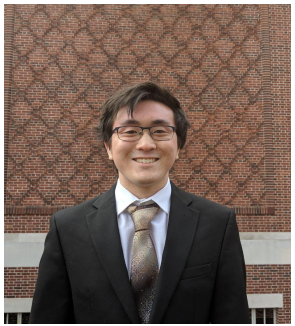
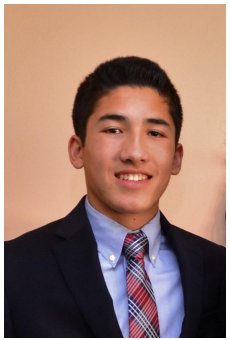
Hacking For Defense

Final Briefing

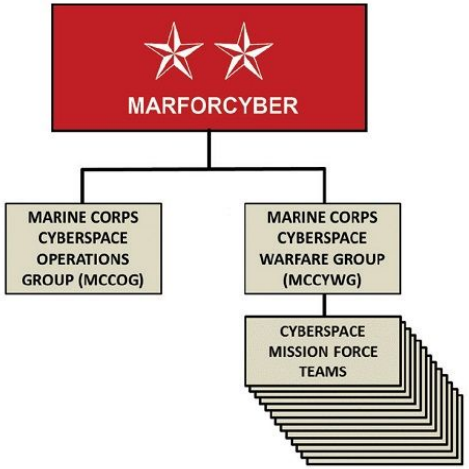


Ryan Carpenter - Nahjee Sowah - Spencer Tani - Nick Lim

Problem Statement

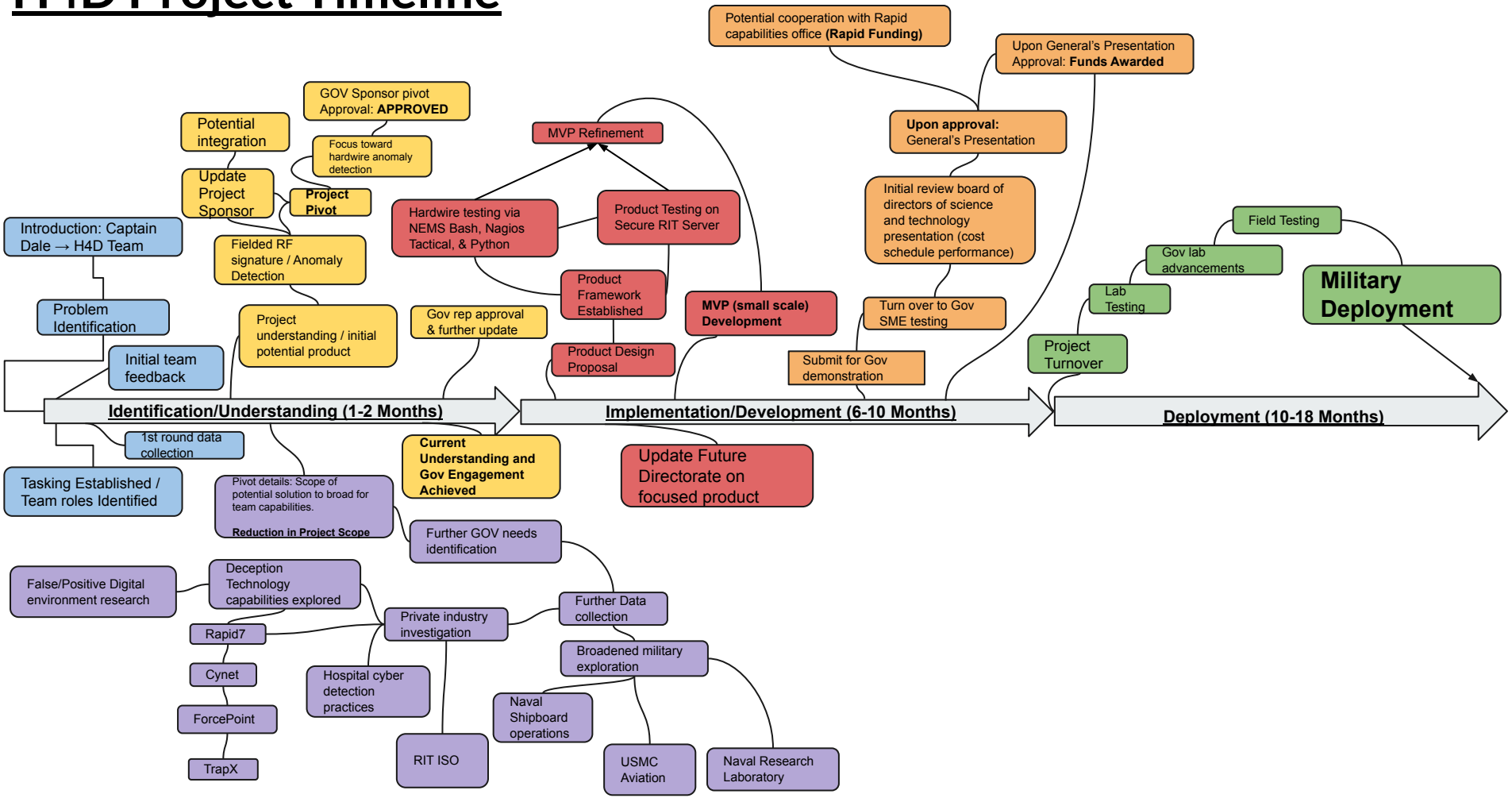
MARFORCYBER, MARCORSYSCOM, and Futures Directorate are currently searching for new abilities focused around improved cyber anomaly detection capabilities.



Problem Statement

Sponsor Problem Statement	Intermediary Problem Statement	Final Problem Statement
“The Cyber Operations Group needs the ability to detect cyber anomalies at a higher rate than the current systems”	“Marine Force Cyber Command requested a RF collection device that operates below the noise floor”	“Edge packet inspection with log aggregation using a probabilistic algorithm to detect cyber anomalies”

H4D Project Timeline



Stage 1: Identification/Understanding

Introduction: Captain Dale → H4D Team

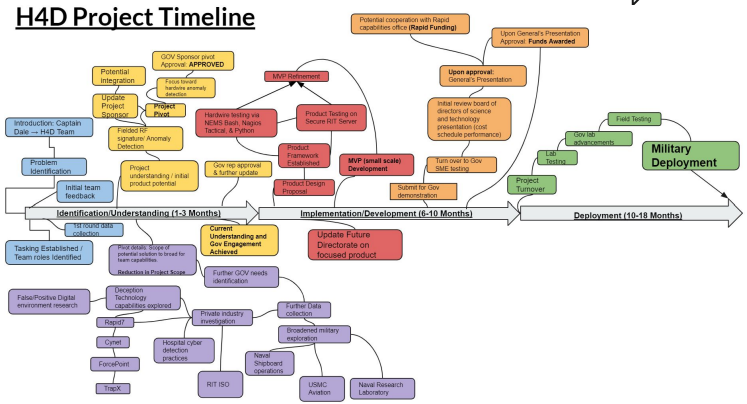
Problem Identification

Initial team feedback

Identification/Understanding (1-2 Months)

1st round data collection

Tasking Established / Team roles Identified



The Mission Model Canvas

Key Partners

- Captain Dale
- Captain Salazar
- RIT CSec Department
  - Bo Yuan
- MCWL
- USAF Research Lab

Key Activities

- Testing
- Interviews
- Research
- Communication
- System Modeling

Key Resources

- RIT Network
- Security Labs
- VMs - Windows OS
- Security Softwares
- MCWL
- Interviewees

Value Propositions

- **Faster, efficient detection**
- **Pattern recognition of network/event logs**
- **Determine harmful computer command sequences**
- **Potential Honeypot capabilities**
- **Compromised data packets**
- **Protect against botnet attacks**
- **Phishing email prevention**
- **Windows OS only**

Buy-in & Support

- Edge Sensor on the network exterior monitoring cyber data traffic .
- *Additional Deception Technology / Honeypot capabilities*

Deployment

- Deployed on public facing end points of MCEN
- Hardware will be packaged & transferred to units via secure military transport

Beneficiaries

- **MARCORSYSCOM**
  - **Captain Dale**
- **MCWL**
- **MCCYWG**
- **Cross Domain Solution**
- **MARFORCYBER**
  - **Captain Salazar**

Mission Budget/Cost

$210,000 - OMA : Initial operations/ staff & engineer hiring
$320,625 - OPA : Production materials, operating costs, potential patents
$500,000 - RDT&E : Product R&D, Database/Experimental Environment creation
$250,000 - Purple/Special case

Mission Achievement/Impact Factors

- Enhance the Cyber capabilities of the U.S. Military.
- Improve detection and prediction of cyber anomalies
- More information on attackers and techniques used

DESIGNED BY: Strategyzer AG & Steve Blank
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

The Mission Model Canvas

VALUE PROPOSITION

- Faster, efficient detection
- Pattern recognition of network/event logs
- Determine harmful computer command sequences
- Potential Honeypot capabilities
- Compromised data packets
- Protect against botnet attacks
- Phishing email prevention
- Windows OS only

BENEFICIARIES

- MARCORSYSCOM
  - Captain Dale
- MCWL
- MCCYWG
- Cross Domain Solution
- MARFORCYBER
  - Captain Salazar

Problem Statement

Sponsor Problem Statement

“The Cyber Operations Group needs the ability to better detect cyber anomalies at a higher rate than the current systems”

Intermediary Problem Statement

“Marine Force Cyber Command requested a RF collection device that operates below the noise floor”

Final Problem Statement

“Edge packet inspection with log aggregation using a probabilistic algorithm to detect cyber anomalies”

Stage 1.2 : Initial Exploration & Potential Solution

Potential integration

Update Project Sponsor

Fielded RF signature/ Anomaly Detection

Project understanding / initial product potential

Focus toward hardwire anomaly detection

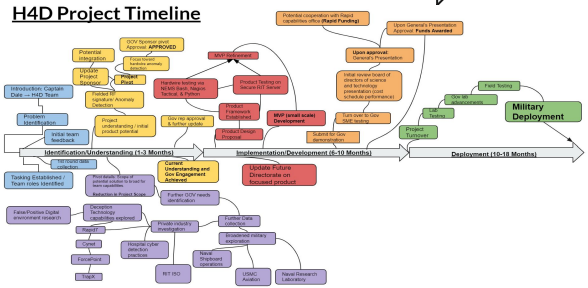
GOV Sponsor pivot Approval: **APPROVED**

Project Pivot

Gov rep approval & further update

Identification/Understanding (1-3 Months)

Current Understanding and Gov Engagement Achieved



Problem Statement

Sponsor Problem Statement

“The Cyber Operations Group needs the ability to detect cyber anomalies at a higher rate than the current systems”

Intermediary Problem Statement

“Marine Force Cyber Command requested a RF collection device that operates below the noise floor”

Final Problem Statement

“Edge packet inspection with log aggregation using a probabilistic algorithm to detect cyber anomalies”

Stage 1.3 : Research & Exploration

Identification/Understanding (1-3 Months)

Pivot details: Scope of potential solution to broad for team capabilities.

Reduction in Project Scope

Further GOV needs identification

False/Positive Digital environment research

Deception Technology capabilities explored

Private industry investigation

Further Data collection

Broadened military exploration

Rapid7

Cynet

ForcePoint

TrapX

Hospital cyber detection practices

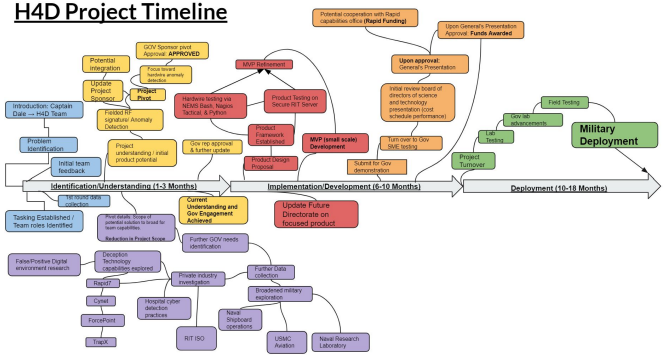
RIT ISO

Naval Shipboard Operations

USMC Aviation

Naval Research Laboratory

H4D Project Timeline



Problem Statement

Sponsor Problem Statement

"The Cyber Operations Group needs the ability to detect cyber anomalies at a higher rate than the current systems"

Intermediary Problem Statement

"Marine Force Cyber Command requested a RF collection device that operates below the noise floor"

Final Problem Statement

"Edge packet inspection with log aggregation using a probabilistic algorithm to detect cyber anomalies"

Stage 2: Implementation/Development

MVP Refinement

Hardwire testing via NEMS Bash, Nagios Tactical, & Python

Product Testing on Secure RIT Server

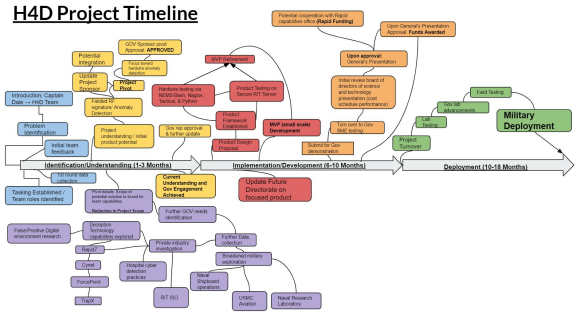
Product Framework Established

Product Design Proposal

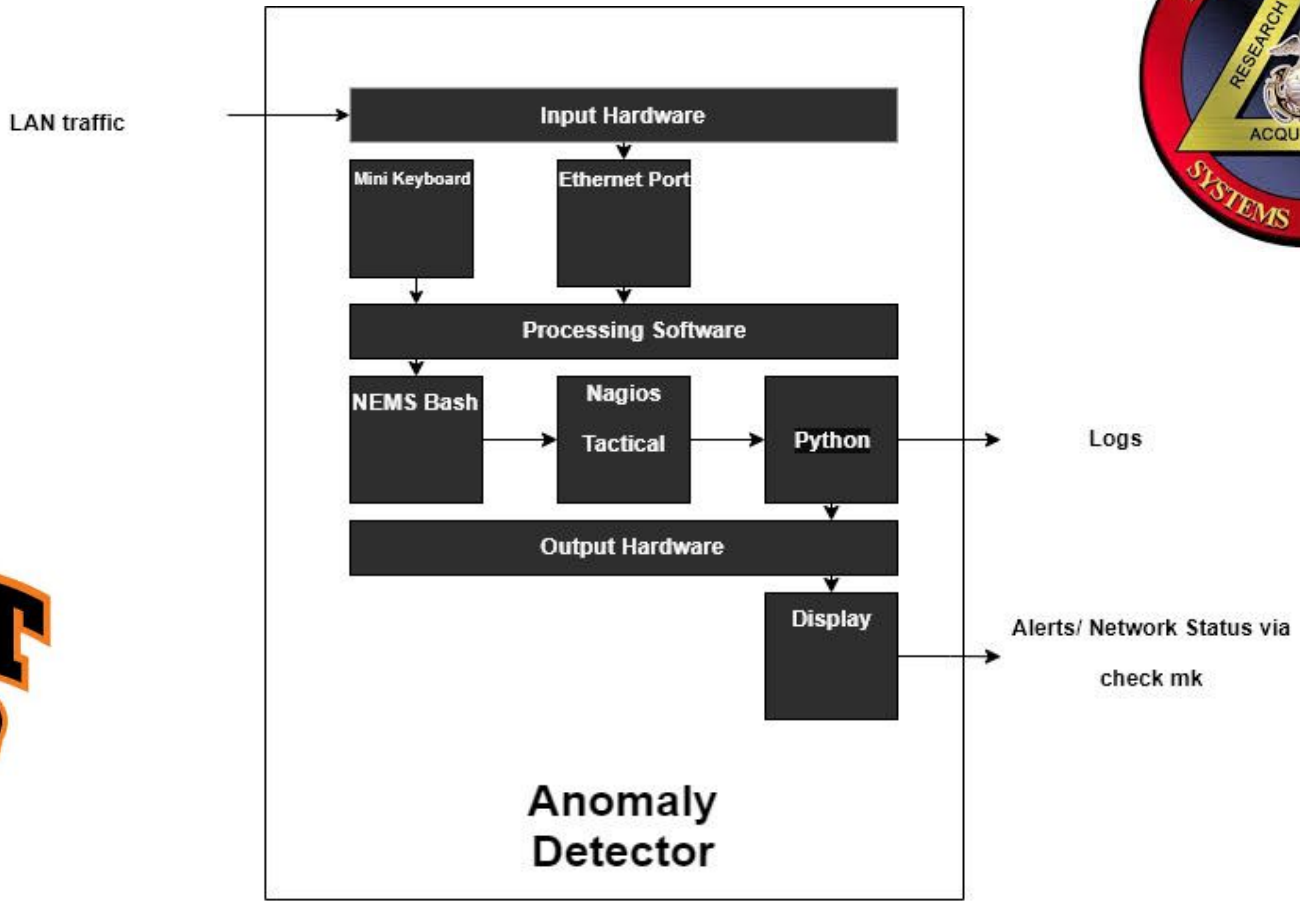
MVP (small scale) Development

Implementation/Development (6-10 Months)

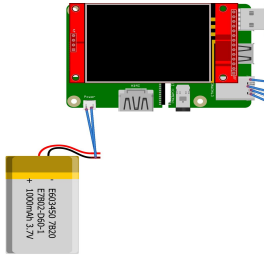
Update Future Directorate on focused product



System Model

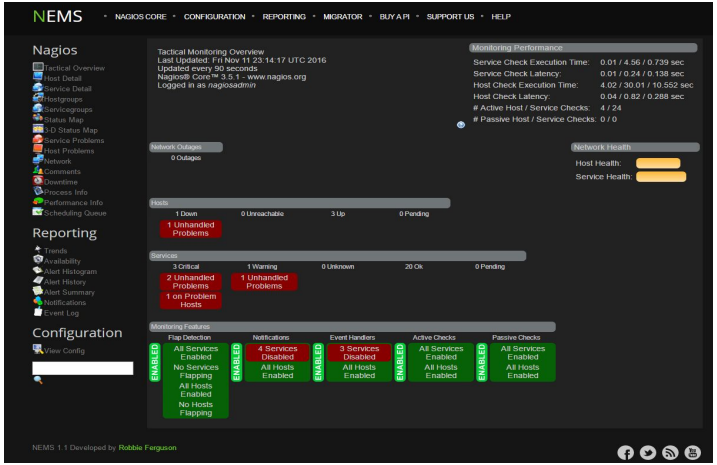


Minimum Viable Product



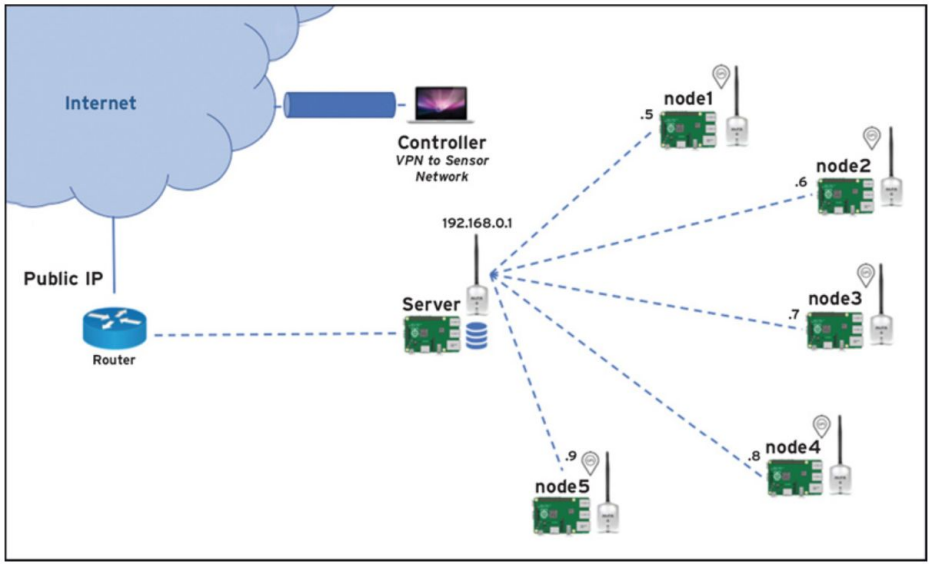
Hardware/Software

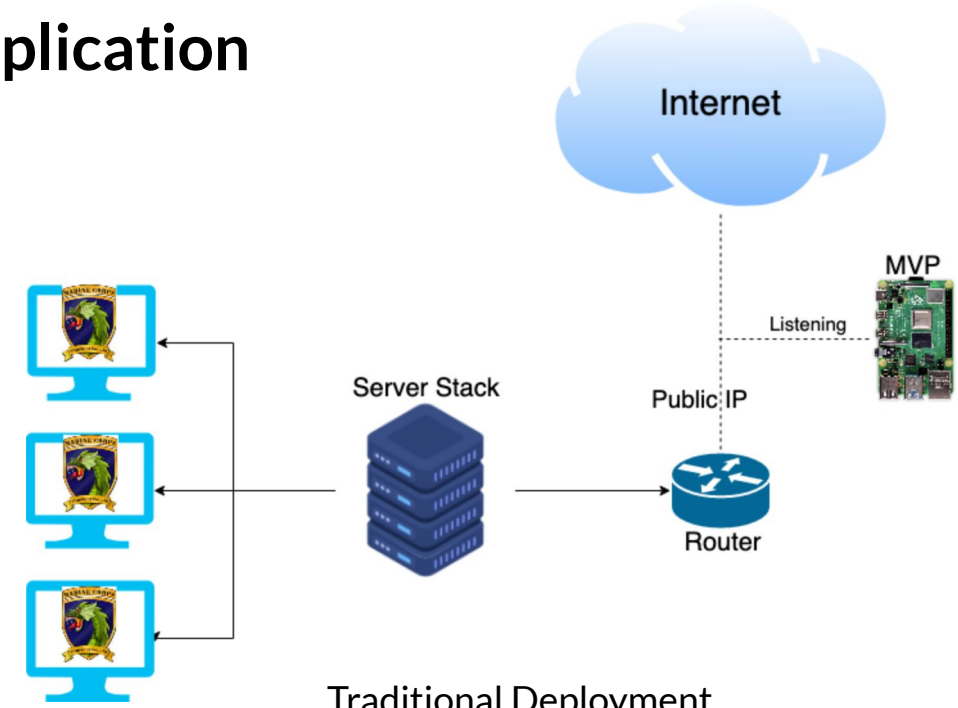
- **Computing / Logic** : Raspberry PI 3, NEMS bash, Nagios Tactical, Python for a Naive Bayes Classifier
- **Traffic Stream**: Ethernet network adaptor
- **Power and Input** : Mini Wireless Keyboard, USB Battery
- **Output** : LCD Screen, Signal data



MVP Application

Advanced Deployment



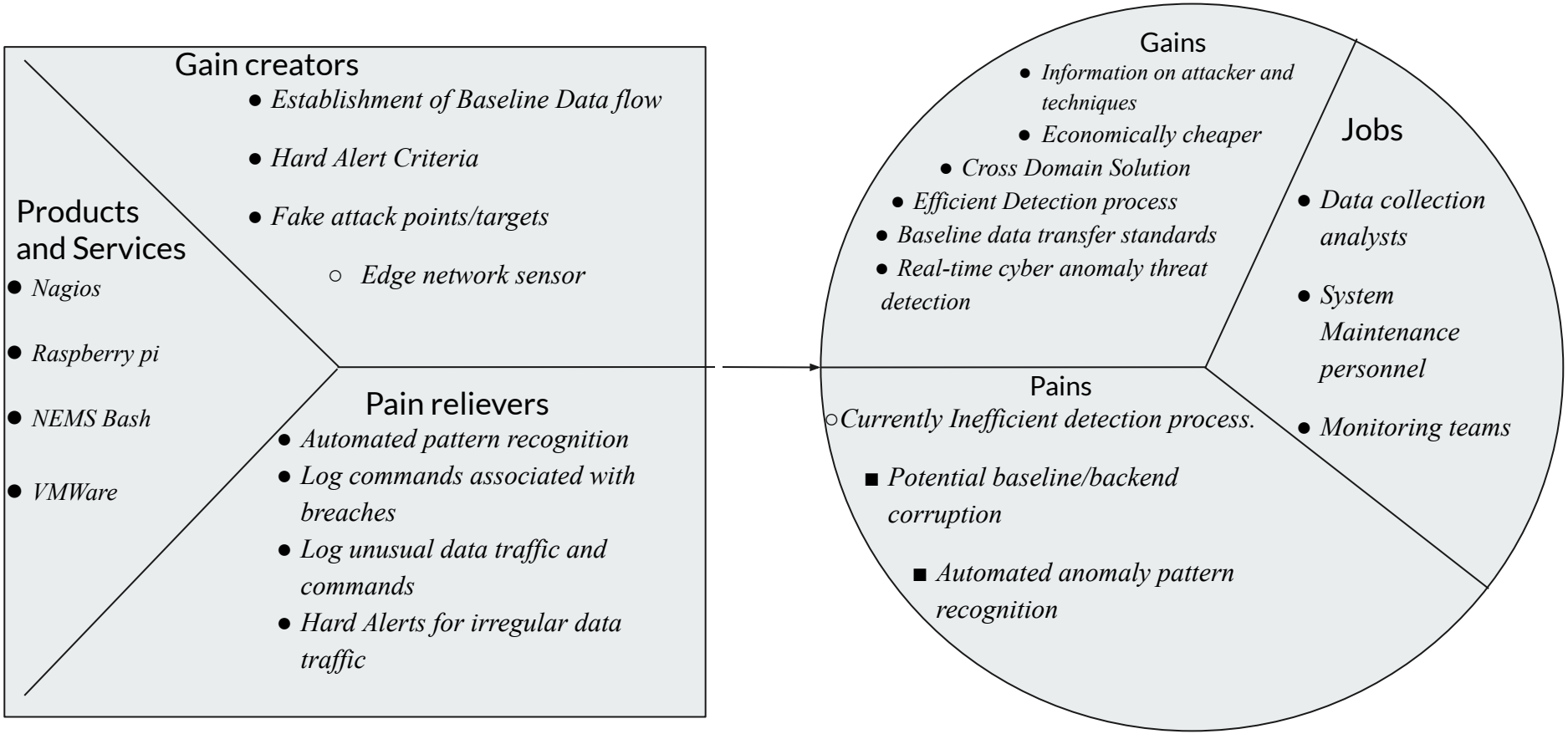


Traditional Deployment

Value Proposition Canvas

Value: Data Traffic Flow Monitoring & Alert Criteria

Beneficiaries: MARCORSYSCOM (Captain Dale), MARFORCYBER (Captain Salazar), Futures Directorate



Stage 2.1 : Government Submission

Potential cooperation with Rapid capabilities office **(Rapid Funding)**

Upon approval: General's Presentation

Upon General's Presentation Approval: **Funds Awarded**

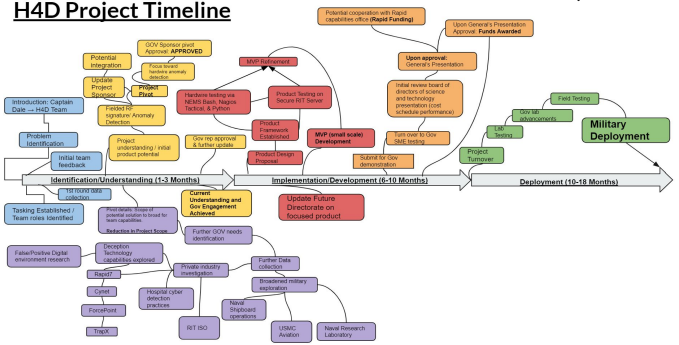
Turn over to Gov SME testing

Initial review board of directors of science and technology presentation (cost schedule performance)

Submit for Gov demonstration

Implementation/Development (6-10 Months)

H4D Project Timeline



Resources/Activities/Partners Over Time

Customer Discovery	Outreach	Approval	Funding	Testing	Manufacturing
↓	↓	↓	↓	↓	↓
	 		 		
					

Partners, Resources, & Activities

Resources

- RIT Faculty
- Security Labs
- VMs - Windows OS
- Security Softwares
- Interviewees & connections
- Research Papers

Activities

- Interviews
- Testing
- System Modeling

Classname
+ field: type
+ method(type): type

- Anomaly Detection
- Research
- Communication

Team

Key Partners

- MCWL (Captain Dale)
- MARFORCYBER (Captain Salazar)
- CSEC & Networking Department

Stage 3: Deployment

Field Testing

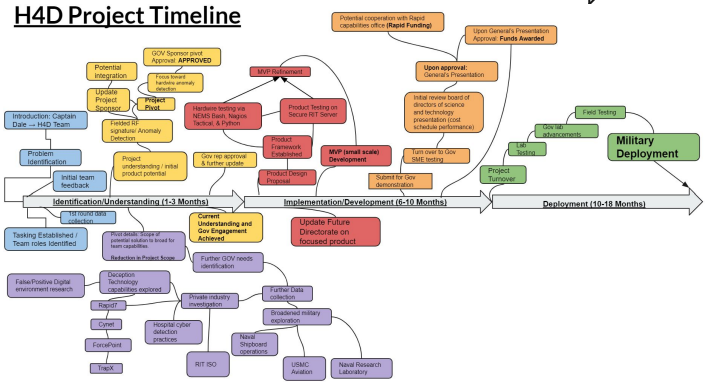
Gov lab advancements

Lab Testing

Military Deployment

Project Turnover

Deployment (10-18 Months)



RISK MANAGEMENT FRAMEWORK (RMF)

Authority To Operate (ATO)

Interim ATO

- "Conditional" ATO in effect for (6) Months
- Granted during development or prototype phase

Initial ATO

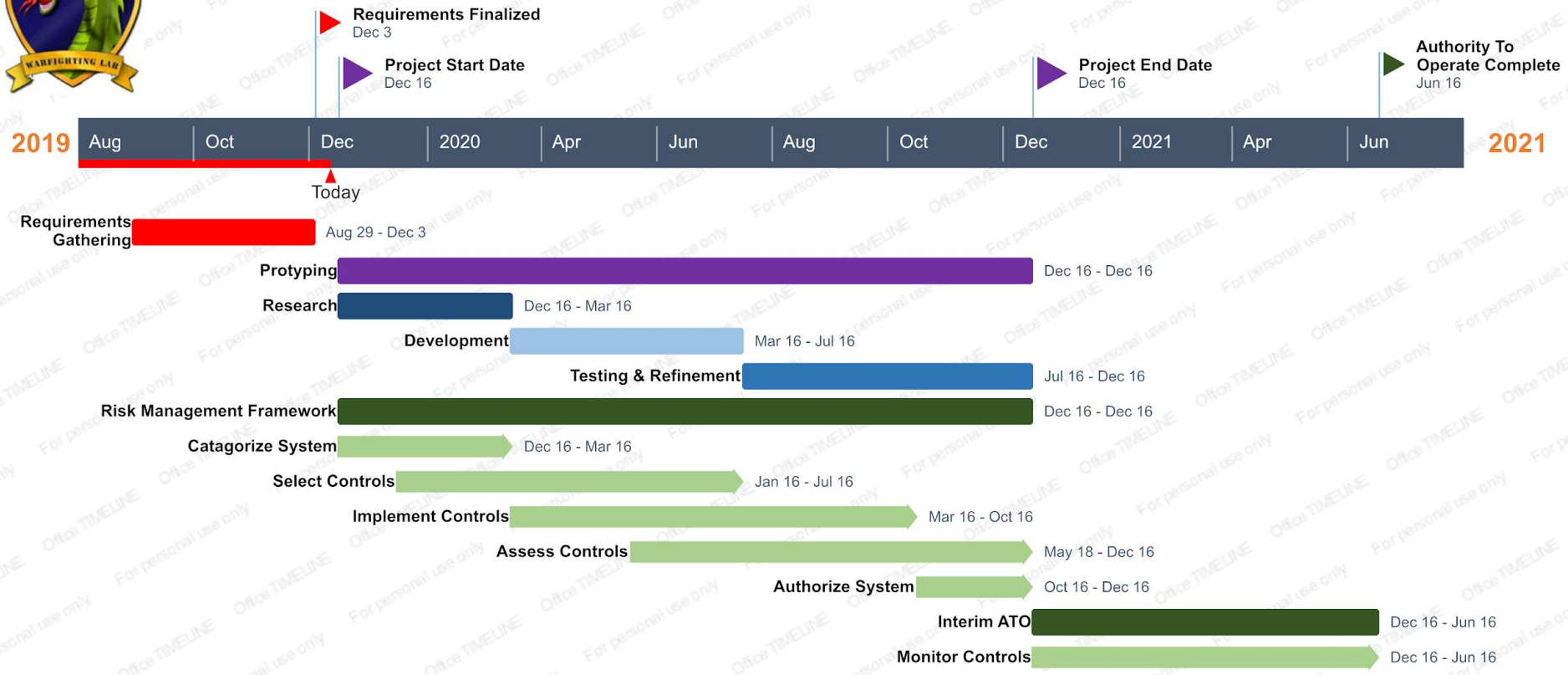
- Must be accomplished before "going live"
- Must occur every (3) years at a minimum

Continuous Monitoring

Reauthorization

- Due after (3) years or significant change to system Risk Level

Gantt Chart



Cyber Anomaly Detection

Speculated Project Budget

The Color of Money

- **OMA**: Operational $'s used for day to day operations
  - Can be used to buy things under $250k and and demonstrate things
  - Can't build prototypes
  - Good for one year - expires at the end of the fiscal year (Sep)
- **OPA**: Procurement $ used to buy major end items (big stuff that costs a lot of $)
  - Good for three years – expires a the end of the 3rd year
  - Can't be used to pay for operations
- **RDT&E**: Research Development, Testing & Evaluation $
  - Good for 2 years – expires a the end of the 2nd year
- **Special cases**
  - "Purple" money (JIDO)
    - Can be used as any of the three above
    - Comes with lots of Congressional oversight
  - Rapid Acquisition Authority – SecDef has the authority to change the "color" of $
    - $200M per year
    - Requires Congressional notification
  - OCO – overseas contingency operations - $'s that pay for missions not part of the budget (Iraq/Afg/Ebola)
  - Continuing Resolutions – Can't plan to spend more than 65% of previous budget

➢ **OMA** (Good for 1yr)**: (Potential Seed: $100,000)**

- **Needed: ($210,000.00)**
  - (3) Engineers: [2] RIT Graduates & [1] SME ($200,000)
  - Small Office with central air ($7,200)

➢ **OPA** (Good for 3yrs)**: $570,625.00**

- 3 Laptop ($6,000)
- 2 Server ($250,000)
- 5 Raspberry Pi ($500.00)
- Hardware Destruction($64,125 [25% buffer])
- 1 extra server & hardware ($150,000)
- Additional backup materials: Drives, Raspberry Pi's, Software ($100,000)

➢ **RDT&E** (Good for 2 years) **: $500,000.00**

- Research and Development
- Database/Experimental Environment creation

***** Project Total: $1,300,000.00*****

Project Burn Chart

BURN RATE CALCULATOR [H4D]		
H4D		**H4D**
Starting date		**Dec 12, 2019**
Total cash in bank	$	-
Where is the money coming from?		
Starting Fund [OMA]	$	210,000
OPA (3yr value)	$	320,625
RDT&E (2yr value)	$	500,000
Special Case ("Purple")	$	250,000.00
Total income (A)	**$**	**1,280,625**
Where is the money going?		
Employee salaries	$	(200,000)
Lease / office rent	$	(7,200)
Server Purchase	$	(250,000)
Laptop Purchase	$	(6,000)
Raspberry PI	$	(500)
Hardware Destruction (25% buffer)	$	(64,125)
Extra Server & Hardware	$	(150,000)
Additional Misc Materials	$	(100,000)
Total spending (B)	$	(777,825)
Monthly cash earn [burn] (A - B)	**$**	**502,800**
Cash zero month		**Jun-2021**
Runway left (months)		**18**

Cyber Anomaly Detection

Edge packet inspection with probabilistic alerting

Project Cost: $1,300,000 (OMA $210K; OPA $570,625K; RDTE $500K)

- **First Requirement Received**: Aug 29th, 2019
- **Project Start Date**: December 16th, 2019
- **Period of Performance**: 12/2020 - 12/2022

Sponsor	FY 2020	FY 2021
USMC	$900,000	$400,000

Objective: Given a specific network, our public facing surveillance nodes will analyze all incoming & outgoing data traffic. Through packet investigation and algorithmic trend analysis baseline standards are established to create alert criteria for network security officers

Operational impact: Provide a real-time alert system for when irregular anomalies are detected. Saves time though automatic detection of botnet attacks/compromised credentials

Performers: MCWL - R&D

Interest:
MCWL (Captain Dale)
MARFORCYBER (Captain Salazar)

Delivery Date: June 16th, 2021

End Users: MCWL

Thank you for all that made this possible

Acknowledgements

Capt. Ferguson Dale, Problem Sponsor

Dr. James Santa, Course Instructor & Mentor

Dr. Richard DeMartino, Endowed Chair for Innovation and Entrepreneurship

Dr. Justin Pelletier, Director of CGI Cyber Range and Training Center

Dr. Sean Hansen, Department Chair of MIS, Marketing, and Digital Business

Dr. Bo Yuan, Department Chair of Computing Security

Interviewees, for their time and valuable insights


Hacking 4 Defense (H4D)
Solving National Security Issues with the Lean Launchpad

Questions?