IDMEF
BEST PRACTICES

15/11/2016

SECURITY EXCHANGE FORMAT

SOMMAIRE

1. Introduction

1.1 Présentation du document

Ce document a été réalisé dans le cadre du projet SECEF (SECurity Exchange Format).

Ce projet est porté par la société CS en partenariat avec Télécom Sud Paris et Centrale Supélec et en collaboration avec le Ministère de la Défense et l'ANSSI. Son objectif est la promotion et l'amélioration des formats standards d'échange d'information de sécurité :

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

Ce document propose des bonnes pratiques d'utilisation du format IDMEF v1. Il est principalement dédié aux sondes de détection d'intrusion pour les guider vers la bonne utilisation du format.

Pour chaque sonde, nous présentons les champs « incontournables » (même si non obligatoires dans la RFC IDMEF 4765). Pour chaque catégorie de sondes, nous identifions les informations les plus pertinentes, également à renseigner.

Nous avons isolé les catégories suivantes :

- ✓ HIDS : par exemple OSSEC, Samhain, TripWire ;
- ✓ NIDS : par exemple Suricata, Snort, Darktrace ;
- ✓ Antivirus : par exemple ClamAV, Avast, Symantec, Kaspersky ;
- ✓ Filtrage de messagerie : par exemple spamassassin, Exchange, Symantec ;
- ✓ Proxy : par exemple Squid, Stormshield ;
- ✓ WAF : par exemple ModSecurity, DenyAll ;
- ✓ Wifi : par exemple Kismet ;
- ✓ Switch / Routeur / Pare-feu : par exemple Cisco, HP, Dell, Juniper, PaloAlto.

Ce document est le résultat de plusieurs groupes de travail auxquels ont participé :

- ✓ Le Ministère de la Défense au travers de la DGA-MI ;
- ✓ L'ANSSI par le Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) ;
- ✓ Télécom Sud Paris : Département Réseaux et Services de télécommunication ;
- ✓ Centrale Supélec : Equipe SSIR (Sécurité des Systèmes d'Information et Réseaux) ;
- ✓ La société CS représentée par l'équipe de développement/déploiement Prelude.

2. Champs IDMEF transverse

Ce chapitre décrit les champs IDMEF à remplir à minima. Il indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

2.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs transverses à minima et complémentaires.

Champs à minima	Champs complémentaires
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 ou alert.analyzer.node.address.address
alert.analyzer.analyzerid	
alert.create_time	

Tableau 1 : Synthèse des champs transverses

2.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.messageid : champ libre. Il permet d'identifier de façon unique une alerte vis-à-vis de l'analyseur l'ayant générée.
  - ➢ Description RFC 4765, chapitre 4.2.2 :

    Optional. A unique identifier for the alert
  - ➢ Recommandation : Le consortium SECEF recommande l'utilisation d'UUIDv1, ou de se baser sur des éléments temporels. Ce messageid est généré une seule fois tout au long de la vie du message. Par exemple la concaténation du nombre de secondes et de milisecondes.
  - ➢ Exemple UUIDv1 : b070f984-892b-11e6-9323 ;
  - ➢ Exemple UUIDv1 : 786d1b69-a603-4eb8-9178-fed2a195a1ed.
  - ➢ Exemple éléments temporels : 304987897801565
  - ➢ Exemple éléments temporels : 109489046210987
- ✓ alert.classification.text : champ libre. Ce champ permet à un humain de comprendre à quoi correspond cette alerte. Il doit contenir une description très brève de l'évènement ayant déclenché la génération de l'alerte.
  - ➢ Description RFC 4765, chapitre 4.2.4.2 :

Required. A vendor-provided string identifying the Alert message.

- Exemple : Denial of service
- Exemple : Installation of unauthorized software programs on a system
- Exemple : Usurpation of rights
- Recommandation : Le consortium SECEF recommande de se baser sur la norme ETSI ISI 002 pour l'utilisation de termes génériques dans ce champ IDMEF. De plus, il est recommandé d'utiliser des termes anglais.

✓ alert.analyzer.name : champ libre. Nom technique de l'analyseur, générant une alerte ou un log source d'une alerte.

- Description RFC 4765, chapitre 4.2.4.1 :

  Optional. An explicit name for the analyzer that may be easier to understand than the analyzerid.
- Exemple : sshd
- Exemple : prelude-correlator
- Exemple : pam
- Recommandation : Le consortium SECEF recommande d'indiquer le logiciel ayant réalisé une certaine analyse avant de générer l'information.

✓ alert.analyzer.manufacturer : champ libre. Nom de l'éditeur de l'analyseur.

- Description RFC 4765, chapitre 4.2.4.1 :

  Optional. The manufacturer of the analyzer software and/or hardware.
- Exemple : OpenSSH
- Exemple : CSSI
- Exemple : Microsoft
- Recommandation : Le consortium SECEF recommande d'indiquer le nom de la société étant éditeur de la solution ou du logiciel.

✓ alert.analyzer.class : champ libre. Classe de l'analyseur.

- Description RFC 4765,chapitre 4.2.4.1 :

  Optional. The class of analyzer software and/or hardware.
- Exemple : NIDS
- Exemple : Antivirus
- Recommandation : Le consortium SECEF conseille d'utiliser les dénominations suivantes en fonction de chaque contexte :
  - Unknown : Si la classification de l'analyseur n'est pas connue.
  - NIDS : Sonde d'analyse réseau
  - SNIDS : Sonde d'analyse réseau basée sur des signatures
  - HIDS : Sonde d'analyse machine

- IPS : Analyseur effectuant directement des actions de prévention aux niveaux des pare-feu.
- File Integrity Checker : Si l'analyseur effectue des actions de vérification d'intégrité de fichiers.
- Integrity Checker : Si l'analyseur effectue des actions de vérification d'intégrité
- Log Analyzer : Si l'analyseur génère des alertes à partir des journaux.
- Network Anti-Virus : Antivirus analysant le réseau
- Host Anti-Virus : Antivirus analysant une machine
- Correlator : Corrélateur
- Firewall : Parefeu
- Honeypot : Analyseur de type « pot de miel »
- Software Monitoring : Si l'analyseur est un système de supervision logiciel
- Hardware Monitoring : Si l'analyseur est un système de supervision matériel
- Active Vulnerability Scanner : Scanneur intrusif de détection de vulnérabilités
- Passive Vulnerability Scanner : Scanneur passif de détection de vulnérabilités
- Alarm Hardware : Système d'alarme pour les intrusions physiques
- Private Branch Exchange : Commutateur de téléphone privé
- ext-class : Valeur utilisée pour étendre cet attribut

✓ alert.analyzer.analyzerid : champ libre. Identifiant unique de l'analyseur par rapport à sa chaine de remontée d'informations

- Description RFC 4765, chapitre 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.

- Recommandation : Le consortium SECEF recommande l'utilisation d'UUIDv1, ou de se baser sur des éléments temporels pour générer un analyzerid. Cet analyzerid est généré une seule fois tout au long de la vie de la sonde ou du manager. Par exemple la concaténation du nombre de secondes et de millisecondes ;
- Exemple UUIDv1 : 79e3ca62-bf56-11e5-827d ;
- Exemple UUIDv1 : 5feb6186-a1e3-11e6-9416-000c2962ca20 ;
- Exemple éléments temporels : 499467516709673 ;
- Exemple éléments temporels : 246252564526243 ;

✓ alert.create_time : champ temps. Ce champ contient l'heure de création de l'alerte.

- Description RFC 4765, chapitre 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.

- Exemple : 2016-10-14T16:03:55.28744+02:00
- Exemple : 2015-08-19T15:30:10.12311
- Recommandation : Le consortium SECEF recommande le suivi de la RFC en respectant la norme ISO 8601:2000 pour le contenu de ces champs. Concernant les fuseaux horaires, l'horaire UTC est employé dans le cas où le système déployé s'étend sur plusieurs fuseaux. Dans le cas contraire, le temps avec le fuseau local est employé.

2.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

- ✓ alert.assessment.impact.completion : champ ayant une liste de valeurs finie. Ce champ permet d'indiquer si l'évènement ayant généré l'alerte est une action réussie ou non.
  - Description RFC 4765, chapitre 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.
  - Les valeurs possibles sont les suivantes :
    - failed : L'évènement est un échec ;
    - succeeded : L'évènement est un succès.
  - Recommandation : Le consortium SECEF recommande de bien faire la différence entre tentative échouée de la part de l'attaquant et une tentative réussie sans pour autant que l'attaquant ait réussi à aller plus loin.
- ✓ alert.assessment.impact.severity : champ ayant une liste de valeurs finie. Ce champ permet d'indiquer la sévérité de l'alerte.
  - Description RFC 4765, chapitre 4.2.6.1 :
    An estimate of the relative severity of the event. The permitted values are shown below. There is no default value.
  - Les valeurs possibles sont les suivantes :
    - info : Alerte de sévérité informationnelle.
    - low : Alerte de sévérité basse
    - medium : Alerte de sévérité moyenne
    - high : Alerte de sévérité haute.
  - Recommandation : le consortium SECEF recommande d'indiquer la sévérité de l'alerte vis-à-vis de la sonde et non vis-à-vis de son contexte. C'est au corrélateur d'adapter cette sévérité.
- ✓ alert.assessment.impact.description : champ libre. Ce champ permet de décrire de manière plus précise, sans limitation de longueur, l'évènement ayant généré l'alerte.

- Description RFC 4765, chapitre 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).
- Exemple : Someone tried to login as jdupond from 192.157.2.4 port 42 using the password method
- Exemple : Une machine a généré beaucoup d'évènements en direction d'une machine précise. Il se peut que ce soit un scan de vulnérabilités
- Recommandation : Le consortium SECEF recommande l'utilisation de phrase complète pour une meilleure compréhension.

✓ alert.detect_time : champ temps. Ce champ contient l'heure de détection de l'évènement ayant amené à créer l'alerte.

- Description RFC 4765, chapitre 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.
- Exemple : 2016-10-14T16:03:55.28744+02:00
- Recommandation : Le consortium SECEF recommande le suivi de la RFC en respectant la norme ISO 8601:2000 pour le contenu de ces champs.

✓ alert.analyzer.node.name ou alert.analyzer.node.address.address : champ libre. Adresse ou nom DNS de la machine hébergeant l'analyseur.

- Description RFC 4765, chapitre 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.
- Exemple : 192.168.12.12
- Exemple : collector.acme.fr
- Recommandation : le consortium SECEF recommande l'utilisation de l'élément le plus pérenne entre l'adresse IP et le nom de domaine, et ce, pour chaque fois qu'un nom ou une adresse doit être présenté.

3. Champs IDMEF spécifiques

Ce chapitre décrit les champs IDMEF à remplir à minima par rapport au domaine d'application de la sonde. Il indique aussi des champs complémentaires qui sont un plus pour l'analyse future également pour chaque domaine d'application.

3.1 HIDS

Un HIDS (host-based intrusion detection system) est un système de détection d'intrusion sur un système d'exploitation. Il supervise et analyse les actions internes de la machine.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type HIDS. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde HIDS générant des alertes au format IDMEF : OSSEC, Samhain ou encore TripWire.

3.1.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux HIDS, à minima et complémentaires.

Champs à minima	Champs complémentaires
alert.target.node.address.address ou 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	

Tableau 2 : Synthèse des champs spécifiques HIDS

3.1.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.target.node.address.address ou alert.target.node.name: champ libre. Adresse ou nom DNS de la machine hébergeant l'analyseur.
  - ➢ Description RFC 4765, chapitre 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.
  - ➢ Exemple : 192.168.12.12

- Exemple : web-server-1.acme.fr

✓ alert.source.user.user_id.type : champ ayant une liste de valeurs finie. Ce champ précise le type d'utilisateur décrit. Il doit valoir « original-user ».

- Description RFC 4765, chapitre 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".
- Valeur : original-user

✓ alert.source.user.user_id.number : champ numérique. Ce champ contient l'UID de l'utilisateur.

- Description RFC 4765, chapitre 4.2.7.3.1 :
  Zero or one. INTEGER. A user or group number.
- Exemple : 513
- Recommandation : Le consortium SECEF recommande d'utiliser les UID les plus transverses au système, par exemple ceux de l'annuaire plutôt que les UID locaux.

✓ alert.source.user.user_id.name : champ libre. Ce champ contient le nom de l'utilisateur.

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

Recommandation : le consortium SECEF recommande l'utilisation du CN de l'annuaire si possible.

Si l'évènement ayant provoqué la génération de l'alerte est liée à une action provenant de l'extérieur, le champ suivant doit être rempli :

✓ alert.source.node.address.address : champ libre. Adresse ou nom DNS de la machine ayant fait déclencher l'évènement.

- Description RFC 4765, chapitre 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.
- Exemple : 94.56.32.6
- Exemple : dsjghlhr.dyndns.fr

3.1.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

✓ alert.classification.reference.origin : champ ayant une liste de valeurs finie. Sur quelle base de connaissance l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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".

- Les valeurs possibles sont les suivantes :
  - unknown : base de connaissance non connue
  - vendor-specific : base de connaissance fournie par l'éditeur
  - user-specific : base de connaissance fournie par l'utilisateur
  - bugtraqid : base de connaissance SecurityFocus
  - cve : base de connaissance Mitre
  - osvdb : base de connaissance osvdb
  - cert-specific : base de connaissance provenant d'un CERT

✓ alert.classification.reference.meaning : champ libre. Description de la base de connaissance.

- Description RFC 4765, chapitre 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".
- Exemple : OSSEC Rule Wiki Documentation
- Exemple : RFC 2476
- Exemple : Windows Event ID
- Recommandation : Le consortium SECEF recommande d'utiliser une description simple et générique. Ce champ ne doit pas détailler la règle décrite.

✓ alert.classification.reference.url : champ libre. URL d'accès à la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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.
- Exemple : http://www.ossec.net/wiki/Rule:31101
- Exemple : http://rfc.net/rfc2476.html
- Exemple : http://www.ultimatewindowssecurity.com/events/com304.html
- Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.

✓ alert.classification.reference.name : champ libre. Nom de la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 4.2.7.1 :
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Exemple : Rule:31101
- Exemple : 5.7.1
- Exemple : %IDS-4-$1_SIG
- Recommandation : Le consortium SECEF recommande l'utilisation d'identifiants numériques

3.2 NIDS

Un NIDS (Network Based Intrusion Detection System) réalise la surveillance de l'état de sécurité du réseau. Sa détection est principalement construite autour de la détection de signatures plus ou moins complexes et plus ou moins enfouies dans un paquet IP.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type NIDS. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde NIDS générant des alertes au format IDMEF : Suricata, Snort ou Darktrace.

3.2.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux NIDS, à minima et complémentaires.

Champs à minima	Champs complémentaires
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 ou 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}: donnée brute détectée par l'analyseur

Tableau 3 : Synthèse des champs spécifiques NIDS

3.2.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.target.node.address.address : champ libre. Adresse ou nom DNS de la machine étant la cible de l'attaque.
  - Description RFC 4765, chapitre 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.
  - Exemple : 192.168.12.12

- Exemple : web-server-1.acme.fr

✓ alert.target.service.port : champ numérique. Numéro du port d'arrivée du flux.

- Description RFC 4765, chapitre 4.2.7.5 :
  Zero or one. INTEGER. The port number being used.
- Exemple : 22 (port de SSH)
- Exemple : 443 (port de HTTPS)

✓ alert.source.node.address.address ou alert.source.node.name: champ libre. Adresse ou nom DNS de la machine étant à l'origine de l'attaque.

- Description RFC 4765, chapitre 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.
- Exemple : 94.56.32.6
- Exemple : dsjghlhr.dyndns.fr

✓ alert.source.service.port : champ numérique. Numéro du port de départ du flux.

- Description RFC 4765, chapitre 4.2.7.5 :
  Zero or one. INTEGER. The port number being used.
- Exemple : 45678

3.2.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

✓ alert.target.service.iana_protocol_number : champ numérique. Entier fournit par IANA pour identifier le protocole.

- Description RFC 4765, chapitre 4.2.7.5 :
  Optional. INTEGER. The IANA protocol number.
- Exemple : 6 (pour TCP)
- Exemple : 17 (pour UDP)

✓ alert.target.service.iana_protocol_name : champ libre. Texte fournit par IANA pour décrire le nom du protocole.

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

✓ alert.target.service.ip_version : champ numérique. Version du protocole utilisé par le flux réseau.

- Description RFC 4765, chapitre 4.2.7.5 :
  Optional. INTEGER. The IP version number.

- Exemple : 4 (pour IPv4)
- Exemple : 6 (pour IPv6)

✓ alert.target.service.protocol : champ libre. Nom du protocole utilisé par le flux réseau. Il s'agit du protocole décodé sur le flux, et non le protocole du flux.

- Description RFC 4765, chapitre 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.
- Exemple : http
- Exemple : dns
- Recommandation : le consortium SECEF recommande de décrire le protocole de la couche applicative du modèle OSI.

✓ alert.target.service.name : champ numérique. Nom du service recevant le flux réseau.

- Description RFC 4765, chapitre 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.
- Exemple : http
- Exemple : dns

✓ alert.classification.reference.origin : champ ayant une liste de valeurs finie. Sur quelle base de connaissance l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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".
- Les valeurs possibles sont les suivantes :
  - unknown : base de connaissance non connue
  - vendor-specific : base de connaissance fournie par l'éditeur
  - user-specific : base de connaissance fournie par l'utilisateur
  - bugtraqid : base de connaissance SecurityFocus
  - cve : base de connaissance Mitre
  - osvdb : base de connaissance osvdb
  - cert-specific : base de connaissance provenant d'un CERT

✓ alert.classification.reference.meaning : champ libre. Description de la base de connaissance.

- Description RFC 4765, chapitre 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".
- Exemple : OSSEC Rule Wiki Documentation
- Exemple : RFC 2476

- Exemple : Windows Event ID
- Recommandation : Le consortium SECEF recommande d'utiliser une description simple et générique. Ce champ ne doit pas détailler la règle décrite.

✓ alert.classification.reference.url : champ libre. URL d'accès à la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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.
- Exemple : http://www.ossec.net/wiki/Rule:31101
- Exemple : http://rfc.net/rfc2476.html
- Exemple : http://www.ultimatewindowssecurity.com/events/com304.html
- Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.

✓ alert.classification.reference.name : champ libre. Nom de la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 4.2.7.1 :
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Exemple : Rule:31101
- Exemple : 5.7.1
- Exemple : %IDS-4-$1_SIG
- Recommandation : Le consortium SECEF recommande l'utilisation d'identifiants numériques

✓ alert.additionnal_data.{type, meaning, data} : donnée brute détectée par l'analyseur. Type doit valoir « byte-string », meaning doit valoir « stream-segment », data contient la donnée brute.

- Description RFC 4765, chapitre 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 : vaut « byte-string » dans le cas présent.
- alert.additionnal_data.meaning : vaut « stream-segment » dans le cas présent
- Exemple pour data :
  R0VUIC9jZW50b3MvNi44L29zL3g4Nl82NC9QYWNrYWdlcy9ubWFwLTUuNTEtNC5lbDYueDg2XzY0LnJwbSBIVFRQLzEuMQ0KVXNlci1BZ2VudDogdXJsZ3JhYmJlci8zLjkuMSB5dW0vMy4yLjI5DQpIb3N0OiBmci5taXJyb3IuYmFieWxvbi5uZXR3b3JrDQpBY2NlcHQ6ICovKg0KDQo="
- Recommandation : Le consortium SECEF recommande que la valeur de data soit en base64.

- Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sien d'IDMEF les données brutes détectées par l'analyseur.

3.3 Antivirus

Un antivirus est un système de détection de virus informatiques dans une machine donnée. La détection est basée sur l'analyse par signature.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type Antivirus. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde Antivirus générant des alertes au format IDMEF : ClamAV, Avast, Symantec, Kaspersky

3.3.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux antivirus, à minima et complémentaires.

Champs à minima	Champs complémentaires
alert.target.node.address.address ou 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 ou alert.source.node.name

Tableau 4 : Synthèse des champs spécifiques Antivirus

3.3.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.target.node.address.address ou alert.target.node.name : champ libre. Adresse ou nom DNS de la machine infectée.
  - Description RFC 4765, chapitre 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.
  - Exemple : 192.168.12.12
  - Exemple : web-server-1.acme.fr
- ✓ alert.target.file.path : champ libre. Chemin vers le fichier infecté.

- Description RFC 4765, chapitre 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.
- Exemple : /root/heartbleed.sh
- Exemple : C:\Windows\System32\hack.exe

3.3.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

- ✓ alert.classification.reference.origin : champ ayant une liste de valeurs finie. Sur quelle base de connaissance l'analyseur s'est reposé pour détecter l'évènement suspect.
  - Description RFC 4765, chapitre 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".
  - Les valeurs possibles sont les suivantes :
    - unknown : base de connaissance non connue
    - vendor-specific : base de connaissance fournie par l'éditeur
    - user-specific : base de connaissance fournie par l'utilisateur
    - bugtraqid : base de connaissance SecurityFocus
    - cve : base de connaissance Mitre
    - osvdb : base de connaissance osvdb
    - cert-specific : base de connaissance provenant d'un CERT
- ✓ alert.classification.reference.meaning : champ libre. Description de la base de connaissance.
  - Description RFC 4765, chapitre 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".
  - Exemple : OSSEC Rule Wiki Documentation
  - Exemple : RFC 2476
  - Exemple : Windows Event ID
  - Recommandation : Le consortium SECEF recommande d'utiliser une description simple et générique. Ce champ ne doit pas détailler la règle décrite.
- ✓ alert.classification.reference.url : champ libre. URL d'accès à la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.
  - Description RFC 4765, chapitre 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.

- Exemple : http://www.ossec.net/wiki/Rule:31101
- Exemple : http://rfc.net/rfc2476.html
- Exemple : http://www.ultimatewindowssecurity.com/events/com304.html
- Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.

✓ alert.classification.reference.name : champ libre. Nom de la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 4.2.7.1 :
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Exemple : Rule:31101
- Exemple : 5.7.1
- Exemple : %IDS-4-$1_SIG
- Recommandation : Le consortium SECEF recommande l'utilisation d'identifiants numériques

Si le virus a été reçu depuis une source identifiée, le champ suivant est à préciser :

✓ alert.source.node.address.address ou alert.source.node.name : champ libre. Adresse ou nom DNS de la machine ayant envoyé le virus.

- Description RFC 4765, chapitre 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.
- Exemple : 94.56.32.9
- Exemple : dsjghlhr.dyndns.fr

3.4 Filtrage messagerie

Un logiciel de filtrage de messagerie permet de nettoyer votre boite mail des courriels non demandés et des pièces jointes dangereuses. Il permet par exemple de ne pas recevoir de publicité non sollicitée et essaye de vous protéger contre l'hameçonnage.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de ce type. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde générant des alertes au format IDMEF : spamassassin, Exchange, Symantec.

3.4.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux logiciels de filtrage de messagerie, à minima et complémentaires.

Champs à minima	Champs complémentaires
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} : score concernant le spam détecté
	alert.additionnal_data.{type, meaning, data} : taille du spam détecté

Tableau 5 : Synthèse des champs spécifiques logiciel de filtrage de messagerie

3.4.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.target.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de préciser le type d'adresse. Pour le cas d'un anti-spam, il doit valoir « e-mail ».
  - Description RFC 4765, chapitre 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".
  - Valeur : e-mail
- ✓ alert.target.node.address.address : champ libre. Ce champ contient l'adresse courriel du destinataire.
  - Description RFC 4765, chapitre 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.
  - Exemple : jean.dupond@acme.fr
  - Recommandation : le consortium SECEF recommande, si ces informations sont disponibles de mettre l'ensemble des courriels concernés par le mail et non uniquement le destinataire.
- ✓ alert.source.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de préciser le type d'adresse. Il doit valoir « e-mail ».
  - Description RFC 4765, chapitre 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".

- Valeur : e-mail

✓ alert.source.node.address.address : champ libre. Ce champ contient l'adresse courriel de l'expéditeur.

- Description RFC 4765, chapitre 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.
- Exemple : jean.dupond@acme.fr
- Recommandation : le consortium SECEF recommande, si ces informations sont disponibles de mettre l'ensemble des courriels expéditeurs qui ont pu être concernés.

3.4.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

✓ alert.target.user.user_id.type : champ ayant une liste de valeurs finie. Ce champ précise le type d'utilisateur décrit. Il doit valoir « target-user ».

- Description RFC 4765, chapitre 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".
- Valeur : target-user

✓ alert.target.user.user_id.number : champ numérique. Ce champ contient l'UID de l'utilisateur.

- Description RFC 4765, chapitre 4.2.7.3.1 :
  Zero or one. INTEGER. A user or group number.
- Exemple : 513
- Recommandation : Le consortium SECEF recommande d'utiliser les UID les plus transverses au système, par exemple ceux de l'annuaire plutôt que les UID locaux.

✓ alert.target.user.user_id.name : champ libre. Ce champ contient le nom de l'utilisateur.

- Description RFC 4765, chapitre 4.2.7.3.1 :
  Zero or one. STRING. A user or group name.
- Exemple : jdupond
- Recommandation : le consortium SECEF recommande l'utilisation du CN de l'annuaire si possible.

✓ alert.additionnal_data.{type, meaning, data} : score concernant le spam détecté. Type doit valoir « integer », meaning doit valoir « score », data contient le score.

- Description RFC 4765, chapitre 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 : vaut « integer » dans le cas présent.
- alert.additionnal_data.meaning : vaut « score » dans le cas présent

- Exemple pour data : 5

✓ alert.additionnal_data.{type, meaning, data} : taille du spam détecté. Type doit valoir « integer », meaning doit valoir « size », data contient la taille du spam.

- Description RFC 4765, chapitre 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 : vaut « integer » dans le cas présent.
- alert.additionnal_data.meaning : vaut « size » dans le cas présent
- Exemple pour data : 145192
- Recommandation : le consortium SECEF recommande d'utiliser l'unité « octet ».
- Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sein d'IDMEF la charge utile et donc naturellement sa taille.

3.5 Proxy

Un proxy est un équipement logiciel ou matériel réalisant le rôle de passerelle. Cela lui permet de tracer les actions réalisées, appliquer des règles de contrôle et potentiellement réaliser une rupture protocolaire.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type Proxy. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde proxy générant des alertes au format IDMEF : Squid, Stormshield

3.5.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux proxy, à minima et complémentaires.

Champs à minima	Champs complémentaires
alert.target.service.web_service.url	alert.additionnal_data.{type, meaning, data} : User-Agent utilisé
alert.target.service.protocol	alert.additionnal_data.{type, meaning, data} : taille de la requête émise
alert.source.node.address.address ou alert.source.node.name	
alert.source.user.user_id.type	
alert.source.user.user_id.number	
alert.source.user.user_id.number	

Tableau 6 : Synthèse des champs spécifiques proxy

3.5.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.target.service.web_service.url : champ libre. Ce champ permet de décrire l'URL accédée.
  - Description RFC 4765, chapitre 4.2.7.5.1 :
    Exactly one. STRING. The URL in the request.
  - Exemple : https://www.ssi.gouv.fr/
  - Exemple : http://www.c-s.fr/CS-federe-les-editeurs-de-solutions-de-securite-autour-de-l-IDMEF-Partner-Program_a754.html
  - Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.
- ✓ alert.target.service.protocol : champ libre. Ce champ contient le protocole utilisé par la requête au proxy.
  - Description RFC 4765, chapitre 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.
  - Exemple : http
  - Exemple : dns
  - Recommandation : le consortium SECEF recommande de décrire le protocole de la couche applicative du modèle OSI.
- ✓ alert.source.node.address.address ou alert.source.node.name : champ libre. Ce champ contient l'adresse IP ou le nom de la machine de l'utilisateur ayant fait la demande au proxy.
  - Description RFC 4765, chapitre 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.
  - Exemple : 172.10.23.11
  - Exemple : web-server-1.acme.fr

Dans le cas où le Proxy requiert une authentification :

- ✓ alert.source.user.user_id.type : champ ayant une liste de valeurs finie. Ce champ précise le type d'utilisateur décrit. Il doit valoir « original-user ».
  - Description RFC 4765, chapitre 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".
  - Valeur : original-user

- ✓ alert.source.user.user_id.number : champ numérique. Ce champ contient l'UID de l'utilisateur.
  - Description RFC 4765, chapitre 4.2.7.3.1 :
    Zero or one. INTEGER. A user or group number.
  - Exemple : 513
  - Recommandation : Le consortium SECEF recommande d'utiliser les UID les plus transverses au système, par exemple ceux de l'annuaire plutôt que les UID locaux.
- ✓ alert.source.user.user_id.name : champ libre. Ce champ contient le nom de l'utilisateur.
  - Description RFC 4765, chapitre 4.2.7.3.1 :
    Zero or one. STRING. A user or group name.
  - Exemple : jdupond

Recommandation : le consortium SECEF recommande l'utilisation du CN de l'annuaire si possible.

3.5.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

- ✓ alert.additionnal_data.{type, meaning, data} : User-Agent utilisé. Type doit valoir « string », meaning doit valoir « user-agent », data contient le user-agent.
  - Description RFC 4765, chapitre 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 : vaut « string » dans le cas présent.
  - alert.additionnal_data.meaning : vaut « user-agent » dans le cas présent
  - Exemple pour data : Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
  - Exemple pour data : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36
  - Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sien d'IDMEF le User-Agent d'une transaction HTTP.
- ✓ alert.additionnal_data.{type, meaning, data} : taille de la requête émise. Type doit valoir « integer », meaning doit valoir « bytes_transmitted », data contient la taille de la requête émise.
  - Description RFC 4765, chapitre 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 : vaut « integer » dans le cas présent.
  - alert.additionnal_data.meaning : vaut « bytes_transmitted » dans le cas présent

- Exemple pour data : 145192
- Recommandation : le consortium SECEF recommande d'utiliser l'unité « octet ».
- Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sien d'IDMEF la charge utile et donc naturellement sa taille.

3.6 WAF

Un WAF (Web Application Firewall) est un pare-feu pour application Web. Il permet de vérifier la structure et le contenu des requêtes effectuées vers le serveur Web ainsi que de vérifier si la réponse du serveur Web est correcte. L'objectif est de protéger une application Web ayant potentiellement des failles de sécurité.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type WAF. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde WAF générant des alertes au format IDMEF : ModSecurity, DenyAll

3.6.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux proxy, à minima et complémentaires.

Champs à minima	Champs complémentaires
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 ou 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 ou alert.target.node.name	

Tableau 7 : Synthèse des champs spécifiques proxy

3.6.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.source.service.iana_protocol_name : champ libre. Ce champ indique le nom du protocole utilisé par l'attaquant.

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

✓ alert.source.service.iana_protocol_number : champ numérique. Ce champ indique le numéro IANA correspondant au protocole.

- Description RFC 4765, chapitre 4.2.7.5 :
  Optional. INTEGER. The IANA protocol number.
- Exemple : 6 (pour TCP)
- Exemple : 17 (pour UDP)

✓ alert.source.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de décrire le type d'adresse utilisé par l'attaquant. Les possibilités sont « ipv4-addr » ou « ipv6-addr ».

- Description RFC 4765, chapitre 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".
- Valeur : ipv4-addr
- Valeur : ipv6-addr

✓ alert.source.node.address.address ou alert.source.node.name : champ libre. Ce champ permet de décrire l'adresse de l'attaquant.

- Description RFC 4765, chapitre 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.
- Exemple : 153.23.53.7
- Exemple : dsjghlhr.dyndns.fr

✓ alert.target.service.iana_protocol_name : champ libre. Ce champ indique le nom du protocole utilisé par le service Web.

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

✓ alert.target.service.iana_protocol_number : champ numérique. Ce champ indique le numéro IANA correspondant au protocole.

- Description RFC 4765, chapitre 4.2.7.5 :
  Optional. INTEGER. The IANA protocol number.
- Exemple : 6 (pour TCP)
- Exemple : 17 (pour UDP)

- ✓ alert.target.service.name : champ libre. Ce champ permet de décrire le nom du service Web impacté.
  - ➢ Description RFC 4765, chapitre 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.
  - ➢ Exemple : http
  - ➢ Exemple : dns
- ✓ alert.target.service.web_service.url : champ libre. Ce champ permet de décrire l'URL que l'attaquant a tenté d'utiliser.
  - ➢ Description RFC 4765, chapitre 4.2.7.5.1 :
    Exactly one. STRING. The URL in the request.
  - ➢ Exemple : https://www.ssi.gouv.fr/
  - ➢ Exemple : http://www.c-s.fr/CS-federe-les-editeurs-de-solutions-de-securite-autour-de-l-IDMEF-Partner-Program_a754.html
  - ➢ Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.
- ✓ alert.target.node.address.address ou alert.target.node.name : champ libre. Ce champ permet de décrire l'adresse du serveur Web impacté.
  - ➢ Description RFC 4765, chapitre 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.
  - ➢ Exemple : 192.168.3.2
  - ➢ Exemple : web-server-1.acme.fr

3.6.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

- ✓ alert.classification.reference.origin : champ ayant une liste de valeurs finie. Sur quelle base de connaissance l'analyseur s'est reposé pour détecter l'évènement suspect.
  - ➢ Description RFC 4765, chapitre 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".
  - ➢ Les valeurs possibles sont les suivantes :
    - o unknown : base de connaissance non connue
    - o vendor-specific : base de connaissance fournie par l'éditeur
    - o user-specific : base de connaissance fournie par l'utilisateur
    - o bugtraqid : base de connaissance SecurityFocus

- cve : base de connaissance Mitre
- osvdb : base de connaissance osvdb
- cert-specific : base de connaissance provenant d'un CERT

✓ alert.classification.reference.meaning : champ libre. Description de la base de connaissance.

- Description RFC 4765, chapitre 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".
- Exemple : OSSEC Rule Wiki Documentation
- Exemple : RFC 2476
- Exemple : Windows Event ID
- Recommandation : Le consortium SECEF recommande d'utiliser une description simple et générique. Ce champ ne doit pas détailler la règle décrite.

✓ alert.classification.reference.url : champ libre. URL d'accès à la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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.
- Exemple : http://www.ossec.net/wiki/Rule:31101
- Exemple : http://rfc.net/rfc2476.html
- Exemple : http://www.ultimatewindowssecurity.com/events/com304.html
- Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.

✓ alert.classification.reference.name : champ libre. Nom de la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 4.2.7.1 :
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Exemple : Rule:31101
- Exemple : 5.7.1
- Exemple : %IDS-4-$1_SIG
- Recommandation : Le consortium SECEF recommande l'utilisation d'identifiants numériques

3.7 Wifi

Une sonde Wifi permet d'analyser les ondes Wifi avoisinantes afin de détecter des potentielles attaquants ou usurpateurs d'identités voire de réseaux.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type Wifi. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde Wifi générant des alertes au format IDMEF : Kismet

3.7.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux sondes Wifi, à minima et complémentaires.

Champs à minima	Champs complémentaires
alert.source.node.address.category	alert.additionnal_data.{type, meaning, data} : Nom du BSSID
alert.source.node.address.address	alert.additionnal_data.{type, meaning, data} : Canal utilisé
alert.target.node.address.category	alert.additionnal_data.{type, meaning, data} : Nom du périphérique en WPS
alert.target.node.address.address	

Tableau 8 : Synthèse des champs spécifiques sondes Wifi

3.7.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.source.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de préciser le type d'adresse. Il doit valoir « mac ».
  - Description RFC 4765, chapitre 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".
  - Valeur : mac
- ✓ alert.source.node.address.address : champ libre. Ce champ contient l'adresse MAC de l'équipement ayant reçu la trame WIFI.
  - Description RFC 4765, chapitre 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.
  - Exemple : 66:36:32:64:63:36
- ✓ alert.target.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de préciser le type d'adresse. Il doit valoir « mac ».
  - Description RFC 4765, chapitre 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".
  - Exemple : mac

- ✓ alert.target.node.address.address : champ libre. Ce champ contient l'adresse MAC de l'équipement ayant envoyé la trame WIFI.
  - Description RFC 4765, chapitre 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.
  - Exemple : 66:36:32:64:63:36

3.7.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

- ✓ alert.additionnal_data.{type, meaning, data} : Nom du BSSID. Type doit valoir « string », meaning doit valoir « BSSID », data contient le nom du BSSID.
  - Description RFC 4765, chapitre 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 : vaut « string » dans le cas présent.
  - alert.additionnal_data.meaning : vaut « BSSID » dans le cas présent
  - Exemple pour data : Wifi-CS-BatB
  - Exemple pour data : FreeWifi
  - Exemple pour data : Livebox-B345
  - Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sien d'IDMEF le BSSID d'un réseau Wifi.
- ✓ alert.additionnal_data.{type, meaning, data} : Canal utilisé. Type doit valoir « integer », meaning doit valoir « Channel », data contient le numéro du canal utilisé.
  - Exemple pour data : 11
  - Description RFC 4765, chapitre 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 : vaut « integer » dans le cas présent.
  - alert.additionnal_data.meaning : vaut « Channel » dans le cas présent
  - Exemple pour data : 10
  - Exemple pour data : 11
  - Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sien d'IDMEF le canal wifi utilisé par le réseau wifi.

- ✓ alert.additionnal_data.{type, meaning, data} : Nom du périphérique en WPS. Type doit valoir « string », meaning doit valoir « WPS Device Name », data contient le nom du périphérique connecté en WPS.
  - ➢ Description RFC 4765, chapitre 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 : vaut « string » dans le cas présent.
  - ➢ alert.additionnal_data.meaning : vaut « WPS Device Name » dans le cas présent
  - ➢ Exemple pour data : pc-42251.acme.fr
  - ➢ Note IDMEFv2 : L'évolution proposée par le consortium SECEF du format IDMEF prévoit de nouveaux champs permettant de positionner au sien d'IDMEF le nom du périphérique WPS connecté.

3.8 Switch / Routeur / Pare-feu

Un switch, routeur ou pare-feu est un équipement réseau physique ou virtuel permettant de répondre à certaines problématiques réseau particulière. Ces équipements sont partout dans nos infrastructures réseau.

Cette section décrit les champs IDMEF à remplir à minima pour les sondes de type Switch / routeur / pare-feu. Elle indique aussi des champs complémentaires qui sont un plus pour l'analyse future.

Exemple de sonde Switch / Routeur / Pare-feu générant des alertes au format IDMEF : HP, Dell, Juniper, PaloAlto.

3.8.1 Tableau récapitulatif

Le tableau ci-dessous synthétise les champs, spécifiques aux switchs / routeurs / pare-feu, à minima et complémentaires.

Champs à minima	Champs complémentaires
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 ou 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 ou alert.target.node.name	
alert.target.interface	

Tableau 9 : Synthèse des champs spécifiques switch / routeur / pare-feu

3.8.2 Champs à minima

Les champs devant être remplis sont les suivants :

- ✓ alert.source.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de préciser le type d'adresse. Il doit valoir « mac ».
  - Description RFC 4765, chapitre 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".
  - Valeur : mac
- ✓ alert.source.node.address.address : champ libre. Ce champ contient l'adresse MAC de l'équipement ayant envoyé la trame réseau.
  - Description RFC 4765, chapitre 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.
  - Exemple : 66:36:32:64:63:36
- ✓ alert.source.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de décrire le type d'adresse utilisé par l'attaquant. Les possibilités sont « ipv4-addr » ou « ipv6-addr ».
  - Description RFC 4765, chapitre 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".
  - Valeur : ipv4-addr

- Valeur : ipv6-addr

✓ alert.source.node.address.address ou alert.source.node.name : champ libre. Ce champ permet de décrire l'adresse de l'attaquant.

- Description RFC 4765, chapitre 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.
- Exemple : 153.23.53.7
- Exemple : dsjghlhr.dyndns.fr

✓ alert.source.interface : champ libre. Ce champ contient le nom de l'interface réseau par lequel le flux réseau est sorti de l'équipement.

- Description RFC 4765, chapitre 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.
- Exemple : FastEthernet0/3/0
- Exemple : eth0

✓ alert.target.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de préciser le type d'adresse. Il doit valoir « mac ».

- Description RFC 4765, chapitre 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".
- Exemple : mac

✓ alert.target.node.address.address : champ libre. Ce champ contient l'adresse MAC de l'équipement ayant reçu la trame réseau.

- Description RFC 4765, chapitre 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.
- Exemple : 66:36:32:64:63:36

✓ alert.target.node.address.category : champ ayant une liste de valeurs finie. Ce champ permet de décrire le type d'adresse utilisé par l'attaquant. Les possibilités sont « ipv4-addr » ou « ipv6-addr ».

- Description RFC 4765, chapitre 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".
- Valeur : ipv4-addr
- Valeur : ipv6-addr

✓ alert.target.node.address.address ou alert.target.node.name : champ libre. Ce champ permet de décrire l'adresse de l'attaqué.

- Description RFC 4765, chapitre 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.
- Exemple : 153.23.53.7
- Exemple : dsjghlhr.dyndns.fr

✓ alert.target.interface : champ libre. Ce champ contient le nom de l'interface réseau par lequel le flux réseau est sorti de l'équipement.

- Description RFC 4765, chapitre 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.
- Exemple : FastEthernet0/3/0
- Exemple : eth0

3.8.3 Champs complémentaires

Les champs complémentaires à remplir sont les suivants :

✓ alert.classification.reference.origin : champ ayant une liste de valeurs finie. Sur quelle base de connaissance l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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".
- Les valeurs possibles sont les suivantes :
  - unknown : base de connaissance non connue
  - vendor-specific : base de connaissance fournie par l'éditeur
  - user-specific : base de connaissance fournie par l'utilisateur
  - bugtraqid : base de connaissance SecurityFocus
  - cve : base de connaissance Mitre
  - osvdb : base de connaissance osvdb
  - cert-specific : base de connaissance provenant d'un CERT

✓ alert.classification.reference.meaning : champ libre. Description de la base de connaissance.

- Description RFC 4765, chapitre 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".
- Exemple : OSSEC Rule Wiki Documentation
- Exemple : RFC 2476
- Exemple : Windows Event ID

- Recommandation : Le consortium SECEF recommande d'utiliser une description simple et générique. Ce champ ne doit pas détailler la règle décrite.

✓ alert.classification.reference.url : champ libre. URL d'accès à la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 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.
- Exemple : http://www.ossec.net/wiki/Rule:31101
- Exemple : http://rfc.net/rfc2476.html
- Exemple : http://www.ultimatewindowssecurity.com/events/com304.html
- Recommandation : Le consortium SECEF recommande l'utilisation d'URL complète et sans redirection afin d'assurer le plus possible la pérennité de l'URL.

✓ alert.classification.reference.name : champ libre. Nom de la règle de la base de connaissance sur laquelle l'analyseur s'est reposé pour détecter l'évènement suspect.

- Description RFC 4765, chapitre 4.2.7.1 :
  Exactly one. STRING. The name of the alert, from one of the origins listed below.
- Exemple : Rule:31101
- Exemple : 5.7.1
- Exemple : %IDS-4-$1_SIG
- Recommandation : Le consortium SECEF recommande l'utilisation d'identifiants numériques

✓ alert.target.service.iana_protocol_number : champ numérique. Entier fournit par IANA pour identifier le protocole.

- Description RFC 4765, chapitre 4.2.7.5 :
  Optional. INTEGER. The IANA protocol number.
- Exemple : 6 (pour TCP)
- Exemple : 17 (pour UDP)

✓ alert.target.service.iana_protocol_name : champ libre. Texte fournit par IANA pour décrire le nom du protocole.

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

✓ alert.target.service.name : champ libre. Ce champ permet de décrire le service de l'équipement réseau impacté lorsqu'il est la cible de l'attaque.

- Description RFC 4765, chapitre 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.

- Exemple : Cisco Discovery Protocol
- Recommandation : le consortium SECEF recommande d'indiquer le nom complet du nom du service et non de son acronyme

4. Conclusion

Pour tout commentaire ou contre-avis, merci d'utiliser le forum d'échange sur SECEF :
https://redmine.secef.net/projects/secef/boards

Ce document reste une proposition, et est voué à évoluer.

Versions successives

Version	Date	Émetteur	Vérificateur	Approbateur	Motif
1.0	26/10/2016	T. Andrejak	C. Gardet C. Widmer	G. Lehmann	Création du document
1.1	03/11/2016				
1.2	15/11/2016				