**Data model considerations**

* Data from intrusions should be immediately tagged to items in the playbook. Make sure your technology choice, custom or COTS, enables this to save time.

**Playbook structure**

|  |  |
| --- | --- |
| **Group name** | |
| **Threat rating** | Very low – very high, use one value that immediately showcases the sense of urgency. |
| **Aliases** | Write down all the other names you know. |
| **2 Row summary** | Max 2 row description of the group. |
| **Actor categorization** | Your internal classification of threat actor groups. Basically your setup of types or categories of groups. |
| **Actor motivation** | Your internal classification of motivations. |
| **Sophistication rating** | Your internal rating to classify their sophistication. |
| **Assessment** | Your analyst team’s assessment on the group. |
| **Activity sightings** | Forecasted yes – forecasted no – sighted yes – sighted no – No assessment yet |
| **Last known and disclosed activity** | Note down the campaign trail of the group. Carefully maintaining this and integrating with other vendor tooling can support you with building a data set between ‘activity sighted in the wild’ and ‘activity sighted in the network’. |
| **Behavioral identifiers** | Applying MITRE’s ATT&CK framework to breakdown. You can apply this both for the group’s behavior or for the tools they utilize   * Tactics * Techniques * Sub-techniques |
| **Key identifiers** | Apply concepts such the cyber kill chain, ATT&CK or Diamond model to identify core identifiers that recognize this group. |
| **Tools** | Breakdown the tools used by this particular group. Preferably correlated with content seen in your intrusion sets. |
| **ATOMIC understanding** | IOC oriented stuff, such as   * Domains * Hashes * etc |