Q: what are we collecting? Types of devices and software? Data from those?

Can we just wrap around an existing open-source tool?

Add Medcurity branding

Filter results for what we care about / is relevant

Prune before adding to DB, exporting to CSV, displaying in UI, formatting to Excel

Open AudIT

* Open-AudIT is an application to tell you exactly what is on your network, how it is configured and when it changes.
* is a database of information, that can be queried via a web interface
* Data about the network is inserted via a Bash Script
* queried for hardware, software, operating system settings, security settings, IIS settings, services, users & groups and much more
* Network devices (printers, switches, routers, etc) can have data recorded such as IP-Address, MAC Address, open ports, serial number, etc, etc.
* Output is available in PDF, CSV and webpages. There are export options for Dia and Inkscape.
* Open-AudIT can be configured to scan your network and devices automatically. A daily scan is recommended for systems, with network scans every couple of hours. That way, you can be assured of being notified if something changes (day to day) on a PC, or even sooner, if something "new" appears on your network.
* We can add to Open source version; or we can recommend paying for it (FirstWave) is cheaper than paying developers to make custom – depends on needs

Manage Engine

* Only windows (?)
* Software and hardware
* Less customization, ability to wrap/api/query/format/etc

SpiceWorks is another option

Lots of information on web crawlers, not so much on network/device/software crawlers

10/10

No need to “crawl” with a “crawler”, just iteratively/systematically query, asking for info

We can use the IT/admin directory if applicable, maybe

Else use nmap??

Use nmap to get network device / os information, then have client add additional information using the GUI to fill out spreadsheet