Lepide

USE CASE GUIDE

HOW TO CONFIGURE A THREAT DETECTION WORKFLOW

Table of Contents

1 Introduction

Threat Detection Workflows allow you to create real time alerts and responses based on a sequence of events. This provides an essential tool to enable organizations to quickly detect and respond to potential attacks. Once the sequence of events is detected by the Lepide Data Security Platform, an alert will be triggered, and immediate action can then be taken to reduce risk and mitigate damage.

2 What are Threat Detection Workflows?

Threat Detection Workflows are a user-specified sequence of events for which you want to create alerts and responses. The administrators, or selected recipients, specify the contents of the sequence and will then receive alerts as email notifications, LiveFeed updates and as push-notifications on our mobile-based application.

Alert sequences can comprise several factors. These could include:

- particular events (eg file copying)
- pre-defined criteria (such as time and date)
- threshold-based criteria

2.1 Threshold Alerting

Typical security breaches display characteristics which can be picked up by the Lepide threshold alerting capability. This ability to detect and alert on file activity which may be suspicious means that potential data breaches can be identified in motion and immediate action taken. So, within the workflow, threshold alerting can be included to provide real time safeguards against repeated events happening over a specified time period, which will reduce the risk of an attack.

2.2 Automated Response

The Lepide Data Security Platform can be configured to execute a customized script whenever a selected change is detected. Scripts can be of the following types:

- VB Script
- PowerShell Script
- Batch File

Using custom script execution, you can shut down users, servers and take other actions to mitigate the effects of a security breach.

3 To Create a Threat Detection Workflow

- Click on the **Alerts** icon

The Alerts screen is displayed.

At the top of the screen are four different tabs. Click on the **Threat Detection Workflows** Tab:

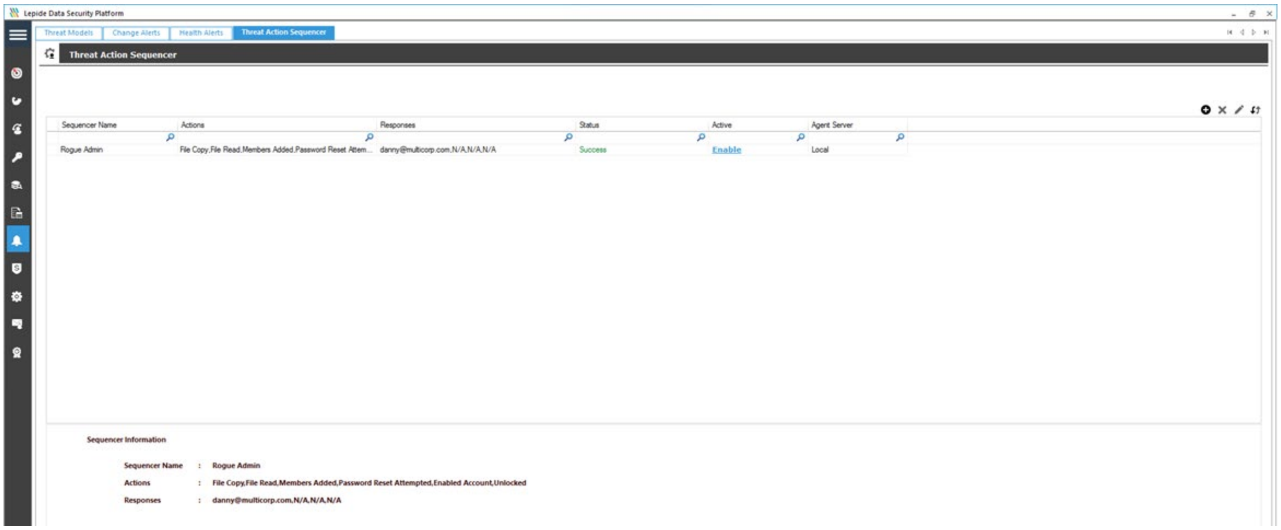

Figure 1: Threat Detection Workflows Screen

The screen will show any Workflows which have already been set up. They can be enabled or disabled from this screen.

- Click the icon to add a new Workflow

A Wizard will start, and the **Select Actions** dialog box is displayed:

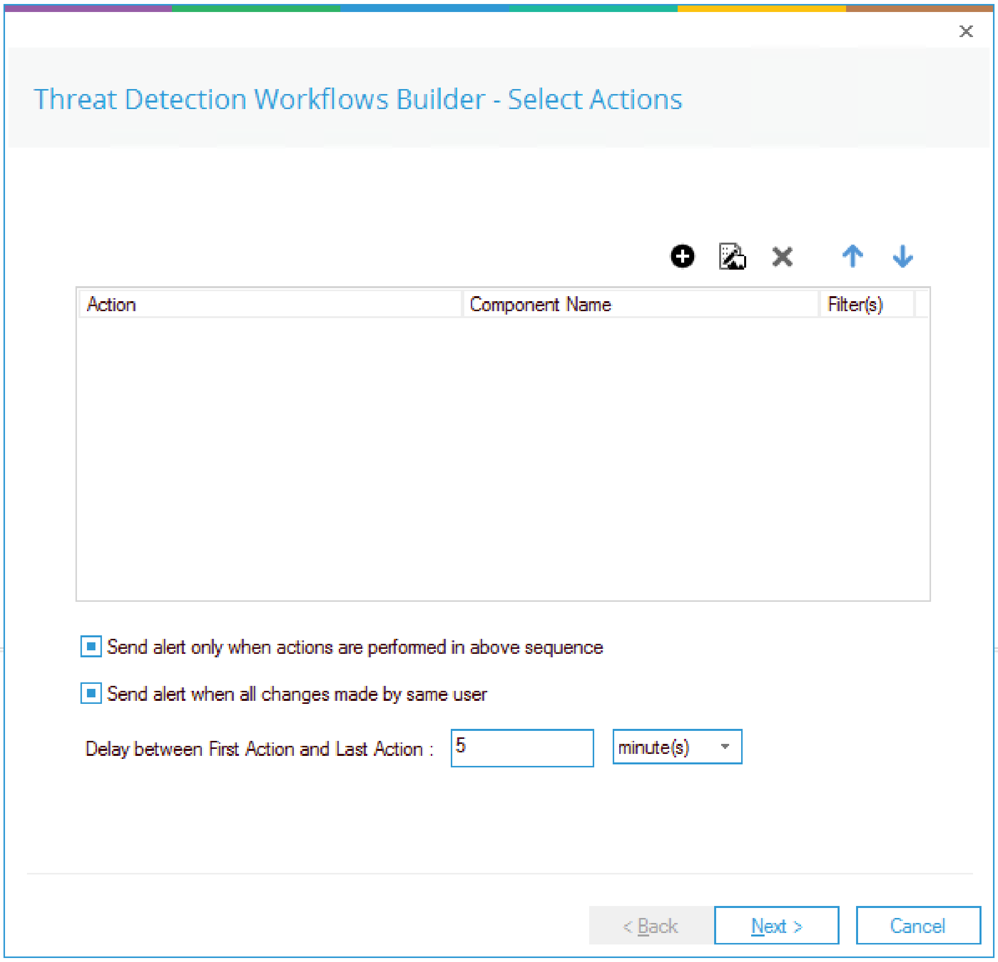

Figure 2: Select Actions

- Click the ⊕ icon to select a new action
- The **Threat Actions** dialog box is displayed:

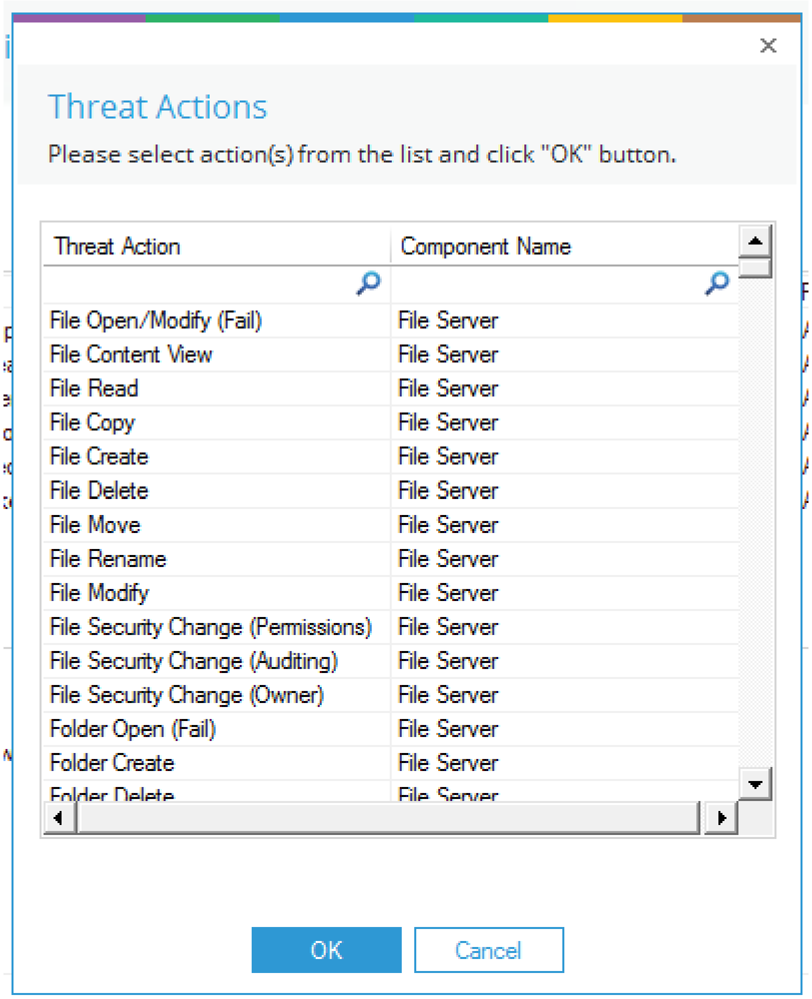

Figure 3: Threat Actions

- Select the Threat Action required and click **OK**
- Repeat these steps for all the actions required for the workflow

  You will return to the Select Actions dialog box each time
- The actions will be evaluated by the Solution in the order you specify so if you need to change the order, click the Up and Down arrow icons from the Select Actions dialog box

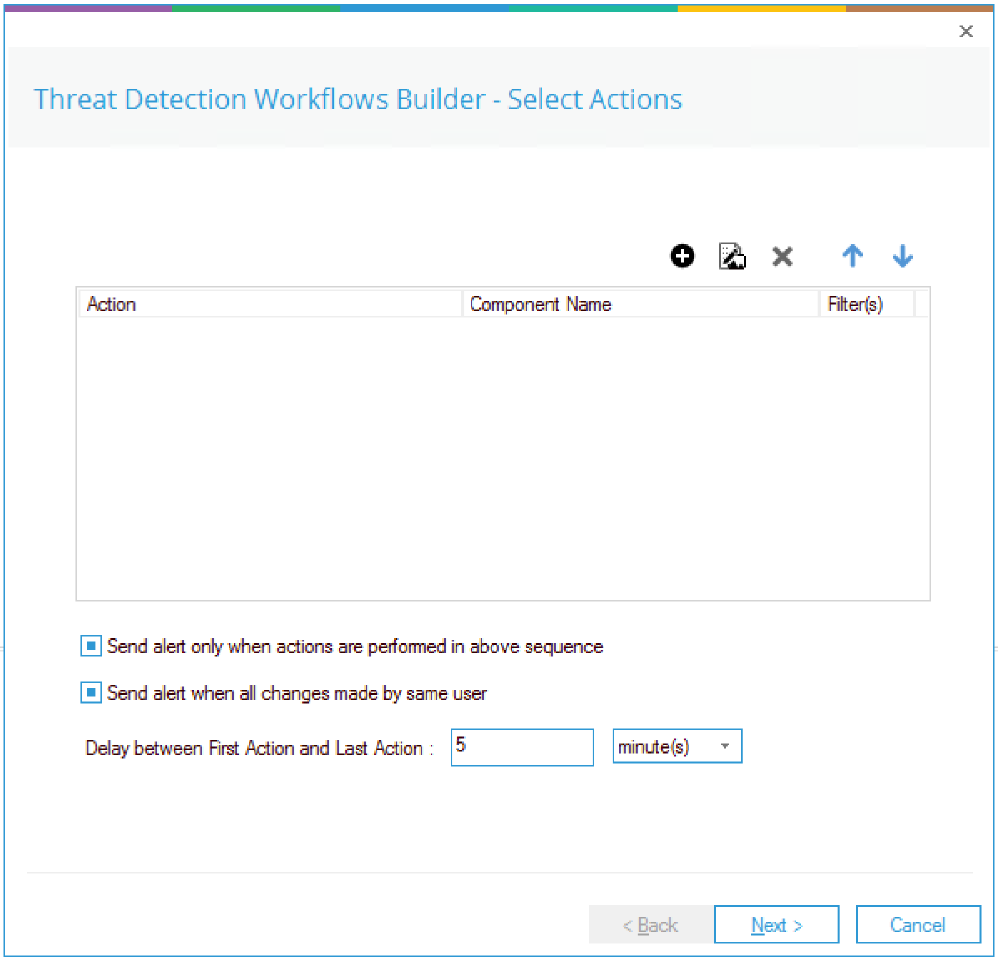

Figure 4: Select Actions

- Further options in the Select Actions dialog box are:
  - **Send alert only when actions are performed in above sequence** – this means that the alert will only be triggered if the actions are carried out in exactly the sequence specified. If this option is left unchecked, the alert will be triggered if all the actions are carried out but in **any** sequence
  - **Send alert when all changes made by same user** – the alert will only be triggered if all actions are carried out by one user. If left unchecked, the alert will be triggered when the actions are carried out by any combination of users
  - **Delay between First Action and Last Action -** this sets a time frame for when the actions are carried out. In this example, 5 minutes is specified so here all the actions would have to be carried out within 5 minutes for the alert to be triggered.
- Click **Next**

The **Select Response** dialog box is displayed:

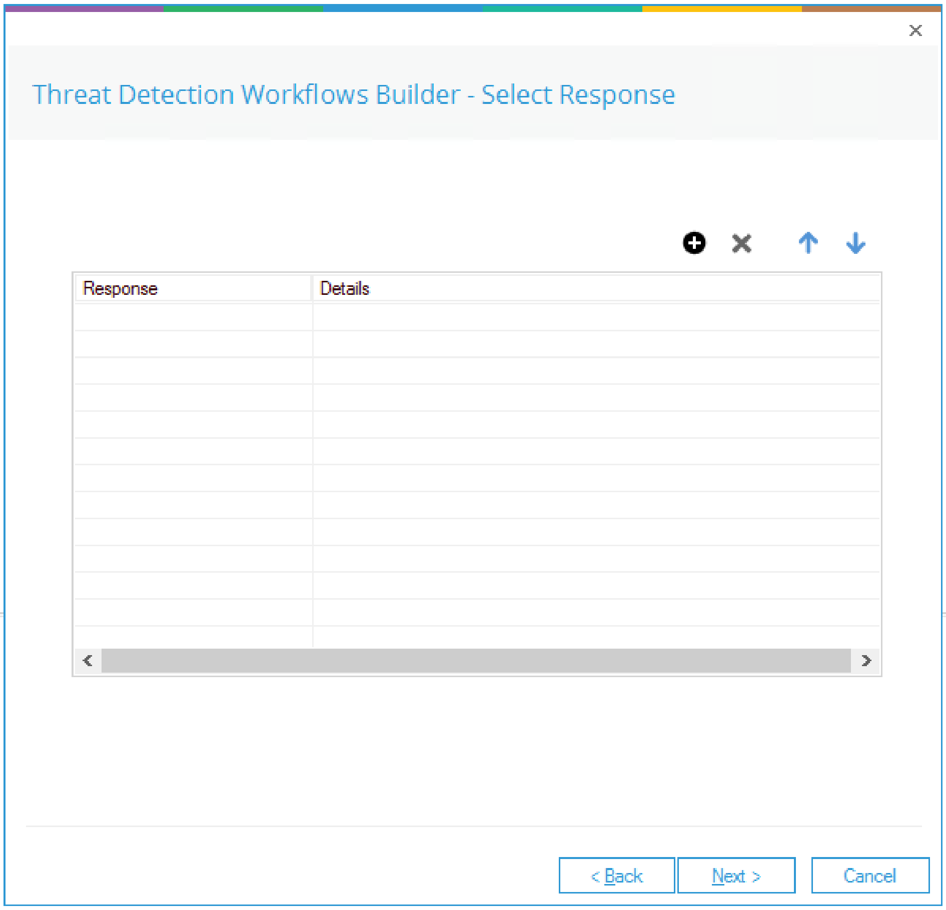

Figure 5: Select Response

- Click the ⊕ icon to select a response to the Workflow

The **Add Alert Action** dialog box will be displayed:

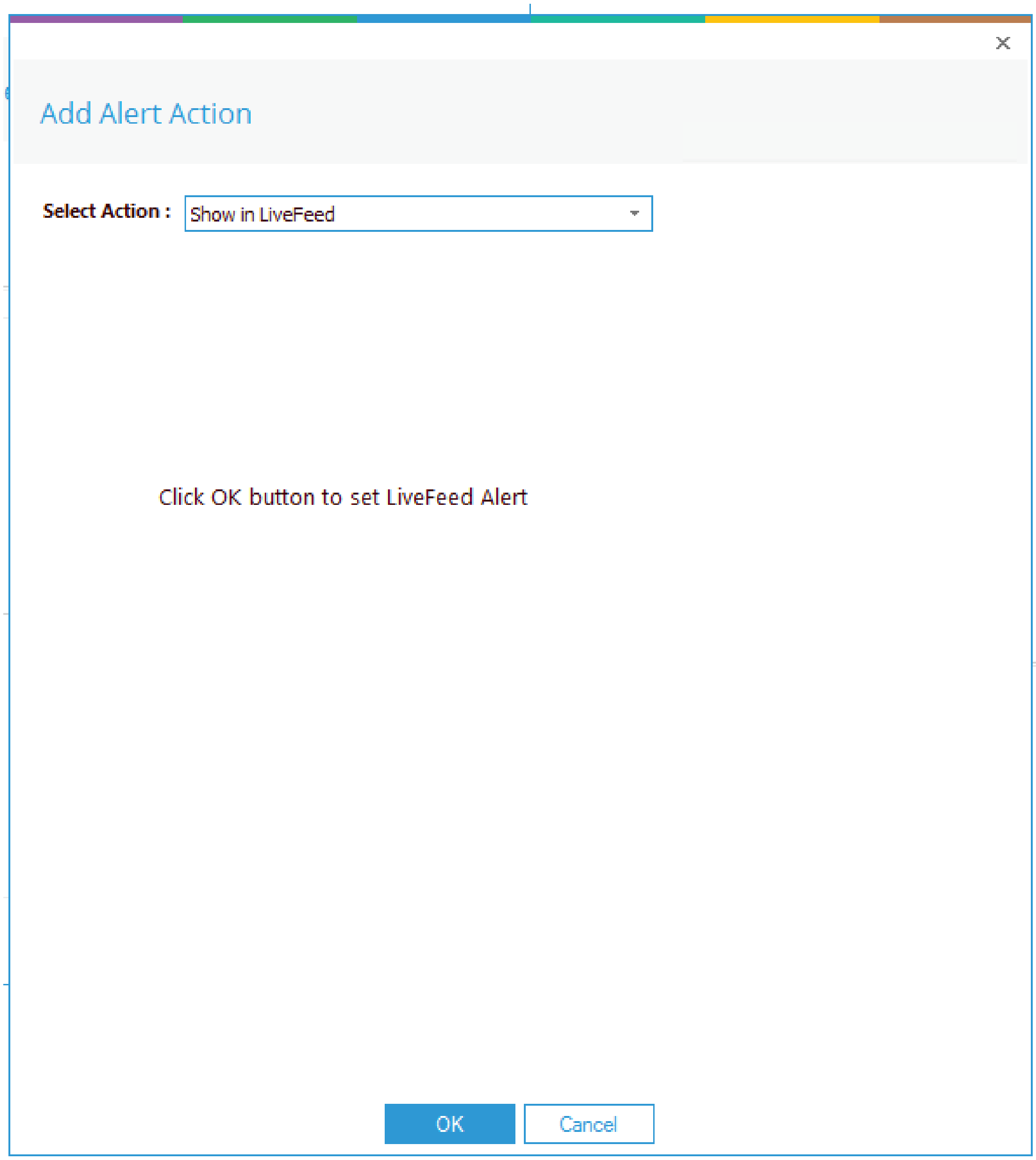

Figure 6: Add Alert Action

- Click the **Select Action** drop down arrow to see a list of actions available:

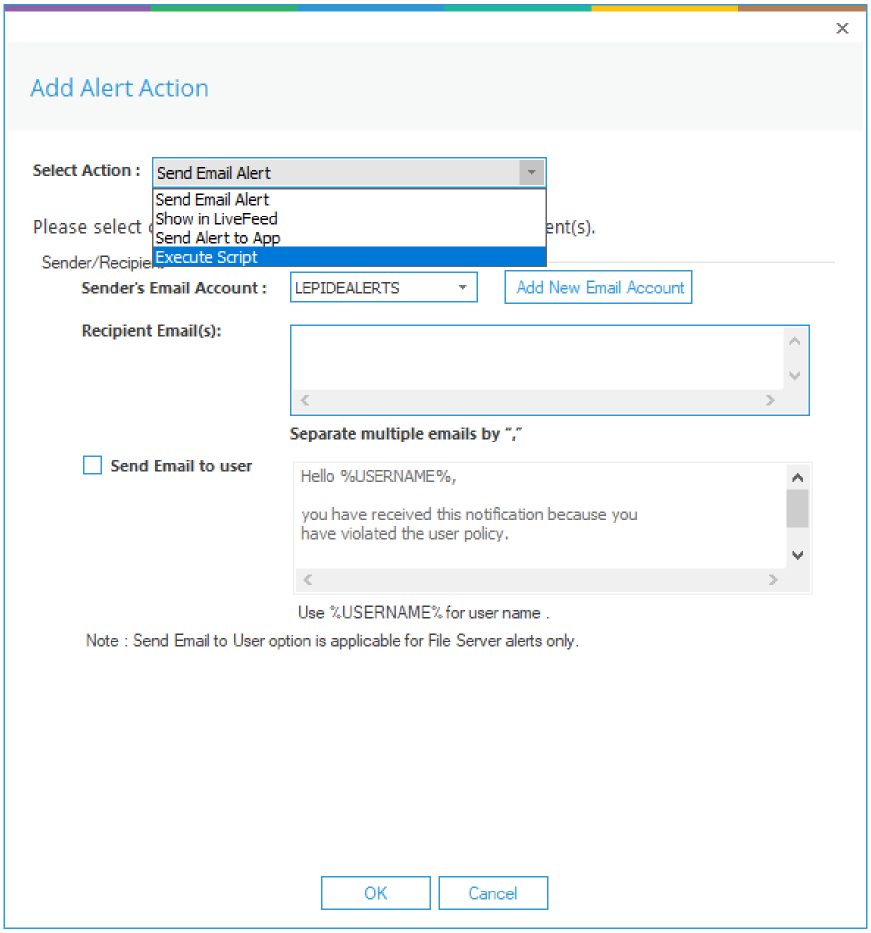

Figure 7: Add Alert Action Options

The Alert Actions are as follows:

- Send Email Alert
- Show in LiveFeed
- Send Alert to App
- Execute Script

The configuration of each of these actions is explained below:

1. Send Email Alert

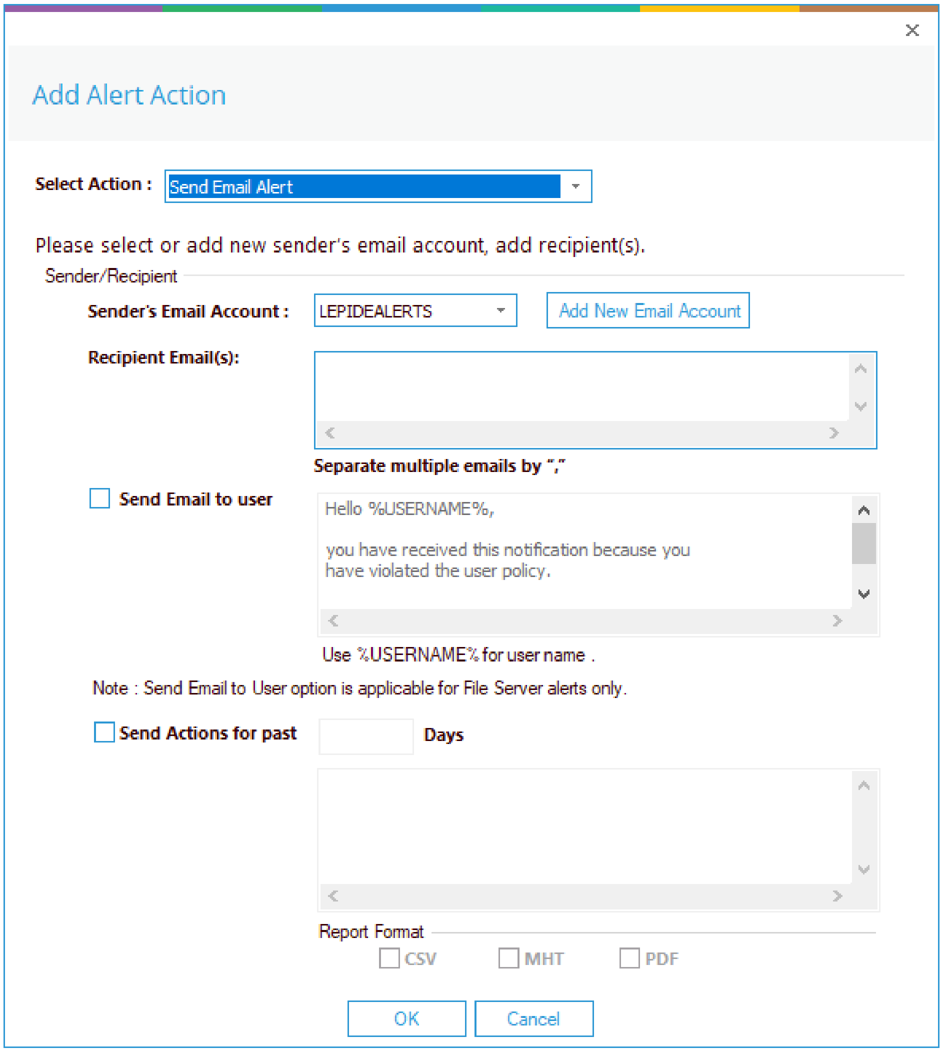

Figure 8: Add Alert Action – Send Email Alert

This option allows you to send an email once an alert has been triggered. The elements of the dialog box are as follows:

Sender's Email Account: The Sender's email account will be displayed here if it has been selected. Click **Add New Email Account** to enter a new Sender's Email Account

Recipient Email(s): Add recipient emails by typing the email addresses into the box. If there are multiple email addresses. separate them with a ','

Send Email to user: Check this box to send an email to the user. The content of the email can be typed into the text box. To include the username within the content, use the

	variable %USERNAME%. **Note** that this option is only applicable to File Server alerts.
Send Actions for past xx days:	This option allows you to see everything that this user has done over the last number of specified days. For example, if an alert is triggered because they have been copying files, then you may want to see what else they have been doing. Check this box and specify the number of days and an email will be sent with an attachment listing everything that the user has done over the specified number of days. The attachment will contain a report and the format(s) can be specified by checking the relevant box. The formats are CSV, MHT and PDF.

- Click **OK** to return to the **Select Response** dialog box

2. Show in LiveFeed

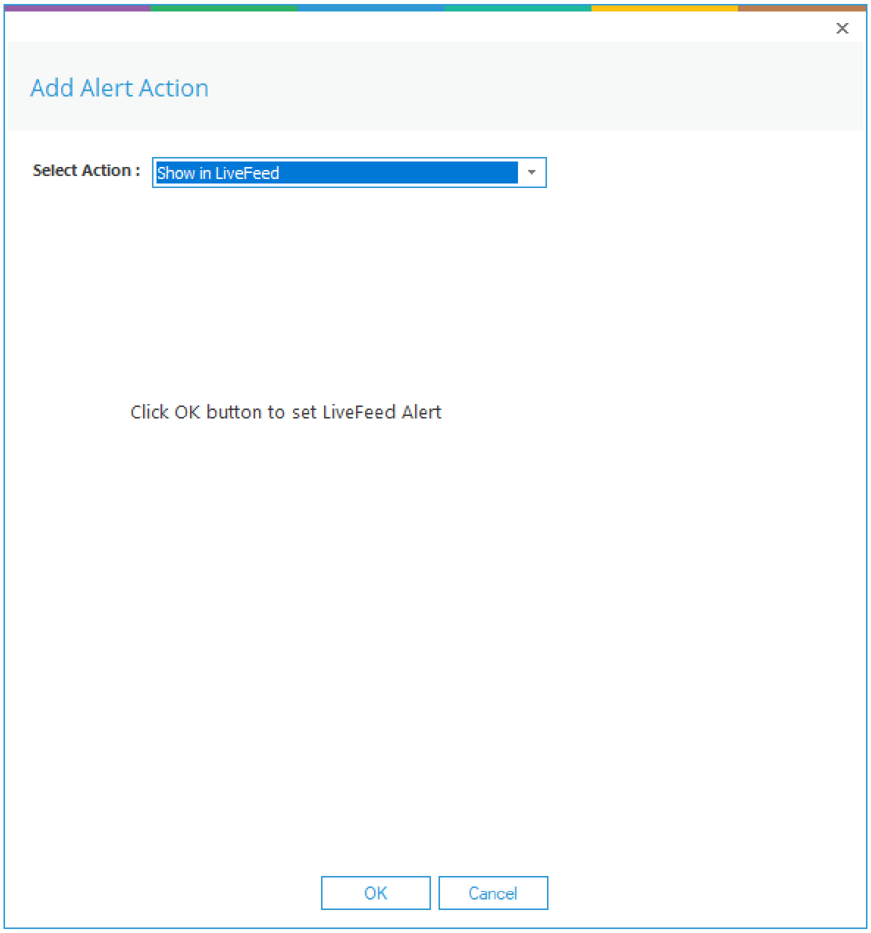

Figure 9: Add Alert Action – Show in LiveFeed

Show in LiveFeed means that the alert will be sent to the Lepide dashboard.

- Click **OK** to switch the **LiveFeed** alert on and return to the **Select Response** dialog box

3. Send Alert to App

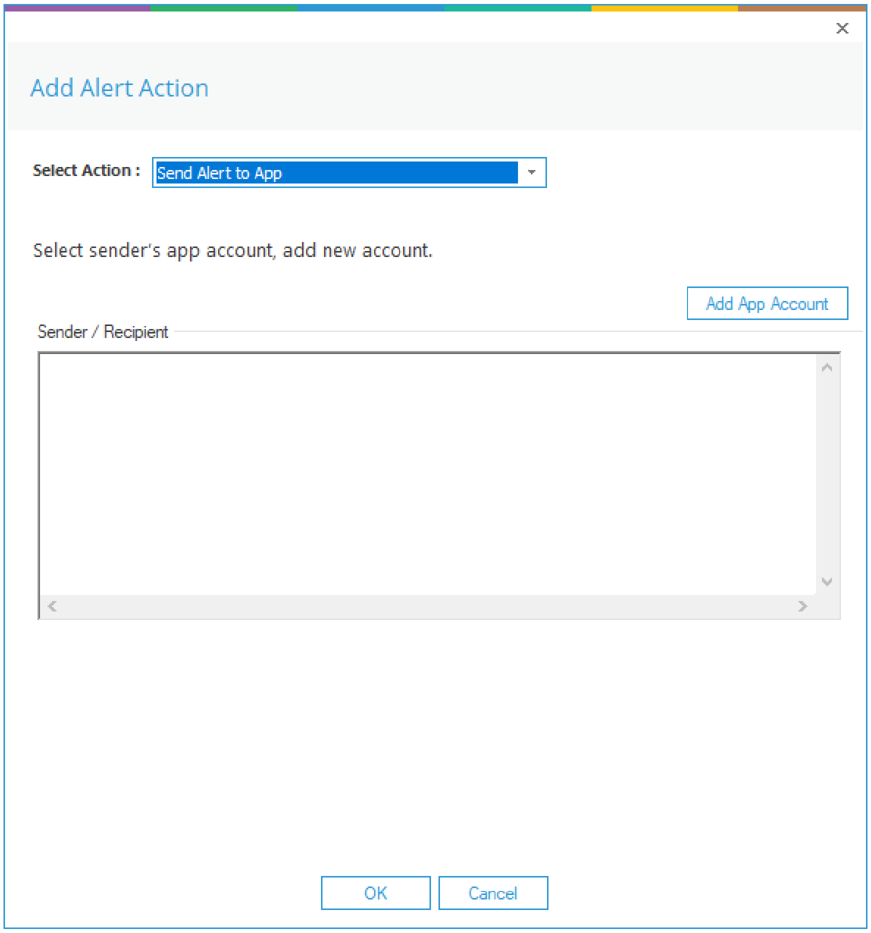

Figure 10: Add Alert Action – Send Alert to App

The **Send Alert to App** option sends the alert to a mobile device.

- Click **Add App Account** to add a new mobile account. The following dialog box is displayed:

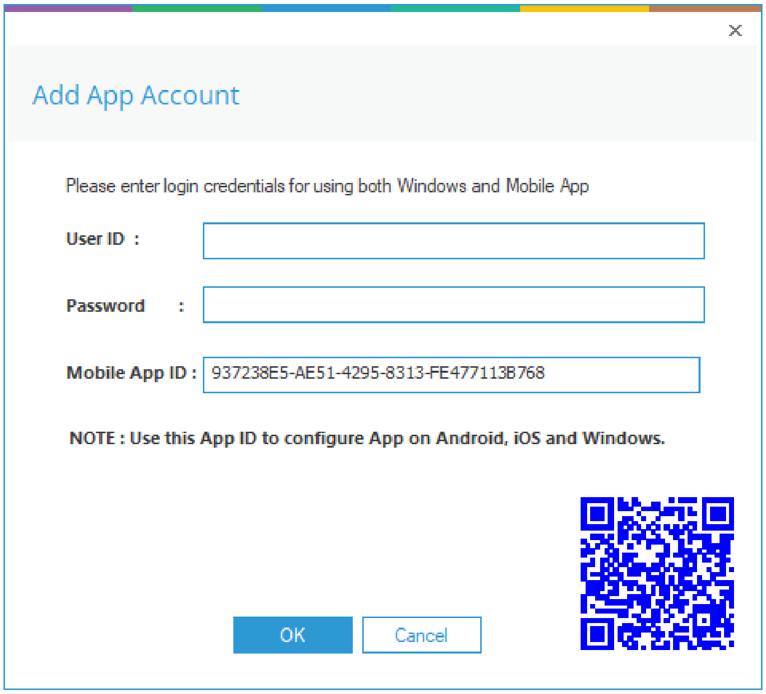

Figure 11: Add App Account

- Enter the **User ID** and **Password**
- Enter the **Mobile App ID** which is generated by using the mobile device to scan the QR code displayed at the bottom of the dialog box.
- Click **OK** to return to the **Select Response** dialog box

4. Execute Script

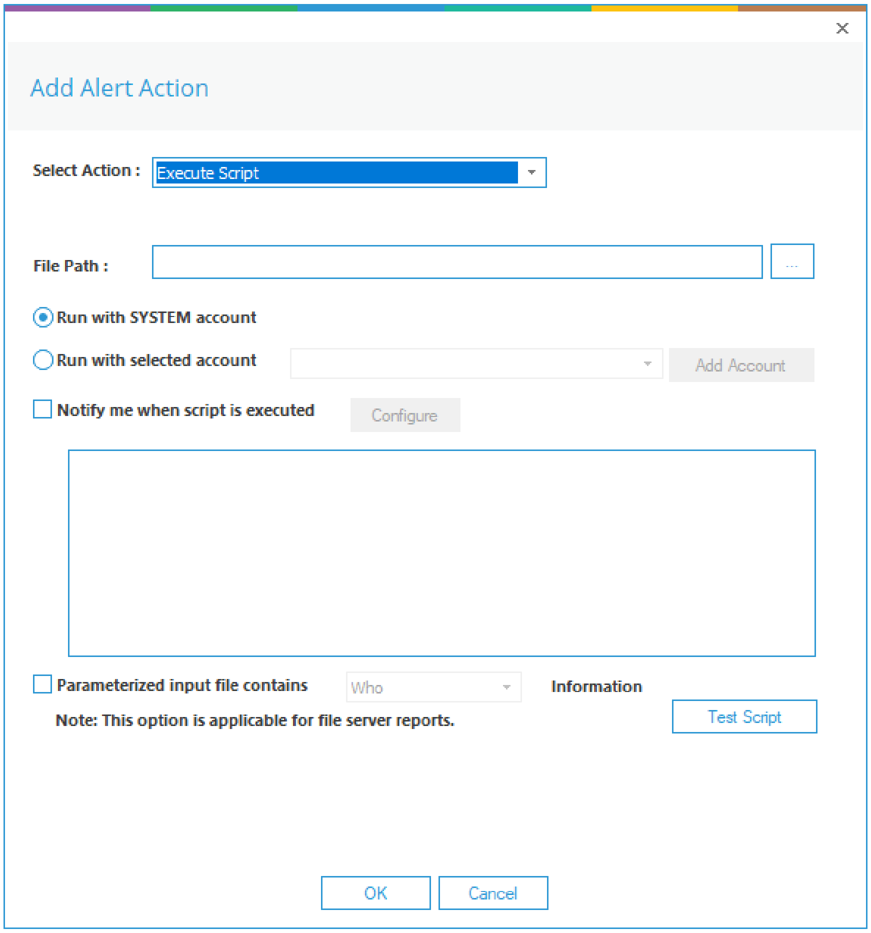

Figure 12: Add Alert Action – Execute Script

The last action from the drop-down menu is **Execute Script**

This sets up the option to execute one of the predefined PowerShell scripts when an alert is triggered.

The elements of the dialog box are as follows:

File Path: Browse to choose the file path of the PowerShell script by clicking ...

Choose either **Run with SYSTEM account** or

Run with selected account.

If you choose **Run with selected account**, you can use the drop-down to select the account or click **Add Account** to specify the account to be used.

Choose **Notify me when a script is executed** to send an email on script execution.

When this option is checked, the **Configure** button becomes available. Choose **Configure** to set up the sender's account and recipient's email address.

Choose **Parameterized input file contains** to specify a variable to include in the script. When this option is checked, a drop-down menu becomes available to choose a variable:

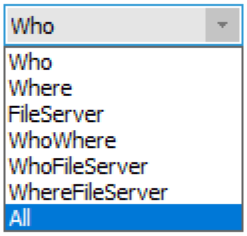

Figure 13: List of Variables

- Click **Test Script** to test that the specified script runs with no errors.
- Click **OK** to return to the **Select Response** dialog box.
- Click **Next**

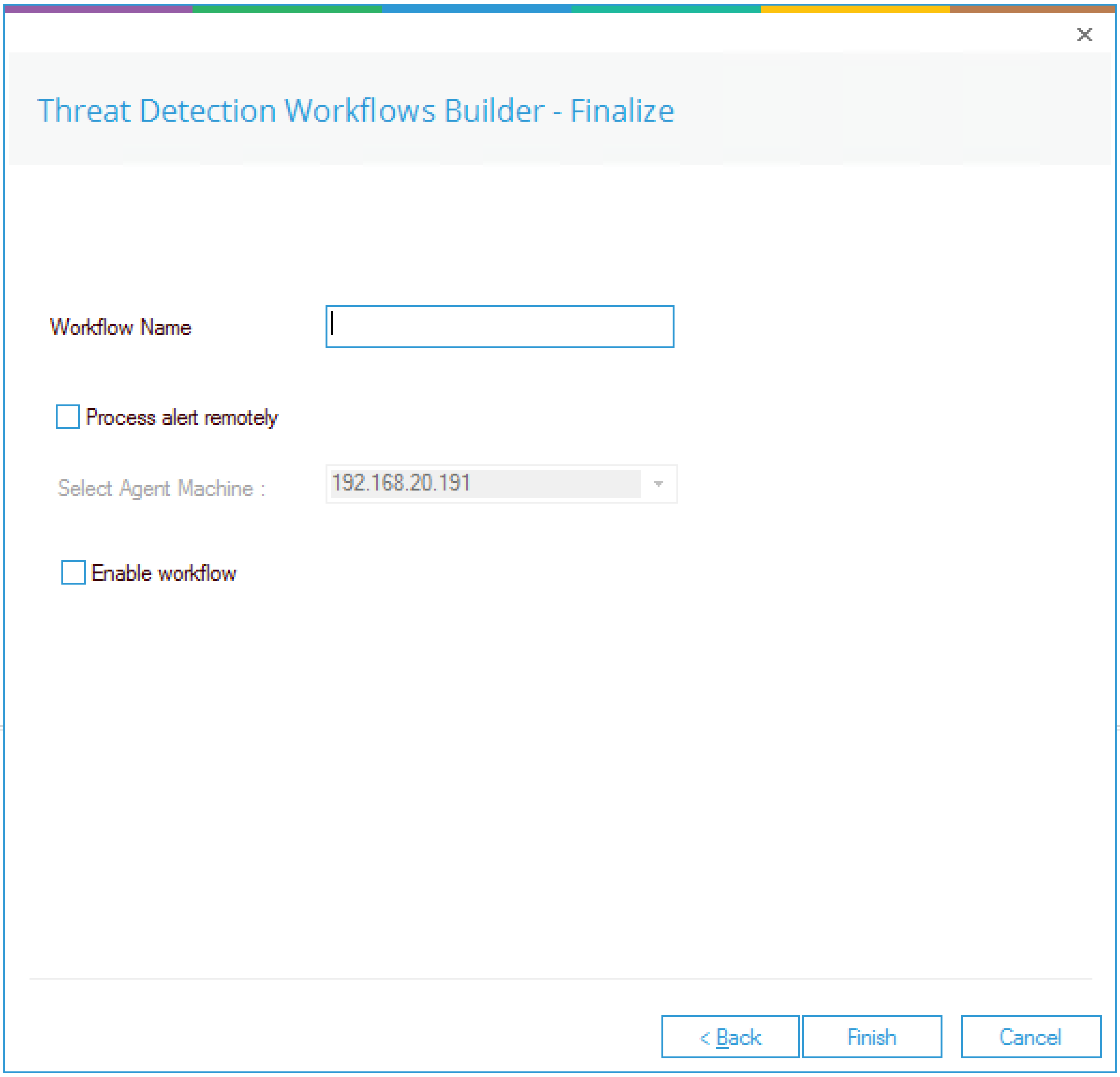

Figure 14: Finalize

- Add a **Workflow Name**
- Select whether to process the alert remotely
- Selecting this option will then allow you **to Select Agent Machine**
- Check the **Enable workflow** box to set the workflow to run
- Click **Finish**

4 To Modify a Threat Detection Workflow

- Click the icon to display the Threat Models screen
- Click on the Tab at the top of the screen called **Threat Detection Workflows**

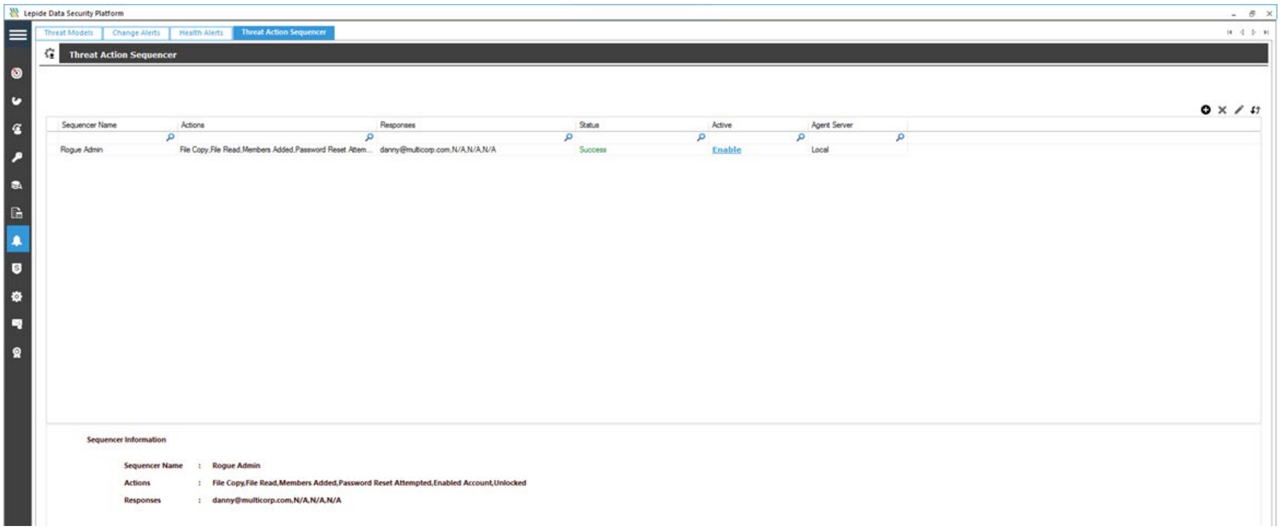

Figure 15: Threat Detection Workflows Screen

- Select the Workflow you want to modify
- Click the icon

The Wizard will start and display the Select Actions dialog box:

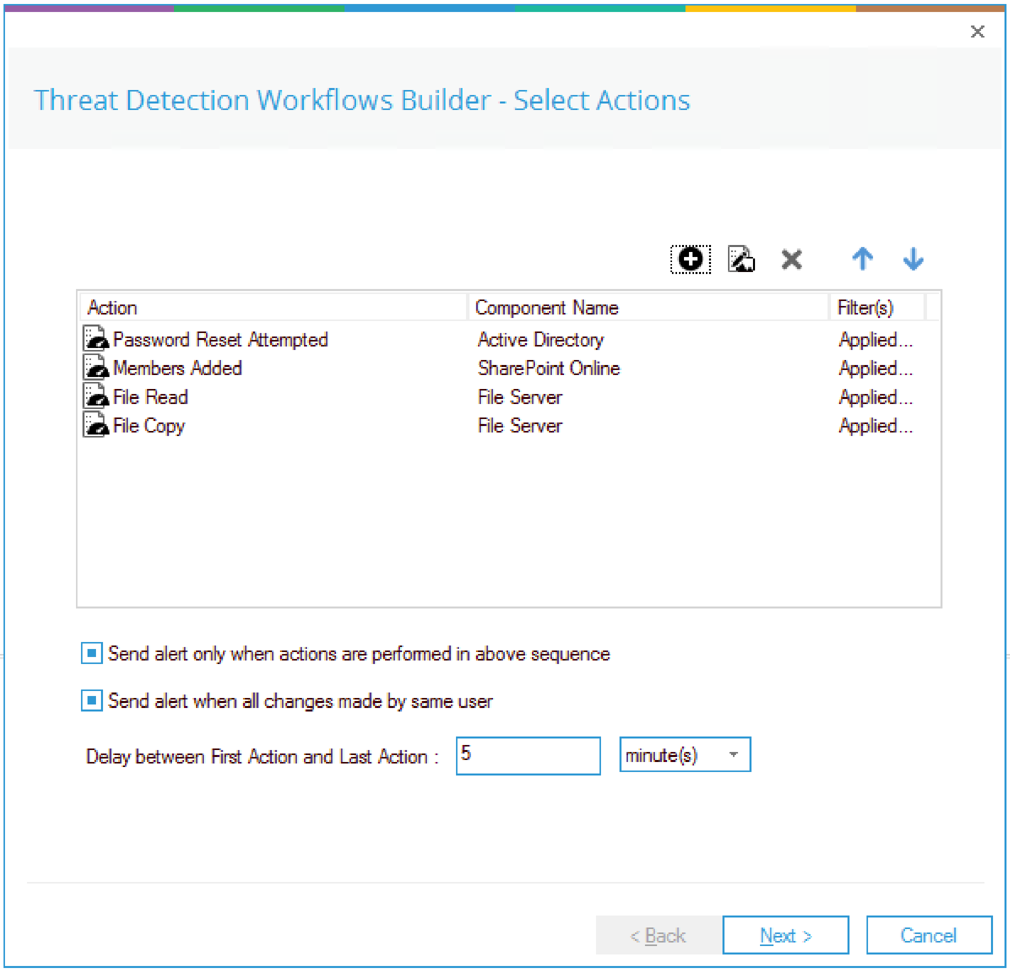

Figure 16: Select Actions

- From here you can:

  - Add a new action
  - Filter a selected action
  - Remove an action
  - Change the order of the actions

- Further options in the Select Actions dialog box are:
  - **Send alert only when actions are performed in above sequence** – this means that the alert will only be triggered if the actions are carried out in exactly the sequence specified. If this option is left unchecked, the alert will be triggered if all the actions are carried out but in **any** sequence
  - **Send alert when all changes made by same user** – the alert will only be triggered if all actions are carried out by one user. If left unchecked, the alert will be triggered when the actions are carried out by any combination of users
  - **Delay between First Action and Last Action -** this sets a time frame for when the actions are carried out. In this example, 5 minutes is specified so here all the actions would have to be carried out within 5 minutes for the alert to be triggered.
- Click **Next**

The Select Responses dialog box is displayed:

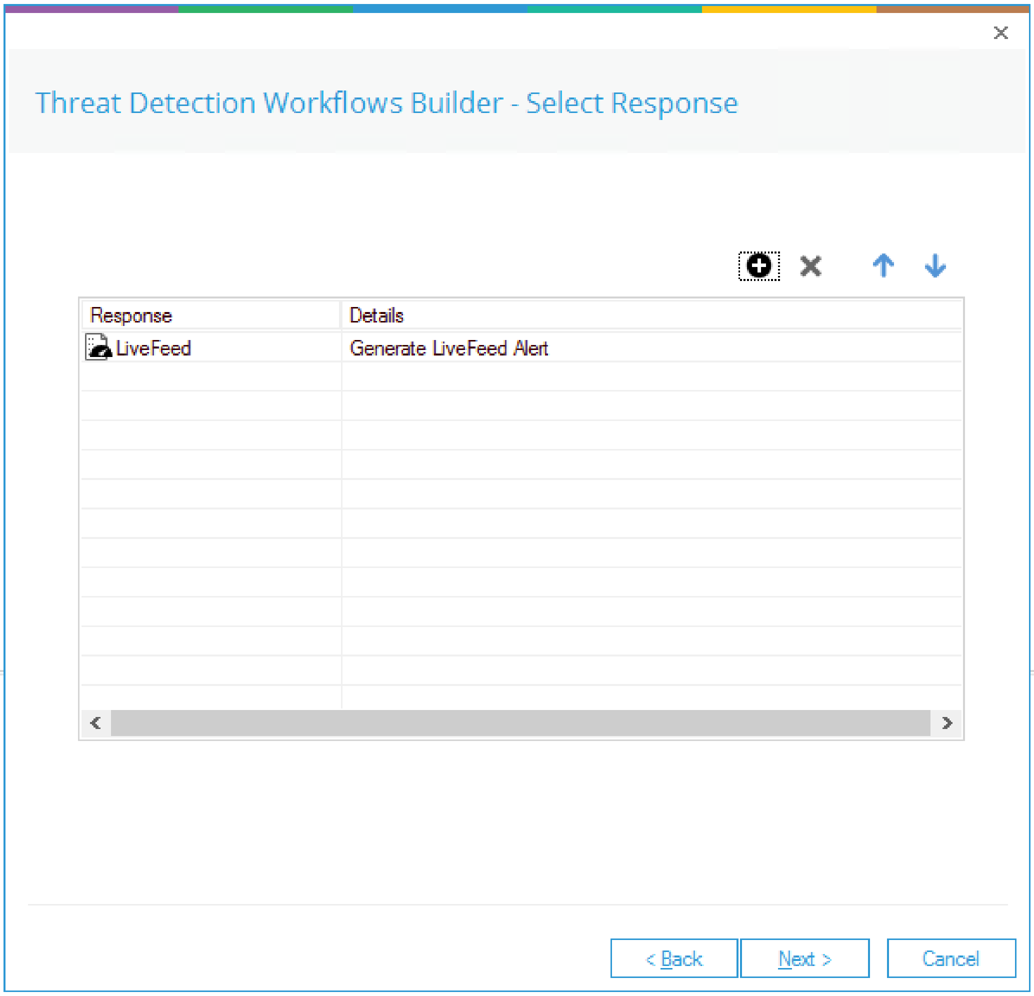

Figure 18: Select Response

- From here you can:

  - Add a new response
  - Remove a response
  - Change the order of the responses

- Click **Next**
- The Finalize dialog box is displayed:

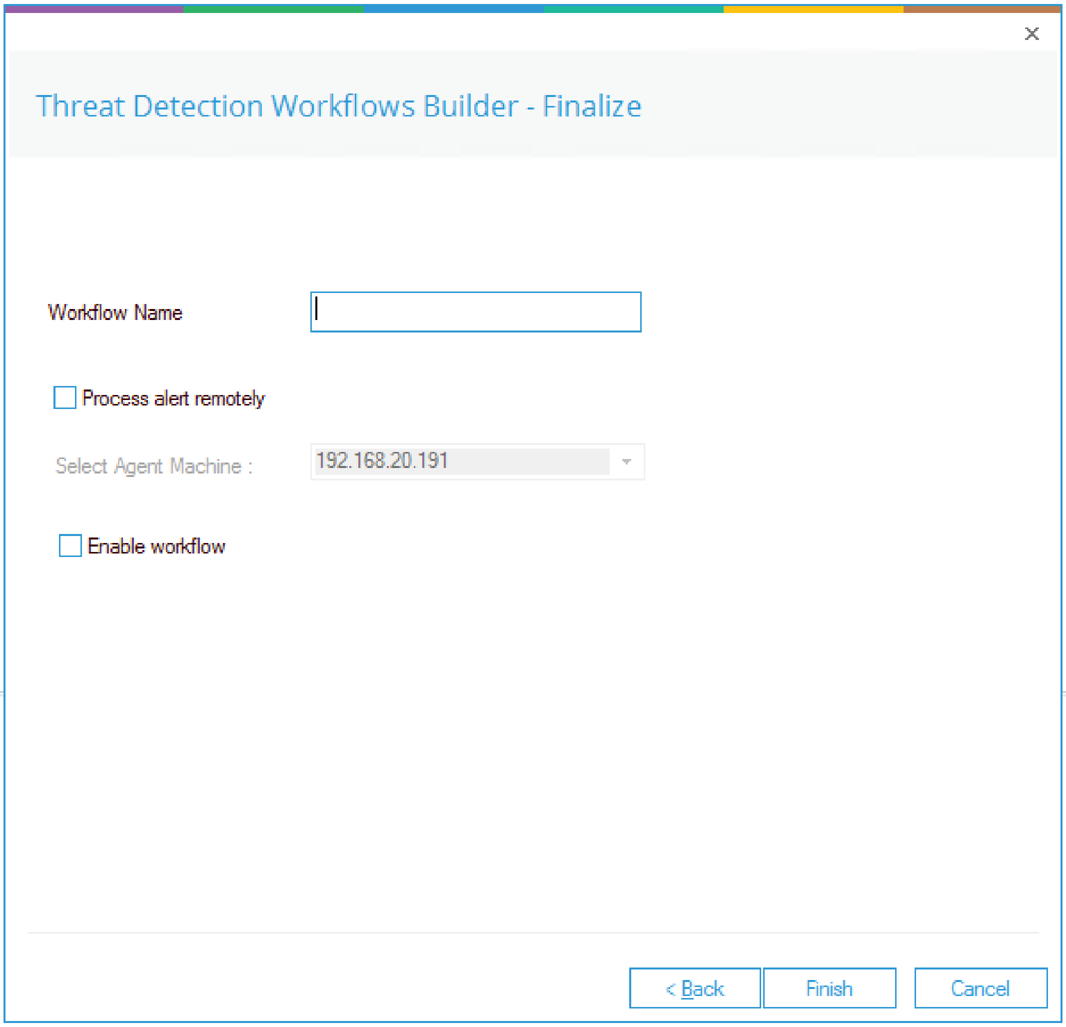

Figure 19: Finalize

- Click **Finish**

5 Support

If you are facing any issues whilst installing, configuring, or using the solution, you can connect with our team using the below contact information.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

6 Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.