

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	<p>Applicable as users care that the data has accurate information about an incident such as an indicator of compromise (IOC).</p> <p>Metric: If the data accurately indicates or tells about an incident Value: 'Presence of malware URL', 'Presence of phishing URL', 'Hash value of malware'</p>	'Presence of malware URL', 'Presence of phishing URL', 'Hash value of malware'
Precision	<p>Applicable as users care that the data is precise enough for taking further action, such as takedowns.</p> <p>Metric: One metric identified is multi-valued and categorical - 'what specific details the data has about an incident'. Value: 'complete URL', 'source IP address', 'destination IP address', 'timestamp', 'hash value(s) of related software/malware', 'network protocol type', 'port number(s)', 'geo-location(s)'.</p>	'Complete URL', 'source IP address', 'destination IP address', 'timestamp', 'hash value(s) of related software/malware', 'network protocol type', 'port number(s)', 'geo-location(s)'
Understandability	<p>Applicable to ensure the data is in a format that makes data easily understood and facilitate analysis.</p> <p>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'</p>	'Can be exported as a CSV file', 'Displayed structured in a table'
Currentness	<p>Applicable as users are concerned that the data is current and not outdated.</p> <p>Metric: Shows the current date and timestamp of the data Value: 'Shows current date'</p>	'Shows current date - 12/02/2023 1:28:00 AM' which is the date of evaluation
Completeness	<p>Applicable as users care about the sufficiency of data for further incident response action.</p> <p>Metric: Data is sufficient for a further incident response such as escalation to Service Provider</p>	'Has a complete URL', 'Has IP address', 'Has date', 'Has timestamp', 'Has ASN number', 'Name of malware', 'Has malware hash value'

	Value: 'Has a complete URL', 'Has IP address', 'Has date', 'Has timestamp', 'Has ASN number', 'Name of malware', 'Has malware hash value'	
Credibility	<p>Applicable as users care the data is credible to support incident response.</p> <p>Metric: Source of data is from a known reliable data provider. Value: 'Yes/No'</p> <p>Metric: The data has information it intends to provide. Value: 'Yes/No'</p>	<p>'Yes'</p> <p>'Yes'</p>
Efficiency	<p>Applicable as users care that the data is efficient in terms of less time consuming to identify indicators to initiate incident response.</p> <p>Metric: Time taken to identify an indicator of compromise from the data. Value: 'Number - second/minute/hour'</p>	<p>'6 seconds'</p>

