**IR Plan**

1. Gather information and evidence – logs and screenshots
2. Create a hypothesis on what occurred based on the information
3. Determine remediation – what steps do we take to ensure the same route is not taken and eliminate any persistence
4. Execute plan
5. Detail report – summarize steps 1-4

|  |  |
| --- | --- |
| Location of Malware | give file path or registry location? |
| Method of Detection | what are our options? Anti-virus, autoruns, process table, etc. |
| Systems/services impacted | host that it was on and the services running on it if any were interrupted |
| summary | what should we specifically talk about, how we found it? or more about how it got there  At 6:21 anti-virus detected malware in word documents stored in c:\users\.... The anti-virus quarantined and cleaned the malicious file. There were no other indicators that the malware persisted. |
| mitigation | what action we took against it |