**SITREP**

**LAST 72**

*This portion of the SITREP documents significant events that happened in the past 72 hours, providing broad descriptions of what is going on. In the planning phase of operations, the staff element creates a notional timeline of the mission; this is to ensure that the CPT is staying on that timeline.*

Examples:

* CPT members have arrived on site at 1700 EST and have begun doing X, Y, and Z
* The CPT Mission Commander, along with senior members of the CPT, has conducted the interview with the mission and network owners.
* Mission analysis has begun.
* Network validation, host discovery and design assessment have been initiated.
* The Discovery and Counter Infiltration (DCI) analysts have started reviewing the network’s organic sensor capabilities to determine network visibility.
* Compliance and policy assessments have begun.
* The Cyber Threat Emulation (CTE) operators are working with the All-Source Analyst to develop threat intelligence and Indication and Warnings (I&Ws).
* The CTE operators will work with other mission elements to develop and prepare for the Participated Defensive Evaluation of the network.
* The CPT staff element is working with external organizations to provide support as needed to the CPT on site.
* The CPT on site has identified suspicious activity. They created SPOTREP 01 and created a Request for Analysis (RFA), which was sent to CNMF Battle Bridge for additional malware triage and forensics.

**NEXT 72**

*This portion of the SITREP documents what the CPT is doing in the next 72 hours, providing broad descriptions of what is going on. In the planning phase of operations, the staff element creates a notional timeline of the mission; this is to ensure that the CPT is staying on that timeline.*

Examples:

* Mission analysis will have been completed.
* Network validation, host discovery and design assessment will continue.
* The DCI analysts will develop a sensor emplacement plan, with the local cyber defender’s assistance, to provide proper network visibility
* Compliance and policy assessments will continue.
* The Threat Intelligence Report will be disseminated to the CPT on site. The ASA’s will continue to use internal and external resources to continue to develop I&Ws.

The CTE operator will continue to work with other mission elements to develop and prepare for the Participative Defensive Evaluation of the network.

* Lines of communication will be established between the CPT on site and all supporting organizations.
* CPT Mission Commander will work with the Supported Command to identify, contain and eradicate procedures based on suspicious malware and analysis.

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

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

**PRIORITIES OF WORK**

*This portion of the SITREP documents, at a high level, the mission’s priority for the next 72 hours.*

Examples:

1. Mission Analysis (Staff and command-specified mission elements)
2. Identify and Validate C-KT (Command-specified mission elements)
3. Network and Host enumeration (Command-specified mission elements, DCI)
4. Compliance, Policy, Design and Vulnerability Assessments (Command-specified mission elements)
5. Network and Host baselining (DCI, command-specified mission elements)
6. Cyber Dependency Model (Command-specified mission elements)
7. Request for Information (RFI) / Request for Analysis (RFA)

**ISSUES**

*This portion of the SITREP documents any issues that cannot be handled by the CPT Team Lead or Mission Commander. These issues will affect the overall mission if not taken care of within a reasonable amount of time. These issues may even need Higher Headquarters to intervene to accomplish the mission.*

Examples:

* The deployed CPT doesn’t have enough members to conduct the mission. Requesting additional support. Will need X, Y and Z (by name request or position request) to continue mission on time.
* The deployed CPT doesn’t have the correct tool kit to continue mission. Will need X, Y and Z (additional capabilities, tools, forensics support, etc.).
* The deployed CPT still is trying to gain access to the supported network. The Network Owner has yet to provide usernames and passwords for X number of CPT members.
* The deployed CPT does not have enough space to employ all members of the CPT. Will need to work in three shifts to adjust to space issues. Still working with the Supported Command to obtain more X, Y and Z.
* The deployed CPT has waited for X amount of time for malware analysis. Must receive malware analysis no later than X time to continue mission.