Log Analysis Assignment Report

This report presents findings from the analysis of sample security logs provided by Global Tech, a mid-sized financial technology company. The objective of this assignment was to identify potential security incidents or anomalies within the logs and propose remediation steps. The analysis focused on authentication attempts, incident reports, and vulnerability scan results.

Findings and Recommendations

Incident 1: Brute Force / Unauthorized Login Attempts
Evidence: Multiple failed logins for admin, network_admin, and sysuser accounts. Repeated lockouts observed for accounts such as jdoe, sysuser, and guest.
Concern: Indicates a possible brute force or credential stuffing attack. Frequent lockouts may also disrupt legitimate user access.
Remediation: Implement MFA on privileged accounts, enforce lockout policies with alerts, block suspicious IPs, and provide user training on phishing and password hygiene.

Incident 2: Data Exfiltration (Unresolved Cases)
Evidence: Critical data exfiltration attempts on db-server-02 and high-severity activity on user-workstation-10. Both incidents remain under investigation.
Concern: Suggests possible data breaches with sensitive financial or client information at risk. This can result in regulatory, reputational, and financial consequences.
Remediation: Isolate affected systems, perform forensic investigation, enhance Data Loss Prevention (DLP) controls, apply network segmentation, and involve compliance teams if sensitive data exposure is confirmed.

Incident 3: Unpatched Critical Vulnerabilities
Evidence: Remote Code Execution (CVE-2023-9012) detected on db-server-02 and webserver-01. SQL Injection (CVE-2023-1234) detected on app-server-03 and db-server-02 across multiple scans.
Concern: These vulnerabilities could allow system compromise or data theft. They may also be linked to the other incidents observed.
Remediation: Apply vendor patches immediately, establish a vulnerability management program with regular patching cycles, deploy a Web Application Firewall (WAF), and perform validation scans after patching.

Conclusion
The analysis highlights multiple critical risks, including brute force attempts, ongoing data exfiltration, and unresolved critical vulnerabilities. Prompt remediation is essential to reduce Global Tech’s exposure to potential breaches, ensure regulatory compliance, and maintain trust with clients.