Login Chronicles: CyberSecurity Insights of EY 2024 UMD IC

OUR TEAM

Oluwatimilehin Olayinka

Leon Tang

Dale Neumeister

Chris Humbert

MISSION STATEMENT

Our goal was to identify cyber security vulnerabilities by analyzing Ernst & Young's (EY) authentication logs for unusual patterns and risks. The analysis covered data familiarization to in depth reviews of employee actions and security integrity.

Methodology

C++

- Developed data structures for processing login attempt data focusing on frequency analysis and failure detection.
- Used for manipulating data like hash tables, sorting & searching, and finding non employee login attempts.

Excel

- Applied Microsoft Excel for data analysis using pivot tables to gather daily login activities and finding key metrics.
- Generated charts and graphs to visualize trends and distribution of login attempts to show easier interpretation.

ChatGPT

- Used for pattern recognition in data set.
- Creating formulas for excel.

Part 1: Familiarization and Basics of the Data

Day of Week	Attempts per/day
Friday	200,303
Monday	186,711
Saturday	50,520
Sunday	17,543
Thursday	198,295
Tuesday	197,488
Wednesday	197,002
Grand Total	1,047,862

Total # of Logins: 1,047,862

% of Logins Failed: 20% (209,520/1,047,862)

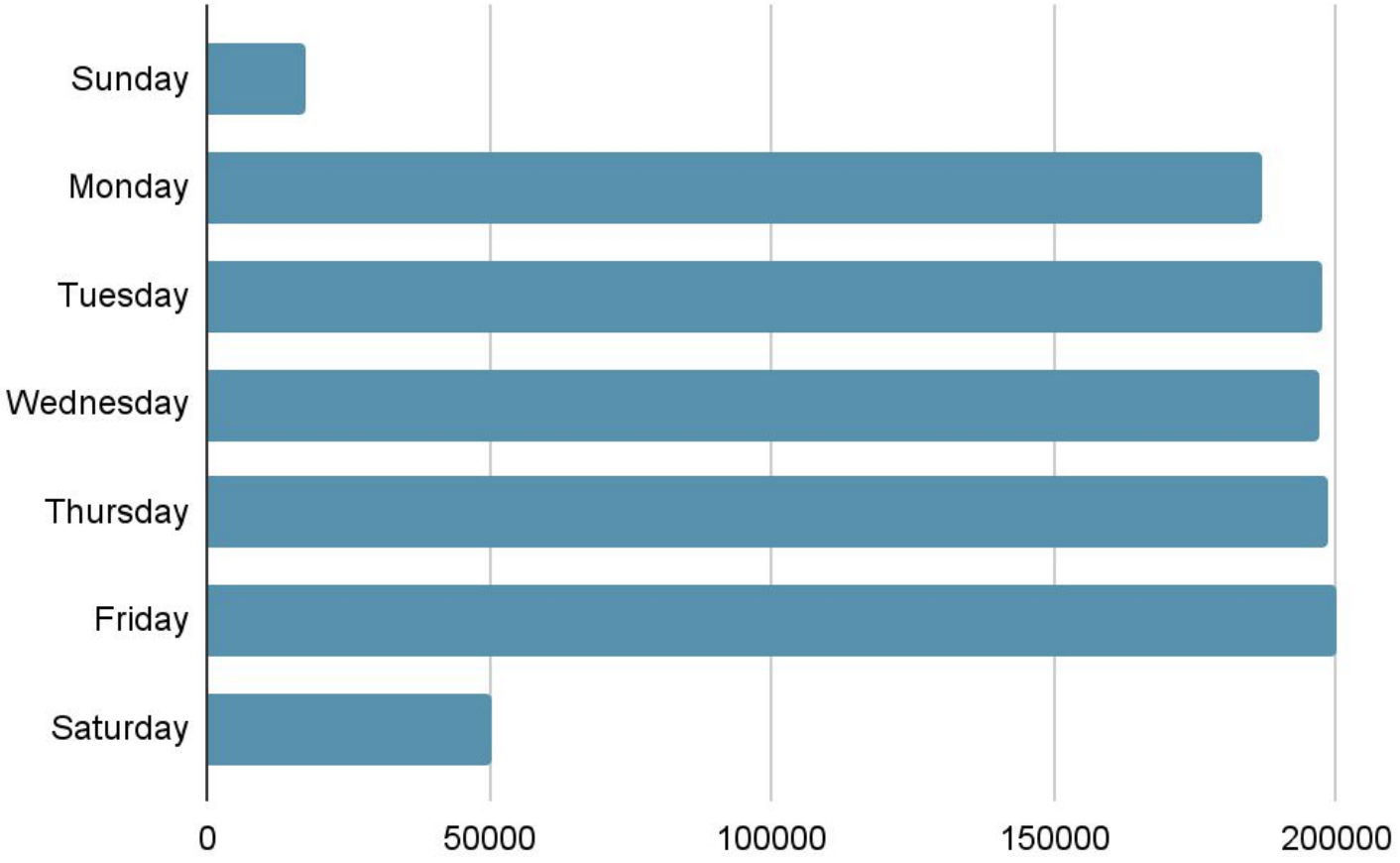
We filtered for login failures on Excel then divided their total by all login attempts to compute the failure rate.

Total # of login attempts per/day: Converted the date to a weekday name with the formula 'TEXT(C2, "dddd") in a new column, then summarize the total login attempts each day of the week by creating a pivot table.

Avg. # daily login attempts per employee: 5987.78

Used pivot table to summarize logins by date and employee then applied the AVERAGE function on the summarized data.

Logins per day



Part 2: Employee Analysis

A. Employee Login Summary

B. Failure Login Rate

C. Post Termination Login

D. Inactive Employee Login

E. Unmatched Login Attempts

Explanation of Part 2

A

Employee Login Summary

Used an excel PivotTable to display records of Username, Full name, Total Successful and Unsuccessful logins, then sorted the data by highest successes.

B

Failure Login

Used another PivotTable with Username, Full name, and Fail Rate (total fails/total attempts), then sorted by highest fail rate.

C

Post Termination Login

In Excel, filtered for employees with a termination date. Found the final date of login for each user with a pivot table. Created function that would write users name if the date they last logged in was greater than their termination date.

D

Inactive Employee Login 45 Days

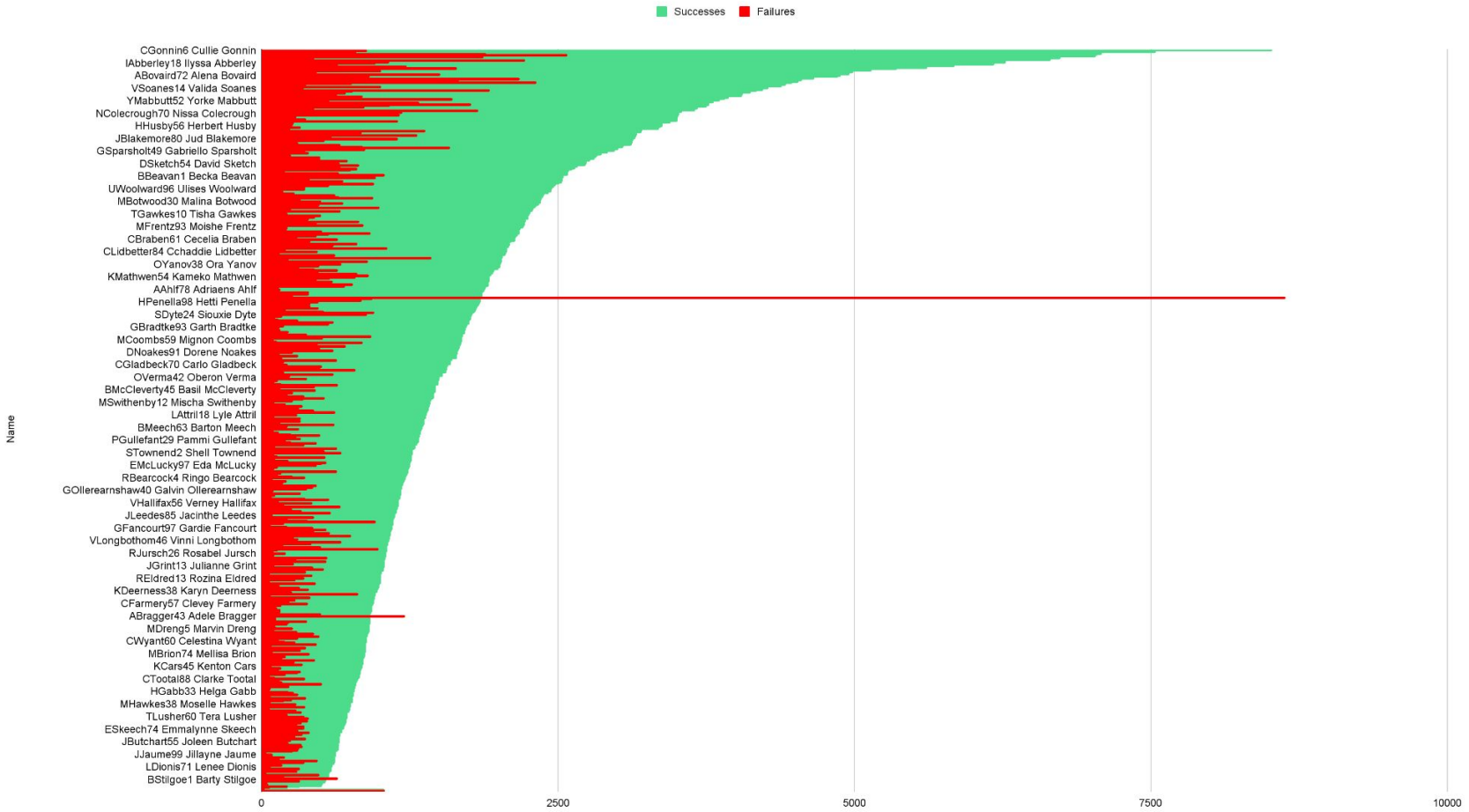
Created pivot table showing users' last login using Excel, filtering for logins prior to 45 days before December 1st.

E

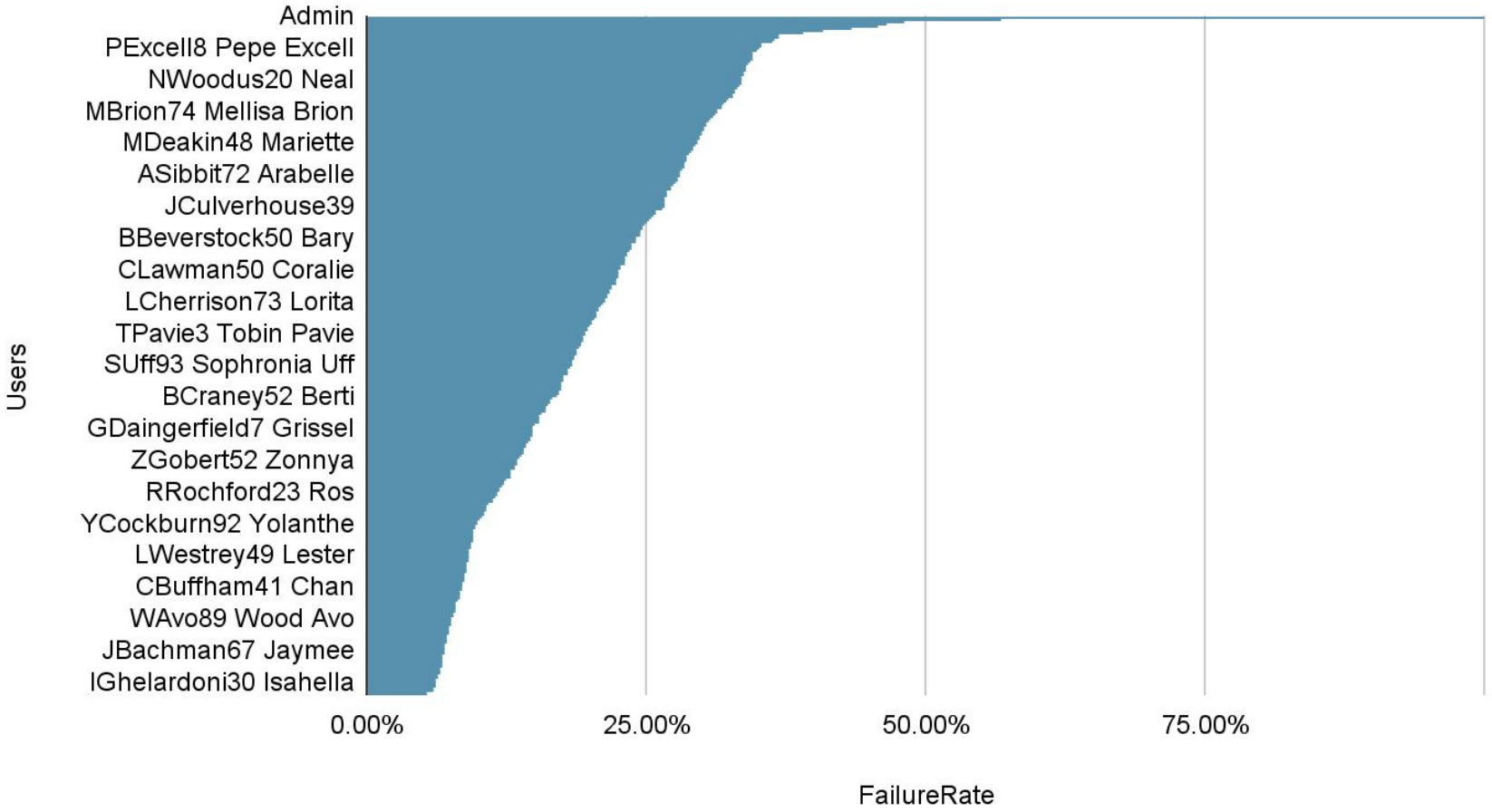
Unmatched Login Attempts

Used a hash table in C++ to determine if a login corresponded with an active employee's username. Ultimately, the list just revealed 'admin' with 1032 attempts

Successes and Failures



FailureRate vs. Users



Post Term Logins

DOlech99: Dennie Olech

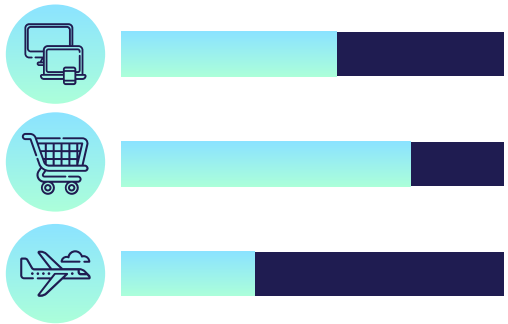
Termination Date: 09/28/22
Last Log Entry: 6109793
Last Login Date: 10/25/22

BAldington1: Bancroft Aldington

Termination Date: 10/4/22
Last Log Entry: 6109808
Last Login Date: 10/25/22

Kmathwen: kameko Mathwen

Termination Date: 09/14/13
Last Log Entry: 6107450
Last Login Date: 10/24/22



Inactive Employees

AFilon70: Audre Filon

Last Log entry:5698767

Last Login Date: 8/16/22

Ejeanneau51: Evyn Jeanneau

Last Log entry:6062451

Last Date: 10/17/22

Unmatched Logins

There were 1032 login attempts from “Admin”. Based on the fact that there was not a single successful login attempt and every attempt was outside of the U.S, we theorized these are from malicious outsiders who assumed there would be an administrator account of said name and attempted to login through said account

Part 3: Data Integrity

Log Entries Missing

439

Missing LogEntry Numbers

https://docs.google.com/document/d/1WMixADjvaTHPhqMfdxE6EGGlWsjS97wMHunWGSO3ndc/edit?usp=sharing

Potential Record Deleter

EJeanneau51
NNemrow20
ALewis1
DLunt07
AFilon70

Explanations of Part 3

Login Entries Missing

Used a loop in C++ to compare each log number with its predecessor, storing the previous number in a variable. If the difference between the current and previous numbers was greater than 1, then a missing log chain was identified. Simultaneously added the difference in past and current log num to a sum of missing log numbers.

Missing LogEntry Numbers

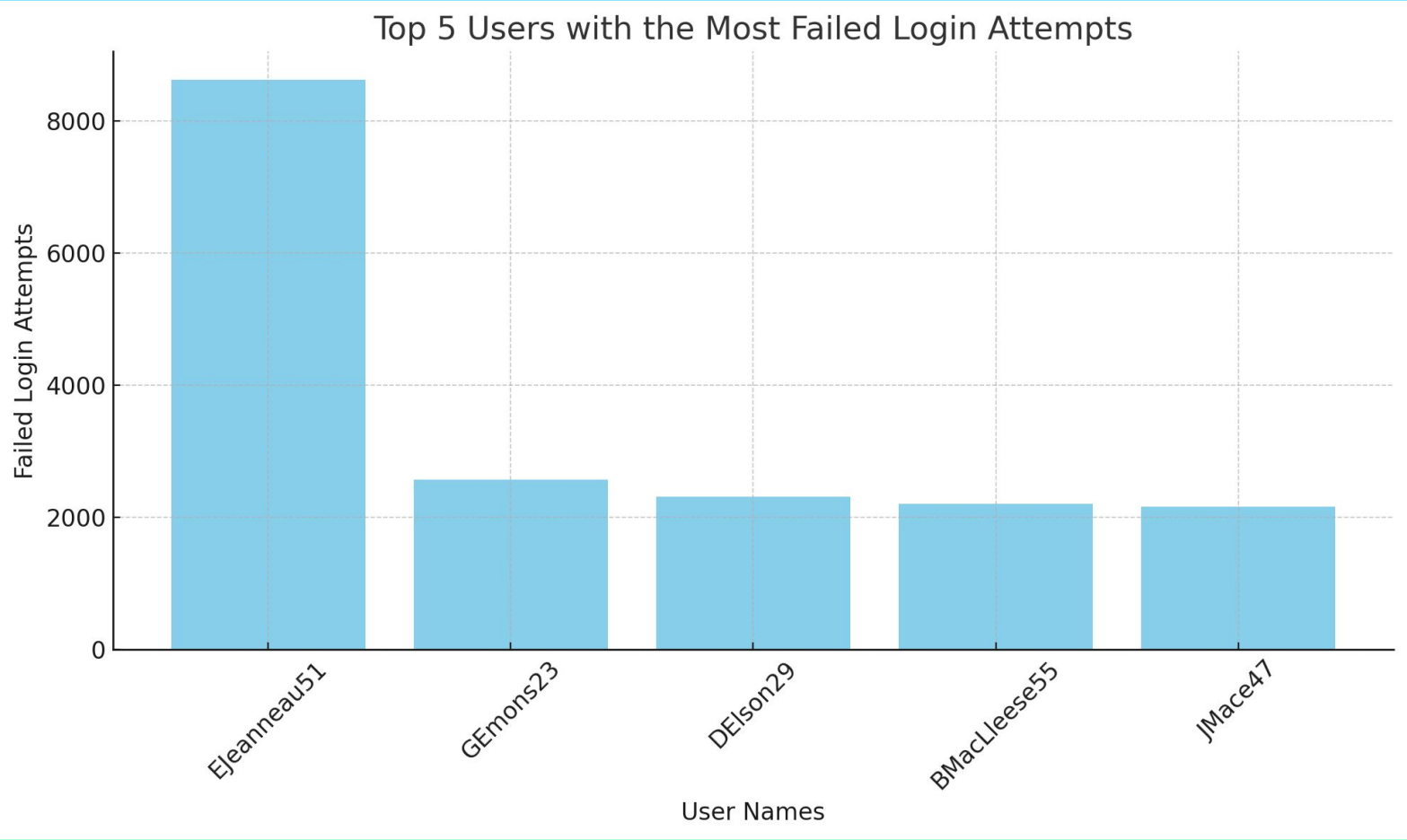
Used a loop in C++ to compare each log number with its predecessor, storing the previous number in a variable. If the difference between the current and previous numbers was greater than 1, then a missing log was identified.

Potential Record Deleter

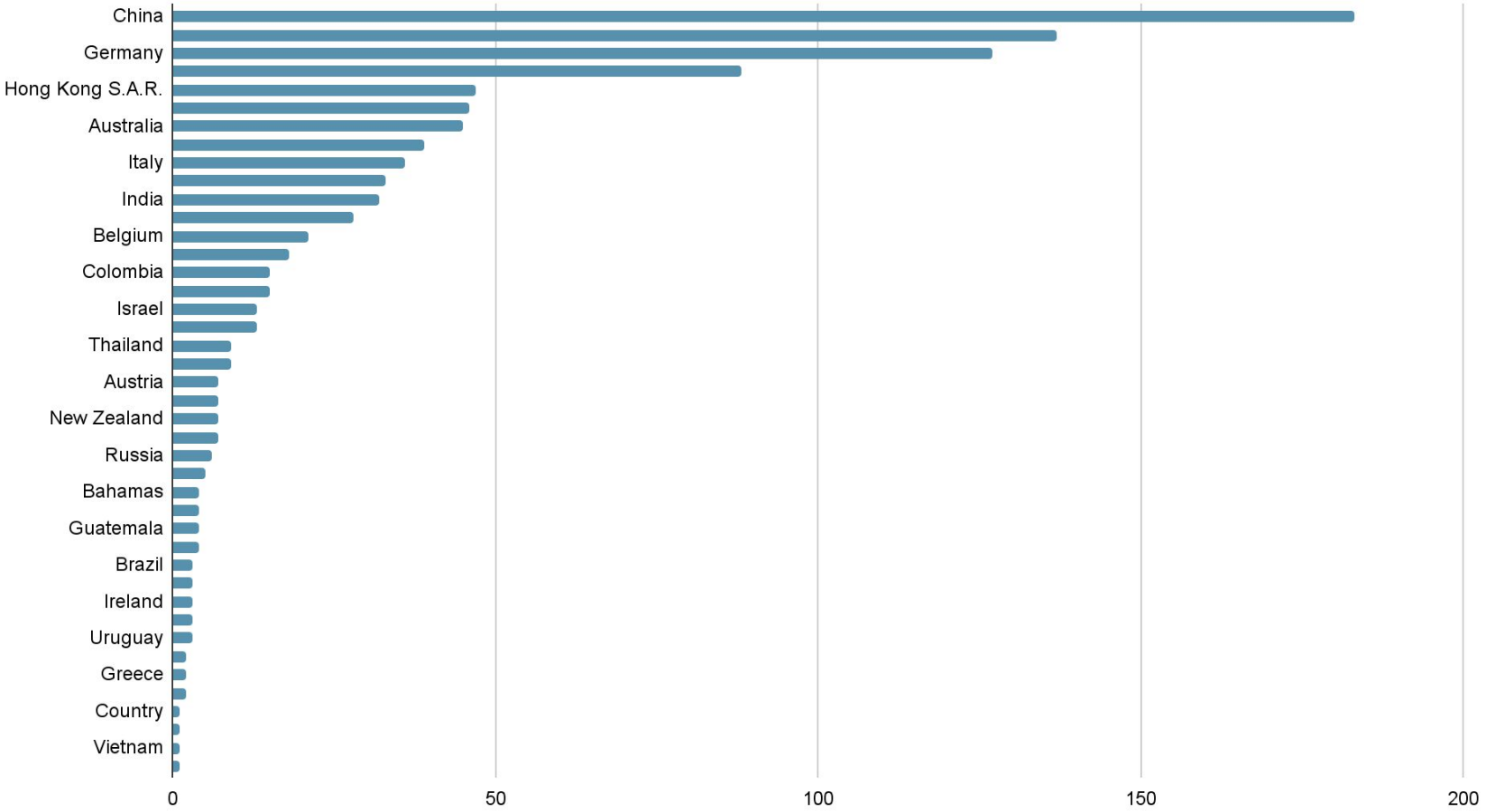
EJeanneau51 had the most failed logins found using Excel.

3 Other users have no start or termination date, and have no login attempts, potentially because all of their attempts were removed

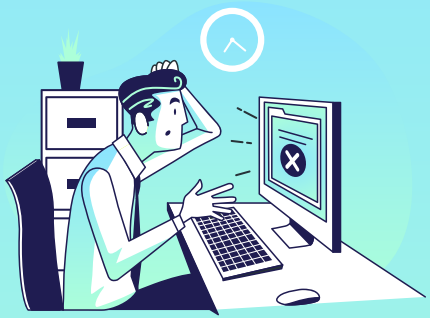
AFilon70 could have deleted the records because the deletions stopped slightly before their inactivity.


Top 5 Users with the Most Failed Login Attempts
Failed Login Attempts
0
2000
4000
6000
8000
EJeanneau51
GEmons23
DElson29
BMacLleese55
JMace47
User Names

Admin Attempts

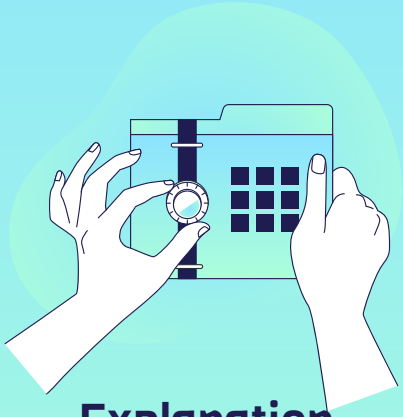


Part 4: Holidays



Logins on Holidays

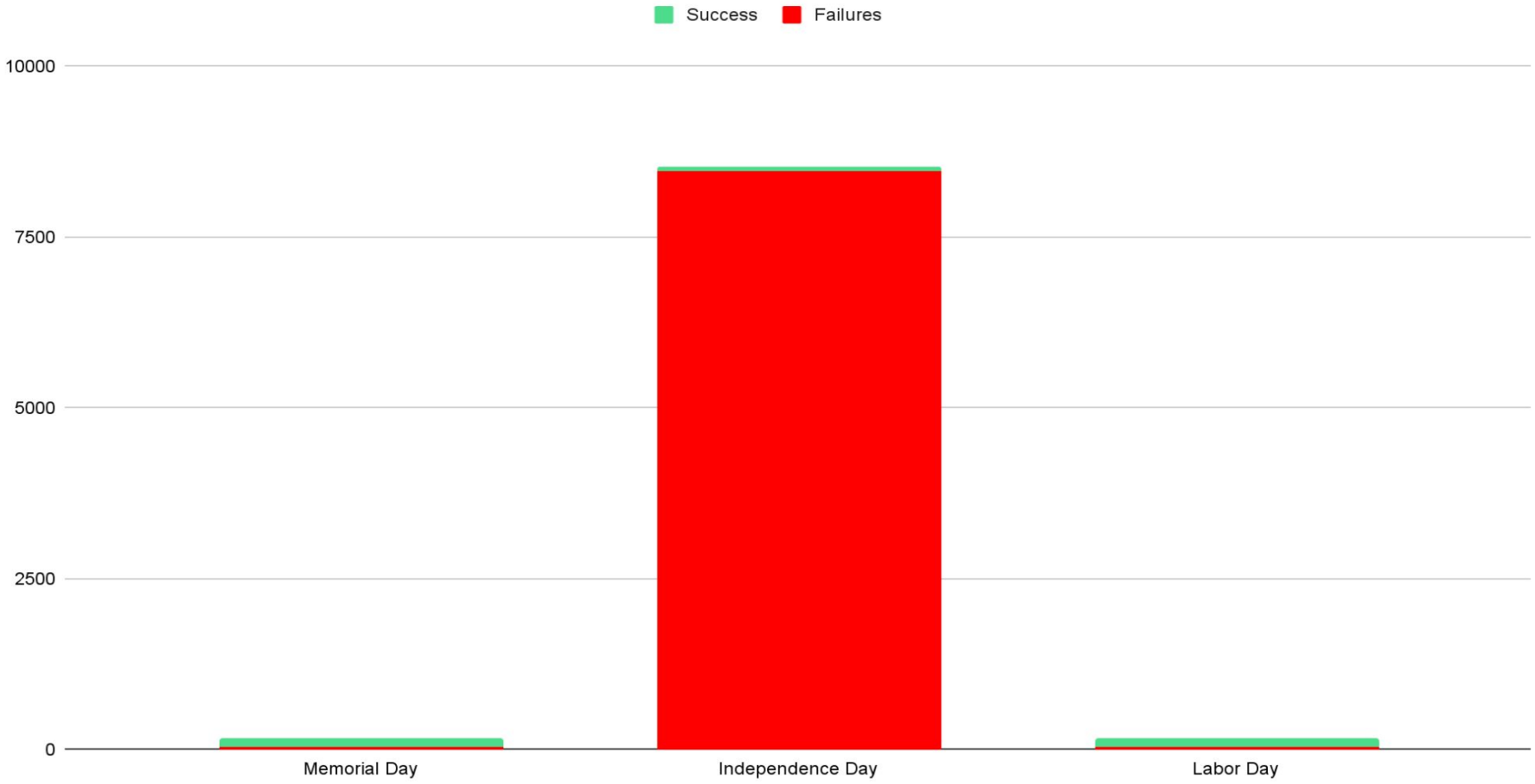
8,445 logins by EJeanneau51 in Pyongyang, North Korea on Independence Day

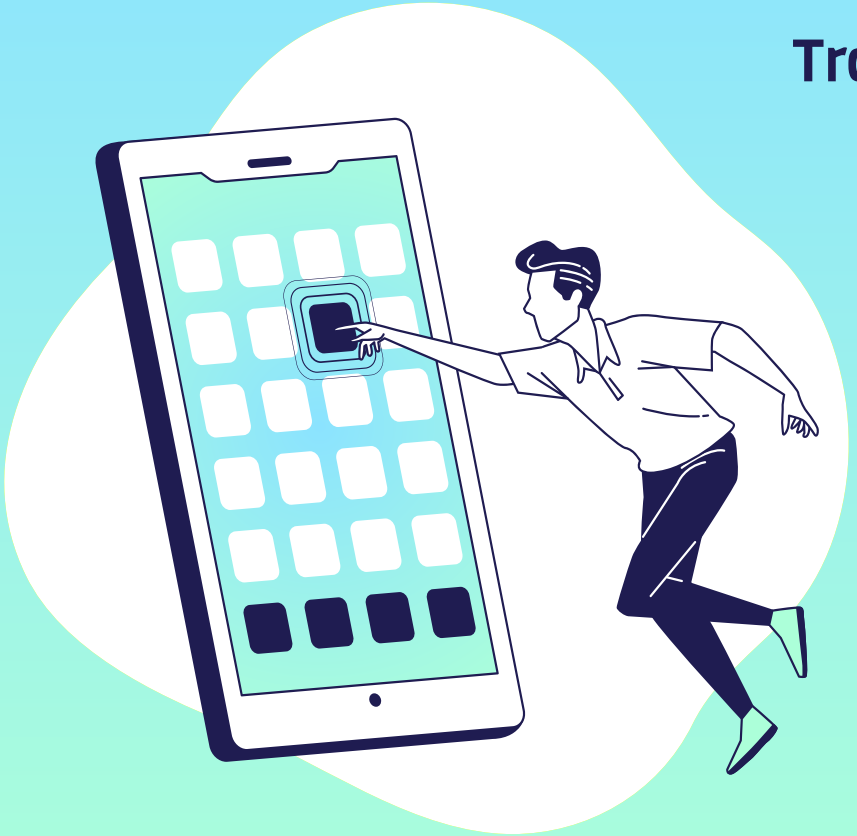


Explanation

Used Excel's sorting and filtering capabilities to isolate login attempts on Memorial Day, Independence Day, and Labor Day. This methodology allowed us to compare the volume of logins against expected activity levels for these holidays to see deviations and anomalies.

Login Attempts on Holidays





Travel Distances for Suspicious Logins

User MPiddlesden66 often makes rapid round trips from California to Illinois and back, flying in and out on the same day despite the logistical challenges.

We took user's past login attempt dates and times, then compared past and current longitudinal differences.

Conclusion

The greatest lacking security controls for EY are the amount of login attempts a user can have and the location a user can attempt to login from . User Ejeanneau51 was able to attempt of 8000 logins in a single day, given more time it is entirely possible EY could have been breached. This would be preventable by a simple limit on login attempts. Secondly, no one outside the US has a successful login attempt which means we can assume all employees should be in the US. Therefore should be a geo lock on where a user can attempt to log in.