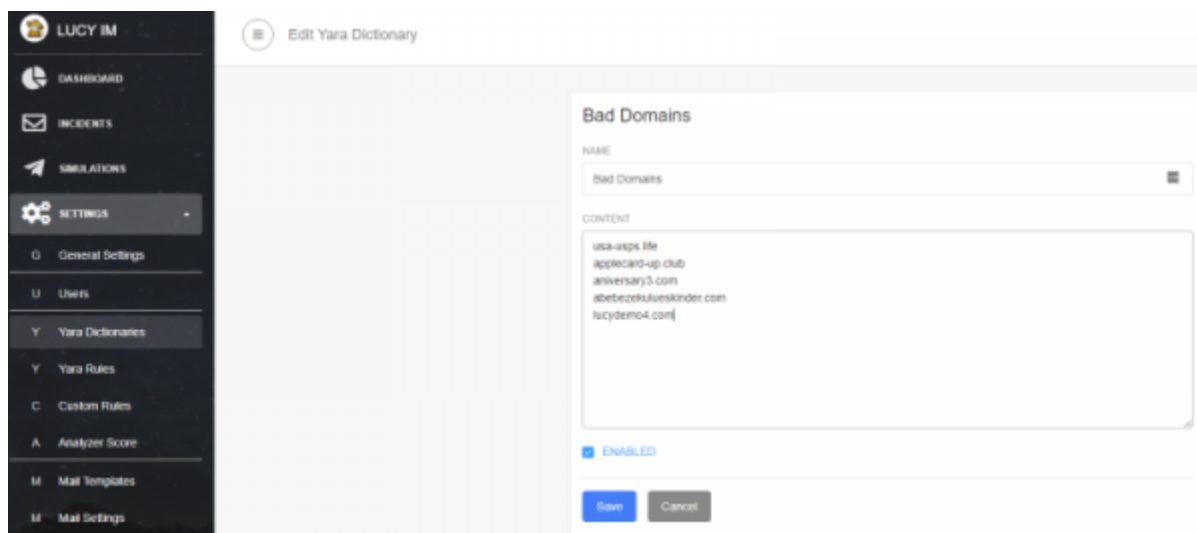


Yara Dictionaries

On this page you can create the dictionaries for use in the [Yara rules](#).

For example, you need to assign additional scores to the domains from the big list.

So create the dictionary called **BadDomains.dict** with the domain list (line by line):

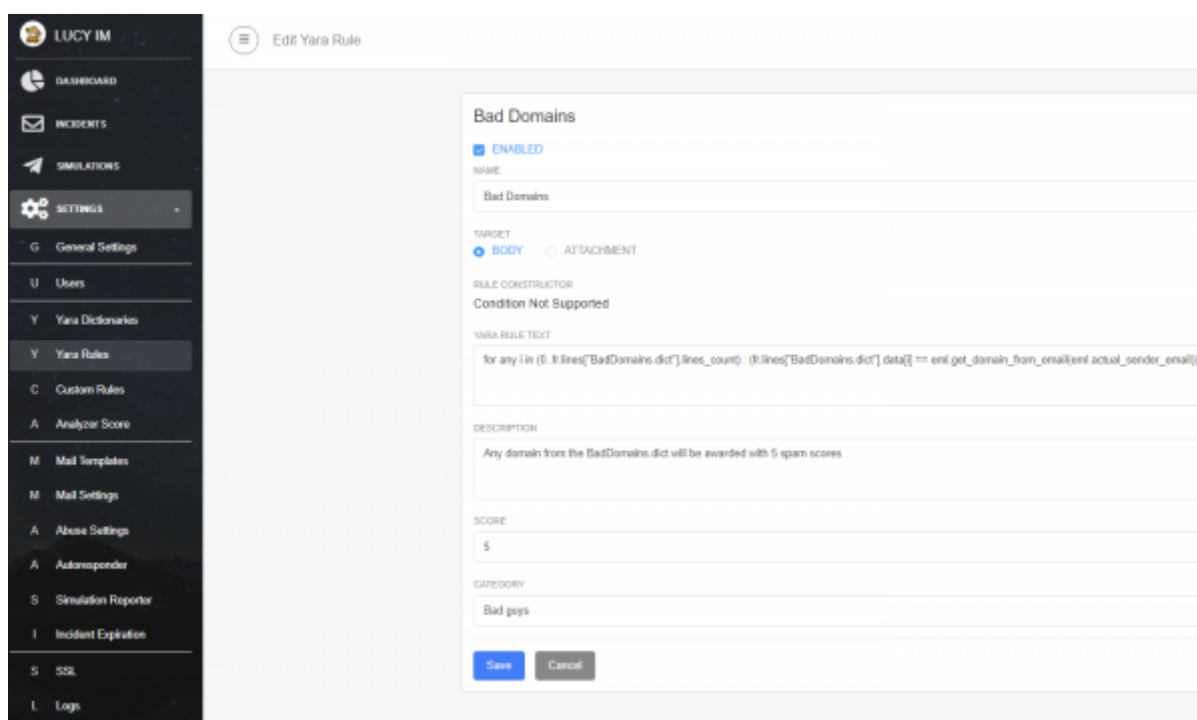


The screenshot shows the 'Edit Yara Dictionary' interface. The left sidebar contains the following menu items: LUCY IM, DASHBOARD, INCIDENTS, SIMULATIONS, SETTINGS (selected), General Settings, Users, Yara Dictionaries, Yara Rules, Custom Rules, Analyzer Score, Mail Templates, and Mail Settings. The main panel is titled 'Edit Yara Dictionary' and shows a form for 'Bad Domains'. The form includes a 'NAME' field with the value 'Bad Domains', a 'CONTENT' text area containing the following domains: usa-aspe life, applecard-up club, anniversary3.com, abetbezokuleskinder.com, lucydemo4.com, an 'ENABLED' checkbox, and 'Save' and 'Cancel' buttons.



For dictionaries, we recommend using names without spaces, special characters and ending with ".dict"

And then you will be able to use this dictionary in the [Yara rules](#)



The screenshot shows the 'Edit Yara Rule' interface. The left sidebar contains the following menu items: LUCY IM, DASHBOARD, INCIDENTS, SIMULATIONS, SETTINGS (selected), General Settings, Users, Yara Dictionaries, Yara Rules (selected), Custom Rules, Analyzer Score, Mail Templates, Mail Settings, Abuse Settings, Autoresponder, Simulation Reporter, Incident Expiration, SQL, and Logs. The main panel is titled 'Edit Yara Rule' and shows a form for 'Bad Domains'. The form includes a 'NAME' field with the value 'Bad Domains', a 'TARGET' field with 'BODY' selected, a 'RULE CONSTRUCTOR' field with the value 'Condition Not Supported', a 'YARA RULE TEXT' field containing the following YARA rule snippet:

```
for any i in (if (if (lines["BadDomains.dict"].lines_count) : (if (lines["BadDomains.dict"] detx{[ == enil get_domain_from_email(enil actual_sender_email))
```

, a 'DESCRIPTION' field with the value 'Any domain from the BadDomains.dict will be awarded with 5 spam scores', a 'SCORE' field with the value '5', a 'CATEGORY' field with the value 'Bad guys', and 'Save' and 'Cancel' buttons.

In this example, any message from the email contained the domain from the **BadDomains.dict** will get 5 spam scores.

From:

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

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=screener_yara_dictionaries

Last update: **2021/04/28 11:04**

