# HUNTING WIKI

Use this document to plan your hunting wiki. This should be a shared resource accessible by all analysts in your organization. You'll be tempted to restrict edit access to senior analysts but resist that urge. Learning how to document useful hunting information is a skill everyone should work towards developing from the start.

Organizing Principles:

- Each section should be organized for browsing or a data dump for searching.
- Every analyst/hunter should have open read and edit access to the wiki.
- Use of the wiki should be required and integrated into a hunter's workflow.
- The software that facilitates the wiki should be:
    - Simple: You don't need a lot of fancy features
    - Resilient: An open model requires tracking and reversion capabilities.
    - Secure: The knowledgebase contains sensitive information and should be protected with role-based access control and two-factor authentication.

## SECTION 1: EXPEDITIONS

This is an area to document notes from specific hunting exercises. You or others will likely revisit this content as you revisit hunting approaches.

Structure

`Attacks`

- `Credential Theft`
- `HTTP C2`
- `LNK File Downloads`
- `More Attacks`

`Data`

- `HTTP User Agent`
- `OS Execution Logs`
- `Zeek Downloaded MIME Types`
- `More Data Fields`

Individual Page Content

- `Searches`: The useful searches you conducted during the expedition.
- `Data Transformations`: The other data transformation that were useful.
- `Code`: Any code you created or found for parsing data.
- `Explained Anomalies`: A brief explanation for any legitimate anomalies you found.
- `False Positives`: Anything initially assume malicious but later explained.
- `Reference Links`: For ABH, examples of attacks that drove your expedition. For DBH, reference material related to the data source.

## SECTION 2: BEHAVIORS

This is an area to document common or atypical behaviors of applications, users, and systems. Anything that caught your attention that you might reference later should go here.

Structure

- Applications
  - Skype
  - Web Backup Software
  - More Applications
- Users
  - csanders
  - jsmith
  - More Users
- Systems
  - WEB70
  - Sales Laptops
  - More Systems

Individual Page Content Examples

- Web Backup software uses port 9001 and has a large upload:download ratio
- Developer workstations often setup temporary web servers for dev testing
- nettech is a service account used by our Cisco consultants
- jcalipari is in sales/recruiting and travels a lot. He often logs into the VPN from a lot of places in a short time.
- The encrypted p989 traffic going to the 97.21.*.* range is update traffic for the HVAC management app

## SECTION 3: UNSOLVED MYSTERIES

This is an area to document behaviors that you haven't been able to explain. You can dump anything into this area. Everyone should subscribe to this page so they can see new additions in case they have an explanation.

Structure

This can be a single page, or you can divide it by applications, users, and systems.

- Applications
  - What is csupdate.exe?
- Users
  - Purpose of frequent visits to abcxyz.com over HTTPS for accounting users
- Systems
  - Encrypted UDP 443 traffic on DB servers

Individual Page Content Examples

- What is the source of this encrypted traffic?
- Why does this user do that?
- How does this process work?
- Is this thing normal for that user?
- Is it okay for this user to be standing up that service?