OSINT Threat Assessment Tool

Denning Technology & Management Program Capstone Project Team:

Sarah Duong, ID Mwenda Mbui, CS

Kaylin Nolan, IAML Christopher Parker, CS

Tony Tanory, CS

T&M Project Advisors:

Bob Burgess John Stanford

Corporate Affiliate:

risk3sixty

Roswell, Georgia

Capstone Project Sponsors:

Kevin Ketts Jessica Lucas

CS/MGT/ME 4742

Georgia Institute of Technology

Denning Technology & Management Program Capstone Project

Spring Semester 2025

Submitted April 27th, 2025

Executive Summary

The Denning Technology & Management Program capstone team investigated the viability of a tool capable of creating a personalized threat assessment report that leverages artificial intelligence and uses only open-source intelligence (OSINT) sites to generate the content. The capstone team was successful in creating a minimum viable product (MVP) that will serve as the corporate affiliate's proof of concept and foundation for a future iteration integrated into their offensive security platform.

The capstone team aims to solve the problem small-to-medium sized companies face to combat cyber-attacks. One well-executed cyberattack can have disastrous effects on any company and it is critical for companies to install preventative security measures. Small-to-medium sized companies often do not have the resources necessary to maintain an in-house cybersecurity team and must make decisions on which services are most necessary to combat cyber-threat actors. The tool offers a service that is free to use for companies and only requires minimal information about the company's geographic location, size, and web services. The capstone team's tool provides companies who do not have the resources for an in-house cybersecurity team to understand their cyber threat landscape and the most impactful security measures to implement. This tool also offers a marketing opportunity for the corporate affiliate to interface with potential new clients who may use the tool and grow interested in the corporate affiliate's paid services. The output of a pdf threat intelligence report also serves to help a company meet the threat intelligence requirement for cybersecurity compliance frameworks such as ISO 27001.

The capstone team researched and evaluated different OSINT sites to pull information from to build the threat assessment tool. The considerations for which OSINT sites could be integrated into the tool included legal restrictions, application programming interface compatibility, and if the content of the sites related to cybersecurity and threat intelligence. Through the twenty plus subject matter expert (SME) interviews conducted at the beginning of the project, the capstone team developed a list of potential sites to investigate for the tool.

The capstone team created proof of concepts for each of the selected OSINT sites to confirm the sources are compatible with the tool. The capstone then began investigating which methods, tools, and language learning model would be incorporated in the tool. The capstone team faced a challenge of integrating all the sources into one database. Through extensive research, the capstone team identified a solution to be funneling each source's output into an individual table and then integrating the tables into a database. The method allows the data to be cleaned and organized into one format. The capstone team solved the challenge using an innovative solution which displayed mastery of the scraping data from OSINT sites.

The capstone team's next challenge was selecting the large language model (LLM) and researching how to leverage the tool with artificial intelligence. The capstone team selected ChatGPT as the LLM because its capabilities best suited the project and supported tools such as LangChain that became critical to the success of this web application. The capstone team's backend developers learned that LangChain, a library in the python coding language, was a strong choice to retrieve the most suitable information. This library also best prompted ChatGPT to create the final pdf report and dashboard inputs.

The capstone team also worked extensively with the corporate affiliate to make sure the web application's interface was aligned with the branding guidelines outlined for the project. Originally, the branding guidelines for the tool matched the corporate affiliate's consulting services platform called fullCircle. However, the corporate affiliate decided the tool should be rebranded to align with its offensive security platform called ARMADA. The capstone team's UI/UX designer developed several drafts and iterations of the design flow until the capstone team settled on the final iteration. These drafts were created based on the feedback received from the SME interviews and looking to the market of current products that provide similar services. The capstone team agreed that building trust and ease of use were the two primary considerations when building the front end of the tool. Throughout the design process, the capstone team met with the corporate affiliate to ensure alignment and make any changes when necessary.

The capstone team successfully created a web application that scrapes six OSINT sites to deliver a unique, ChatGPT enhanced, pdf report and dashboard meant for small-to-medium sized companies to use. The OSINT Threat

Assessment Tool allows a company to create a password protected profile and input five pieces of information: company size, location, industry, cloud service provider, and service produced by company. These inputs prompt the LLM to pull relevant information from the OSINT sites to populate a dashboard and pdf report. The dashboard provides a snapshot of a company's threat landscape that is expanded-upon in the pdf. The pdf report includes indicators of compromise, threat actors and groups, common vulnerabilities and exposures, operations, targeted industries, and more. The success of this tool indicates an opportunity to expand on the MVP and integrate a future iteration into the corporate affiliates paid offensive security services.

The capstone team recommended three improvements to investigate for future iterations of the tool. The capstone team first recommended considering increasing the number of inputs required for a company to provide on the web application to enhance the performance of the tool's output pdf report. The inputs directly influence what information from the database is considered relevant and included in the report. Currently, the inputs ask for high level information that does not provide a deep understanding of the firm requesting a service. Conducting user testing with the current web application would likely result in identifying which inputs result in the most relevant data and suggestions for additional information to implement. The future iteration of this tool that will be integrated with the corporate affiliate's paid services can increase the detail required for the inputs without the concern of building reliability and trust with a single-use customer.

The capstone team also recommended researching how to implement time series analysis to the cataloged information in the database. The capstone team had many discussions on the feasibility of finding a way to catalog the data within the MVP, however this feature did not make it into the product. However, the capstone team recognizes the value of this feature and the advanced capabilities that would result if the data was time-stamped. For example, the report could analyze trends over time and identify relevant threat attacks based on recency. This feature would enhance the overall accuracy and relevancy of the pdf and making the product valuable to a customer.

The third recommendation is to research methods for generating graphs that can visualize the intelligence in a more digestible manner. This is another feature that the capstone team hoped to implement in the current iteration, however it was not within the scope of the MVP. The capstone team identified that graphs would increase user engagement and better meet the needs of the clients. Furthermore, visualizations would enhance the user experience and increase readability since the client will likely have more interest in reading a shortened report. The graphs would likely require data stamped to allow the LLM to create visualizations. This likely means recommendation two and three should be considered in tandem.

The capstone team also discussed future iterations including paywalls to increase revenue on select features of the tool. Placing a paywall on the dashboard feature or requiring a monthly subscription for generating reports monthly could create another stream of income for the corporate affiliate. To maintain the free-to-use nature of the tool, only certain extended features of the tool would require paywalls.

By creating a free-to-use tool, the proposed solution can provide a marketing opportunity that reaches new markets and increases the corporate affiliate's brand credibility. The tool uses OSINT sites that do not require payment to scrape information from and the corporate affiliate already owns a subscription to the LLM selected for this tool. The only cost incurred for the project is the subscription for a slack channel used to communicate during the duration of the capstone project. Thus, the tool did not incur any additional costs. Furthermore, the OSINT Threat Assessment Tool saves the corporate affiliate four months of research and development by salaried employees to investigate a proof of concept for a similar tool intended for the corporate affiliate's offensive security platform ARMADA.

The capstone team had an enriching experience working on an end-to-end web application product. The corporate affiliate offered an amazing opportunity and provided the capstone team with an abundance of resources and hands-on experience. The capstone team was made up of an interdisciplinary team of students with backgrounds ranging in computer science, industrial design, and international relations. The diverse skillset fostered a creative and collaborative environment which resulted in a comprehensive tool that met the corporate affiliates needs and could be expanded upon.

Capstone Project Team Contact Information

Sarah Duong

Industrial Design

sarahduong@gmail.com

linkedin.com/in/sarahduongg/

Mwenda Mbui

Computer Science

Mwenda2022@gmail.com

linkedin.com/in/mwenda-mbui/

Kaylin Nolan

International Affairs and Modern Languages

mariekaylin1221@gmail.com

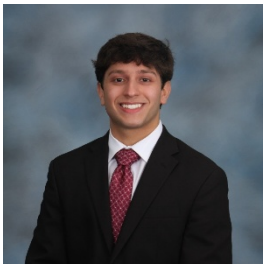
linkedin.com/in/kaylinnolan/

Christopher Parker

Computer Science

chrispark2003@gmail.com

linkedin.com/in/christopher-c-parker/



Tony Tanory

Computer Science

tanoryt@gmail.com

linkedin.com/in/tony-tanory/

Corporate Sponsors' Contact Information

Kevin Ketts

Chief Technology Officer

risk3sixty

Kevin.Ketts@risk3sixty.com

linkedin.com/in/kevinketts/

Jessica Lucas

Vice President of People

risk3sixty

jessica.lucas@risk3sixty.com

linkedin.com/in/jessica-ahn-andree/

Denning Technology & Management Program Contact Information

Ms. Sheena Brown
Academic Program Manager
sheena.brown@scheller.gatech.edu

Mr. Robert "Bob" Burgess
Administrative Director
robert.burgess@scheller.gatech.edu
linkedin.com/in/robert-h-burgess

Ms. Anne Lynch
Communications Manager
anne.lynch@scheller.gatech.edu
linkedin.com/in/annelynch

Mr. John Stanford
Senior Manager, Corporate Relations & Student Counseling
john.stanford@scheller.gatech.edu
linkedin.com/in/johnostanford