From: AIG Cyber & Information Security Team

To: Product Development Team

Subject: Urgent: Critical Security Vulnerability in Product Development Staging Environment

Hi John Doe,

We're notifying you of a **critical vulnerability (CVE-2021-45046)** affecting the **Product Development Staging Environment** due to the use of **Apache Log4j**. This flaw is exploited to deploy malware (e.g., cryptominers, botnets).

What We Need To Do

Identify Affected Assets

Inventory all systems using Log4j (assume all Java-based assets may be impacted).

Include cloud, on-prem, and hybrid environments.

Patch Immediately

Update to the latest Log4j version.

Monitor for vendor updates.

Threat Hunting & Monitoring

Use CISA's and CERT/CC's scanners to check for exposure.

Review logs for unusual activity.

Document Your Work

Track patch status, user access, and system locations.

Keep records of all remediation steps.

Next Steps

Please confirm:

Affected assets have been identified.

Patches are applied or scheduled.

Initial threat checks are complete.

Deadline for status update: July 30th, 2025

Let us know if you need help or have questions.

Kind Regards,

AIG Cyber & Information Security Team