Security Architectures in the Evolving Enterprise

Arun K. Sood

Co-Director of the International Cyber Center,

Professor of Computer Science

George Mason University

Evolving Security Approaches

- Compliance Driven FISMA OMB-130A
- Continuous Monitoring 800-137
- Risk Management 800-37, 800-39
- Agile Defense 800-39

Multi-National Security Breach

- http://news.bbc.co.uk/2/hi/technology/7118452.stm
- If a user searched Google for terms such as
  - "hospice", "cotton gin and its effect on slavery", "infinity" and many more
  - The first result pointed to a website from which malicious software was downloaded and embedded on user system.
- Criminals in country A created domains that were mostly bought by companies in country B and hosted in country C. Tens of thousands of domains were used.
- These domains tricked the indexing strategy of Google to believe that these web pages were good and reliable source of information.

Our focus: targeted and organized attacks.

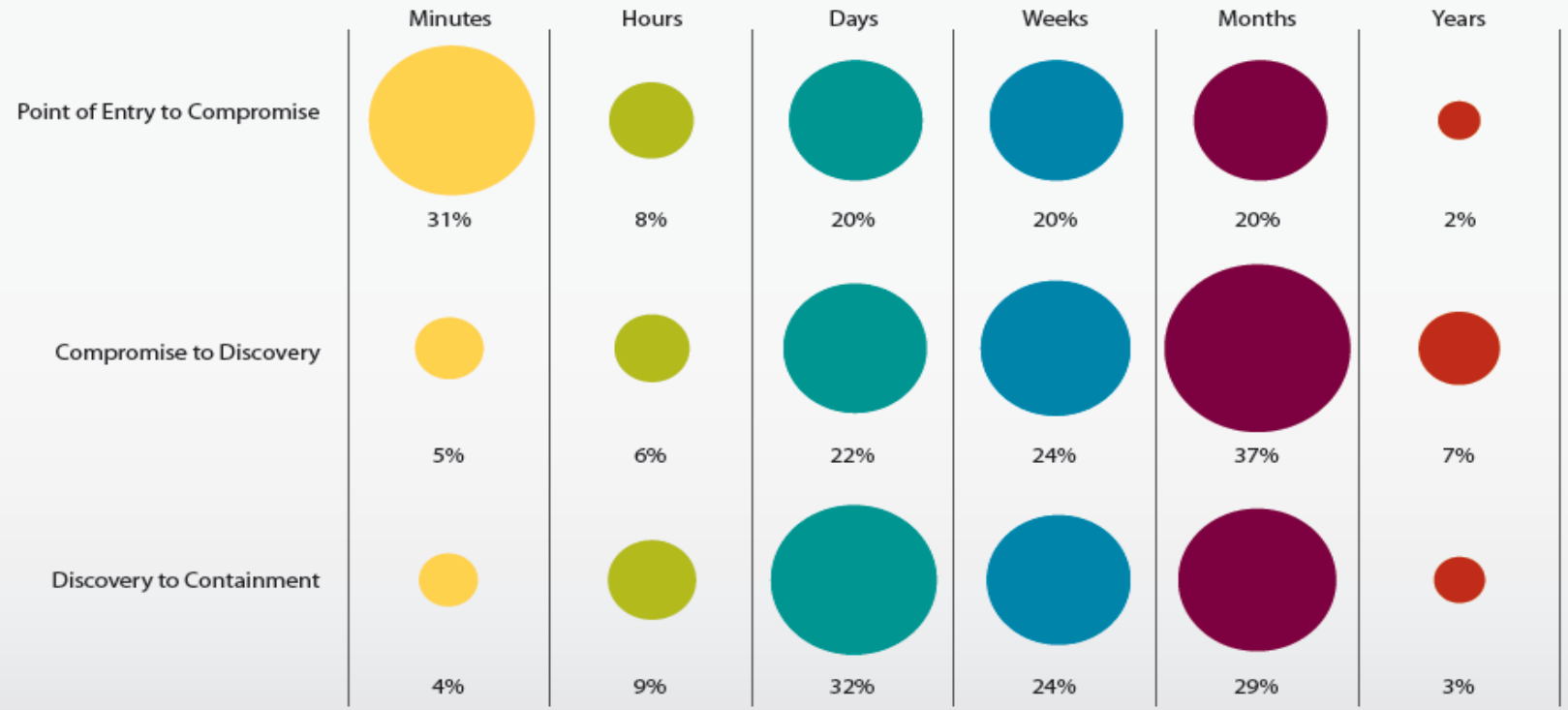
The Problem

- Verizon Business (DBIR2009, 2010): Customized malware hard to detect. Intrusion persists for days, weeks, months.
- Network Solutions, Wyndham Hotels.
- Symantec produced 920,000 malicious signatures in 2009.
- Recovery from a breach is costly: $6.3M [Ponemon Inst]

Current reactive approaches are inadequate. An intrusion tolerance layer would help.

Verizon DBIR 2010

Figure 35. Timespan of events by percent of breaches



TREND MICRO

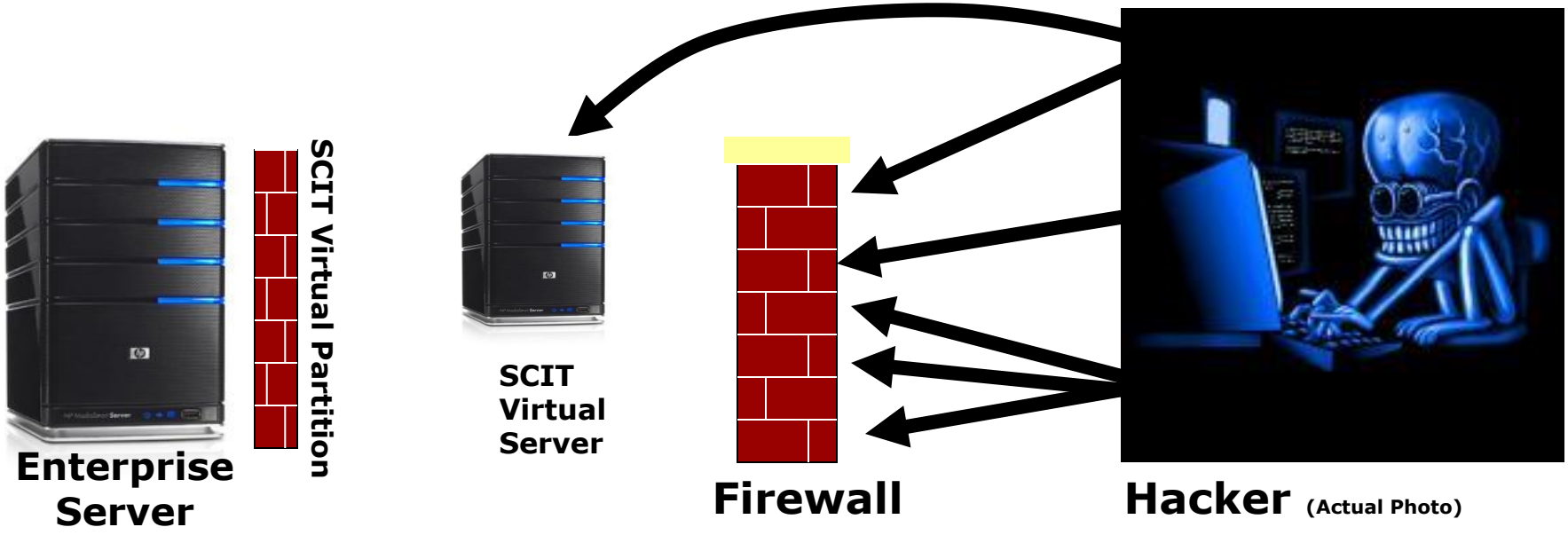
Produced by: CSO BUSINESS RISK LEADERSHIP

Defense in Depth

- Best if layers are independent.
- Firewalls depend on inspection of incoming packets.
- IDS/IPS depend on inspection of incoming and outgoing packets.
- Threat independent approaches are needed.
  - White list of software.
  - Recovery-based intrusion tolerance.

Self Cleansing Intrusion Tolerance (SCIT)

SCIT provides Intrusion Tolerance for servers…



Every minute SCIT software cleans and restores the virtual server to its pristine state

SCIT Solution Properties

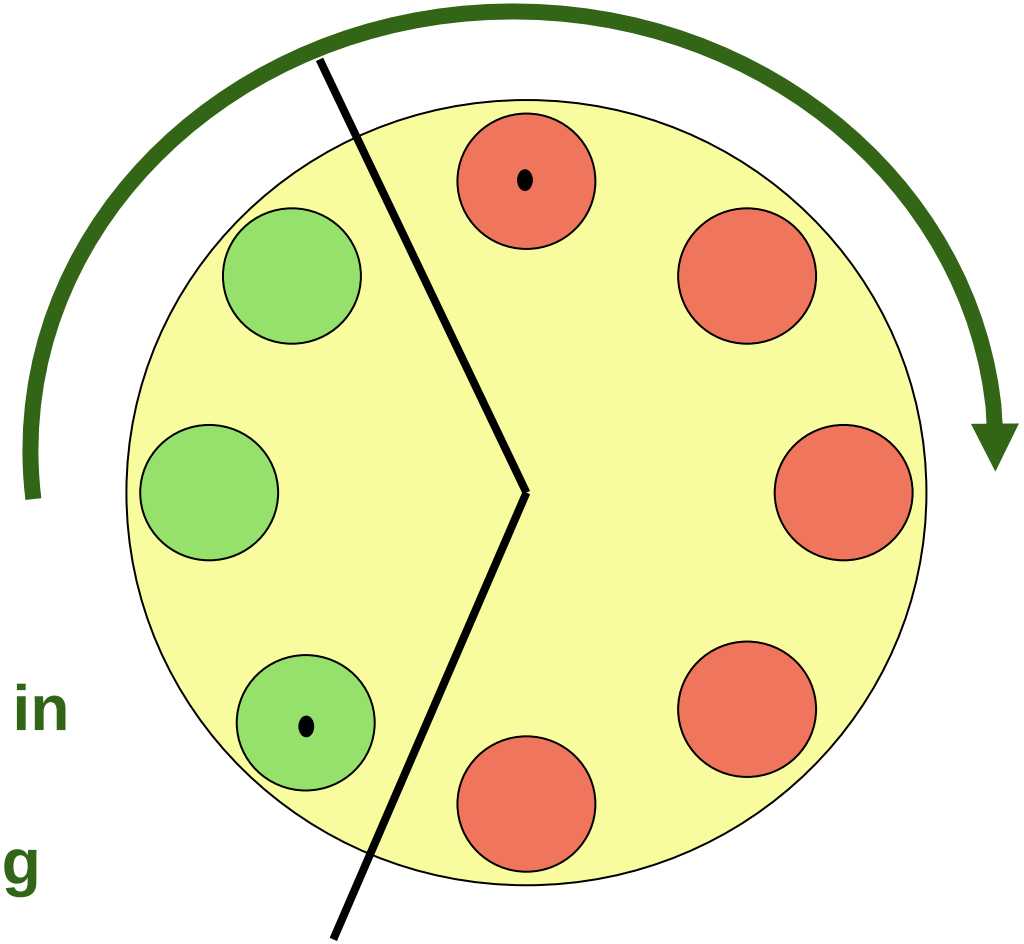
- Static Servers Converted to Dynamic Environment
- Threat Independent
- Rapid Recovery: Work Through an Attack
- Emphasize Temporal Dimension
- Virtualization as a New Framework for Server Security

Compare Reactive Approaches and Intrusion Tolerance

Issue	Firewall, IDS, IPS	Intrusion tolerance
Risk management.	Reactive.	Proactive.
A priori information required.	Attack models. Software vulnerabilities.	Exposure time. Length of longest transaction.
Protection approach.	Prevent all intrusions.	Limit losses.
System Administrator workload.	High. Manage reaction rules. Manage false alarms.	Less. No false alarms generated.
Design metric.	Unspecified.	Exposure time.
Packet/Data stream monitoring.	Required.	Not required.
Higher traffic volume requires.	More computations.	Computation volume unchanged.
Applying patches.	Must be applied immediately.	Can be planned.

How SCIT Works

Servers
-Virtual
-Physical



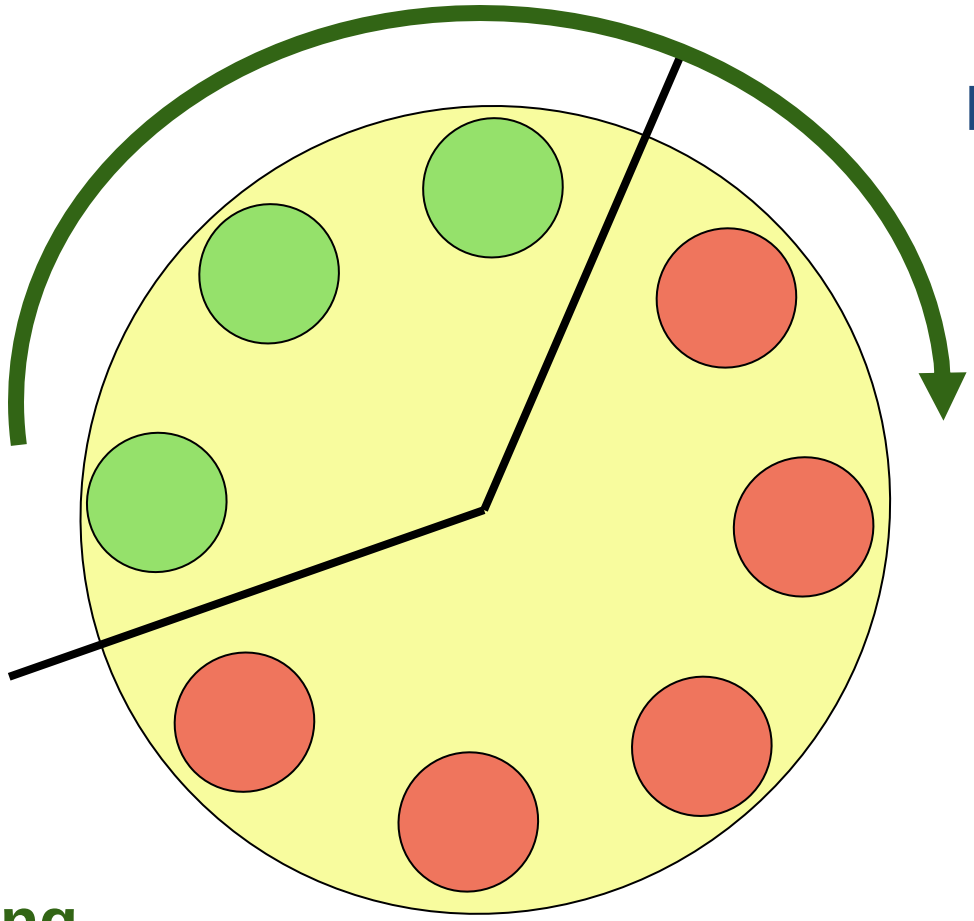
Server Rotation

Offline servers; in self-cleansing

Online servers; potentially compromised

How SCIT Works - 2

Servers
-Virtual
-Physical



Server Rotation

Online servers; potentially compromised

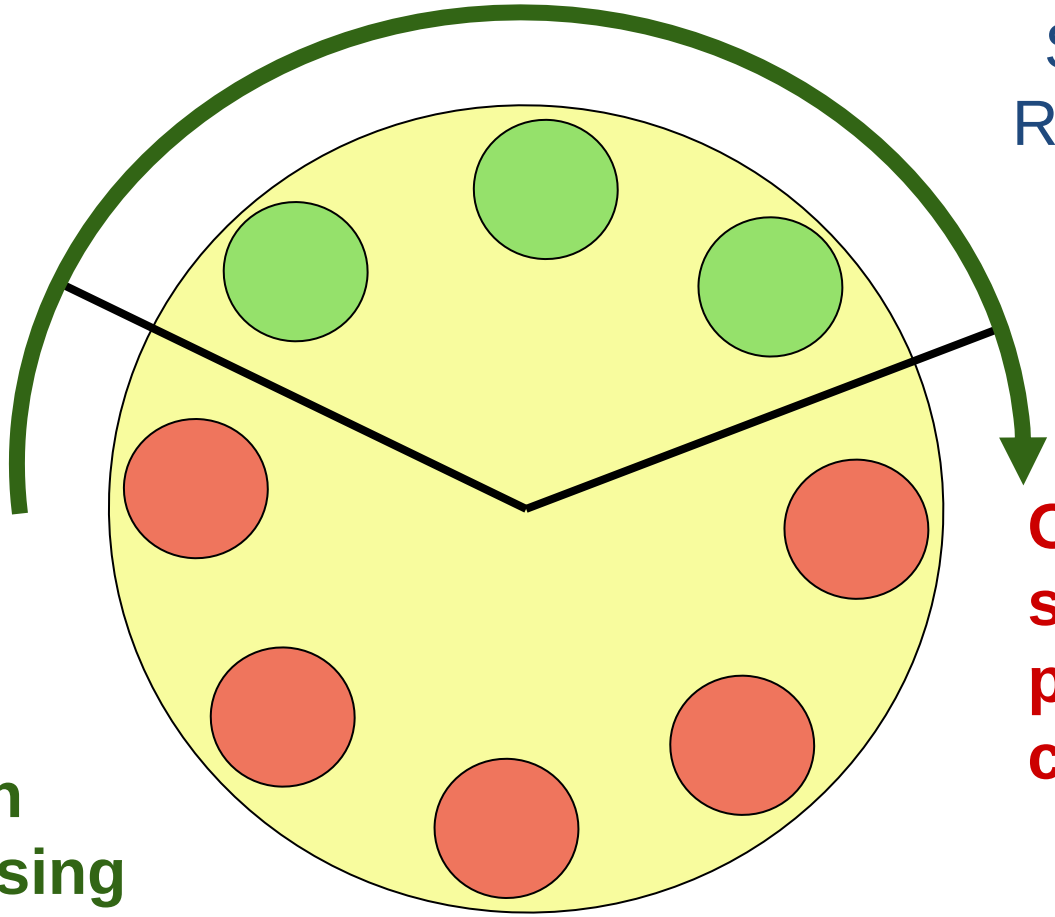
Offline servers; in self-cleansing

TREND MICRO

Produced by: CSO BUSINESS RISK LEADERSHIP

How SCIT Works - 3

Servers
-Virtual
-Physical

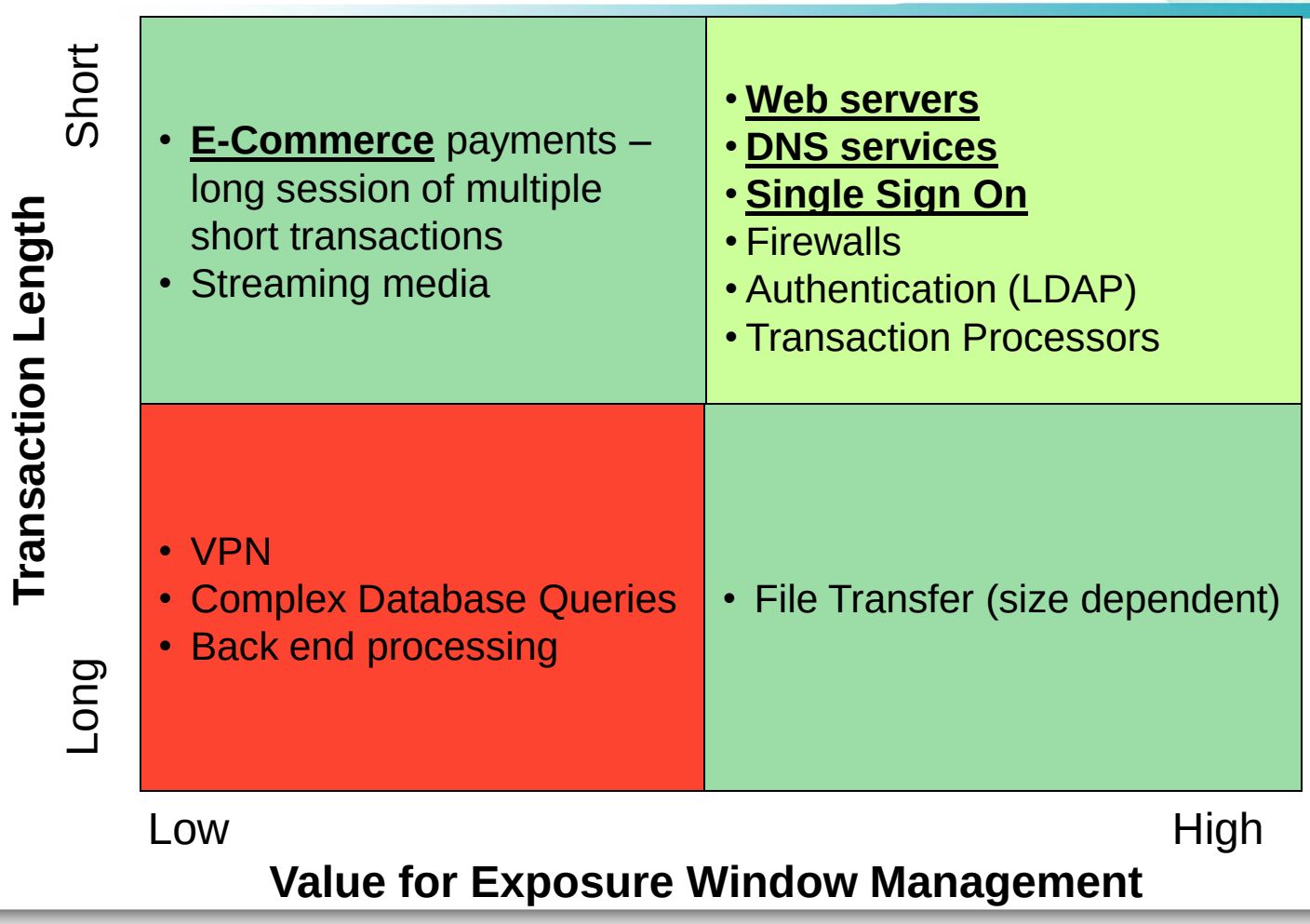


Server Rotation

Online servers; potentially compromised

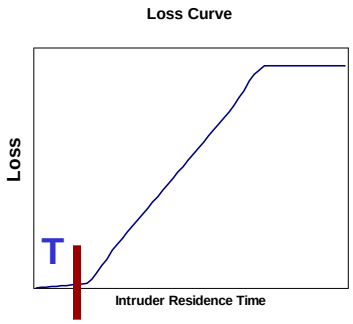
Offline servers; in self-cleansing

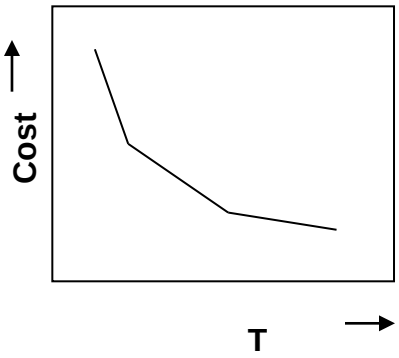
Target Applications



SCIT Solution Properties

- Increase security by reducing exposure window
- Decreasing available time for compromise exploitation
- No packet inspection; No signatures; No detection
- SCIT does not eliminate vulnerabilities but makes it difficult to exploit the vulnerability
- Integrated system: prevention, detection, tolerance systems
- Adaptive SCIT
- Reduce managed services cost
- Increase availability – reduce down time for upgrades – fewer reboots





Collaboration with Systems Integrators

- Lockheed Martin
  - Testing and validation of SCIT servers.
  - Funded SCIT research
- Northrop Grumman
  - Testing and validation of SCIT servers.
  - Matching partner – Virginia CTRF project
- Raytheon
  - Collaborated on SBIR proposal

Testing – Northrop Grumman

Component	Test Objectives	Findings
Basic Web Server with Session persistence	Defacement (recovery) System Compromise (limit effects) Data Corruption (recovery) Data ex-filtration (limit effects)	The resilience of the underlying VM architecture proved effective at thwarting any long term or permanent damage to the platform as a result of malicious activity.
E-Commerce Application	Defacement (recovery time) System Compromise (limit effects) Data Corruption (recovery) Data ex-filtration (limit effects) Shopping Cart Price manipulation	The findings were the same as the basic web server and the shopping cart was not subject to manipulation
Single Sign-On	SQL injection System Compromise Unauthorized access	Due to effective firewall and authentication input filtering the SSO architecture proved immune to O/S Corruption and Database Exploitation attack vectors. The underlying rotation of SSO Virtual Machine instances proved transparent throughout the entire course of testing.

Overall

The SCIT platform does reduce exposure time and confuses attacker efforts.

There is a slight performance degradation as exposure time is reduced.

Review + Other Issues

- SCIT: Why? How? Scope. Independent Validation.
- Performance.
- DOD Network. Specific Server: SCIT – DNS.
- Scalability.
- Plans.

Demo