Incident Response Package

Healthcare Organization — September 20, 2025

Prepared by: Jamie Christian — Cybersecurity Analyst

Incident Report

Brute force attack detected on RDP access. 500+ failed logins, 1 compromised account, outbound anomalies.

Playbook

Step-by-step response guide for brute force incidents: detection, actions, containment, recovery.

Lessons Learned

Rapid detection worked, but weak passwords & exposed RDP were gaps. Action items defined and tracked.