1.3.1 Thomas Hughes

* Detect:
  + *When and by which user did a suspicious file get to your desktop?*
  + 3/7/2018, WIN2012R2\Administrator

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* + *Could there be other potentially malicious data on your computer? How can you find it?*
    - *Malicious data can be hidden by enabling that property and will go unseen to the naked eye. You can detect or find these potential threats by going to [view>hidden items] and looking for and inspecting suspicious files. You can also download or run some sort of antivirus software like AVG Business Security. It’s also important to check for hidden processes in the task manager and end them if necessary.*
  + *What applications and/or services could have been used to get these files there?*
    - *Executable files, scripting / programming languages, downloading / clicking on suspicious links*
  + *Are there any files missing from the computer?*

Graphical user interface, text, application

Description automatically generated

* Respond:
  + *What actions should you take to resolve the security threats?*
    - Delete any suspicious files and end any processes pertaining to the suspicious files / executables.
* Recover:
  + *How do you recover any missing data?*
    - Check the recycling bin and reinstall or move any applications you are missing
* Identify
  + The asset is your computer and its data.
* Protect:
  + *What are the security measures you should take to secure your computer and ensure this does not happen again?*
    - Make sure the windows firewall is enabled and disable any outbound file sharing or https ports that you don’t want in the inbound rules of the firewall settings.

Graphical user interface, text, application, email

Description automatically generated