Incident Response Metrics

https://campus.barracuda.com/doc/77402149/

This page describes the main metrics you can use in the Incident Response results.

You can use these metrics:

- to add to custom column layouts, as described in Working with Results Tables.
- to make custom reports in the Summary Fields, as described in How to Create Custom Reports.
- in the Filter in the left panel to locate specific records within Outbound Analysis results, as described in Working with Results Tables.

Metric Name	Format	Description
Antivirus Description	free text	Explanation of antivirus score.
Antivirus Score	free text	Antivirus score for this email.
Campaign Message #	list of available values	If the message refers to a campaign email, the Message Number from the campaign.
Campaign Message ID	list of available values	If the message refers to a campaign email, the Message ID from the campaign.
Disposition	list of available values	The disposition for this incident response message.
From	free text	The From field for the email message.
Incident Response Mailbox	list of available values	The incident response mailbox that received the message.
Message Body Summary	free text	The body of the email in plain text.
Message ID	free text	The Message ID header value for the inbox.
Notes	list of available values	Notes that were entered manually.
Original Date Time	calendar value	The date and time this email was reported by the original reporter, specified as a range from *at least* to *at most*.
Original From	free text	Original Name and Email on the mock phishing attempt.
Original From Domain	free text	Original From address domain on the mock phishing attempt.
Original From Email	free text	Original From email address on the mock phishing attempt message.

Original Reporter	free text	Name and Email of the person who originally reported the phishing attempt.
Original Reporter Domain	free text	Domain of the original reporter's email address.
Original Reporter Email	free text	Stripped email address of the original reporter.
Original Reporter Name	free text	Name of the original reporter.
Original Subject	free text	Subject of the original phishing attempt message.
Parent Email	free text	Email that contained this email as an attachment.
Report Day of Week	list of available values	Day of the week when emails were reported.
Report Hour of Day	list of available values	Hour of the day when emails were reported.
Report Month	list of available values	Month in which emails were reported.
Report Quarter	list of available values	Quarter of the year in which emails were reported.
Report Year	list of available values	Year in which emails were reported.
Report Year Month	list of available values	Year/Month combination in which emails were reported.
Report Year Quarter	list of available values	Year/Quarter combination in which emails were reported.
Report Year Week	list of available values	Year/Week combination in which emails were reported.
Reported Time	calendar date	Time the phishing attempt was reported to the Incident Response Dashboard, specified as a range from *at least* to *at most* .
Risk Score	free text	Risk Score of the email, specified as a range from *at least* to *at most* .
Size	free text	The overall size of the mail message in bytes, specified as a range from *at least* to *at most* .
Spam Description	free text	Detailed explanation of spam score.
Spam Score	free text	Spam Score of the email, specified as a range from at least to at most.
Subject	free text	Subject of the email message.
Time	calendar date	The timestamp when the email was originally received, specified as a range from *at least* to *at most* .
Time Priority	list of available values	The priority of the message based on its age.
To	free text	From field for the email message.

Wrap Level	free text	Number of levels deep this message was wrapped in the message sent to the Incident Response Dashboard, specified as a range from *at least* to *at most* .