Rochester Institute of Technology
B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Computing Security

~ Project Proposal Approval Form ~

Student Name: Nishith Savdas Lakhnotra (nsl6625@rit.edu)

Project Title: Intelligence Driven Cyber Threat Modeling

Project Area: Threat Intelligence, Threat Research, Cyber Threat Modeling.

~ MS Project Committee ~

Name	**Signature**	**Date**
Justin Pelletier (jxpics@rit.edu) Chair		08/14/2020
Michael DeBolt (mdebolt@intel471.com) Committee Member		08/14/2020

Approved: ___________________ Date: ____/____/____ electronic copy received

TABLE OF CONTENTS

INTRODUCTION

Threat Modeling has been a diverse topic amongst the security community and each organization has set their own standards and processes as to how they wish to realize this process. It can be defined as a process by which potential threats can be identified, enumerated, and mitigated to protect confidential data and intellectual property [1] [2]. Threat Modeling is a complex process since the end goals are diverse depending upon the organization proposing the methodology, but they have a common goal that is an improved security posture overall. It is a proactive approach aimed at addressing the threats and vulnerabilities and resolving them even before they occur.

One of the major concerns with respect to the threat modeling is the time frame that is takes to create and deploy a threat model given the overwhelming number of new threats emerging each day. This becomes a problem when different organizations come up with different approaches to counter the same objective that is to organize and prioritize the intel to make more proactively informed decisions. The aim here is to unify those efforts and hence create a standard that can be followed by majority of professional and academic organizations across the security community. In this project, the author aims to propose a methodology to create a playbook with Essential Elements of Information which maps to Tactics Techniques and Procedures, Technical Indicators and Default Variables of different types of attacks and emphasize the strategies around behavior fingerprinting of the same. The General Intelligence Requirements that shall provide to be the baseline here for the creation of a goal-oriented methodology contribute towards maximization of resources, measured success criteria and a demonstrated Cyber Threat Intelligence return of investment notion.

There are two pressing questions being answered through the process of building out this project: what is being solved and to whom does it serve. The major points being addressed here are also Fear, Data Overload, Proactivity. The security professionals from Tactical and Technical, Operational and Strategic departments shall greatly be influenced and benefitted from this literature and the model of intelligence driven security.

RELATED WORK

With the increasing cyber-attacks each day and new threat emerging every day, each organization has come up with threat modeling methodologies, but they vary in quality, implementation, return of investment and consistency. The aim here is to unify those efforts and propose a framework that can be actively referenced by the researchers, analysts and cyber threat intelligence planners. There are numerous existing threat modeling standards being developed by different organizations to counter the varying consequences of the new threats that are emerging every day. Microsoft has a very well-rounded method of approaching threat modeling where the five major steps involve defining, creating, identifying, mitigating, and validating security requirements to address threats [3]. The Spoofing Tampering Repudiation Information Message Disclosure Denial of Service and Elevation of Privilege or the STRIDE model focusses on the Developer side of threat modeling [4]. The idea here is to ensure that the Microsoft developers keep into account the security perspective during the design phase. The Trike Threat Modeling is a methodology that focusses on requirements model which is concentrates on the acceptable risk amongst the stakeholders [5]. The PASTA threat modeling approach is very close to what purple teaming is referred to in the present security community. It focusses on the attacker centric overview involving risk and impact analysis [6]. The VAST threat modeling focusses on enterprise security which was proposed due to the lack of efficiency in implementation phase of steps in the threat modeling methodology [7]. The major source of aligning literature to this project work is the Intel471 General Intelligence Requirements that the mentor has agreed on providing with and is available on request to the interested and is referenced to this document [8].

METHODOLOGY

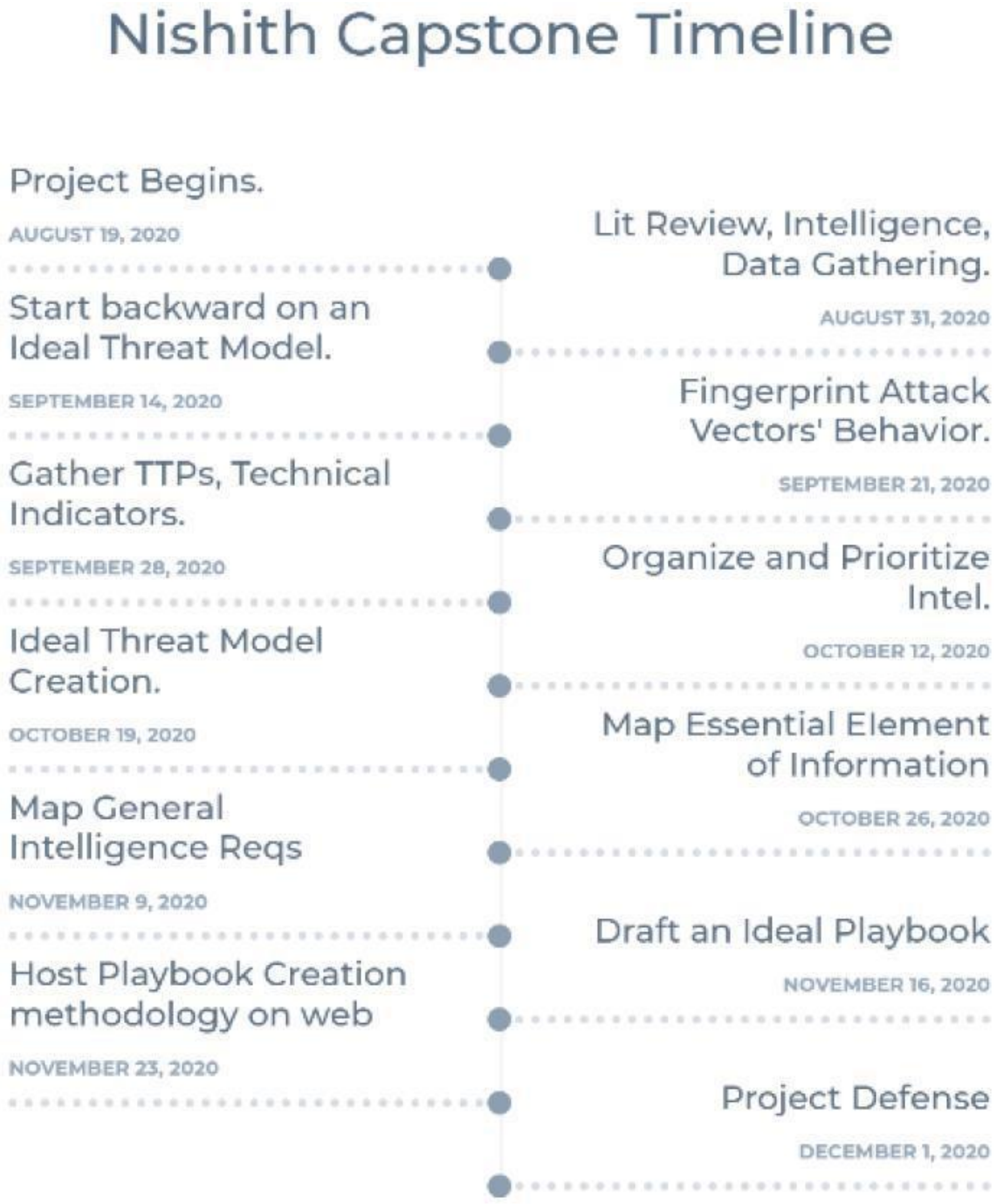
The approach towards this project begins by proposing questions like who are the adversaries, what their motives are, if we are under attack or not, how we would prepare, if they have been successful, how do we respond and finding answers to them. These questions are usually unanswered at first and therefore there is a need for intelligence driven security. The intelligence requirements can be met through realizing a framework wherein the operational environment goes under collection phase which gives the product of data. This data then undergoes the processing and exploitation phase which gives the product of information which in turn goes under analysis and production phase and finally intelligence is obtained as the product. The general intelligence requirements which are a major part of the methodology are inspired by the famous Marine Corps Intelligence Activity: Mountain Girh literature. These general requirements are aimed at addressing three major factors viz Normalization, Prioritization and Synchronization. Normalization is when there is no common language to map the intelligence requirements, Prioritization in this context deals with the different use cases mapped to single cyber threat intelligence team and Synchronization throws light on the absence of a universally accepted process to be followed. Therefore, the importance of threat modeling can be realized by organizing, prioritizing, producing, and measuring production of cyber intelligence. The author intends to start backward on an ideal threat model and mark that as a major step in the methodology approach after substantial amount of literature review, intelligence and data gathering. The next step would be to fingerprint the attack vectors' behavior and gather TTPs (Tactics, Techniques and Procedures) and technical indicators of different types of attacks. Following that the mitigation and the default variables will be gathered to organize and prioritize intel which shall lead the project towards an ideal threat model creation. After the EEIs (Essential Elements of Information) can be mapped and address any gaps that need to be closed. Finally, the general intelligence requirements can be mapped to draft an ideal playbook. Using this process as an example, the major deliverable of this project is rather a methodology to create a playbook for different kinds of attacks in different domains in set amount of time.

PROJECT STATEMENT

“Intelligence Driven Cyber Threat Modeling”

The claim that the system is secure in today's ever-changing landscape of cyber-attacks is tough to justify. By creating a methodology to produce a playbook with Essential Elements of Information (EEI) that maps Tactics, Techniques and Procedures (TTPs), Technical Indicators, Mitigation, and Default Variables to organize, prioritize, produce and measure the production of Cyber Intelligence can greatly help the Cyber Threat Intelligence Planners, Analysts, and Researchers. Furthermore, it can be used as a standard to develop Intelligence Requirements and measure intel teams' value to vendors and stakeholders. There is no standard response to different types of attacks and therefore formulating threat modeling strategies should be emphasized around behavior fingerprinting of different types of attacks. The baseline of the playbook will be built around the General Intelligence Requirements that the Intel471 has agreed on collaborating and sharing. This shall greatly contribute to an even bigger purpose: to counter cyber terrorism and identify, approach the threat modeling process of complex systems.

TIMELINE



Nishith Capstone Timeline

Project Begins.

AUGUST 19, 2020

Lit Review, Intelligence, Data Gathering.

AUGUST 31, 2020

Start backward on an Ideal Threat Model.

SEPTEMBER 14, 2020

Fingerprint Attack Vectors' Behavior.

SEPTEMBER 21, 2020

Gather TTPs, Technical Indicators.

SEPTEMBER 28, 2020

Organize and Prioritize Intel.

OCTOBER 12, 2020

Ideal Threat Model Creation.

OCTOBER 19, 2020

Map Essential Element of Information

OCTOBER 26, 2020

Map General Intelligence Reqs

NOVEMBER 9, 2020

Draft an Ideal Playbook

NOVEMBER 16, 2020

Host Playbook Creation methodology on web

NOVEMBER 23, 2020

Project Defense

DECEMBER 1, 2020

<u>Note:</u> This Timeline has tentative dates, this project could extend beyond this and a request for extension can be made given the scope of the project.

DELIVERABLES

- A Methodology for creating a cyber threat modeling playbook.
- A website that gives out automated mapping of input attacks/ adversaries to threat models.
- Standard possible playbook parameters for a given input.

Note: This list is non-exhaustive, and its scope would expand once the project is in process.

REFERENCES

[1] "Threat model", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Threat_model. [Accessed: 14- Aug- 2020].

[2] "What Is Threat Modeling and How Does It Impact Application Security?", *Security Intelligence*, 2020. [Online]. Available: https://securityintelligence.com/posts/what-is-threat-modeling-and-how-does-it-impact-application-security/. [Accessed: 14- Aug- 2020].

[3] "Microsoft Security Development Lifecycle Threat Modelling", *Microsoft.com*, 2020. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling. [Accessed: 14- Aug- 2020].

[4] "STRIDE chart - Microsoft Security", *Microsoft Security*, 2020. [Online]. Available: https://www.microsoft.com/security/blog/2007/09/11/stride-chart/. [Accessed: 14- Aug- 2020].

[5] "Trike", *octotrike.org*, 2020. [Online]. Available: https://www.octotrike.org/. [Accessed: 14- Aug- 2020].

[6] *Owasp.org*, 2020. [Online]. Available: https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf. [Accessed: 14- Aug- 2020].

[7] "Threat Modeling Methodologies: What is VAST? | ThreatModeler", *ThreatModeler Software, Inc.*, 2020. [Online]. Available: https://threatmodeler.com/threat-modeling-methodologies-vast/. [Accessed: 14- Aug- 2020].

[8] Cyber Underground General Intelligence Requirements Handbook by Intel471.