IDMEF
BEST PRACTICES

15/11/2016

SECURITY EXCHANGE FORMAT

TABLE OF CONTENTS

1. Introduction

1.1 Document layout

This document has been produced as part of the SECEF (SECurity Exchange Format) project.

This project is carried by the CS company, in partnership with Télécom Sud Paris and Centrale Supélec, in association with the Ministry of Defence and ANSSI. Its main goal is promoting and improving the security exchange format standards:

- ✓ IDMEF (RFC 4765): https://www.ietf.org/rfc/rfc4765.txt;
- ✓ IODEF (RFC 5070): https://www.ietf.org/rfc/rfc5070.txt.

This document presents best practices of the IDMEF v1 format. It's dedicated to publisher of intrusion detection sensors, to guide them to a proper use of the format.

For each sensor, we show the "key attributes" (even if not mandatory in the RFC IDMEF 4765). For each kind of sensor, we identify relevant data to transmit.

Here are the categories of sensor:

- ✓ HIDS: OSSEC, Samhain, TripWire, for example;
- ✓ NIDS: Suricata, Snort, Darktrace, for example;
- ✓ Antivirus: ClamAV, Avast, Symantec, Kaspersky, for example;
- ✓ Messaging filter: Spamassassin, Exchange, Symantec, for example;
- ✓ Proxy: Squid, Stormshield, for example;
- ✓ WAF: ModSecurity, DenyAll, for example;
- ✓ Wireless: Kismet, for example;
- ✓ Switch / Router / Firewall: Cisco, HP, Dell, Juniper, PaloAlto, for example;

This document is the outcome of multiple working groups, attended by:

- ✓ The Ministry of Defence through the DGA-MI;
- ✓ ANSSI through the Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI);
- ✓ Télécom Sud Paris: Network and Telecommunication Services department;
- ✓ Centrale Supélec: SSIR (Sécurité des Systèmes d'Information et Réseaux) team;
- ✓ CS company, through the Prelude development/rollout team.

2. IDMEF Cross-attributes

This chapter describes the IDMEF attributes to fill in an alert, as a minimum. Also, it presents additional attributes, relevant for future analysis.

2.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF cross-attributes.

Minimum attributes	Additional attributes
alert.messageid	alert.assessment.impact.completion
alert.classification.text	alert.assessment.impact.severity
alert.analyzer.name	alert.assessment.impact.description
alert.analyzer.manufacturer	alert.detect_time
alert.analyzer.class	alert.analyzer.node.name or alert.analyzer.node.address.address
alert.analyzer.analyzerid	
alert.create_time	

Chart 1 : Cross-attributes overview

2.2 Minimum attributes

The attributes that should be filled in are:

- ✓ alert.messageid: string attribute. Used to identify an alert to an analyzer where it's generated.
  - Description RFC 4765, section 4.2.2:
    Optional. A unique identifier for the alert
  - Recommendation: The SECEF consortium recommends the usage of UUIDv1, or to rely on temporal elements. This messageid is generated once throughout the life of the message. For example, the concatenation of the number of seconds and milliseconds.
  - Example UUIDv1: b070f984-892b-11e6-9323;
  - Example UUIDv1: 786d1b69-a603-4eb8-9178-fed2a195a1ed;
  - Example temporal elements: 304987897801565;
  - Example temporal elements: 109489046210987.
- ✓ alert.classification.text: string attribute. This attribute allows a human to understand what the alert is about. It must contain a brief description of the event that triggered the generation of the alert.
  - Description RFC 4765, section 4.2.4.2:
    Required. A vendor-provided string identifying the Alert message.

- Example: Denial of service;
- Example: Installation of unauthorized software programs on a system;
- Example: Usurpation of rights;
- Recommendation: The SECEF consortium recommends to rely on the ISI 002 ETSI standard for the use of generic terms in this IDMEF attribute. In addition, it is recommended to use English terms.

✓ alert.analyzer.name: string attribute. Technical name of the analyzer, generating an alert or source log of an alert.

- Description RFC 4765, section 4.2.4.1:
  Optional. An explicit name for the analyzer that may be easier to understand than the analyzerid.
- Example: sshd;
- Example: prelude-correlator;
- Example: pam;
- Recommendation: The SECEF consortium recommends to indicate the software that has performed the analysis before generating information.

✓ alert.analyzer.manufacturer: string attribute. Name of the analyzer editor.

✓ Description RFC 4765, section 4.2.4.1:
Optional. The manufacturer of the analyzer software and/or hardware.

- Example: OpenSSH;
- Example: CSSI;
- Example: Microsoft;
- Recommendation: The SECEF consortium recommends to indicate the name of the company being editor of the solution or software.

✓ alert.analyzer.class: string attribute. Analyzer class.

- Description RFC 4765, section 4.2.4.1:
  Optional. The class of analyzer software and/or hardware.
- Example: NIDS;
- Example: Antivirus;
- Recommendation: The SECEF consortium recommends using the following names according to each context:
  - Unknown: If the classification of the analyzer is not known;
  - NIDS: Network analysis sensor;
  - SNIDS: Network analysis sensor, based on signatures;
  - HIDS: Host analysis sensor;
  - IPS: Analyzer directly carrying out preventive actions to firewalls levels;
  - File Integrity Checker: If the analyzer performs file integrity verification actions;

- Integrity Checker: If the analyzer performs integrity verification actions;
- Log Analyzer: If the analyzer generates alerts from the logs;
- Network Anti-Virus: Network analysis antivirus;
- Host Anti-Virus: Host analysis antivirus;
- Correlator: Correlator;
- Firewall: Firewall;
- Honeypot: Honeypot;
- Software Monitoring: If the analyzer is a software monitoring system;
- Hardware Monitoring: If the analyzer is a hardware monitoring system;
- Active Vulnerability Scanner: Intrusive scanner of vulnerability;
- Passive Vulnerability Scanner: Passive scanner of vulnerability;
- Alarm Hardware: Alarm system for physical intrusion;
- Private Branch Exchange: Private phone commutator;
- ext-class: Used to extend this attribute.

✓ alert.analyzer.analyzerid: string attribute. Unique identifier of the analyzer.

- Description RFC 4765, section 4.2.4.1:
  Optional. A unique identifier for the analyzer;
  This attribute is only "partially" optional. If the analyzer makes use of the "ident" attributes on other classes to provide unique identifiers for those objects, then it MUST also provide a valid "analyzerid" attribute. This requirement is dictated by the uniqueness requirements of the "ident" attribute (they are unique only within the context of a particular "analyzerid"). If the analyzer does not make use of the "ident" attributes, however, it may also omit the "analyzerid" attribute.
- Recommendation: The SECEF consortium recommends the usage of UUIDv1, or to rely on temporal elements to generate an analyzerid. This analyzerid is generated once throughout the life of the sensor or the manager. For example, the concatenation of the number of seconds and milliseconds;
- Example UUIDv1: 79e3ca62-bf56-11e5-827d;
- Example UUIDv1: 5feb6186-a1e3-11e6-9416-000c2962ca20;
- Example temporal elements: 499467516709673;
- Example temporal elements: 246252564526243.

✓ alert.create_time: date attribute. This attribute contains the time of the alert creation.

- Description RFC 4765, section 4.2.2:
  Exactly one. The time the alert was created. Of the three times that may be provided with an Alert, this is the only one that is required.
- Example: 2016-10-14T16:03:55.28744+02:00
- Example: 2015-08-19T15:30:10.12311

- Recommendation: The SECEF consortium recommends the standard ISO 8601:2000 for those attributes. About time zones, UTC time is used in case the deployed system spans multiple time zones. Otherwise, the local time is used.

2.3 Additional attributes

The additional attributes that can be filled are:

- ✓ alert.assessment.impact.completion: enumerated attribute. This attribute specifies whether the event that generated the alert is a successful action or not.
  - Description RFC 4765, section 4.2.6.1:
    An indication of whether the analyzer believes the attempt that the event describes was successful or not. The permitted values are shown below. There is no default value.
  - The possible values are:
    - failed: The event is a failure;
    - succeeded: The event is a success.
  - Recommendation: The SECEF consortium recommends to make the difference between failed attempt from the attacker and a successful attempt without the attacker has managed to go further.
- ✓ alert.assessment.impact.severity: enumerated attribute. This attribute is used to indicate the severity of the alert.
  - Description RFC 4765, section 4.2.6.1:
    An estimate of the relative severity of the event. The permitted values are shown below. There is no default value.
  - The possible values are:
    - info: Informational alert;
    - low: Low severity alert;
    - medium: Medium severity alert;
    - high: High severity alert.
  - Recommendation: The SECEF consortium recommends to indicate the severity of the sensor alert and not its context. It is the correlator to adapt this severity.
- ✓ alert.assessment.impact.description: string attribute. This attribute is used to describe in detail, without limiting length, the event that triggered the alert.
  - Description RFC 4765, section 4.2.6.1:
    The Impact class is used to provide the analyzer's assessment of the impact of the event on the target(s).
  - Example: Someone tried to login as jdupond from 192.157.2.4 port 42 using the password method
  - Example: A machine has generated a lot of events, targeting a specific machine. It may be a scan of vulnerabilities

- Recommendation: The SECEF consortium recommends using full sentences for better understanding.

✓ alert.detect_time: date attribute. This attribute contains the detection time of the event, source of the alert.

- Description RFC 4765, section 4.2.2:
  Zero or one. The time the event(s) leading up to the alert was detected. In the case of more than one event, the time the first event was detected. In some circumstances, this may not be the same value as CreateTime.
- Example: 2016-10-14T16:03:55.28744+02:00
- Recommendation: The SECEF consortium recommends the standard ISO 8601:2000 for those attributes.

✓ alert.analyzer.node.name or alert.analyzer.node.address.address: string attribute. Address or DNS name of the machine hosting the analyzer.

- Description RFC 4765, section 4.2.7.2:
  Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
  Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 192.168.12.12
- Example: collector.acme.fr
- Recommendation: The SECEF consortium recommends using the most lasting element between the IP address and domain name, and this, each time a name or address must be presented.

3. Specific IDMEF attributes

This chapter describes the minimum IDMEF attributes to fill in, compared to the scope of the sensor. Also, it presents additional attributes, relevant for future analysis.

3.1 HIDS

A HIDS (host-based intrusion detection system) is an intrusion detection system on an operating system. It monitors and analyzes the internal actions of the machine.

This section describes the minimum IDMEF attribute to fill in, for the HIDS type sensors. Also, it presents additional attributes, relevant for future analysis.

Example of HIDS sensors generating IDMEF alerts: OSSEC, Samhain, TripWire.

3.1.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for HIDS.

Minimum attributes	Additional attributes
alert.target.node.address.address or alert.target.node.name	alert.classification.reference.origin
alert.source.user.user_id.type	alert.classification.reference.meaning
alert.source.user.user_id.number	alert.classification.reference.url
alert.source.user.user_id.name	alert.classification.reference.name
alert.source.node.address.address	

Chart 2 : HIDS attributes overview

3.1.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.target.node.address.address or alert.target.node.name: string attribute. Address or DNS name of the machine hosting the analyzer.
  - Description RFC 4765, section 4.2.7.2:
    Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
    Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: 192.168.12.12
  - Example: web-server-1.acme.fr

- ✓ alert.source.user.user_id.type: enumerated attribute. This attributes contains the kind of user described in the alert. It should be « original-user ».
  - Description RFC 4765, section 4.2.7.3.1:
    Optional. The type of user information represented. The permitted values for this attribute are shown below. The default value is "original-user".
  - Value: original-user
- ✓ alert.source.user.user_id.number: numeric attribute. This attributes contains the user UID.
  - Description RFC 4765, section 4.2.7.3.1:
    Zero or one. INTEGER. A user or group number.
  - Example: 513
  - Recommendation: The SECEF consortium recommends to use the most cross-system UID, like those from a directory instead of local ones.
- ✓ alert.source.user.user_id.name: string attribute. The user name.
  - Description RFC 4765, section 4.2.7.3.1:
    Zero or one. STRING. A user or group name.
  - Example: jdupond

Recommendation: The SECEF consortium recommends the CN of the directory, when possible.

If the event which caused the generation of the alert is associated with an action from outside, this attribute need to be filled:

- ✓ alert.source.node.address.address: string attribute. Address or DNS name of the machine hosting the analyzer.
  - Description RFC 4765, section 4.2.7.2:
    Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
    Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: 94.56.32.6
  - Example: dsjghlhr.dyndns.fr

3.1.3 Additional attributes

The additional attributes to fill are:

- ✓ alert.classification.reference.origin: enumerated attribute. On what knowledge database the analyzer relied to detect the suspicious event.
  - Description RFC 4765, section 4.2.7.1:
    Required. The source from which the name of the alert originates. The permitted values for this attribute are shown below. The default value is "unknown".
  - Possible values are:
    - unknown: Unknown knowledge database;

- vendor-specific: editor knowledge database;
- user-specific: use knowledge database;
- bugtraqid: SecurityFocus knowledge database;
- cve: Mitre knowledge database;
- osvdb: osvdb knowledge database;
- cert-specific: CERT knowledge database;

✓ alert.classification.reference.meaning: string attribute. Knowledge database description.

- Description RFC 4765, section 4.2.7.1:
  Optional. The meaning of the reference, as understood by the alert provider. This field is only valid if the value of the <origin> attribute is set to "vendor-specific" or "user-specific".
- Example: OSSEC Rule Wiki Documentation
- Example: RFC 2476
- Example: Windows Event ID
- Recommendation: The SECEF consortium recommends using a simple and generic description. This attribute must not describe the used rule.

✓ alert.classification.reference.url: string attribute. URL of the rule from the knowledge base, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. A URL at which the manager (or the human operator of the manager) can find additional information about the alert. The document pointed to by the URL may include an in-depth description of the attack, appropriate countermeasures, or other information deemed relevant by the vendor.
- Example: http://www.ossec.net/wiki/Rule:31101
- Example: http://rfc.net/rfc2476.html
- Example: http://www.ultimatewindowssecurity.com/events/com304.html
- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.classification.reference.name: string attribute. Name of the knowledge database rule, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Example: Rule:31101
- Example: 5.7.1
- Example: %IDS-4-$1_SIG
- Recommendation: The SECEF consortium recommends using numeric identifiers.

3.2 NIDS

A NIDS (Network-Based Intrusion Detection System) performs the monitoring of network security status. Its detection is primarily built around the detection more or less complex signatures and more or less embedded in an IP packet.

This section describes the minimum IDMEF attribute to fill in, for the NIDS type sensors. Also, it presents additional attributes, relevant for future analysis.

Example of NIDS sensors generating IDMEF alerts: Suricata, Snort, or Darktrace.

3.2.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for NIDS.

Minimum attributes	Additional attributes
alert.target.node.address.address	alert.target.service.iana_protocol_number
alert.target.service.port	alert.target.service.iana_protocol_name
alert.source.node.address.address or alert.source.node.name	alert.target.service.ip_version
alert.source.service.port	alert.target.service.protocol
	alert.target.service.name
	alert.classification.reference.origin
	alert.classification.reference.meaning
	alert.classification.reference.url
	alert.classification.reference.name
	alert.additionnal_data.{type, meaning, data}: raw data

Chart 3 : NIDS attributes overview

3.2.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.target.node.address.address: string attribute. Address or DNS name of the machine being the target of the attack.
  - Description RFC 4765, section 4.2.7.2:
    Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
    Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: 192.168.12.12
  - Example: web-server-1.acme.fr

- ✓ alert.target.service.port: numeric attribute. Port number of the stream end.
  - ➢ Description RFC 4765, section 4.2.7.5:
    Zero or one. INTEGER. The port number being used.
  - ➢ Example: 22 (port de SSH)
  - ➢ Example: 443 (port de HTTPS)
- ✓ alert.source.node.address.address or alert.source.node.name: string attribute. Address or DNS name of the machine being the source of the attack.
  - ➢ Description RFC 4765, section 4.2.7.2:
    Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
    Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - ➢ Example: 94.56.32.6
  - ➢ Example: dsjghlhr.dyndns.fr
- ✓ alert.source.service.port: numeric attribute. Port number of the stream start.
  - ➢ Description RFC 4765, section 4.2.7.5:
    Zero or one. INTEGER. The port number being used.
  - ➢ Example: 45678

3.2.3 Additional attributes

The additional attributes to fill are:

- ✓ alert.target.service.iana_protocol_number: numeric attribute. Integer from IANA to identifying the protocol.
  - ➢ Description RFC 4765, section 4.2.7.5:
    Optional. INTEGER. The IANA protocol number.
  - ➢ Example: 6 (for TCP)
  - ➢ Example: 17 (for UDP)
- ✓ alert.target.service.iana_protocol_name: string attribute. Text from IANA to describe the protocol.
  - ➢ Description RFC 4765, section 4.2.7.5:
    Optional. STRING. The IANA protocol name.
  - ➢ Example: tcp
  - ➢ Example: udp
- ✓ alert.target.service.ip_version: numeric attribute. Protocol version number used by the network stream.
  - ➢ Description RFC 4765, section 4.2.7.5:
    Optional. INTEGER. The IP version number.
  - ➢ Example: 4 (for IPv4)

- Example: 6 (for IPv6)

✓ alert.target.service.protocol: string attribute. Name of the protocol used by the network stream. It must be the decoded protocol, and not the stream protocol.

- Description RFC 4765, section 4.2.7.5:
  Zero or one. STRING. Additional information about the protocol being used. The intent of the protocol field is to carry additional information related to the protocol being used when the <Service> attributes iana_protocol_number or/and iana_protocol_name are filed.
- Example: http
- Example: dns
- Recommendation: The SECEF consortium recommends to describe the protocol of the application layer from the OSI model.

✓ alert.target.service.name: numeric attribute. Name of the service receiving the network stream.

- Description RFC 4765, section 4.2.7.5: Zero or one. STRING. The name of the service. Whenever possible, the name from the IANA list of well-known ports SHOULD be used.
- Example: http
- Example: dns

✓ alert.classification.reference.origin: enumerated attribute. On what knowledge database the analyzer relied to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Required. The source from which the name of the alert originates. The permitted values for this attribute are shown below. The default value is "unknown".
- Possible values are:
  - unknown: unknown knowledge database;
  - vendor-specific: editor knowledge database;
  - user-specific: user knowledge database;
  - bugtraqid: SecurityFocus knowledge database;
  - cve: Mitre knowledge database;
  - osvdb: osvdb knowledge database;
  - cert-specific: CERT knowledge database.

✓ alert.classification.reference.meaning: string attribute. Knowledge database description.

- Description RFC 4765, section 4.2.7.1:
  Optional. The meaning of the reference, as understood by the alert provider. This field is only valid if the value of the <origin> attribute is set to "vendor-specific" or "user-specific".
- Example: OSSEC Rule Wiki Documentation
- Example: RFC 2476
- Example: Windows Event ID

- Recommendation: The SECEF consortium recommends using a simple and generic description. This attribute must not describe the used rule.

✓ alert.classification.reference.url: string attribute. URL of the rule from the knowledge base, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. A URL at which the manager (or the human operator of the manager) can find additional information about the alert. The document pointed to by the URL may include an in-depth description of the attack, appropriate countermeasures, or other information deemed relevant by the vendor.
- Example: http://www.ossec.net/wiki/Rule:31101
- Example: http://rfc.net/rfc2476.html
- Example: http://www.ultimatewindowssecurity.com/events/com304.html
- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.classification.reference.name: string attribute. Name of the knowledge database rule, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Example: Rule:31101
- Example: 5.7.1
- Example: %IDS-4-$1_SIG
- Recommendation: The SECEF consortium recommends using numeric identifiers.

✓ alert.additionnal_data.{type, meaning, data}: raw data detected by the analyzer. “Type” should be « byte-string », “meaning” should be « stream-segment », “data” should be the raw data.

- Description RFC 4765, section 4.2.2:
  Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
- alert.additionnal_data.type: « byte-string » in this case.
- alert.additionnal_data.meaning: « stream-segment » in this case.
- Example for data:
  R0VUIC9jZW50b3MvNi44L29zL3g4Nl82NC9QYWNrYWdlcy9ubWFwLTUuNTEtNC5lbDYueDg2XzY0LnJwbSBIVFRQLzEuMQ0KVXNlci1BZ2VudDogdXJsZ3JhYmJlci8zLjkuMSB5dW0vMy4yLjI5DQpIb3N0OiBmci5taXJyb3IuYmFieWxvbi5uZXR3b3JrDQpBY2NlcHQ6ICovKg0KDQo="
- Recommendation: The SECEF consortium recommends the values of data should be base64 encoded.
- Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill raw data detected by the analyzer.

3.3 Antivirus

An antivirus is a virus detection system on a given machine. The detection is based on signature analysis.

This section describes the minimum IDMEF attribute to fill in, for the antivirus type sensors. Also, it presents additional attributes, relevant for future analysis.

Example of antivirus sensors generating IDMEF alerts: ClamAV, Avast, Symantec, Kaspersky

3.3.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for antivirus.

Minimum attributes	Additional attributes
alert.target.node.address.address or alert.target.node.name	alert.classification.reference.origin
alert.target.file.path	alert.classification.reference.meaning
	alert.classification.reference.url
	alert.classification.reference.name
	alert.source.node.address.address or alert.source.node.name

Chart 4 : Antivirus attributes overview

3.3.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.target.node.address.address or alert.target.node.name: string attribute. Address or DNS name of the machine being infected.
  - Description RFC 4765, section 4.2.7.2:
    Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
    Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: 192.168.12.12
  - Example: web-server-1.acme.fr
- ✓ alert.target.file.path: string attribute. Path to the infected file.
  - Description RFC 4765, section 4.2.7.6:
    Exactly one. STRING. The full path to the file, including the name. The path name should be represented in as "universal" a manner as possible, to facilitate processing of the alert.

- Example: /root/heartbleed.sh
- Example: C:\Windows\System32\hack.exe

3.3.3 Additional attributes

The additional attributes to fill are:

- ✓ alert.classification.reference.origin: enumerated attribute. On what knowledge database the analyzer relied to detect the suspicious event.
  - Description RFC 4765, section 4.2.7.1:
    Required. The source from which the name of the alert originates. The permitted values for this attribute are shown below. The default value is "unknown".
  - Possible values are:
    - unknown: unknown knowledge database;
    - vendor-specific: editor knowledge database;
    - user-specific: user knowledge database;
    - bugtraqid: SecurityFocus knowledge database;
    - cve: Mitre knowledge database;
    - osvdb: osvdb knowledge database;
    - cert-specific: CERT knowledge database.
- ✓ alert.classification.reference.meaning: string attribute. Knowledge database description.
  - Description RFC 4765, section 4.2.7.1:
    Optional. The meaning of the reference, as understood by the alert provider. This field is only valid if the value of the <origin> attribute is set to "vendor-specific" or "user-specific".
  - Example: OSSEC Rule Wiki Documentation
  - Example: RFC 2476
  - Example: Windows Event ID
  - Recommendation: The SECEF consortium recommends using a simple and generic description. This attribute must not describe the used rule.
- ✓ alert.classification.reference.url: string attribute. URL of the rule from the knowledge base, used by the analyzer to detect the suspicious event.
  - Description RFC 4765, section 4.2.7.1:
    Exactly one. STRING. A URL at which the manager (or the human operator of the manager) can find additional information about the alert. The document pointed to by the URL may include an in-depth description of the attack, appropriate countermeasures, or other information deemed relevant by the vendor.
  - Example: http://www.ossec.net/wiki/Rule:31101
  - Example: http://rfc.net/rfc2476.html
  - Example: http://www.ultimatewindowssecurity.com/events/com304.html

- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.classification.reference.name: string attribute. Name of the knowledge database rule, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Example: Rule:31101
- Example: 5.7.1
- Example: %IDS-4-$1_SIG
- Recommendation: The SECEF consortium recommends using numeric identifiers.

If the virus was received from an identified source, the following attribute should be filled:

✓ alert.source.node.address.address or alert.source.node.name: string attribute. Address or DNS name of the machine sending the virus.

- Description RFC 4765, section 4.2.7.2:
  Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
  Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 94.56.32.9
- Example: dsjghlhr.dyndns.fr

3.4 Mail filtering

A mail filtering software cleans your inbox from unsolicited emails and dangerous attachments. It allows for example to block unsolicited advertising and trying to protect you against phishing.

This section describes the minimum IDMEF attribute to fill in, for this kind of sensors. Also, it presents additional attributes, relevant for future analysis.

Example of mail filtering sensor generating IDMEF alerts: spamassassin, Exchange, Symantec.

3.4.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for mail filtering softwares.

Minimum attributes	Additional attributes
alert.target.node.address.category	alert.target.user.user_id.type
alert.target.node.address.address	alert.target.user.user_id.number
alert.source.node.address.category	alert.target.user.user_id.name
alert.source.node.address.address	alert.additionnal_data.{type, meaning, data} : spam score
	alert.additionnal_data.{type, meaning, data} : spam size

Chart 5 : Mail filtering softwares attributes overview

3.4.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.target.node.address.category: enumerated attribute. This attribute should be used to precise the address type. In the antispam case, it should be « e-mail ».
  - Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - Value: e-mail
- ✓ alert.target.node.address.address: string attribute. This attribute contains the recipient e-mail address.
  - Description RFC 4765, section 4.2.7.2:
    Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: jean.dupond@acme.fr
  - Recommendation: The SECEF consortium recommends, if that information is available, to fill all the concerned e-mail, and not just the recipient.
- ✓ alert.source.node.address.category: enumerated attribute. This attribute should be used to precise the address type. It should be « e-mail ».
  - Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - Value: e-mail
- ✓ alert.source.node.address.address: string attribute. This attribute contains the sender e-mail address.
  - Description RFC 4765, section 4.2.7.2:
    Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.

- Example: jean.dupond@acme.fr
- Recommendation: The SECEF consortium recommends, if that information is available, to fill all the concerned e-mail, and not just the sender.

3.4.3 Additional attributes

The additional attributes to fill are:

- ✓ alert.target.user.user_id.type: enumerated attribute. This attribute is used to precise the user type. It should be « target-user ».
  - Description RFC 4765, section 4.2.7.3.1:
    Optional. The type of user information represented. The permitted values for this attribute are shown below. The default value is "original-user".
  - Value: target-user
- ✓ alert.target.user.user_id.number: numeric attribute. This attribute contains the user UID.
  - Description RFC 4765, section 4.2.7.3.1:
    Zero or one. INTEGER. A user or group number.
  - Example: 513
  - Recommendation: The SECEF consortium recommends to use the most cross-system UID, like those from a directory instead of local ones.
- ✓ alert.target.user.user_id.name: string attribute. This attribute contains the user name.
  - Description RFC 4765, section 4.2.7.3.1:
    Zero or one. STRING. A user or group name.
  - Example: jdupond
  - Recommendation: The SECEF consortium recommends the CN of the directory, when possible.
- ✓ alert.additionnal_data.{type, meaning, data}: detected spam score. “Type” should be « integer », “meaning” should be « score », “data” contains the score.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
  - alert.additionnal_data.type: « integer » in this case.
  - alert.additionnal_data.meaning: « score » in this case.
  - Example for data: 5
- ✓ alert.additionnal_data.{type, meaning, data}: size of the detected spam. “Type” should be « integer », “meaning” should be « size », “data” contains the size of the spam.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF

- alert.additionnal_data.type: « integer » in this case.
- alert.additionnal_data.meaning: « size » in this case.
- Example for data: 145192
- Recommendation: The SECEF consortium recommends using “octet” unit.
- Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill the payload and thus its size.

3.5 Proxy

A proxy is a software or hardware equipment performing as a gateway. This allowing to trace the actions performed, apply control rules and potentially make a protocol rupture.

This section describes the minimum IDMEF attribute to fill in, for the proxy type sensors. Also, it presents additional attributes, relevant for future analysis.

Example of proxy sensors generating IDMEF alerts: Squid, Stormshield

3.5.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for proxy.

Minimum attributes	Additional attributes
alert.target.service.web_service.url	alert.additionnal_data.{type, meaning, data} : User-Agent used
alert.target.service.protocol	alert.additionnal_data.{type, meaning, data} : request size
alert.source.node.address.address or alert.source.node.name	
alert.source.user.user_id.type	
alert.source.user.user_id.number	
alert.source.user.user_id.number	

Chart 6 : Proxy attributes overview

3.5.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.target.service.web_service.url: string attribute. This attribute contains the reached URL.
  - Description RFC 4765, section 4.2.7.5.1:
    Exactly one. STRING. The URL in the request.
  - Example: https://www.ssi.gouv.fr/

- Example: http://www.c-s.fr/CS-federe-les-editeurs-de-solutions-de-securite-autour-de-l-IDMEF-Partner-Program_a754.html
- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.target.service.protocol: string attribute. This attribute contains the protocol used by the request to the proxy.

- Description RFC 4765, section 4.2.7.5: Zero or one. STRING. Additional information about the protocol being used. The intent of the protocol field is to carry additional information related to the protocol being used when the <Service> attributes iana_protocol_number or/and iana_protocol_name are filed.
- Example: http
- Example: dns
- Recommendation: The SECEF consortium recommends to describe the protocol of the application layer from the OSI model.

✓ alert.source.node.address.address or alert.source.node.name: string attribute. This attribute contains the IP address or the host name of the user machine, performing the request to the proxy.

- Description RFC 4765, section 4.2.7.2:
  Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
  Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 172.10.23.11
- Example: web-server-1.acme.fr

In case of the proxy require authentication:

✓ alert.source.user.user_id.type: enumerated attribute. This attribute is used to precise the user type. It should be « original-user ».

- Description RFC 4765, section 4.2.7.3.1:
  Optional. The type of user information represented. The permitted values for this attribute are shown below. The default value is "original-user".
- Value: original-user

✓ alert.source.user.user_id.number: numeric attribute. This attribute contains the user UID.

- Description RFC 4765, section 4.2.7.3.1:
  Zero or one. INTEGER. A user or group number.
- Example: 513
- Recommendation: The SECEF consortium recommends to use the most cross-system UID, like those from a directory instead of local ones.

✓ alert.source.user.user_id.name: string attribute. This attribute contains the user name.

- Description RFC 4765, section 4.2.7.3.1:
  Zero or one. STRING. A user or group name.
- Example: jdupond

Recommendation: The SECEF consortium recommends the CN of the directory, when possible.

3.5.3 Additional attributes

The additional attributes to fill are:

- ✓ alert.additionnal_data.{type, meaning, data}: User-Agent used. “Type” should be « string », “meaning” should be « user-agent », “data” contains the user-agent.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
  - alert.additionnal_data.type: « string » in this case.
  - alert.additionnal_data.meaning: « user-agent » in this case.
  - Example for data: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
  - Example for data: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36
  - Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill the User-Agent of a HTTP transaction.
- ✓ alert.additionnal_data.{type, meaning, data}: size of the performed request. “Type” should be « integer », “meaning” should be « bytes_transmitted », “data” contains the size of the request.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
  - alert.additionnal_data.type: « integer » in this case.
  - alert.additionnal_data.meaning: « bytes_transmitted » in this case.
  - Example for data: 145192
  - Recommendation: The SECEF consortium recommends using the “octet” unity.
  - Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill the payload, thus its size.

3.6 WAF

A WAF (Web Application Firewall) is a firewall for web application. It allows you to check the structure and content of requests made to the web server and check if the web server response is correct. The aim is to protect a web application potentially having security vulnerabilities.

This section describes the minimum IDMEF attribute to fill in, for the WAF type sensors. Also, it presents additional attributes, relevant for future analysis.

Example of WAF sensors generating IDMEF alerts: ModSecurity, DenyAll.

3.6.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for WAF.

Minimum attributes	Additional attributes
alert.source.service.iana_protocol_name	alert.classification.reference.origin
alert.source.service.iana_protocol_number	alert.classification.reference.meaning
alert.source.node.address.category	alert.classification.reference.url
alert.source.node.address.address or alert.source.node.name	alert.classification.reference.name
alert.target.service.iana_protocol_name	
alert.target.service.iana_protocol_number	
alert.target.service.name	
alert.target.service.web_service.url	
alert.target.node.address.address or alert.target.node.name	

Chart 7 : WAF attributes overview

3.6.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.source.service.iana_protocol_name: string attribute. This attribute contains the name of the protocol used by the attacker.
  - Description RFC 4765, section 4.2.7.5:
    Optional. STRING. The IANA protocol name.
  - Example: tcp
  - Example: udp
- ✓ alert.source.service.iana_protocol_number: numeric attribute. IANA protocol number.
  - Description RFC 4765, section 4.2.7.5:
    Optional. INTEGER. The IANA protocol number.

- Example: 6 (for TCP)
- Example: 17 (for UDP)

✓ alert.source.node.address.category: enumerated attribute. This attribute contains the type of the address used by the attacker. Possible values are « ipv4-addr » or « ipv6-addr ».

- Description RFC 4765, section 4.2.7.2:
  Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
- Value: ipv4-addr
- Value: ipv6-addr

✓ alert.source.node.address.address or alert.source.node.name: string attribute. This attribute contains the address of the attacker.

- Description RFC 4765, section 4.2.7.2:
  Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
  Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 153.23.53.7
- Example: dsjghlhr.dyndns.fr

✓ alert.target.service.iana_protocol_name: string attribute. This attribute contains the name of the protocol used by the web service.

- Description RFC 4765, section 4.2.7.5:
  Optional. STRING. The IANA protocol name.
- Example: tcp
- Example: udp

✓ alert.target.service.iana_protocol_number: numeric attribute. IANA protocol number.

- Description RFC 4765, section 4.2.7.5:
  Optional. INTEGER. The IANA protocol number.
- Example: 6 (for TCP)
- Example: 17 (for UDP)

✓ alert.target.service.name: string attribute. This attribute contains the name of the impacted web service.

- Description RFC 4765, section 4.2.7.5:
  Zero or one. STRING. The name of the service. Whenever possible, the name from the IANA list of well-known ports SHOULD be used.
- Example: http
- Example: dns

✓ alert.target.service.web_service.url: string attribute. This attribute contains the URL used by the attacker.

- Description RFC 4765, section 4.2.7.5.1:
  Exactly one. STRING. The URL in the request.
- Example: https://www.ssi.gouv.fr/
- Example: http://www.c-s.fr/CS-federe-les-editeurs-de-solutions-de-securite-autour-de-l-IDMEF-Partner-Program_a754.html
- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.target.node.address.address or alert.target.node.name: string attribute. This attribute contains the address of the impacted web server.

- Description RFC 4765, section 4.2.7.2:
  Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
  Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 192.168.3.2
- Example: web-server-1.acme.fr

3.6.3 Additional attributes

The additional attributes to fill are:

✓ alert.classification.reference.origin: enumerated attribute. On what knowledge database the analyzer relied to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Required. The source from which the name of the alert originates. The permitted values for this attribute are shown below. The default value is "unknown".
- Possible values are:
  - unknown: unknown knowledge database;
  - vendor-specific: editor knowledge database;
  - user-specific: user knowledge database;
  - bugtraqid: SecurityFocus knowledge database;
  - cve: Mitre knowledge database;
  - osvdb: osvdb knowledge database;
  - cert-specific: CERT knowledge database.

✓ alert.classification.reference.meaning: string attribute. Knowledge database description.

- Description RFC 4765, section 4.2.7.1:
  Optional. The meaning of the reference, as understood by the alert provider. This field is only valid if the value of the <origin> attribute is set to "vendor-specific" or "user-specific".
- Example: OSSEC Rule Wiki Documentation

- Example: RFC 2476
- Example: Windows Event ID
- Recommendation: The SECEF consortium recommends using a simple and generic description. This attribute must not describe the used rule.

✓ alert.classification.reference.url: string attribute. URL of the rule from the knowledge base, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. A URL at which the manager (or the human operator of the manager) can find additional information about the alert. The document pointed to by the URL may include an in-depth description of the attack, appropriate countermeasures, or other information deemed relevant by the vendor.
- Example: http://www.ossec.net/wiki/Rule:31101
- Example: http://rfc.net/rfc2476.html
- Example: http://www.ultimatewindowssecurity.com/events/com304.html
- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.classification.reference.name: string attribute. Name of the knowledge database rule, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Example: Rule:31101
- Example: 5.7.1
- Example: %IDS-4-$1_SIG
- Recommendation: The SECEF consortium recommends using numeric identifiers.

3.7 Wireless

A wireless sensor can analyze neighboring wireless to detect potential attackers or identity/network thieves.

This section describes the minimum IDMEF attribute to fill in, for the wireless type sensors. Also, it presents additional attributes, relevant for future analysis.

Example of wireless sensors generating IDMEF alerts: Kismet.

3.7.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for wireless sensors.

Minimum attributes	Additional attributes
alert.source.node.address.category	alert.additionnal_data.{type, meaning, data} : BSSID name
alert.source.node.address.address	alert.additionnal_data.{type, meaning, data} : Channel used
alert.target.node.address.category	alert.additionnal_data.{type, meaning, data} : WPS device name
alert.target.node.address.address	

Chart 8 : Wireless sensors attributes overview

3.7.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.source.node.address.category: enumerated attribute. This attribute contains the type of the address. It should be « mac ».
  - Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - Value: mac
- ✓ alert.source.node.address.address: string attribute. This attribute contains the MAC address of the equipment receiving the wireless frame.
  - Description RFC 4765, section 4.2.7.2:
    Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: 66:36:32:64:63:36
- ✓ alert.target.node.address.category: enumerated attribute. This attribute contains the type of the address. It should be « mac ».
  - Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - Example: mac
- ✓ alert.target.node.address.address: string attribute. This attribute contains the MAC address of the equipment sending the wireless frame.
  - Description RFC 4765, section 4.2.7.2:
    Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - Example: 66:36:32:64:63:36

3.7.3 Additional attributes

The additional attributes to fill are:

- ✓ alert.additionnal_data.{type, meaning, data}: BSSID name. “Type” should be « string », “meaning” should be « BSSID », “data” contains the BSSID name.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
  - alert.additionnal_data.type: « string » in this case.
  - alert.additionnal_data.meaning: « BSSID » in this case.
  - Example for data: Wifi-CS-BatB
  - Example for data: FreeWifi
  - Example for data: Livebox-B345
  - Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill the BSSID of a wireless network.
- ✓ alert.additionnal_data.{type, meaning, data}: Channel used. “Type” should be « integer », “meaning” should be « Channel », “data” contains the used channel number.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
  - alert.additionnal_data.type: « integer » in this case.
  - alert.additionnal_data.meaning: « Channel » in this case.
  - Example for data: 10
  - Example for data: 11
  - Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill the used channel number.
- ✓ alert.additionnal_data.{type, meaning, data}: WPS device name. “Type” should be « string », “meaning” should be « WPS Device Name », “data” contains the name of the connected device in WPS.
  - Description RFC 4765, section 4.2.2:
    Zero or more. Information included by the analyzer that does not fit into the data model. This may be an atomic piece of data, or a large amount of data provided through an extension to the IDMEF
  - alert.additionnal_data.type: « string » in this case.
  - alert.additionnal_data.meaning: « WPS Device Name » in this case.
  - Example for data: pc-42251.acme.fr
  - Note IDMEFv2: The IDMEF v2 evolution, proposed by the SECEF consortium, includes new IDMEF attributes to fill the WPS device name.

3.8 Switch / Router / Firewall

A switch, router or firewall is a physical or virtual network equipment to meet certain network problems. This kind of hardware are everywhere in our network infrastructure.

This section describes the minimum IDMEF attribute to fill in, for these types of sensors. Also, it presents additional attributes, relevant for future analysis.

Example of switch / router / firewall sensors generating IDMEF alerts: HP, Dell, Juniper, PaloAlto.

3.8.1 Recap chart

The chart below summarize the additional and as a minimum IDMEF attributes for switchs / routers / firewalls.

Minimum attributes	Additional attributes
alert.source.node.address.category	alert.classification.reference.origin
alert.source.node.address.address	alert.classification.reference.meaning
alert.source.node.address.category	alert.classification.reference.url
alert.source.node.address.address or alert.source.node.name	alert.classification.reference.name
alert.source.interface	alert.target.service.iana_protocol_number
alert.target.node.address.category	alert.target.service.iana_protocol_name
alert.target.node.address.address	alert.target.service.name
alert.target.node.address.category	
alert.target.node.address.address or alert.target.node.name	
alert.target.interface	

Chart 9 : Switchs / routers / firewalls attributes overview

3.8.2 Minimum attributes

The attributes to be filled are:

- ✓ alert.source.node.address.category: enumerated attribute. This attribute contains the type of the address. It should be « mac ».
  - ➢ Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - ➢ Value: mac

- ✓ alert.source.node.address.address: string attribute. This attribute contains the MAC address of the hardware sending the network frame.
  - ➢ Description RFC 4765, section 4.2.7.2:
    Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - ➢ Example: 66:36:32:64:63:36
- ✓ alert.source.node.address.category: enumerated attribute. This attribute contains the type of the address used by the attacker. Possible values are « ipv4-addr » or « ipv6-addr ».
  - ➢ Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - ➢ Value: ipv4-addr
  - ➢ Value: ipv6-addr
- ✓ alert.source.node.address.address or alert.source.node.name: string attribute. This attribute contains the address of the attacker.
  - ➢ Description RFC 4765, section 4.2.7.2:
    Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
    Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
  - ➢ Example: 153.23.53.7
  - ➢ Example: dsjghlhr.dyndns.fr
- ✓ alert.source.interface: string attribute. This attribute contains the network interface from where the attack came.
  - ➢ Description RFC 4765, section 4.2.7.2:
    Optional. May be used by a network-based analyzer with multiple interfaces to indicate which interface this source was seen on.
  - ➢ Example: FastEthernet0/3/0
  - ➢ Example: eth0
- ✓ alert.target.node.address.category: enumerated attribute. This attribute contains the type of the address. It should be « mac ».
  - ➢ Description RFC 4765, section 4.2.7.2:
    Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
  - ➢ Example: mac
- ✓ alert.target.node.address.address: string attribute. This attribute contains the MAC address of the hardware receiving the network frame.

- Description RFC 4765, section 4.2.7.2:
  Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 66:36:32:64:63:36

✓ alert.target.node.address.category: enumerated attribute. This attribute contains the type of address targeted by the attacker. Possible values are « ipv4-addr » or « ipv6-addr ».

- Description RFC 4765, section 4.2.7.2:
  Optional. The "domain" from which the name information was obtained, if relevant. The permitted values for this attribute are shown in the table below. The default value is "unknown".
- Value: ipv4-addr
- Value: ipv6-addr

✓ alert.target.node.address.address or alert.target.node.name: string attribute. This attribute contains the targeted address.

- Description RFC 4765, section 4.2.7.2:
  Name: Zero or one. STRING. The name of the equipment. This information MUST be provided if no Address information is given.
  Address: Zero or more. The network or hardware address of the equipment. Unless a name (above) is provided, at least one address must be specified.
- Example: 153.23.53.7
- Example: dsjghlhr.dyndns.fr

✓ alert.target.interface: string attribute. This attribute contains the name of the targeted network interfaces.

- Description RFC 4765, section 4.2.7.2:
  Optional. May be used by a network-based analyzer with multiple interfaces to indicate which interface this source was seen on.
- Example: FastEthernet0/3/0
- Example: eth0

3.8.3 Additional attributes

The additional attributes to fill are:

✓ alert.classification.reference.origin: enumerated attribute. On what knowledge database the analyzer relied to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Required. The source from which the name of the alert originates. The permitted values for this attribute are shown below. The default value is "unknown".
- Possible values are:
  - unknown: unknown knowledge database;
  - vendor-specific: editor knowledge database;

- user-specific: user knowledge database;
- bugtraqid: SecurityFocus knowledge database;
- cve: Mitre knowledge database;
- osvdb: osvdb knowledge database;
- cert-specific: CERT knowledge database.

✓ alert.classification.reference.meaning: string attribute. Knowledge database description.

- Description RFC 4765, section 4.2.7.1:
  Optional. The meaning of the reference, as understood by the alert provider. This field is only valid if the value of the <origin> attribute is set to "vendor-specific" or "user-specific".
- Example: OSSEC Rule Wiki Documentation
- Example: RFC 2476
- Example: Windows Event ID
- Recommendation: The SECEF consortium recommends using a simple and generic description. This attribute must not describe the used rule.

✓ alert.classification.reference.url: string attribute. URL of the rule from the knowledge base, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. A URL at which the manager (or the human operator of the manager) can find additional information about the alert. The document pointed to by the URL may include an in-depth description of the attack, appropriate countermeasures, or other information deemed relevant by the vendor.
- Example: http://www.ossec.net/wiki/Rule:31101
- Example: http://rfc.net/rfc2476.html
- Example: http://www.ultimatewindowssecurity.com/events/com304.html
- Recommendation: The SECEF consortium recommends using complete and non-redirect URL, preserving its durability.

✓ alert.classification.reference.name: string attribute. Name of the knowledge database rule, used by the analyzer to detect the suspicious event.

- Description RFC 4765, section 4.2.7.1:
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Example: Rule:31101
- Example: 5.7.1
- Example: %IDS-4-$1_SIG
- Recommendation: The SECEF consortium recommends using numeric identifiers.

✓ alert.target.service.iana_protocol_number: numeric attribute. Integer from IANA to describe the protocol.

- Description RFC 4765, section 4.2.7.5:
  Optional. INTEGER. The IANA protocol number.

- Example: 6 (for TCP)
- Example: 17 (for UDP)

✓ alert.target.service.iana_protocol_name: string attribute. Text from IANA to describe the protocol.

- Description RFC 4765, section 4.2.7.5:
  Optional. STRING. The IANA protocol name.
- Example: tcp
- Example: udp

✓ alert.target.service.name: string attribute. This attribute contains the service name of the targeted network hardware.

- Description RFC 4765, section 4.2.7.5:
  Zero or one. STRING. The name of the service. Whenever possible, the name from the IANA list of well-known ports SHOULD be used.
- Example: Cisco Discovery Protocol
- Recommendation: The SECEF consortium recommends using the full name of the service, and not its short name.

4. Conclusion

For any comments, or suggestions, please use the SECEF exchange boards:
https://redmine.secef.net/projects/secef/boards

This document is a draft, and destined to be completed.

Versioning

Version	Date	Written by	Verified by	Approved by	Reason
1.0	26/10/2016	T. Andrejak	C. Gardet C. Widmer	G. Lehmann	Document creation