

|  |
| --- |
|  |
| **Log Monitoring Workflow** |
| By: Curtis Crawford |

# tABLE OF CONTENTS

**Title Page1**

Table of Contents2

Workflow Summary3

**Programming & Tools4**

Key Commands & Scripts5

Key Commands & Scripts cont’d6

**Cron Job Schedule7**

Importance, Documenting, Sharing, What To Watch For & Improvements8

References & Citations9



|  |  |
| --- | --- |
|  | Decorative |
| workflow summary |
| **Detailed below is a quick overview of how I would conduct my workflow while being employed as an Access Log Analyst at Turn a New Leaf.**  **Workflow:**   1. **Log Collection**: Collect network logs daily to monitor logins. 2. **Log Analysis**: Analyze logs to detect failed logins. 3. **Threshold Check**: Compare the number of failed logins against a threshold. 4. **Alert Generation**: If the threshold is exceeded, generate an alert. 5. **Documentation**: Log the analysis results and alerts. 6. **Weekly Report**: Create a weekly report of logs, analysis, and alerts to send to the manager.   **Frequency:**   * **Daily**: Log collection and analysis. * **Weekly**: Reporting to the manager. |

|  |  |
| --- | --- |
|  | Decorative |
| programming & tools |
| Scripting **Python** would be used for scripting, testing, and writing code for automation. Log Analysis **Regex** would be used for log parsing and analysis, alongside a Python Data Analysis Library known as **Pandas**.   Automated emails &Cron Jobs For scheduling scripts that will run at specific times, **Cron Jobs** is the obvious choice. To have logs and alerts sent directly to my work email and that of my boss, **SMTPLib** would be used. |
| A person standing in front of a brick wall with notes |
| Figure 1 |

|  |  |  |
| --- | --- | --- |
|  |  | Decorative |
| Bar graph with upward trendList Group brainstorm |  | key commands & Scripts |
| log collectionlog analysis    thresholds & alerts  documentation |

|  |  |
| --- | --- |
| Importance,  Documenting,  Sharing,  What to watch for,  &  Improvements | Decorative |
| cron Job schedule |
| **Cron Job Scheduling:**  • Daily log collection and analysis: shell  0 0 \* \* \* /usr/bin/python3 /path/to/log\_collection\_script.py  • Weekly report generation: shell  0 0 \* \* MON /usr/bin/python3 /path/to/weekly\_report\_script.py   1. Daily Logs: Collection of daily log files. 2. Analysis Results: Count of failed login attempts. 3. Alerts: Emails sent to the manager when failed login attempts exceed the threshold. 4. Weekly Report: A compiled report of the week's log analysis results.   A Beginner's Guide To Cron Jobs  **Importance**  • Ensures network security by monitoring unusual activity.  • Provides timely alerts to address potential security breaches.  • Keeps a record of network activity for future reference.  **Documentation**  • Log Analysis Results: Store results in a CSV file (log\_analysis\_results.csv).  • Weekly Reports: Generate and email a CSV report (weekly\_report.csv) to the manager.  • Alert Logs: Maintain a log of all alerts sent, including timestamp and reason.  **Sharing with Manager**  • Daily alerts via email when thresholds are exceeded.  • Weekly summary reports emailed every Monday.  **Unusual Behaviour**  Flags:  • Number of failed login attempts exceeding the threshold (e.g., 100 attempts).  • Sudden spikes or patterns in failed login attempts.  • Multiple failed logins from the same IP address.  **Potential Iterations**  • Enhanced Analysis: Apply machine learning for detecting patterns.  • Real-Time Monitoring: Shift from daily to real-time analysis of logs.  • Visualization: Designing dashboards that can visualize log data in real-time.  • Integration: Connecting to SIEM (Security Information and Event Management) systems for a complete security watch. |

|  |
| --- |
| Decorative |
| REFERENCES & CITATIONS **How to Import RegEx in Python –**  <https://www.freecodecamp.org/news/how-to-import-a-regular-expression-in-python/#:~:text=Python%20provides%20the%20re%20module,the%20import%20keyword%3A%20import%20re>  **Python for Data Analysis -**  <https://www.reddit.com/r/learnpython/comments/12b848s/python_for_data_analysis/>  **Pandas –**  <https://pandas.pydata.org>  **How to send emails in Python –**  https://www.youtube.com/watch?v=S465v4mWsRg  **Sending email with smtplib library with Python –**  <https://stackoverflow.com/questions/67953000/sending-email-with-smtplib-library-with-python>  **The Log Analysis Process –**  <https://www.exabeam.com/explainers/log-management/what-is-log-analysis-process-techniques-and-best-practices/>  **Coding Assistance w/ ChatGPT –**  <https://chatgpt.com>  **Crontab Generator**  https://crontab-generator.org |