# Incident Report — Intrusion Detection & Response

Prepared by: Jamie Christian — Cybersecurity Analyst

## Executive Summary

On September 20, 2025, a brute force attack targeted RDP access. Over 500 failed logins were detected, one account was compromised, and outbound anomalies observed. The incident was contained within 3 hours with no confirmed PHI loss.

## Incident Timeline

|  |  |
| --- | --- |
| Time (UTC) | Event |
| 02:12 | First failed login alert |
| 02:40 | 250+ failed attempts detected |
| 02:50 | Outbound anomaly detected |
| 03:05 | Account disabled & IP blocked |
| 04:00 | Forensic scan completed |

## Technical Findings

|  |  |
| --- | --- |
| Category | Details |
| Attack Vector | Brute Force on RDP (3389) |
| Compromised Host | 10.10.24.57 |
| User Impacted | j.smith |
| Source IP | 88.199.34.12 |
| Risk | Potential PHI exposure (HIPAA relevant) |

## Containment Actions

✅ Disabled compromised account

✅ Blocked malicious IPs at firewall

✅ Patched and hardened RDP access

✅ Enforced MFA

✅ Tuned SIEM alerts for failed logins

## Recommendations

☑ Enforce MFA for all remote access

☑ Restrict RDP to VPN/allowlisted IPs

☑ Strengthen password policies

☑ Regularly tune SIEM detection thresholds