

Team: Team 3

Inject Number: 25

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 09:02:57 -0500

From: Security Ops

To: Infrastructure Team

Subject: [P-215] Incident Response Plan

We are now handling Private and Confidential data. You need to develop an incident handling policy in the event of unauthorized disclosure. Refer to NIST 800-61 for ideas on policy elements. The concern is that we may have a data breach and won't have an effective incident response plan.

Develop your thoughts around:

- 1.) Initial Containment
- 2.) Notification obligations
- 3.) Collecting evidence to determine how, when and what was breached
- 4.) Whether to involve law enforcement

Respond with your Incident Response Policy document, that has been implemented within your team.

Thank you.

Security Ops