

Team: Team 1

Inject Number: 7

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 10 Nov 2018 15:16:42 +0000

From: Security Ops

To: Infrastructure Team

Subject: Configure a Centralized Logging Server

Security policies require a centralized logging service to be used for auditing purposes. It is also a good practice to keep abreast on events being logged.

Please configure all boxes to forward their logs to a central server of your choosing. You can accomplish this using native functionality or a 3rd party product. Just so long as it works Provide screenshots of a sample of the composite logs as well as screenshots of the logging configurations from all devices via the Blue Team portal. This should be a single document with screen captures clearly labeled.

Thank you.

Security Ops