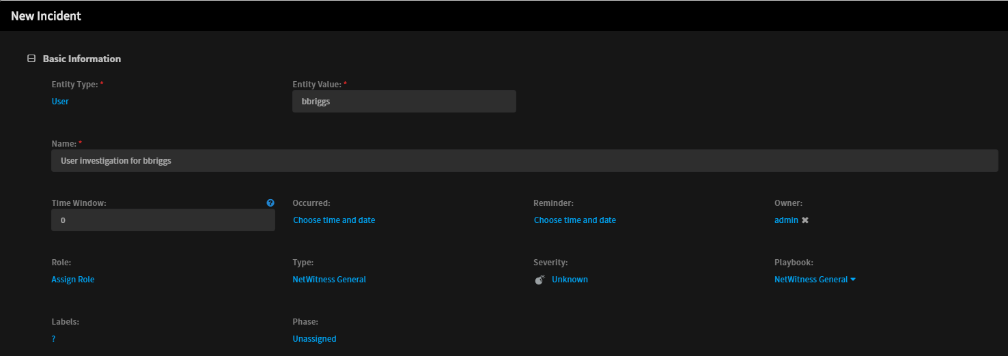
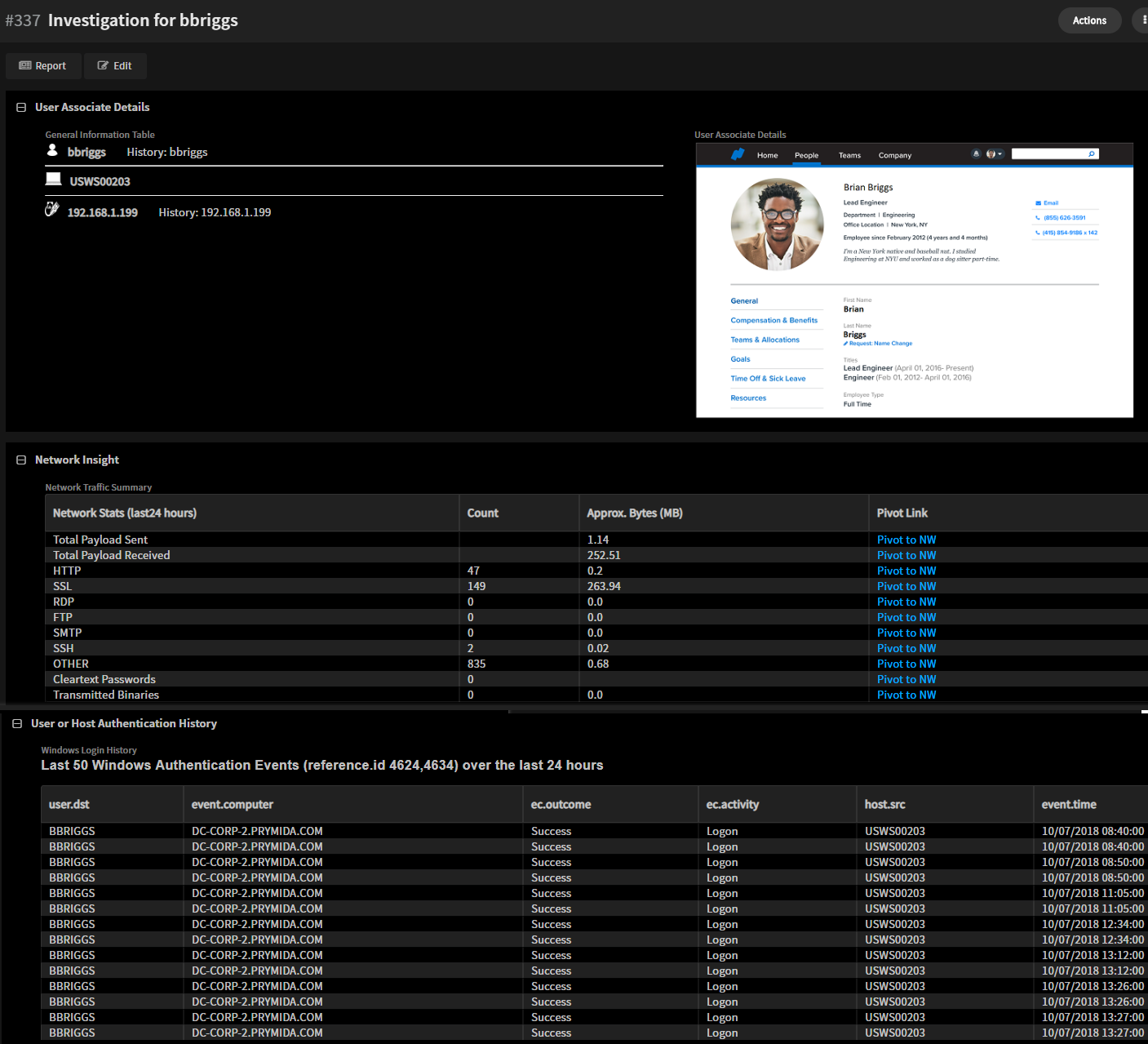
# NetWitness General Enrichment (#0106)

Primary purpose: Given an IP, Username, or Hostname, populate as much information as we can including authentication history, HR system information, and network information. Should be expanded to pull other things as well, like AV history, proxy history, etc. General framework only.





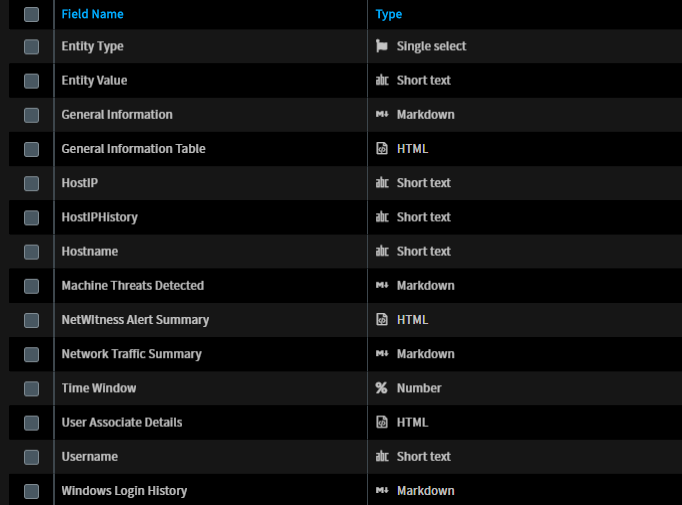
## Playbooks (new):

* “NetWitness General” – Primary Playbook
  + Inputs (before first run, playbook must be modified as part of top task heading)
    - nwourl (Orchestrator base url ex. <https://192.168.1.153>)
    - netwitnessurl (Netwitness investigation base url ex. <https://192.168.1.129/investigation/12/navigate/query/>)
    - netwitnessrespondurl (Respond base URL ex. <https://192.168.1.129/respond/incident/>)
* “NetWitness Enrichment” – Sub Playbook
  + Current Querys for and Populates:
    - Authentication Logs (Uses windows event 4624)
      * Populates Auth History
      * Populates Entity Info given IP, Username, or Hostname
    - Network packet history (all services)
* “Extract Info From NetWitness Alerts” – Sub Playbook

## Automations (new):

* “NetWitnessEntityInfo”
* “NetWitnessNetStats”
* “NetWitnessQueryToTable”
* “LastImageToField”

## Fields (new – sample incident layout also provided)



## Instructions

1. Create a new incident type called “NetWitness General” (you can use other names as well, you’ll just have to modify the incident fields json and search/replace the mapped incident name). Or create the fields manually if you don’t want them locked to a specific incident type.
2. Import custom fields:
   1. “incidentfields\_0106.json” in Settings > Advanced > Fields
3. Import all 3 layouts and map to NetWitness General (Settings > Layout Builder):
   1. “layout-details\_0106.json” > Incident Summary
   2. “layout-edit\_0106.json” > New/Edit form
   3. “layout-quickView\_0106.json” > Incident Quick View
4. Import custom automations
5. Import sub playbooks
   1. “Extract\_Info\_From\_Netwitness\_Alerts.yml”
   2. “NetWitness\_Enrichment.yml”
6. Import main playbook:
   1. “NetWitness\_General.yml”
7. Map the new playbook as a default playbook for the “NetWitness General” incident type

## Data Required to Populate:

* Windows Event log 4624 including username, hostname, IP address
* Network data associated with IP Address