**Report**

# Log Monitoring Workflow

Student: Ismail Yasin

**Date 28.01.2024**

**Lighthouse Labs**

**Table of Contents**

Workflow……………………………………………………………………………………………………………………………………………………………………..……… Page 3  
Programming… .….Page 3  
Expected Output… .….Page 5  
Documentation… ….Page 5  
Unusual Behavior… ….Page 5  
Potential Iterations… ….Page 5  
References… ….Page 6

**Workflow:**

A cyber security workflow, the established process for managing security events within an organization, involves identifying potential threats, assessing their potential impact, implementing preventive measures, and monitoring their effectiveness. Clear documentation and communication are essential for ensuring consensus among all stakeholders.

This workflow, tailored for Turn a New Leaf, a medium-sized non-profit organization supporting youth, emphasizes monitoring Windows and Linux machines on Thursdays when the system is highly active and vulnerable. Members must log in every Thursday to confirm or update their employment status. The primary focus is on identifying unusual network traffic or signs of an attack. The initial step is defining the system scope, including identifying all computers, network components, and users with special privileges. The second step involves selecting and implementing logging and monitoring tools, configuring log sources, and aggregating logs into a centralized repository. Establishing a baseline, using cyber security frameworks like NIST, SANS, and Shared Assessments, follows to recognize normal behavior and detect anomalies.

Creating rules and alerts based on known attack patterns is crucial. Regular reviews based on organizational risk profiles, log reviews, and periodic audits help identify and address security issues promptly. Developing an incident response plan is the next step, outlining actions to take post-incident based on discovered security issues in the logs. In addition to routine audits and compliance inspections, Turn a New Leaf should invest in regular cyber security awareness training for its employees to enhance overall security posture. This comprehensive approach, from monitoring to response planning and ongoing training, strengthens the organization's resilience against potential security threats.

**Programming Part:**

In order to examine unsuccessful login attempts in Linux, one may develop a straightforward shell script that extracts and presents pertinent data from the system records. The following is a rudimentary illustration employing the **grep** and **awk**.

Commands:

**For Window:** In order to examine unsuccessful logon attempts in Windows via PowerShell, one may utilize the Windows Event Log. The PowerShell script that retrieves and analyzes unsuccessful login credentials is shown below.

The Script to a file with a .ps1 extension (e.g., analyze\_failed\_logins.ps1). To run the script, open a PowerShell console, navigate to the script's location, and execute it using .\analyze\_failed\_logins.ps1. The script uses event ID 4625, which corresponds to failed login attempts in the Security log. The properties used to extract the username and IP address may vary based on your system configuration. Adjust the script accordingly if needed.

**Python Scripting:**

**Expected Output:**

Through the utilization of monitoring commands and scripts, the log activity of the New Leaf network for both Windows and Linux PCs should be transformed into a summary that is easily understandable. In order to generate data that includes timestamps, user privileges, and both successful and unsuccessful login attempts, it is recommended that a Python script be utilized. This report is essential for determining whether or not there are any unusual trends that might point to a potential security risk, such as an unexpected increase in the number of unsuccessful tries to login.

**Documentation:-**

The monitoring procedure will utilize both written reports and logs for documentation. Examined information will be systematically recorded in a log file generated by the Python script, ensuring secure storage. Additionally, the manager will receive a weekly email report summarizing any detected anomalous activities or patterns observed during the monitoring process. Beyond serving as a comprehensive record of network activity and aiding in the identification of potential security vulnerabilities, this documentation plays a crucial role in meeting regulatory compliance requirements.

A manager might be alerted to an abnormal surge in unsuccessful login attempts, particularly outside regular business hours. Any noteworthy alterations in user privileges or activity patterns, such as a sudden rise in the updating of employment statuses, could also signify a security event. The following examples outline potential indicators:

* Multiple Failed Login Attempts
* Abnormal Network Traffic
* Irregular Login Times
* Peculiar File Access Patterns
* Unusual User Privilege Changes

**Potential Iteration:-**

The presented workflow encompasses fundamental steps that are universally applicable to various systems, extending beyond the specific context of the Turn a New Leaf organization. An advanced iteration of this workflow could involve refining the scripts to conduct more intricate detections, incorporating machine learning algorithms to discern intricate patterns indicative of potential security threats. This enhancement would enable a more nuanced and proactive approach to identifying and addressing security concerns within the system.

**References:**

*Monitoring failed login attempts on linux*. Network World. (2020). <https://www.networkworld.com/article/969378/monitoring-failed-login-attempts-on-linux.html>

Maruthamuthu, M. (2020). *Bash script to check successful and failed user login attempts on linux*. 2DayGeek. <https://www.2daygeek.com/bash-script-to-check-successful-and-failed-user-login-attempts-on-linux/>

*What is log aggregation and why to use it? - crowdstrike*. crowdstrike.com. (2024). https://www.crowdstrike.com/cybersecurity-101/observability/log-aggregation/

Cobb, M. (2011). *Best practices for audit, log review for IT security investigations: Computer Weekly*. ComputerWeekly.com. <https://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations>.

Written by Rachel (2023). How to establish a cybersecurity baseline that works for your organization. Bitsight. <https://www.bitsight.com/blog/establish-cybersecurity-baseline>

Scripting and PowerShell command

*Chatgpt. ChatGPT. (n.d.). https://chat.openai.com/*