7: Analyzer Categories

ext-Category
Optional. A means by which to extend the Category attribute. (see Section 4.1.1)

Data
Optional. Type of data analyzed during the detection.

Rank	Keyword	Description
0	Undetermined	Analyzer data is undetermed.
1	Light	ambient light levels, flicker detection
2	Acoustics	sound pressure, specific frequencies
3	Contact	physical interaction, switch state
4	Vibration	mechanical oscillation, structural health
5	Temperature	ambient, device, or surface
6	Humidity	relative humidity, moisture in air
7	Rain	precipitation detection
8	Water	leak detection, immersion, water flow
9	Fog	visibility reduction, optical density

10	Particles	dust, smoke, airborne contaminants
11	Seismic	ground motion, earthquakes, vibrations
12	Magnetic	magnetic anomaly detection, proximity
13	Images	visible spectrum cameras
14	Thermal	infrared imaging, heat signatures
15	Lidar	laser-based distance measurement, 3D mapping
16	Network	traffic, bandwidth, connectivity
17	Flow	netflow, packet flow analysis
18	Protocol	protocol anomalies, compliance
19	Datagram	packet-level inspection
20	Host	server or device health, uptime
21	Connection	session establishment, drops
22	Port	open/closed, scanning activity
23	SNMP	simple network management protocol data
24	Authentication	login attempts, failures, anomalies
25	Log	system, application, security logs
26	File	file integrity, access, changes
27	Content	payload inspection, data content

28	Data	generic data streams, sensor data
29	Reporting	summary reports, alerts from other systems
30	Alert	triggered notifications
31	Relay	alert forwarding, escalation
32	External	third-party alerts, threat intelligence feeds
33	ext-value	A value used to indicate that this attribute is extended and the actual value is provided using the corresponding ext-* attribute. (see Section 4.1.1)

Table 8: Analyzer Data

ext-Data
Optional. A means by which to extend the Data attribute. (see Section 4.1.1)

Method
Optional. Detection method.

Rank	Keyword	Description
0	Undetermined	Analyzer method is undetermed
1	AI	An analyzer that uses machine learning, deep learning, or other artificial intelligence techniques to learn normal behavior and detect sophisticated or novel threats.
2	Anomaly	An analyzer that identifies deviations from established norms or baselines without relying on predefined signatures, often flagging unusual patterns in traffic, behavior, or system activity.

3	Behavioral	An analyzer that monitors and analyzes the actions of users, entities, or processes over time to detect malicious or suspicious activities that deviate from expected behavior patterns.
4	Biometric	An analyzer that uses electronic devices to capture and measure unique physical or behavioral characteristics (e.g., fingerprint, iris, voice) for identification or authentication purposes.
5	Blackhole	A method that analyses traffic destined for a non-existent or sinkhole route to identify malicious activity, such as connections to known command-and-control servers or scanning from infected hosts.
6	Contextual	An analyzer that enriches raw events with additional context (e.g., asset value, user role, time of day, business criticality) to prioritize alerts and assess true impact.
7	Correlation	An analyzer that aggregates and examines multiple, disparate data streams or events to identify complex relationships, patterns, sequences, or dependencies that indicate a security incident.
8	Ensemble	An analyzer that combines multiple detection methods (e.g., signature, anomaly, behavioral) to improve accuracy, reduce false positives, and detect threats that single methods might miss.
9	Fingerprinting	An analyzer that creates unique identifiers or "fingerprints" for devices, applications, or network stacks to detect spoofing, unauthorized devices, or configuration changes.

10	Frequency	An analyzer that detects incidents based on the rate or regularity of events (e.g., repeated failed logins, rapid-fire requests) exceeding or falling below expected frequencies.
11	Fusion	An analyzer that combines data from multiple heterogeneous sensors and sources to create a comprehensive, high-confidence view of an incident, reducing ambiguity and false alerts.
12	Geolocation	An analyzer that determines the physical location of an asset or event (e.g., login attempt, IP address, device) and flags activities occurring from unexpected or high-risk locations.
13	Graph-based	An analyzer that models relationships between entities (users, devices, processes) as graphs and detects anomalies or attack paths by analyzing connections, dependencies, and traversals.
14	Heat	An analyzer (sensor or device) that detects, measures, and monitors thermal energy (infrared radiation) to identify anomalies like fires, overheating equipment, or human presence.
15	Heuristic	An analyzer that detects potentially unknown threats by using algorithmic logic, rules of thumb, or suspicious characteristics rather than relying on specific signature matches.
16	Honeypot	A decoy system or resource designed to lure, detect, and analyze malicious activity by mimicking a legitimate target, diverting attackers away from real assets.
17	Hygiene	An analyzer that continuously checks systems and configurations against security best practices, compliance

		standards, or hardening guidelines to identify weaknesses or drift.
18	Integrity	An analyzer that monitors critical system components (files, configurations, registry keys) for unauthorized changes, verifying their integrity against a known good baseline.
19	Metadata	An analyzer that examines the data about data (e.g., file creation timestamps, email headers, connection logs) to uncover hidden relationships or suspicious attributes.
20	Monitor	An analyzer that continuously observes a system, network, or environment to track its state, health, or activity, often providing real-time alerts on specific conditions.
21	Movement	An analyzer (sensor or system) that detects, tracks, and quantifies physical motion using technologies like radar, lidar, or video analytics.
22	Orchestration	An analyzer that coordinates and triggers automated response actions based on detected incidents, often integrated with SOAR (Security Orchestration, Automation, and Response) platforms.
23	Pattern	An analyzer that identifies specific sequences, combinations, or recurring arrangements of events or data that indicate malicious activity, even if individual elements appear benign.
24	Policy	An analyzer that evaluates events, configurations, or behaviors against a set of predefined rules, configurations, or compliance requirements to detect violations or misconfigurations.

25	Predictive	An analyzer that uses historical data and modeling to forecast potential future incidents, vulnerabilities, or attack vectors before they occur.
26	Protocol	An analyzer that validates network traffic or communications against expected protocol specifications, RFC compliance, or standard behavior to detect anomalies or malicious variations.
27	Recon	An analyzer that actively or passively probes or monitors an environment to discover assets, services, or vulnerabilities, often as part of a defensive assessment or adversary simulation.
28	Reputation	An analyzer that evaluates the trustworthiness of an entity (e.g., IP address, domain, file hash) by checking it against known threat intelligence lists, blocklists, or reputation scores.
29	Rule-based	An analyzer that applies conditional logic (if-then-else statements) defined by experts to correlate events and generate alerts based on specific combinations of conditions.
30	Sequence	An analyzer that detects threats by examining the order and timing of events, identifying attack chains or kill chain progressions (e.g., scan → exploit → installation → C2).
31	Signature	An analyzer that detects known threats by matching events or patterns against a database of specific signatures, hashes, or Indicators of Compromise (IoCs).
32	Statistical	An analyzer that detects anomalies by establishing a baseline of normal behavior and identifying events that

		deviate significantly from expected statistical parameters.
33	Tarpit	A mechanism that intentionally slows down or delays suspicious connections (e.g., network connections or login attempts) to hinder automated attacks and scanning.
34	Threat Intelligence	An analyzer that ingests and matches internal events against external threat feeds, IoC lists, and adversary TTPs (Tactics, Techniques, and Procedures) to identify known threats.
35	Threshold	An analyzer that detects incidents by comparing a metric or count (e.g., number of failed logins, traffic volume) against a predefined limit or threshold.
36	Trend	An analyzer that monitors data over extended periods to identify gradual changes, emerging patterns, or long-term shifts that may indicate evolving threats or security degradation.
37	ext-value	A value used to indicate that this attribute is extended and the actual value is provided using the corresponding ext-* attribute. (see Section 4.1.1)

Table 9: Analyzer Methods

ext-Method
: Optional. A means by which to extend the Method attribute. (see Section 4.1.1)

GeoLocation
: Optional. GPS coordinates for the analyzer.

UnLocation
: Optional. Standard UN/Locode for the analyzer.

Location
Optional. Internal name for the location of the analyzer.

5.4. The Sensor Class

The Sensor class describes the module that captured the data before sending it to an analyzer. The Sensor may be a subpart of the Analyzer.

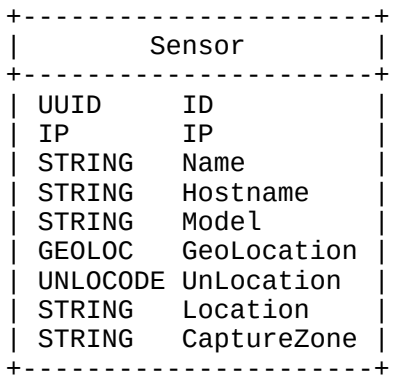

Figure 6: The Sensor class

The Sensor class has the following attributes:

ID
Mandatory. Unique identifier for the sensor.

IP
Optional. The sensor’s IP address.

Name
Mandatory. Name of the sensor, which must be reasonably unique, however still bear some meaningful sense.

This attribute usually denotes the hierarchy of organizational units the sensor belongs to and its own name. It MAY also be used to distinguish multiple sensors running with the same IP address.

Hostname
Optional. The sensor’s hostname.

This SHOULD be a fully qualified domain name, but may not conform exactly because values extracted from logs, messages, DNS, etc. may themselves be malformed.

An empty string MAY be used to explicitly state that this value was inquired but not found (missing DNS entry).

Model
Optional. The sensor model’s description (usually its generic name, brand and version).

GeoLocation
Optional. GPS coordinates for the analyzer.

UnLocation
Optional. Standard UN/Locode for the sensor.

Location
Optional. Internal name for the location of the sensor.

CaptureZone
Optional. A string that describes the "capture zone" of the sensor, as a JSON-serialized string.

Depending on the type of sensor, the capture zone may for instance refer to:

* A JSON object describing a camera’s settings (elevation, horizontal and vertical field of view, azimuth, etc.)

* A description of the IP network where packet capture is taking place.

5.5. The Source Class

The Source class describes the origin(s) of the event(s) leading up to the creation of this alert.

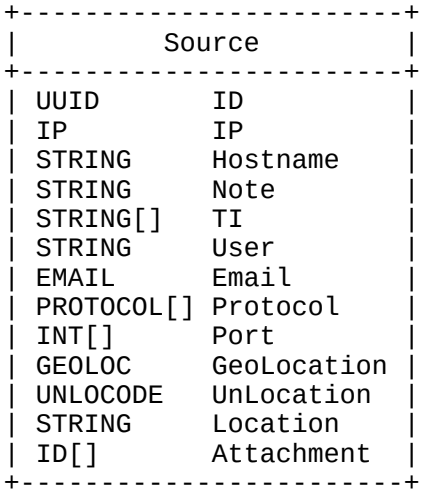

Figure 7: The Source class

The Source class has the following attributes:

ID
: Mandatory. Unique identifier for the source.

IP
: Optional. Source IP address.

Hostname
: Optional. Hostname of this source.

  This SHOULD be a fully qualified domain name, but may not conform exactly because values extracted from logs, messages, DNS, etc. may themselves be malformed.

  An empty string MAY be used to explicitly state that this value was inquired but not found (missing DNS entry).

Note
: Optional. Free text human-readable additional note for this source.

TI
: Optional. Threat Intelligence data about the source.

Values in this list MUST use the format "attribute:origin", where "attribute" refers to the attribute inside this source found inside a Threat Intelligence database, and "origin" contains a short identifier for the Threat Intelligence database. E.g. "IP:Dshield".

Please note that the same attribute may appear multiple times inside the list (because a match was found in multiple Threat Intelligence databases).

User
Optional. User ID or login responsible for the incident.

Email
Optional. Email address responsible for the incident.

E.g. the value of the "Reply-To" or "From" header inside a phishing e-mail.

Protocol
Optional. Protocols related to connections from/to this source.

If several protocols are stacked, they MUST be ordered from the lowest (the closest to the medium) to the highest (the closest to the application) according to the ISO/OSI model.

Port
Optional. Source ports involved in the incident.

Values in this list MUST be integers and MUST be in the range 1-65535.

GeoLocation
Optional. GPS coordinates for the source.

UnLocation
Optional. Standard UN/Locode for the source.

Location
Optional. Internal name for the location of the source.

Attachment
Optional. Identifiers for attachments related to this source.

Each identifier listed here MUST match the "Name" attribute for one of the attachments described using the Attachment class (Section 5.7).

5.6. The Target Class

The Target class describes the target(s) impacted by the event(s) leading up to the creation of this alert.

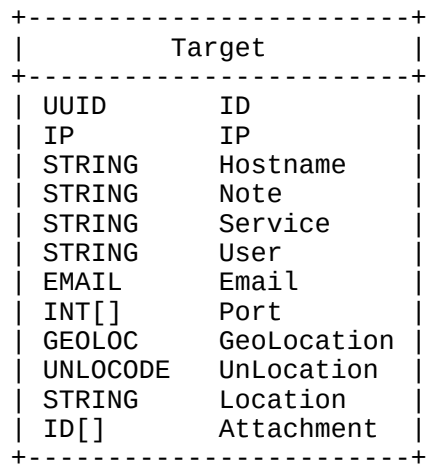

Figure 8: The Target class

The Target class has the following attributes:

ID
: Mandatory. Unique identifier for the target.

IP
: Optional. Target IP address.

Hostname
: Optional. Hostname of this target.

  This SHOULD be a fully qualified domain name, but may not conform exactly because values extracted from logs, messages, DNS, etc. may themselves be malformed.

  An empty string MAY be used to explicitly state that this value was inquired but not found (missing DNS entry).

Note
: Optional. Free text human-readable additional note for this target.

Service
: Optional. Service or process impacted by the incident.

User
Optional. User ID or login impacted by the incident.

Email
Optional. Email address impacted by the incident.

E.g. the value of the "To" header inside a phishing e-mail.

Port
Optional. Target ports involved in the incident.

Values in this list MUST be integers and MUST be in the range 1-65535.

GeoLocation
Optional. GPS coordinates for the target.

UnLocation
Optional. Standard UN/Locode for the target.

Location
Optional. Internal name for the location of the target.

Attachment
Optional. Identifiers for attachments related to this target.

Each identifier listed here MUST match the "Name" attribute for one of the attachments described using the Attachment class (Section 5.7).

5.7. The Attachment Class

The Attachment class contains additional data which was captured in relation with the event.

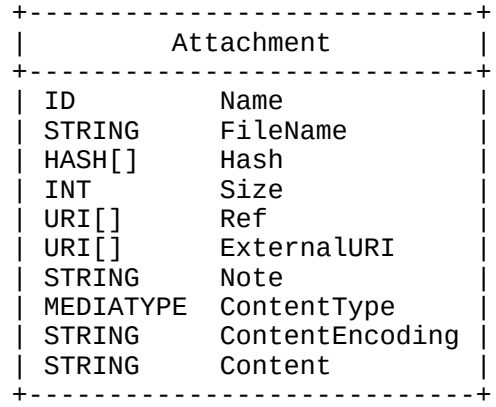

Figure 9: The Attachment class

The Attachment class has the following attributes:

Name
: Mandatory. A unique identifier among attachments that can be used to reference this attachment from other classes using the "Attachment" attribute.

FileName
: Optional. Attachment filename.

  This will usually be the original name of the captured file or the name of the file containing the captured content (e.g. a packet capture file).

Hash
: Optional. A list of hash results for the attachment’s Content.

  The values in this list are computed by taking the raw value of the attachment’s "Content" attribute. The hash result is computed before any other transformation (e.g. Base64 encoding) is applied to the content, so that a receiving IDMEF system may reverse the transformation, apply the same hashing function and obtain the same hash result. See also the definition for the "ContentEncoding" attribute below.

  It is RECOMMENDED that compatible implementations use one of the hashing functions from the SHA-2 [RFC6234] or SHA-3 [NIST.FIPS.202] families to compute the hash results in this list.

Size
: Optional. Length of the content (in bytes).

This value MUST be a non-negative integer.

Ref
Optional. References to sources of information related to the incident and/or vulnerability, and specific to this attachment.

ExternalURI
Optional. If the attachment’s content is available and/or recognizable from an external resource, this is the URI (usually a URL) to that resource.

This MAY also be a URN in a registered or unregistered ad-hoc namespace bearing reasonable information value and uniqueness, such as "urn:mhr:55eaf7effadc07f866d1eaed9c64e7ee49fe081a" or "magnet:?xt=urn:sha1:YNCKHTQCWBTRNJIV4WNAE52SJUQCZO5C".

Note
Optional. Free text human-readable additional note for this attachment.

ContentType
Optional. Internet Media Type of the attachment.

For compatibility reasons, implementations SHOULD prefer one of the well-known media types registered in IANA .

ContentEncoding
Optional. Content encoding.

The following encodings are defined in this version of the specification:

* "json": The content refers to a JSON object which has been serialized to a string using the serialization procedure defined in [RFC8259].

* "base64": The content has been serialized using the Base64 encoding defined in [RFC4648].

The "base64" encoding SHOULD be used when the content contains binary data. If omitted, the "json" encoding MUST be assumed.

Content
Optional. The attachment’s content, in case it is directly embedded inside the message.

For large attachments, it is RECOMMENDED that implementations make use of the "ExternalURI" attribute to refererence a copy of the content saved in an external storage mechanism.

5.8. The JavaScript Object Notation Serialization Method

This serialization method aims to convert IDMEFv2 messages to a format that is easy to parse and process, both by software/hardware processors, as well as humans. It relies on the the JavaScript Object Notation (JSON) Data Interchange Format defined in [RFC8259].

Conforming implementations MUST implement all the requirements specified in [RFC8259].

In addition, the following rules MUST be observed when serializing an IDMEFv2 message:

* The top-level Alert class (Section 4.2) is represented as a JSON object ([RFC8259]). This JSON object is returned to the calling process at the end of the serialization process.

* Aggregate classes are represented as JSON objects and stored as members of the top-level JSON object, using the same name as in the IDMEF data model. E.g. the appears under the name "Analyzer" inside the top-level JSON object.

* Attributes are stored as members of the JSON object representing the class they belong to, using the same name as in the IDMEF data model. E.g. the "Version" attribute from the is stored under the name "Version" inside the top-level JSON object.

* Lists from the IDMEF data model are represented as JSON arrays ([RFC8259]). This also applies to aggregate classes where a list is expected. E.g. the "Sensor" member inside the top-level JSON object contains a list of objects, where each object represents an instance of the .

* The various string-based data types listed in Section 3 are represented as JSON strings ([RFC8259]). Please note that the issues outlined in [RFC8259] regarding strings processing also apply here.

* IDMEF attributes with the "NUMBER" data type are represented as JSON numbers ([RFC8259]).

6. Security Considerations

This document describes a data representation for exchanging security-related information between incident detection system implementations. Although there are no security concerns directly applicable to the format of this data, the data itself may contain security-sensitive information whose confidentiality, integrity, and/or availability may need to be protected.

This suggests that the systems used to collect, transmit, process, and store this data should be protected against unauthorized use and that the data itself should be protected against unauthorized access.

The underlying messaging format and protocol used to exchange instances of the IDMEF MUST provide appropriate guarantees of confidentiality, integrity, and authenticity. The use of a standardized security protocol is encouraged.

The draft-lehmann-idmefv2-https-transport-01.txt document defines the transportation of IDMEF over HTTPs that provides such security.

7. IANA Considerations

This document creates 10 identically structured registries to be managed by IANA:

* Name of the registry group: "Incident Detection Message Exchange Format v2 (IDMEF)"

* URL of the registry: http://www.iana.org/assignments/idmefv2

* Namespace format: A registry entry consists of:

  - Rank. A uniq integer for this namespace. Range starts at 0 and ends at the length of this list. The maximum length of this list is 255.

  - Keyword. A keyword for a given IDMEF attribute. It MUST conform to the formatting specified by the IDMEF "ENUM" data type (Section 3.3.1).

  - Description. A short description of the enumerated keyword.

  - Reference. An optional list of URIs to further describe the value.

* Allocation policy: Expert Review per [RFC8126]. This reviewer will ensure that the requested registry entry conforms to the prescribed formatting. The reviewer will also ensure that the entry is an appropriate value for the attribute per the information model (Section 5).

The registries to be created are named in the "Registry Name" column of Table 10. Each registry is initially populated with ranks, keywords and descriptions that come from an attribute specified in the IDMEF model (Section 5). The initial Ranks, Keywords and Description fields of a given registry are listed in "Initial Values". The "Initial Values" column points to a table in this document that lists and describes each enumerated keyword. Each enumerated keyword in the table gets a corresponding entry in a given registry. The initial value of the Reference field of every registry entry described below should be this document.

Registry Name	Initial Values
Alert-Type	Table 2 (Alert class (Section 5.2))
Alert-Category	Table 3 (Alert class (Section 5.2))
Alert-Cause	Table 4 (Alert class (Section 5.2))
Alert-Priority	Table 6 (Alert class (Section 5.2))
Alert-Status	Table 5 (Alert class (Section 5.2))
Analyzer-Category	Table 7 (Alert class (Section 5.2))
Analyzer-Data	Table 8 (Analyzer class (Section 5.3))
Analyzer-Method	Table 9 (Analyzer class (Section 5.3))

Table 10: IANA Enumerated Value Registries

8. Acknowledgement

The following groups and individuals contributed to the creation of this document and should be recognized for their efforts.

* The former Prelude SIEM team : Thomas Andrejak & Franois Poirotte (Co-authors of the first version of this document), Antoine Luong, Song Tran, Selim Menouar and Camille Gardet

* The core members of the SECEF (SECurity Exchange Format) consortium : Herve Debar (Author of RFC 4765 - IDMEFv1), Guillaume Hiet and Franois Dechelle

* The H2020 7SHIELD project (Safety and Security Standards of Space Systems, ground Segments and Satellite data assets , via prevention, detection, response and mitigation of physical and cyber threats) who implemented in real scale first versions of IDMEFv2 on five pilots around Europe helping greatly to improve it.

* The CESNET team for their work on the [IDEA0] format (based on IDMEFv1) which inspired multiples concepts to IDMEFv2.

* The [ENISA-RIST] Reference Security Incident Taxonomy Working Group

9. References

9.1. Normative References

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[UNICODE] Unicode Consortium, "Unicode Standard", version 14.0.0, 14 September 2021, <https://www.unicode.org/versions/Unicode14.0.0/>.

[ENISA-RIST] ENISA, "Reference Incident Classification Taxonomy", 26 January 2018, <https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md>.

[IANA_media_types] IANA, "Media Types", <http://www.iana.org/assignments/media-types>.

[IANA_hash_function_text_names] IANA, "Hash Function Textual Names", <http://www.iana.org/assignments/hash-function-text-names>.

[UN-LOCODE]
UNECE, "UN/LOCODE Code List by Country and Territory", 6 July 2021, <https://unece.org/trade/cefact/unlocode-code-list-country-and-territory>.

9.2. Informative References

[RFC4765] Debar, H., Curry, D., and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)", RFC 4765, DOI 10.17487/RFC4765, March 2007, <https://www.rfc-editor.org/info/rfc4765>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[NIST.FIPS.202]
Dworkin, Morris J., "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", NIST NIST FIPS 202, DOI 10.6028/NIST.FIPS.202, July 2015, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>.

[WGS84] National Imagery and Mapping Agency, "Department of Defense World Geodetic System 1984: Its Definition and Relationships with Local Geodetic Systems", Third Edition, 1984, <https://apps.dtic.mil/sti/pdfs/ADA280358.pdf>.

[IDEA0] CESNET, "Intrusion Detection Extensible Alert version 0", 25 September 2015, <https://idea.cesnet.cz/en/definition>.

Appendix A. Examples

This section contains several examples of events/incidents which may be described using the IDMEF Data Model defined in.

For each example, the serialization method listed in Section 5 was used on the original IDMEF message to produce a JSON representation.

A.1. Physical intrusion

Listing 1 describes an incident where an unidentified man was detected on company premises near the building where server room A is located.

```
{
  "Version": "2.D.V07",
  "ID": "819df7bc-35ef-40d8-bbee-1901117370b1",
  "Description": "Potential intruder detected",
  "Type": "Physical",
  "Priority": "Low",
  "Status": "Incident",
  "Cause": "Malicious",
  "CreateTime": "2021-05-10T16:52:13.075994+00:00",
  "StartTime": "2021-05-10T16:52:13+00:00",
  "Category": [
    "Access.Forced"
  ],
  "Analyzer": {
    "Name": "BigBrother",
    "Hostname": "bb.acme.com",
    "Model": "Big Brother v42",
    "Category": [
      "PHY.HAR",
      "FRC.FR-CAM"
    ],
    "Data": [
      "Images"
    ],
    "Method": [
      "Movement",
      "Biometric",
      "AI"
    ],
    "IP": "192.0.2.1"
  },
  "Sensor": [
    {
      "IP": "192.0.2.2",
      "Name": "Camera #23",
      "Model": "SuperDuper Camera v1",
      "Location": "Hallway to server room A1"
    }
  ],
  "Source": [
    {
      "Note": "Black Organization, aka. APT 4869"
```

```
      }
    ],
    "Attachment": [
      {
        "Name": "wanted",
        "FileName": "fbi-wanted-poster.jpg",
        "Size": 1234567,
        "Ref": ["https://www.fbi.gov/wanted/topten"],
        "ContentType": "image/jpg",
        "ContentEncoding": "base64",
        "Content": "..."
      },
      {
        "Name": "pic01",
        "Note": "Hi-res picture showing John Doe near server room A1",
        "ExternalURI": ["ftps://192.0.2.1/cam23/20210510165211.jpg"],
        "ContentType": "image/jpg"
      }
    ]
  }
```

A.2. Cyberattack

Listing 2 describes an incident related to a potential bruteforce attack against the "root" user account of the server at 192.0.2.2 and 2001:db8::/32.

```
  {
    "Version": "2.D.V07",
    "ID": "819df7bc-35ef-40d8-bbee-1901117370b2",
    "Description": "Potential bruteforce attack on root user account",
    "Type": "Cyber",
    "Priority": "Medium",
    "CreateTime": "2021-05-10T16:55:29.196408+00:00",
    "StartTime": "2021-05-10T16:55:29+00:00",
    "Category": [
      "Access.Forced"
    ],
    "Analyzer": {
      "Name": "SIEM",
      "Hostname": "siem.acme.com",
      "Model": "Concerto SIEM 5.2",
      "Category": [
        "SIEM.SIEM",
        "SIEM.LOG"
      ],
      "Data": [
        "Log"
```

```
        ],
        "Method": [
          "Monitor",
          "Signature"
        ],
        "IP": "192.0.2.1"
      },
      "Sensor": [
        {
          "IP": "192.0.2.5",
          "Name": "syslog",
          "Hostname": "www.acme.com",
          "Model": "rsyslog 8.2110",
          "Location": "Server room A1, rack 10"
        }
      ],
      "Target": [
        {
          "IP": "192.0.2.2",
          "Hostname": "www.acme.com",
          "Location": "Server room A1, rack 10",
          "User": "root"
        },
        {
          "IP": "2001:db8::/32",
          "Hostname": "www.acme.com",
          "Location": "Server room A1, rack 10",
          "User": "root"
        }
      ]
    }
```

A.3. Server outage

Listing 3 describes an incident where the webserver at "www.example.com" encountered some kind of failure condition resulting in an outage.

```
{
  "Version": "2.D.V07",
  "ID": "819df7bc-35ef-40d8-bbee-1901117370b3",
  "Description": "A server did not reply to an ICMP ping request",
  "Type": "Availability",
  "Priority": "Medium",
  "Status": "Incident",
  "Cause": "Unknown",
  "CreateTime": "2021-05-10T16:59:11.875209+00:00",
  "StartTime": "2021-05-10T16:59:11.875209+00:00",
  "Category": [
    "Availability.Outage"
  ],
  "Analyzer": {
    "Name": "NMS",
    "Hostname": "nms.example.com",
    "Model": "Concerto NMS 5.2",
    "Category": [
      "SIEM.NMS"
    ],
    "Data": [
      "Network"
    ],
    "Method": [
      "Monitor"
    ],
    "IP": "192.0.2.1"
  },
  "Target": [
    {
      "IP": "192.168.1.2",
      "Hostname": "www.acme.com",
      "Service": "website",
      "Location": "Server room A1, rack 10"
    }
  ]
}
```

A.4. Combined incident

Listing 4 describes a combined incident resulting from the correlation of the previous physical, cyber and availability incidents.

```
   {
     "Version": "2.D.V07",
     "ID": "819df7bc-35ef-40d8-bbee-1901117370b4",
     "Description": "Intrusion and Sabotage detected",
     "Type": "Combined",
     "Priority": "High",
     "Status": "Incident",
     "Cause": "Malicious",
     "CreateTime": "2021-05-10T16:59:15.075994+00:00",
     "StartTime": "2021-05-10T16:52:11+00:00",
     "Category": [
       "Access.Unauthorized",
       "Sabotage.Data",
     ,
     "CorrelID": [
       "819df7bc-35ef-40d8-bbee-1901117370b1",
       "819df7bc-35ef-40d8-bbee-1901117370b2",
       "819df7bc-35ef-40d8-bbee-1901117370b3"
     ],
     "Analyzer": {
       "Name": "Correlator",
       "Hostname": "correlator.acme.com",
       "Model": "Concerto Hybrid Correlator v5.2",
       "Category": [
       ],
       "Data": [
         "Alert"
       ],
       "Method": [
         "Correlation"
       ],
       "IP": "192.0.2.1"
     },
     "Source": [
       {
         "Note": "Black Organization, aka. APT 4869"
       }
     ],
     "Target": [
       {
         "Location": "Server room A1"
       },
       {
         "IP": "192.0.2.2",
         "Hostname": "www.acme.com",
         "User": "root"
       },
       {
```

```
        "IP": "192.0.2.2",
        "Hostname": "www.acme.com",
        "Service": "website"
      }
    ]
  }
```

A.5. Hazard incident

Listing 5 describes a heavy snow storm announced in 48h on Paris and Versailles.

```
{
  "Version": "2.D.V07",
  "ID": "819df7bc-35ef-40d8-bbee-1901117370b1",
  "Description": "Snow storm forecast",
  "Priority": "Low",
  "Status": "Incident",
  "Cause": "Hazard",
  "Confidence": 0.8,
  "CreateTime": "2021-05-10T16:52:13.075994+00:00",
  "StartTime": "2021-05-12T10:00:00+00:00",
  "EndTime": "2021-05-12T10:00:00+00:00",
  "Type": ["Physical"],
  "Category": [
    "Meteo.Snow",
    "Meteo.Wind",
    "Meteo.Cold"
  ],
  "Analyzer": {
    "Name": "Weather Monitor",
    "Hostname": "weather.acme.com",
    "IP": "192.0.2.1"
  },
  "Source": [
    {
      "Note": "Heavy snow storm coming from North"
    }
  ],
  "Target": [
    {
      "GeoLocation": "48.8584,2.2945",
      "UnLocation": "FR PAR",
      "Location": "Acme Paris Site"
    },
    {
      "GeoLocation": "48.8019,2.1301",
      "UnLocation": "FR VER",
      "Location": "Acme Versailles Site"
    }
  ]
}
```

Appendix B. JSON Validation Schema (Non-normative)

Listing 5 contains a JSON Schema that can be used to validate incoming IDMEF messages prior to processing. Please note that extraneous linebreaks have been included due to formatting constraints.

```
   {
       "description": "JSON schema for the Incident Detection Message Exchange Format (ID
MEF) version 2",
       "properties": {
           "Version": {
               "description": "The version of the IDMEF format in use by this alert.",
               "type": "string",
               "pattern": "^2\\.[A-Z]\\.V[0-9]{2}$"
           },
           "ID": {
               "description": "Unique identifier for the alert.",
               "$ref": "#/definitions/uuidType"
           },
           "OrganisationName": {
               "description": "Corporate/Main Office Organisation Name Useful if alerts a
re sent to a multi-organisation incident detection system. Example: ACME Corporation",
               "type": "string"
           },
           "OrganisationId": {
               "description": "Corporate/Main Office Organisation ID. Where possible offi
cial organisation ID manage by national authority.",
               "type": "string"
           },
           "EntityName": {
               "description": "Entity Name, monitored by the organisation, where the inci
dent occurred.",
               "type": "string"
           },
           "EntityId": {
               "description": "Entity ID, monitored by the organisation, where the incide
nt occurred.",
               "type": "string"
           },
           "EntitySector": {
               "description": "Economic sector(s) and sub-sector(s) in which the entity o
perates.",
               "type": "array",
               "items": {
                   "type": "string"
               }
           },
           "Type": {
               "description": "Incident type.",
               "type": "array",
               "items": {
                   "$ref": "#/definitions/alertTypeEnum"
               }
           },
           "Category": {
               "description": "Incident category.",
               "type": "array",
               "items": {
                   "$ref": "#/definitions/alertCategoryEnum"
               }
```

```
            },
            "ext-Category": {
                "description": "A means by which to extend the Category attribute.",
                "type": "string"
            },
            "Cause": {
                "description": "Incident cause.",
                "$ref": "#/definitions/causeEnum"
            },
            "Description": {
                "description": "Short free text human-readable description of the event.",
                "type": "string"
            },
            "Status": {
                "description": "Event state in the overall event lifecycle.",
                "$ref": "#/definitions/statusEnum"
            },
            "Priority": {
                "description": "Priority of the alert.",
                "$ref": "#/definitions/priorityEnum"
            },
            "Confidence": {
                "description": "A floating-point value between 0 and 1 indicating the anal
yzer’s confidence.",
                "type": "number",
                "minimum": 0,
                "maximum": 1
            },
            "Note": {
                "description": "Free text human-readable additional note.",
                "type": "string"
            },
            "CreateTime": {
                "description": "Timestamp indicating when the alert was created.",
                "$ref": "#/definitions/timestampType"
            },
            "StartTime": {
                "description": "Timestamp indicating the deduced start of the event.",
                "$ref": "#/definitions/timestampType"
            },
            "EndTime": {
                "description": "Timestamp indicating the deduced end of the event.",
                "$ref": "#/definitions/timestampType"
            },
            "AltNames": {
                "description": "Alternative identifiers.",
                "type": "array",
                "items": {
                    "type": "string"
```

```
                }
            },
            "AltCategory": {
                "description": "Alternate categories from a reference other than ENISA-RIS
T.",
                "type": "array",
                "items": {
                    "type": "string"
                }
            },
            "Ref": {
                "description": "References to sources of information related to the incide
nt.",
                "type": "array",
                "items": {
                    "type": "string",
                    "format": "uri"
                }
            },
            "CorrelID": {
                "description": "Identifiers for the messages which were used as informatio
n sources.",
                "type": "array",
                "items": {
                    "$ref": "#/definitions/uuidType"
                }
            },
            "AggrCondition": {
                "description": "A list of IDMEF fields used to aggregate events.",
                "type": "array",
                "items": {
                    "type": "string"
                }
            },
            "PredID": {
                "description": "A list containing the identifiers of previous messages whi
ch are obsoleted.",
                "type": "array",
                "items": {
                    "$ref": "#/definitions/uuidType"
                }
            },
            "RelID": {
                "description": "A list containing the identifiers of other messages relate
d to this message.",
                "type": "array",
                "items": {
                    "$ref": "#/definitions/uuidType"
                }
            },
            "Analyzer": {
                "type": "object",
                "description": "The Analyzer class describes the module that has analyzed
the data.",
```

```
                "properties": {
                    "ID": {
                        "description": "Unique identifier for the analyzer.",
                        "$ref": "#/definitions/uuidType"
                    },
                    "IP": {
                        "description": "Analyzer IP address.",
                        "$ref": "#/definitions/ipType"
                    },
                    "Name": {
                        "description": "Name of the analyzer.",
                        "type": "string"
                    },
                    "Hostname": {
                        "description": "Hostname of this analyzer.",
                        "type": "string"
                    },
                    "Model": {
                        "description": "Analyzer model description.",
                        "type": "string"
                    },
                    "Category": {
                        "description": "Analyzer categories.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/analyzerCategoryEnum"
                        }
                    },
                    "ext-Category": {
                        "description": "A means by which to extend the Category attribute.
",
                        "type": "string"
                    },
                    "Data": {
                        "description": "Type of data analyzed during the detection.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/analyzerDataEnum"
                        }
                    },
                    "ext-Data": {
                        "description": "A means by which to extend the Data attribute.",
                        "type": "string"
                    },
                    "Method": {
                        "description": "Detection method.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/analyzerMethodEnum"
```

```
                    }
                },
                "ext-Method": {
                    "description": "A means by which to extend the Method attribute.",
                    "type": "string"
                },
                "GeoLocation": {
                    "description": "GPS coordinates for the analyzer.",
                    "$ref": "#/definitions/geolocType"
                },
                "UnLocation": {
                    "description": "Standard UN/Locode for the analyzer.",
                    "$ref": "#/definitions/unlocodeType"
                },
                "Location": {
                    "description": "Internal name for the location of the analyzer.",
                    "type": "string"
                }
            },
            "additionalProperties": false,
            "type": "object",
            "required": ["Name"]
        },
        "Sensor": {
            "type": "array",
            "items": {
                "description": "The Sensor class describes the module that captured th
e data.",
                "properties": {
                    "ID": {
                        "description": "Unique identifier for the sensor.",
                        "$ref": "#/definitions/uuidType"
                    },
                    "IP": {
                        "description": "The sensor’s IP address.",
                        "$ref": "#/definitions/ipType"
                    },
                    "Name": {
                        "description": "Name of the sensor.",
                        "type": "string"
                    },
                    "Hostname": {
                        "description": "The sensor’s hostname.",
                        "type": "string"
                    },
                    "Model": {
                        "description": "The sensor model’s description.",
                        "type": "string"
                    },
```

```
                        "GeoLocation": {
                            "description": "GPS coordinates for the sensor.",
                            "$ref": "#/definitions/geolocType"
                        },
                        "UnLocation": {
                            "description": "Standard UN/Locode for the sensor.",
                            "$ref": "#/definitions/unlocodeType"
                        },
                        "Location": {
                            "description": "Internal name for the location of the sensor."
,
                            "type": "string"
                        },
                        "CaptureZone": {
                            "description": "A string that describes the capture zone of th
e sensor.",
                            "type": "string"
                        }
                    },
                    "additionalProperties": false,
                    "type": "object",
                    "required": ["Name"]
                }
            },
            "Source": {
                "type": "array",
                "items": {
                    "description": "The Source class describes the origin(s) of the event(
s).",
                    "properties": {
                        "ID": {
                            "description": "Unique identifier for the source.",
                            "$ref": "#/definitions/uuidType"
                        },
                        "IP": {
                            "description": "Source IP address.",
                            "$ref": "#/definitions/ipType"
                        },
                        "Hostname": {
                            "description": "Hostname of this source.",
                            "type": "string"
                        },
                        "Note": {
                            "description": "Free text human-readable additional note for t
his source.",
                            "type": "string"
                        },
                        "TI": {
                            "description": "Threat Intelligence data about the source.",
                            "type": "array",
                            "items": {
                                "type": "string"
```

```
                        }
                    },
                    "User": {
                        "description": "User ID or login responsible for the incident.
",
                        "type": "string"
                    },
                    "Email": {
                        "description": "Email address responsible for the incident.",
                        "type": "string",
                        "format": "email"
                    },
                    "Protocol": {
                        "description": "Protocols related to connections from/to this
source.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/protocolType"
                        }
                    },
                    "Port": {
                        "description": "Source ports involved in the incident.",
                        "type": "array",
                        "items": {
                            "type": "integer",
                            "minimum": 1,
                            "maximum": 65535
                        }
                    },
                    "GeoLocation": {
                        "description": "GPS coordinates for the source.",
                        "$ref": "#/definitions/geolocType"
                    },
                    "UnLocation": {
                        "description": "Standard UN/Locode for the source.",
                        "$ref": "#/definitions/unlocodeType"
                    },
                    "Location": {
                        "description": "Internal name for the location of the source."
,
                        "type": "string"
                    },
                    "Attachment": {
                        "description": "Identifiers for attachments related to this so
urce.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/attachmentNameType"
                        }
                    }
                },
                "additionalProperties": false,
```

```
                    "type": "object"
                }
            },
            "Target": {
                "type": "array",
                "items": {
                    "description": "The Target class describes the target(s) impacted by t
he event(s).",
                    "properties": {
                        "ID": {
                            "description": "Unique identifier for the target.",
                            "$ref": "#/definitions/uuidType"
                        },
                        "IP": {
                            "description": "Target IP address.",
                            "$ref": "#/definitions/ipType"
                        },
                        "Hostname": {
                            "description": "Hostname of this target.",
                            "type": "string"
                        },
                        "Note": {
                            "description": "Free text human-readable additional note for t
his target.",
                            "type": "string"
                        },
                        "Service": {
                            "description": "Service or process impacted by the incident.",
                            "type": "string"
                        },
                        "User": {
                            "description": "User ID or login impacted by the incident.",
                            "type": "string"
                        },
                        "Email": {
                            "description": "Email address impacted by the incident.",
                            "type": "string",
                            "format": "email"
                        },
                        "Port": {
                            "description": "Target ports involved in the incident.",
                            "type": "array",
                            "items": {
                                "type": "integer",
                                "minimum": 1,
                                "maximum": 65535
                            }
                        },
                        "GeoLocation": {
                            "description": "GPS coordinates for the target.",
```

```
                        "$ref": "#/definitions/geolocType"
                    },
                    "UnLocation": {
                        "description": "Standard UN/Locode for the target.",
                        "$ref": "#/definitions/unlocodeType"
                    },
                    "Location": {
                        "description": "Internal name for the location of the target."
,
                        "type": "string"
                    },
                    "Attachment": {
                        "description": "Identifiers for attachments related to this ta
rget.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/attachmentNameType"
                        }
                    }
                },
                "additionalProperties": false,
                "type": "object"
            }
        },
        "Attachment": {
            "type": "array",
            "items": {
                "description": "The Attachment class contains additional data captured
 in relation with the event.",
                "properties": {
                    "Name": {
                        "description": "A unique identifier among attachments.",
                        "$ref": "#/definitions/attachmentNameType"
                    },
                    "FileName": {
                        "description": "Attachment filename.",
                        "type": "string"
                    },
                    "Hash": {
                        "description": "A list of hash results for the attachment’s Co
ntent.",
                        "type": "array",
                        "items": {
                            "$ref": "#/definitions/hashType"
                        }
                    },
                    "Size": {
                        "description": "Length of the content (in bytes).",
                        "type": "integer",
                        "minimum": 0
                    },
                    "Ref": {
```

```
                            "description": "References to sources of information related t
o this attachment.",
                            "type": "array",
                            "items": {
                                "type": "string",
                                "format": "uri"
                            }
                        },
                        "ExternalURI": {
                            "description": "URI to an external resource for the attachment
’s content.",
                            "type": "array",
                            "items": {
                                "type": "string",
                                "format": "uri"
                            }
                        },
                        "Note": {
                            "description": "Free text human-readable additional note for t
his attachment.",
                            "type": "string"
                        },
                        "ContentType": {
                            "description": "Internet Media Type of the attachment.",
                            "$ref": "#/definitions/mediatypeType"
                        },
                        "ContentEncoding": {
                            "description": "Content encoding.",
                            "type": "string",
                            "enum": ["json", "base64"]
                        },
                        "Content": {
                            "description": "The attachment’s content.",
                            "type": "string"
                        }
                    },
                    "additionalProperties": false,
                    "type": "object",
                    "required": ["Name"]
                }
            }
        },
        "additionalProperties": false,
        "type": "object",
        "required": ["Analyzer", "Version", "ID", "CreateTime"],
        "definitions": {
            "alertTypeEnum": {
                "enum": ["Cyber", "Physical", "Availability", "Combined"],
                "description": "Possible incident types"
            },
            "alertCategoryEnum": {
```

```
                "enum": [
                    "Abuse.Grooming", "Abuse.Harassment", "Abuse.Coercion", "Abuse.Traffic
king",
                    "Abuse.Extremism", "Abuse.Other", "Access.Compromise", "Access.Escalat
ion",
                    "Access.Backdoor", "Access.Unauthorized", "Access.Tailgating", "Access
.Forced",
                    "Access.Lost", "Access.Cloned", "Access.Authorized", "Access.Other",
                    "Availability.DoS", "Availability.DDoS", "Availability.Outage", "Avail
ability.Failure",
                    "Availability.Misconfiguration", "Availability.Overload", "Availabilit
y.HeartBeat",
                    "Availability.Other", "Fraud.Usage", "Fraud.Copyright", "Fraud.Masquer
ade",
                    "Fraud.Phishing", "Fraud.Corruption", "Fraud.Espionage", "Fraud.Other"
,
                    "Insider.Malicious", "Insider.Negligent", "Insider.Other", "Sabotage.V
andalism",
                    "Sabotage.Graffiti", "Sabotage.Destruction", "Sabotage.Tampering", "Sa
botage.Equipment",
                    "Sabotage.Disruption", "Sabotage.Data", "Sabotage.Other", "Safety.Expl
osion",
                    "Safety.Fire", "Safety.Aggression", "Safety.Sexual", "Safety.Accident"
,
                    "Safety.Hostage", "Safety.Other", "SupplyChain.Disruption", "SupplyCha
in.Compromise",
                    "SupplyChain.Other", "Theft.Equipment", "Theft.Data", "Theft.Machinery
", "Theft.PII",
                    "Theft.IP", "Theft.FinInfo", "Theft.Breach", "Theft.Other", "Operation
al.Misuse",
                    "Operational.PolicyViolation", "Operational.ProcessFailure", "Operatio
nal.Other",
                    "Recon.Network", "Recon.Landscape", "Recon.Aerial", "Recon.OSINT", "Re
con.Other",
                    "National.Terrorism", "National.Conflict", "National.Cyber", "National
.Crime",
                    "National.Environmental", "National.Economic", "National.Societal", "N
ational.Other",
                    "SocialEng.Phishing", "SocialEng.SpearPhishing", "SocialEng.Vishing",
"SocialEng.Smishing",
                    "SocialEng.Pretexting", "SocialEng.Baiting", "SocialEng.QuidProQuo", "
SocialEng.Other",
                    "Malware.Virus", "Malware.Worm", "Malware.Trojan", "Malware.Ransomware
",
                    "Malware.Spyware", "Malware.Adware", "Malware.Rootkit", "Malware.Other
",
                    "Geophysical.Earthquake", "Geophysical.MassMovement", "Geophysical.Vol
canic", "Geophysical.Other",
                    "Meteo.Heat", "Meteo.Cold", "Meteo.Fog", "Meteo.Rain", "Meteo.Snow", "
Meteo.Wind",
                    "Meteo.Other", "Hydro.Flood", "Hydro.Landslide", "Hydro.Wave", "Hydro.
Other",
                    "Climat.Drought", "Climat.LakeOutburst", "Climat.Wildfire", "Climat.Ot
her",
                    "Biological.Epidemic", "Biological.Insect", "Biological.Animal", "Biol
ogical.Zombies",
                    "Biological.Other", "Extraterrestrial.Impact", "Extraterrestrial.Alien
s",
                    "Extraterrestrial.SpaceWeather", "Extraterrestrial.Other", "Other.Unca
tegorized",
                    "Other.Undetermined", "Other.Test", "ext-value"
                ],
```

```
            "description": "Possible incident categories"
        },
        "causeEnum": {
            "enum": ["Normal", "Error", "Malicious", "Malfunction", "Hazard", "Unknown
"],
            "description": "Possible incident causes"
        },
        "statusEnum": {
            "enum": ["Event", "Incident", "Open", "Closed", "FalsePositive"],
            "description": "Possible incident statuses"
        },
        "priorityEnum": {
            "enum": ["Unknown", "Info", "Low", "Medium", "High"],
            "description": "Possible incident priorities"
        },
        "analyzerCategoryEnum": {
```

```
                "enum": [
                    "Undetermined", "APP.BAST", "APP.DAST", "APP.IAST", "APP.RASP", "APP.S
AST",
                    "CLD.CASB", "CLD.CIEM", "CLD.CSPM", "CLD.CWPP", "DDoS.ANTI-DDOS", "DDo
S.SCRUB",
                    "DDoS.WAF-DDOS", "EMAIL.ANTI-PHISH", "EMAIL.DMARC", "EMAIL.SEG", "EMAI
L.SPAM-FILTER",
                    "END.AM", "END.AV", "END.DLP-EP", "END.EDR", "END.EPP", "END.HIDS", "E
ND.HIPS",
                    "END.HPT", "END.RASP", "ID.DCAP", "ID.DLP", "ID.IAM", "ID.IRM", "ID.PA
M", "ID.PIM",
                    "ID.UEBA", "NET.DNS-FW", "NET.DPI", "NET.FW", "NET.NAC", "NET.NBAD", "
NET.NDR",
                    "NET.NGFW", "NET.NIDS", "NET.NIPS", "NET.PROXY", "NET.WAF", "NET.WIDS"
, "NET.WIPS",
                    "OT.IoT-IDS", "OT.OT-IDS", "OT.PLC-SCAN", "PHY.1D-LAS", "PHY.1D-LiDAR"
, "PHY.2D-LAS",
                    "PHY.2D-LiDAR", "PHY.3D-LAS", "PHY.3D-LiDAR", "PHY.ACCESS-CTRL", "PHY.
ADS",
                    "PHY.FR-CAM", "PHY.GLASS-BRK", "PHY.HAR", "PHY.LWIR", "PHY.MOT-SEN", "
PHY.MWIR",
                    "PHY.OBJ-DET", "PHY.SWIR", "PHY.VAD", "PHY.VNIR", "SIEM.ETL", "SIEM.LO
G", "SIEM.NMS",
                    "SIEM.SIEM", "SIEM.SOAR", "TI.CTI", "TI.TI-FEED", "TI.TIP", "VM.ASM",
"VM.PENTEST",
                    "VM.VULN-SCANNER", "ext-value"
                ],
                "description": "Possible analyzer categories"
            },
            "analyzerDataEnum": {
                "enum": [
                    "Undetermined", "Light", "Acoustics", "Contact", "Vibration", "Tempera
ture",
                    "Humidity", "Rain", "Water", "Fog", "Particles", "Seismic", "Magnetic"
,
                    "Images", "Thermal", "Lidar", "Network", "Flow", "Protocol", "Datagram
",
                    "Host", "Connection", "Port", "SNMP", "Authentication", "Log", "File",
                    "Content", "Data", "Reporting", "Alert", "Relay", "External", "ext-val
ue"
                ],
                "description": "Possible analyzer data types"
            },
            "analyzerMethodEnum": {
                "enum": [
                    "Undetermined", "AI", "Anomaly", "Behavioral", "Biometric", "Blackhole
",
                    "Contextual", "Correlation", "Ensemble", "Fingerprinting", "Frequency"
,
                    "Fusion", "Geolocation", "Graph-based", "Heat", "Heuristic", "Honeypot
",
                    "Hygiene", "Integrity", "Metadata", "Monitor", "Movement", "Orchestrat
ion",
                    "Pattern", "Policy", "Predictive", "Protocol", "Recon", "Reputation",
                    "Rule-based", "Sequence", "Signature", "Statistical", "Tarpit",
                    "ThreatIntelligence", "Threshold", "Trend", "ext-value"
                ],
                "description": "Possible analyzer methods"
            },
            "attachmentNameType": {
                "description": "A unique identifier among attachments.",
                "type": "string",
```

```
            "pattern": "^[a-zA-Z0-9]+$"
        },
        "timestampType": {
            "description": "A JSON string containing a timestamp conforming to RFC 333
9.",
            "type": "string",
            "pattern": "^[0-9]{4}-(0[0-9]|1[012])-([0-2][0-9]|3[01])T([0-1][0-9]|2[0-3
]):[0-5][0-9]:([0-5][0-9]|60)(\\.[0-9]+)?(Z|[-+]([0-1][0-9]|2[0-3]):[0-5][0-9])?$"
```

```
            },
            "geolocType": {
                "description": "Geolocation coordinates (e.g. \"+48.75726, +2.299528, +65.
1\").",
                "type": "string",
                "pattern": "^[-+]?([0-9]+(\\.[0-9]*)?)(, ?[-+]?([0-9]+(\\.[0-9]*)?)){1,2}$
"
            },
            "unlocodeType": {
                "description": "A valid UN/LOCODE location (e.g. \"FR PAR\").",
                "type": "string",
                "pattern": "^[A-Z]{2} ?[A-Z]{3}$"
            },
            "ipType": {
                "description": "An Internet Protocol address, either version 4 or version
6.",
                "type": "string",
                "pattern": "^(((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.){3}(25[0-5]|2[0-4
][0-9]|[01]?[0-9][0-9]?)|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7
}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){
1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-
F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-
fA-F]{1,4}){1,6})|:((:[0-9a-fA-F]{1,4}){1,7}|:)|fe80:(:[0-9a-fA-F]{0,4}){0,4}%[0-9a-zA-Z]
{1,}|::(ffff(:0{1,4}){0,1}:){0,1}((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])\\.){3,3}(25[0-
5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])|([0-9a-fA-F]{1,4}:){1,4}:((25[0-5]|(2[0-4]|1{0,1}[0-9]
){0,1}[0-9])\\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9]))$"
            },
            "mediatypeType": {
                "description": "A valid media type (e.g. \"text/plain\").",
                "type": "string",
                "pattern": "^[-!#$%&'*+.^_`|~0-9a-zA-Z]+/[-!#$%&'*+.^_`|~0-9a-zA-Z]+([ \t]
*;[ \t]*[-!#$%&'*+.^_`|~0-9a-zA-Z]+=([-!#$%&'*+.^_`|~0-9a-zA-Z]+|\"([]-~\t !#-[\\x80-\\xF
F]|\\\\([\t 0-9a-zA-Z\\x80-\\xFF]))*\"))*$"
            },
            "uuidType": {
                "description": "Canonical textual representation for an UUID (e.g. \"e5f9b
bae-163e-42f9-a2f2-0daaf78fefb1\")",
                "type": "string",
                "pattern": "^[0-9A-Fa-f]{8}(-[0-9A-Fa-f]{4}){3}-[0-9A-Fa-f]{12}$"
            },
            "protocolType": {
                "description": "A service or protocol name from the IANA registry.",
                "type": "string",
                "pattern": "^[a-zA-Z0-9](-?[a-zA-Z0-9])*$"
            },
            "hashType": {
                "description": "A cryptographic hash (e.g. \"sha256:a02735ed8b10ad432d557b
d4849c0dac3b23d64706e0618716d6df2def338374\")",
                "type": "string",
                "pattern": "^[a-zA-Z0-9-]+:([a-fA-F0-9]{2})+$"
            }
        },
        "$schema": "http://json-schema.org/draft-06/schema#",
        "title": "IDMEF 2"
    }
```

Author's Address

Gilles Lehmann
Telecom SudParis
France
Email: gilles.lehmann@telecom-sudparis.eu