STAKEHOLDER BRIEFING

At 17:23 on September 12, our network sensors detected an attack against a purposely vulnerable lab machine (Metasploitable2). The attacker exploited an old FTP backdoor. We immediately isolated the affected virtual machine, blocked the attacker's IP, and captured forensic logs. No production systems or sensitive data were affected. Recommended next steps are to keep test systems isolated, remove or patch known vulnerable services, and implement automated alerts that isolate compromised machines faster. We archived evidence and will provide a fuller technical report and remediation timeline if needed.