

Team: Team 8

Inject Number: 9

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 13 Feb 2021 15:10:15 +0000

From: General Counsel

To: Infrastructure Team

Subject: MONM - Implement Logon Banners

After the investigation of a recent incident, it has become clear that we need to have a central logging facility. Select a technical solution, a software product, then configure all servers and devices to send their event logs to this central server.

Respond with a business memo that addresses:

- 1.) Which server houses the central log, why was that server selected.
- 2.) What software solution did you choose.
- 3.) Show screenshots of the configuration settings on each server and the FW that document that events are being sent to the central logging server.
- 4.) What protocol is used to send events and address the security issues that may concern you and that should be addressed in the future.
- 5.) Specifically note how were the Windows servers configured to accomplish this.

Thank you.

General Counsel