PREMIÈRE MINISTRE
*Liberté*
*Égalité*
*Fraternité*

Agence nationale de la sécurité
des systèmes d'information

**Secrétariat général de la défense et de la sécurité nationale**

# Rapport de certification ANSSI-CSPN-2023/02

## Suricata

### Version 6.0.8

Paris, le 1er Mars 2023

Le Directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

# AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

| |
|---|
| Référence du rapport de certification<br>**ANSSI-CSPN-2023/02** |
| Nom du produit<br>**Suricata** |
| Référence/version du produit<br>**Version 6.0.8** |
| Catégorie de produit<br>**Détection d'intrusions** |
| Critère d'évaluation et version<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)** |
| Commanditaire<br>**Agence nationale de la sécurité des systèmes d'information**<br>51 boulevard de la Tour Maubourg<br>75700 Paris 07 SP, France |
| Développeur<br>**Open Information Security Foundation** |
| Centre d'évaluation<br>**AMOSSYS**<br>11 rue Maurice Fabre<br>35000 Rennes, France |
| Fonctions de sécurité évaluées<br>Innocuité ;<br>Autoprotection ;<br>Extraction des métadonnées ;<br>Journalisation et notification. |
| Fonctions de sécurité non évaluées<br>Sans objet |
| Restriction(s) d'usage<br>Non |

# PREFACE

## La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

## TABLE DES MATIERES

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « Suricata, Version 6.0.8 » développé par Open Information Security Foundation.

Ce produit est un système de détection d'intrusions réseau (*Network Intrusion Detection System*) *open source*, qui analyse le trafic réseau à la recherche de toute activité suspecte, en se basant sur des règles de détection. Il peut être utilisé de manière passive (dans ce cas il génère uniquement des alertes en cas de problème détecté), ou de manière active (dans ce cas il peut bloquer les flux réseau en cas de problème détecté).

Suricata est disponible pour les systèmes d'exploitation de type Unix (Linux, FreeBSD et OpenBSD).

La figure ci-dessous présente un cas typique d'utilisation de Suricata :

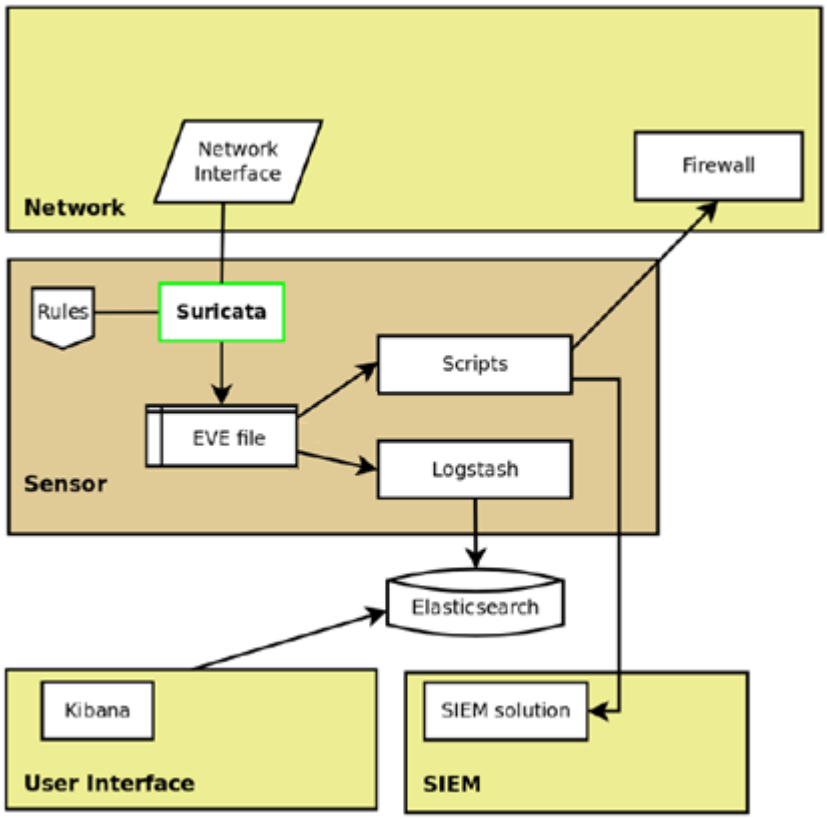



**Figure 1 – Exemple d'intégration de Suricata.**

## 1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

### 1.2.1 *Catégorie du produit*

| | | |
|---|---|---|
| ☒ | **1** | **détection d'intrusions** |
| ☐ | 2 | anti-virus, protection contre les codes malicieux |
| ☐ | 3 | pare-feu |
| ☐ | 4 | effacement de données |
| ☐ | 5 | administration et supervision de la sécurité |
| ☐ | 6 | identification, authentification et contrôle d'accès |
| ☐ | 7 | communication sécurisée |
| ☐ | 8 | messagerie sécurisée |
| ☐ | 9 | stockage sécurisé |
| ☐ | 10 | environnement d'exécution sécurisé |
| ☐ | 11 | terminal de réception numérique (*Set top box*, STB) |
| ☐ | 12 | matériel et logiciel embarqué |
| ☐ | 13 | automate programmable industriel |
| ☐ | 99 | autre |

### 1.2.2 *Identification du produit*

| Produit | |
|---|---|
| Nom du produit | Suricata |
| Numéro de la version évaluée | Version 6.0.8 |

La version certifiée du produit peut être identifiée :

- en exécutant la commande suivante :
```
# suricata -V
This is Suricata version 6.0.8 RELEASE
```

- ou encore lorsque l'aide du binaire suricata apparait :

```
amossys@debian:~/Downloads/suricata-6.0.8$ suricata
Suricata 6.0.8
USAGE: suricata [OPTIONS] [BPF FILTER]

        -c <path>                               : path to configuration file
        -T                                      : test configuration file (use with -c)
        -i <dev or ip>                          : run in pcap live mode
        -F <bpf filter file>                    : bpf filter file
        -r <path>                               : run in pcap file/offline mode
        -s <path>                               : path to signature file loaded in addi
```

### 1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

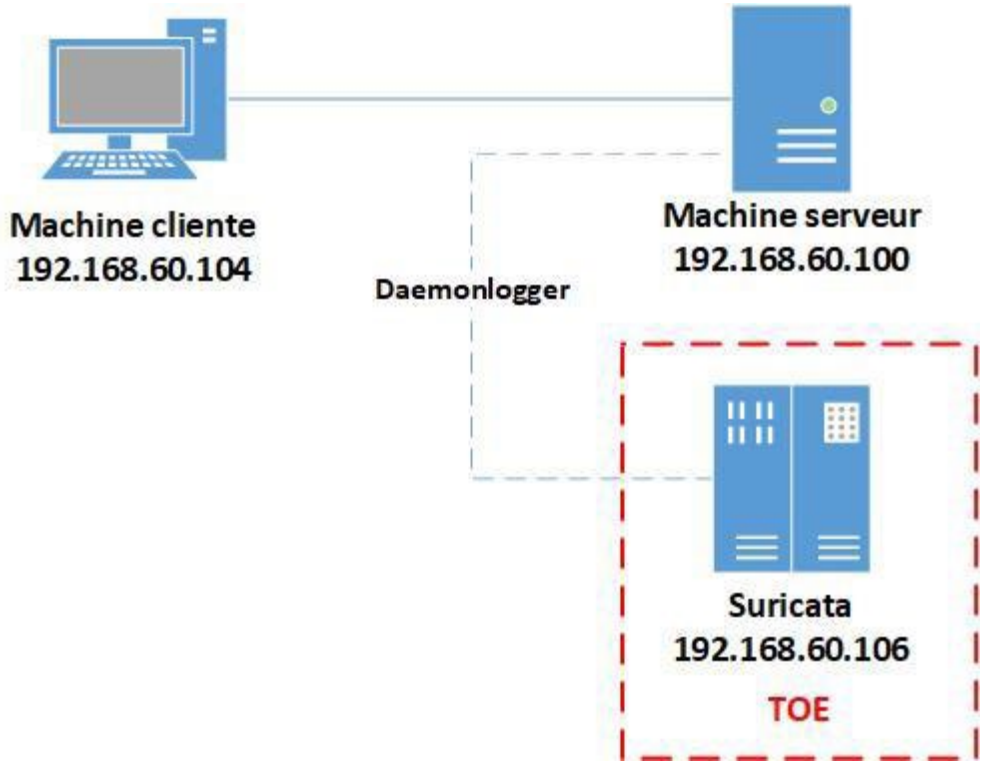
- Innocuité ;
- Autoprotection ;
- Extraction des métadonnées ;
- Journalisation et notification.

### 1.2.4 *Configuration évaluée*

La configuration évaluée correspond au produit installé manuellement sur Linux Debian à partir des sources, en suivant les règles Debian/Ubuntu, avec quelques adaptations (voir 2.2.1.2).

La plateforme de test est constituée des éléments suivants :

- une machine cliente (Kali Linux) qui émet des flux légitimes et illégitimes vers la machine serveur.
- une machine serveur (Ubuntu 20.04) qui possède un serveur web nginx écoutant sur les ports 80 et 443. Un certificat auto signé est présent dans la configuration.
- une machine Suricata (Debian 10) qui contient la cible d'évaluation (*target of evaluation* ou TOE) et qui écoute les flux en entrée de sa carte réseau.
- un service *Daemonlogger* qui simule un TAP. Il permet de recopier l'intégralité des flux émis et reçus de la machine serveur et de les envoyer à la cible d'évaluation.



# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

## 2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

### 2.2.1 *Installation du produit*

#### *2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation*

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

Pour s'assurer d'évaluer la dernière version à jour, l'évaluateur a installé la version 6.0.8 à partir des sources du produit.

L'évaluateur a d'abord installé les prérequis décrits dans la documentation de l'éditeur.

Puis l'évaluateur a suivi la documentation avancée proposée par l'éditeur pour une installation depuis la compilation de l'archive *Suricata 6.0.8*.

#### *2.2.1.2 Description de l'installation et des non-conformités éventuelles*

Certaines erreurs peuvent être rencontrées lors de l'installation :

- Lors de l'exécution de « *configure* », si les prérequis recommandés sur l'URL suivante https://suricata.readthedocs.io/en/suricata-6.0.8/install.html#ubuntu-debian ont été installés, alors une erreur, indiquant que « libjansson » est introuvable, peut apparaître.
- Si l'installation complète est réalisée avec la commande*« make install-full »,* alors une erreur *« pyyaml is required »* peut apparaître.
- La documentation recommande d'installer la version *rustc* présente dans les paquets Debian. Néanmoins, à la rédaction de ce rapport, cette version ne permet pas de compiler Suricata sans obtenir l'erreur *« could not compile `der-parser` »*. Cette erreur est connue et peut être résolue en utilisant une version *rustc* provenant du site officiel de Rust.
- Il est possible de définir manuellement un service Suricata. Pour cela, le dossier d'installation du produit propose un fichier *« Suricata service »*. Néanmoins, ce fichier contient des erreurs de configuration, qui peuvent être corrigées manuellement avant de créer un nouveau service Suricata.
- Le fichier /etc/suricata/suricata.yaml déposé lors d'une installation *« full »* contient des erreurs, qui peuvent être corrigées manuellement.

Cependant, ces erreurs rencontrées sont toujours explicites et faciles à corriger par un administrateur compétent.

De plus, ces éventuelles erreurs ne remettent pas en cause la sécurité du produit.

#### *2.2.1.3 Notes et remarques diverses*

Sans objet.

### 2.2.2 *Analyse de la documentation*

Suricata est un produit *OpenSource*, son code et sa documentation sont disponibles en ligne sur le dépôt *Github* associé et le site officiel du développeur, voir [GUIDES].

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

La documentation d'installation et de configuration est complète et l'évaluateur n'a pas rencontré de problème en l'utilisant. De plus, elle contient des sections dédiées à la résolution des différentes erreurs pouvant survenir lors des phases d'utilisation et de configuration.

### 2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

L'évaluateur estime que le code source est de bonne qualité.

### 2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

### 2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

### 2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

#### *2.2.6.1 Liste des vulnérabilités connues*

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

#### *2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert*

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

### 2.2.7 *Analyse de la facilité d'emploi*

#### *2.2.7.1 Cas où la sécurité est remise en cause*

L'évaluateur n'a pas identifié de cas où la sécurité de la cible d'évaluation est remise en cause.

#### *2.2.7.2 Avis d'expert sur la facilité d'emploi*

Le produit est relativement simple à installer à partir des sources à compiler.

Bien que des erreurs puissent survenir lors de l'installation, la levée de ces erreurs est intuitive ce qui facilite la résolution de problème.

#### *2.2.7.3 Notes et remarques diverses*

Aucune note, ni remarque n'a été formulée dans le [RTE].

## 2.3 Analyse de la résistance des mécanismes cryptographiques

Le produit ne comporte pas de mécanismes cryptographiques.

## 2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'évaluation.

# 3 La certification

## 3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Suricata, Version 6.0.8 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

## 3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | Cible de sécurité de référence pour l'évaluation :<br>- Cible de sécurité CSPN – Produit Suricata version 6.0.8, référence CSPN-ST-Suricata-1.02, version 1.02, 29 septembre 2022. |
| [RTE] | Rapport technique d'évaluation :<br>- Rapport Technique d'Evaluation CSPN – Produit Suricata version 6.0.8, référence CSPN-RTE-SURICATA2-2.02, version 2.02, 9 janvier 2023. |
| [GUIDES] | Guides d'utilisation, d'administration et d'installation du produit :<br>- Documentation :<br>o https://github.com/OISF/suricata<br>o https://suricata.readthedocs.io/en/suricata-6.0.8/<br>- *Release notes* :<br>https://redmine.openinfosecfoundation.org/projects/suricata |

# ANNEXE B. Références liées à la certification

| | |
|---|---|
| Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. | |
| [CSPN] | Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 4.0, 3 mars 2022.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018. |