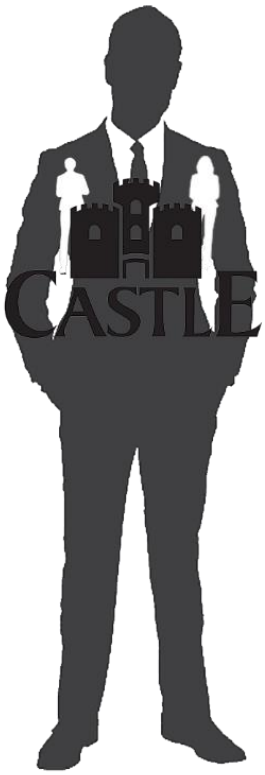
CASTLE

Rapport de benchmarking



En partenariat avec l'ensibs

Rapport de benchmarking des solutions de sécurité *Blue team*

Synthèse des notations et pondérations

Critère	Suricata		Snort	
	Note	**Poids**	**Note**	**Poids**
Détection	4	5	1	5
Capacité d'analyse	3	5	2	5
Complexité d'analyse	2	4	3	4
Export des résultats	1	4	4	4
Création de règles	2	3	3	3
Export de fichier suspect	3	2	2	2
Prévention	4	1	1	1
Note finale	**63**		**57**	

Appréciation

D'après les résutats ci-dessus, la solution de sécurité défensive dont vous avez besoin est :

Suricata

Rapport de benchmarking des solutions de sécurité *Blue team*

Résultats détaillés de l'évaluation de suricata

Critère : Détection	**Description du critère de notation :**
	Fonction principale d'un IDS, capacité à détecter des anomalies

Note attribuée pour ce critère : 4 / 5

L'outil à detecté entre 70 et 80% des attaques.

Critère : Capacité d'analyse	**Description du critère de notation :**
	Capacité de l'IDS à bien surveiller les flux réseau entrants et sortants

Note attribuée pour ce critère : 3 / 5

L'outil analyse dix à vingt Go par seconde.

Critère : Complexité d'analyse	**Description du critère de notation :**
	Capacité de l'IDS à connaître et comprendre les protocoles réseaux

Note attribuée pour ce critère : 2 / 5

L'outil à la capacité à analyser la couche réseau applicative.

Critère : Export des résultats	**Description du critère de notation :**
	Clarté et pertinence des résultats de l'IDS une fois exportés

Note attribuée pour ce critère : 1 / 5

L'outil permet un export partiel des résultats.

Critère : Création de règles	**Description du critère de notation :**
	Configuration rapide et précise des règles de détection au cœur de l'IDS

Note attribuée pour ce critère : 2 / 5

L'outil permet la création de règles au format standard.

Critère : Export de fichier suspect	**Description du critère de notation :**
	Possibilité d'exporter un fichier suspect pour analyse ultérieure

Note attribuée pour ce critère : 3 / 5

L'outil permet l'extraction manuelle via l'interface graphique.

Critère : Prévention	Description du critère de notation :
	Rôle plutôt associé aux IPS, capacité de l'IDS à prévenir une menace

Note attribuée pour ce critère : 4 / 5

L'outil propose un blocage suffisant de l'attaque, drop du trafic malicieux, blocage de la connexion.

Rapport de benchmarking des solutions de sécurité *Blue team*

Résultats détaillés de l'évaluation de snort

Critère : Détection	Description du critère de notation :
	Fonction principale d'un IDS, capacité à détecter des anomalies

Note attribuée pour ce critère : 4 / 5

L'outil à detecté entre 70 et 80% des attaques.

Critère : Capacité d'analyse	Description du critère de notation :
	Capacité de l'IDS à bien surveiller les flux réseau entrants et sortants

Note attribuée pour ce critère : 3 / 5

L'outil analyse dix à vingt Go par seconde.

Critère : Complexité d'analyse	Description du critère de notation :
	Capacité de l'IDS à connaître et comprendre les protocoles réseaux

Note attribuée pour ce critère : 2 / 5

L'outil à la capacité à analyser la couche réseau applicative.

Critère : Export des résultats	Description du critère de notation :
	Clarté et pertinence des résultats de l'IDS une fois exportés

Note attribuée pour ce critère : 1 / 5

L'outil permet un export partiel des résultats.

Critère : Création de règles	Description du critère de notation :
	Configuration rapide et précise des règles de détection au cœur de l'IDS

Note attribuée pour ce critère : 2 / 5

L'outil permet la création de règles au format standard.

Critère : Export de fichier suspect	Description du critère de notation :
	Possibilité d'exporter un fichier suspect pour analyse ultérieure

Note attribuée pour ce critère : 3 / 5

L'outil permet l'extraction manuelle via l'interface graphique.

Critère : Prévention	Description du critère de notation :
	Rôle plutôt associé aux IPS, capacité de l'IDS à prévenir une menace

Note attribuée pour ce critère : 4 / 5

L'outil propose un blocage suffisant de l'attaque, drop du trafic malicieux, blocage de la connexion.