Evaluation of Shadowserver Data Source

Criteria	Metrics and Values	Result and Value
		Shadowserver Data Feed
Confidentiality	Not applicable (NA) to end users of this service (national CSIRTs) because they don't have concerns about the confidentiality of the data feeds (which are public)	NA
Accuracy	Applicable as users care that the data has accurate information about an incident such as an indicator of compromise (IOC). Metric: If the data accurately indicates or tells about an incident Value: 'Presence of malware URL', 'Presence of phishing URL', 'Hash value of malware'	'Presence of malware URL', 'Presence of phishing URL', 'Hash value of malware'
Precision	Applicable as users care that the data is precise enough for taking further action, such as takedowns. Metric: If data has specific details about an incident Value: 'Has complete URL', 'Has source IP address with date and timestamp' (to detect hosts using DHCP IP address), 'Has a hash value of malware', 'Has Internet protocol type', 'Has a port number', 'Has IP geo-location'	'Has complete URL', 'Has source IP address with date and time stamp', 'Has a hash value of malware', 'Has Internet protocol type', 'Has a port number', 'Has IP geolocation'
Understandability	Applicable to ensure the data is in a format that makes data easily understood and facilitate analysis. Metric: The format that can be understood by human users to facilitate analysis Value: 'Can be exported as a CSV file', 'Displayed structured in a table'	'Can be exported as a CSV file', 'Displayed structured in a table'
Currentness	Applicable as users are concerned that the data is current and not outdated. Metric: Shows the current date and timestamp of the data Value: 'Shows current date'	'Shows current date - 12/02/2023 1:28:00 AM' which is the date of evaluation
Completeness	Applicable as users care about the sufficiency of data for further incident response action. Metric: Data is sufficient for a further incident response such as escalation to Service Provider Value: 'Has a complete URL', 'Has IP address, 'Has date', 'Has timestamp', 'Has ASN number', 'Name of malware', 'Has malware hash value'	'Has a complete URL', 'Has IP address', 'Has date', 'Has timestamp', 'Has ASN number', 'Name of malware', 'Has malware hash value'

Credibility	Applicable as users care the data is credible to support incident response. Metric: Source of data is from a known reliable data provider. Value: 'Yes/No' Metric: The data has information it intends to provide. Value: 'Yes/No'	 'Yes' 'Yes'
Efficiency	Applicable as users care that the data is efficient in terms of less time consuming to identify indicators to initiate incident response. Metric: Time taken to identify an indicator of compromise from the data. Value: 'Number - second/minute/hour'	 '6 seconds'