Team: Team 15

Inject Number: 31

Inject Duration: 90 Minutes

Inject Start Date/Time: Sat, 02 Feb 2019 20:53:57 +0000

From: IT Director

To: Infrastructure Team

Subject: 3.3.1 using syslog-ng to Configure Centralized Logging

Installing syslog-ng on Ubuntu and Debian URL below
https://www.syslog-ng.com/community/b/blog/posts/installing-the-latest-syslog-ng-on-ubuntu-and-other-deb-distributions

Our current policy requires centralized logging services to be used. We currently lack any such service and you need to get one configured. Configure your logging solution to monitor logs for all networked devices - this includes logs from the Palo Alto Firewall.

1) Document your installation and report when completed with a screen capture of your terminal or GUI interface
2) Provide screenshots of logging configurations for each device.
3) Provide screenshots or sample composite log files showing network devices are forwarding logging.
4) Provide screenshots that demonstrate the logging server and the rest of your environment are in sync by generating a logged event on one device and comparing it to the time stamp on the logging server.

Thank you.

IT Director