Team: Team 02 - ASU

Inject Number: 11

Inject Duration: 180 Minutes

Inject Start Date/Time: Sat, 28 Jan 2017 10:03:49 -0800

From: Felonius Gru

To: IT Staff

Subject: Log Management

Team,

I don't believe in ghosts and want to get to the bottom of the weirdness that has been happening with technology around here. There must be a logical explanation and I want you to find it. My first thought is we are doing a lousy job of managing our logging which makes any real detailed investigation too time consuming. Please install some log management solution (SPLUNK, ELK, etc) of your choice. Just make sure whatever you pick is free, quick to deploy, provides SIEM capabilities, and is able to forward to the companies central QRadar solution (forward details to follow).

I am giving you 3 hours. Get something installed and configured. I want you to prepare a document telling me the product you chose, why it seemed ideal for our particular environment, and what setup options and configurations were implemented (this should include the logs/events you choose to monitor on the dashboard and why). Include in this document a screen capture or two of the dashboard. Also give me the dashboard IP address. I will want to show it off.

Thank you.

Felonius Gru