

Response Detection

For accurate statistics, Lucy has the functionality to work with emails that came in response to a phishing email. Thus, you can determine which of the recipients did not actually receive the e-mail (for example email was not delivered and Lucy received a response from the mail server) or do not include the auto-responses in the statistics.



Please note that Automated Response Detection will not work if some conditions are not met:

1. Sender's domain (used in the Scenario Settings > Message Template) must have MX records pointed to the Lucy server. If MX records configured correctly, responses to the sender email will be delivered to the Lucy server and Lucy will be able to process these responses. Otherwise, if MX record of the sender domain is not pointed to the Lucy server, responses do not deliver to the Lucy, and Automated Response Detection option will not work.
2. You need to enable Track Responses option in the campaign Base Settings:

Home / Campaigns / Lucy Phishing Campaign / Base Settings

Lucy Phishi... Campaign Status Not Started ▶

Results

- Summary
- Statistics
- Reports
- Exports

Configuration

- Base Settings
- Awareness Settings
- Schedule
- Recipients

Name Lucy Phishing Campaign

Client Lucy Security AG

Industry N/A

Notes

☒ Enduser Profiles Enabled

☒ Track Responses

☐ Email Tracking

Antivirus/Firewall Protection off

This option will enable Automated Response Detection in the **all** scenarios of this campaign.

3. If you need to enable this option for a separate scenario, open the Scenario Base Settings > Message Template page and enable Receive Sender E-Mail Replies option in the Advanced Email Settings section:

▼ Attachments

▼ General email settings

▲ Advanced Email Settings

☒ Receive Sender E-Mail Replies

☐ Send Plain-Text Email

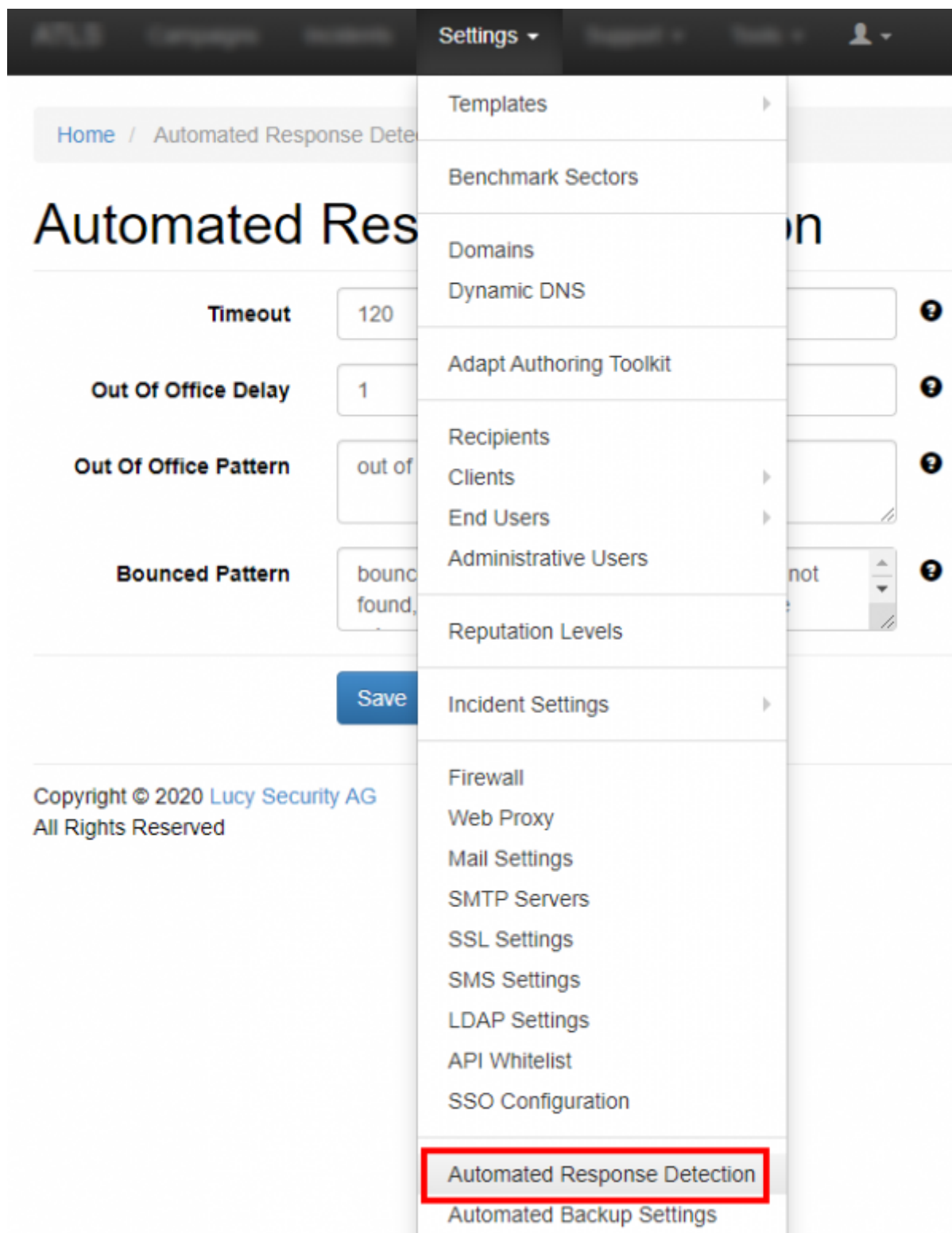
☐ Random email ⓘ

☒ DKIM Support ⓘ

Please add the following TXT record to miktestlucy.host domain's DNS records:

Automated Response Detection settings

You could change settings of Automated Response Detection here:



There are 4 main types of track responses settings:

Automated Response Detection

1	Timeout	<input type="text" value="60"/>	?
2	Out Of Office Delay	<input type="text" value="1"/>	?
3	Out Of Office Pattern	<input type="text" value="office,away,vacation,holidays"/>	?
4	Bounced Pattern	<input type="text" value="error 450, not found"/>	?


Save

1. Emails returned immediately after sending a phishing emails are most likely an auto-reply. If an email will arrive within the given period (in seconds) after submitting an attack email, the incoming email will be treated as an automated response.
2. The best way to coverage all recipients in a campaign is to resend phishing email to victims who for some reason set up an automated response. Since most likely the victim is not in the workplace or he does not read the email, it is best to resend the message in a few days. In this field, specify number of days to wait until sending a reminder for the victim that is out of office.
3. Patterns to find in replies to mark them as 'out of office' responses. For example its can be patterns related with holidays or business trip. A repeated email will arrive in the number of days specified in "Out Of Office Delay"
4. Each mail server has its own template of bounced emails. In this field, you can specify pattern to find in replies to mark them as 'bounced' responses or some errors from mail server.

Mail Manager

The mail manager allows interactive communication with the recipient. First of all, this type of communication must be activated in the campaign. Please make sure the MX record for the sender email points to LUCY. See [response detection chapter](#).

World

Campaign Status Running 

Results

Summary

Statistics

Reports

Exports

Configuration

Base Settings

Awareness Settings

Schedule

Recipients

Name

World

Client

Lucy Test

Industry

N/A

Notes

☐ Enduser Profiles Enabled

☒ Track Responses

☐ Email Tracking

Antivirus/Firewall Protection

off

You can the see email replies in the mail manager which is accessible here:

The screenshot shows the Lucy Security AG web interface. At the top, there is a navigation bar with links for 'Home', 'Campaigns', 'Tools', 'Settings', 'Support', and a user profile icon. Below the navigation bar, the 'Campaigns' page is displayed. It features a search bar and a table of campaigns. The table has columns for 'Campaign', 'Type', and 'Status'. Two campaigns are listed: 'Lucy Test' and 'Lucy Phishing Campaign'. Below the table, there is a copyright notice: 'Copyright © 2020 Lucy Security AG All Rights Reserved'. On the right side, a dropdown menu is open, showing various system management options. The 'Mail Manager' option at the bottom of the menu is highlighted with a red rectangle.

Campaign	Type	Status
<input type="checkbox"/> Lucy Test	!	-
<input type="checkbox"/> Lucy Phishing Campaign	!	▶

Copyright © 2020 Lucy Security AG
All Rights Reserved

- Status
- Manual
- Changelog
- Test email
- Performance Test
- System Monitoring
- Spam Test
- Backups
- Migration Tool
- Exports
- License
- Tickets
- Invoices
- Update
- Reboot
- SSH Password
- Enable SSH Access
- Send Logs
- Service Logs
- Mail Manager**

The multi-staged interactive communication can then continue within the mail manager:

Mail Manager

Filter ▾

Search

From Date

09.04.2020

To Date

10.04.2021

☐ Search in message body (may take longer)




Campaign

Unsorted ▾

Type

All ▾

Update

Time	From	Subject	Type	Actions
09.04.2021 09:13	Nick Vyatkin (nick@lucysecurity.com)	Fwd: This is not SPAM!	Reports	  

Your copyright goes here

From:
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=response_detection

Last update: **2021/04/14 09:45**

