Date

Subject: StreamStream Security Assessment Report

Dear [sender],

To meet your request we have thoroughly reviewed the systems that are part of the network and a discovered the following vulnerabilities along with proposed corrective actions.

1. System. Network Infrastructure
   Vulnerability: Lack of network segmentation
   Description: Not having proper network segmentation exposes the entire network to potential threats allowing lateral movement in the case of a security breach.
   Correction: Implement network segmentation to isolate critical segments, reducing the risk of lateral movement and enhancing overall network security.
2. System: Web Application
   Vulnerability: Missing security headers.
   Description: The web application lacks essential security headers, increasing the risk of various attacks such as XSS (cross-site scripting) and clickjacking
   Correction: Implement necessary security headers (e.g., Content Security Policy, Strict-Transport-Security) to enhance web application security and mitigate the risk of common web-based attacks.
3. System Employee Workstations
   Vulnerability: Outdated antivirus software
   Description: Some employees workstations have outdated antivirus software, leaving them susceptible to the latest malware threats.
   Correction: Update antivirus software on all workstations promptly to ensure protection against the latest malware and enhance overall endpoint security.
4. System User Authentication
   Vulnerability: Weak password policy
   Description: The existing password policy is relatively weak, making it easier for attackers to compromise user accounts through brute -force attacks
   Correction: Strengthen the password policy by enforcing complex password requirements, regular password changes, and multi-factor authentication to enhance user authentication security.
5. System: Server Configuration
   Vulnerability: Unnecessary open ports on servers.

Description: Some servers have unnecessary open ports, increasing the attack surface and potential exposure to unathorized access.
Correction: Close unnecessary open ports on servers to minimize the attack surface and reduce the risk of unathorized access.

We stand committed to implementing the corrective actions provided above and by the end of the day, we will have promptly addresses these concerns.

Should any immediate questions or requirements for additional information arise, please feel free to contact us.

Thank you.

Best regards,

[name]
[position]
[contact information]