Hacking for Defense Summarization

MGIS 489 - Seminar in MIS

Ryan Carpenter, Nick Lim, Spencer Tani, Nahjee Sowah

Rochester Institute of Technology

Hacking For Defense

12 December 2019

Dr. Santa

Overview

For the Fall 2019 semester, Rochester Institute of Technology's Hacking for Defense (H4D) team was tasked with developing a faster, more efficient system to combat the increasing number of cyber anomalies the United States Marine Corps (USMC) faces on a regular basis. Cyber anomalies can be quantified under three classifications: trends of increase (or decrease) in phishing activities, sudden spikes (or drop-offs) in infections from malware, and general shifts in source or target geolocations. With a general idea of the problem at hand, we embarked on roughly sixty beneficiary discovery interviews to understand the core issue. With the intention to find common ground surrounding the cyber threat, our discovery interviews included military personnel, military-sponsored research laboratories, and private industry entities. After conducting a portion of interviews with stakeholders, we were able to create the first version of our minimum viable product (MVP). It was clear that the core challenge resided in understanding the flow of data traffic within networks, regardless of industry. As we dove deeper into research and gained a higher understanding of the issue, the requirement for a more sophisticated solution began to appear.

The H4D team agreed that our solution needed to focus on the inspection and monitoring of network traffic. Placed on the public-facing edge of the network, our surveillance node would have the ability to record, log, and establish baseline measurements of network data traffic. Once a baseline level of network traffic has been established, barriers and alerts can be implemented to warn internal users of malicious acts against their network.

Heilmeyer's Questions

I. What are you trying to do?

The H4D team set out to develop a faster, more efficient system for cyber anomaly detection using public-facing nodes placed outside of firewalls with the intent to analyze the characteristics of inbound and outbound data traffic of a network. Through logging and algorithmic practices, our device would provide the ability to establish a baseline understanding of a specific network data flow. Once a baseline is established, the surveillance node would develop alert criteria to illuminate any activity exceeding network standards. This process can be conducted both internally and externally on any medium sized network.

II. What is the current practice?

Currently, the USMC utilizes firewall systems for exterior protection and dual authentication systems to monitor users. We discovered that the USMC has taken more of a responsive posture to cyber anomaly and infiltration by incorporating Cyber Protection Teams (CPT). CPT's are deployed on a case by case operation schedule in response to cyber catastrophe. These teams are tasked with patching network holes and attempted recovery of network data.

III. What is new in your approach and why do you think this will be successful?

Our proposed solution will provide a plug-and-play option with minimal installation. This device will come with preloaded logging hardware on a Raspberry PI and a military authorized ethernet cord which will physically plug into any desired network. A network administrator will then be required to finalize installation by uploading software that is packaged and shipped separately. Our approach has privacy and analysis as the top priorities. As such, no analysis is performed within the network and data collection is positioned outside the network. Through positioning, packets are tracked as they leave and enter the network, while being invisible to those

inside and outside the network being monitored. We offer a product that is secure from the kernel out. This implies that the core properties of our product will be secure from any malicious behavior through the incorporation of NEMSBash. The data is then exported to an external database for analysis through Nagios and Python. Once analyzed, alert criteria is established for logs that seem harmful to the network.

IV. What is the significance of your research if successful?

The significance of our research provides a cross domain solution. This means that our solution provides a capability that is beneficial to more than just the USMC. Having a product with the ability to detect cyber anomalies before hitting the network is a desired capability beneficial to all. By tweaking the product to work on Linux and macOS, the product can be merged with existing security technologies or act as a standalone security device, regardless of industry. Furthermore, the information gathered through Nagios tactical analysis could be employed in multiple directions. For one, networks can be hardened by implementing defenses based off of persistent attacks seen by Nagios. Secondly, by analyzing alerts, users have the ability to gain an understanding on the origins of the attack. This can lead to the identification of threat actors and organizations.

V. What are the risks and your mitigation plan?

The main risks of our proposed solution deals with the introduction of security vulnerabilities. Adding or connecting any device to the network gives attackers an additional point of access. Vulnerabilities in such a device could lead to the opportunity for pivots into secure networks resulting in the compromise of data. Considering that, our proposed device lies on the public-facing side of a selected network, we expect these devices to experience a barrage of attacks daily. With this in mind, we have incorporated the approach of securing the kernel of our device

with the intent of creating an impenetrable wall surrounding the core. In addition, NEMSbash and Nagios Tactical will have the ability to self-destruct the device in the event it is compromised internally, thus destroying the connection made to the physical network being monitored and analyzed. Our device will also be subject to the military's standard Risk Management Framework (RMF) along with standard Authority to Operate (ATO) procedures. Each step will be implemented over the course of the prototyping phase: before development, during development, and after development. Once the selected security controls are implemented then finalized, they will be constantly monitored to ensure the integrity of the system. The system will undergo ATO and RMF recertification every three years or after significant change to the system risk level.

VI. What are the metrics for success for your research?

Our customer, Marine Corps Systems Command (MARCORSYSCOM) stressed the need for an out of the box solution providing real time network monitoring in order to better understand and identify cyber anomalies . Our proposed solution is offered as an out of the box product requiring minimal setup and minimal training for end users. This allows for a smooth and easy deployment throughout selected networks. Once properly setup, cyber security analysts will be notified of cyber anomalies through log aggregation and automation of alerts. Additional criteria can be added to the system to provide future hard alerts that will specify a level of criticality corresponding with the type of attack. This can be specified by Indicators of Compromise (IOC). Because the system will be sitting on the exterior of the network, it is able to sniff out malicious packets before hitting the network. This provides as close to real time detection and alerting as possible.

Target Programs

With the intention of assisting our main customer; the United States Marine Corps, specifically Marine Corps Forces Cyberspace Command (MARFORCYBER) and MARCORSYSCOM, we focused our solution around the military-oriented networks both for command usage and the warfighter downrange. We strongly believe our solution contains extensive cross-domain capabilities that could be utilized by various units within all branches of the military, even reaching as far as private industry.

With this being said, Captain Ferguson Dale of MARCORSYSCOM will remain as our primary customer, point of contact, and recipient of our developed product and cyber anomaly detection solution all the way through development, testing, and deployment of this product and proposed solution.

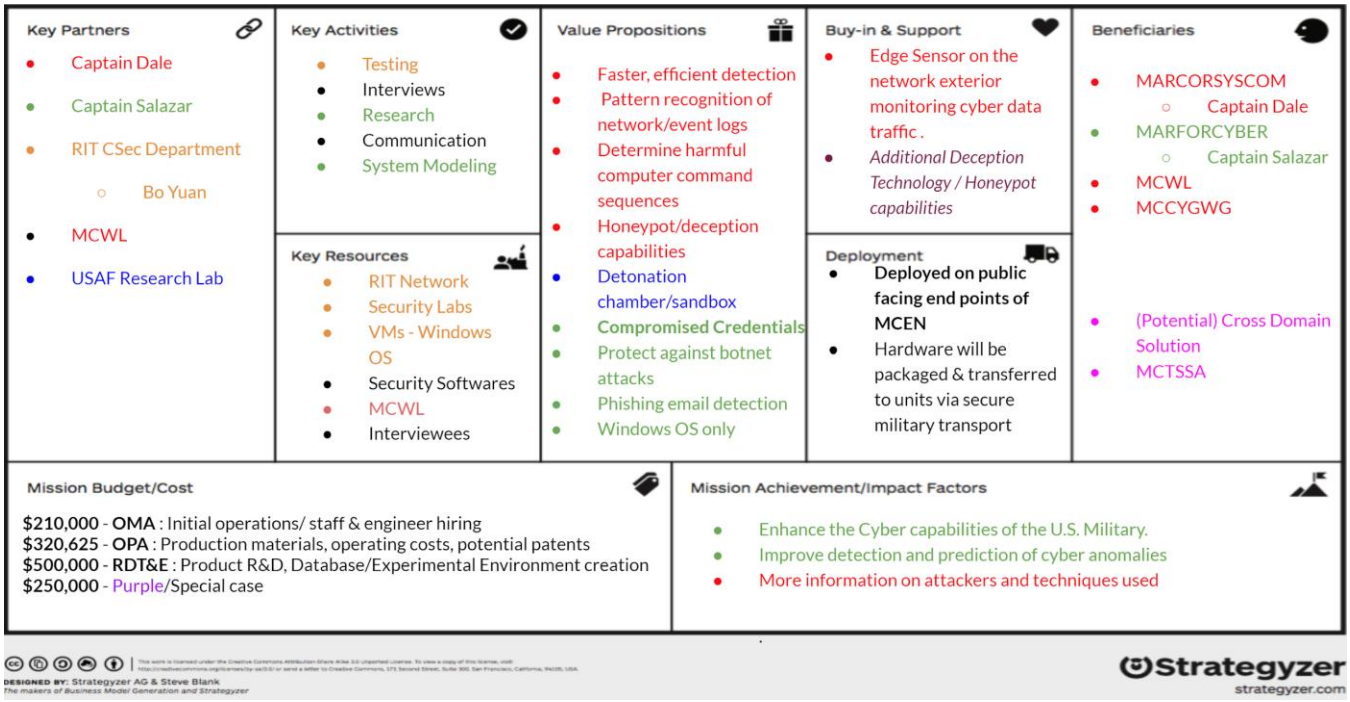
Conclusion

The threat of the cyber environment is similar to the old Wild West; its an untamed and unregulated environment that is constantly evolving and accelerating at unimaginable speeds. The cyber threats of today are vastly different from the threats of tomorrow; research has supported that this method is increasing in popularity due to the rapidly changing state of modern warfare for both nation states and smaller self-interest groups. As the world continues to become more reliant on technology, the threat of opportunity and intent increases exponentially. By monitoring networks and truly understanding the flow of data surrounding a specific network, we can understand the environment and vulnerabilities within our own military networks. With an established understanding, we begin to develop more preventative behaviors, opposed to the current reactionary approach that is utilized today. By committing to this stance of reaction, our

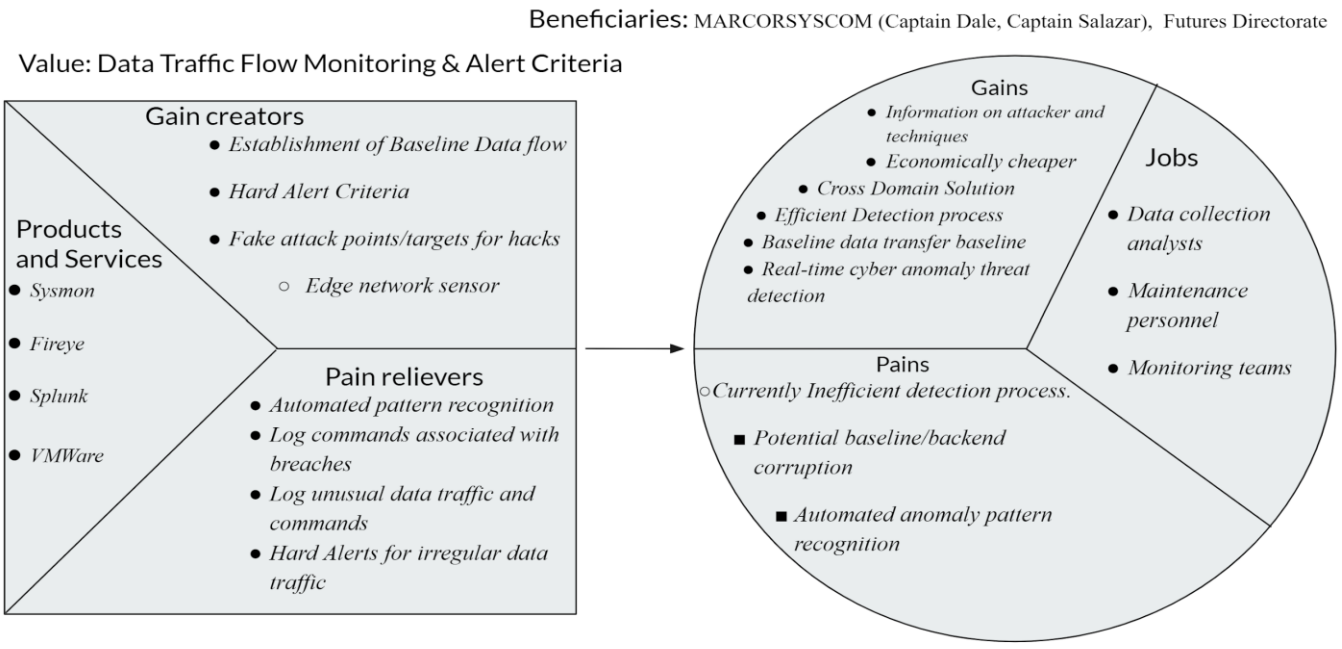
military is leaving holes of exposure that can result in catastrophic loss and this is the location of necessary change.

Addendum:

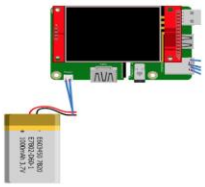
Mission Mode Canvas (MMC)



Value Proposition Canvas (VPC)

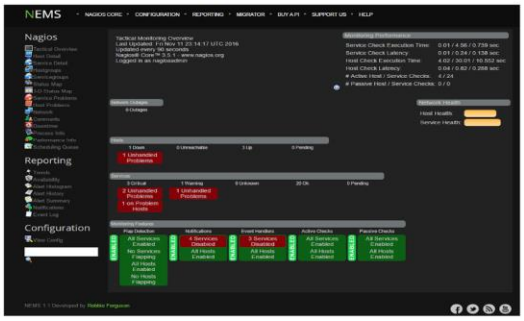


Minimum Viable Product (MVP)

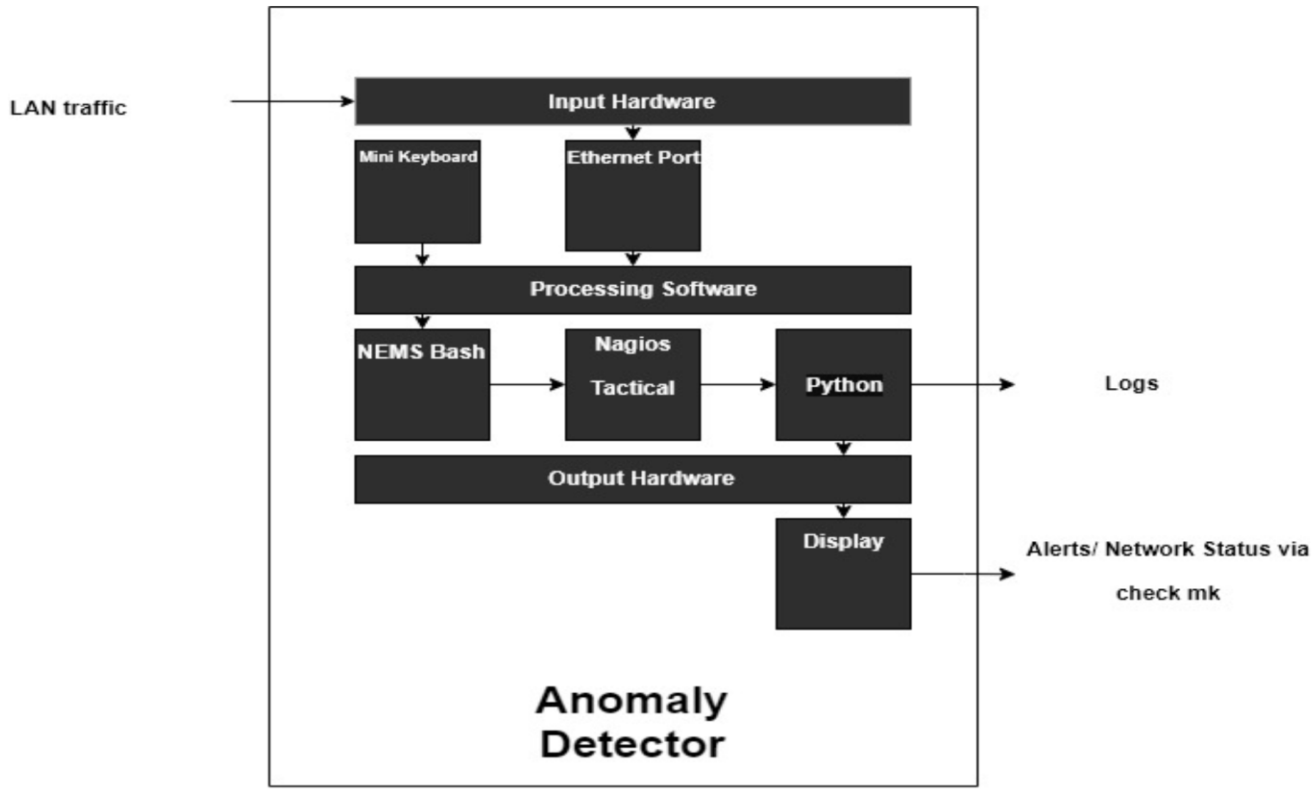


Hardware/Software

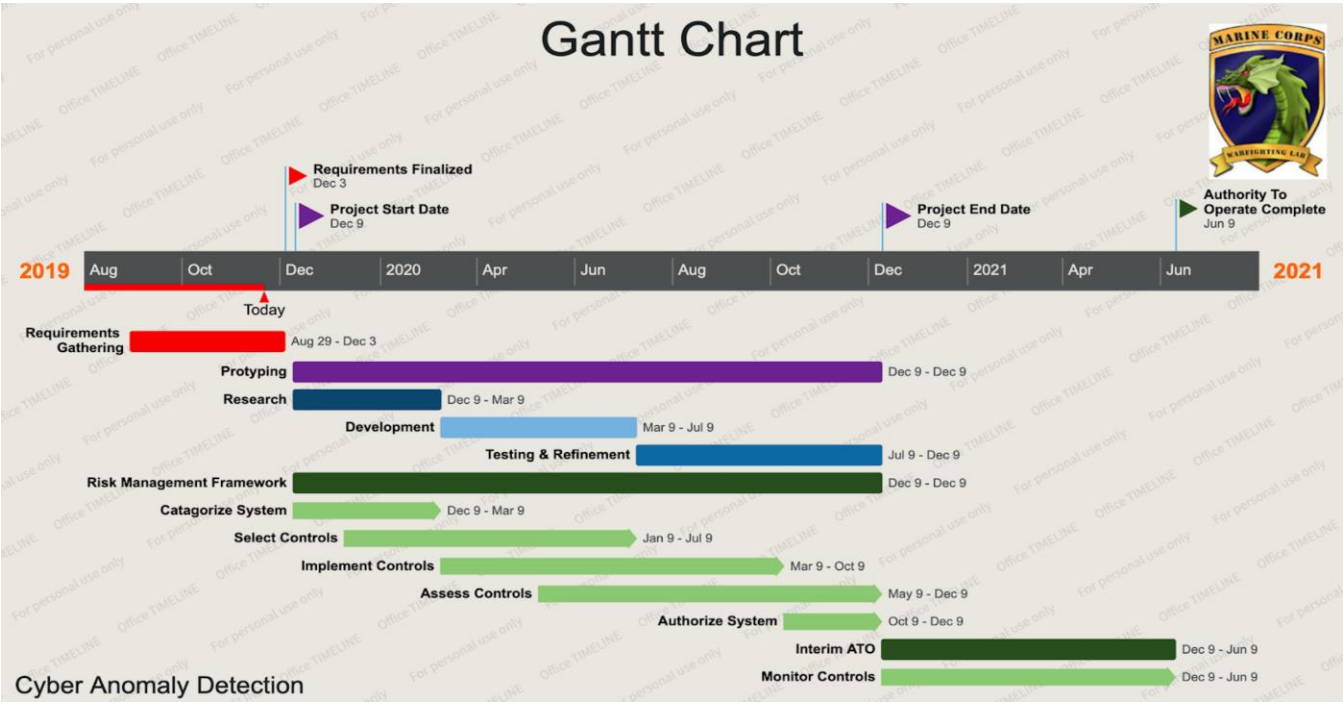
- **Computing/ Logic** : Raspberry PI 3, NEMS, Nagios Tactical, Bash, Python For a Naive Bayes Classifier
- **Traffic Stream**: Ethernet network adaptor
- **Power and Input** : Mini Wireless Keyboard, USB Battery
- **Output** : LCD Screen, Signal data



System Model



Gantt Chart


Gantt Chart
Requirements Finalized
Dec 3
Project Start Date
Dec 9
Project End Date
Dec 9
Authority To Operate Complete
Jun 9
2019
Aug
Oct
Dec
2020
Apr
Jun
Aug
Oct
Dec
2021
Apr
Jun
2021
Today
Requirements Gathering
Aug 29 - Dec 3
Protyping
Dec 9 - Dec 9
Research
Dec 9 - Mar 9
Development
Mar 9 - Jul 9
Testing & Refinement
Jul 9 - Dec 9
Risk Management Framework
Dec 9 - Dec 9
Catagorize System
Dec 9 - Mar 9
Select Controls
Jan 9 - Jul 9
Implement Controls
Mar 9 - Oct 9
Assess Controls
May 9 - Dec 9
Authorize System
Oct 9 - Dec 9
Interim ATO
Dec 9 - Jun 9
Monitor Controls
Dec 9 - Jun 9
Cyber Anomaly Detection