Team: Team 3

Inject Number: 16

Inject Duration: 120 Minutes

Inject Start Date/Time: Fri, 23 Mar 2018 19:31:01 -0500

From: IT Director

To: Infrastructure Team

Subject: [B-105] Configure Centralized Logging

Configure centralized logging using the Splunk server. Have all your hosts, the firewall, LAN switch and head-end router log to this service. Configure the Phantom tool to automate responses to attacks. Respond with a memo that documents that this configuration is complete. Describe how you have configured Phantom and supply screen shots to show each device logging to Splunk and logging messages.

Thank you.

IT Director