NSOC Incident Central

Create new tab called “IDS/SIEM Workflow”

**Create section for schedule and escalation contact**

* Static data for duty coverage based on Srini’s schedule rota
* Static escalation detail with Charles Kim and Srini splitting the horizon for support.

**Create Section for SOP**

* Content will be links posted by Ken Skorupski
* Standard templates to be used for all documentation; Process, Reference, and Instruction

**Create Section for Shift Turnover**

* Add Shift Turnover Form
  + - Shift Detail
      * Date Selection (Date Picker)
      * Shift Selection (A, B, C)
    - Offenses Detail
      * Offenses generated in shift (Free Text)
      * Offenses Processed (Free Text)
      * Last Offense # (Free Text)
    - *Escalated Offenses*
    - *Offenses no (Free Text)*
    - *Date Selection (Date Picker)*
    - *SR# (Free Text)*
    - *Offense description (Free Text)*
    - *Escalated by ‘Username’ (may be from SSO or Free Text)*
    - *Action Taken / Comments (Free Text) – to be entered the shift analyst (or) Charles Kim/ Srini*

* + - Sensor Issues
      * New Issues
        + Select IDS device
        + If device selected, provide Free Text field for comment
      * Known Issues
        + Carry over entry from past report

OR

* + - * + Select IDS device
        + If device selected, provide Free Text field for comment
* Provide report/list for past shift turnovers