GoSecure IDR – Quarantine Admin Experience

CUSTOMER GUIDE

CONTENTS

Version 3.0

April 22nd , 2022

OVERVIEW

TPx Managed Inbox and Detection and Response (IDR), powered by GoSecure, is an advanced anti-phishing solution, used to submit any suspicious email to the GoSecure Threat Detection Center for expert analysis. Reporting suspicious emails strengthens your organizations security posture and helps prevent phishing attacks.

As an IT/Security administrator for your company, you have access to the managed IDR portal to view all reported messages and their status. You can also manually change status and view online reports of overall usage.

This guide covers the quarantine Administrator experience and what to expect while using TPx Managed IDR.

SUPPORTED APPLICATIONS

TPx IDR integrates with Microsoft Office 365 and is currently supported in the following versions of Microsoft Outlook:

- Microsoft Outlook Desktop Client
  - Outlook 2016 or newer
- Microsoft Outlook Web Access (OWA) Client
- Microsoft Outlook for iOS
- Microsoft Outlook for Android

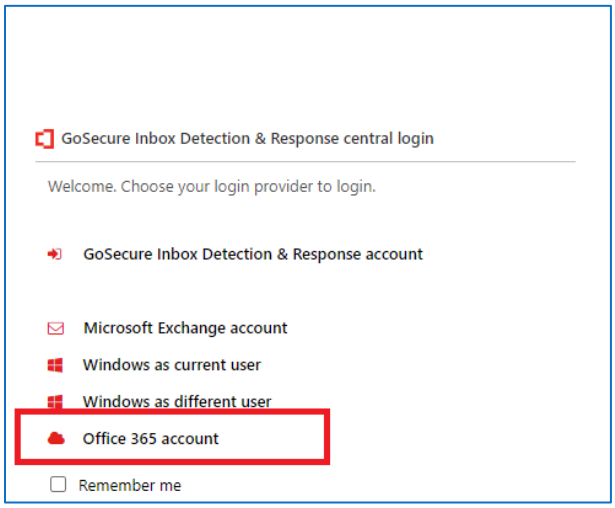
QUARANTINE ADMIN ROLE

The Quarantine Administrator has access to the GoSecure IDR Admin Center, which includes visibility on the Statistics page and the ability to view and manage messages submitted for Analysis in the Quarantine section.

HOW TO ACCESS THE GOSECURE ADMIN CENTER

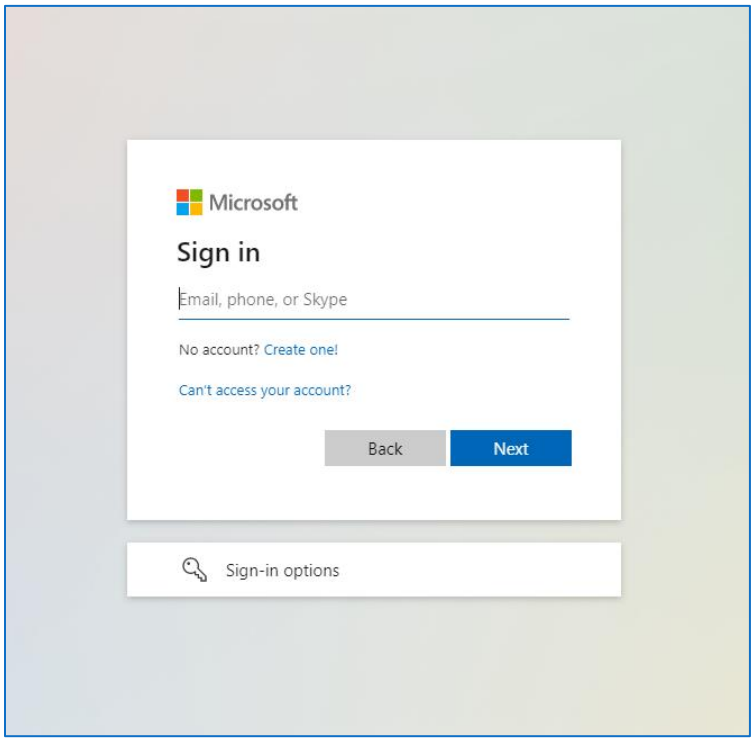
The GoSecure Admin Center is accessed navigating to: https://portal.idr.gosecure.net)

1. On the login page, there are four login options:

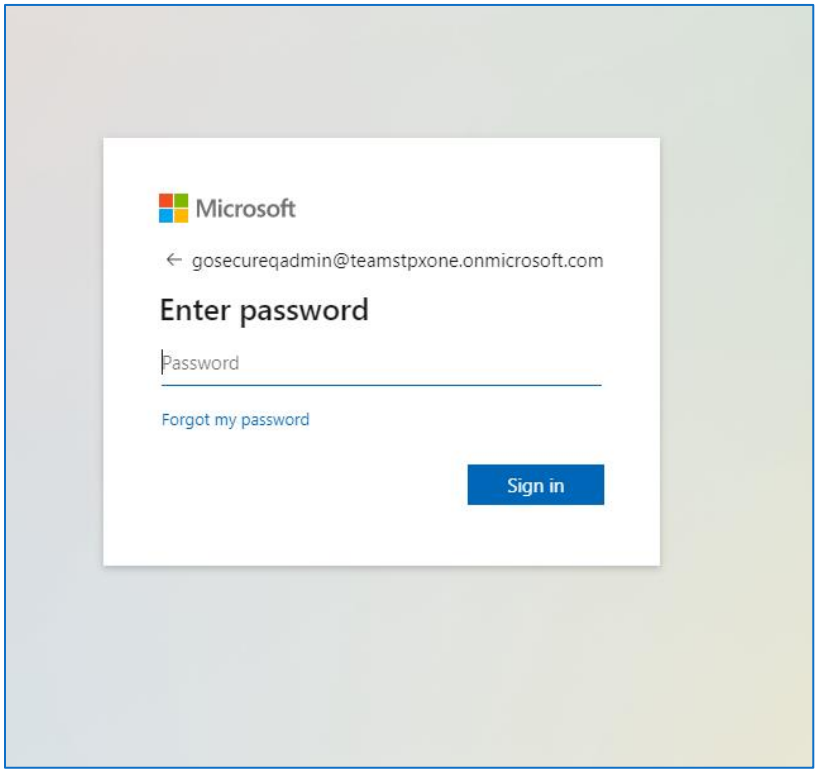


	NOTE: Select Office 365 Account to access the Admin Center to go to the Microsoft sign-in screen.

2. Enter your email address, then click Next.



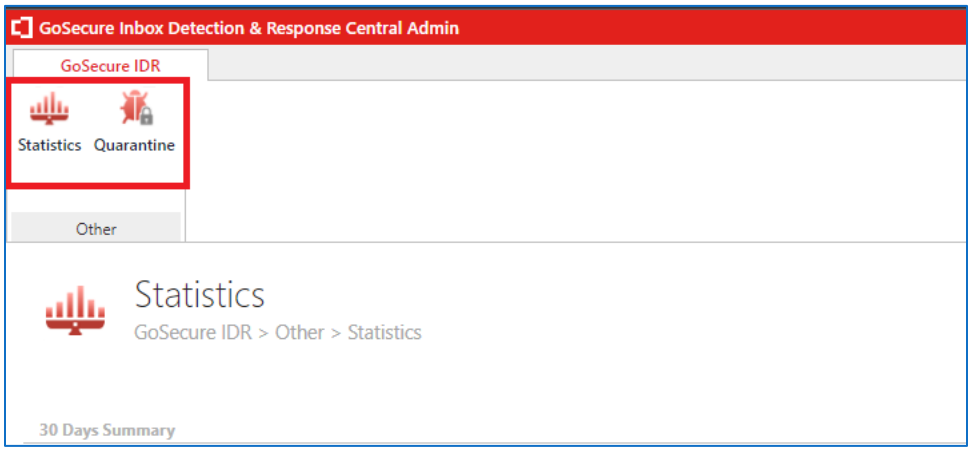
3. Enter your password, then click **Sign in**.



4. Once logged in, the Statistics Overview page displays.

	NOTE: For any subsequent logins after your first login, the portal defaults to the last page visited in the prior of the admin center.

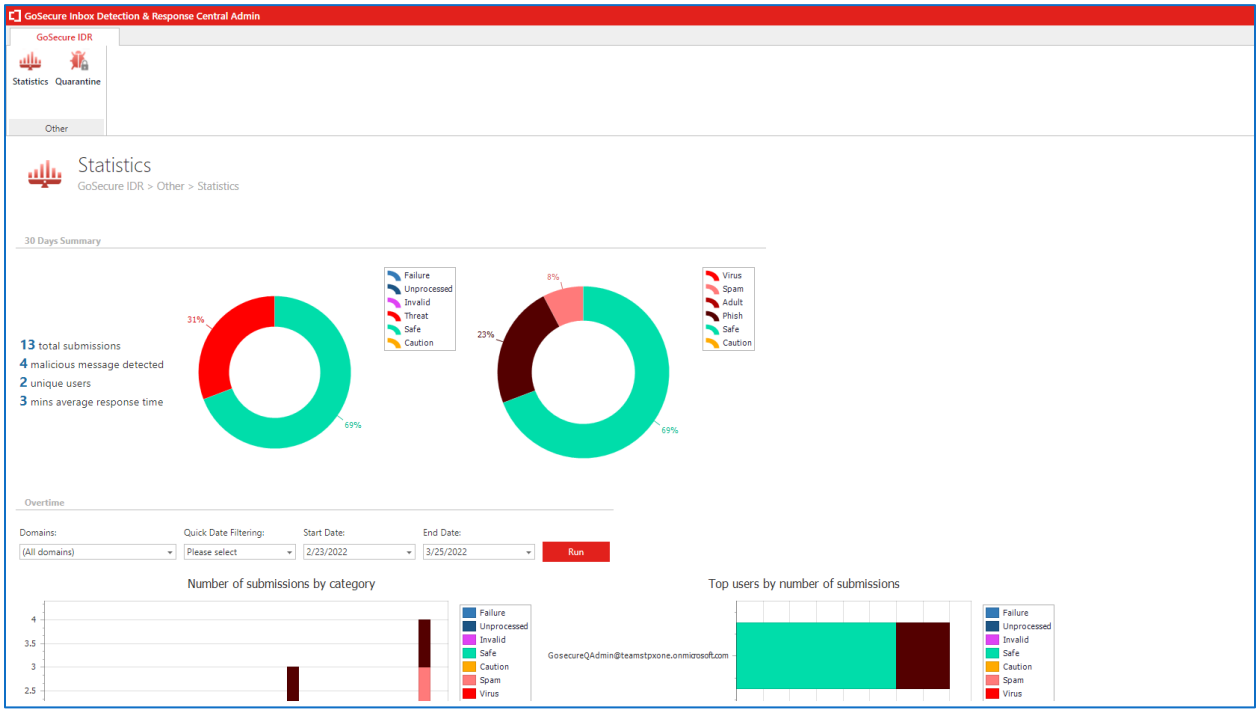
5. You can change between the **Statistics** and **Quarantine** pages, from the navigation pane on the top of the screen.



STATISTICS OVERVIEW

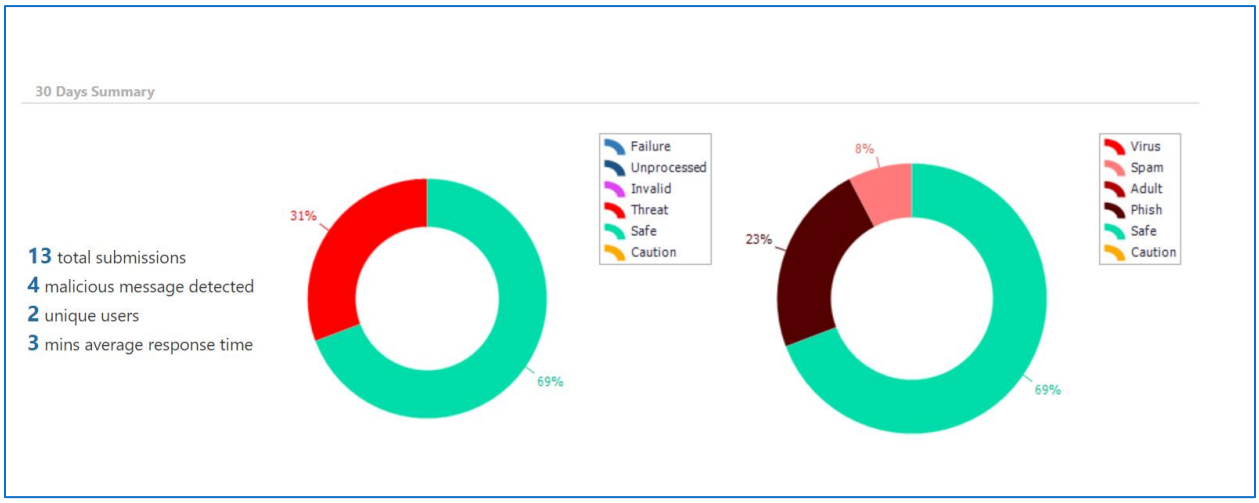
The Statistics Overview page summarizes your organization's submitted messages, broken down in various charts, graphs and tables – the 3 main categories are:

- 30-Days Summary
- Overtime
- Recently Reported Emails



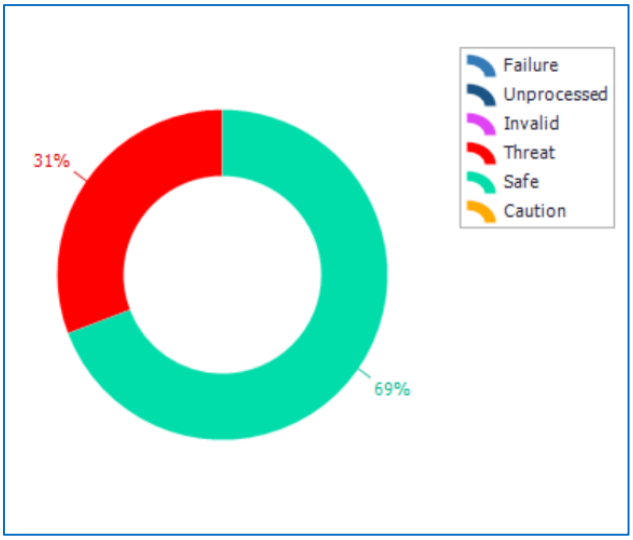
30 DAYS SUMMARY

The top section, **30 Days Summary** includes two donut graphs with a breakdown of the total number of submissions over the last 30 days.

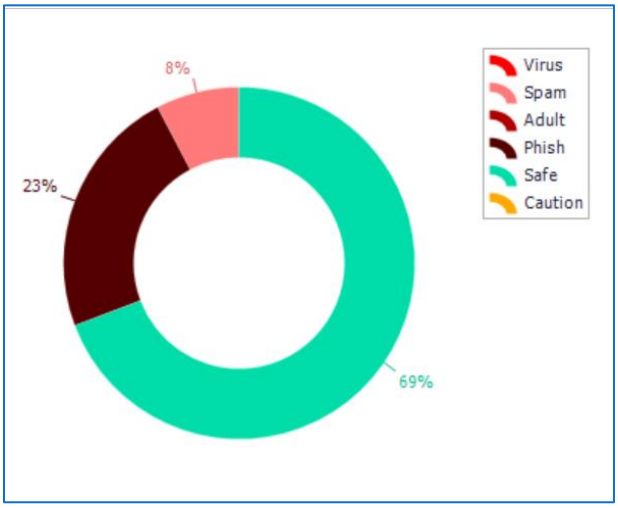


1. There is a quick summary of the total amount of message submissions over the last 30 days, number of malicious messages detected, number of unique users submitting messages, and the average response time for receiving an **Alert Status** classification for the message. (For additional detail around the different classifications, refer to Appendix A: Classification Definitions & Predefined Actions).

2. The first donut chart breaks down the number of submissions the classification provided (**Safe**, **Caution**, **Threat**) and the exception classifications (failure, unprocessed, invalid).

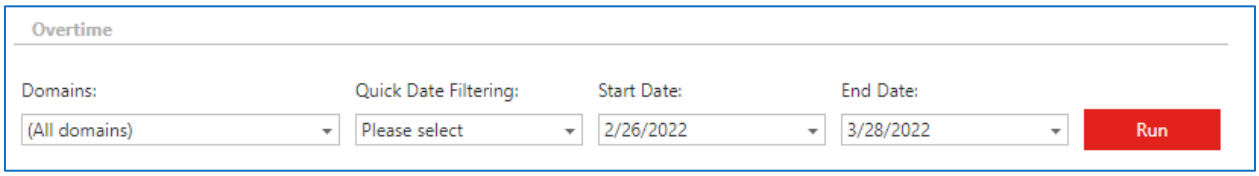


3. The second donut chart breaks down the classification by safe, caution and a granular classification for threats (Virus, Spam, Adult, Phishing).



OVERTIME

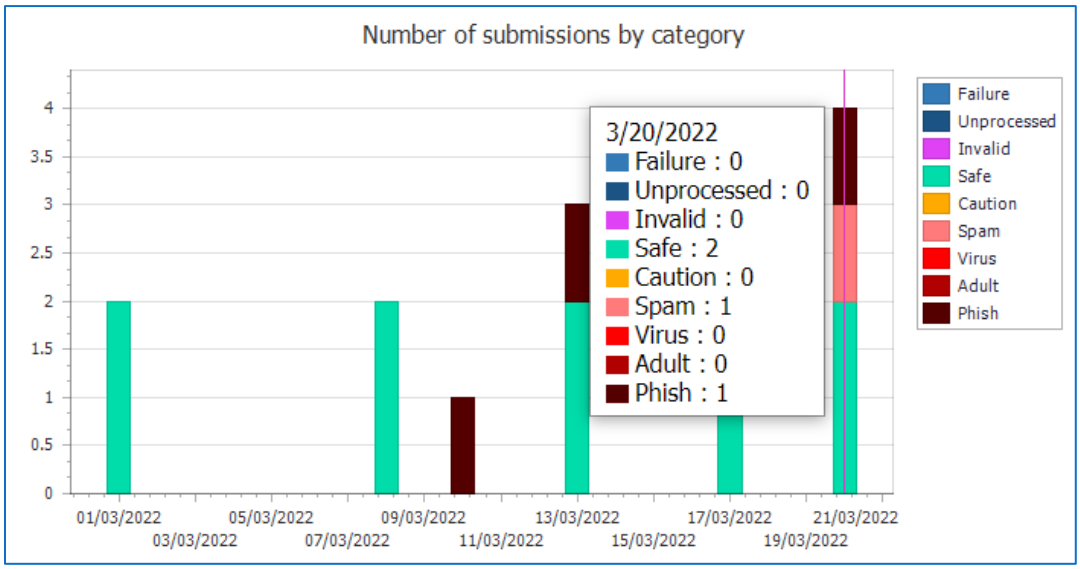
The next area of the Statistics section is labeled as Overtime. This section displays Domain and date filter bar drop-down menus which apply to each of the 4 various graphs detailed below.



1. Domains – used to display all Microsoft domains associated with TPx Managed IDR (default) or select an individual domain. In most circumstances, you only have a single domain listed here.
2. Quick Date Filtering – used to filter these graphs based on a calculated date range. The options include:
    a. Today
    b. Last 7 Days
    c. Last 30 Days
    d. Last 90 Days
3. Start Date/End Date – used to filter these graphs based on an absolute date range. This displays a specific submission timeframe outside of quick date filtering options.

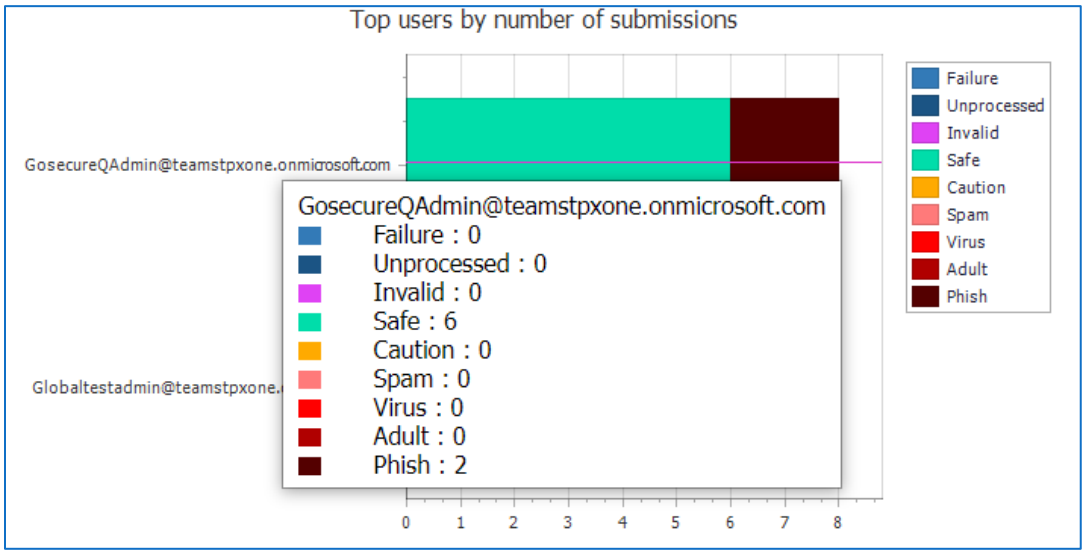
NUMBER OF SUBMISSIONS BY CATEGORY

The first graph displayed is the Number of Submissions by category stacked bar chart. This chart displays the number of submissions on a given date with categories represented by assorted colors on each day. Hovering your cursor over the chart displays more details for the submission history on that day.



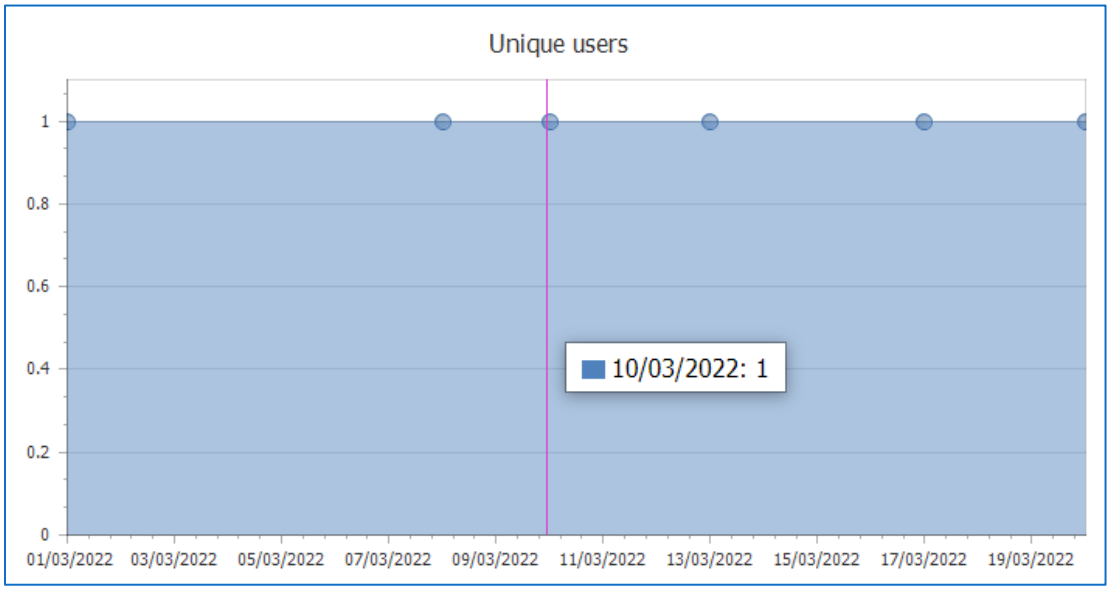
TOP USERS BY NUMBER OF SUBMISSIONS

The next graph displays a breakdown of how many messages users submitted for analysis. Each user email address is associated with your Microsoft Tenant. Like the number of submissions by category graph, each bar has colors representing the classification of each submission. You can also hover to view additional details on this graph.



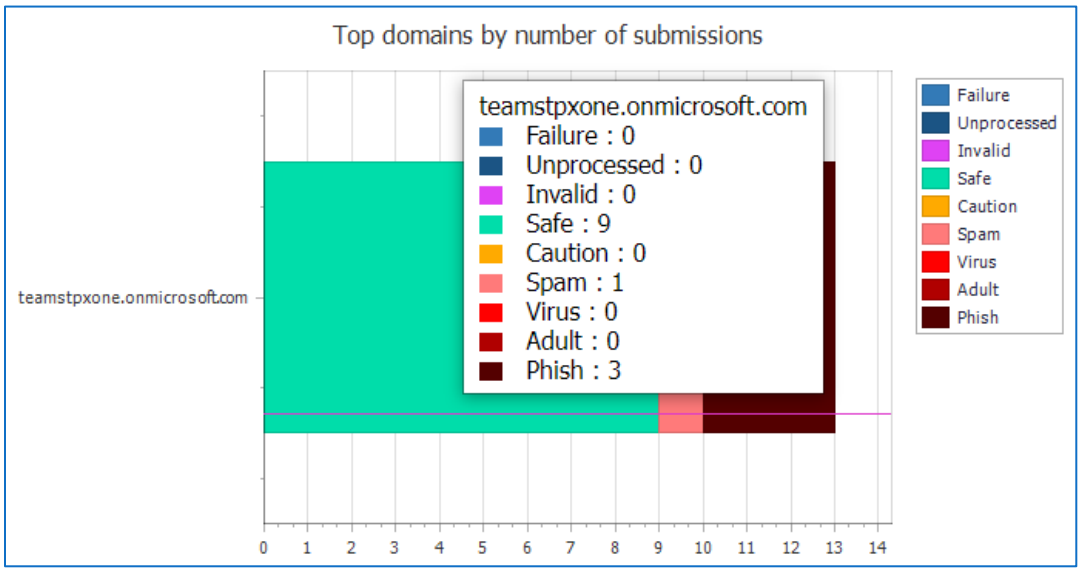
UNIQUE USERS

This line area chart displays the running count of how many unique users utilized TPx Managed IDR on a particular day. You can also hover to view additional details on this chart.



TOP DOMAINS BY NUMBER OF SUBMISSIONS

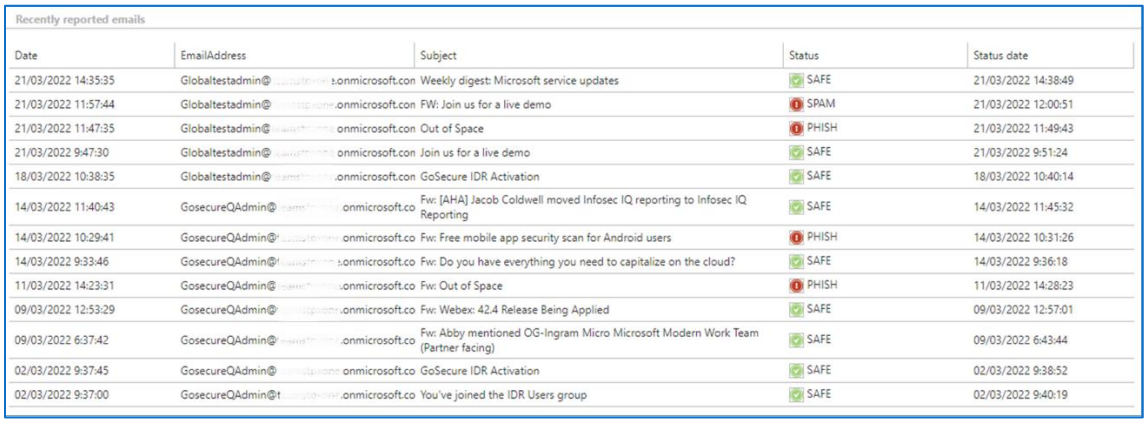
The top Domains by number of submissions stacked bar chart displays a breakdown of the submissions made on your Microsoft Tenant, broken down by domain. You can also hover to view additional details on this chart.



RECENTLY REPORTED EMAILS

The last section displays a table of your organization's most recently submitted messages for analysis by the GoSecure Threat Detection Center. The following fields are available:

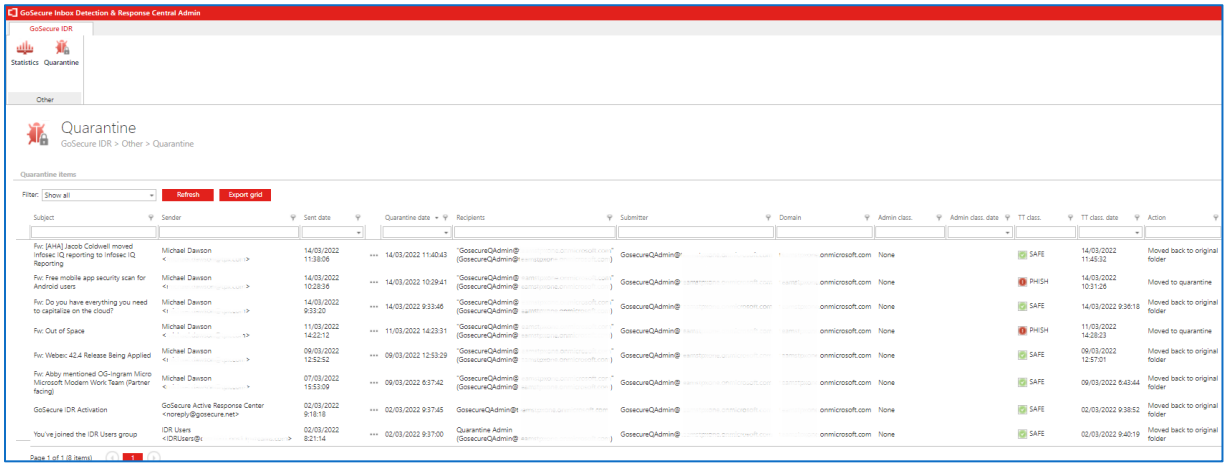
- Date
  - The date the original submitter sent in their message for analysis.
- Email Address
  - The email address associated with the user submitting the message.
- Subject
  - The subject line of the submitted message.
- Status
  - The classification given to the message based on the analysis performed by the GoSecure Threat Detection Center. For additional information on classifications, please refer to Appendix A: Classification Definitions & Predefined Actions section.
- Status Date
  - The date and time the **Status** is given for the reported message.


Recently reported emails

Date	EmailAddress	Subject	Status	Status date
21/03/2022 14:35:35	Globaltestadmin@ .onmicrosoft.com	Weekly digest: Microsoft service updates	SAFE	21/03/2022 14:38:49
21/03/2022 11:57:44	Globaltestadmin@ .onmicrosoft.com	FW: Join us for a live demo	SPAM	21/03/2022 12:00:51
21/03/2022 11:47:35	Globaltestadmin@ .onmicrosoft.com	Out of Space	PHISH	21/03/2022 11:49:43
21/03/2022 9:47:30	Globaltestadmin@ .onmicrosoft.com	Join us for a live demo	SAFE	21/03/2022 9:51:24
18/03/2022 10:38:35	Globaltestadmin@ .onmicrosoft.com	GoSecure IDR Activation	SAFE	18/03/2022 10:40:14
14/03/2022 11:40:43	GosecureQAdmin@ .onmicrosoft.co	Fw: [AHA] Jacob Coldwell moved Infosec IQ reporting to Infosec IQ Reporting	SAFE	14/03/2022 11:45:32
14/03/2022 10:29:41	GosecureQAdmin@ .onmicrosoft.co	Fw: Free mobile app security scan for Android users	PHISH	14/03/2022 10:31:26
14/03/2022 9:33:46	GosecureQAdmin@ .onmicrosoft.co	Fw: Do you have everything you need to capitalize on the cloud?	SAFE	14/03/2022 9:36:18
11/03/2022 14:23:31	GosecureQAdmin@ .onmicrosoft.co	Fw: Out of Space	PHISH	11/03/2022 14:28:23
09/03/2022 12:53:29	GosecureQAdmin@ .onmicrosoft.co	Fw: Webex: 42.4 Release Being Applied	SAFE	09/03/2022 12:57:01
09/03/2022 6:37:42	GosecureQAdmin@ .onmicrosoft.co	Fw: Abby mentioned OG-Ingram Micro Microsoft Modern Work Team (Partner facing)	SAFE	09/03/2022 6:43:44
02/03/2022 9:37:45	GosecureQAdmin@ .onmicrosoft.co	GoSecure IDR Activation	SAFE	02/03/2022 9:38:52
02/03/2022 9:37:00	GosecureQAdmin@t .onmicrosoft.co	You've joined the IDR Users group	SAFE	02/03/2022 9:40:19

QUARANTINE OVERVIEW

The Quarantine section displays the pertinent details for every submitted email from your organization. It includes classifications assigned to each message action taken on that message, logs showing the history of that message, and the ability to view the message itself for further analysis.

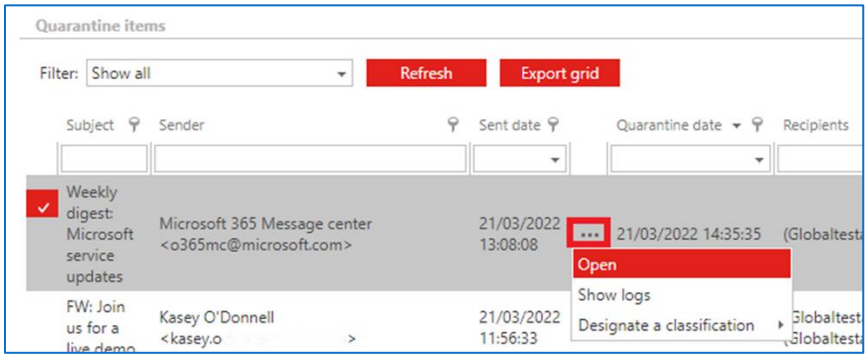


QUARANTINE CLASSIFICATION/ACTION

The classifications and action taken on submitted messages displays information on how the message is managed after submission for analysis. A detailed breakdown of each classification and the default actions taken can are referenced in Appendix A: Classification Definitions & Predefined Actions section.

OPENING A MESSAGE

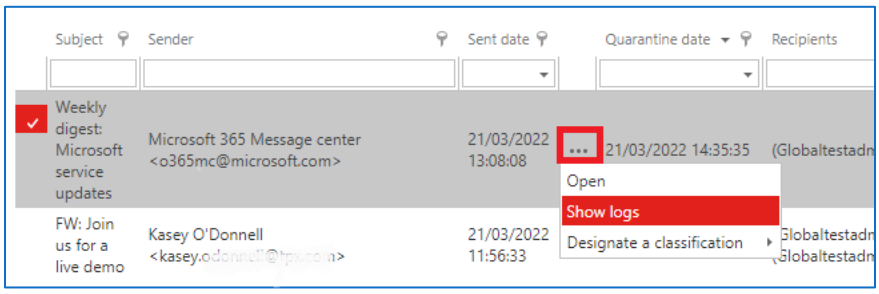
Quarantine Administrators can review the body of a submitted message at any time using the ellipsis icon, then clicking **Open** in from the menu.



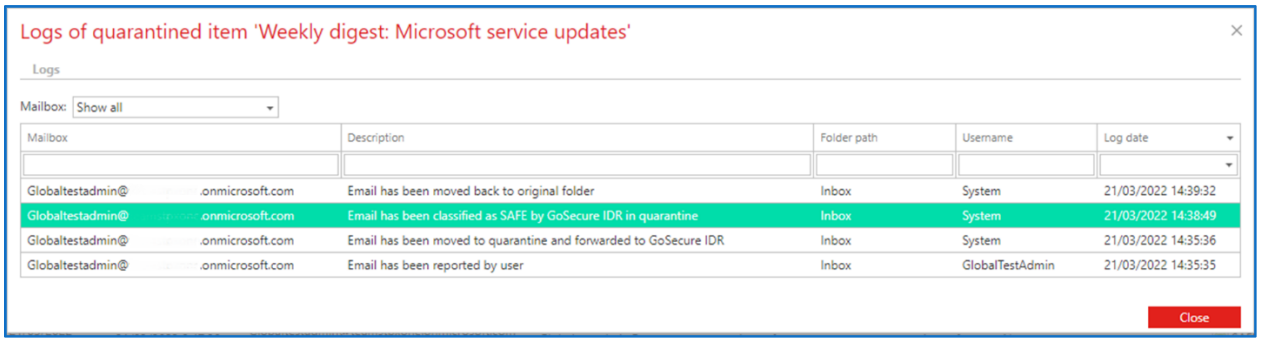
NOTE: Opening an email from quarantine downloads the message as an .eml file, which opens within your preferred Outlook client. Take caution when accessing a cautious or malignant message.

VIEWING MESSAGE LOGS

At any time, you can also view the full history of how a submitted message is managed. Click the ellipsis icon for the desired message, then select **Show logs** from the menu.



The Log details display:

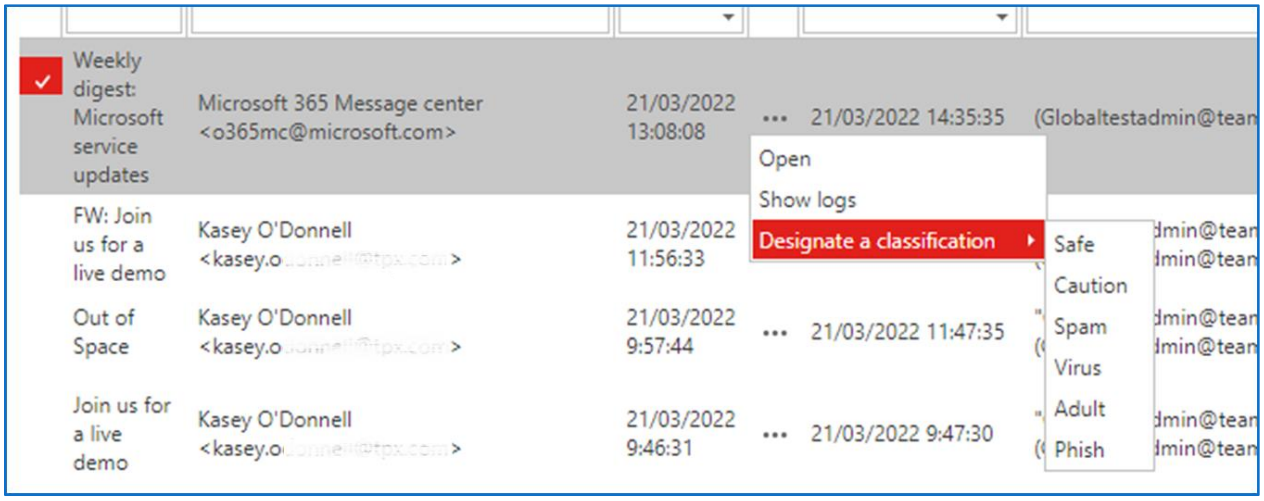


The logs display the submitter mailbox, description of the action taken, username of who made the changes, and a date the change is made.

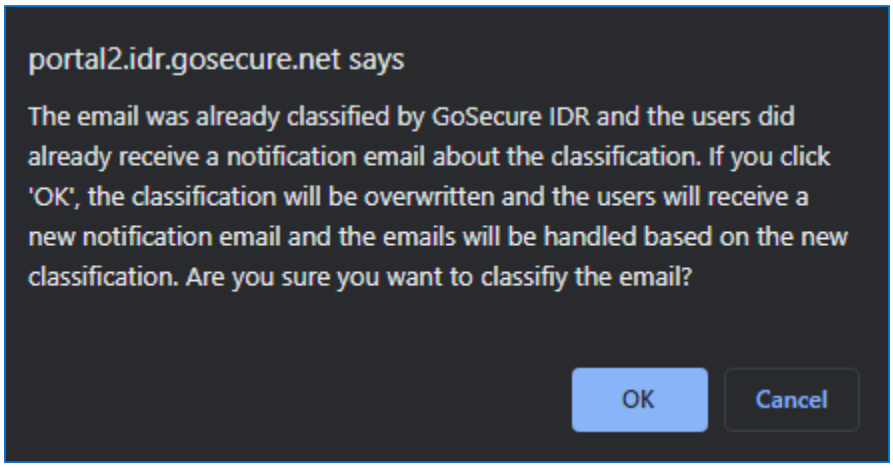
DESIGNATING A CLASSIFICATION

In some circumstances, you may determine after reviewing a message that you need to assign an alternative classification. This also changes the action taken on the message. For a breakdown of each classification and the default action, please refer to Appendix A: Classification Definitions & Predefined Actions.

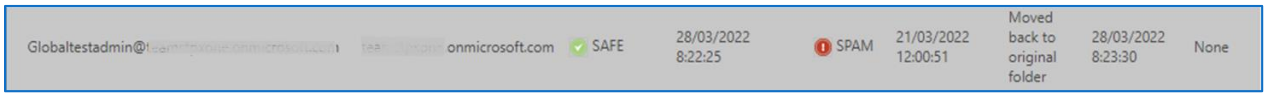
To change the classification of a message, click the ellipsis icon for the desired message, then select **Designate a classification** from the menu: **Safe, Caution, Spam, Virus, Adult, Phish**.



Note the following prompt after selecting the new classification:



There are now two additional fields populated: *Admin class* and *Admin Class. Date*. These fields display newly assigned classification for the message and date changed by an administrator. This overrides the original classification and action. In the below example, we changed a message reported as *Spam* to *Safe*.



The action was updated to *Move back to original folder* because it is now SAFE.

APPENDICES

APPENDIX A: CLASSIFICATION DEFINITIONS & PREDEFINED ACTIONS

Within various areas of the GoSecure Admin Center, there are several "classifications" that fall into our various "Status Alert" emails that show the status of the message, which determine action taken on that message.

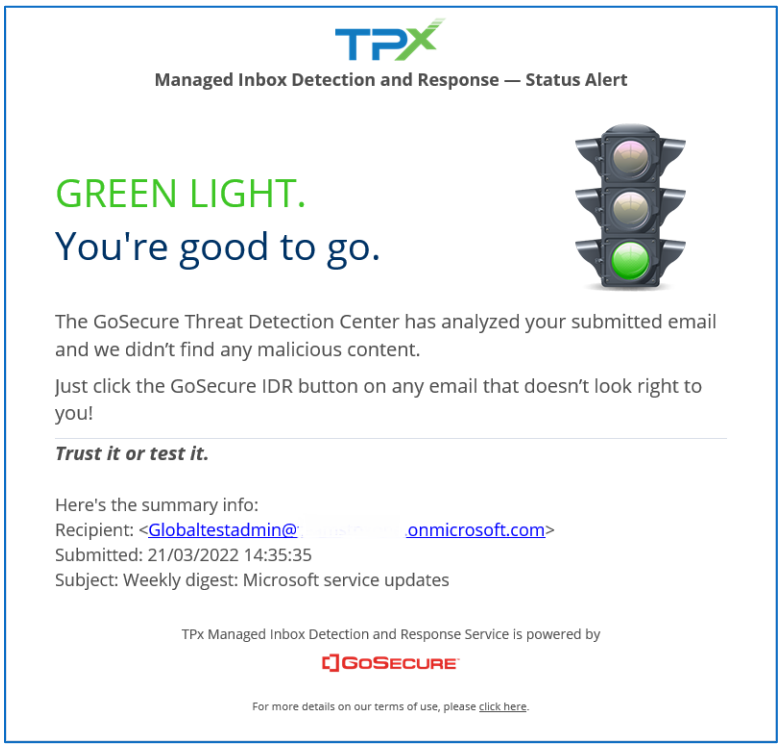
The 3 main statuses end users receive are:

- Green Light
- Yellow Light
- Red Light

There is a 4th section (administrative) planned to capture classifications that do not apply to these main statuses. Below, each Status lists default action, as well as which classifications fall under which status.

GREEN LIGHT

By default, Green Light messages are returned to the submitter inbox and are deemed safe.



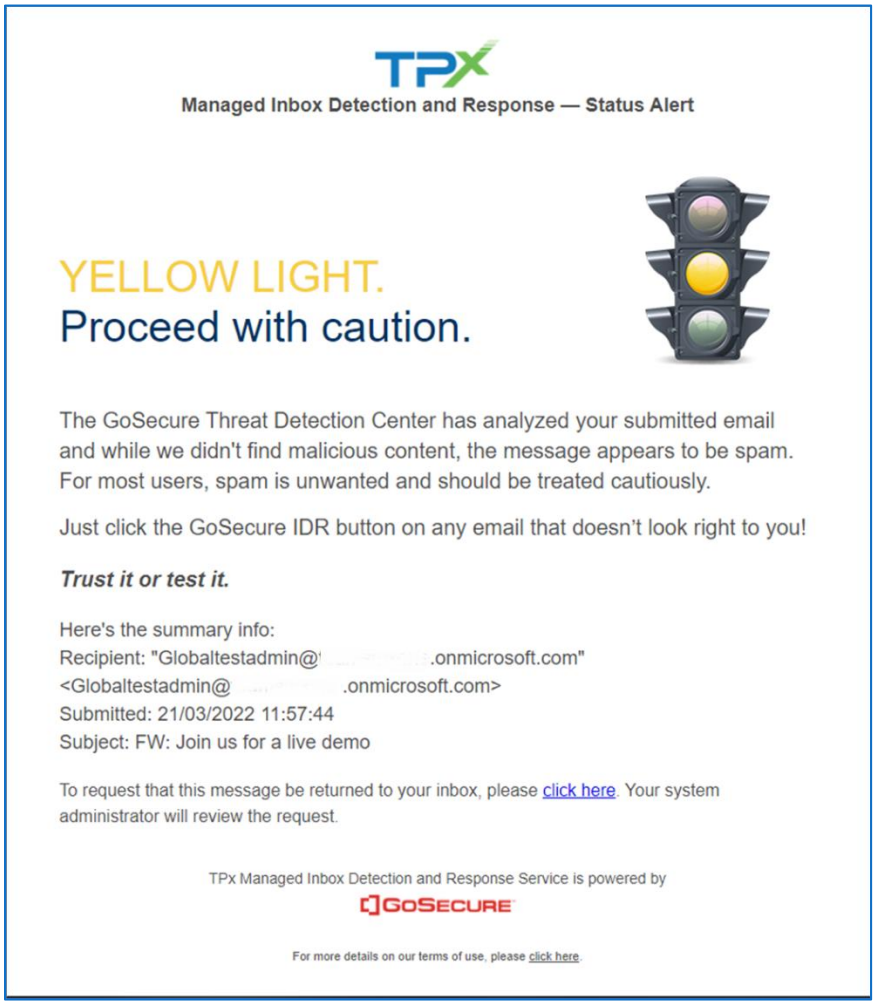
An example of a Green Light Status Alert Message

The classification that falls under the Green Light Status is:

SAFE - There are no immediate threats to the end user and the message is safe.

YELLOW LIGHT

By default, Yellow Light messages do not go back to the submitter inbox immediately. They message are quarantined for further inspection.



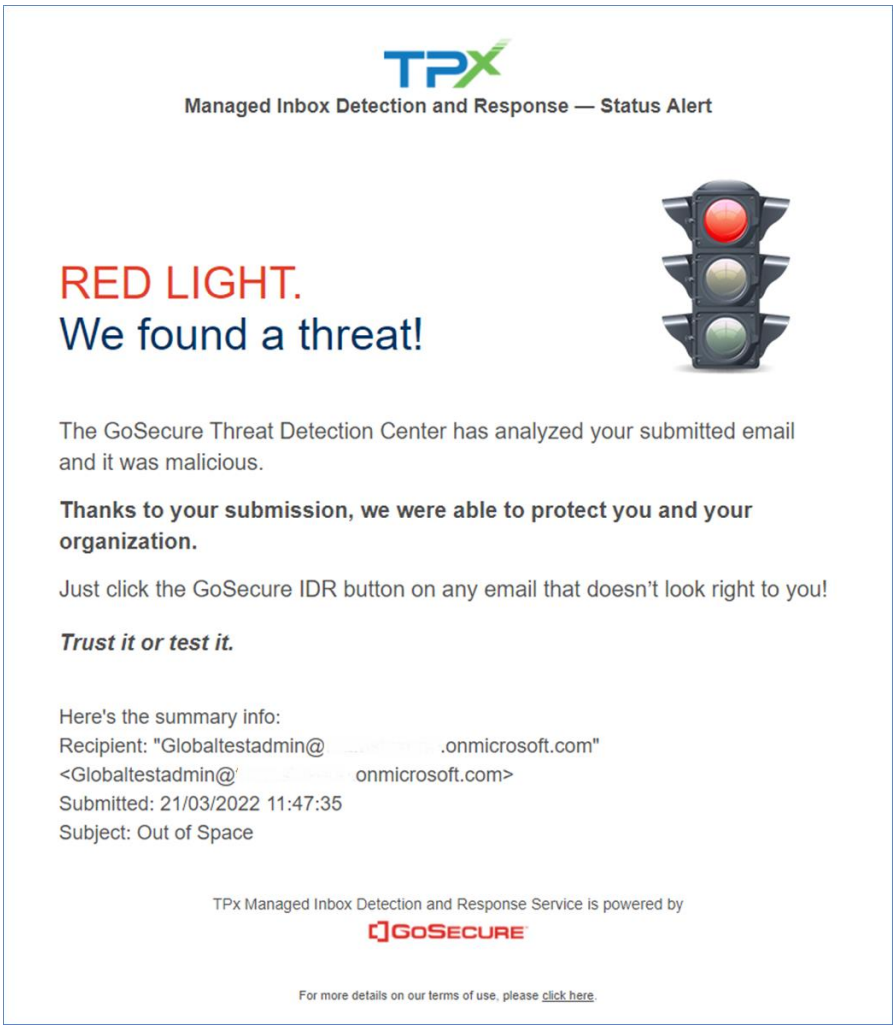
An Example of a Yellow Light Status Alert Message

The various classifications that fall under Yellow Light status are:

- Spam - No immediate threat to end user, it is just spam.
- Caution - There is no direct threat found in the message, however based on previously submitted messages to this one, it may lead to a direct threat.

RED LIGHT

By default, Red Light messages are not sent back to the submitter inbox and are quarantined.



An Example of a Red Light Status Alert Message

The classification that falls under the Red-Light Status is:

Threat - The message is deemed malignant and there is an immediate threat to the end user opening or accessing content in the message.

ADMINISTRATIVE

This section covers classifications that are typically only visible within the GoSecure IDR Admin Center. The various classifications, actions taken, and a brief description of what the classification means are:

- Invalid
    - Invalid indicates that there was an issue with the submitted message, where the GoSecure Threat Detection Center did not receive the submission.
    - The default action is to return the message back to the submitter's original inbox folder.
- Unprocessed

    - Indicates an issue with the submitted message, where it was received, and that it could not be processed.
    - The default action is to attempt to reprocess the email (2 attempts) prior to returning to the submitter's original inbox folder.
- Failure
    - Indicates that the message was received, the GoSecure Threat Detection Center attempted to process the message, but it did not work.
    - Default action is to return the message back to the submitter's original inbox folder.
- SAE Training Message
    - This is a message sent by a Security Awareness Education vendor. As an administrator, you can see which submitted messages were legitimate submissions or test emails sent by your selected SAE Vendor. End users cannot distinguish these messages from a legitimate suspicious or malicious email.
    - By default, these messages are kept in quarantine.

GLOBAL REDACTION

Global Redaction allows end users to submit suspicious or malicious emails and also pull from other tenant mailboxes, when they are classified as unsafe (refer to the Yellow Light and Red Light sections above for additional information on which classifications are affected).

Global Redaction is enabled by default.