Lepide Data

SIEM Integration
Table of Contents

1. Introduction......................................................................................................................................................... 2
2. Purpose of this Document........................................................................................................................................ 2
3. How to Configure SIEM solution to be used with Lepide Data Security Platform.............................................. 2
4. Configuring Lepide Data Security Platform to be used with SIEM application................................................. 5
5. Support...................................................................................................................................................................... 9
6. Trademarks .............................................................................................................................................................. 9

1. Introduction

Welcome to the SIEM document of Lepide Data Security Platform.
Maximize your ROI by integrating Lepide Data Security Platform with your existing SIEM solution and giving real, actionable context to data.

2. Purpose of this Document

The purpose of this document is to make you familiar with the SIEM integration module of Lepide Data Security Platform.

3. How to Configure SIEM solution to be used with Lepide Data Security Platform

We need to configure the port inside the SIEM solution, to be used by Lepide Data Security Platform for communication. Given below is the guide for configuring SPLUNK, the settings may vary from solution to solution.

1. Login to Splunk and go to Settings and click to Data Inputs.
2. Click on TCP to configure the Port for incoming data, e.g. Syslog

3. Click on New Local TCP.
4. Please assign the port which is free for the application.

5. In the Input Settings, please select “Operating System” and “Syslog” further as the “Source Type”. Select DNS as host and click on Review.
4. Configuring Lepide Data Security Platform to be used with SIEM application

Please follow these steps to configure LA to be used with SIEM application:

1. Click on the “Plus” sign on the right corner to add the SIEM Profile. Fill in the details and click OK.
2. Configure the alert feed from the next window.

3. Select the reports for which you want to send the alerts.
4. Configure the alerts and apply the required filters.

5. As soon as the alert is sent, the column “Alert Sent to SIEM” will update with the relevant time stamp. If the connection is broken, it will be shown as “Unsuccessful”.
6. You can enable or disable the SIEM account at any time by clicking the Status field.

7. You can remove the account by clicking on the cross icon.
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 [http://www.lepide.com/contactus.html](http://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 [http://www.lepide.com/Lepide Data Security Platform/](http://www.lepide.com/Lepide Data Security Platform/).

6. Trademarks

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.