**Last Touched:**  
Analyst: \_\_\_\_\_\_\_\_\_\_\_ 🞏 AM 🞏 PM Date: \_\_\_\_\_\_\_\_\_\_\_\_  
 **Purpose:** To assist analysts in the daily processing of tickets in RTIR. The companion document, *Incident Handling Procedures* (available on Box) provides additional guidance and is authoritative for all incident handling matters.

* **1.** Review the Disconnection Ledger.
  + **1.1** Lock the *Disconnection Ledger* on Box to prevent other analysts from making simultaneous edits.
  + **1.2** Review entries that do not have an Action listed (or whose action indicate *Deferred*), and examine the **Latest Incident** and its corresponding Investigation in RTIR for new communication from the LSP/user. Update Ledger entry, along with new **Disconnect By** dates, as appropriate.
  + **1.3** Begin disconnection process for any entry whose **Disconnect By** date is either today’s date or a date in the past and whose **Action** is blank or *Deferred*.
* **2.** Process RTIR Tickets using searches and process listed in *RTIR Saved Search Procedures* (available on Box).
  + **2.1** Resolve Outstanding Tickets
  + **2.2** Claim Unassigned Tickets
  + **2.3** Bulk Reject Cruft
  + **2.4** Filter Spam
  + **2.5** Process Incidents
    - 2.5.1 Set **Type** to *Other credential compromise* for REN-ISAC Credential Compromise or SpamCop reports.
    - 2.5.2 In Ledger under **NOC Response**, list the Incident Report number of any NOC replies confirming blocks/disconnects/whitelists.
    - 2.5.3 Refer to the “Related” window in the Incident Report when handling Host Compromises to avoid duplication or misclassification of ticket type. Duplication is defined as having more than one Incident within 7 calendar days for the same host or user for the same general concern.
    - 2.5.4 Mark as **Type** *Proactive* those Incidents who were externally reported but were previously identified and reported as an Incident by the IDS.
    - 2.5.5 Send a Disconnection Warning and enter into the Disconnection Ledger individuals/systems who receive a **second notification after 7 but no later than 45 calendar days after the date of the original *Incident*.**
  + **2.6** Process DMCA
* **3.** Review reports for irregularities
  + **3.1** *Wired/Wireless Host Compromises – Last Week* should not list more than 1 Incident.
  + **3.2** *Wired/Wireless Host Compromises – Last Month* should not list more than 4 Incidents. **Any users/systems with two or more entries should be listed in the Disconnection Ledger.**
  + **3.3** Examine the **External** tickets referenced in the *Proactive vs External – Last Week/Month* queries, and ensure each ticket was properly handled.
  + **3.4** Any *Outstanding Incidents/Incident Reports* that are not consultative in nature should be resolved as soon as possible.
* **4.** Contact NOC for pending blocks/disconnects/whitelists that haven’t been responded to (as determined by having a blank field in **NOC Response** in the Ledger) within 2 days of the **NOC Request Sent** date.
* **5.** Unlock the *Disconnection Ledger*.

**References**

|  |
| --- |
| **NOC D/C Responses**  Should contain the following  fields (as applicable): |
| PennKey |
| MAC Address |
| Connection Type |
| Customer |
| Type |