Team: Team 3

Inject Number: 24

Inject Duration: 30 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 09:00:29 -0500

From: IT Director

To: Infrastructure Team

Subject: [P-201] Status Report for Management Meeting

We have had a number of problems lately with regard to the FW, head-end router and potential unauthorized intrusions. Develop a memo that addresses the following topics:

1.) What has been done with the Firewall to improve its stability, and are we only allowing expected services to be reachable from the outside ?
2.) What have we done to insure that only authorized inside traffic exits our environment ?
3.) Is the head-end router secure and is it screening out obvious unwanted packets ?
4.) Have we implemented software firewalls on each server ?
5.) To what degree have we deployed the Phantom tool with Splunk to automate remediation tasks ?

Thank you.

IT Director