

Team: Team 2

Inject Number: 6

Inject Duration: 8 Hours

Inject Start Date/Time: Sat, 01 Feb 2020 16:32:03 +0000

From: CIO

To: IT Staff

Subject: INCIDENT REPORTING

If you suspect an incursion by the Red Team, please submit an Incident Report with as much detail as possible. Many of the points lost due to Red Team activity can be recouped through diligent, thorough, and complete reporting of known and suspected attacks. Please submit one report for each incident; be as detailed as possible.

Include the following information:

- * date/time the attack started (if known)
- * date/time the attack was discovered
- * attacker source address
- * target system name / address
- * target port / service
- * type of attack (virus, hacking, DoS, etc)
- * result of attack
- * vulnerability that allowed the attack
- * how discovered
- * how contained
- * remediation actions / controls
- * result of remediation

Thank you.

CIO