Malware Response SOP

1. Disconnect infected machine from the network
2. Perform full malware scan
3. Analyze suspicious files in sandbox
4. Re-image system if needed
5. Notify SecOps and document