Red Flags Report

What's a Red Flags Report?

Lighthouse prepares these reports for recently departed or onboarded employees. At a glance, our Red Flags reporting will tell you of the risk associated with that employee – did they take any data from your network when they departed or did they bring any from their last employer?

Lighthouse offers flat-rate pricing on this service for consistent, predictable results. This means that challenging or voluminous data won't drive up your bill.

What triggers a Red Flag Report?

You should consult with counsel on this, but many of our clients will run these reports on specific attributes of employees coming or going from their company. Often, they will run reports on:

- certain employee ranks and above; e.g. Senior Vice President and higher;

- employees with access to particularly sensitive information, like programmers, sales managers, or executives; and

- employees coming or going under particularly contentious terms.

What's in a Red Flags Report?

1. **Summary of General Findings -** This is often just a few bullet points on things that we found that stood out. For example, highlighting a custodian that purged their trash and deleted their Dropbox folder days before their departure, or if there were any suspicious external devices that were connected to the computer.

2. **Recommended Next Steps -** Are any recommendations that we have for you based on what we saw in the data. We might encourage you to ask certain departments for more information, ask the custodian questions, or pursue other data sources.

3. **Collection of Attachments -** Often times, the red flag analysis report will also come with a number of attachments. For example, a list of files that were stored in cloud storage (e.g. a personal Dropbox account), a list of files that were deleted and where those files were located in the machine, or a list of recent documents there were accessed. Additionally, this could include highlights and comments by the investigator. A common example is a recently accessed client-specific sales deck that is located on the user's personal Dropbox account.

4. **Specific Analysis Categories with Risk Ratings -** This is conducted by the forensics investigator who goes through a number of different risk categories and gives it a risk score between 1 and 10 (10 showing evidence of high risk and 1 showing no evidence of risk). For example, for Google search history, there is no risk if there were no suspicious searches done. It would be high risk if there are searches like "how do I permanently delete emails?"Below are the specific categories we cover:

   - Usage Period
   - Google Search History
   - Internet Browsing History
   - Large Files on Disk

LIGHTHOUSE

- Cloud Storage Exfiltration
- Email Exfiltration
- Removable Device Exfiltration
- Application Usage
- Deletion Activity

What comes after a Red Flag Report?

Based on the needs of your investigation or what we find in the Red Flags analysis, there could be more angles to explore beyond what's in our basic reporting. We'll make recommendations on specifically what items you might want us to explore further or you can consult with us based on your needs.

To discucss these options further, connect with us today!

Sample of Red Flags Report

Contact us for more information about Lighthouse's Red Flags Reports.

(206) 223–9690 | lighthouseglobal.com | info@lighthouseglobal.com

LIGHTHOUSE