



In this project, you will demonstrate how to apply the programming tools and commands that you have learned about to a professional Cyber Security scenario. You will establish a workflow to monitor for unusual traffic, including the key commands or scripts you will use, expected output, and next steps.

## My Submissions

The status of your previous submissions to this project are displayed here. However, you have not submitted this project.

Submit Project

Description	<a href="#">Eval Rubric</a>
-------------	-----------------------------

## Project Description

In this project, you will select, crate and apply scripting to routine Cyber Security tasks. You will establish a workflow to monitor for unusual traffic, including the key commands or scripts you will use, expected output, and next steps.

## Scenario

### Company Profile

Turn a New Leaf is a medium-sized non-profit organization that supports youth in a range of rural communities to seek employment. In order to support government regulatory requirements, their members must log into the company system every Thursday to confirm or update their employment status, and input any updates on their job searches, including links to job listings they are actively pursuing.

The company uses both Windows & Linux machines, and has two web servers in their network.

### The Request

You work as an Access Log Analyst at Turn a New Leaf. Your manager has asked you to monitor the logs for any unusual network traffic, and send them an alert if there is an unusual number of failed logins. They've asked you to ensure there is documentation of this, and to provide a weekly update by email.

You want to create a workflow for this process, using programming to make it as efficient and low-maintenance as possible.

# Workflow Structure

Your workflow should include the following components:

- **Workflow:** a short description of the steps to be taken to successfully monitor and document the logs in the network. Consider what you will monitor, when, and how often.
- **Programming:** Outline what programming tools you will use to successfully complete the task. Be sure to include key commands and/or scripts that you will use or create.
- **Expected Output:** What are the expected results of the commands or scripts you are planning to use? Why are they important or useful?
- **Documentation:** How will you capture and document the monitoring process? Consider the timing and how you will share it with your manager.
- **Unusual Behaviour:** Identify what elements in your monitoring would constitute a “flag” to alert your manager.
- **Potential Iterations:** What elements of your workflow would you want to improve, and why? Identify some ways you could develop skills to support this improvement.

## Project Learning Outcomes

In completing this project, learners will be able to:

- Select, create and apply scripting to regular Cyber Security tasks
- Develop basic scripts to verify and identify usual and unusual network behaviour
- Organize and filter logs for monitoring purposes

## Submission Guidelines

- Submit a link to a Google doc that contains your report. This report will be evaluated according the evaluation rubric.
- Make sure you change the share settings to the doc to allow and access to all.
- To submit your project, use the *Project Submission* button given at the top and follow the instructions.
- your project should be follow an Executive Summary format



**There is more than one way to approach this problem.**

After you have submitted your workflow, you may also want to share it with your peers on Discord, and take a look at the various approaches your peers used.

## Evaluation Guidelines

- Familiarize yourself with the Eval Rubric tab so you can read about the competencies you will be evaluated on for this particular project, and review what the different levels of each competency require.
- If you receive Unsatisfactory for any competency, your project will be given feedback to implement before it is accepted. Review the feedback provided, make changes to your project, and aim to resubmit your updated project within 48 hours.

**This is not a bad thing; having to resubmit is an opportunity for you to improve and it is common for students to need to implement feedback on their projects before being accepted.**

## Project Requirements

- Executive Summary

- Code should include essential commands with explanatory comments.
- Provide sample output demonstrating the script's execution results.
- Document the monitoring process thoroughly.
- Identify flag elements for manager alerts, linked to Indicators of Compromise (IoCs).
- Utilize both Bash and Python languages.


# Report Format


Organize all the information you gathered into a report and be sure to include the following: \* Table of Contents \* Introduction \* Solutions Section (Where you discuss your script and how it functions) \* Potential iterations Section (where you discuss potential improvements) \* Conclusion \* References

## References

References are crucial for credibility, validating arguments, and avoiding plagiarism. References enable readers to verify information; build on existing knowledge, and uphold ethical standards while promoting transparency. All the resources you access should be listed in a References List at the end of your work.

You may use tools, like [Citation Machine](#), to generate citations for your work.

The widely accepted citation format in the cyber security industry is the APA format. Use this format for all projects in the program. Once you enter the industry, you may follow a different citation style if instructed by your organization.



**Examples:** A guide to digital forensics and cybersecurity tools. Forensics Colleges. (2022, May 19). <https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

Whitman, M., & Mattord, H. (2017). Principles of information security (6th ed.). CENGAGE Learning Custom Publishing.

# Log Monitoring Workflow

Tue Jul 23

Project Details »