**Incident Response Report**

**Cyber Security Internship — Task 2**

**Prepared by:** TIYA MEHTA  
**Date:** 30 June 2025

**Executive Summary**

During routine monitoring on 30 June 2025, multiple suspicious activities were detected, including brute-force login attempts, SQL injection, malware infections, phishing attacks, port scanning, privilege escalation, denial of service, and unauthorized access.  
This report summarizes the findings, assesses their impact, and provides actionable recommendations.

**Table of Contents**

1. Introduction
2. Timeline of Events
3. Alert Analysis & Classification
4. Impact Assessment
5. Recommendations
6. Screenshots

**Introduction**

This report documents the security alerts identified from simulated log data. The aim is to analyze the alerts, classify them by severity, assess their potential impact, and recommend mitigation actions.

**Timeline of Events**

| **Time** | **Event** |
| --- | --- |
| 08:25 | Brute Force Login — Alice — 192.168.1.101 |
| 08:29 | SQL Injection Attempt — Charlie — 203.0.113.45 |
| 08:31 | Malware Infection — Eve — 198.51.100.23 |
| 08:35 | Phishing Email Clicked — Frank — 198.51.100.24 |
| 08:40 | Port Scanning — Mallory — 198.51.100.25 |
| 08:46 | Privilege Escalation — Trudy — 198.51.100.26 |
| 08:50 | Denial of Service — Bob — 203.0.113.50 |
| 08:52 | Unauthorized Access — Admin — 10.0.0.1 |

**Alert Analysis & Classification**

| **Alert #** | **Time** | **Type of Threat** | **User** | **Source IP** | **Severity** |
| --- | --- | --- | --- | --- | --- |
| 1 | 08:25 | Brute Force Login | Alice | 192.168.1.101 | High |
| 2 | 08:29 | SQL Injection Attempt | Charlie | 203.0.113.45 | High |
| 3 | 08:31 | Malware Infection | Eve | 198.51.100.23 | High |
| 4 | 08:35 | Phishing Email Clicked | Frank | 198.51.100.24 | Medium |
| 5 | 08:40 | Port Scanning | Mallory | 198.51.100.25 | Medium |
| 6 | 08:46 | Privilege Escalation | Trudy | 198.51.100.26 | High |
| 7 | 08:50 | Denial of Service | Bob | 203.0.113.50 | High |
| 8 | 08:52 | Unauthorized Access | Admin | 10.0.0.1 | High |

**Impact Assessment**

These incidents pose a critical risk to the organization. If not addressed promptly, they could lead to unauthorized access, data breaches, service disruption, and compromise of sensitive information.

**Recommendations**

✅ **Immediate Actions:**

* Block all identified malicious IPs immediately.
* Isolate and clean infected hosts.
* Reset passwords of compromised accounts.

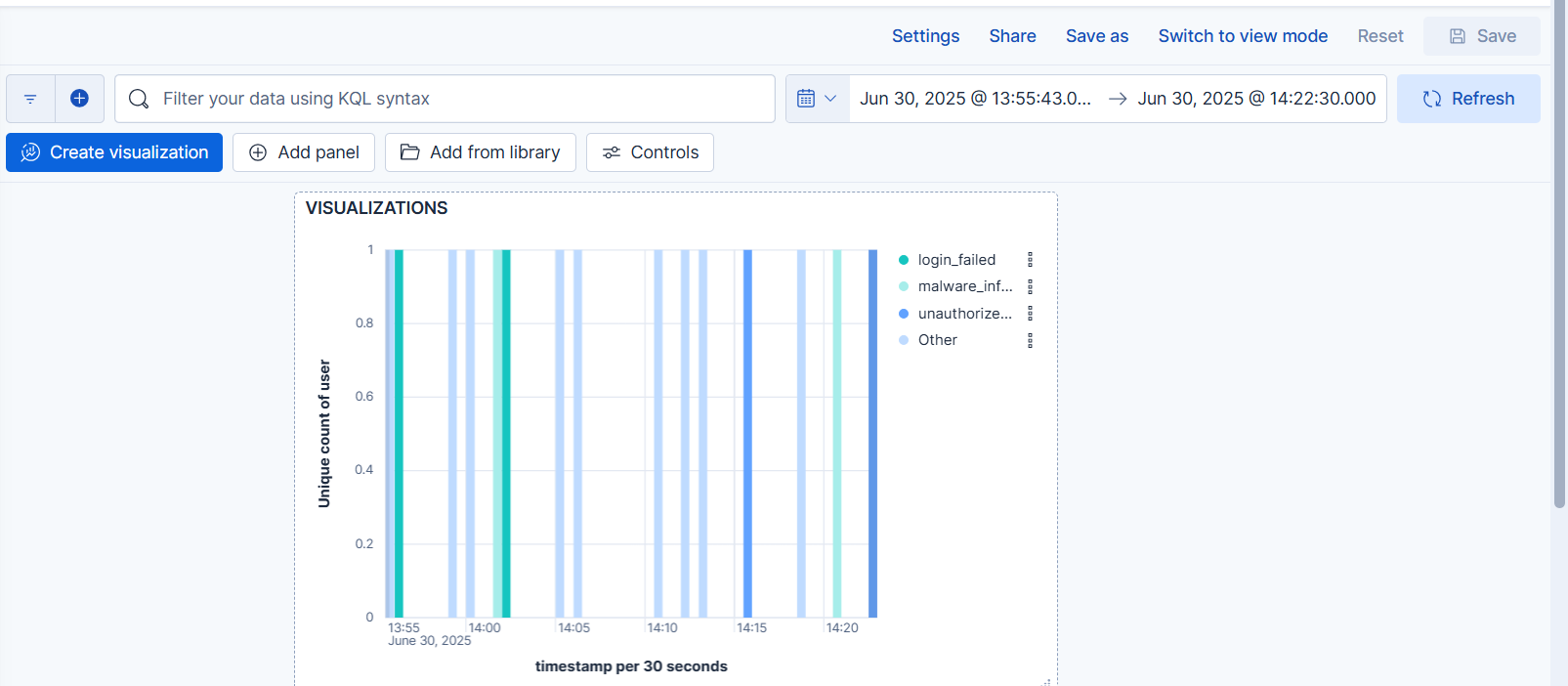
✅ **Medium-term Measures:**

* Enforce strong password policies and enable MFA.
* Regularly update and patch systems.

✅ **Long-term Strategy:**

* Conduct employee awareness training.
* Deploy IDS/IPS for proactive monitoring.

**Screenshots**

**Figure 1:** SIEM Dashboard Overview  


**Figure 2:** Detailed Alert View — SQL Injection  
