

Team: Team 3

Inject Number: 48

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 14:47:07 -0500

From: Chief Information Security Officer

To: Infrastructure Team

Subject: [O-230] Splunk Audit Reporting

The external auditors have begun their assessment of our system security. They require a report from Splunk showing our top talkers from the various networks. In particular they are asking for top talkers from the following networks: Internal, User, and Public. Provide the results in a memorandum format that includes tables of the top talkers by network. If you are unable to provide the requested information, our audit score will suffer but provide a detailed description of why and provide the best approximation of the requested information for the described networks via other means. Also describe what is required to provide the requested information from Splunk in the manner requested.

Thank you.

Chief Information Security Officer