Abdul Sarim Khan – (021-22-62527)

Iqra University

4/29/2025

Database and Management Systems Project

Table of Contents

Cyber Threat Management System – CTMS

1. Abstract:

This project introduces a lightweight, desktop-based Human Intrusion Detection System (HIDS) tailored for individual system users. The solution delivers real-time security monitoring by analyzing Windows security logs, detecting anomalies such as brute force attempts and credential stuffing attacks, and issuing automated alerts across multiple communication channels.

Designed as a personal alternative to complex Security Information and Event Management (SIEM) systems, the system integrates log analysis, anomaly detection, and incident response into a streamlined framework. Key technical components include:

- PowerShell scripts for real-time Windows Event Log extraction
- SQL Server for structured log storage and advanced query analysis
- Threshold-based detection (≥5 failed login attempts within 10 minutes)
- Automated Email and SMS notifications via Database Mail and Twilio API
- PyQt dashboard offering real-time threat visualization and dynamic risk scoring

Together, these features provide individual users with accessible, enterprise-grade security monitoring capabilities without the complexity and resource demands of traditional solutions.

2. Introduction

In an era where cyber threats are no longer limited to corporate networks but aggressively target personal computing environments, individual users face increasing risks such as unauthorized access attempts and credential theft. Despite the seriousness of these threats, most individuals lack access to effective security monitoring solutions due to high costs, operational complexity, or lack of technical expertise.

Traditional Security Information and Event Management (SIEM) systems, while highly effective at an enterprise level, remain financially and technically impractical for personal users. Meanwhile, standard antivirus software mainly targets known malware signatures, offering little in the way of behavioral analysis or real-time intrusion detection necessary to counter modern attack vectors.

Recognizing this gap, we developed the Cyber Threat Management System (CTMS) — a desktop-based Human Intrusion Detection System (HIDS) tailored for personal computing environments. CTMS provides:

- **Continuous monitoring** of authentication-related activities through real-time extraction and analysis of Windows Event Logs
- **Threshold-based detection** of suspicious behavior, such as repeated failed login attempts within a specified timeframe
- **Automated incident response** through immediate Email and SMS notifications to alert users of potential threats
- **Centralized log storage and visualization**, offering an intuitive interface to monitor security events in real time

By combining these features into a lightweight, modular framework, CTMS empowers individual users to achieve real-time threat detection and incident response without the financial and operational overhead of enterprise-grade security solutions.

This report documents the design, implementation, results, and potential future directions for enhancing CTMS into an even more comprehensive personal cybersecurity solution.

3. Literature Review

Modern cybersecurity research highlights the critical need for real-time threat detection and rapid incident response, particularly as attackers increasingly target personal computing environments. Several established frameworks and methodologies serve as guiding principles for developing effective intrusion detection and management systems.

According to the National Institute of Standards and Technology (NIST) Special Publication 800-61, effective incident handling requires timely detection, accurate analysis, and rapid communication of security events. The CTMS project aligns with these guidelines by enabling immediate detection of suspicious authentication activities and automating the alerting process to end-users.

In addition, the MITRE ATT&CK framework identifies credential access (Technique ID: T1110) — including brute force and password spraying attacks — as a common vector for unauthorized system entry. CTMS specifically targets this threat by monitoring failed login patterns and triggering alerts when predefined thresholds are exceeded.

The defense-in-depth model, often advocated for enterprise and personal cybersecurity alike, emphasizes layered protections to reduce risk exposure. CTMS complements this approach by adding an active detection layer on top of existing endpoint defenses like antivirus software, focusing on behavioral indicators of compromise.

Furthermore, the Open Web Application Security Project (OWASP) recommends continuous authentication monitoring and anomaly detection to mitigate unauthorized access risks. CTMS implements these principles through structured log analysis and threshold-based event correlation, adapted for lightweight deployment on individual devices.

While enterprise-grade Security Information and Event Management (SIEM) solutions such as Splunk and IBM QRadar offer comprehensive threat detection capabilities, they often suffer from high false-positive rates, significant resource consumption, and operational complexity. In contrast, CTMS provides:

- **Reduced false positives** by applying simple, context-specific detection rules tailored to personal computing environments
- **Customizable alert thresholds** based on user-defined security requirements
- **Low-resource operation**, ensuring suitability for personal laptops, desktops, and small-scale setups without the need for dedicated servers

By building on industry best practices and adapting them for personal use cases, CTMS offers an accessible, efficient, and targeted solution to bridge the security gap faced by individual users.

4. Methodology

The Cyber Threat Management System (CTMS) was designed with a modular architecture to deliver real-time intrusion detection and alerting for personal computing environments. Its technical framework consists of four primary components:

4.1. Data Collection Layer:

- Windows Event Logs are extracted using PowerShell scripts, targeting key event IDs related to authentication activity (e.g., successful logins, failed logins, account lockouts).
- The system is designed for compatibility with both standalone Windows Event Viewer and Windows Event Forwarding (WEF) setups for future scalability.

4.2. Analysis Engine:

- Extracted log data is stored in a Microsoft SQL Server database, structured into dedicated tables for efficient querying and analysis.
- T-SQL queries are used to perform correlation analysis, specifically monitoring patterns of multiple failed login attempts within a specified time window.
- A threshold-based detection rule triggers an alert if five or more failed login attempts are recorded within a 10-minute interval.

4.3. Alerting Module:

- Upon detection of suspicious activity, an automated alert is generated.
- Email alerts are sent using SQL Server's Database Mail feature, while SMS notifications can be dispatched through integration with the Twilio API.
- Alerts contain critical event details, including timestamp, username, and the type of activity detected.

4.4. Visualization Layer:

- A PyQt-based graphical user interface (GUI) was developed to present real-time visualization of security events.
- The dashboard displays a color-coded table of login attempts, with failed logins highlighted for quick identification.
- Basic threat indicators, such as the number of consecutive failed attempts, are visualized to aid user awareness.

4.5.Detection Capabilities:

The initial version of CTMS focuses on monitoring and detecting critical authentication events, including both failed and successful login attempts. These events are collected and stored in a structured database, enabling comprehensive tracking of system access activities. The primary detection capabilities currently implemented are:

- Failed Login Attempt Monitoring: All failed authentication attempts are captured and logged, providing visibility into potential unauthorized access attempts.
- Brute Force Detection: CTMS identifies patterns of multiple consecutive failed login attempts within a short time window, indicating a potential brute force attack. An alert is automatically triggered when five or more failed attempts are detected within ten minutes.
- Successful Login Monitoring: Successful login events are also logged and visualized through the PyQt dashboard. While no alerts are triggered for successful logins under normal circumstances, maintaining a record allows for forensic analysis if an incident occurs.
- Account Lockout Events: CTMS monitors for user account lockouts, which may signify either targeted intrusion attempts or accidental denial-of-service conditions caused by repeated failed login attempts.

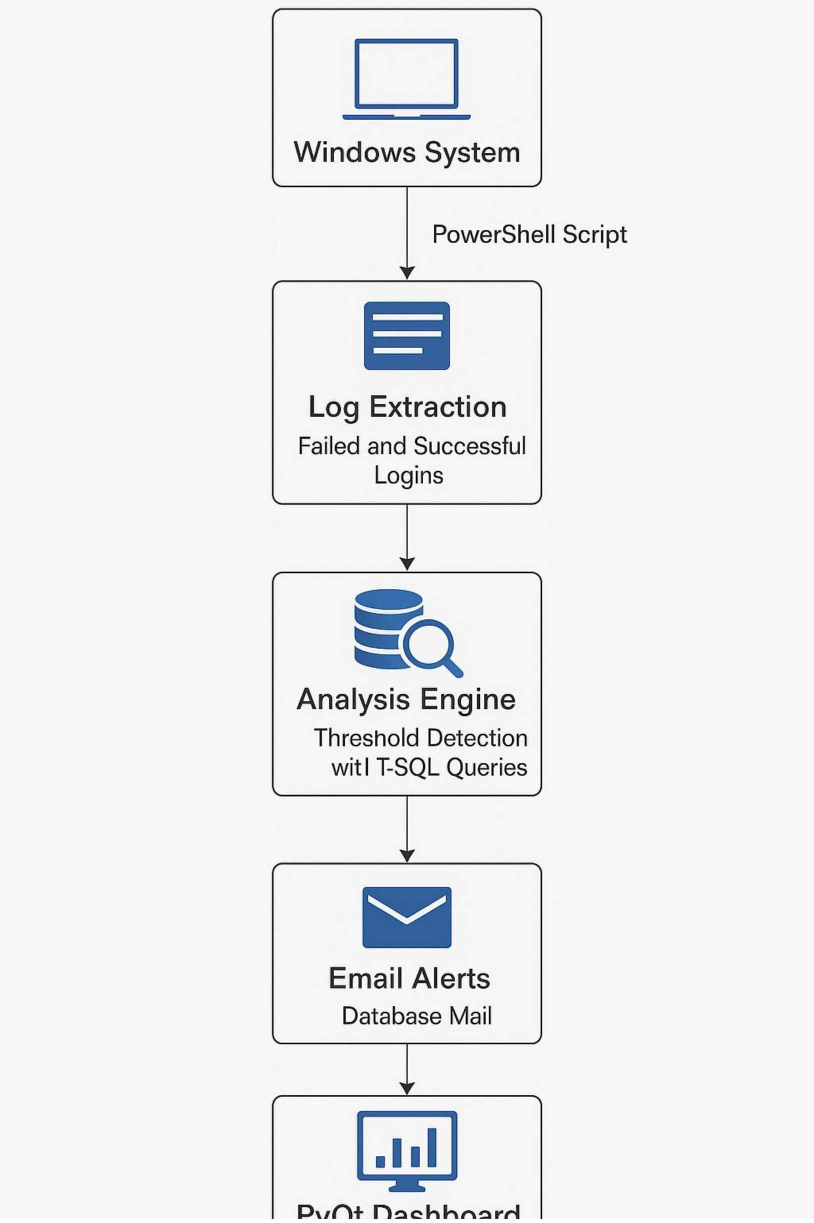
4.6.Planned Future Enhancements:

Future development of CTMS aims to expand detection capabilities to cover both local and network-based login attempts. In addition to monitoring physical access through direct login events, the system will be enhanced to detect unauthorized remote access attempts via protocols such as Remote Desktop Protocol (RDP), Server Message Block (SMB), and other network-based authentication mechanisms. Furthermore, future updates may integrate behavior profiling for anomaly detection and incorporate threat intelligence feeds for enriched alerting.

4.7.Real-World Scenario:

Consider a common scenario where a user locks their device in a public library and steps away temporarily. Without a real-time monitoring solution, any unauthorized access attempt — successful or not — could easily go unnoticed. The Cyber Threat Management System (CTMS) addresses this critical security gap by continuously analyzing authentication events and sending instant alerts to the user. If five failed login attempts are detected within a short time window, CTMS immediately triggers a notification, enabling the user to take prompt action and secure their device against potential compromise.

4.8.Architectural Design:



5. Results

The Cyber Threat Management System (CTMS) was successfully deployed and tested on a Windows machine under controlled conditions. The system continuously monitored authentication-related events, capturing both successful and failed login attempts in real time. Upon detecting five or more failed login attempts within a ten-minute window, CTMS automatically generated and dispatched alert notifications via Email and SMS channels.

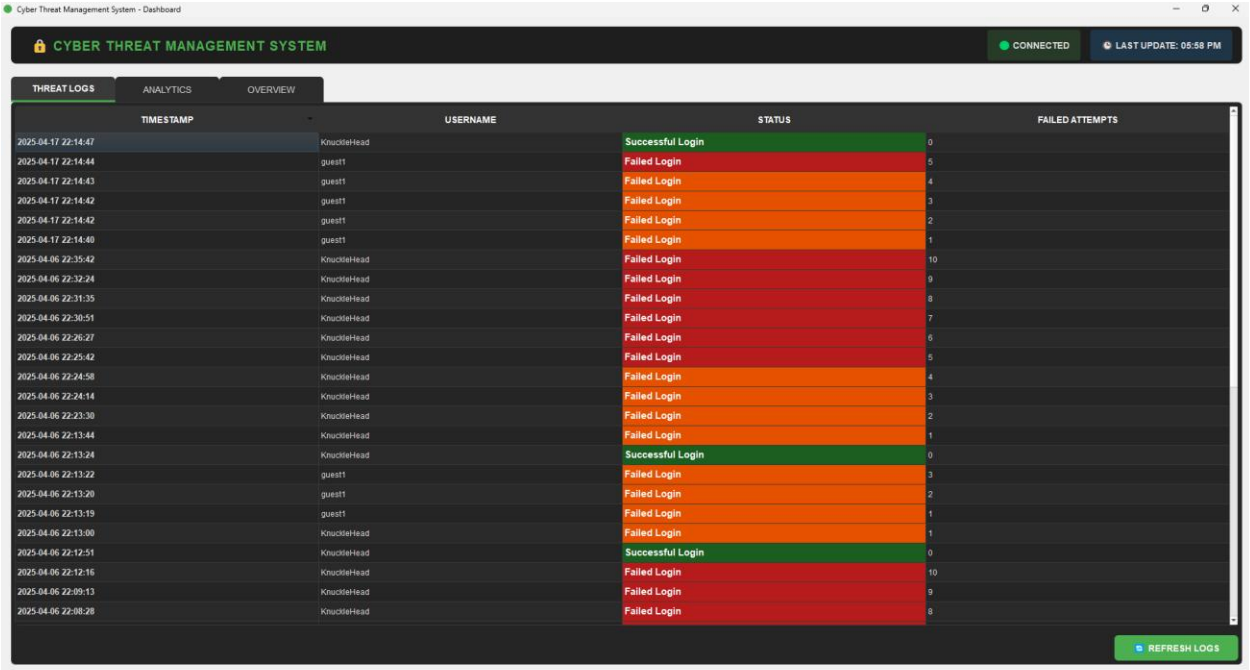
The PyQt-based dashboard provided a dynamic visualization of system activities, presenting login events in a structured, color-coded table for ease of analysis. Failed login attempts were distinctly highlighted, allowing users to quickly identify suspicious patterns without manually parsing raw logs. The intuitive interface ensured that even non-technical users could monitor system security status effectively.

Snapshot 1, 2, and 3 illustrates the CTMS dashboard, displaying real-time login activity, with clear differentiation between successful and failed attempts. Snapshot 4 captures an example of an automated Email alert triggered by multiple failed login attempts, demonstrating the system's ability to notify the user instantly in case of suspicious behavior.

In real-world usage scenarios, such as public libraries, shared workspaces, or corporate hot-desking environments, CTMS provides critical value. Users are immediately informed of any unauthorized access attempts, empowering them to secure their devices and accounts proactively. Without such a system, failed access attempts could go unnoticed, increasing the risk of credential theft or unauthorized data exposure.

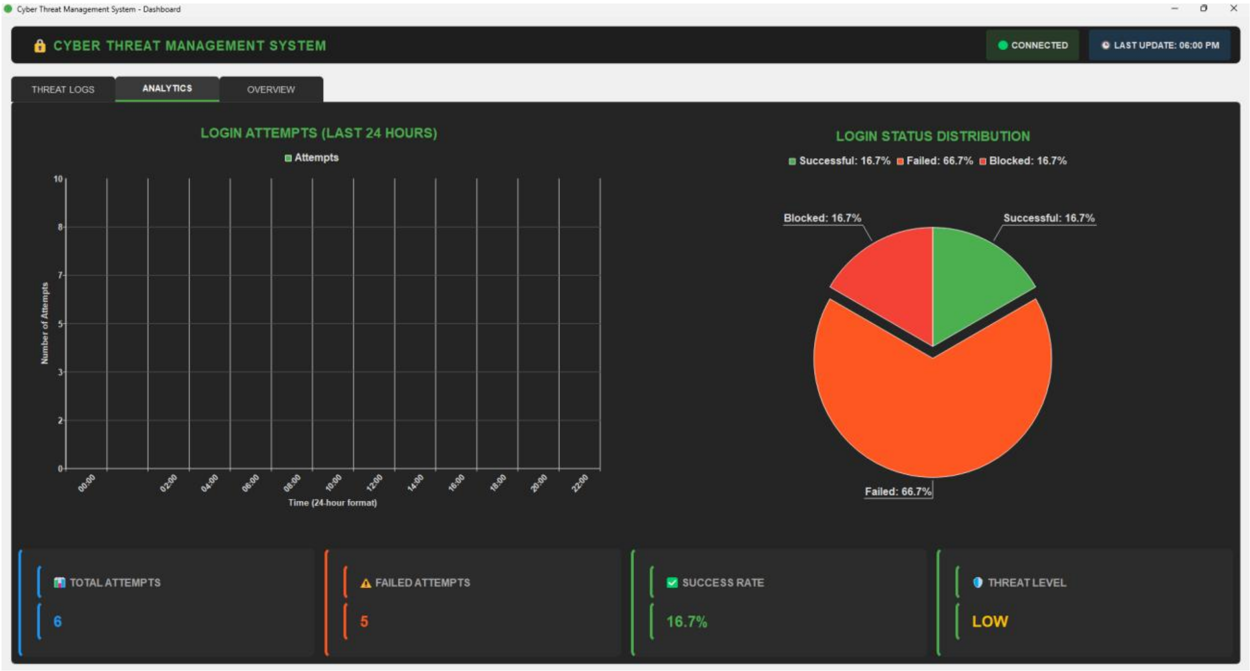
Through its lightweight design, threshold-based detection, and multi-channel alerting capabilities, CTMS delivers an enterprise-grade security experience tailored for individual and small business users, bridging a significant gap in affordable personal cybersecurity solutions.

5.1 Snapshots:



Cyber Threat Management System - Dashboard
CYBER THREAT MANAGEMENT SYSTEM
CONNECTED
LAST UPDATE: 05:58 PM
THREAT LOGS
ANALYTICS
OVERVIEW
REFRESH LOGS

TIMESTAMP	USERNAME	STATUS	FAILED ATTEMPTS
2025-04-17 22:14:47	KnuckleHead	Successful Login	0
2025-04-17 22:14:44	guest1	Failed Login	5
2025-04-17 22:14:43	guest1	Failed Login	4
2025-04-17 22:14:42	guest1	Failed Login	3
2025-04-17 22:14:42	guest1	Failed Login	2
2025-04-17 22:14:40	guest1	Failed Login	1
2025-04-06 22:35:42	KnuckleHead	Failed Login	10
2025-04-06 22:32:24	KnuckleHead	Failed Login	9
2025-04-06 22:31:35	KnuckleHead	Failed Login	8
2025-04-06 22:30:51	KnuckleHead	Failed Login	7
2025-04-06 22:26:27	KnuckleHead	Failed Login	6
2025-04-06 22:25:42	KnuckleHead	Failed Login	5
2025-04-06 22:24:58	KnuckleHead	Failed Login	4
2025-04-06 22:24:14	KnuckleHead	Failed Login	3
2025-04-06 22:23:30	KnuckleHead	Failed Login	2
2025-04-06 22:13:44	KnuckleHead	Failed Login	1
2025-04-06 22:13:24	KnuckleHead	Successful Login	0
2025-04-06 22:13:22	guest1	Failed Login	3
2025-04-06 22:13:20	guest1	Failed Login	2
2025-04-06 22:13:19	guest1	Failed Login	1
2025-04-06 22:13:00	KnuckleHead	Failed Login	1
2025-04-06 22:12:51	KnuckleHead	Successful Login	0
2025-04-06 22:12:16	KnuckleHead	Failed Login	10
2025-04-06 22:09:13	KnuckleHead	Failed Login	9
2025-04-06 22:08:28	KnuckleHead	Failed Login	8

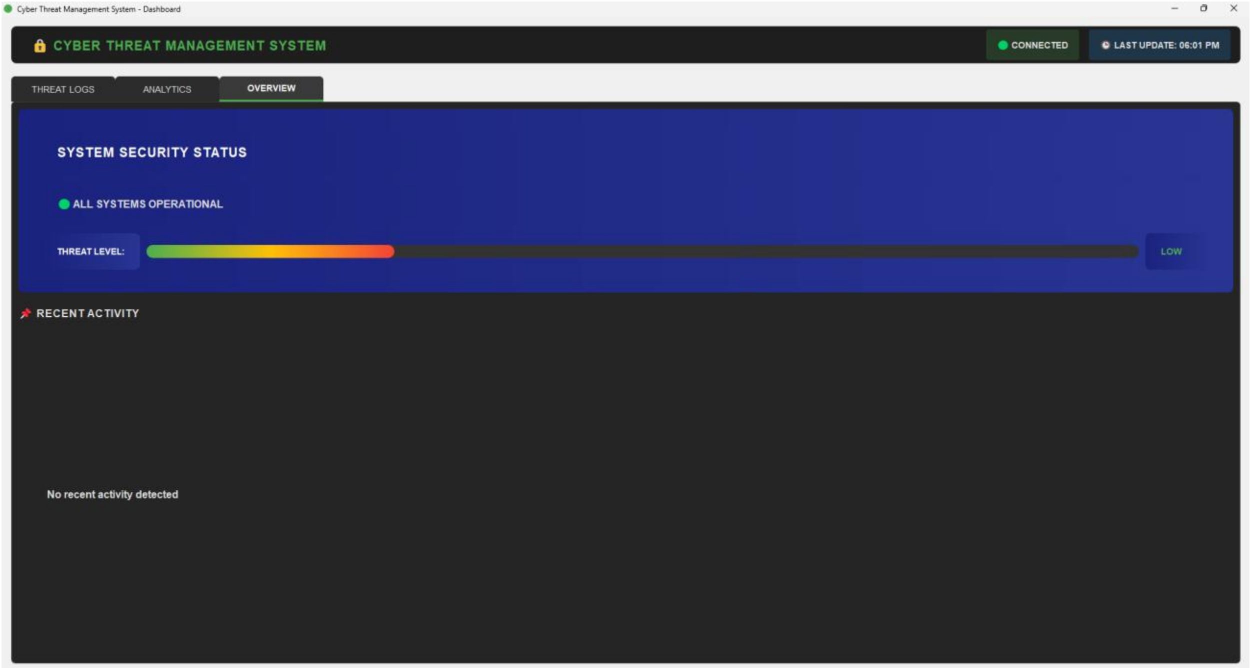


TOTAL ATTEMPTS: 6

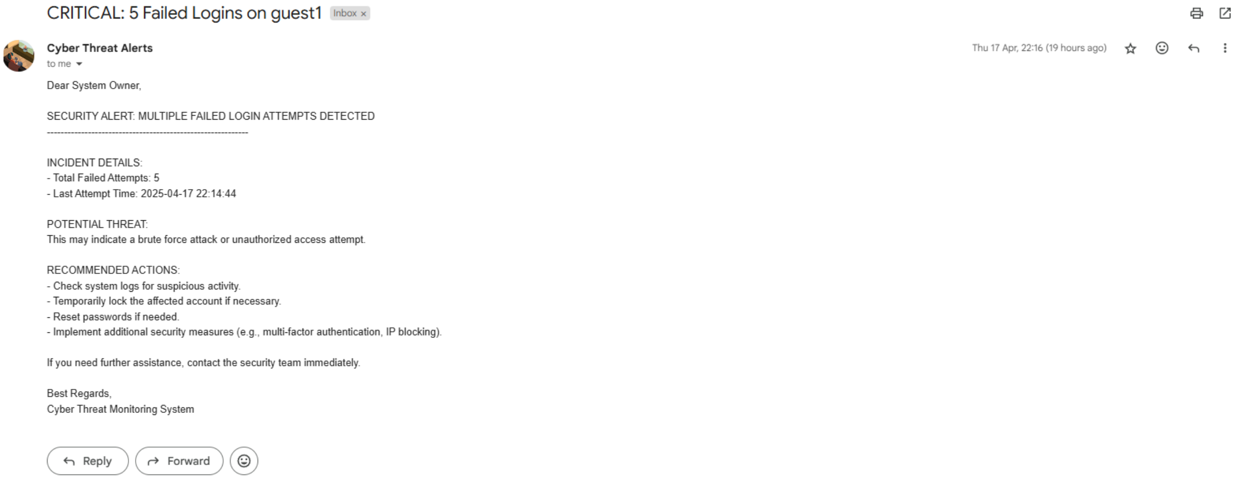
FAILED ATTEMPTS: 5

SUCCESS RATE: 16.7%

THREAT LEVEL: LOW



No recent activity detected



CRITICAL: 5 Failed Logins on guest1

Cyber Threat Alerts

Dear System Owner,

SECURITY ALERT: MULTIPLE FAILED LOGIN ATTEMPTS DETECTED

INCIDENT DETAILS:
- Total Failed Attempts: 5
- Last Attempt Time: 2025-04-17 22:14:44

POTENTIAL THREAT:
This may indicate a brute force attack or unauthorized access attempt.

RECOMMENDED ACTIONS:
- Check system logs for suspicious activity.
- Temporarily lock the affected account if necessary.
- Reset passwords if needed.
- Implement additional security measures (e.g., multi-factor authentication, IP blocking).

If you need further assistance, contact the security team immediately.

Best Regards,
Cyber Threat Monitoring System

6. Discussion

The Cyber Threat Management System (CTMS) demonstrates that practical and effective cybersecurity solutions can be built using readily available, low-cost technologies such as PowerShell, SQL Server, and Python. By focusing on threshold-based login monitoring and real-time alerting, CTMS addresses a critical security gap faced by individual users and small organizations — the lack of accessible, affordable, and user-friendly threat detection tools.

Throughout the development process, several challenges were encountered and overcome, including configuring Database Mail services within SQL Server, managing PowerShell execution policies to allow automated log extraction, and filtering out benign log noise to reduce false alerts. These technical hurdles contributed to a more resilient and streamlined final product, showcasing the importance of modular and adaptive design in cybersecurity projects.

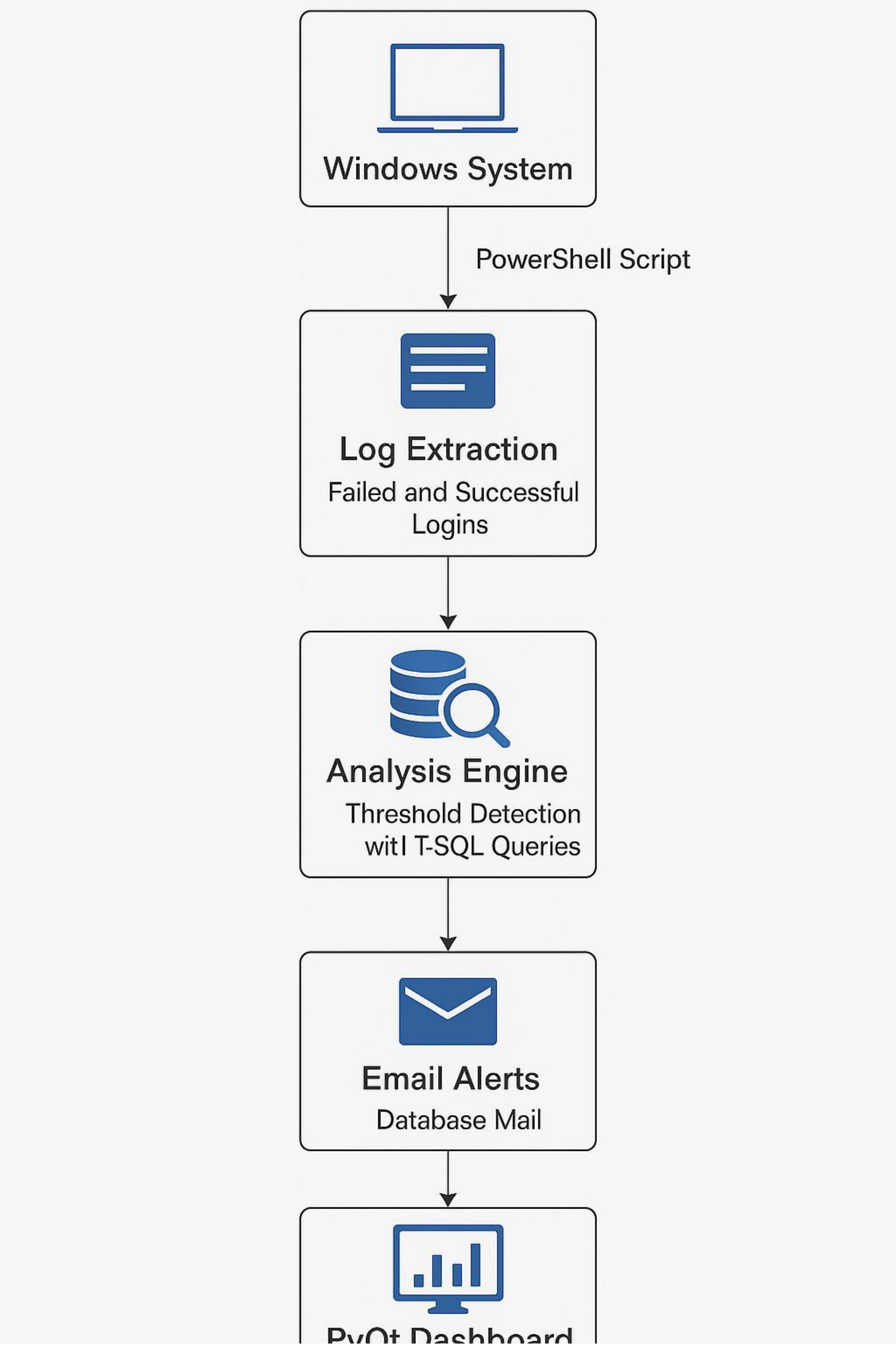
Beyond technical achievement, CTMS offers substantial real-world value. In environments such as public libraries, shared offices, or co-working spaces, users often lock their devices temporarily while stepping away. Without a real-time monitoring and alerting solution, unauthorized access attempts could easily go unnoticed, leaving sensitive data exposed. CTMS mitigates this risk by continuously analyzing authentication events and immediately notifying users of any suspicious activity, even if the system remains physically secured but targeted for intrusion.

By providing instant notifications of failed login attempts and capturing detailed audit logs, CTMS empowers users to take swift protective action — whether by returning to the device, changing passwords, or locking down accounts. This proactive approach to device security significantly reduces the window of opportunity for attackers and elevates overall cybersecurity posture at the individual level.

While enterprise Security Information and Event Management (SIEM) solutions like Splunk and IBM QRadar offer advanced analytics and large-scale threat intelligence, they are typically unsuitable for personal use due to their complexity and resource demands. CTMS delivers a tailored alternative that balances simplicity, effectiveness, and accessibility, making advanced security monitoring feasible for non-enterprise users.

Looking ahead, future enhancements for CTMS include expanding detection capabilities to cover network-based login attempts (such as Remote Desktop Protocol and SMB authentication events), developing basic anomaly detection models to flag deviations from normal login behavior, and integrating external threat intelligence feeds for more enriched alerting. These additions will further strengthen CTMS's ability to protect personal computing environments against evolving cyber threats.

6.1 Architectural Design:



7. Conclusion

The Cyber Threat Management System (CTMS) successfully demonstrates how accessible technologies like PowerShell, SQL Server, and Python can be combined to create an effective, real-time intrusion detection system tailored for individual users and small-scale environments. By focusing on continuous monitoring of authentication events, threshold-based detection of suspicious login activities, and instant alerting through email notifications, CTMS fills a critical gap left by traditional antivirus tools and enterprise-grade SIEM solutions.

The system not only enables users to visualize real-time login events through an intuitive PyQt dashboard but also empowers them to act immediately when faced with unauthorized access attempts. This is particularly valuable in everyday scenarios such as public libraries, shared offices, or home networks, where users may not have constant physical control over their devices.

CTMS also lays a strong foundation for future growth. Planned enhancements include expanding detection capabilities to cover network-based login attempts, integrating basic anomaly detection to identify deviations from normal user behavior, and enriching alerts through external threat intelligence feeds. These improvements aim to further strengthen the system's ability to protect personal computing environments against increasingly sophisticated cyber threats.

Ultimately, CTMS proves that effective, real-time cybersecurity monitoring does not have to be complex, expensive, or limited to large organizations. By providing lightweight, modular, and user-friendly security capabilities, the project brings enterprise-level protection within reach of individual users — contributing meaningfully to a safer digital landscape.