Team: Team 07

Inject Number: 13

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 30 Jan 2016 12:08:29 -0800

From: B.G. Cheese

To: Blue Team

Subject: Install and Configure SPLUNK

Team, a centralized logging service is critical to diagnosing both security and mundane system problems. Please install SPLUNK on Snoke and configure it to monitor, at minimum, User Logins across all workstations and servers. Provide screenshots of the logs from the Splunk server (dashboard view).

Monitoring these logs for unknown logins is something recommended.

Thank you.

B.G. Cheese