**SITREP**

**LAST 24**

* The Discovery and Counter Infiltration (DCI) analysts finished network validation, host discovery and sensor placement
* The Discovery and Counter Infiltration (DCI) analysts began monitoring and looking for suspicious network traffic
* The Discovery and Counter Infiltration (DCI) analysts began host analysis on several machines
* Senior members of the CPT started MDMP on eradication and recover efforts
* The All-Source Analyst (ASA) documented and mapped newly found IoCs

**NEXT 24**

* MDMP will be complete
* Network validation, host discovery and design assessment be complete, new map delivered to customer.
* The DCI analysts will develop a detection strategy, with the local cyber defender’s assistance.
* The Cyber Threat Emulation (CTE) operators will begin working on a plan to test new detection strategies

**Below this line, the information will be filled out by the CND Manager**

**==========================================================================**

**PRIORITIES OF WORK**

1. Complete MDMP
2. Move into eradication and recovery phase
3. Start a detection plan
4. Start a threat emulation plan to test detection plan

**ISSUES**

None