

Internal Memorandum

**To:** CIO

**CC:**

**From:** Sara Aladham

**Date:** 10/21/2018

**Memo #:** 007

**Re:** Follow-Up

Good Afternoon,

Team A has discovered multiple services and actions on our systems today. Each of these

discoveries have been addressed and mitigated within the given time-frame. Details below:

**Suspicious Users**

* “Managed Service Accounts”
* “Test”
* “s”
* “testuser”

**Solution**

Restrict access to the system by setting disabling each account within Active Directory Users and Computers.

**Suspicious Service**

* “TigerVNC Server”

**Solution**

Uninstalling program from the control panel.

**Updating Permissions**

* “Windows Firewall with Advanced Security”

**Solution**

Updating service value within the registry editor and starting the service to enable Windows Firewall.

If you have any additional questions, please let us know.

Regards,

Sara Aladham

Team A