LESSONS LEARNED

What Worked:

Rapid detection by email security module,

Quick user identification,

Fast credential reset process,

Effective user notification,

Good evidence preservation,

What Failed:

Insufficient email authentication (SPF/DKIM/DMARC),

No MFA protection,

Limited user awareness,

No phishing simulation training,

Weak brand protection

Key Lessons:

1. User awareness is critical - 2/47 users compromised despite being trained employees
2. Credential attacks are dangerous - No MFA allowed credential-only compromise
3. Email authentication matters - Domain spoofing was trivial without proper authentication
4. Detection is only half the battle - Prevention through MFA would have been more effective
5. Social engineering works - Brand impersonation successfully tricked users

Process Improvements:

1. Implement MFA organization-wide (prevents credential attacks)
2. Deploy email authentication (prevents domain spoofing)
3. Conduct regular phishing simulations (improves user awareness)
4. Create incident response playbook (enables faster response)
5. Implement advanced threat protection (catches sophisticated attacks)