**A logo with colorful ribbons

Description automatically generated**

**Austria, Gian Carlo**

**Maddela, Aireen**

**Taule, Love**

**Southern Alberta Institute of Technology**

**Spring 2025 Capstone Project (PROJ-309-ISA)**

**Assignment 2 – Business Case**

**Piyushi Singh**

**May 14, 2025**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Problem Statement** | | **Solution Statement** | | **End Users** | | **Other Stakeholders** | |
| *How would you describe the problem that your project will solve?*  *Cybersecurity threats, such as phishing emails, malicious files, and vulnerable websites, pose significant risks to individuals, students, and organizations. Existing tools often lack integration, user-friendliness, or accessibility, making it challenging for non-experts to proactively detect and mitigate these threats. Students and small organizations, in particular, need an affordable or free website, web-based solution that simplifies threat detection and enhances security awareness without requiring advanced technical expertise.* | | *What is a brief description of your high-level solution to the problem?*  *Our SaaS platform, delivers a web-based cybersecurity toolkit with three specialized tools: an Email Analyzer to detect phishing and malicious content, a File Integrity Checker with visualization and collaboration features, and a Website Checker for evaluating website security and availability. Powered by the VirusTotal API, our tool provides an intuitive, accessible, and integrated solution to empower users to proactively combat cyber threats.* | | *Who are the end users that would use your product?*  *Students: To protect against phishing emails and malicious files in academic environments.*  *Small Businesses: Seeking affordable cybersecurity tools to secure communications and assets.*  *Educational Institutions: To enhance campus cybersecurity and educate users on threat detection.*  *Individual Users: Non-technical users needing simple tools to verify emails, files, and websites.* | | *Who else would be relevant to your idea? Include potential vendors, coaches, instructors, team members, industry members, sponsors, etc.*  *Vendors: VirusTotal (API provider)*  *Coaches/Instructors: University professors or cybersecurity mentors to guide development.*  *Team Members: Developers, UI/UX designers, project managers, and product testers.*  *Industry Members: Cybersecurity professionals for feedback and validation.*  *Peers: Fellow students for user testing and collaboration.* | |
|  | | | | | | | |
| **Competitive Analysis** | | **Differentiator** | | **Elevator Pitch** | | **Assumptions** | |
| *Who are the competitors that have similar solutions, and what is a one-line description of their solution?*  ***Barracuda Sentinel****: AI-based email protection against phishing and impersonation attacks.*  ***Malwarebytes****: Endpoint security with file scanning and threat detection capabilities.*  ***SiteLock****: Website security platform with malware scanning and vulnerability checks.*  ***Mimecast****: Cloud-based email security with phishing and attachment protection.*  ***Qualys****: Cloud platform for vulnerability management and website security assessments.* | | *How will your solution be better/different from the competitors?*  *Our Tool stands out by offering an integrated, web-based toolkit tailored for non-experts, combining email, file, and website security in a single, affordable platform. Unlike competitors, it emphasizes user-friendly interfaces, educational features for students, and collaborative tools like policy creation and activity logs, all enhanced by VirusTotal’s robust API for real-time threat detection.*  *Our tool will generate a comprehensive report summarizing the requested information, presented through an intuitive, detailed dashboard and user-friendly interface.* | | *What is your 30 second pitch to peak the interest of someone who has never heard your idea?*  *A new tool is an intuitive, all-in-one cybersecurity platform that empowers everyone—students, businesses, and individuals—to stay safe online. With tools to analyze emails for phishing, verify file integrity, and check website security, it uses VirusTotal’s API to block malicious content and vulnerabilities. Accessible, affordable, and designed for non-experts, our tool delivers peace of mind through a sleek dashboard. Join us to simplify cybersecurity and protect what matters!* | | *What are you assuming to be true, that if not could have a significant impact on your ability to execute this project?*  *API Availability: VirusTotal’s API remains accessible for student projects.*  *User Adoption: Non-technical users will find the platform intuitive and valuable.*  *Team Skills: Team members can learn required technical skills (e.g., API integration, UI design) within the project timeline.*  *Data Privacy: Users will trust the platform to handle sensitive data securely.* | |
|  | | | | | | | |
| **Major Milestones** | **Technical Skills Requested** | | **Industry/vertical specific knowledge required** | | **Professional Skills required** | | **Constraints** |
| *What are the major milestones of your project?*  *Project Planning (Week 1-2): Define requirements, assign roles, and finalize tech stack.*  *Prototype Development (Week 3-6): Build MVP for Email Analyzer, File Integrity Checker, and Website Checker.*  *API Integration (Week 7-8): Integrate VirusTotal API for threat detection across tools.*  *UI/UX Design (Week 9-10): Develop user-friendly dashboards and GUIs.*  *Testing & Iteration (Week 11-12): Conduct user testing with peers and refine based on feedback.*  *Presentation Preparation (Week 13): Create demo and pitch for professors/peers.*  *Deployment (Week 14): Launch SaaS platform on cloud hosting and generate results.txt report.* | *What technical skills are required for this project?*  *Programming: Python (backend logic)*  *JavaScript (frontend), HTML/CSS (UI)*  *API Integration: Experience with REST APIs (VirusTotal API).*  *Cloud Computing: Knowledge of AWS, Azure, or similar for SaaS deployment.*  *UI/UX Design: Tools like Thinkter for creating intuitive dashboards and GUIs.*  *Cybersecurity: Understanding of phishing, file integrity, and website security concepts.* | | *What skills and industry knowledge are required to complete the project?*  *Cybersecurity Fundamentals: Knowledge of phishing, malware, and website vulnerabilities.*  *SaaS Architecture: Understanding of web-based software delivery models.*  *Network Security: Familiarity with DNS, ping, traceroute, and server analysis.*  *Data Privacy: Awareness of GDPR and other privacy regulations for user data.*  *Threat Intelligence: Experience with threat detection tools like VirusTotal.* | | *What professional skills will be required to complete this project?*  *Teamwork: Collaborating effectively across development, design, and testing roles.*  *Project Management: Planning, scheduling, and tracking progress using tools,*  *Communication: Presenting ideas clearly to peers, professors, and stakeholders.*  *Problem-Solving: Addressing technical and design challenges creatively.*  *Leadership: Taking initiative to lead sub-teams or mentor peers.*  *Time Management: Balancing project work with academic and personal commitments.* | | *What do you already know to be true that impacts your ability to complete the project (e.g. course schedules, completion dates, etc)?*  *Timeline: Must be completed within a semester (14 weeks) for presentation to professors.*  *Budget: Limited funds for API subscriptions or cloud hosting; reliance on free tiers.*  *Skill Gaps: Team members may need to learn new tools (e.g., VirusTotal API, web deployment).*  *Course Schedules: Team availability may be restricted by classes and exams.*  *Scope: Must balance feature richness with feasibility for a student project.* |

## Part One: The Template

## Part Two: Product Backlog

Complete the product backlog based on the end users and stakeholders identified in Part One. Anything with priority status must be part of your minimum viable product.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User Story ID** | **As a…** | **I want to be able to…** | **So that…** | **Priority** | **Sprint** | **Status** |
| 1 | Developer | Create a flowchart as a guide for coding | Plan and streamline the development process for the SecureSuite platform | 1 |  |  |
| 2 | Developer | Create Python code that implements the Email Analyzer for phishing detection | Enable users to detect phishing emails effectively | 6 |  |  |
| 3 | Developer | Build an interactive dashboard for visualizing malicious files | Verify the connectivity and potential malicious attacks | 11 |  |  |
| 4 | Developer | Gather information on how to integrate the tools we individually created into one | Build a cohesive SaaS platform with seamless functionality | 2 |  |  |
| 5 | Developer | Research the framework | Select the best tools and technologies for developing SecureSuite | 3 |  |  |
| 6 | Developer | Find a web server available | Host the SecureSuite platform reliably in the cloud | 5 |  |  |
| 7 | Developer | Integrate the VirusTotal API into the Email Analyzer and File Integrity Checker | Enhance threat detection capabilities across multiple tools | 10 |  |  |
| 8 | Developer | Develop a user-friendly GUI for the Website Checker | Provide users with an intuitive interface to perform website security checks | 8 |  |  |
| 9 | Project Manager | Create a project timeline with milestones | Ensure the team meets deadlines for developing SecureSuite | 4 |  |  |
| 10 | Project Manager | Track team progress on development tasks | Identify and address any delays or blockers promptly | 13 |  |  |
| 11 | Project Manager | Facilitate team communication and collaboration | Ensure seamless integration of the Email Analyzer, File Integrity Checker, and Website Checker | 12 |  |  |
| 12 | Project Manager | Present project updates to stakeholders (e.g., professors, sponsors) | Demonstrate progress and gather feedback to improve SecureSuite | 36 |  |  |
| 13 | Tester | Verify if the ping function is working and showing results | Ensure the Website Checker provides accurate connectivity results | 24 |  |  |
| 14 | Tester | Verify if the scanning of links within email is working | Ensure the scanning functions correctly and showing correct results | 22 |  |  |
| 15 | Tester | Verify if the traceroute function is working and displaying accurate results | Ensure the Website Checker correctly traces network paths to identify potential issues or attacks for users | 26 |  |  |
| 16 | Tester | Verify if the Website Checker’s homepage content validation is working and displaying accurate results | Ensure users can trust the Website Checker to identify safe and legitimate website content | 30 |  |  |
| 17 | Tester | Verify if the file scanning functionality within the Email Analyzer using VirusTotal is working and showing results | Ensure users can reliably detect malware or malicious content in email attachments | 19 |  |  |
| 18 | Tester | Verify if the Email Analyzer’s phishing detection through email header analysis is working and providing accurate results | Ensure users are protected from fraudulent emails by confirming the Email Analyzer’s effectiveness | 17 |  |  |
| 19 | Tester | Verify if the DNS security check functionality in the Website Checker accurately identifies insecure configurations | Ensure users can trust the Website Checker to confirm secure DNS settings and protect against threats | 28 |  |  |
| 20 | Tester | Verify if the dashboard for visualizing malicious files displays accurate and user-friendly threat data | Ensure users can easily identify and understand potential threats in scanned files | 32 |  |  |
| 21 | Tester | Verify if the Email Analyzer’s link scanning functionality using VirusTotal correctly identifies malicious links | Ensure users can safely interact with email links without being directed to malicious sites | 21 |  |  |
| 22 | User | Ping a website | Verify the website’s connectivity and availability | 23 |  |  |
| 23 | User | Validate the homepage content | Ensure the website’s content is safe and legitimate | 29 |  |  |
| 24 | User | Perform traceroute | Trace the network path to identify potential issues or attacks | 25 |  |  |
| 25 | User | Perform DNS security checks | Confirm the website’s DNS configuration is secure and free from threats | 27 |  |  |
| 26 | User | See a dashboard visualizing malicious files | Easily identify and understand potential threats in scanned files | 31 |  |  |
| 27 | User | Detect phishing attempts by analyzing email header details | Protect myself from fraudulent emails and phishing attacks | 16 |  |  |
| 28 | User | Scan files within emails using VirusTotal | Ensure email attachments are free from malware or malicious content | 18 |  |  |
| 29 | User | Check links within emails using VirusTotal | Verify email links are safe and not leading to malicious sites | 20 |  |  |
| 30 | User | View daily activity logs | Monitor and review my interactions with the SecureSuite tools | 33 |  |  |
| 31 | User | Download daily activity logs | Keep a record of my security checks for future reference or auditing | 34 |  |  |
| 32 | User | Log in to the SecureSuite platform with my credentials | Access the Email Analyzer, File Integrity Checker, and Website Checker securely | 14 |  |  |
| 33 | Developer | Create Python code that implements the File Integrity Checker | Enable users to verify the integrity and safety of files | 7 |  |  |
| 34 | User | Upload and check the integrity of files | Ensure files are unmodified and free from malicious content | 35 |  |  |
| 35 | Developer | Implement a logging system to store user activity data | Enable users to view and download their daily activity logs | 9 |  |  |
| 36 | Tester | Verify if the authentication system correctly validates user credentials | Ensure users can securely log in to the SecureSuite platform | 15 |  |  |
| 37 | Developer | Create a flowchart as a guide for coding | Plan and streamline the development process for the SecureSuite platform | 1 |  |  |
| 38 | Developer | Create Python code that implements the Email Analyzer for phishing detection | Enable users to detect phishing emails effectively | 6 |  |  |
| 39 | Developer | Build an interactive dashboard for visualizing malicious files | Verify the connectivity and potential malicious attacks | 11 |  |  |
| 40 | Developer | Create a github repository | The codes are stored in a repository properly | 1 |  |  |
| 41 | Project manager | Create a Trello board and update it and documentation | Everything is documented properly | 1 |  |  |

**REFERENCES**

Barracuda Networks, Inc. (n.d.). *Barracuda Sentinel: AI-based email protection against phishing and impersonation attacks* [Software]. Retrieved from <https://www.barracuda.com/products/sentinel>

Malwarebytes. (n.d.). *Malwarebytes: Endpoint security with file scanning and threat detection capabilities* [Software]. Retrieved from <https://www.malwarebytes.com/business/endpoint-security>

SiteLock. (n.d.). *SiteLock: Website security platform with malware scanning and vulnerability checks* [Software]. Retrieved from <https://www.sitelock.com/>

Mimecast. (n.d.). *Mimecast: Cloud-based email security with phishing and attachment protection* [Software]. Retrieved from <https://www.mimecast.com/>

Qualys, Inc. (n.d.). *Qualys: Cloud platform for vulnerability management and website security assessments* [Software]. Retrieved from <https://www.qualys.com/>