Project Plan Outline

Project and Team:

Project Title	#19 Live Analysis
Team	Amandeep Kaur, Jacob McCabe, Rachid Soro, Jacob Robinson

Project Requirements

Background

In most organizations there exists some form of *ticket* and *ticket resolution* system. The system may exist in customer service, logistics, or even R&D. A successful outcome to a ticket requires both ticket participation and fast ticket resolution. This project is focused around ticket participation and ticket resolution by security operation center (SOC) analyst trainees participating in an optional university course. The goal of the course is to simulate SOC analyst duties with real life network data in order to have practical hands-on education in network security. The team going to use statistical analysis and research to determine the answer to two questions:

1. *What leads to increased ticket participation on a ticket?*
2. *What leads to a faster resolution of a ticket?*

The project is primarily attempting to contribute to education. While the primary stakeholder consists of instructors and students at a University level, any findings that are uncovered by the end of the project could potentially be applied to other *ticket* and *ticket resolution* systems that overshadow the SOC industry. Additionally, The SOC industry is much younger than other pre-existing industries and professional SOC analysts are traditionally highly technical operators. These factors coupled with a fast paced and high stress environment could lead to poor ticket creation. The subsequent consequences being misunderstanding, confusion, and unnecessary delays around ticket resolution. Having a methodology for effectively training analysts on how to make quality tickets could ultiametly benefit any industry.

Project Opportunity

What is the customer's need?

The team is going to attempt to find an analytical link between ticket attributes and the speed of ticket resolution among security operations center (SOC) analyst trainees reacting to real life network data. Any findings aim to assist instructors have a better understanding of what factors contribute to increased ticket participation and quicker ticket resolution. These factors will subsequently help improve the process of training and educating current and future SOC analyst trainees.

How does this need fit in the industrial context?

Educational SOC and "Threat Hunting" programs are relatively a new addition to curriculums nationally and presumably globally. Naturally this leads to the conclusion that these curricula have room for improvement but could potentially help any organization that relies on ticket and ticket resolution for project complications or outages. Better ticket creation, participation and resolution is a multi-sector and multi-industry problem.

Project Objectives and Success Criteria

Why does the customer need this research?

While analysis of ticket data was conducted previously by another student, the team now possesses significantly more ticket data and metadata. The significantly large dataset of ticket data will allow the team to ideally identify variables that indicate causation for faster ticket resolution and better ticket participation. If the team can find statistical evidence of how or what makes a ticket more meaningful or efficiently resolvable these findings can be disseminated in a way more concrete to future and current students.

How will the customer know that the research is a success?

Due to the nature of this project, findings may or may not prove the questions mentioned in the "Background" section of this document. Ultimately any findings will support the research effort on this topic. Any conclusive findings will be considered a success for the project.

However, in the event that the team does find conclusive evidence for independent variables related to the questions described in the project proposal these findings can be used to advance the education of SOC analyst trainees. Therefore, the customer can verify that the research is a success if there is an increase in ticket participation and faster resolution times compared to previous class sections.

Customer and Market Needs

Having a better understanding of what makes students participate in solving tickets will help instructors train them more effectively. In result, it will help SOC analysts trainees have a better understanding of how to create high quality tickets. If these trends can be recreated in the rest of the SOC analyst community it could lead to a net positive on the entire field. Leading to a community better equipped for the increasingly more hostile cybersecurity landscape.

Project Risks

- Organization Level Risk
    - An important part of any project is to maintain both on time and keep the project within scope. If anything impedes the project related to project management or organization past sustainable thresholds the project could become unrecoverable. The team is currently using project management tools and singular communication channels in order to remain on schedule as much as possible. The team does not consider this a high risk category.

- Performance Risk
    - Currently the team is not 100% confident on expectations on future tasks related to the project. A lot of this is stemming from the ambiguity from the project itself as well as the delay in resources meant to be provided. The team will take steps to communicate with the project sponsor in order to get both guidance and feedback within the progress functions of the project. The team does not anticipate any knowledge gaps to have a considerable impact on the deadlines of the project.
- Financial Risk
    - Currently the budgetary concerns for the project are low. Most research articles on any related subjects should be easily accessible online or via the university library. Any tools we use will normally be open source (Python, R, etc.). However, in the event where a seemingly potentially important paper or tool is a paid product the team will make the necessary budgetary accommodations.

Vision of the Solution

Vision Statement

The team intends on creating a digestible and meaningful statistical analysis on student SOC analyst ticket metadata. These findings aim to improve the training and education of current and future SOC analyst trainees.

Major Features

The team will create and test a hypothesis with the metadata that is provided. These findings will then be synthesized into statistical analysis, graphical representations, and modifiable formulas in order to easily disseminate the findings in a digestible manner alongside the research paper publication.

Assumptions and Dependencies

The research results rely primarily on the data and the hypotheses. While our hypothesis being proven or not does not affect the definition of success for the team efforts, poor data could lead to results that are unreliable or unusable. It is the team's mission to make the collection of data as reliable and usable as possible in the data clean up phase. That way these attributes can transcend to the ultimate findings barring the nature of the results compared to the hypothesis.

Scope and Limitations

Scope of Initial Release

Ultimately, the initial scope of this project is to improve the process by which instructors teach SOC analyst trainees. The team's intention is to accomplish this by determining what factors lead to increased activity on a ticket as well as the faster resolution of a ticket. After developing an informed hypothesis, we intend to test via statistical analysis.

Scope of Subsequent Releases

Through subsequent releases, our team aims to produce modifiable visual tools in an effort to make any findings more comprehensible to groups who might be less familiar with the area of research. In addition, we will report all findings within a formal paper for presentation. We will possibly take a social networking approach to determine if there are any more findings from our data that did not show up from statistical analysis.

Limitations and Exclusions

Previous research on this topic was very limited due to a small dataset. While it stands to assume that the new, larger dataset will be beneficial, it is also possible that the usable data is small enough that we are unable to produce any new findings.

Project Context

Stakeholder Profiles

Michael Tsikerdekis, PhD - PISCES:
Acting as the primary stakeholder and advisor, Dr. Tsikerdekis will oversee and help to guide the research through its lifetime. By helping us to determine what would be considered a success for the research, he gave us a guideline for how to extend the previous research with access to the new data. From the project, he needs us to determine what, if anything, makes for a well made ticket.

SOC Analysts:
Since the research aims to determine what factors lead to faster resolution of tickets, any future SOC students indirectly stand to benefit from the research since it would lead to better guidance and instruction for making tickets.

Research Team:
The group is primarily responsible for conducting the research. This group is expanding upon research done by previous researchers. By looking through the previous research, the new team will use the advice from Dr. Tsikerdekis to determine how to better train future SOC Analysts.

Future Collaborators:
In the same way that we are expanding upon previous research done on a smaller dataset, any future researchers will directly benefit from the team's research. They might have a need for any scripts, processes, and documentation of what was done to accomplish our research.

Project Priorities

1. Hypothesis Creation
2. Statistical Analysis
3. Dataset Analysis
4. Research Paper to Present Findings

5. Data Visualization Tools

Operating Environment

The research will be used by PISCES instructors to train SOC analysts. If the research is a success, it may be used by companies and other schools or institutions to train SOC Analysts. The research findings could also inspire further research on the same subject.

Project Operations:

Fall Quarter Update:

- The first quarter of three was primarily spent on planning. Initial delays in resources led to a reimagining of what will be the goals for each quarter. This led to the creation of the entries into the “Key Milestones” section and further flushing out of the project timeline.
- Additionally, team members worked on independent research on both the testing environment, research methodologies, and project related martials.

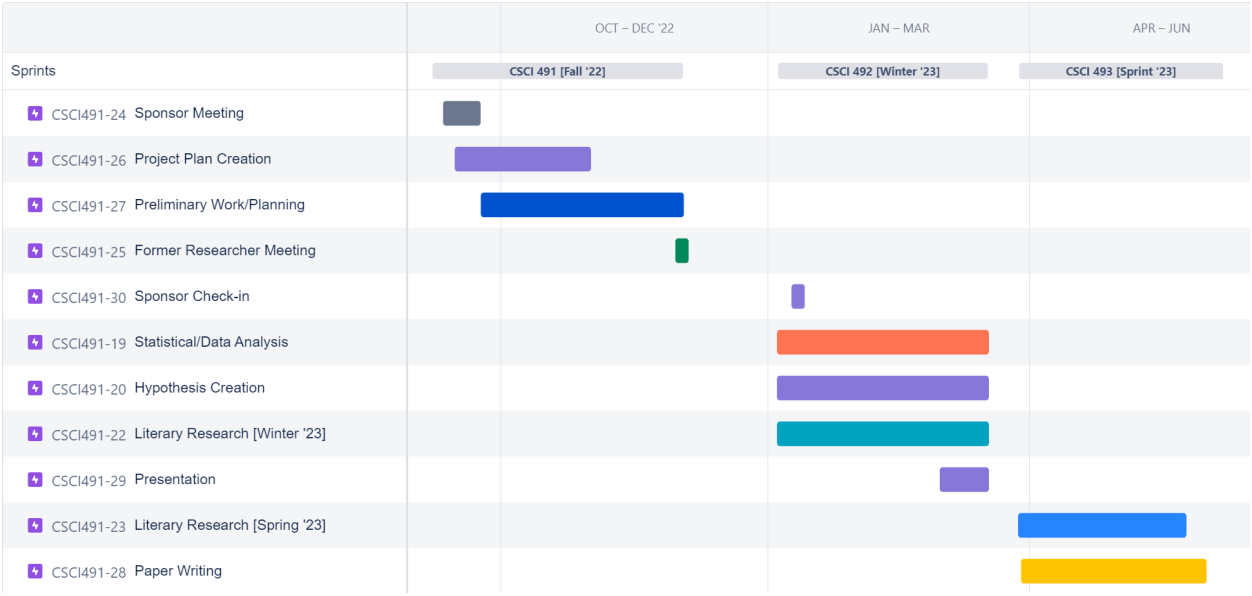
Winter Quarter Update:

- This is the second quarter and will be focused on following the plan set during the first quarter. The team has received the sql file that will be used to organize the data more effectively, and it will give the team more information to work with. This quarter the team will focus on making more progress on the project.

Spring Quarter Update:

- This quarter will be wrapping up the project. Team members will be wrapping up their analysis and compiling all results, whether or not they are conclusive, in order to start drafting the research paper.
- Team members will also be working on the final presentation.
- In case team members would like to continue to work on interesting points or data sets found later, the start of the quarter will be dedicated to completing any research left. The latter half of the quarter will be dedicated to writing the draft, however team members will still be able to continue data analysis.

Scheduling



Key Milestones

Milestone	Target Date	Comment
Data Clean Up	Mid December	The team has been notified that some of the data we will be working with may not help the team's ultimate goal. I.E Test Data, duplicate tickets, tickets by mistake, etc.
Project Proposal	Early October	Project proposal submitted on Oct 12
Project Plan Initialization	Early October	The Team is currently working on the Project plan and should be able to submit it on 10/24/2022
Hypothesis Creation	Late November	The team will be making hypotheses to discover independent variables that reflect the research questions proposed in the project proposal.
Hypothesis Check-in	Early December	Checking with the project advisor to gain feedback or other insight on the hypothesis created before findings are collected..
Data Set Analysis Initiation	Mid December	After data clean up, the team will start organizing it to make it more understandable and attempt to find independent variables related to the research questions..
Preliminary Findings	Early March	Compile and document any preliminary findings the team has come up with.
Paper Initiation.	Early April	After spending quite some time analyzing the data and creating the hypothesis, the team will assemble all the findings and start working on

		the paper.
Paper Submission	Mid/Late May	A comprehensive paper noting all of the work done and results found will be submitted as the final deliverable. This will be a thorough draft of a formal research paper.

Individual Responsibilities

Team Member	Responsibilities
Robinson	● Primary communicator with advisor. ● Statistical Research. ● Insights into ticket participation. ● Project Plan and Project Proposal contributor. ● Hypothesis Creation.
Kaur	● Secondary communicator ● Research ways to analyze tickets. ● Research on data cleaning. ● Statistical Research. ● Project Plan and Project Proposal contributor. ● Hypothesis Creation.
Soro	● Data Analysis/Statistical Analysis ● Research on industry related “Ticket Creation”. ● Project Plan and Project Proposal contributor. ● Hypothesis Creation.
McCabe	● Data Analysis/Statistical Analysis. ● Researching ticket resolution ● Researching ways to clean up data. ● Project Plan and Project Proposal contributor. ● Hypothesis Creation.

Deliverables

Capstone I

Deliverable	Category	Comments	Required/Nice to Have
Confluence Page	Other	Will contain project overview, timeline, and	Required

		group member ownership of tasks.	
Revised Project Plan	Documentation	An updated version of the project plan with more details	Required
Project Timeline	Documentation		Required

Capstone II

Deliverable	**Category**	**Comments**	**Required/Nice to Have**
Preliminary Findings/Quarter Report	Key Presentation	A summary of the most important findings, roadblocks and how they were overcome.	Required
Modifiable Tools/Scripts	Software	Will be useful for successor(s) of the project	Nice to Have
Visuals/Gifs	Documentation	Visualization of preliminary findings	Required
End of Quarter Presentation	Presentation	Showing the findings and progress made on the project this quarter	Required

Capstone III

Deliverable	**Category**	**Comments**	**Required/Nice to Have**
Hypothesis Creation	Documentation	With established key Independent/Dependent variables.	Required
Research Paper Draft	Documentation	Formal paper	Required
Final Presentation	Key Presentation	High level overview of the findings and process of the project.	Required
GitLab Contributions	Data files / created / used	Gitlab	Required
Graphs / Charts	Documentation	Final Research Paper	Nice to have
Literature Review	Documentation	Final Research Paper	Required

Document Version Control:

Current Version: 1.25

Date	Version	Editor	Comment
Oct 15, 2…	1.0	Robinson	Document Created: ● Project and Team ● Document Vers. Control added ● Other Headings Added
Oct 17, 2022	1.1	Kaur	Edited: ● Project Opportunity #1 ● Project Objective and Success Criteria ● Customer and market needs
Oct 17, 2022	1.11	McCabe	Edited: ● Scope & Limitations: Limitations ● Sort of Stakeholders
Oct 18, 2022	1.2	Soro	Edited: ● Project Opportunity ● Project Objective and Success Criteria ● Customer and market needs ● Operating Environment
Oct 20, 2022	1.21	McCabe	Edited: ● Scope of Initial Release ● Scope of Subsequent Releases
Oct 22, 2…	1.22	Robinson	Edited: ● Project requirements ● Responded to issues raised ● Vision Statement
Oct 23, 2…	1.23	Robinson	Edited: ● Changed ○ all mention of “Business” to “project”. ○ all mention of “product” to “research” ○ Research context. ● “Background” section ● Gantt Chart ● Other Responsibility Tables(started) ● Deliverables section. ● Vision section complete ● Moved `Document Control` to the end of the document. ● Milestones

Oct 23, 2…	1.23	Soro	Edited: ● Project Risks ● Customer and Market needs ● Operating Environment ● Project Objective and Success Criteria ● Responsibilities
Oct 24, 2022	1.24	Kaur	Edited: ● Individual responsibilities ● Customer needs ● Project risks ● Milestones
Oct 24, 2…	1.25	Soro	Edited: ● Key Milestones ● Operating Environment ● Individual responsibilities
Oct 24, 2…	1.25	McCabe	Edited: ● Individual Responsibilities ● Project Priorities ● Stakeholder Profiles ● Scope of Initial Release ● Scope of Subsequent Releases
Oct 24, 2…	1.25	Robinson	Edited: ● General editing/formatting ● Vision ● Background ● Deliverables ● Format ● Font
Oct 24, 2022	1.25	Kaur	Edited/Reviewed: ● Background ● All mentions of analysts to Analysts ● Project Objectives and Success Criteria ● Scope and Limitations
Nov 29, 2…	1.26	Robinson	Revisiting Deliverables and Timeline: Reformatted
Jan 11, 2023	2.0	Robinson	Start of Winter ‘23 session: ● v2. ● New Deliverables ● New Details of the Project ○ Added “Project Operations”
Jan 18, 2023	2.0	McCabe	Edited:

			● New Deliverable ● Updated Scheduling ● Project Opportunity - Customer's need
Jan 20, 2023	2.0	Soro	Edited: ● New Deliverables ● Key Milestones ● Project Operations
Feb 23, 2023	2.1	McCabe	Added: ● Stakeholder profile for the current research team Edited: ● Removed SNA from document ● Updated Roadmap ● Updated Deliverables for Capstone 2 ● Updated Individual Responsibilities to reflect removing SNA
Feb 27, 2023	2.2	Robinson	Moved: ● Hypothesis creation to capstone iii Added: ● Additional info about "preliminary findings"
Apr 18, 2023	3.0	Robinson	Changed verbiage in final deliverable: ● Set gitlab contributions to required ● Changed paper to "paper draft" per Michael's expectations
Apr 19, 2023	3.1	McCabe	Edited: ● Responsibilities of Jacob McCabe ● Added milestone for paper submission ● Rephrased the "Spring Quarter Update"
Apr 19, 2023	3.2	Kaur	Edited: ● Deliverable Capstone III ● Edited and added to Spring Quarter Update