Greetings Team!

I know that it’s a bit early, but I really must spring this on your team in order to get the proper process started and ready to flow.

We currently are in need of a rehaul of our incident response policy as well as our incident response forms. Please provide for me the following in your next report:

1. An incident response policy
2. An incident response form template

Your incident response form *should* have at minimum:

* Date and time of incident
* Type of incident (Malware, Breach, Other)
* Description of incident
* Source IP, IP of Breached System, and as much detail of attack vector as possible.
* Impact on services
* Impact on information (i.e. were records accessed, modified, etc.)

Basically, we need something that should tell us the who, what, when, where, why, and how.

Now I know you’re going to be pressed for time, but please ensure that if we need to report an incident that the proper forms are filled out with as much information as possible to assist in any investigation that may occur.

\*Competition NOTE: ANY IR report that is turned in without a source IP of the attacker WILL NOT be considered and WILL BE THROWN OUT!

Isaac Waterfield  
CTO