**GONZAGA UNIVERSITY**

**School of Engineering and Applied Science**

**Center for Engineering Design and Entrepreneurship**

**Medcurity Network Inventory**

**Project Overview**

**Plan Section 01**

**Release:**

**Draft v0.2**

**PROJECT PLAN DRAFT STAGE DOCUMENT**

**October 1, 2023**

**Medcurity Network Inventory Team**



**Brandon Huyck**

**Colleen Lemak**

**Artis Nateephaisan**

**Jack Nealon**

**1 Project Overview**

**1.1 Project Summary**

*Provide a clear and concise two-paragraph summary of your project. The first paragraph of the summary must provide a high level description of your project’s “why” (i.e., the problem the project is trying to address) and the second paragraph your project’s “what” (i.e., how your project is going to address the problem). The summary should be written for someone who is unfamiliar with the project domain (including jargon used within the domain).*

Online scammers and hackers are capable of causing serious damages. Whether motivated by ransom money, identity theft, or power and status, attackers are able to leverage their unauthorized access to systems, placing individuals and companies at high risk for digital security breaches and malicious attacks. Notably, these targeted attacks are strategic, and mainly aim to exploit large amounts of sensitive and private data. Thus, to be proactive, professionals in a data-driven field must allocate and invest in resources to engineer layers of security. For instance, implementing these security precautions will allow professionals in the medical industry to ensure private medical records are kept confidential and to protect client safety and data. Adhering to medical record compliance protects sensitive patient health information from being disclosed without patient consent or knowledge and thus follows our Sponsor’s mission of helping clients meet their federal digital security standards, known as *HIPAA* standards.

Our software inventory tool implements security precautions with an authentication process, requiring that an administrator or client enter correct credentials to access the tool. Next, the tool will send out a special agent that scans the client’s network and adds its information discovered to our database. The agent is looking for server identification addresses, information about devices on the network, location of the server, and encryption methods, among other attributes. After data has been loaded into the database, we give the user access to an exportable customized spreadsheet report that details the information discovered. Identifying devices and software within the network domain will demystify connections that may be unsafe to allow into the network. To ensure clients will only be able to access their own information, the tool will link client information to only their accounts, reinforcing authentication and checking the user has access to their information and no one else’s.

**1.2 Project Objectives**

*Provide a description of the major project business objectives (i.e., business goals/desired outcomes of the project). Be sure each objective is concrete, specific, measurable, and has been vetted with your project sponsor/liaison.*

The main desired outcome of the Medcurity Network Inventory Team is to develop a new tool that complies to HIPAA standards and can be used by the sponsor to help in their goal of organizing, managing, and controlling the numerous tasks healthcare organizations are responsible for. The tool must be able to scan a client’s network for devices that are currently connected to it and identify the client’s needs and diagnose issues. While the solution is a standalone product, it should work seamlessly with the sponsor’s current environment and should be easy to understand, access, and deploy. The resulting product should be able to output customized reports, either through a CSV file or Microsoft Excel spreadsheet, that have filtering capabilities and be easy to read. Documentation is necessary in order to allow future developers to understand the code and sufficient testing is necessary to ensure the project works as expected.

**1.3 Project Stakeholders**

*Provide a brief description of the main stakeholders of the project. This should include yourselves as developers, your project sponsor and liaison, your faculty advisor, your design advisory board members, and the target user communities you are building your product for (note that there may be multiple potential user communities being targeted). For each concrete project stakeholder, be sure to include their affiliation (organization) and their role in the project. Describe your target user communities in enough detail to give the reader confidence you understand the needs of these groups relevant for your project.*

The main stakeholders of the project include our Liaisons, Rachel Kunkel and Amanda Hepper, who are both directly affiliated with Medcurity. They are responsible for communicating with the Medcurity Network Inventory Team, relaying specifications for the project, and addressing any overall questions the team may have.

The design advisory board (DAB) member, Richard Weeks, who works at F5 as a version control specialist, is responsible for giving advice and guidance. Since the DAB members have had experiences in past projects and qualifications, they are able to provide a different perspective to the rest of the team and are able to help solve specific technical issues the team may run into.

Similar to the DAB member, the advisor, Mike Mudge, who is a senior manager at Avista, provides guidance to the team. Unlike the DAB member, the advisor is responsible for guidance relating to the high-level aspects of the project. They are also responsible for evaluating the team’s progress, routinely checking up with them to ensure they are on pace to complete their project.

The main developers are the students at Gonzaga University, Brandon, Colleen, Artis, and Jack. They are responsible for the majority of the project work and are expected to collaborate through good communication, organization, and providing unique perspectives to any given scenario. Their work and their process aligns with what their future career will potentially look like.

Along with the DAB member, the Medcurity IT department members are the ones likely to provide the team specific information regarding the content of the project. Since they are responsible for upholding the current software systems at Medcurity, they will be able to give tips and warnings on how the team will integrate the new software tool that will become a part of their current system.

The network management departments are a part of the general industry. The team’s work is going to contribute to Medcurity’s systems, which are involved in the network management systems. This means it is important to consider the general industry standards relating to this subject when the team is assembling their software solution as it may lead to unforeseen circumstances. Medcurity also has a lot of clients so they must be accounted for when developing the project.

**1.4 Project Deliverables**

*Provide a brief description of each project deliverable. The main deliverable will be the software product you are developing. Other deliverables may include software documentation (e.g., a users or developers manual), a software installer, performance evaluation results, maintenance plans, etc. For each deliverable give a description of what it will generally include and how it will be delivered and/or deployed.*

The main deliverable will be the software tool as described in 1.2 and 1.5. This includes a network crawler agent, a database, an Excel spreadsheet, and a UI. The network crawler agent and the UI will be packaged to be executed as a bash command. When the command is executed, the UI will pop up, triggering the network crawler agent; when the agent is complete, it will export its findings to the Excel spreadsheet. The database will be hosted in the cloud on AWS. In addition, documentation for users and future developers, testing methods and results, and a report describing the future work that could be added will be provided. All of this will be submitted via a Git repository with a README.md file.

**1.5 Project Scope**

*Provide a brief description of the project scope that states what aspects of the project already exist (out of scope) versus what aspects you will be developing from scratch (in scope). Your description must be accompanied by a high-level context diagram, highlighting the components that are outside of the scope of your project and how they will generally interact with your system.*

This project is a stand-alone tool, and as such there are minimal out-of-scope aspects to consider. It has four in-scope features: the agent that scrapes the network for devices and software, the database that stores the devices and software that the agent finds, the UI that displays status and results and offers minor user interaction functionality, and the Excel spreadsheet that will be generated from the database. There is not any existing software that our tool will need to be integrated into. Perhaps noteworthy, our database will be MariaDB using MySQL hosted on AWS, all of which could be considered out-of-scope.

|  |
| --- |

**Figure 1**

**1.6 Related Work**

*Provide a description of existing systems and/or approaches that try to solve a similar problem as yours. Identify and describe the system most-closely related to the one you are planning on building, discussing both the similarities and the differences between this system and yours. Additionally, summarize the major similarities and differences of those less related, but still similar to your project. The goal of this section is to show that you have examined and understand the product landscape and have a clear idea of the needs of your project and how they are similar and different to the current systems/approaches available. Provide a link or reference (as a footnote) to each system you describe.*

As a main component of our project, working with security and IT management, there are many software development companies that invest in and offer network scanning and device-tracking applications along with supporting management software.

Auvik[[1]](#footnote-0) —

The network management system offered by Auvik Networks provides real-time network discovery and mapping by collecting data from various sources allowing users to visualize their network's structure and understand how devices are connected, mirroring our project plans. Additionally, Auvik automates inventory and documentation, capturing information including the device’s make, model, serial number, IP address, and switchport connections. These additional features lie outside of our current project plans but could potentially be implemented after initial designs with sponsor’s permission. Lastly, the Auvik program assists in hardware lifecycle management by identifying devices that may need upgrades or replacements. It retrieves data about support contracts, available software updates, security patch eligibility, and device availability for purchase. This feature will also not be included in our project plans.

Famatech[[2]](#footnote-1) —

Provided by the Famatech corporation, the “Advanced IP Scanner” shows all the connected network devices and provides remote control of computers via RDP and Radmin. Additionally, the program also gives the user access to shared folders. Comparing this software to our project, the only major difference is that the Advanced IP Scanner uses Radmin, a third-party company, for remote connection.

SolarWinds[[3]](#footnote-2) —-

The “User Device Tracker” offered by SolarWinds shares some close similarities with the plans we have for our project and has some shared functionality. Altogether, shared functionalities include the ability for the client to identify users and devices on their network with a comprehensive network topology and store that in a database for further analysis. Additionally, the SolarWinds program offers an active directory integration with an interactable interface allowing the user to whitelist hosts, track sensitive or suspicious devices and remotely turn switch ports on and off. As for current plans, this additional functionality offered by the SolarWinds program is not planned for our project, however, can be added as potential features to be added after initial development.

1. Auvik Network Management - <https://www.auvik.com/features/> [↑](#footnote-ref-0)
2. Famatech Advanced IP Scanner - <https://www.advanced-ip-scanner.com/> [↑](#footnote-ref-1)
3. SolarWinds User Device Tracker - <https://www.solarwinds.com/user-device-tracker> [↑](#footnote-ref-2)