Cyber Threat Landscape

SCIT Concept

SCIT Technical

Case Studies

SCIT Status

Questions?

New Approach

Cyber Risk = Threats X Vulnerabilities x Consequences

Cyber Kill Chain: Get In – Stay In – Act

Cyber Threat Landscape
SCIT Concept
SCIT Technical
Case Studies
SCIT Status
Questions?

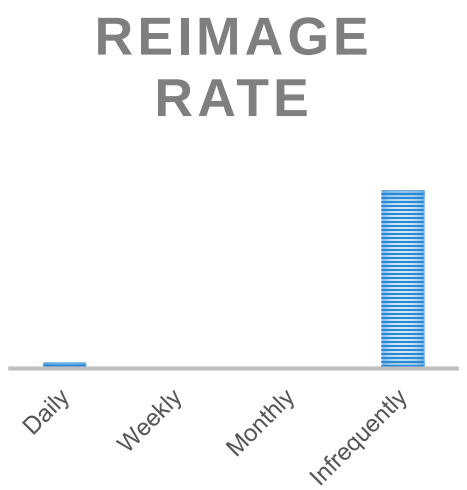
Preliminary Survey

- How often are your servers reimaged?

  {Daily, Weekly, Monthly, Infrequently}

  What if attacker is in?

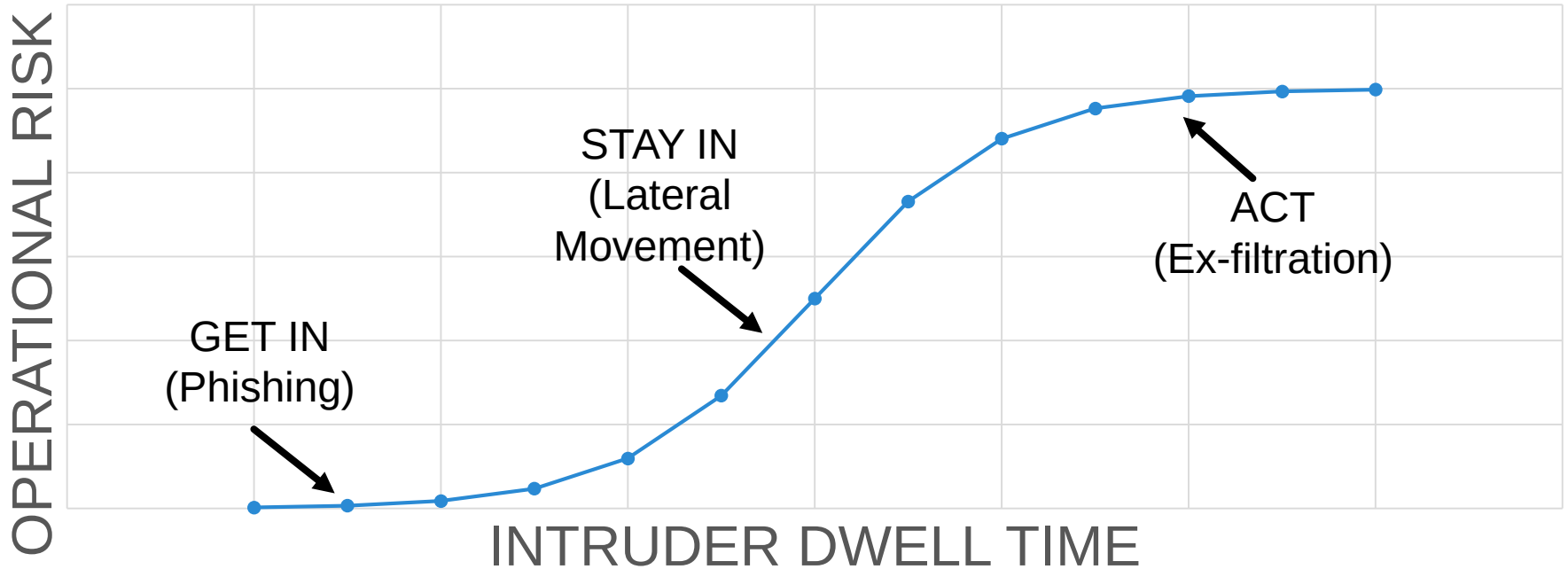
Preliminary Survey



- How often are your servers reimaged?
  - {Daily, Weekly, Monthly, Infrequently}
  - What if attacker is in?
- How long before patches are applied?
  - {Day, Week, Month, 3 Months, 6 Months}
  - How are the servers protected in this period?
- How do you protect your Data Centers and Clouds:
  Infrequently used servers, Un-patchable legacy systems, DevOps?
- Future apps: Internet of Things – transport, ground stations, etc.

Cyber Threat Landscape
SCIT Concept
SCIT Technical
Case Studies
SCIT Status
Questions?

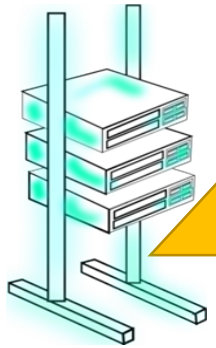
Operational Risk vs Intruder Dwell Time



- Intrusions can go undetected for 8 months
- Time for successful attack = 4 to 6 days
- Time to resolve an attack = 46 days
- Overreliance on detection of cyber intruders is unwise

Cyber Threat Landscape
SCIT Concept
SCIT Technical
Case Studies
SCIT Status
Questions?

SCIT – Resilience, Restoration, Recovery, Forensics



SCIT Controller governs virtual Server rotation. Cyber Attack Interrupted.

SCIT

Server

V. SVR1 "cold"

V. SVR "X" "malware"

V. SVR2 "hot"

V. SVR3 "cold"

V. SVR "X"

QUARANTINE

Mission Environment

Compromise detected

1. Virtual Server quarantined
2. Alert sent to cyber defender
3. Analysis on virtual server

KEY

Cyber Attack

User defined rotations.

A New Way of Doing Business

Cyber Threat Landscape

SCIT Concept

SCIT Technical

Case Studies

SCIT Status

Questions?

Efficiency of SCIT Design Affordable and Cost Effective

- Current situation: dwell time is months
- SCIT dwell time determined by system security requirement
- Number of active servers is dependent on the application
  - Number of spare servers is dependent on application and available hardware
  - Higher dwell time requires fewer “cold” servers (less redundancy)
- 90 second dwell time: VMs - 1 active, 2 cold
- 60 minute dwell time: VMs -15 active,1 cold
- 2 hour dwell time: VMs - 30 active; 1 cold

SCIT Overview

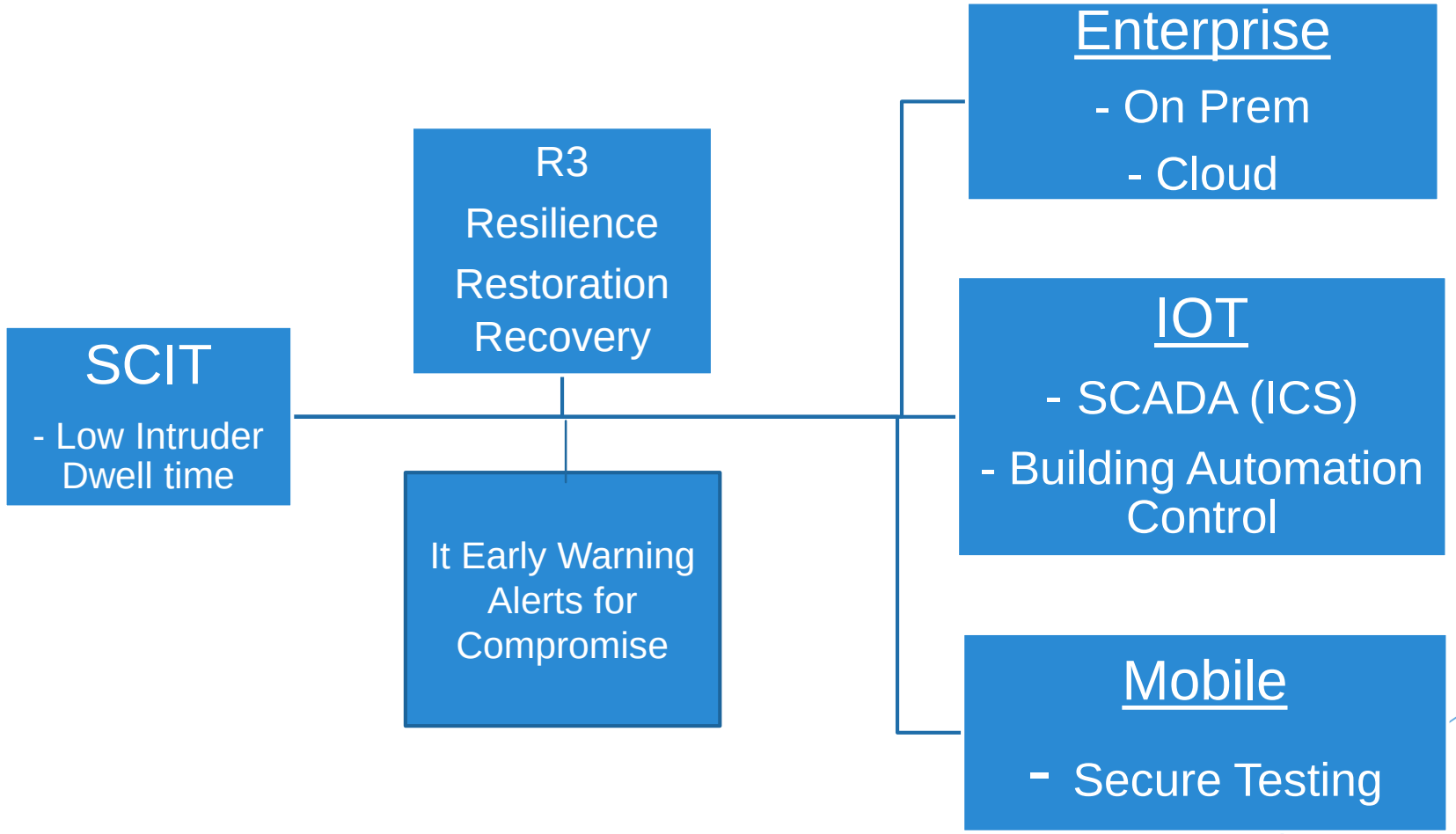
- Cyber Kill Chain
  - Get In. Stay In. Act.
- Most Cyber Defenses Focus on Preventing Get In
  - Works some of the time
  - Prevents known attacks
  - Requires constant updating to counter new threats
  - Many examples of intruders staying in the system for weeks
- SCIT Reduces Time for Stay In and Act
  - Complements (or augments) existing cyber defenses. Does not replace them.
  - Terminates APT attacks in minutes
  - Resilience, Restoration, Recovery
- IT Early Warning
  - Discover undiscovered exploits, including Zero Days
  - Rapid isolation of comprised VM

SCIT Disrupts Attacks

- Restores servers to pristine state in minutes
- Reduces malware persistence
- Disrupts “stay in” and “act” stages
- Eliminates detected and undetected attacks

Breaches are inevitable. Relying on detection is yesterdays war

SCIT Technology - Applications



Cyber Threat Landscape
SCIT Concept
SCIT Technical
Case Studies
SCIT Status
Questions?

Case Study: Tactical Cyber Attack Deterrence (TCAD)

SPAWAR Systems Center PACIFIC

One of the most vulnerable aspects in tactical cyber security arises from the need to fuse data from secure and unsecure (usually local or regional) data. The field commander needs to rely on reliable data fusion strategies to guide and inform the daily decision making. While many of the data sources have been vetted, the typical tactical command and control center accepts information from sources that have not been vetted.

Solutions Provided

- Restored the data collection servers to a pristine state every minute, thus removing any malicious codes installed on the computer
- Increased Cyber Resiliency
- Used Redundancy to provide uninterrupted service

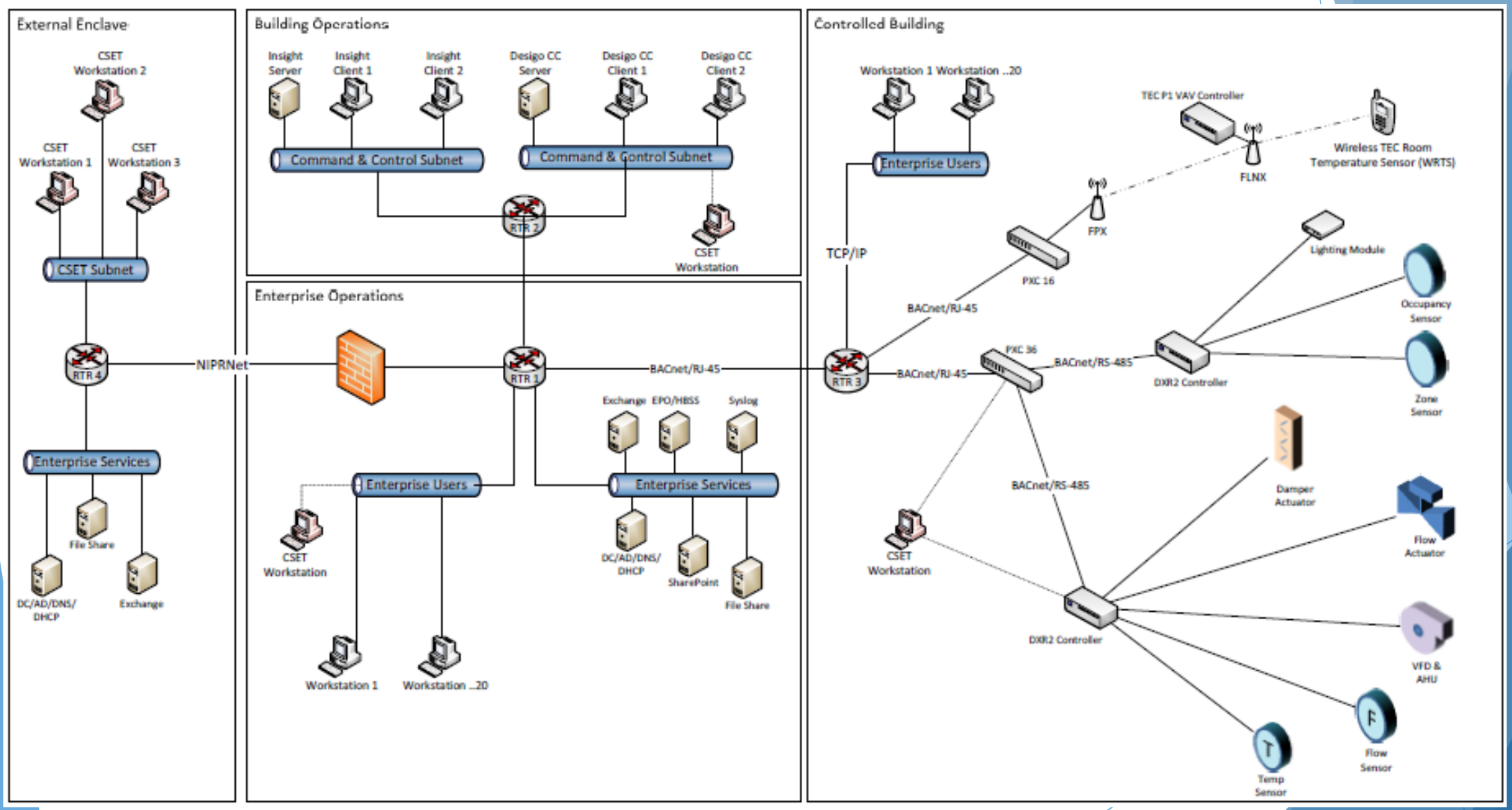
Business Results

- Made it significantly harder to steal critical tactical data
- Reduced the opportunity to spread infection to other systems

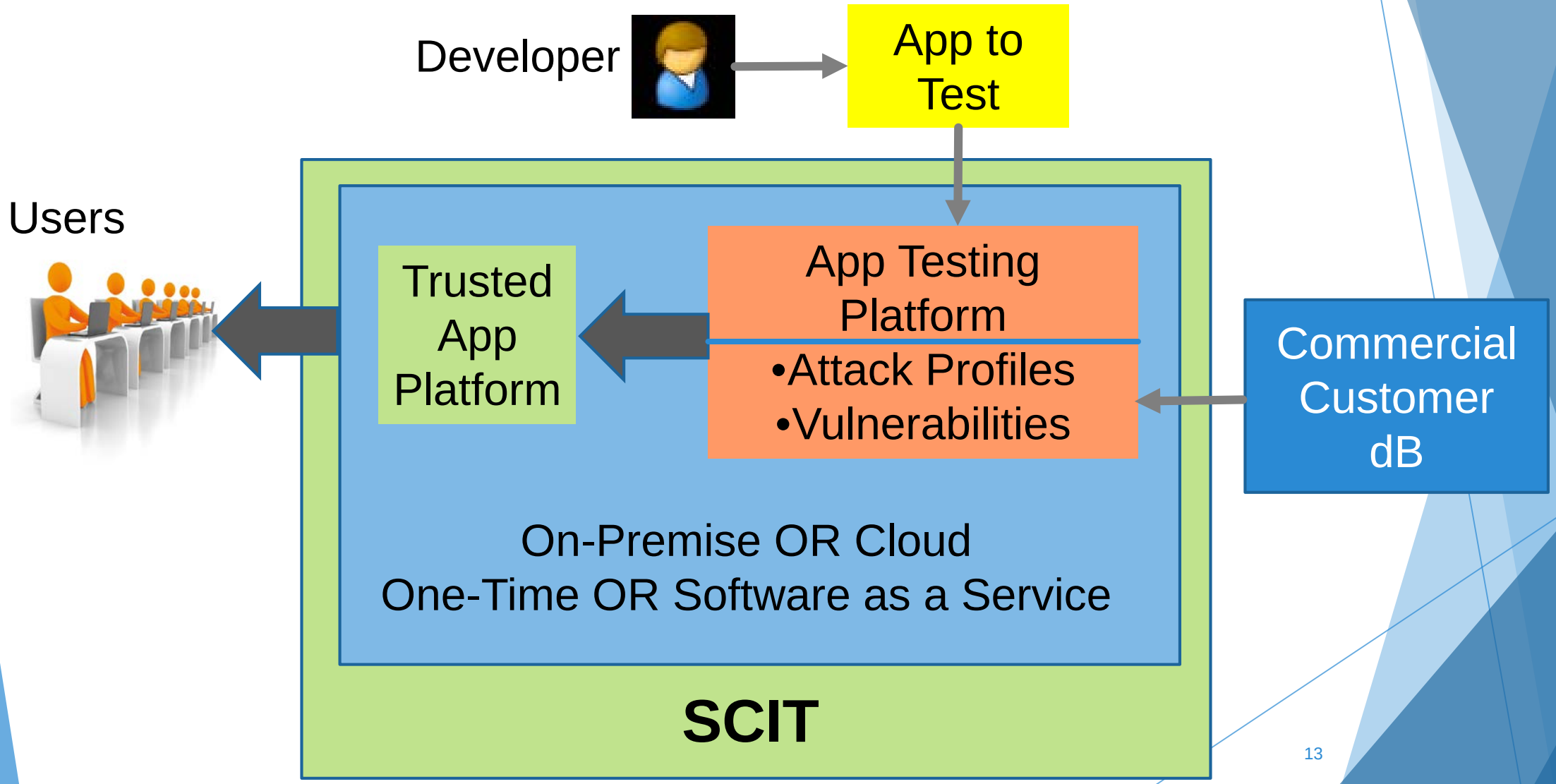
Next Project: Tactical Cloud Server Protection (TCSP)

Space and Naval Warfare Systems Center, Pacific (SSC Pacific), San Diego

National Cyber Range – Building Automation Control System



Secure Application Testing and Hosting



SCIT Advantage

Security : Resilience

- Mitigate APT attacks: Reduce data ex-filtration losses
- IT early warning alerts: Discover zero days
- Respond to high threat intensity
- Recovery
- Forensic

System and Network Management

- Operational Resilience. No memory leaks
  - Apply hot patches
- Configuration Management
- Automatically replace compromised VMs
- Disaster Recovery

SCIT Advantage

Security

- Mitigate APT attacks: Reduce data ex
- IT early warning alerts: Discover
- Respond to high threat inte
- Recovery
- Forensic

System and

- Operati memory leaks
  - Apply h
- Configurati nagement
- Automatically replace compromised VMs
- Disaster Recovery

Not dependent on detection!

Status of SCIT

- Implemented on VMware, AWS Cloud, Rackspace Cloud
- Awarded 6 US Patents
- Interfaced with other security tools: HP Fortify, CA APIM Gateway
- Demonstrated to SPAWAR SCP and DOD JCTD Office.
- Cyber Quest 18 – short listed

"SCIT technology shifts the cyber security focus from vulnerability elimination to consequence management."

– *Gen. Michael Hayden, (Ret) former Director of the Central Intelligence Agency and National Security Agency.*

Questions ?

Arun Sood

asood@gmu.edu

asood@scitlabs.com

703.347.4494