Continuation of the VA Security Operations Center (SOC)

Team members: Nixy Camacho, Masrik Dahir, G Attard, Jack Watkins | **Faculty Advisor/Mentor:** Robert Dahlberg | **Sponsor:** VA Department of Elections (ELECT)

Problem Statement

- Small businesses make up 44% of total U.S GNP
- Most are not equipped with cybersecurity teams or professionals

Existing Solutions

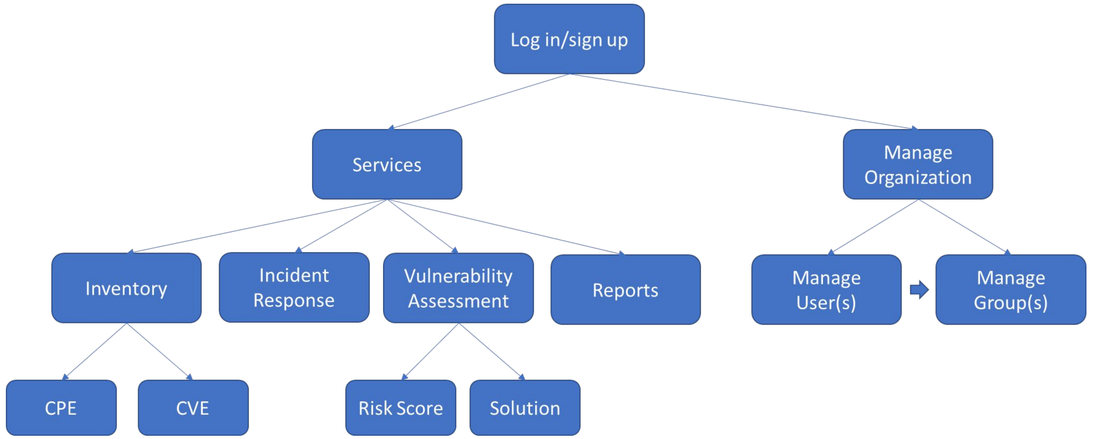
- Antivirus software
- VPNs
- Other services – *not* cost-effective for small businesses

Social Value

- **To provide** businesses with an easy-to-use *Security Operations Center* (SOC) to safeguard the integrity, confidentiality, and availability of their IT systems and data.
- Service-Oriented Engineering:
  - Needed services can be implemented as customers request

Illustrations

Entity-Relational (ER) Diagram



CPE/CVE Inventory Reporting (Example)

CPE ▸ CVE

CVEs

Add

Show 15 entries Search:

	CVE ID	Published	Last Modified	Status	References	Problem
::tablet_pc:*:x64:*	CVE-2019-5620	2020-04-29T23:15:13.033	2020-05-06T18:18:07.373	Analyzed	https://www.rapid7.com/db/modules/exploit/windows/scada/abb_wserver_exec	ABB MicroSCADA Pro SYS600 version 9.3 suffers from an instance of CWE-306: Missing Authentication for Critical Function.

Previous 1 Next

Services/Features

1. **<u>User/Organization</u>** sign-in accounts
   - Securely encrypted (hashed) user passwords stored in backend database
2. **<u>Inventory</u>** for any 3rd-party services & software used by business
   - On-demand, up-to-date vulnerability (*CVE* & *CPE*) reports for 3rd-party products, [via *<u>NIST</u>* APIs*]
3. **<u>Vulnerability Assessments</u>**
   - Report to organization about risk factor(s)
4. ***<u>Escalated</u>* <u>User Privileges</u>**:
   - <u>Admins</u>: Manage Organization User(s), Group(s)
   - <u>Regular user</u>: Basic access to services

Technologies Used:

*APIs used from:

NIST National Institute of Standards and Technology

http://vcusoc.com