Cyber Attack Orchestration Test Bed for Automation and Threat Monitoring in Virtual Environment (CTAM)

Dr. Leonel Lagos
Principle Investigator
Florida International University
lagosl@fiu.edu

Dr. Himanshu Upadhyay
Co-Principle Investigator
Florida International University
upadhyay@fiu.edu

Research Funded by
OSD Test Resources Management Center
T&E S&T Program, Cyberspace Test Technology
Project Description

- CTAM is a Cyberspace Test Technology for T & E purposes to monitor and analyze behavior during cyber attacks and also the impact on the current mission.
- CTAM is based on fine-grained introspection of kernel data structures, data collection and advanced cyber analytics using Artificial Intelligence / Machine Learning techniques.
- CTAM consists of three platforms:
  - Virtualization
  - Advanced Cyber Analytics
  - Test Control Center
CTAM System Diagram

Virtualization Platform
- Hypervisor
- Security & Kernel Agent
- Smart Memory Acquisition
- Introspector

Advanced Cyber Analytics
- Database Server
- Machine Learning Model
- Prediction and Data Analytics

Test Control Center
- Testbed Monitoring
- Test Case Management
- Data Analytics & Visualization
- Operator
- Virtual Machine Administration

Malware Repository

Advancing the research and academic mission of Florida International University.
System Overview

CTAM – System Overview

Test Control Center
- Virtual Machine Administration
- Testbed monitoring to observe Malware impact
- Manage multiple models and testcases
- Visualize Data Analytics results
- Malware management

Test Vector Repository

Cyber Analytics Platform
- Machine Learning Algorithms
- Build machine learning models from training data
- Analyze test data using machine learning models
- Database and Analytics Server
- Security/Kernel Listener for data transfer

Virtualization Platform
- System Under Test Linux/Windows VM
- Smart Memory Acquisition with LibVM/VI
- Security and Kernel Agent/Drivers for data extraction
- Security/Kernel Monitor for data transfer
- Intrinspector for Command and Control

- Xen Hypervisor

Virtualization Platform
- System Under Test Linux/Windows VM
- Smart Memory Acquisition with LibVM/VI
- Security and Kernel Agent/Drivers for data extraction
- Security/Kernel Monitor for data transfer
- Intrinspector for Command and Control

- QEMU/KVM Hypervisor

Cyber Threat Automation and Monitoring System

Advancing the research and academic mission of Florida International University.
CTAM - Virtualization

- Virtualization platform is built on Xen and KVM hypervisors
- System under test includes Linux /Windows virtual machines
- LibVMI library for Virtual Memory Introspection
- Security and kernel agent / drivers for data extraction
- Security kernel monitor for data transfer from the virtualization platform to the database server
- Introspector to send commands to the System under test from Test control center
CTAM – Virtualization

Following data structures are implemented

- Process List Structure
- System Call Structure
- Interrupt Descriptor
- Invariant System Call
- Networks Socket
- File Monitor
- DLL Injection Monitor
CTAM – Cyber Analytics

- Cyber Analytics module consists of Database server and Machine learning server for in-memory analytics.
- Machine learning models with different algorithms are built using the training data.
- Models are used to predict the impact of the test vectors on a specific mission.
Following machine learning algorithms are implemented:

- Random Forest
- Support Vector Machine
- Logistic Regression
- Gradient Boosting
- Neural Network
- Ensemble
Test Control Center (TCC) consists of following modules:

- VM Management
- Model Management
- Test Case Management
- Test Vector Management
- Network Map
- Testbed Administration
- Configuration
- Introspector Configuration
- Help
### TCC - VM Management

![Cyber Threat Automation and Monitoring](image)

**VM Hosts Available**

- **Connect to Host(s):**
  - XEN
  - KVM

**Virtual Machine Manager**

<table>
<thead>
<tr>
<th>Host ID</th>
<th>Host Name</th>
<th>VM UUID</th>
<th>VM Name</th>
<th>OS</th>
<th>O State</th>
<th>Status</th>
<th>Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>11144</td>
<td>Hypervisor 110 - Rene</td>
<td>af9b404d-972c-4f65-a5e1-0956b27bd0ce</td>
<td>Linux-Rene</td>
<td>Linux</td>
<td></td>
<td>Running</td>
<td>Healthy</td>
</tr>
<tr>
<td>11144</td>
<td>Hypervisor 110 - Rene</td>
<td>709e2220-a3a0-4a20-ace8-ad247ab2b0e9</td>
<td>Hardik VM QA_QC</td>
<td>Windows</td>
<td></td>
<td>Stopped</td>
<td>Healthy</td>
</tr>
<tr>
<td>11144</td>
<td>Hypervisor 116 - Rene</td>
<td>af025ba0-9354-4644-b226-151a14f9072</td>
<td>Windows-Rene2</td>
<td>Windows</td>
<td></td>
<td>Running</td>
<td>Healthy</td>
</tr>
<tr>
<td>11144</td>
<td>Hypervisor 116 - Rene</td>
<td>45dbdc5b-5754-440c-9a8a-476b64a30a4</td>
<td>TCC-Linux</td>
<td>Linux</td>
<td></td>
<td>Stopped</td>
<td>Healthy</td>
</tr>
<tr>
<td>11144</td>
<td>Hypervisor 116 - Rene</td>
<td>489c0ed-4351-4269-bbba-9b8058ed3bf</td>
<td>windows-srujana</td>
<td>Windows</td>
<td></td>
<td>Stopped</td>
<td>Healthy</td>
</tr>
</tbody>
</table>
TCC – Model Management

Model Management

Model Type: Manual
Hypervisor: Xen, KVM
Host: HyperVisor 142 KVM

Current Model ID: None

Model Definition
Model Name: Model1-KVM-Windows
Model Description: Model1-KVM-Windows
Scan System Processes

Baseline Selection
Connect to VM
Start Baseline Scan
Complete Benign Selection

Show Results
TCC - Test Case Management

Test Case Management

Test Case Definition
- Test Case Name: Testcase1-KVM-Window
- Test Case Description: Testcase1-KVM-Window
- User Model: Malware/AV System Model
- Select Model: KVM-Mode1-04162018

Baseline Selection
- Please follow the steps below in order to get the proper baseline scan:
  1. Connect to VM
  2. Run baseline user applications
  3. Run a baseline scan
- Connect to VM
- Get Applications
- Select Application
- Start Baseline Invariant Scan
- Start Baseline DLL Scan
- Complete Baseline Selection

Test Vector Installation
- Please follow the steps below in order to test vector scan:
  1. Connect to VM
  2. Install malware or other test vectors
  3. Run a test vector scan
- Connect to VM
- Start Malware Invariant Scan
- Start Malware DLL Scan
- Start Plugin Scan
- Complete Test Vector Selection

Test Prediction
- Algorithms:
  - Random Forest
  - Support Vector Machine
  - Logistic Regression
- Run Test Case Prediction

Current Test Case ID: 888
### Test Vector Management

<table>
<thead>
<tr>
<th>MalwareID</th>
<th>MalwareName</th>
<th>Version</th>
<th>FileName</th>
<th>FileType</th>
<th>Classification</th>
<th>Select Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Banker-NBH</td>
<td>0.57</td>
<td>00a685184992808a48e5e6b2c37ccf29</td>
<td>Win32 EXE</td>
<td>Trojan</td>
<td>Select</td>
</tr>
<tr>
<td>3</td>
<td>Cryptor</td>
<td>0.8</td>
<td>0477bea2a27266a6732b018edc408d9ae</td>
<td>Win32 EXE</td>
<td>Virus</td>
<td>Select</td>
</tr>
<tr>
<td>4</td>
<td>Emotet-AI</td>
<td>none</td>
<td>0a9e56289d5373245865996823db6bc1</td>
<td>None</td>
<td>Trojan</td>
<td>Select</td>
</tr>
<tr>
<td>5</td>
<td>Adload</td>
<td>0.49</td>
<td>0ab8e438e608e470d317e7c52fa42bb</td>
<td>Win32 EXE</td>
<td></td>
<td>Select</td>
</tr>
<tr>
<td>6</td>
<td>AdwareSig</td>
<td>0.2</td>
<td>0b08a394f3343463ca54f0e1cfcfb31</td>
<td>None</td>
<td>Adware</td>
<td>Select</td>
</tr>
<tr>
<td>7</td>
<td>BrowseFox.BU</td>
<td></td>
<td>0b7880d1cd7a993dd3f75e5d404ecc0c</td>
<td>None</td>
<td></td>
<td>Select</td>
</tr>
<tr>
<td>8</td>
<td>Agent-AQRA</td>
<td></td>
<td>10a4a462896fa5b6c569f14dc4ae722</td>
<td>Win32 EXE</td>
<td></td>
<td>Select</td>
</tr>
<tr>
<td>9</td>
<td>Malware-gen</td>
<td></td>
<td>8e4c3f6f1f8b75ed18f8b7250905f689</td>
<td>None</td>
<td></td>
<td>Select</td>
</tr>
<tr>
<td>10</td>
<td>GenMaliciousA-THX</td>
<td></td>
<td>9d2fcaed2109fbda24af5895e8d42d99</td>
<td>None</td>
<td></td>
<td>Select</td>
</tr>
<tr>
<td>11</td>
<td>AutoRun-BOW / Worm.VB.NZQ</td>
<td></td>
<td>c71892b3f3a19d12f82401be8f61679</td>
<td>Win32 EXE</td>
<td></td>
<td>Select</td>
</tr>
</tbody>
</table>

- **Search Test Vector:**
- **Select Malware:**
- **Add Malware**

Select Malware to display additional properties
CTAM - Test Vector Management - Analysis

<table>
<thead>
<tr>
<th>Hash</th>
<th>File Type</th>
<th>Sub System</th>
<th>File Type Extension</th>
<th>File Size</th>
<th>Select Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa98326ecb641af3e0eb9666f6a91905</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>272.0 KB (278528 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>aa99b27d0b502f7f7dea1d4f20fca71d</td>
<td>Win32 EXE</td>
<td>Windows GUI</td>
<td>exe</td>
<td>974.2 KB (997624 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>aa9e7f117cb98655073180e233cf3187</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>272.0 KB (278528 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>aa9b244b91866ca6c54b46d4556542c2</td>
<td>Win32 EXE</td>
<td>Windows GUI</td>
<td>exe</td>
<td>405.4 KB (415127 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>aa9d14e8b35287db19c51d688e2eeb7f</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>21.8 KB (22342 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>aa9e101b5f203dd040b99d66a486df9f</td>
<td>Win32 EXE</td>
<td>Windows GUI</td>
<td>exe</td>
<td>705.8 KB (722693 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>aae076224s524064a1657718f1666c</td>
<td>Win32 EXE</td>
<td>Windows GUI</td>
<td>exe</td>
<td>908.7 KB (930533 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>e8b897df91331e4e8ac7134e4459bcff</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>177.5 KB (181760 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>e9a429a87d872b23993e82546dfcfeeb</td>
<td>Win32 EXE</td>
<td>Windows GUI</td>
<td>exe</td>
<td>164.5 KB (168448 bytes)</td>
<td>Select</td>
</tr>
<tr>
<td>e9aad5a98c64221d5c44c2c659cb0c6</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>9.0 KB (9276 bytes)</td>
<td>Select</td>
</tr>
</tbody>
</table>

Select Malware to display additional properties
CTAM - Network Map

[Diagram of VM Network Map with various nodes and connections labeled with different operating systems and names like Windows-Paul, Linux-Rene, Windows-KVM, etc.]
Advancing the research and academic mission of Florida International University.

CTAM - Network Map – List View

VM Network Map

Switch View | TestBed View - List | TestBed View - Blocks

TCC-Linux
- Host: Hypervisor 116
- OS: Linux
- State: Stopped
- Status: Healthy

windows-srujana
- Host: Hypervisor 116
- OS: Windows
- State: Stopped
- Status: Healthy

Windows-azizul
- Host: Hypervisor 116
- OS: Windows
- State: Running
- Status: Healthy

Windows-Test-David
- Host: Hypervisor 116
- OS: Windows
- State: Running
- Status: Healthy
## Model Administration

<table>
<thead>
<tr>
<th>Model ID</th>
<th>VM Name</th>
<th>Operating System</th>
<th>Model Name</th>
<th>Description</th>
<th>Data Structure Name</th>
<th>Benign Application</th>
<th>Malware Application</th>
<th>User Name</th>
<th>Inserted On</th>
</tr>
</thead>
<tbody>
<tr>
<td>692</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model12</td>
<td>SK-Win142-KVM-Model12</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 2:15:32 PM</td>
</tr>
<tr>
<td>691</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model11</td>
<td>SK-Win142-KVM-Model11</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 2:09:43 PM</td>
</tr>
<tr>
<td>690</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model10</td>
<td>SK-Win142-KVM-Model10</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 1:49:12 PM</td>
</tr>
<tr>
<td>689</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model9</td>
<td>SK-Win142-KVM-Model9</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 12:20:33 PM</td>
</tr>
<tr>
<td>688</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model8</td>
<td>SK-Win142-KVM-Model8</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 12:08:04 PM</td>
</tr>
<tr>
<td>687</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model7</td>
<td>SK-Win142-KVM-Model7</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 11:36:09 AM</td>
</tr>
<tr>
<td>686</td>
<td>Windows-Persistant</td>
<td>model test kvm</td>
<td>model test kvm</td>
<td>model test kvm</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 11:29:59 AM</td>
</tr>
<tr>
<td>685</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model6</td>
<td>SK-Win142-KVM-Model6</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 11:17:00 AM</td>
</tr>
<tr>
<td>684</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model6</td>
<td>SK-Win142-KVM-Model6</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 11:12:53 AM</td>
</tr>
<tr>
<td>683</td>
<td>Win142_sk</td>
<td>Windows</td>
<td>SK-Win142-KVM-Model5</td>
<td>SK-Win142-KVM-Model5</td>
<td>Process List</td>
<td>N/A</td>
<td>N/A</td>
<td>Admin</td>
<td>4/25/2018 11:07:16 AM</td>
</tr>
<tr>
<td>Test Case ID</td>
<td>VM Name</td>
<td>Model Name</td>
<td>TestCaseName</td>
<td>BenignApplication</td>
<td>MalwareApplication</td>
<td>InsertedOn</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>874</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model20 without sys-processes</td>
<td>sk-test-without-sys-processes-1</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 5:02:06 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>873</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model17</td>
<td>sk-Test1-apr-26-18</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 4:01:19 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>872</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model15</td>
<td>sk-Test1-apr-26-17</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 3:36:31 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>871</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model15</td>
<td>sk-Test1-apr-26-16</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 3:32:11 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>870</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model15</td>
<td>sk-Test1-apr-26-15</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 3:28:20 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>869</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model15</td>
<td>sk-Test1-apr-26-14</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 3:02:18 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>868</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model9</td>
<td>sk-Test1-apr-26-13</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 2:50:18 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>867</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model9</td>
<td>sk-Test1-apr-26-12</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 2:28:13 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>866</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model9</td>
<td>sk-Test1-apr-26-11</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 11:33:20 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>865</td>
<td>Win_142_sk</td>
<td>SK-Win142-KVM-Model9</td>
<td>sk-Test1-apr-26-10</td>
<td>None</td>
<td>N/A</td>
<td>4/26/2018 11:26:41 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CTAM - Configuration

Cyber Threat Automation and Monitoring

VM Color Configuration

- Description: VM State
  - Running
  - Stopped
  - Paused
  - Normal
  - Suspect
  - Infected
- Color Hex Value
- Color Code: 1, 5, 3, 6, 7, 8
- Comments:
  - Hypervisor VM return code
  - Hypervisor VM return code
  - Hypervisor VM return code
  - Algorithm Accuracy < 50%
  - Algorithm Accuracy between 50% and 80%
  - Algorithm Accuracy > 80%

Host Configuration

- Host ID
- HostUniqueID
- HostName
- HostIP
- HostPort
- LibvirtIP
- LibvirtPort
- AgentListenerIP
- AgentListenerPort
- TestControlCenterIP
- TestControlCenterPort
- MachineConnectPort
- MalwareRepositoryPath

- Description:
  - Hypervisor 132 KVM
  - David 111
  - Astral_111
  - Hypervisor 142 KVM
  - Hypervisor 123 Staging
- Comments:
  - 172.16.10.132
  - 28171
  - 3838
  - 0
  - 172.16.10.132
  - 80
  - 0
  - 172.16.10.76
  - 29171
  - 172.16.10.76
  - 80
  - 0
  - 172.16.10.98
  - 29171
  - 172.16.10.98
  - 80
  - 0
  - 172.16.10.215
  - 29172
  - 172.16.10.76
  - 80
  - 0
  - 172.16.10.200
  - 29171
  - 172.16.10.197
  - 0
  - 0
# CTAM - Introspector Configuration

## Cyber Threat Automation and Monitoring

### Choose Introspector to Configure

- **Host IP**: 172.16.10.110
- **Select**

### Introspector Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTROSPECTOR LOCAL ENDPOINT IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTROSPECTOR LOCAL PORT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOCAL SERVER ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIBVIRT ENDPOINT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIBVIRT PORT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENABLE DEBUG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENABLE ASYNCHRONOUS UPDATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMMUNICATION PORT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX TEMPLATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUTO TEMPLATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CTAM - Help

Cyber Threat Automation and Monitoring

VM Manager

VM Manager is used by the operator to manage the VM creation and functionality

VM Host Available

Connect to Host: VM Host 1

Connect to host to start...

• The top section of the VM Manager shows the available VM Host.

VM Host Available

Connect to Host: VM Host 1

Connect to host to start...

• By selecting the host and clicking "Connect to Host" the operator can get the list of VM running on the host and update the TCC application with available VMs.
CTAM Phase 3

1. CTAM Integrated Platform
   - Virtualization using Xen and QEMU/KVM hypervisors
   - Virtualization using only the Xen hypervisor
   - Virtualization using only the QEMU/KVM hypervisor

2. Deep Learning and Stream Analytics

3. CTAM as a Service

4. Advanced Analytics Platform

5. Package Deployment and Support
CTAM as a service Platform

Cyber Threat Automation and Monitoring System
Advanced Analytics Platform

Heterogeneous Data Source

- Structured Data
- Unstructured Data
- Stream Data

Data Integration Layer (Extract/Load/Transform and Validate)

- XML Loader
- JSON Loader
- File Loader
- RDBMS Loader
- CSV Loader
- ODBC Loader

Analytics Control Center

- Administration Console
- Test Case Management
- Dashboard
- Data Management
- Model Management
- Reports

Advanced Analytics Platform

Machine Learning / Distributed Computing

Cyber Threat Automation and Monitoring System

Advancing the research and academic mission of Florida International University.
Contacts

If you have a DoD testing need for any of the three Platforms and want to work with us as a transition partner, contact:

David D. Mareno III
Executing Agent
TRMC T&E/S&T Cyberspace Test Technology
David.Mareno@us.af.mil

Michael K. Shields, Ph.D.
Deputy Executing Agent
TRMC T&E/S&T Cyberspace Test Technology
Michael.Shields.13.ctr@us.af.mil
Q & A

Thank You