



# NOMADS

## Navy Operational Machine Auditing Development Suite

Nick Arenberg, Matthew Chen, Andy Ho, Nick Mattair, Max Medearis

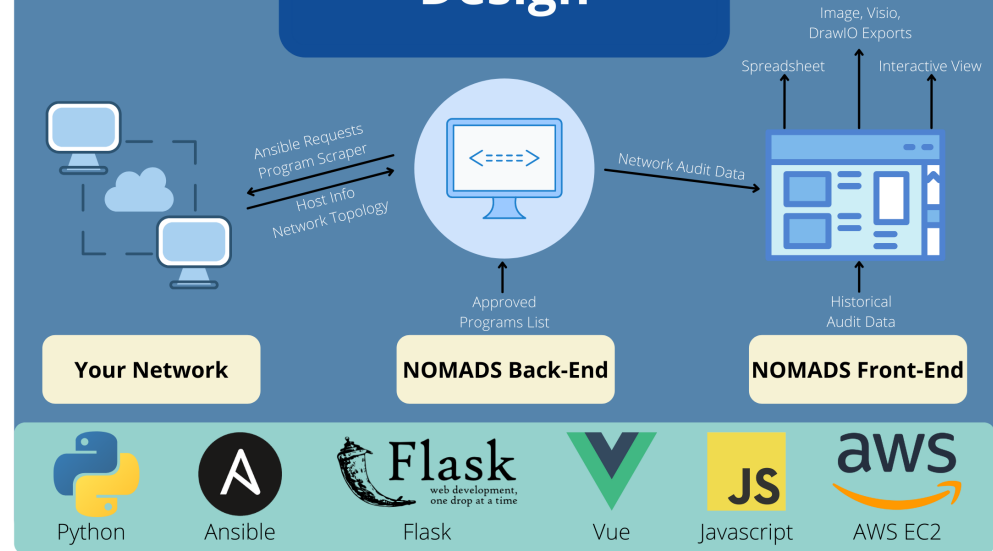
### Motivation

- Cyber-crimes cost the global economy **1 Trillion** dollars per year.
- **445 Million** cyber-attacks occurred in the first half of 2020.
- Large organizations have **millions of computers** that must be secured.
- Manually searching each computer would take years.
- Human security talents are wasted on data collection.
- NOMADS thwarts attacks and increases the efficiency of security teams.

"The Navy needs process automation and visualization to audit system state, network scanning to enumerate network design, ports, protocols. Nothing does all of the above or provides it in the format we need"

- Michael Cloud, TTSD DISSM NAWCWD

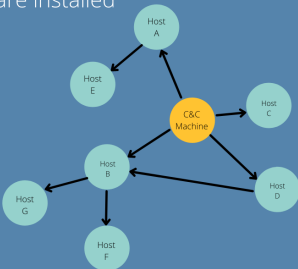
### Design



### Solution

#### Fetch

- NOMADS builds a tree of hosts on the network using methods with varying levels of intrusiveness based on user preference
- It then audits those hosts to determine the hardware and software installed



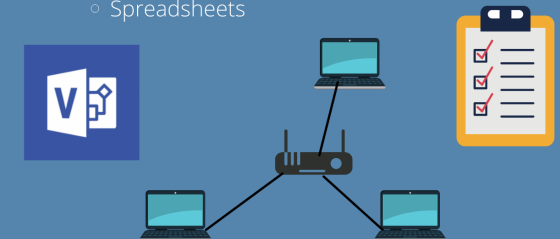
#### Process

- Retrieved data is flagged appropriately based on a provided list of approved programs.
- Data is then stored into json data dumps and parsed into human readable spreadsheets



#### Present

- NOMADS UI displays processed information into a variety of different formats.
  - Topological Network Diagram
  - Hardware/Software Lists
  - Spreadsheets



Special thanks to Jianwen Su, Chandra Krintz, and Mason Corey from UCSB



Special thanks to Mike Cloud, Doug Bradley, Kevin Burk, and Angel Zamarron from NAWCWD and NAVAIR