Evaluation of VirusTotal and Hybrid Analysis Tools – Product Quality

Criteria	**Metrics**	**Result and Value**	
Security		**VirusTotal**	**Hybrid Analysis**
Confidentiality	Not Applicable (NA) because end users of this service (national CSIRTs) are not concerned about the confidentiality of the data to authorised users only.	NA	NA
Integrity	Applicable because end users care about data integrity (such as data is not sniffed, modified or manipulated by a third party). Metric 1: If the data transmission is encrypted end to end using HTTPS (Binary: Yes and No) Metric 2: If the online service is hacked by a malicious party who can manipulate the data before it is sent to the end users (Binary: Yes and No)	Yes No	Yes No
Authenticity	Applicable because end users care about the authenticity of the server. Metric 1: If the HTTPS protocol is used to provide service authentication (Binary: Yes and No) Metric 2: To what extent can end users be sure about the real identity of the service provider or the developer if there is no service provider (e.g., a company's registration record, paid membership official contract documents, natural person's real-world identity), whose value can be one of the following: • the real identity can be fully obtained • the real identity can be partially obtained (e.g., just an online account, but not real-world identity) • the real identity cannot be obtained	Yes. HTTPS is used 'The real identity can be fully obtained' from a DomainTools whois search, with the below result: IP: 74.125.34.46 IP Location: California – Mountain View – Google ASN: AS15169, Google, US (registered Mar 30, 2000) Company information provided on its website as: Virus Total, USA	Yes. HTTPS is used 'The real identity can be fully obtained' from a DomainTools whois search, with the below result: IP: 104.18.34.183 IP Location: California – San Jose – CloudFlare Inc. ASN: AS13335, Cloudflare-net, US (registered Jul 14, 2010) Company information provided on its website as: Hybrid Analysis, Germany
Usability			

Learnability	Applicable because end users care about how easily they can learn about the features of the service. Metric: The amount of time a typical end user (such as a member of technical staff at a national CSIRT) takes to learn the task of submitting a file to the tool in order to get the result or output after submitting the file. Measurement method: this metric can be measured by asking several typical end users about the time taken to learn the task of submitting an URL to the tool in order to get the result or output after submitting the URL. of the tool.	'5 minutes' (judged based on the researcher's testing of learning the task of submitting a file because trying the UI is straightforward for any technical person)	'8 minutes' (judged based on the researcher's testing of learning the task of submitting a file because trying the UI is straightforward for any technical person)
Operability	Applicable because end users want to use a system with easy control -- User Interface (UI) Metric 1: If the service has a GUI that can be used by a junior-technical person (Binary: Yes and No) Metric 2: If the service has an online interface that can be used by anyone with Internet access (Binary: Yes and No) Metric 3: If the service has an API so that a member of the technical staff at a national CSIRT can automate the use of the service (Binary: Yes and No)	Yes Yes Yes	Yes Yes Yes
User Interface Aesthetics	Applicable as technical staff of national CSIRTs are concerned about the simplicity of the menu to make the task less complicated. Metric: How the result is presented Value: 'In a table', 'Colour codes legend', 'Buttons for detail result'	Result is presented in 'structured table' form on the page. Has 'colour code', e.g. Red – indicates the file submitted is detected as malware, Green – indicates not malware. Colour code of Confidence Level of the result: Red – indicates low confidence level,	Result is 'not presented in table form'. Has 'colour code', e.g. Red – indicates the file submitted is detected as malware, Green – indicates Clean. Has a 'button to display details' of the result

		Green – indicates high confidence level. Has a 'button to display details' of the result	
Accessibility	Applicable as technical staff of national CSIRTs is concerned if they can have access to the tool for investigation purposes. Metric: If access to the tool is enabled for users with cognitive or physical impairments Value: 'Font size', 'Sound control', 'Colour palettes', 'Brightness of the web page can be adjusted', 'Font size of the web page can be enlarged'	'Has option for night and day screen viewing', 'Font size of the web page can be enlarged'	'Font size of the web page can be enlarged'
Maintainability			
Maintainability	Applicable since the service can be updated and the provider can make the updates visible to users. Metric: If the tool shows the current year of the tool, visible to users Value: 'Current year 2003 is shown', 'Current year 20023 is not shown'	'Current year 2023 is not shown' on the web page	'Current year is shown' as: ©2023 Hybrid Analysis
Supportability	Applicable as users are concerned that they can get support and help when any issues arise while using the tool. Metric: What type of support is provided by the tool Value: '24x7 Live Support', 'Online Support', 'Chat Bot'	'24x7 Live Support', 'Online Support', 'Chat Bot'	'Online Support'
Analysability	This is applicable as users should be able to know causes of failures that might occur while using the tool. Metric: If causes of failures can be identified (Binary: Yes and No)	Yes	Yes
Modifiability	Not applicable to free tools		
Compatibility			
Interoperability	Applicable as users is concerned that the tool can be integrated with other third-party applications.		

	Metric: If the tool allows integration and information exchange with third-party applications Value: ‘Has an API for integration with third-party applications’, ‘Has an export feature that allows data exchange’	‘Has API integration’ with 14 third party applications	‘Has API integration’ with 1 third party applications
Functionality			
Functionality	Applicable as users are concerned that the tool functions cover all the specified tasks in the tool and meet the user's objective. Metric: if the tool has a file scanning feature and performs the specified functionality (feature) accordingly (Binary: Yes and No)	Yes. The tools is able to scan a file and diagnose a malicious file as malicious In contrast, when input a clean file, the file is detected as clean	Yes. The tools is able to scan a file and diagnose a malicious file as malicious In contrast, when input a clean file, the file is detected as clean
Performance Efficiency			
Time behaviour	Applicable because end users care how fast they can get the results. Metric: The amount of time taken to obtain the result when input a file or URL (from the start to the return of the results)	‘2 seconds’ (according to researcher’s testing)	‘9 seconds’ (according to researcher’s testing)
Capacity	Applicable because end users care about the size of the file that can be uploaded to the website to perform the analysis. Metric: ‘maximum file size that can be uploaded for analysis’ Measurement method: from the official documents and testing it yourself	650 MB can be uploaded to the website	100 MB to the website
Money	Not applicable (NA) because this is a free service.	NA	NA
Human Effort	Not applicable (NA) because this is an automated online tool.	NA	NA
Material	Applicable as users want to know how many inputs or materials need	‘1 file input’ is sufficient to generate the result’	‘1 file input’ is sufficient to generate the result’

	to be provided to get the desired result. Value: ‘1 file input’, ‘More than 1 file input’		
Reliability			
Reliability	Applicable as users are concerned that the tool provides accurate result. Metric: The tool returns accurate result for the input given. (Binary: Yes and No)	Yes.	Yes.
Availability	Applicable as users are concerned the service is available to perform the tasks whenever required. Metric: If the tool can run if any third-party libraries or data sources it relies upon are down. (Binary: Yes and No) Metric: If the tool can run offline even if its web server is down Value: Not able to evaluate this as there was no circumstances of the web server was down during the evaluation exercise. By description of the tool, the value should be ‘No’, as the tool is an online service (not offline) Metric: The availability of the tool to perform its intended function without failure during the evaluation period. Value: ‘99.999% uptime’	Yes. The tool can run and gives the required result No ‘99.999% uptime’ during the evaluation period	Yes. The tool can run and gives the required result No ‘99.999% uptime’ during the evaluation period
Compliance	Applicable as the tool needs to comply with any standards or industry practices. Metric: If the tool complies with one or more specific industry standards or practices. Value: ‘Name of Standard’, ‘Not found’	‘Not found’	‘Not found’
Certification	Applicable, as a certified or accredited tool is always a good sign of its quality.	‘Not found’	‘Not found’

	Metric: If it is certified and publicised, what certifying body and Standard. Value: ‘Name of Certification’, ‘Not found’		

Evaluation of VirusTotal and Hybrid Analysis Tools – Quality in Use

Criteria	**Metrics**	**Result and Values**	
Context Coverage		VirusTotal	Hybrid Analysis
Flexibility	Applicable as users are concerned about the tool’s flexibility to specific users (e.g. non-expert users) to achieve intended goals. Metrics: If users perceive the software is flexible for non-expert users. (Binary: Yes and No) These perceptions can be obtained from ``External reports" and ``Estimations with Co-workers from a national CSIRT". If the above external reports or estimation with co-workers could not be obtained, the value is ``Not found". However, if a national CSIRT wants to evaluate a tool based on this criterion, it is best to survey and gather opinions and insights on the software's flexibility to get the value.	Yes	No
Usability			
Satisfaction			
User Experience	Applicable as users are concerned that they perceive and are satisfied with the usefulness of the result. Metric: If users perceive the result from the tool as useful. (Binary: Yes and No) Measurement: Based on how users perceive the usefulness. These perceptions can be obtained from ``External reports" and ``Estimations with Co-workers from a national CSIRT". If the above external reports or estimation with co-workers could not be obtained, the	Yes	Yes

	value is ``Not found". However, if a national CSIRT wants to evaluate a tool based on this criterion, it is best to survey to get the value.		
Usefulness	Applicable as users are concerned that they perceive and are satisfied with the usefulness of the result. Metric: If users perceive the result from the tool as useful. (Binary: Yes and No) Measurement: Based on how users perceive the usefulness. These perceptions can be obtained from ``External reports" and ``Estimations with Co-workers from a national CSIRT". If the above external reports or estimation with co-workers could not be obtained, the value is ``Not found". However, if a national CSIRT wants to evaluate a tool based on this criterion, it is best to survey to get the value.	Yes	Yes
Trust	Applicable as users care if they have confidence in the tool that it functions as it is supposed to be. Metric: if users have confidence that the tool will function as it should. (Binary: Yes and No) Measurement: Based on users' trust and confidence. This trust and confidence level can be obtained from ``External reports" and ``Estimations with Co-workers from a national CSIRT". If the above external reports or estimation with co-workers could not be obtained, then the value is ``Not found". However, if a national CSIRT wants to evaluate a tool based on this criterion, it is best to survey to get the value.	Yes	Yes
Comfort	Not applicable (NA) for online services.	NA	NA
Effectiveness			
Effectiveness	Applicable as users care if the tool meets the specified requirements and performs the functions. Metric: if the tool fulfils the specified requirements and performs the specified functions correctly. (Binary: Yes and No)	Yes	Yes
Freedom from Risk			

Sustainability	Applicable as users want to make sure the tool is sustained without depletion (with the very basic feature) by the Publisher. Metric: how the sustainability of the tool is guaranteed.	Maintained by a large, well-known organisation	Dependent on single company's existence and business-driven decision
Harm from use	Applicable as users want to make sure no negative consequences regarding health, safety, finances or the environment that result from the use of the system. Metric: if the tool posed health hazards to the user. (Binary: Yes and No)	No	No
Popularity	Applicable as users care if the tool is used by others, such as national CSIRTs or other security organisations. Metrics: How many security organisations or national CSIRTs use the tool. Value: ‘Large’, ‘Medium’, ‘Low’ This information can be obtained from ‘External reports’ and ‘Informal discussions with the security community’. If the above external reports or discussions could not be obtained, the value is ‘Not known’. However, if a national CSIRT wants to evaluate a tool based on this criterion, it is best to survey to get the value.	Used by ‘large’ number of national CSIRTs (based on the researcher’s informal discussion with national CSIRTs)	Used by ‘medium’ number of national CSIRTs (based on the researcher’s informal discussion with national CSIRTs)