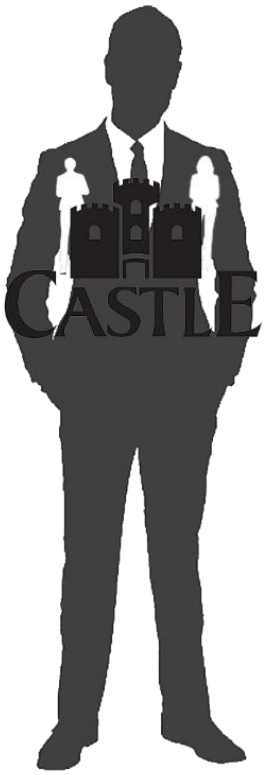
CASTLE

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