UNIVERSITI TEKNOLOGI MARA

MATHEMATICS LETTERS
https://sites.google.com/tmsk.uitm.edu.my/mathematicsletters

Data Validation and Quality Assurance in Cybersecurity Reporting at EC-Council Global Services

[1,*]Siti Aisyah Ahmad Nizam
[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia
[1]2023115637@tudent.uitm.edu.my
*Corresponding author

Received: 1/9/2025 Revised: 25/9/2025 Accepted: 20/10/2025 Published: 5/11/2025

ABSTRACT

This technical report details an analytical study conducted within the Cyber Defense Department and Security Operations Center (SOC) at EC-Council Global Services (ECGS). The study focuses on data validation, quality assurance, and the preparation of monthly Incident Analysis (IAM) reports to support real-time threat monitoring and decision-making. Raw security logs and incident records were extracted and cleaned using Microsoft Excel's Power Query, employing functions such as ISBLANK and IFERROR to address missing fields, duplicate entries, and timestamp anomalies. Cleaned datasets were then transformed using PivotTables to visualize login activities, access trends, and security anomalies over specific time intervals. The results demonstrated that rigorous data cleaning significantly corrected misleading incident counts and clarified trend analysis, preventing the misinterpretation of system maintenance as security failures. Ultimately, the integration of structured data management techniques ensures the reliability of cybersecurity reporting and enhances organizational situational awareness.

Keywords: Cybersecurity reporting, Data validation, EC-Council Global Services, Power Query, Security Operations Center (SOC).

INTRODUCTION

EC-Council Global Services (ECGS) is a globally recognized cybersecurity consulting firm headquartered in Malaysia. Acting as the consulting arm of the International Council of E-Commerce Consultants (EC-Council), ECGS provides comprehensive services including penetration testing, threat intelligence, and incident response to help organizations comply with standards such as ISO 27001, GDPR, and PCI DSS.

The Cyber Defense Department operates within the Security Operations Center (SOC) and is responsible for monitoring, detecting, analyzing, and responding to cyber threats in real time. A critical component of this operation is the generation of accurate security reports from large volumes of log data. Raw data extracted from various security platforms often contain inconsistencies, missing fields, and duplicate entries, which can severely compromise threat monitoring if left unaddressed. Therefore,

this study outlines the implementation of systematic data validation and quality assurance workflows to ensure the accuracy and reliability of monthly SOC reports.

THE PROPOSED METHOD

Data Validation and Quality Assurance

The process began with the extraction of raw logs containing details such as incident types, timestamps, device names, severity levels, and IP addresses. Microsoft Excel's Power Query was utilized to automate the data transformation process. The key validation steps included:

- Removing redundant columns and applying the "Remove Duplicates" function to prevent repeated logs from skewing summary statistics.
- Highlighting entries with blank fields using conditional formatting and applying the ISBLANK() function to flag missing critical values.
- Implementing the IFERROR() function to identify and resolve formula errors in calculated columns.
- Detecting temporal anomalies by flagging records with future timestamps or dates outside the reporting period.

Monthly IAM Report Preparation

For the Incident Analysis (IAM) Report, raw log data from identity and access management systems—such as SIEM dashboards and Active Directory reports—were extracted. Power Query was used to group data into hourly and daily intervals and to combine multiple datasets through merging and joining techniques. PivotTables were subsequently generated to summarize metrics such as daily logins, failed login attempts by department, and access events by user role.

EVALUATION AND RESULTS

Impact of Data Cleaning on Trend Analysis

The implementation of rigorous data validation procedures resulted in a significant correction of incident records. Initially, duplicate logs caused misleading volume figures; however, post-cleaning, the total count of incidents became accurate and consistent. Visualizing the cleaned data provided clearer operational insights (See Figure 1). The visualization revealed a sharp drop in daily logs during the middle of the month, which was confirmed to be scheduled system maintenance rather than a threat detection failure.

Insights from IAM Reporting

The IAM reporting highlighted recurring security themes, such as unauthorized access attempts, allowing the SOC team to maintain vigilance over persistent threats. Graphical representations of the data further prevented analytical misinterpretations (See Figure 2). The login activity graph showed expected drops during weekends and a sudden weekday decrease. Because the data had been accurately binned into daily intervals using Power Query, the team successfully traced this anomaly back to known system maintenance, proving that clean data processing directly enhances situational awareness.

Figure 1

Daily Log trend

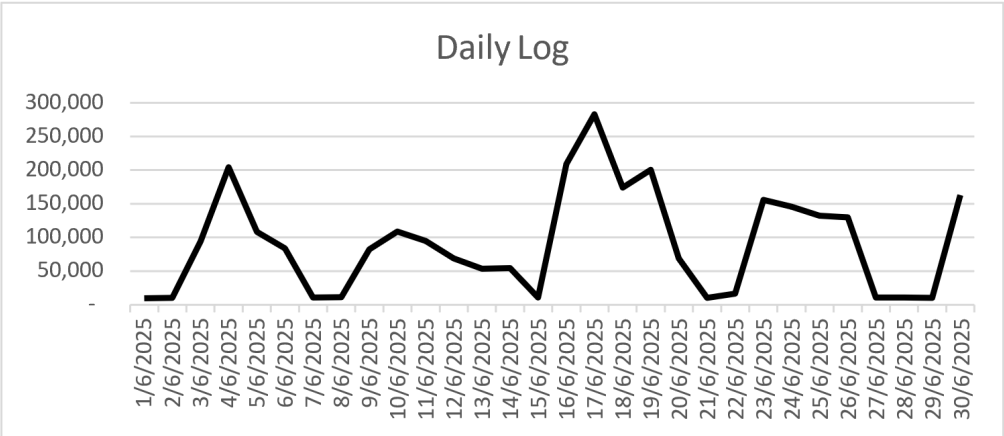
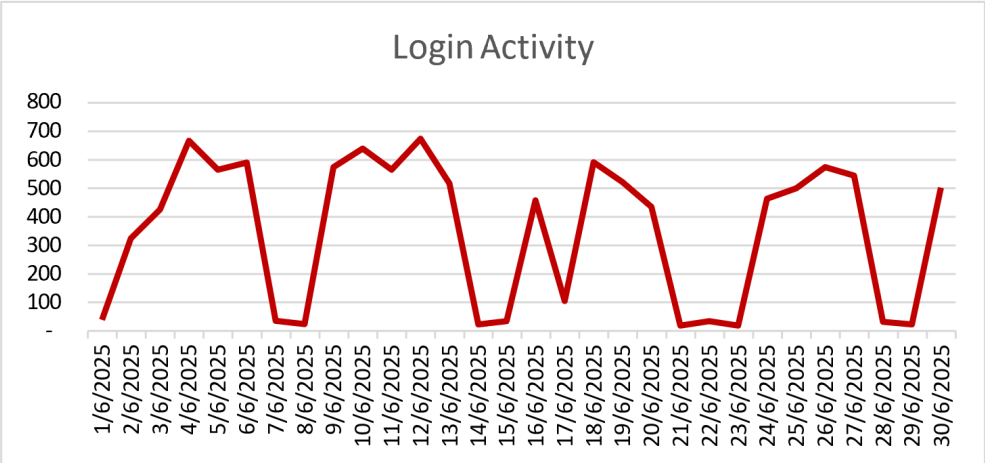


Figure 2

Login Activity for the month



CONCLUSION

The analytical tasks conducted at EC-Council Global Services demonstrate the foundational importance of data quality in cybersecurity operations. By applying structured data cleaning techniques via Power Query and generating visualizations through PivotTables, raw security logs were successfully transformed into actionable intelligence. These processes prevented the misinterpretation of system events and improved the reliability of SOC reporting. Moving forward, cybersecurity departments are encouraged to continue automating data validation workflows, as establishing repeatable data cleaning protocols is essential for rapid and accurate threat detection.

ACKNOWLEDGEMENT

The author extends profound gratitude to Universiti Teknologi MARA for supporting this work. The author expresses sincere gratitude to EC-Council Global Services, specifically the Security Operations Center (SOC) team, for providing a collaborative and hands-on learning environment during this industrial training. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest
The authors have no conflicts of interest to declare.

Non-funded
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

EC-Council Global Services. (n.d.). *Organization Background*. Retrieved from internal reporting documentation.