MONTCLAIR STATE
UNIVERSITY

Log Management Project Plan

Compiled By:	**Joseph Santiago**

Objectives/Goals

Identify key components of logs

- List of identifiers to look out for:
  - Event ids
  - Host ids
  - Timestamps
  - Source IPs
  - Protocols
  - Access Reasons

- Create Use Cases depending on:
  - Access Reasons
  - Event ids

Build a testing environment

- Environment to test and modify existing log implementation
  - Isolated testing vm to check for integrity of graylog extractors and collectors

- Configure graylog vm to perform the following actions:
  - Deploy the ova graylog version of choice onto vm application
  - Configure graylog interface to contain a working static IP
  - Send first messages into Graylog using syslog function
  - Search for this data within Graylog and create charts or graphs
  - Create a dashboard to consolidate this data and monitor it

- Test Alerts based on the following cases:
  - Number of x vulnerabilities discovered in a scan
  - Differing severity levels output different levels of alerts
  - Configure alert intervals within graylog server.conf file

Deploy srcfire logging into live Graylog

- Create extractors, streams, update vulnerability dashboard, alerts
  - Import these from testing environment and adjust depending on live settings

Integrate logging alerts into slack

- Configure slack to display alerts to the security team with Access Reasons and Event IDs from extracted logs
  - Different alerts can go into varying channels