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?

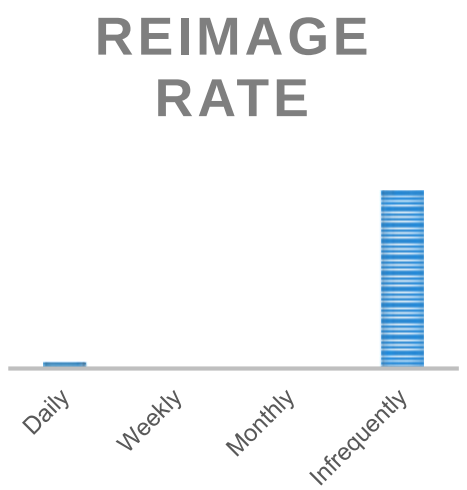
Preliminary Survey

- 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.

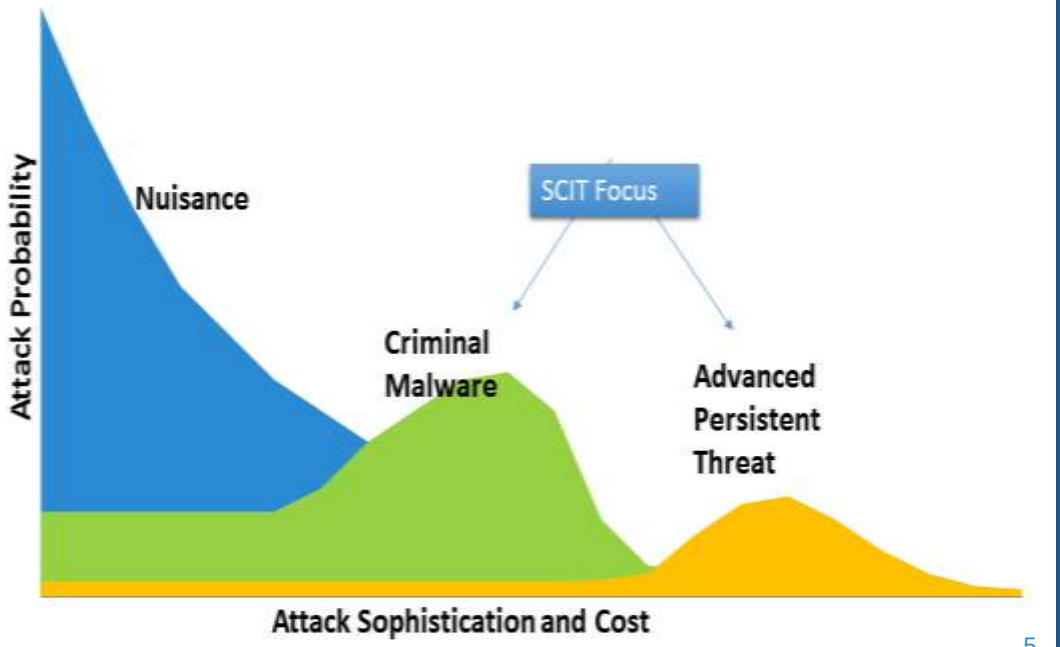
Cyber Threat Landscape

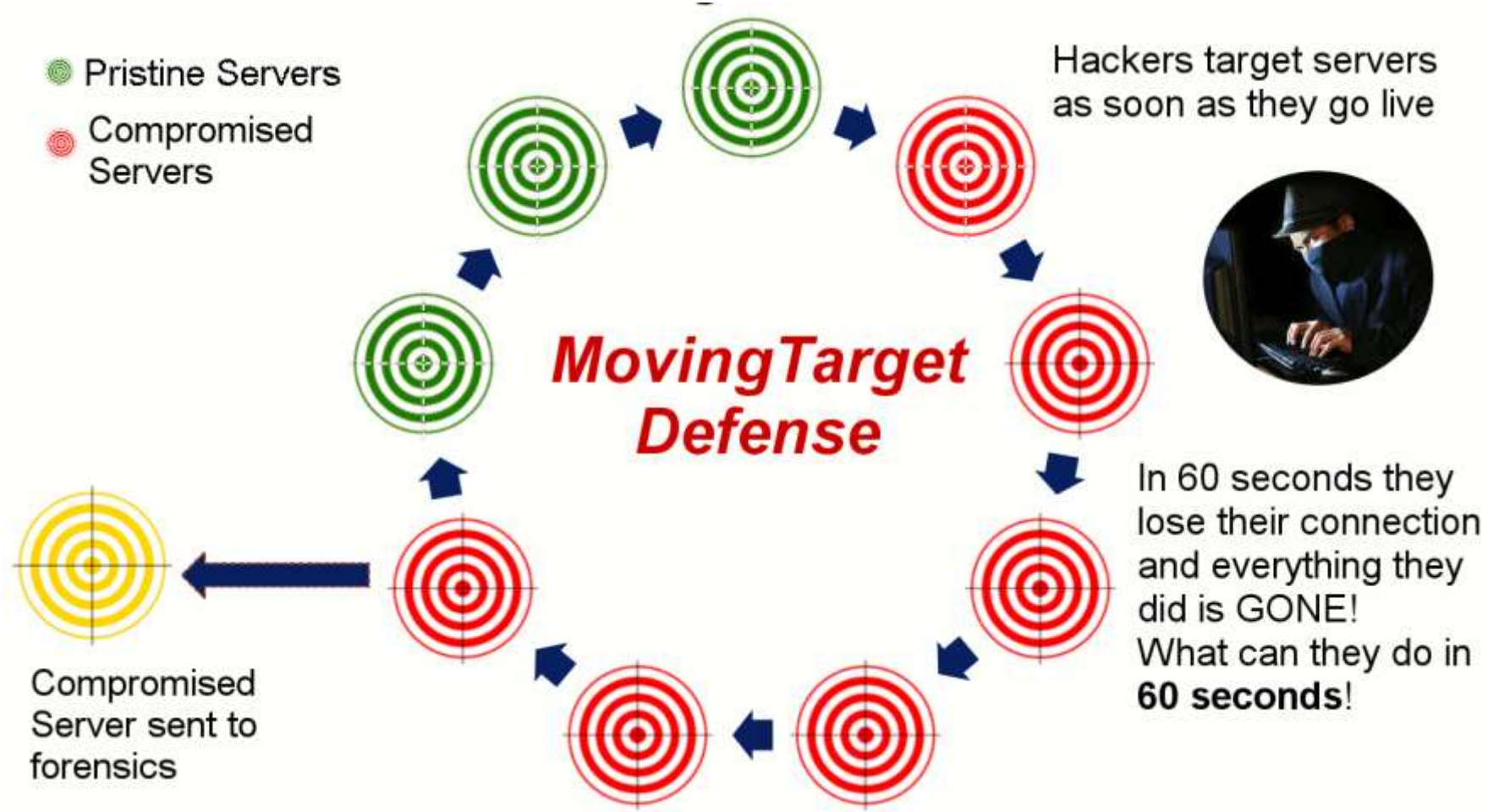
Cyber attacks	• are overwhelming enterprises • only some breaches are high profile
Reality	• attacks occur daily
Threat landscape	• changes rapidly • can security tools and personnel adapt? • can tools respond to unknown issues?

Most breaches discovered by law enforcement

U.S. OPM	• 300 days until detection • 22 million employees data exposed
Target	• 20 days in system • 40 million credit and debit cards exposed
JP Morgan Chase	• 76 million households and 7 million small businesses exposed
Experian	• 15 million T-Mobile customers data exposed • Over 100+ breaches
E-trade, Scottrade, Dow Jones	• Only learnt of breach via law enforcement

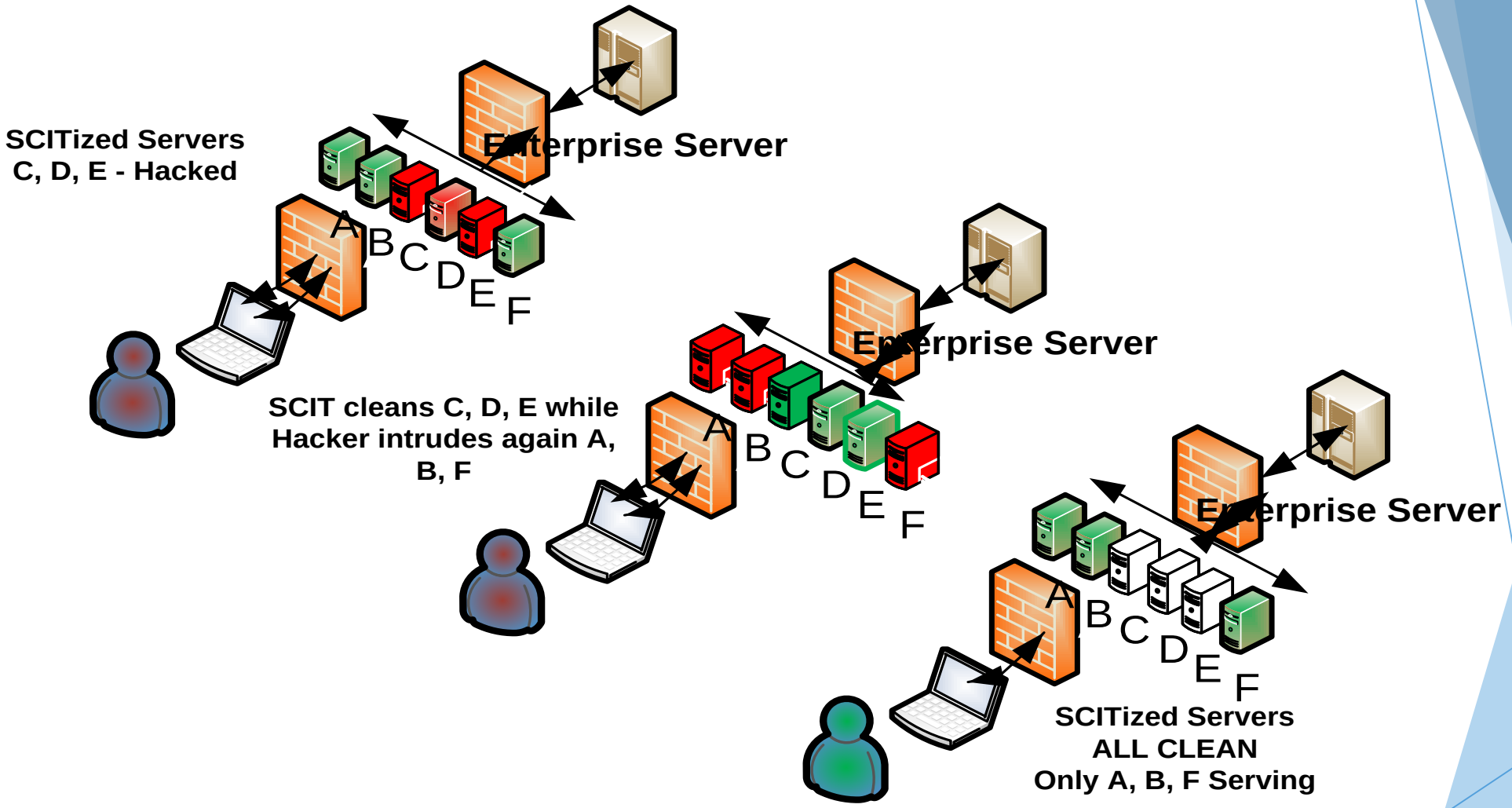
- Attackers are agile and constantly searching
- Intrusions can go undetected for 8 months
- Time for successful attack = 4 to 6 days
- Time to resolve an attack = 46 days
- Overreliance on detection of cyber intruders is unwise





SCIT – Resilience, Restoration, Recovery, Forensics

A New Way of Doing Business



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

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

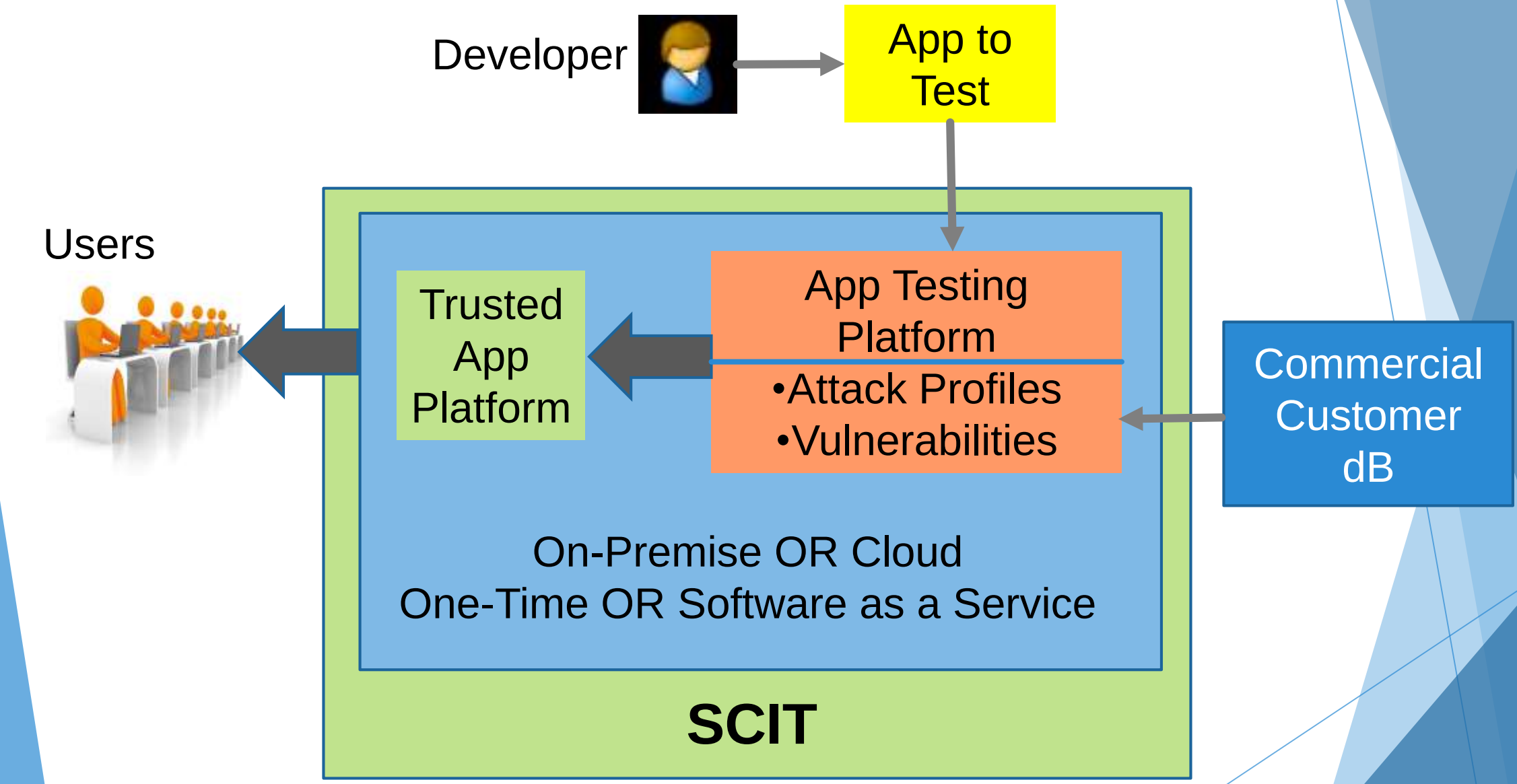
- Restored the data collection servers to a pristine state every minute, thus removing any malicious codes installed on the computer
- Increased Cyber Resiliency
- Used Redundancy to provide uninterrupted service

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



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 e
- IT early warning alerts: Discover
- Respond to high threat inte
- Recovery
- Forensic

System an ement

- 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.
- App protection proposal reviewed by DHS S&T (2/2017) – rated selectable

"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