

Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

© 2015 Carnegie Mellon University.

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0002537



Software Engineering Institute

Carnegie Mellon University

CERT® Alignment with Cyber COI Challenges and Gaps
SEI Webinar
© 2015 Carnegie Mellon University

Generalized Automated Cyber-Readiness Evaluator (ACE)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Rotem Guttman



Core DoD Challenge Problem

Evaluating Mission Readiness For Cyber Operators

- Scalable
- Objective
- Reliable
- Valid

US cyberspace force to expand further -
Pentagon chief



Photo: EPA

US Defense Secretary Chuck Hagel said Friday the cyberspace force at US Cyber Command will grow to **more than 6,000** by the year 2016.

Polling Question

Do you know how evaluations are currently being conducted?

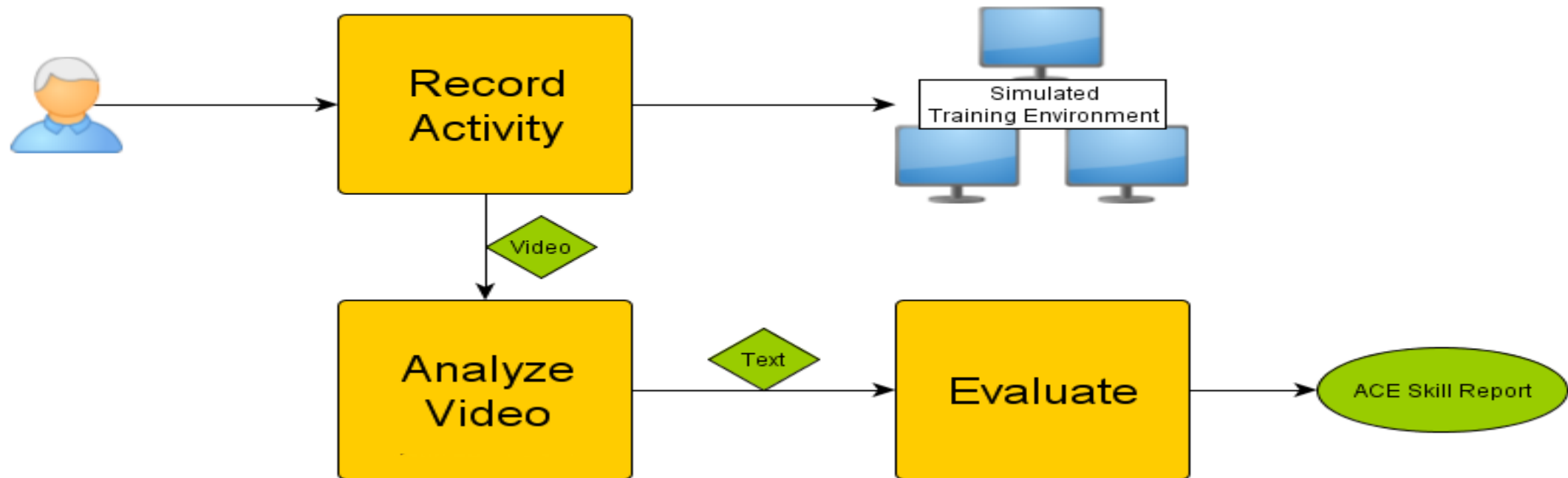
ACE

- Develop Automated Cyber-Readiness Evaluator.
- System will:
 - Place users in a cyber operator scenario similar to their normal work environment.
 - Allow users to perform cyber operator tasks in that scenario.
 - Understand the actions of the user within the scenario.
 - Verifiably determine a user's mission readiness based on their actions within the scenario.
- Benefits:
 - Automated analysis
 - Specific deficiencies isolated
 - Automated remediation plans
 - Recording available for future review

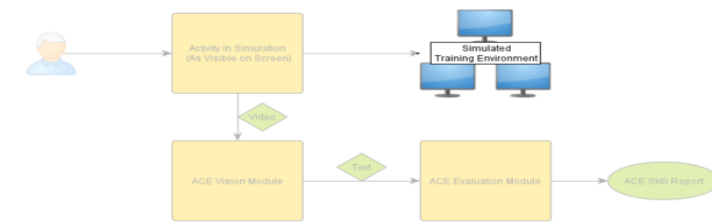
Technical Approach

Automated Cyber-Readiness Evaluator (ACE)

- Evaluate mission readiness by tracking actual performance



Technical Approach



Role Choice

- Forensic Analyst
- 2 Hours
- Matching DoD Standards



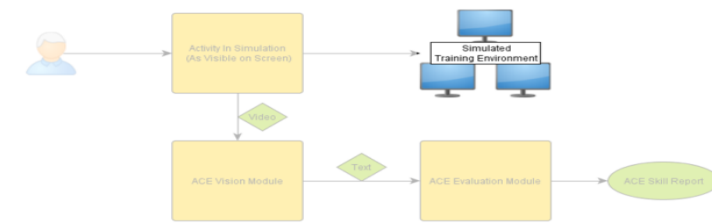
**Joint Cyberspace Training &
Certification Standards (JCT&CS)**

Technical Approach

Scenario I & II Details

- Missing Person
 - Foul Play Suspected
- Classified* Documents Exfiltrated
 - Computer Drive Image
 - Multiple Layers of Story
 - APT1
 - USB
 - Personal Email

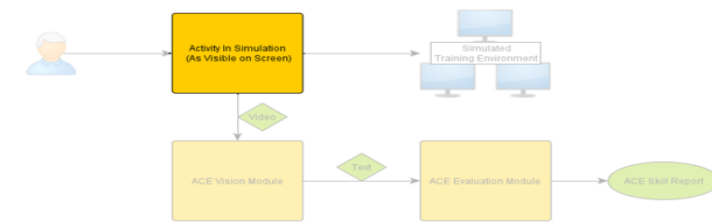
* Fabricated documents (Not actual classified data)



Technical Approach

Data Capture Capability

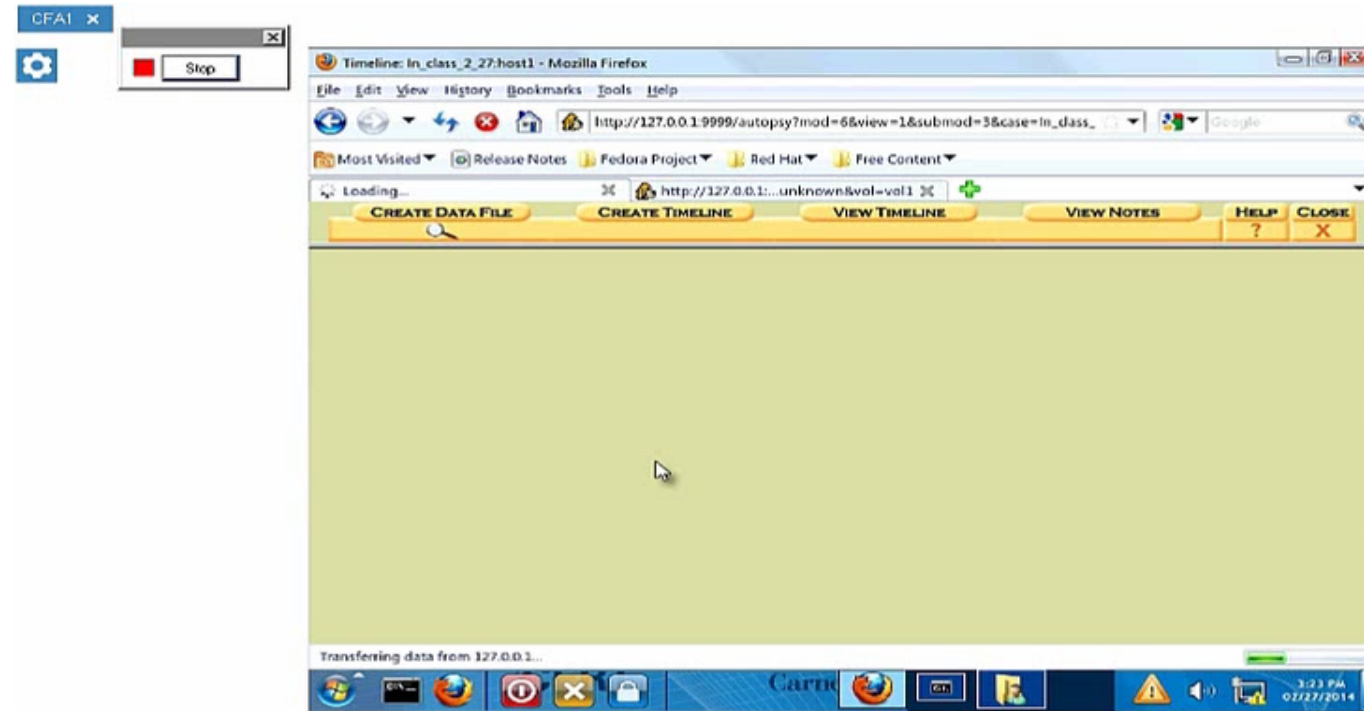
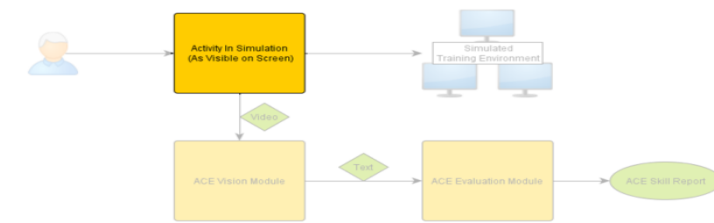
- Background Data Collection
- Restricted to Environment
- Scalable



Technical Approach

Data Collection

- CERT Staff
- CMU Graduate Students
- GCD Participant Groups
- DoD Personnel
- NCFTA Volunteers
- Pending: CMU Information Security Office



Polling Question

What Makes Computer Vision Difficult?

CREATE DATA FILE

CREATE TIMELINE

VIEW TIMELINE

VIEW NOTES

HELP

CLOSE

Creating Timeline using all dates (Time Zone:)

Timeline saved to /home/examiner/Autopsy/In_class_2_27/host1/output/all.txt

Entry added to host config file

Calculating MD5 Value

MD5 Value: BC9CCC8A1240EF450523D8B90182DB64

OK

(NOTE: It is easier to view the timeline in a text editor than here)

Done



CREATE DATA

Creating Timeline us

Timeline saved to /h

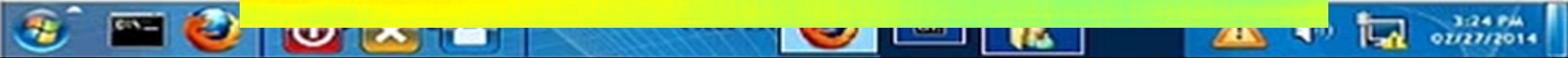
Entry added to host c

Calculating MDS Valu

MDS Value: BC9CCC

OK

(NOTE: It is easier to



HELP ? CLOSE X

CREATE DATA FILE

CREATE TIMELINE

VIEW TIMELINE

VIEW NOTES

HELP

CLOSE

Creating Timeline using all dates (Time Zone:)

Timeline saved to /home/examiner/Autopsy/In_class_2_27/host1/output/all.txt

Entry added to host config file

Calculating MD5 Value

MD5 Value: **BC9CCC8A1240EF450523D8B90182DB64**

OK

(NOTE: It is easier to view the timeline in a text editor than here)

| | A | B | C |
|-----|---------|---|---------|
| 148 | 0:50:52 | Focused on Shell2 Window | GUI |
| 149 | 0:51:00 | Focused on Shell4 Window | GUI |
| 150 | 0:51:13 | sudo autopsy | Shell4 |
| 151 | 0:51:17 | Shell Link Menu opened | Shell4 |
| 152 | 0:51:18 | "Open Link" clicked | Shell4 |
| 153 | 0:51:22 | Focused on Mozilla Firefox Window - http://localhost:9999/autopsy | GUI |
| 154 | 0:51:24 | Firefox "File" Menu opened. | Firefox |
| 155 | 0:51:26 | "Work Offline" menu option clicked | Firefox |
| 156 | 0:51:27 | "Try Again" button clicked. | Firefox |
| 157 | 0:51:30 | "New Case" button clicked | Autopsy |
| 158 | 0:51:34 | Case name: "Silver" | Autopsy |
| 159 | 0:51:41 | Case description: "Missing Persons - Saul Silver" | Autopsy |
| 160 | 0:51:44 | Case Investigator A: "Rotem Guttman" | Autopsy |
| 161 | 0:51:50 | Case Investigator B: "Josh Hammerstein" | Autopsy |
| 162 | 0:51:51 | "New Case" button clicked | Autopsy |
| 163 | 0:51:52 | "Add Host" button clicked | Autopsy |
| 164 | 0:51:59 | gedit switched to investigator_notes | Gedit |
| 165 | 0:52:02 | gedit switched to string_search1.txt | Gedit |
| 166 | 0:52:06 | gedit "Find" window opened | Gedit |
| 167 | 0:52:07 | gedit "Find" button clicked - search for: "hostname" | Gedit |
| 168 | 0:52:09 | gedit switched to string_search1.txt | Gedit |
| 169 | 0:52:18 | Focused on Mozilla Firefox Window - http://localhost:9999/autopsy?mod=0&view=7&case=Silver&x=83&y=6 | GUI |
| 170 | 0:52:21 | Host Name: "saul-n3eruqnyq5" | Autopsy |
| 171 | 0:52:39 | Host Description: "Saul Silver's Computer" | Autopsy |

Stop



The screenshot shows a Windows desktop environment. In the foreground, a Notepad window titled 'Investigative_Notes (-/-case) - gndit' contains the following text:

```

Many Indications of gambling
Possible persons of interest
Vincent Vega
Ted Jones
Possible location of interest
Kings Creek Cemetery up in P
Possible username:
saulsilversurfer
grama.tambelli
Utilized apps: Skype (check
Possible email address:
vncnt.vega94@gmail.com
saulsilversurfer@gmail.com
Possible conversation log:
254272366 WhatSapos;s going
437146900 hey Saul
437149050 I don't mess around Saul, I know you're around
551199446 D(["gn", "Saul Silver"])
551424052 #saulsilversurfer/sgrama.tambelli;7e9eb883ae020c5a
551425050 saulsilversurfer
551426844 Saul, no dice on Philly
1623796399 #saulsilversurfer/sgrama.tambelli;6f3ff4df24c03e263
1623796454 grama.tambelli saulsilversurfergrama.tambelli saulsilversurfergrama.tambelli saulsilversurferGrana Tambelli | Yo G-man, this a
good time??
1623796679 saulsilversurfer
1623796814 #saulsilversurfer/sgrama.tambelli;7e9eb883ae020c5a

```

In the background, a terminal window titled 'examiner@fc14-foren-2011-01-1386--' shows the following commands and output:

```

[examiner@fc14-foren-2011-01-1386 ~]$ ls
bin case core.2810 Desktop Documents Downloads Pictures temp Volatility sp.dd
[examiner@fc14-foren-2011-01-1386 ~]$ echo "grama.tambelli" > case/dirty_words5.txt
[examiner@fc14-foren-2011-01-1386 ~]$ grep -i -f case/dirty_words5.txt > case/string_search6.txt

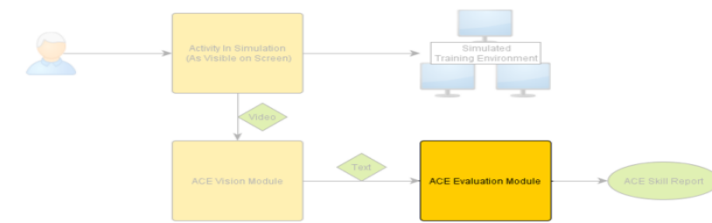
```

The taskbar at the bottom shows the Windows Start button, several application icons, and the system tray with the date and time: 11:27 AM 12/03/2013.

Admin Team Chat with Admin Team

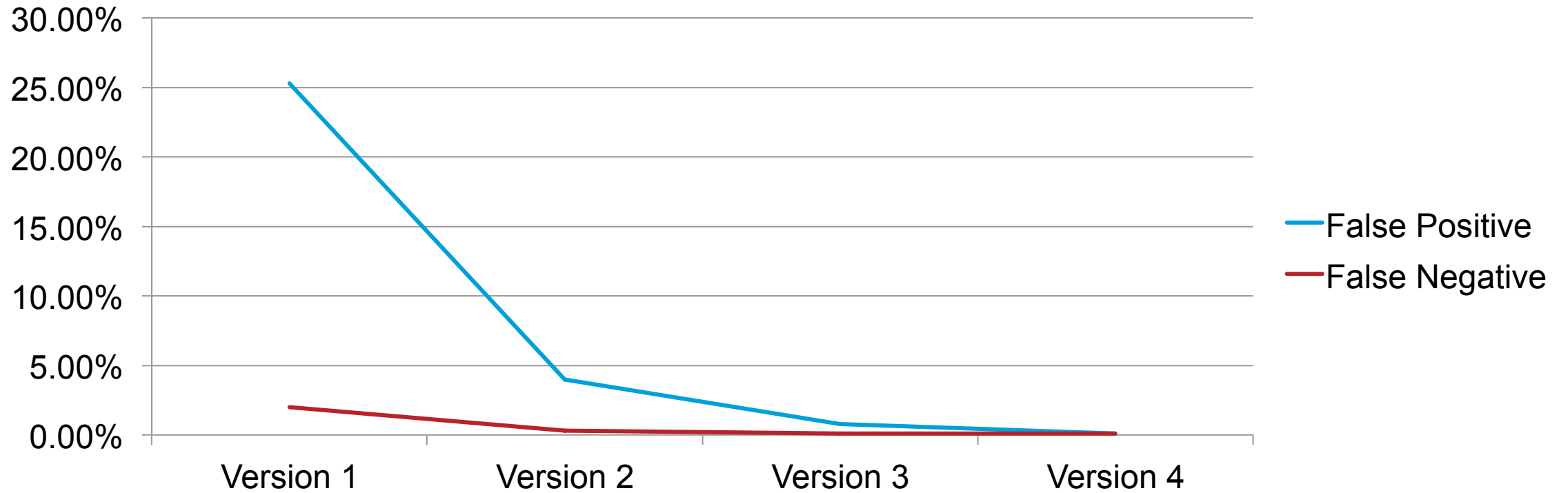
Focused on Shell2 Window (GUI)

Evaluation Module – Layer 2



- Developing evaluation module that will make final mission-readiness determination
- Status: In-Progress
 - Collaboration with CMU Robotics Institute – Machine Learning department
- Currently exploring multiple methods
 - Hidden Markov Models, Spectral Methods, Path Analysis

Results



Expected Outcomes

- Automated Assessment - Individual
- Extendable Roles
- Time and Money saved for DoD
- Follow On Work
 - Group Evaluation
 - Data-Backed Standards
 - Secondary Uses for Vision System (Research Enabling Tool)