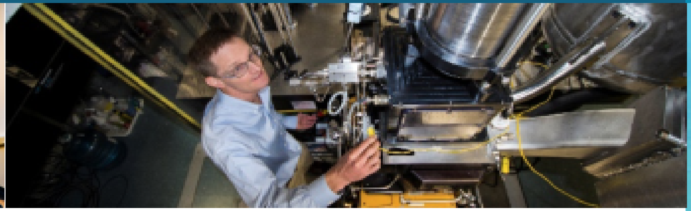
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2022-3533C

Sandia Emulytics Overview



PRESENTED BY

Arthur Hernandez - Sandia National Laboratory (SNL)

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

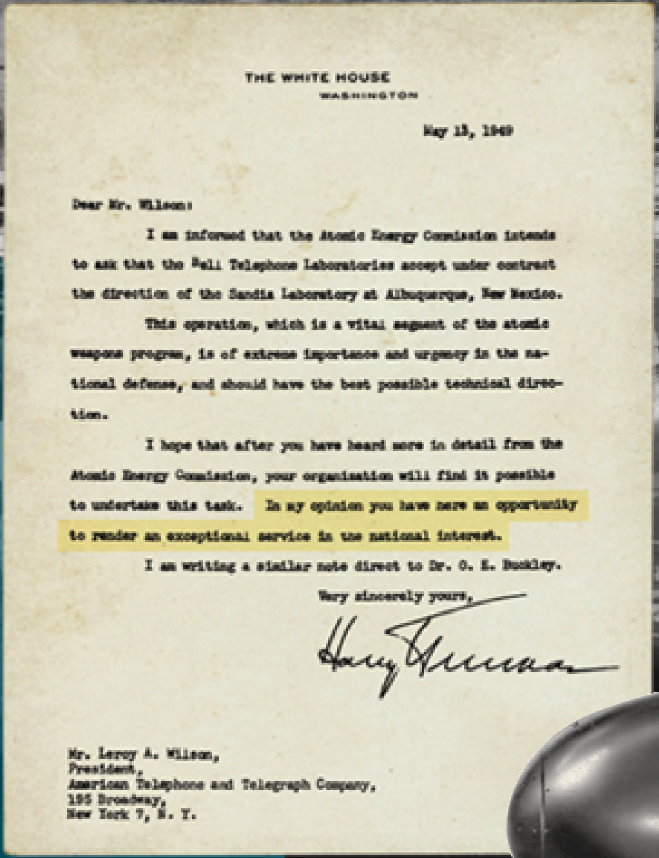
SANDIA'S HISTORY IS TRACED TO THE MANHATTAN PROJECT

> *…In my opinion you have here an opportunity to render an exceptional service in the national interest.*

National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc.

Government owned, contractor operated

FFRDCs are long-term strategic partners to the federal government, operating in the public interest with objectivity and independence and maintaining core competencies in missions of national significance



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

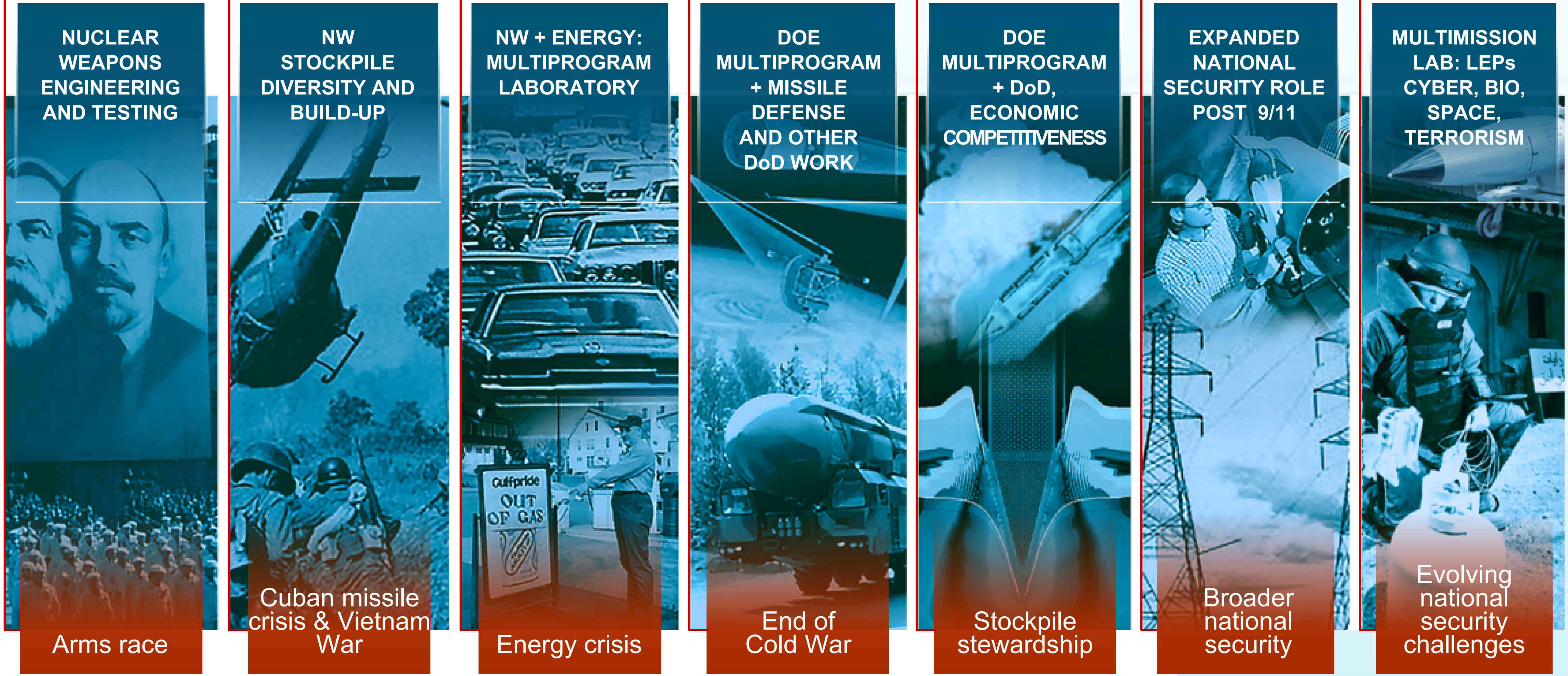
I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely yours,

Harry Truman

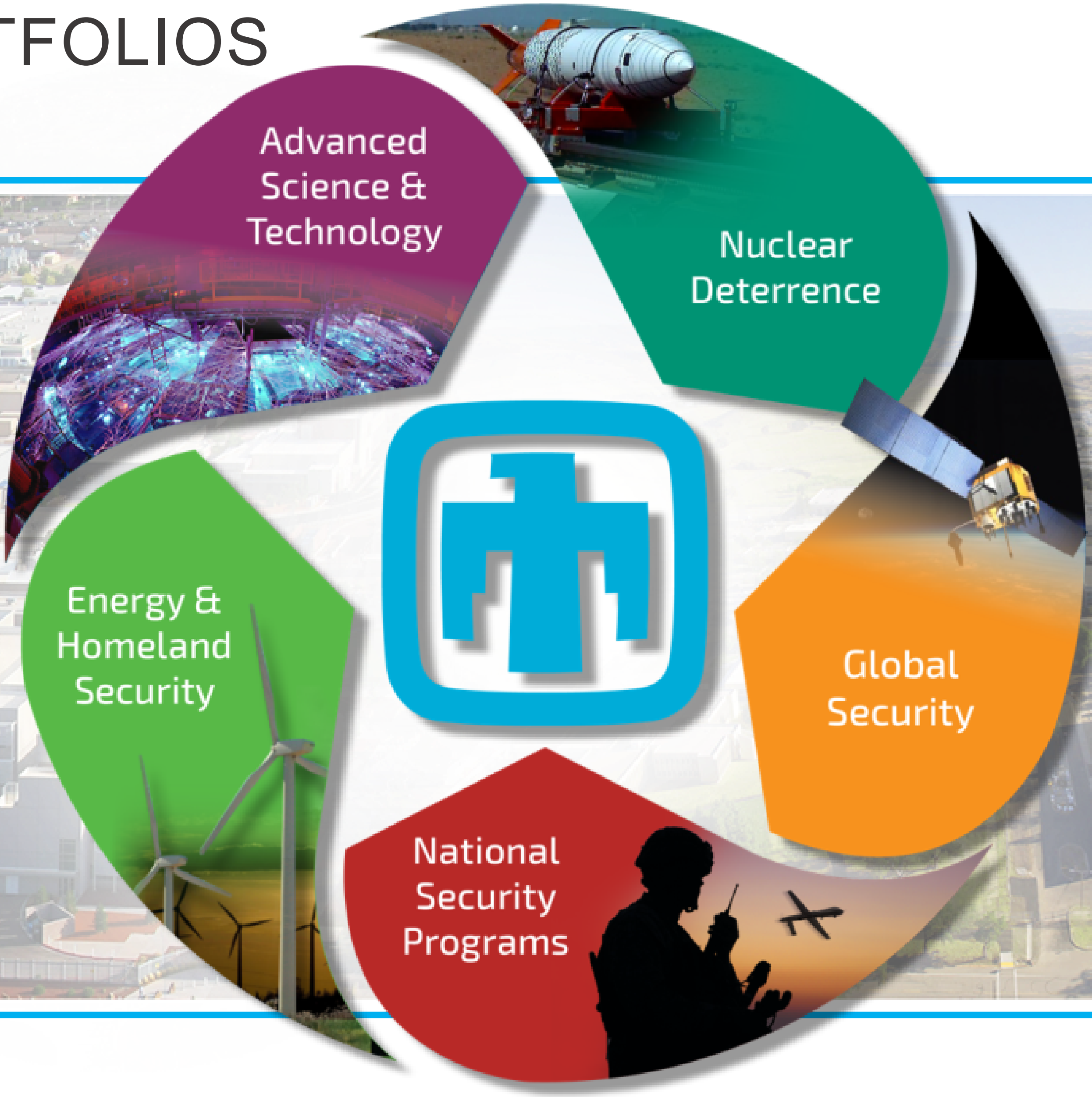
Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

SANDIA ADDRESSES NATIONAL SECURITY CHALLENGES



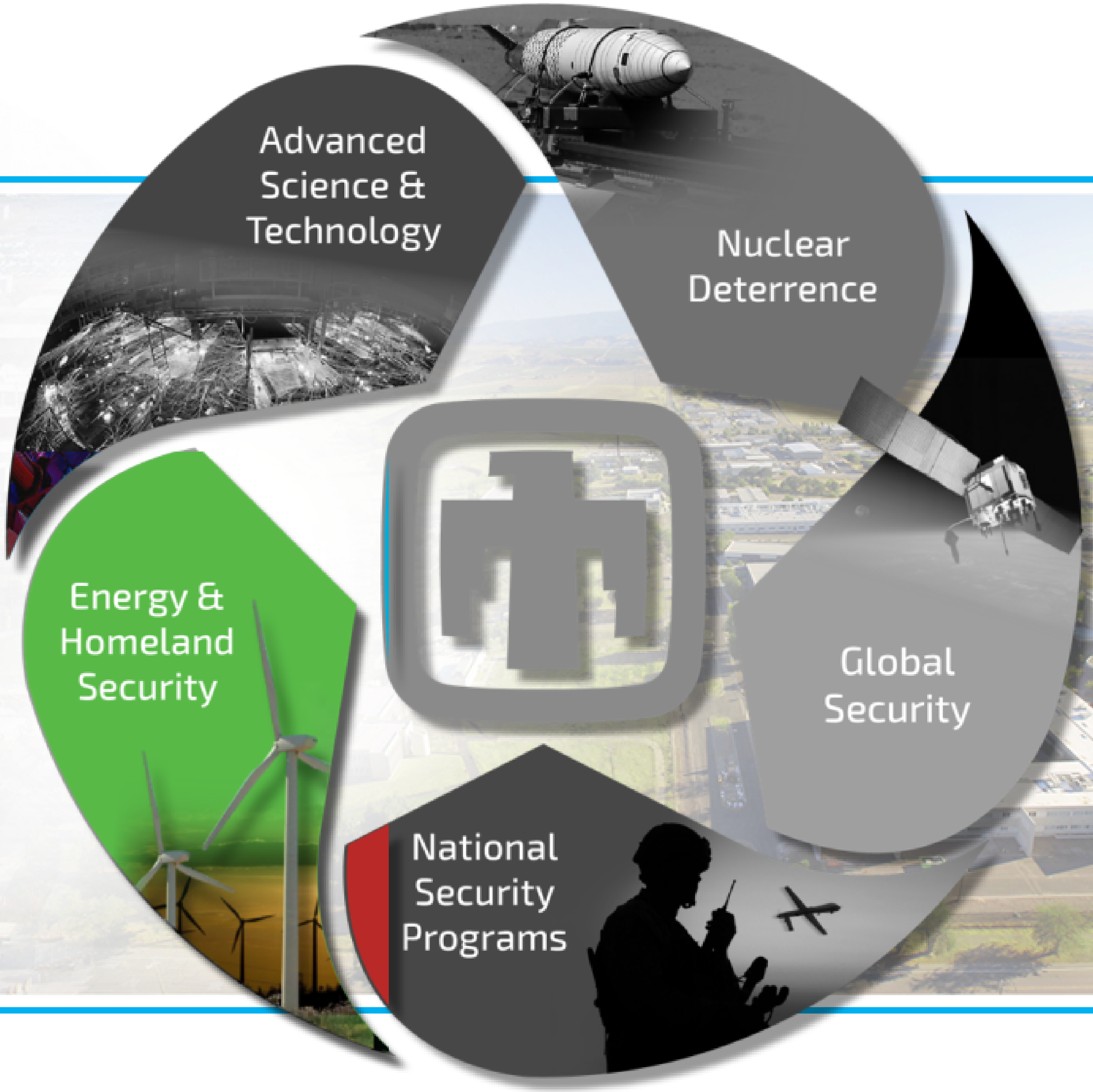
1950s	NUCLEAR WEAPONS ENGINEERING AND TESTING	Arms race
1960s	NW STOCKPILE DIVERSITY AND BUILD-UP	Cuban missile crisis & Vietnam War
1970s	NW + ENERGY: MULTIPROGRAM LABORATORY	Energy crisis
1980s	DOE MULTIPROGRAM + MISSILE DEFENSE AND OTHER DoD WORK	End of Cold War
1990s	DOE MULTIPROGRAM + DoD, ECONOMIC COMPETITIVENESS	Stockpile stewardship
2000s	EXPANDED NATIONAL SECURITY ROLE POST 9/11	Broader national security
2010s	MULTIMISSION LAB: LEPs CYBER, BIO, SPACE, TERRORISM	Evolving national security challenges

SANDIA HAS FIVE MAJOR PROGRAM PORTFOLIOS


Advanced Science & Technology
Nuclear Deterrence
Global Security
National Security Programs
Energy & Homeland Security

SANDIA HAS FIVE MAJOR PROGRAM PORTFOLIOS

- Perform fundamental and applied R&D to support the resilience and security of the nation's energy system
- Provide protection for our nation's digital and physical critical infrastructures
- Reduce U.S. vulnerability to chemical, biological, radiological, and nuclear threats
- Accelerate transformative innovations in the transportation sector through foundational physical and computational research

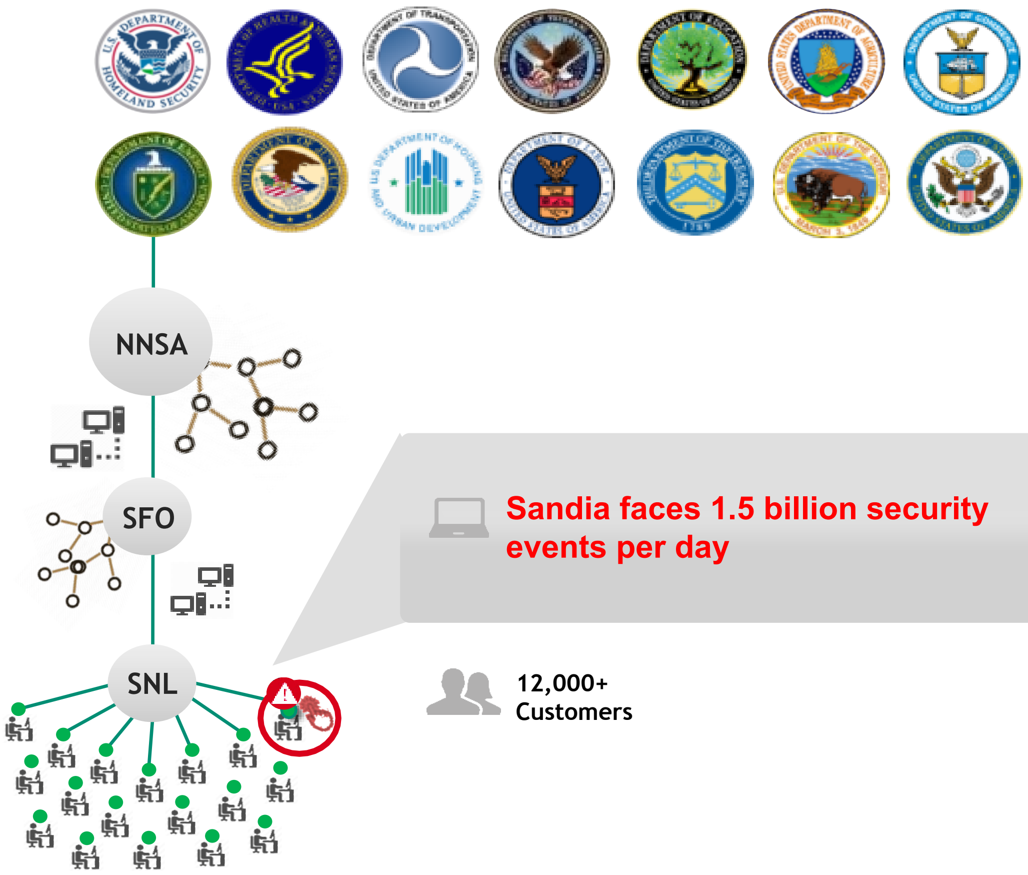

Advanced Science & Technology
Nuclear Deterrence
Global Security
National Security Programs
Energy & Homeland Security

SANDIA CIVILIAN CYBER

Unclassified Unlimited Release - SAND

THE CIVILIAN CYBER CHALLENGE: PROTECTING .GOV AND .COM

CIVILIAN GOVERNMENT PROTECTS 300 DEPARTMENTS & AGENCIES:



NNSA

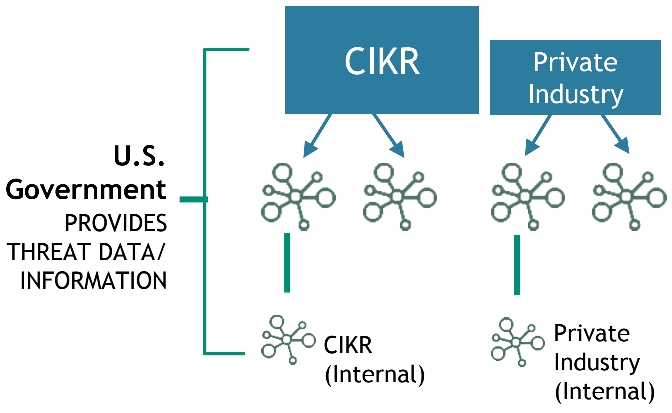
SFO

SNL

Sandia faces 1.5 billion security events per day

12,000+ Customers

CIKR/PRIVATE INDUSTRY.com (.net, .org.)



U.S. Government PROVIDES THREAT DATA/ INFORMATION

CIKR

Private Industry

CIKR (Internal)

Private Industry (Internal)

CIKR - Critical Infrastructure Key Resources

.gov is currently 2.4M people

CIVILIAN CYBER SUPPORT: CAPABILITIES OVERVIEW

Technical and engineering expertise to address unique challenges and support policy decisions in 3 key areas:

Cybersecurity Engineering

Technical expertise and development efforts seek to prevent disruption and enhance recovery capabilities by understanding changes to the technical landscape.

Cybersecurity Risk & Threat

Application of methodologies, tools, and capabilities reduces risks that affect increasingly complex and dynamic systems.

Cybersecurity Modernization

A robust understanding of the threat environment, and current engineering challenges, leads to the development of policy to drive modernization of cybersecurity services.

CIVILIAN CYBER SUPPORT: CYBERSECURITY ENGINEERING

Cybersecurity Engineering

Technical expertise and development efforts seek to prevent disruption and enhance recovery capabilities by understanding changes to the technical landscape.

OPPORTUNITIES FOR PARTNERSHIP

Malware Analysis

Enhance the capabilities of the intrusion detection services by improving the ability to discover and reverse engineer malware.

Advanced Analytics

Evolve capabilities through the addition of Threat Discovery, Behavioral Analytics, and Automated Defense.

CIVILIAN CYBER SUPPORT: CYBERSECURITY RISK & THREAT

Cybersecurity Risk & Threat

Application of methodologies, tools, and capabilities reduces risks that affect increasingly complex and dynamic systems.

OPPORTUNITIES FOR PARTNERSHIP

Risk Metrics

Develop algorithms to identify clusters of threat activity and threat actor capability tiers in order to communicate the value of intrusion prevention services.

Cyber Risk Methodologies

Develop a risk methodology focused on consequences to CI/KR and federal networks that can be leveraged for risk decision making.

CIVILIAN CYBER SUPPORT: CYBERSECURITY MODERNIZATION

Cybersecurity Modernization

A robust understanding of the threat environment, and current engineering challenges, leads to the development of policy to drive modernization of cybersecurity services.

OPPORTUNITIES FOR PARTNERSHIP

Threat & Architecture Analysis

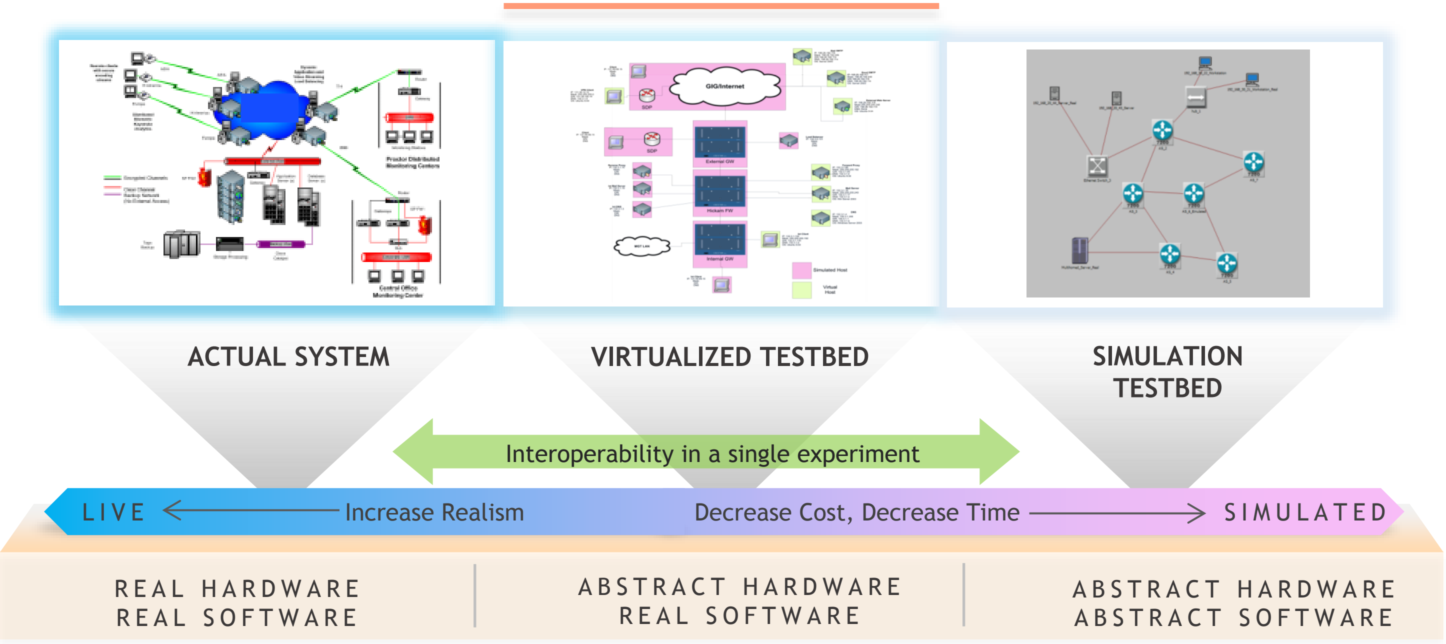
Enable smart investment decisions across the .gov environment through robust architecture and threat analysis.

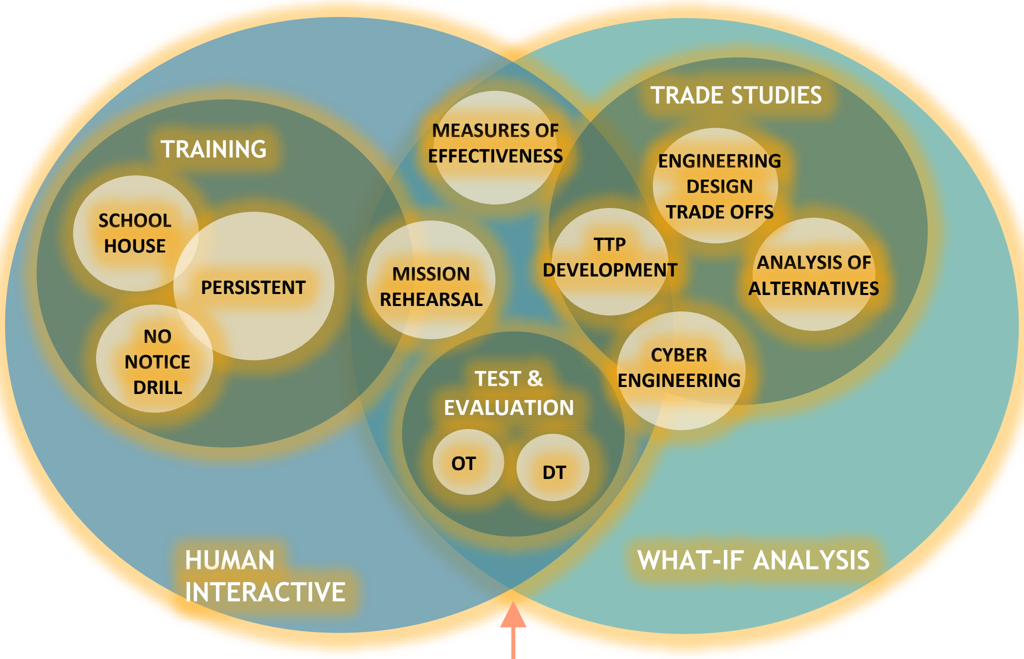
Analysis of Emerging Trends

Understand the breadth of the emerging challenges, and develop mitigation strategies to maintain and evolve cybersecurity capabilities.

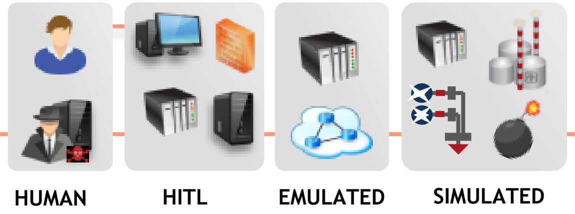
Emulytics Overview and Application

What is Emulytics?





Emulytics



Emulytics Overview

Minimega

Orchestration Platform:

- Launch and manage Virtual Machines & Containers
- Software Defined Networks (SDN)
- Hardware in-the-loop (HITL)
- Built in Command and Control

SCORCH

Experiment Control Platform

- Enables the definition of experiment parameters
- Automated changing of parameters and experiment execution
- Define, configure, run, fuzz, repeat

HADES

Deception and introspection:

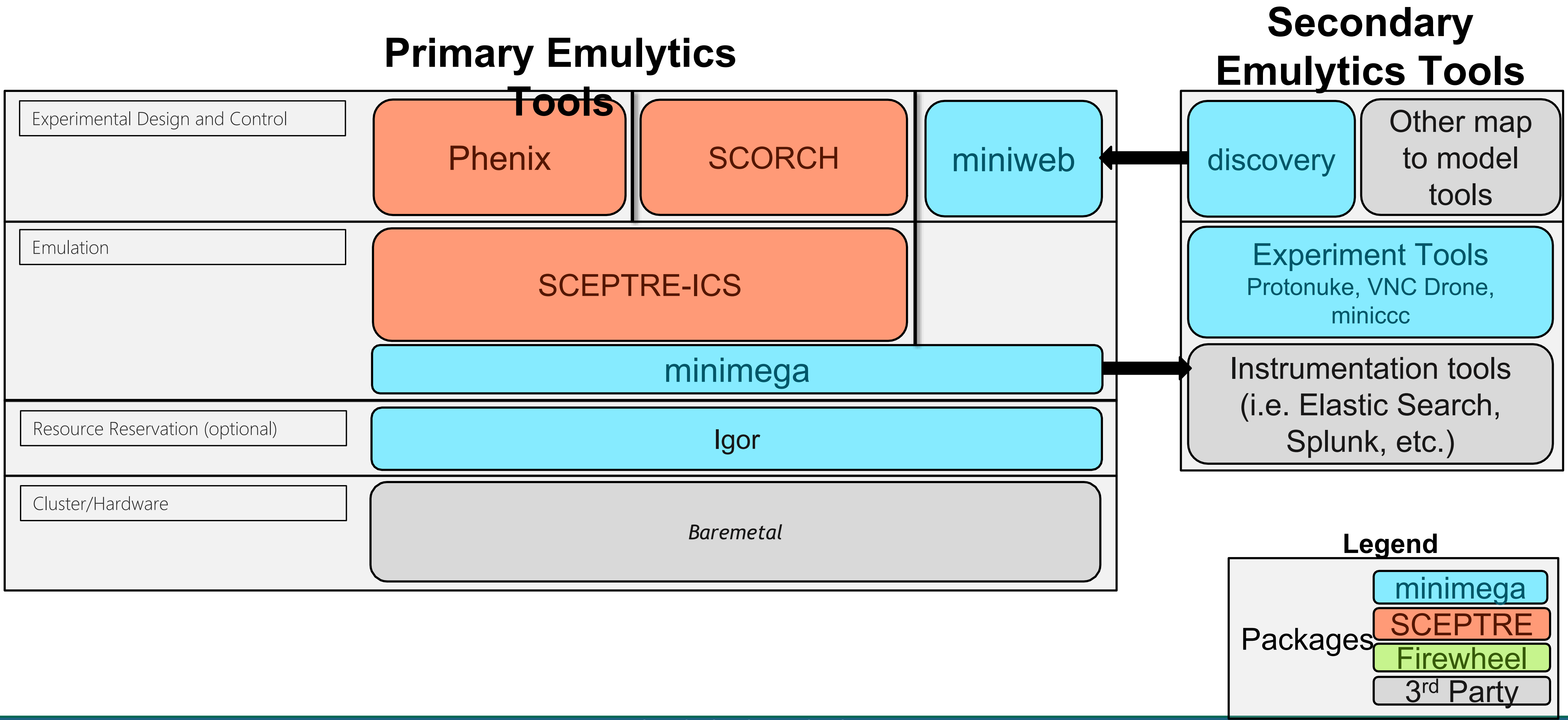
- Creates a deception environment
- Monitor and track active users from inside and outside the deception environment

Sceptre

Cyber-physical processes & Simulations

- Adds Supervisory control and data acquisition (SCADA) & Industrial Control Systems
- Faithful simulation of physical systems

Emulytics Stack



Map to Model – Discovery

Map-to-Model Need:

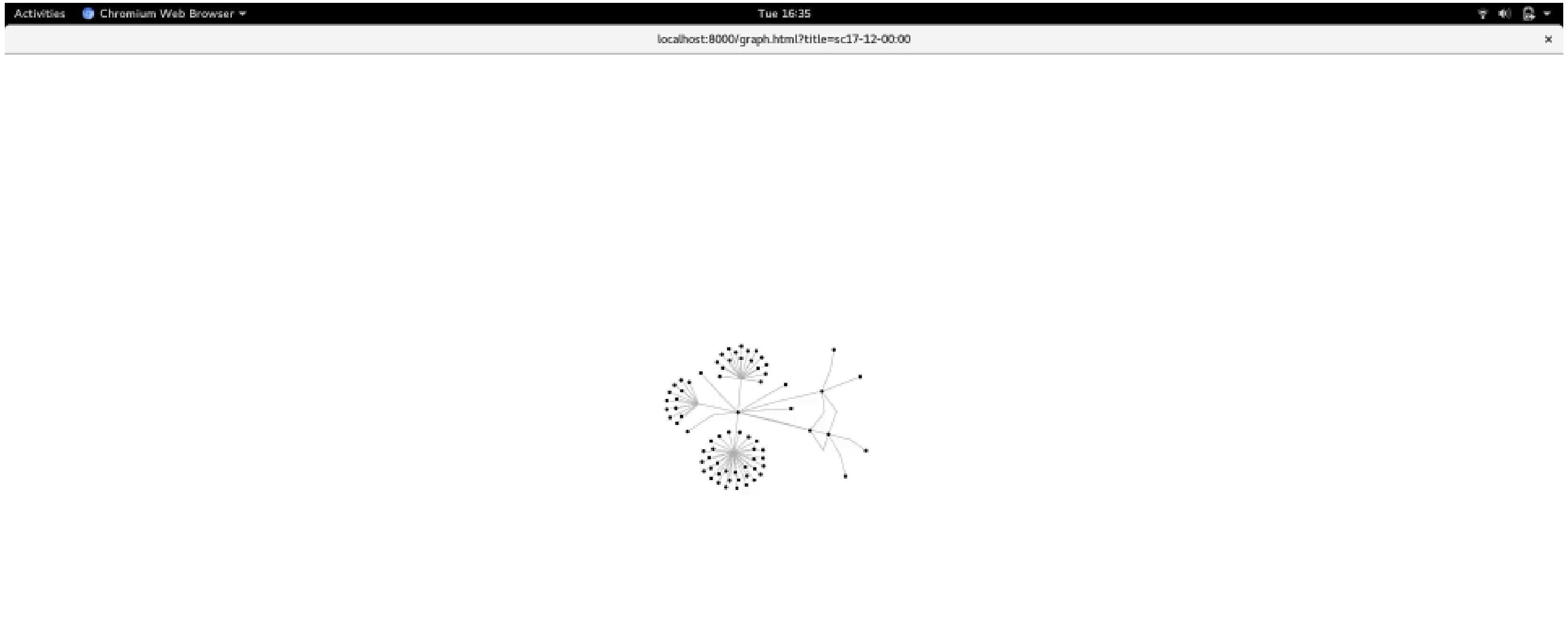
Map-to-model solutions are typically application/customer specific and human intensive.

Operators often do not know what is actually on their network.

Emulytics Solution:

Emulytics network discovery and mapping method was developed to support a rapid iterative map-to-model process.

Super Computing 2016 Model



Map to Model – Discovery

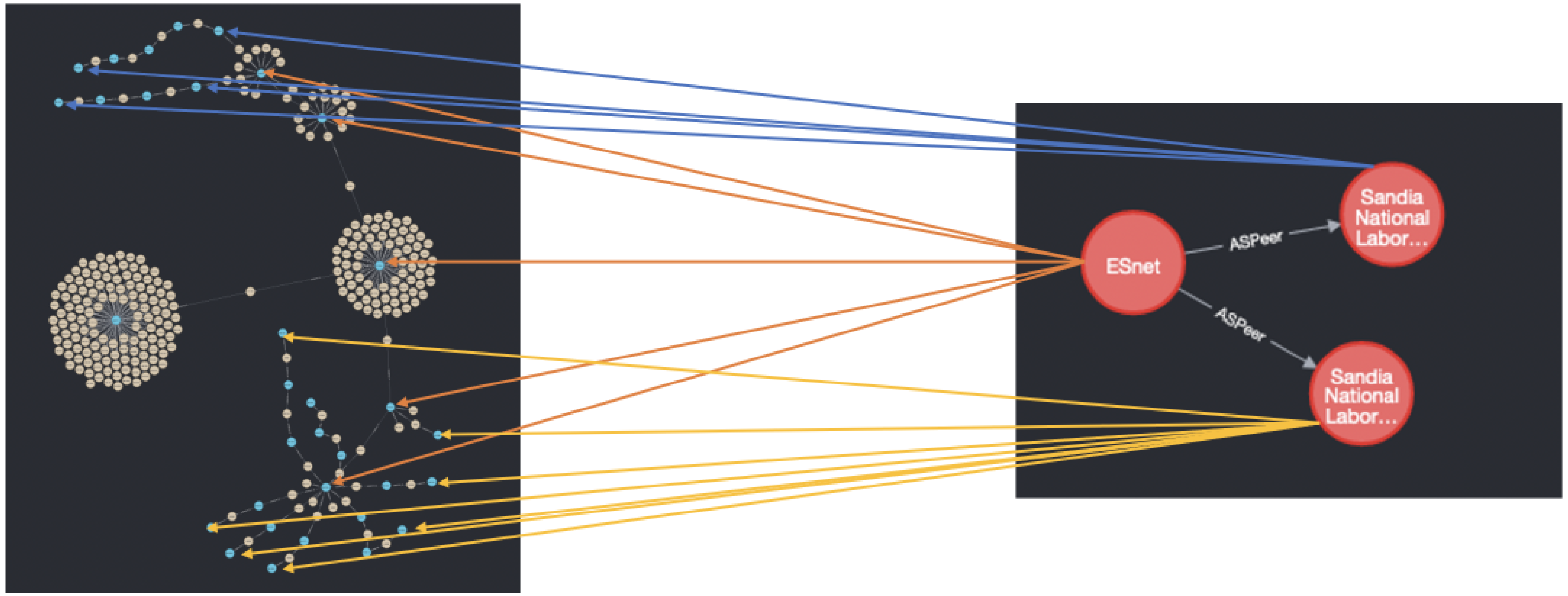
CAIDA and RouteViews:

Using CAIDA traceroute and route views Routing datasets to build areas of the internet that are of interest to study

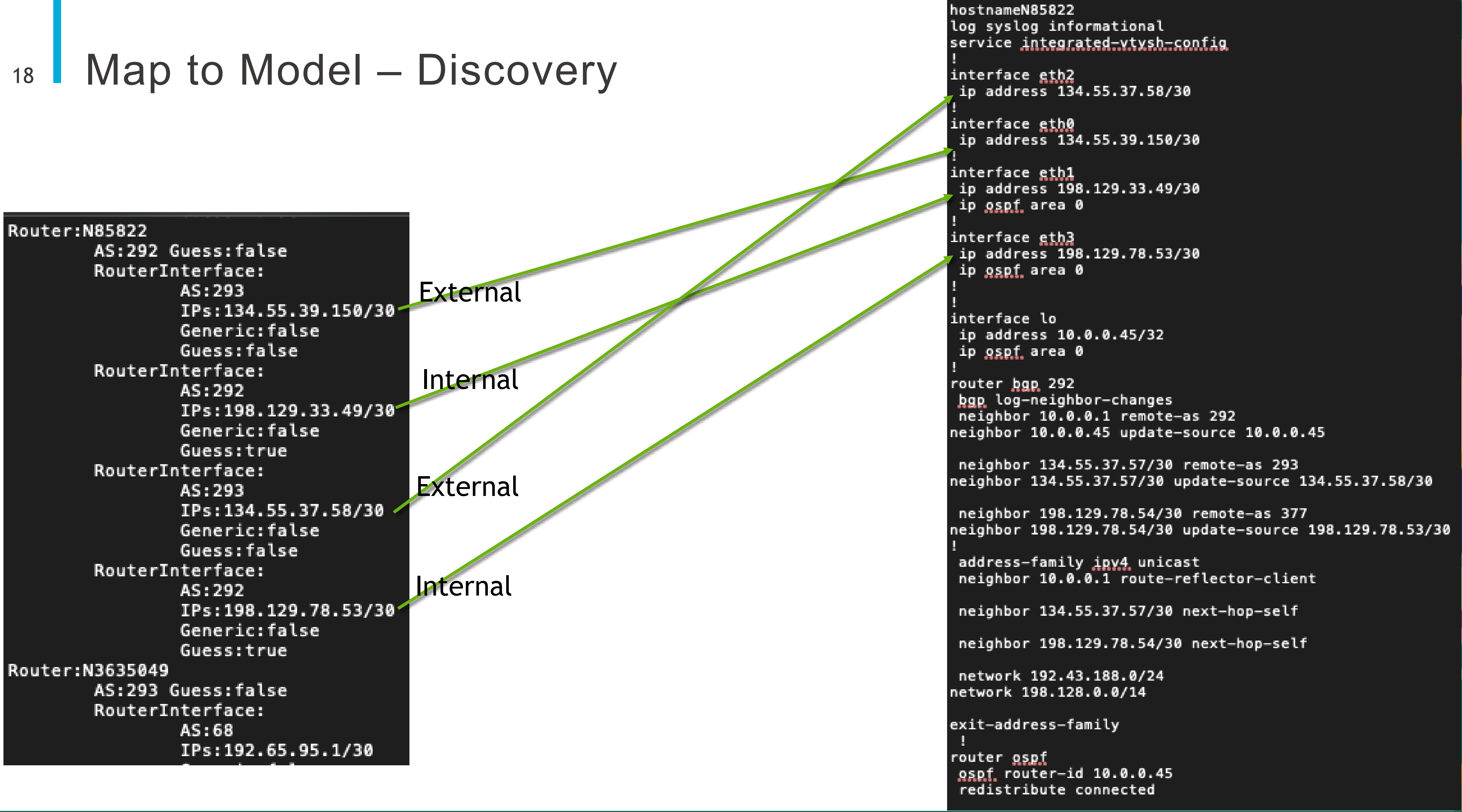
Inferencing:

Build out tools to assist in the inferencing process to get a realistic topological model

Center for Applied Internet Data Analysis (CAIDA)



Map to Model – Discovery



```
Router:N85822
        AS:292 Guess:false
        RouterInterface:
                AS:293
                IPs:134.55.39.150/30
                Generic:false
                Guess:false
        RouterInterface:
                AS:292
                IPs:198.129.33.49/30
                Generic:false
                Guess:true
        RouterInterface:
                AS:293
                IPs:134.55.37.58/30
                Generic:false
                Guess:false
        RouterInterface:
                AS:292
                IPs:198.129.78.53/30
                Generic:false
                Guess:true
Router:N3635049
        AS:293 Guess:false
        RouterInterface:
                AS:68
                IPs:192.65.95.1/30
```

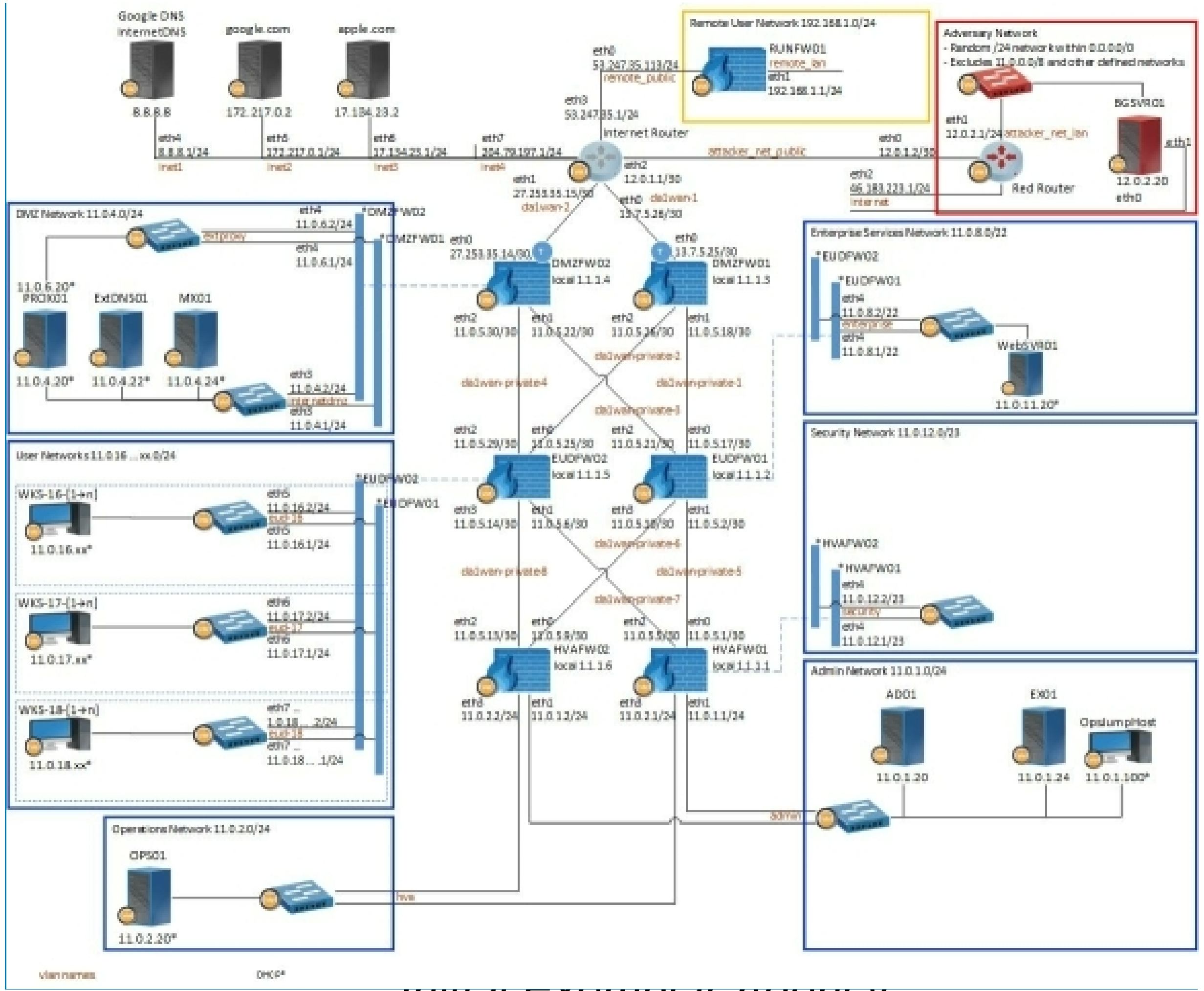
```
hostnameN85822
log syslog informational
service integrated-vtysh-config
!
interface eth2
 ip address 134.55.37.58/30
!
interface eth0
 ip address 134.55.39.150/30
!
interface eth1
 ip address 198.129.33.49/30
 ip ospf area 0
!
interface eth3
 ip address 198.129.78.53/30
 ip ospf area 0
!
!
interface lo
 ip address 10.0.0.45/32
 ip ospf area 0
!
router bgp 292
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 292
neighbor 10.0.0.45 update-source 10.0.0.45

 neighbor 134.55.37.57/30 remote-as 293
neighbor 134.55.37.57/30 update-source 134.55.37.58/30

 neighbor 198.129.78.54/30 remote-as 377
neighbor 198.129.78.54/30 update-source 198.129.78.53/30
!
 address-family ipv4 unicast
 neighbor 10.0.0.1 route-reflector-client

 neighbor 134.55.37.57/30 next-hop-self

 neighbor 198.129.78.54/30 next-hop-self

 network 192.43.188.0/24
network 198.128.0.0/14

exit-address-family
 !
router ospf
 ospf router-id 10.0.0.45
 redistribute connected
```

Emulytics Use Case (Minimega)- Cybersecurity and Operations Exercises

Project Scope

Exploration: Leverage threat modeling and emulation to explore how advanced persistent threats (APTs) can cause adverse effects on the way government functions at the network layer and above.

Experimentation: Deliver an experimentation capability that enables cyber security teams to leverage adversary models within representative emulated networks to answer questions about countermeasure prioritization, detection techniques, adversary attack, impact, etc.



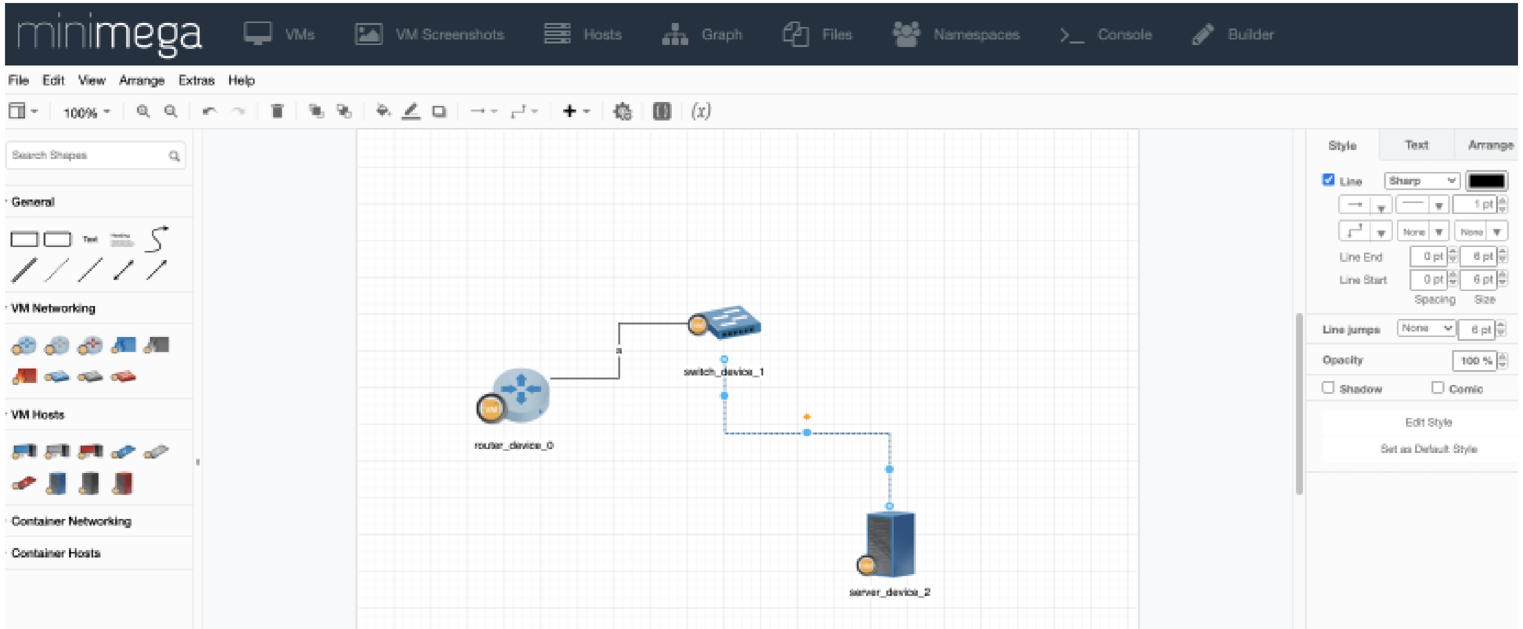
Initial Exemplar Agency Model

minimega UI and fast build

If you can draw it you can launch it

Familiar UI: Leverage the feel of other drawing utilities like visio and lucid charts with the ability to launch virtual machines

Speed of prototyping: increase the speed at which new and experienced users can design and launch experiments.



minibuilder

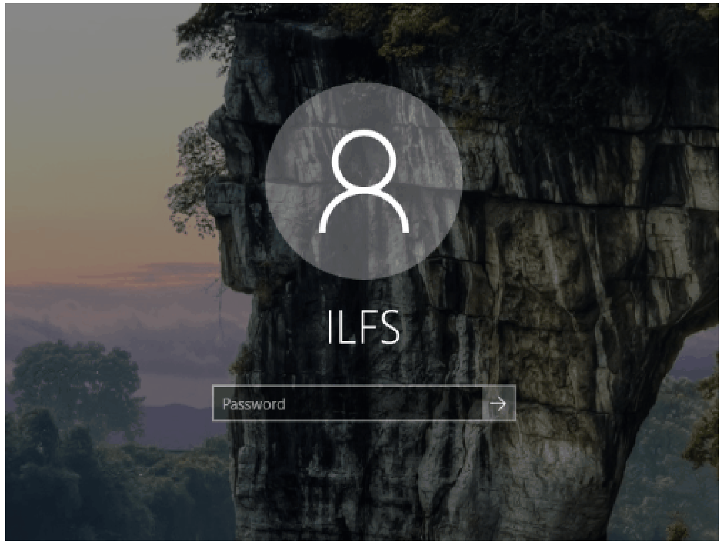
When Drones attack … a network

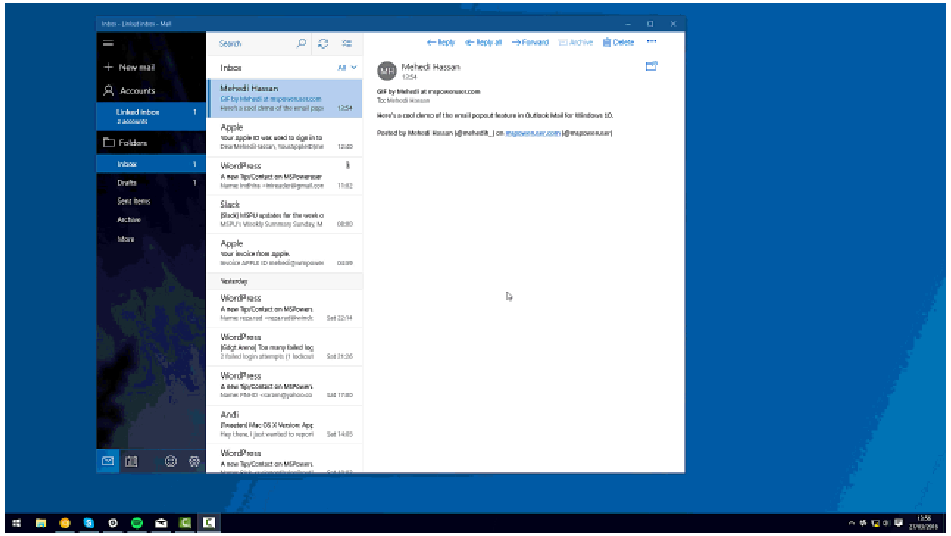
miniccc and VNC Drone

miniccc: is a command and control agent that can be installed on VMs so that you can send/receive files and execute commands from a central location

VNC Drone: simple VNC record and play back features allow users to record behaviors and programmatically play back

Protonuke: simple network generator which contains a client and a server. Can be deployed to serve and generate network traffic using a number of protocols





Mehedi Hassan
GIF by Mehedi at mspoweruser.com
Here's a cool demo of the email popup 12:54

Apple
Your apple ID was used to sign in to
Dear Mehedi Hassan, Your Apple ID 12:00

WordPress
A new Tip/Contact on MSPoweruser
Name: Indhira <indreader@gmail.com 11:02

Slack
[Slack] MSPU updates for the week o
MSPU's Weekly Summary Sunday, M 08:00

Apple
Your invoice from apple.
Invoice APPLE ID mehedi@mspower 03:09

WordPress
A new Tip/Contact on MSPowers
Name: reza.rad <reza.rad@hotm Sat 22:14

WordPress
[Gadget Arena] Too many failed log
2 failed login attempts (1 lockout Sat 21:26

WordPress
A new Tip/Contact on MSPowers
Name: PNHD <carlam@yahoo.co Sat 17:00

Andi
[Freedom] Mac OS X Version: App
Hey there, I just wanted to report Sat 14:05

WordPress
A new Tip/Contact on MSPowers

MH Mehedi Hassan
12:54

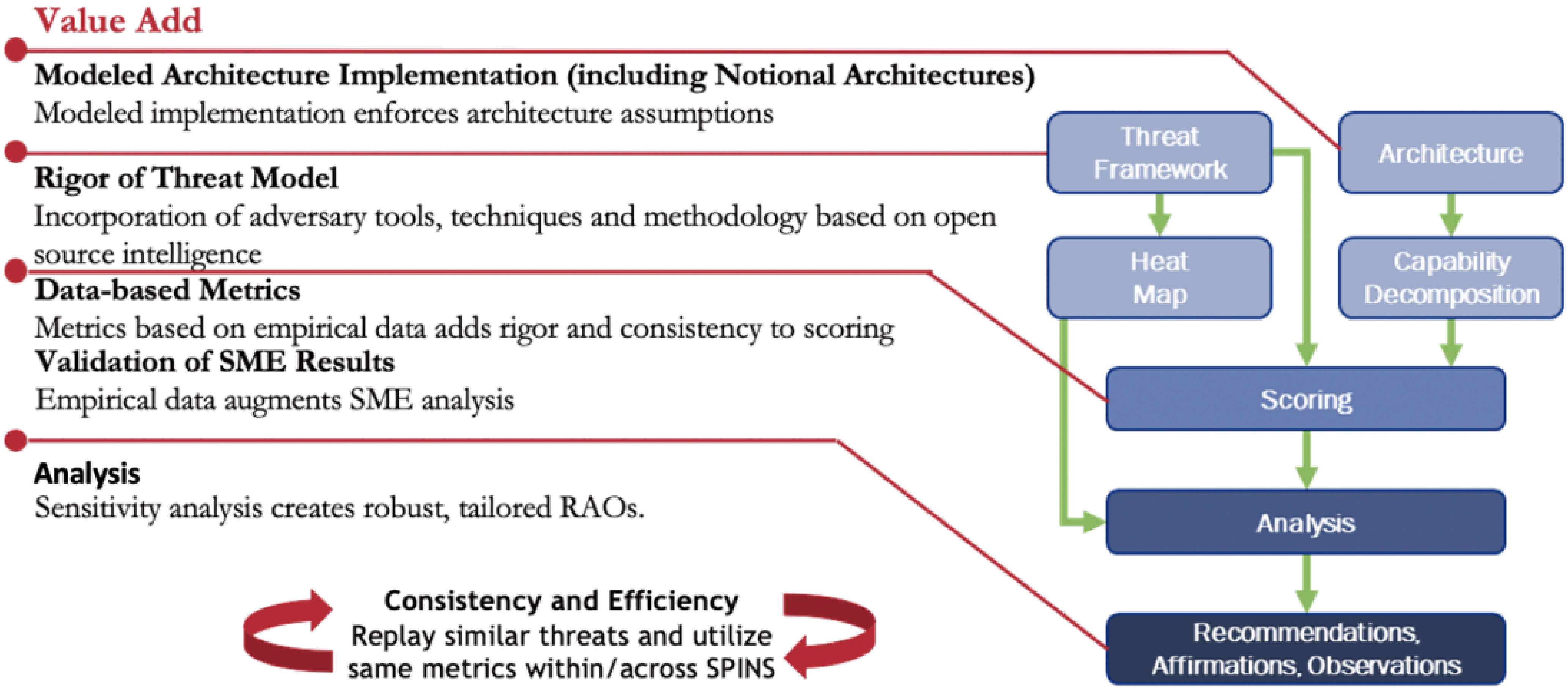
GIF by Mehedi at mspoweruser.com
To: Mehedi Hassan

Here's a cool demo of the email popout feature in Outlook Mail for Windows 10.

Posted by Mehedi Hassan (@mehedih_) on mspoweruser.com (@mspoweruser)

Emulytics Use Case (Minimega) – Architecture and Organizational Investment

- **Inform and Prioritize .gov Cybersecurity Investments:** A cyber threat-driven .gov cybersecurity investment prioritization tool, providing acquisition recommendations to Federal Civilian Departments and Agencies to improve their cybersecurity posture.



Value Add

Modeled Architecture Implementation (including Notional Architectures)
Modeled implementation enforces architecture assumptions

Rigor of Threat Model
Incorporation of adversary tools, techniques and methodology based on open source intelligence

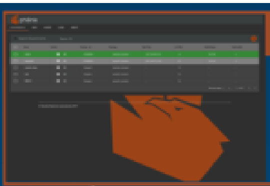
Data-based Metrics
Metrics based on empirical data adds rigor and consistency to scoring

Validation of SME Results
Empirical data augments SME analysis

Analysis
Sensitivity analysis creates robust, tailored RAOs.

Consistency and Efficiency
Replay similar threats and utilize same metrics within/across SPINS

SCEPTRE



phēnix

Sandia's phēnix orchestration tool allows users to quickly deploy, undeploy, and interact with SCEPTRE ICS environments

SCADA Applications

- Industry standard software for SCADA applications, including:
  - Human Machine Interfaces (HMI)
  - OPC and SCADA servers
  - Database historians

Software Defined Networking

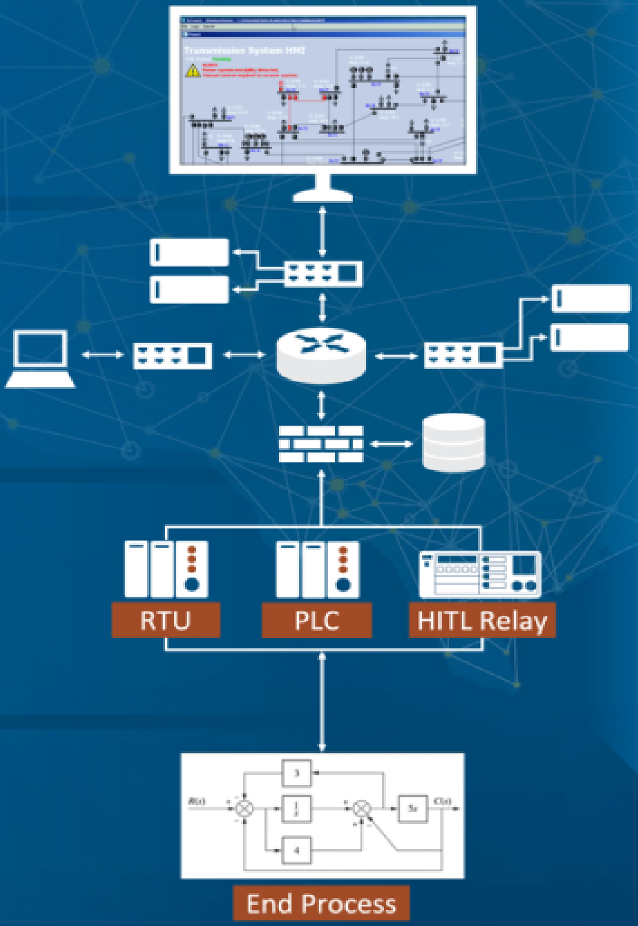
- ICS devices (simulated, emulated, real) communicate and interact via high fidelity SCADA protocols
  - ModbusTCP, DNP3, IEC 61850 and 60870
  - Written to specification
  - Enabling technology that allows communication between Hardware-in-the-Loop (HITL) and simulated devices

SCEPTRE ICS Field Devices

- Simulated ICS devices
  - RTUs, PLCs, protection relays, FEPs
  - Communicate using high fidelity, to spec SCADA protocols
- Emulated PLCs
- HITL devices such as relays, PLCs, RTUs

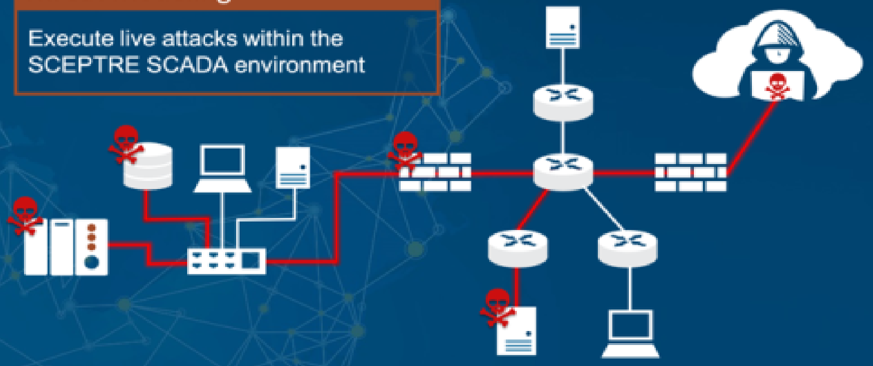
End Process Simulation

- SCEPTRE integrates field devices and end process simulations to provide realistic responses in the physical process as events occur in the control system and vice versa
- Leverage industry standard software to provide realistic end process models



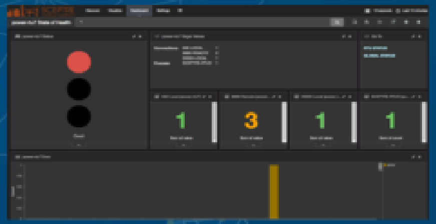
Threat Modeling

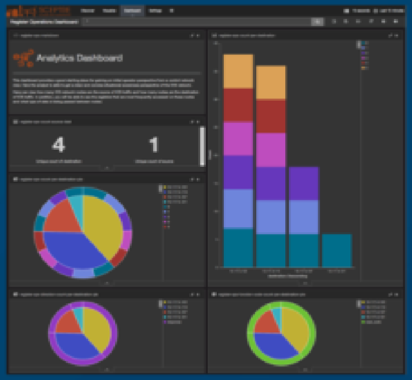
Execute live attacks within the SCEPTRE SCADA environment



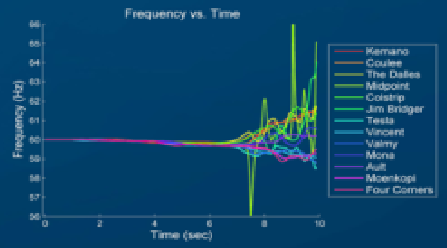
Real Time SCADA Analysis

Continuously collect data for test and evaluation, design, and analytics

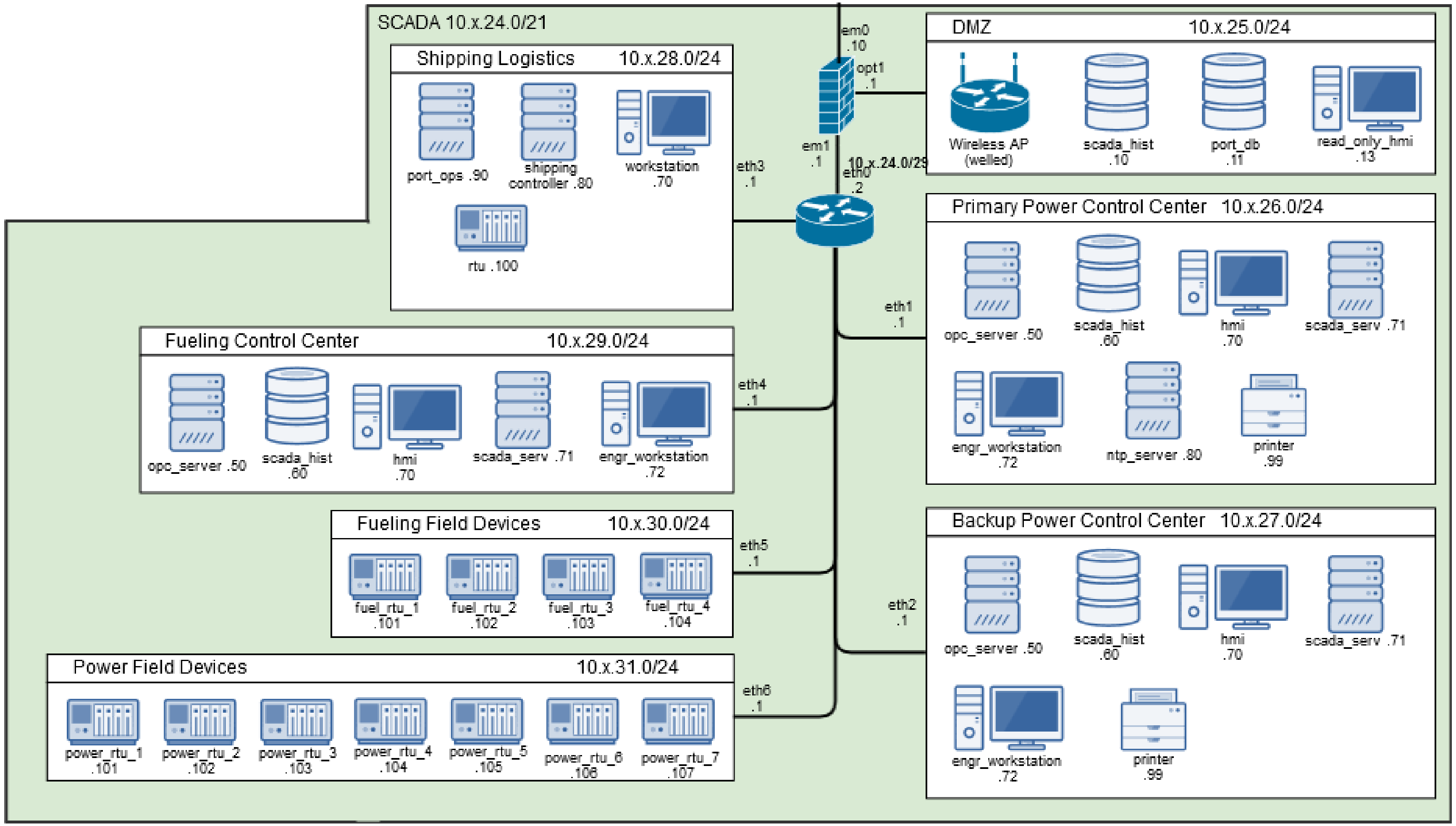




Consequence Modeling



Port Control System Network



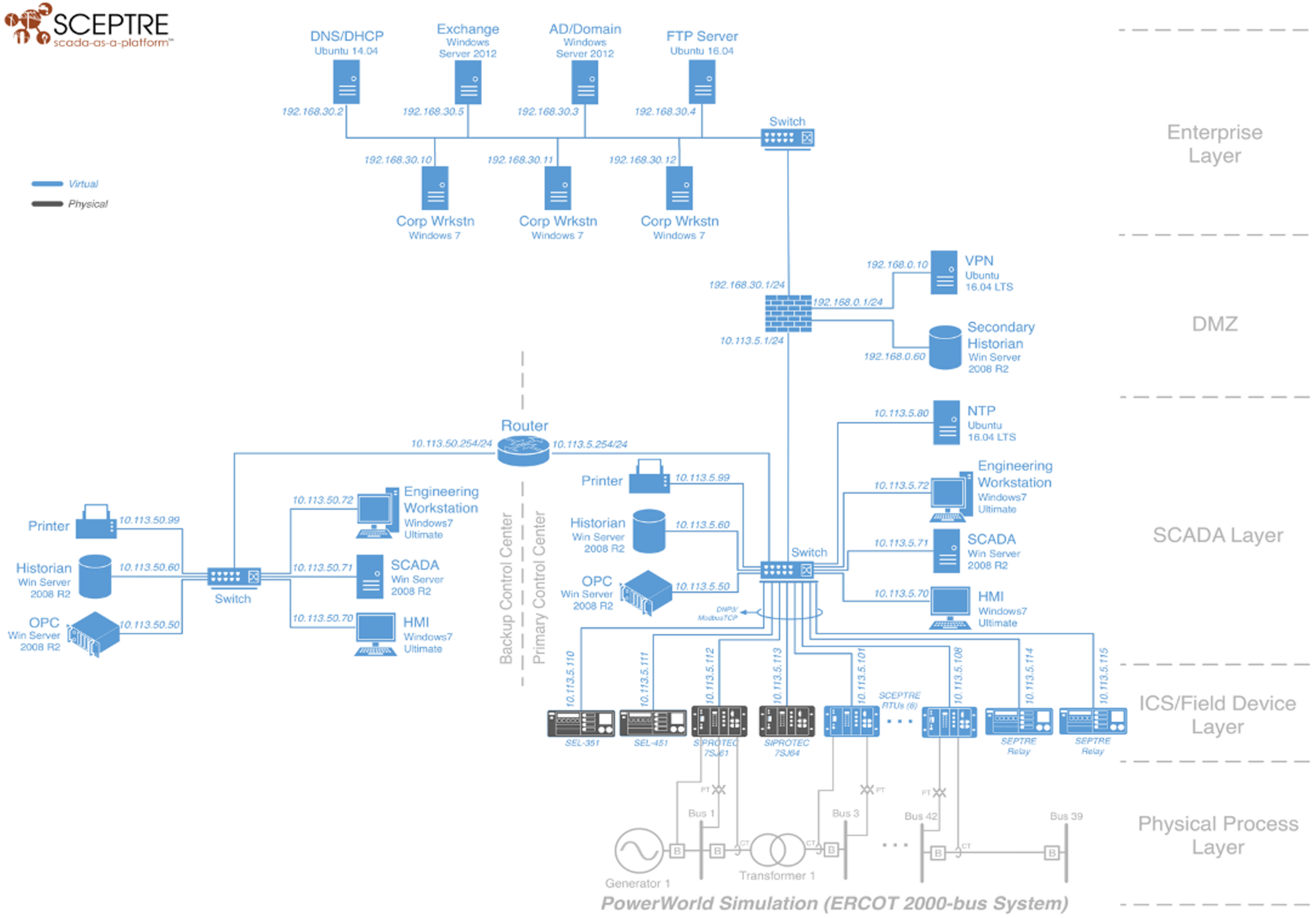
- All of the components run on Windows VMs using the following configuration:
  - Windows Server 2008 R2 Standard x64 Service Pack 1

Emulytics Demonstration

Emulytics Demonstration

Scenario

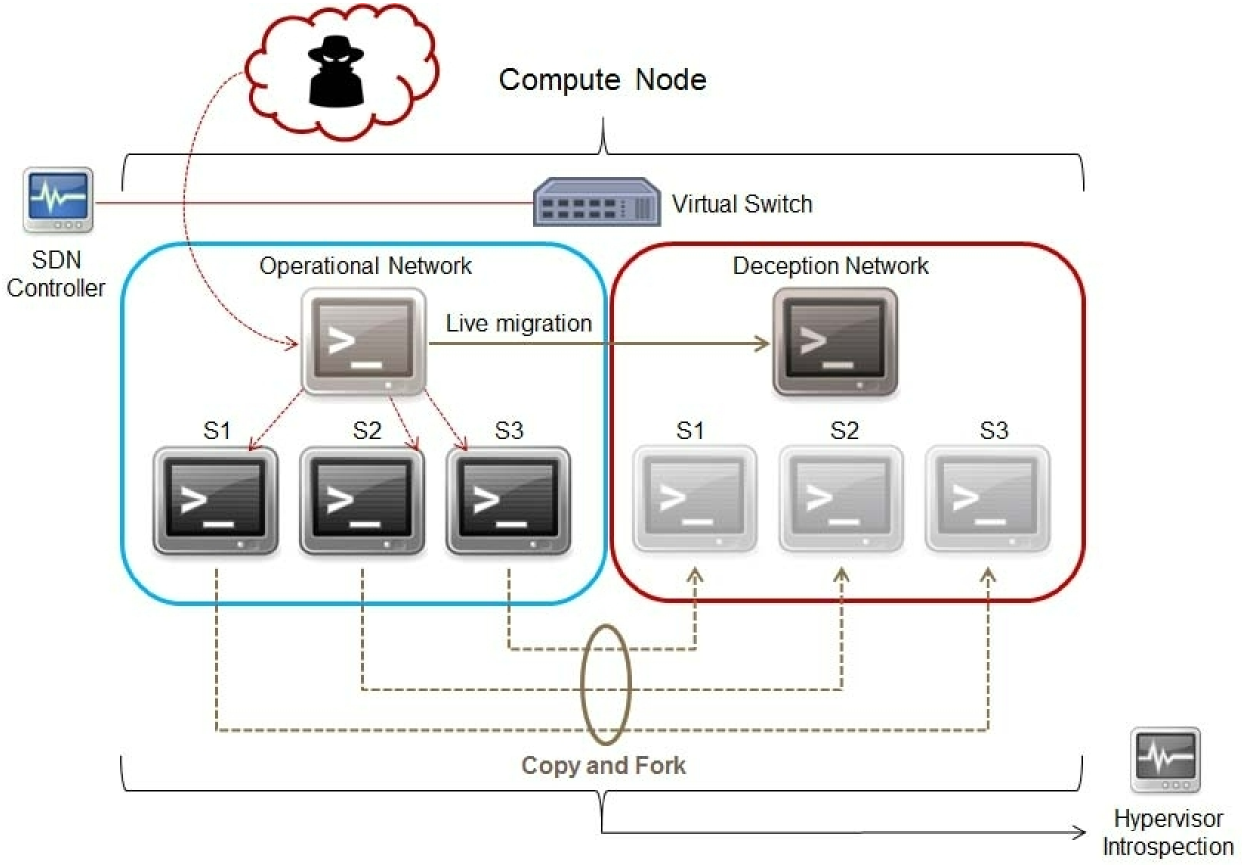
- A fictious power company’s IT and OT infrastructure located in Texas is modeled
- The infrastructure is faithfully modeled from layer 2 and up with all the necessary services and physical simulation
- An enterprise user is social engineered (e.g., phishing email) to go to some website on the internet



High-Fidelity Adaptive Deception and Emulation System (HADES)

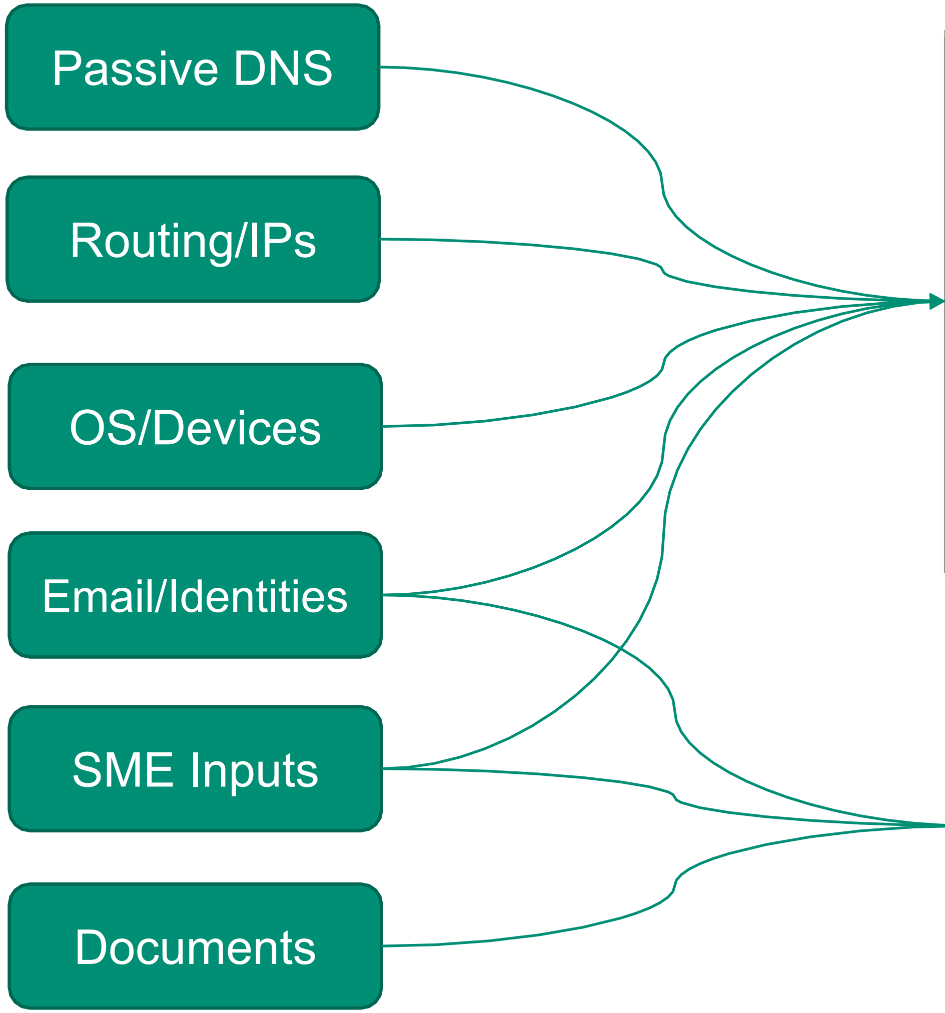
Technical Challenge

- Create a realistic deception environment
- Feels like Real:
  - Network, Applications, Virtual Machines, Users, & Data
- Seamlessly move the adversary to the deception environment
- Monitor and track the attacker with minimal impact on the system to prevent detection by the adversary

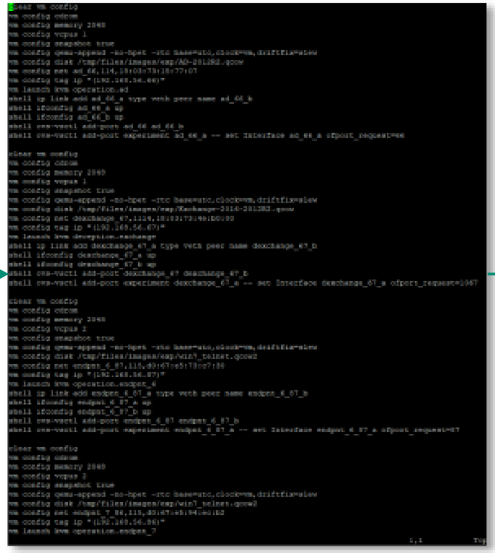


High-Fidelity Adaptive Deception and Emulation System (HADES)

DATA INPUTS



SYSTEM SPECIFICATION



```
clear vm config
vm config cdrom
vm config memory 2048
vm config vcpus 1
vm config snapshot true
vm config qemu-append -no-hpet -rtc base=utc,clock=vm,driftfix=slew
vm config disk /tmp/files/images/exp/AD-2012R2.qcow
vm config net ad_66,114,18:03:73:18:77:07
vm config tag ip "(192.168.56.66)"
vm launch kvm operation.ad
shell ip link add ad_66_a type veth peer name ad_66_b
shell ifconfig ad_66_a up
shell ifconfig ad_66_b up
shell ovs-vsctl add-port ad_66 ad_66_b
shell ovs-vsctl add-port experiment ad_66_a -- set Interface ad_66_a ofport_request=66

clear vm config
vm config cdrom
vm config memory 2048
vm config vcpus 1
vm config snapshot true
vm config qemu-append -no-hpet -rtc base=utc,clock=vm,driftfix=slew
vm config disk /tmp/files/images/exp/Exchange-2016-2012R2.qcow
vm config net dexchange_67,1124,18:03:73:46:b0:03
vm config tag ip "(192.168.56.67)"
vm launch kvm deception.exchange
shell ip link add dexchange_67_a type veth peer name dexchange_67_b
shell ifconfig dexchange_67_a up
shell ifconfig dexchange_67_b up
shell ovs-vsctl add-port dexchange_67 dexchange_67_b
shell ovs-vsctl add-port experiment dexchange_67_a -- set Interface dexchange_67_a ofport_request=1067

clear vm config
vm config cdrom
vm config memory 2048
vm config vcpus 1
vm config snapshot true
vm config qemu-append -no-hpet -rtc base=utc,clock=vm,driftfix=slew
vm config disk /tmp/files/images/exp/win7_telnet.qcow2
vm config net endpnt_6_87,115,40:67:e5:73:c7:86
vm config tag ip "(192.168.56.87)"
vm launch kvm operation.endpnt_6
shell ip link add endpnt_6_87_a type veth peer name endpnt_6_87_b
shell ifconfig endpnt_6_87_a up
shell ifconfig endpnt_6_87_b up
shell ovs-vsctl add-port endpnt_6_87 endpnt_6_87_b
shell ovs-vsctl add-port experiment endpnt_6_87_a -- set Interface endpnt_6_87_a ofport_request=87

clear vm config
vm config cdrom
vm config memory 2048
vm config vcpus 1
vm config snapshot true
vm config qemu-append -no-hpet -rtc base=utc,clock=vm,driftfix=slew
vm config disk /tmp/files/images/exp/win7_telnet.qcow2
vm config net endpnt_7_88,115,40:67:e5:84:ec:b2
vm config tag ip "(192.168.56.88)"
vm launch kvm operation.endpnt_7
                                                            1,1          Top
```

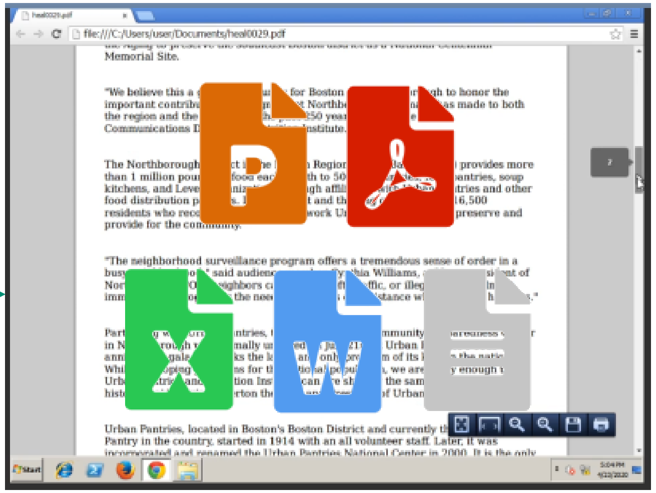
DEPLOYMENT PLATFORM

HADES openstack. vmware ESXi

minimega

OpenAI

NATURAL LANGUAGE GENERATION



heal0029.pdf

file:///C:/Users/user/Documents/heal0029.pdf

Memorial Site.

"We believe this a … for Boston … gh to honor the important contribu… Northb… as made to both the region and the … 250 year… Communications D… nstitute.

The Northborough … Region … provides more than 1 million pou… food eac… th to 50 … pantries, soup kitchens, and Leve… gh affili… tries and other food distribution p… t and th… 16,500 residents who rec… work U… preserve and provide for the community.

"The neighborhood surveillance program offers a tremendous sense of order in a busy … said audien… Williams, … sident of Nor… ighbors c… ffic, or ille… imm… the nee… stance w… ."

Part… ntries, … mmunity … in N… mally … Urban … ann… ks the … m of its … Whi… we are … Urb… tion Ins… can … the sam… hist… rton the … f Urban

Urban Pantries, located in Boston's Boston District and currently th… Pantry in the country, started in 1914 with an all volunteer staff. Later, it was incorporated and renamed the Urban Pantries National Center in 2000. It is the only

5:04 PM

FALSIFIED DOCUMENTS

Questions?