# LOG ANALYSIS ASSIGNMENT

Student Name
Oluwatimilehin Oluwagbemi

Reg. No
2025/GRC/10712

13th September, 2025

Course Title
GRC 102 – Information Security Governance

OVERVIEW

This report presents the findings from the security logs of Global Tech, a mid-sized financial technology company. The security logs were analyzed to identify critical security events or patterns.

The security logs provided are Failed Authentication Attempts, Vulnerability Scan Results and Security Incidents. The three logs were analyzed and security events or patterns identified include Unauthorized Login Attempts, Data Exfiltration, Unauthorized Access, Phishing Attempt and Remote Code Execution.

POTENTIAL SECURITY INCIDENTS FROM THE LOGS:

1. From the Failed Authentication attempt logs, it was detected that there were multiple logins attempts to admin, network_admin, sysuser, jdoe and guest which poses a brute force attack or credential stuffing attempts on their account. The incidents of the multiple login attempts can lock out legitimate user on the system. To remediate this incident, the company should implement MFA on every privileged account, they should enforce account lock-out policies, such that an account will be locked after 3 login attempts for a specified time. Firewalls should be configured to block suspicious IPs. Strong Password policies should be set and enforced, trainings on how to set strong passwords and how to recognize phishing emails should be conducted for users.
2. Data Exfiltration was detected on db-server-02 and user-workstation-10 with high and critical severity, with ongoing investigation. This incident poses a risk of data being breached with critical and sensitive information exposure, which can lead to financial loss, regulatory fines, and reputational damage. To remediate this incident, all affected systems should first be isolated to prevent further spread, Data Prevention Loss control should be implemented, networks should be segmented to prevent all network being breached, confirmation of sensitive data loss from compliance team, also digital forensics should be carried out to know where there's loophole.
3. An Unauthorized access is being investigated on db-server-02 with a high severity. This incident also poses a risk of data breach or system compromise. To remediate this incident the system affected should first be isolated. The system logs should be analyzed to know the entry point, the credentials associated to the compromised system should also be revoked to disable the account created by the attacker, patching should be done.
4. A phishing attempt on user-workstation-10 was detected. This incident can lead to sensitive data loss, financial loss, it can also lead to data breach or system being compromised. To remediate this, passwords need to be changed, multi-factor authentication should be enabled, malware scan should be done on affected systems and all systems on the same network with the affected system.
5. Remote Code Execution (CVE-2023-9012) with critical severity was detected on System webserver-01. This vulnerability could allow an attacker run command on the vulnerable system, this vulnerability can allow attacker have access and steal login credentials, it can also be used to download and execute malware. To remediate this, requires regular patching, continuous vulnerability scanning, deployment of security tools for real-time detection.