INFO 710 Incident Report Guidelines

- Use the provided template to write up an Incident Report on the same malware that you choose for your Forensics project
- You can use all the same research that you have done for your project, I just want you to get the experience of writing it up into an Incident Report format, just like a Forensic Analyst would do
- Pretend that you work for the company that was the victim of this malware attack and it's your job to explain what happened to the CEO
- I would like to see a very thorough and detailed analysis of the malware attack both overall and technically – tell the story of what happened as well as providing those Forensic details like IOC's, hashes, IP addresses, compromised domains, etc.
- While it is definitely the case that as a Forensic Analyst you will never know ALL the answers to any cyber-attack, the goal is to provide as much information as you can
- If you find that your research doesn't line up exactly within the template framework, instead of leaving it mostly blank, the best solution is to write up an additional 1-page addendum explaining all of the technical information that you do know