Data Suitability Checklist

1. Do you have access to multiple passive data sources? In particular:
    a. Do you have a high-speed abstract data source like NetFlow?
    b. Do you have any full packet capture capability?
    c. Do you have access to server logs?
    d. Do you have access to physical access logs, camera records, etc.?
2. Do you have external visibility into your network?
    a. Can you differentiate internal from network facing resources?
    b. Can you identify what's reachable by search engines, crawlers or scanning?
        i. Including what shouldn't be?
3. Are you aware of unloggable assets, and can you compensate with collection next to the asset?
4. If new assets appear on your network, how soon do you identify and instrument them?
5. Do you collect data actively? In particular:
    a. Do you have a host-based collection system in place?
        i. More than AV?
        ii. Are you auditing your host-based collection?
    b. Are you actively scanning your network?
        i. How often do you scan?
        ii. How often do you review and update your scans to keep current with changes or new threats?
6. If you are working with cloud-based collection, how familiar are you with their monitoring and collection systems?
7. How far back do your data sources go? Can an analyst acquire information back 30 days? 60? A year?
8. Are your firewall, router, and other security/networking configurations under source control? Can an analyst recover your security posture back 30 days? 60? A year?
9. Do you have tools to manipulate the data?
    a. Can an analyst take a nonsignificant cut of data and work on it without interfering with normal operations?
    b. Are the tools used commonly understood by your ops team?
10. Do you have common formats for your data?
    a. Are you sure everything is synchronized?
        i. Really?
    b. Is your threat intelligence data easily digested for this purpose?

Operational Suitability Checklist

1. Do you have an audience for threat hunting?
    a. Is that audience the SOC?
    b. Is that audience the users?
    c. Is that audience IT outside of security (particularly the NOC)?
    d. Is that audience the C-suite?
2. Do you have a working threat intelligence program?
    a. Are you already contributing to a threat intelligence program?
3. Who will vet the hunting results?
4. What is the operational impact of a hunter working on hunting?
5. Can you support multiple hunters?
6. Do you have a well-defined set of development tools?
    a. Does your security team have dedicated developers?

Personnel Suitability Checklist

1. Can the candidate hunter work without a fixed workflow?
2. Can the candidate hunter search through Google or other search engines to find information?
   a. Can they read RFCs?
   b. Can they search through newsgroups?
   c. Will they crack open a book?
   d. Will they talk to a person if necessary?
   e. Can they set up an experiment to test an idea?
3. Is the candidate hunter familiar with the structure of your network?
   a. Have they discovered weird features of the network?
4. Is the candidate hunter familiar with your organizational goals?
5. Is the candidate hunter capable of writing code on their own?
   a. Can the candidate hunter set up tools and systems if they need something that isn't present?
6. Can the candidate hunter communicate their results?
   a. Can they communicate the intent of that code to a competent developer?
   b. Can they communicate the result of a hunt effectively to nonsecurity personnel? To network operators? To the C-suite?
7. Can the candidate hunter take criticism constructively?
   a. Can the candidate hunter admit they were wrong?
   b. Can they defend their ideas effectively?