



## Stakeholder Briefing

Subject: Summary of Recent High-Severity Security Incident

Good morning,

I'm briefing you on a high-severity security incident that occurred on September 26th. An external actor attempted to compromise a legacy server by exploiting an unpatched vulnerability in the Samba file-sharing service.

Our Security Operations Center (SOC) detected the threat and initiated an automated response. We achieved a Mean Time to Detect (MTTD) of 1 minute and 5 seconds and a Mean Time to Resolve (MTTR) of 2 minutes and 10 seconds. This rapid response prevented any significant impact.

The incident's root cause was a failure in our legacy system patch management process. Our immediate next steps are to retire this vulnerable service and implement mandatory, organization-wide vulnerability scanning and patching policies. This will strengthen our defenses against similar future attacks.