Proactive Cyber Deterrence – Reducing Zero Day and APT Losses

February 6, 2013

Arun Sood, Ph. D.
CEO, SCIT Labs, Clifton, VA
asood@scitlabs.com

Agenda

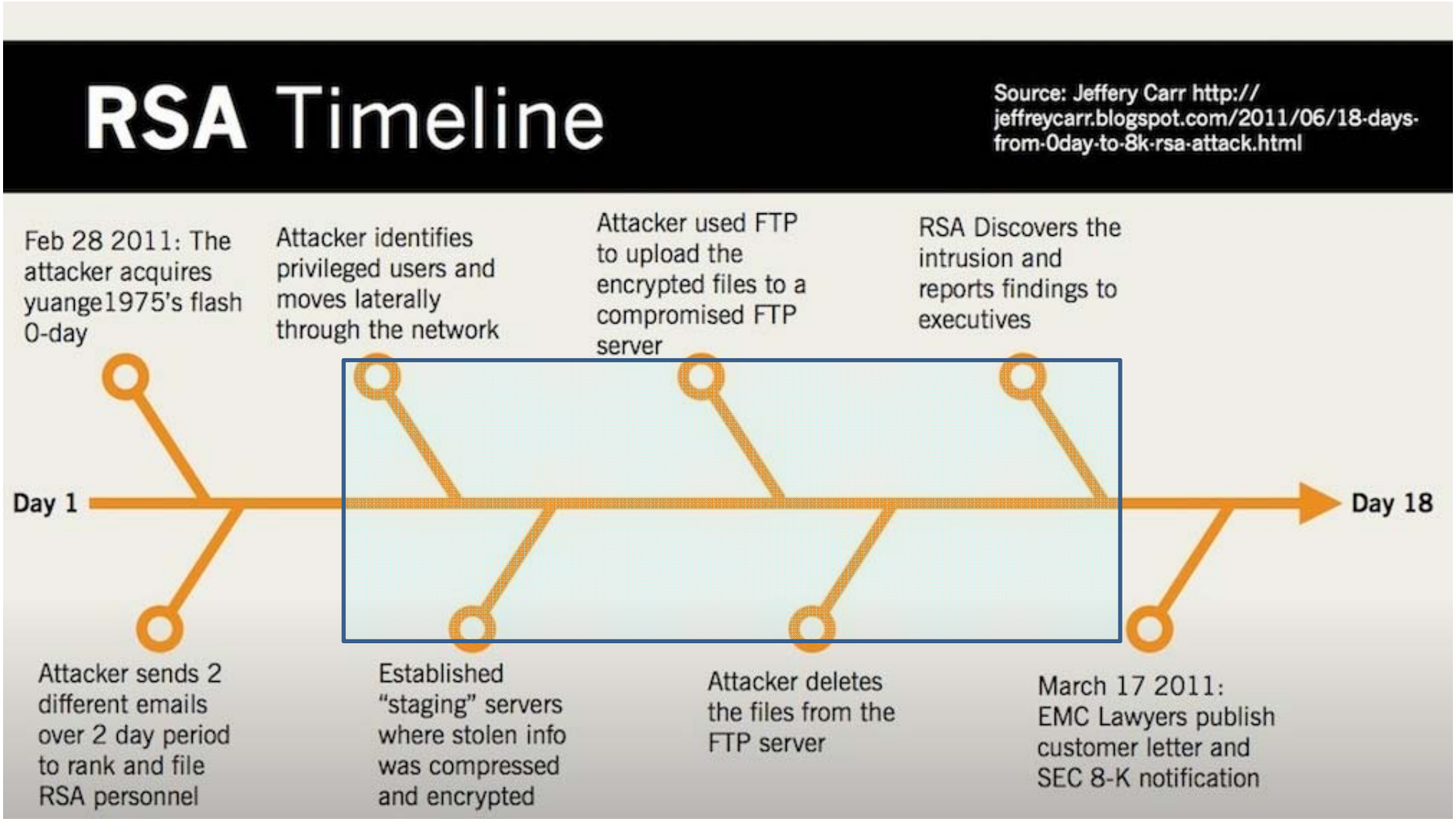
- SCIT Overview: technology, case studies, value proposition, market assessment.
- Mission requirements: moving target defense, dynamic defense, mitigation.
- Zero days and APT – reducing losses

About SCIT Labs

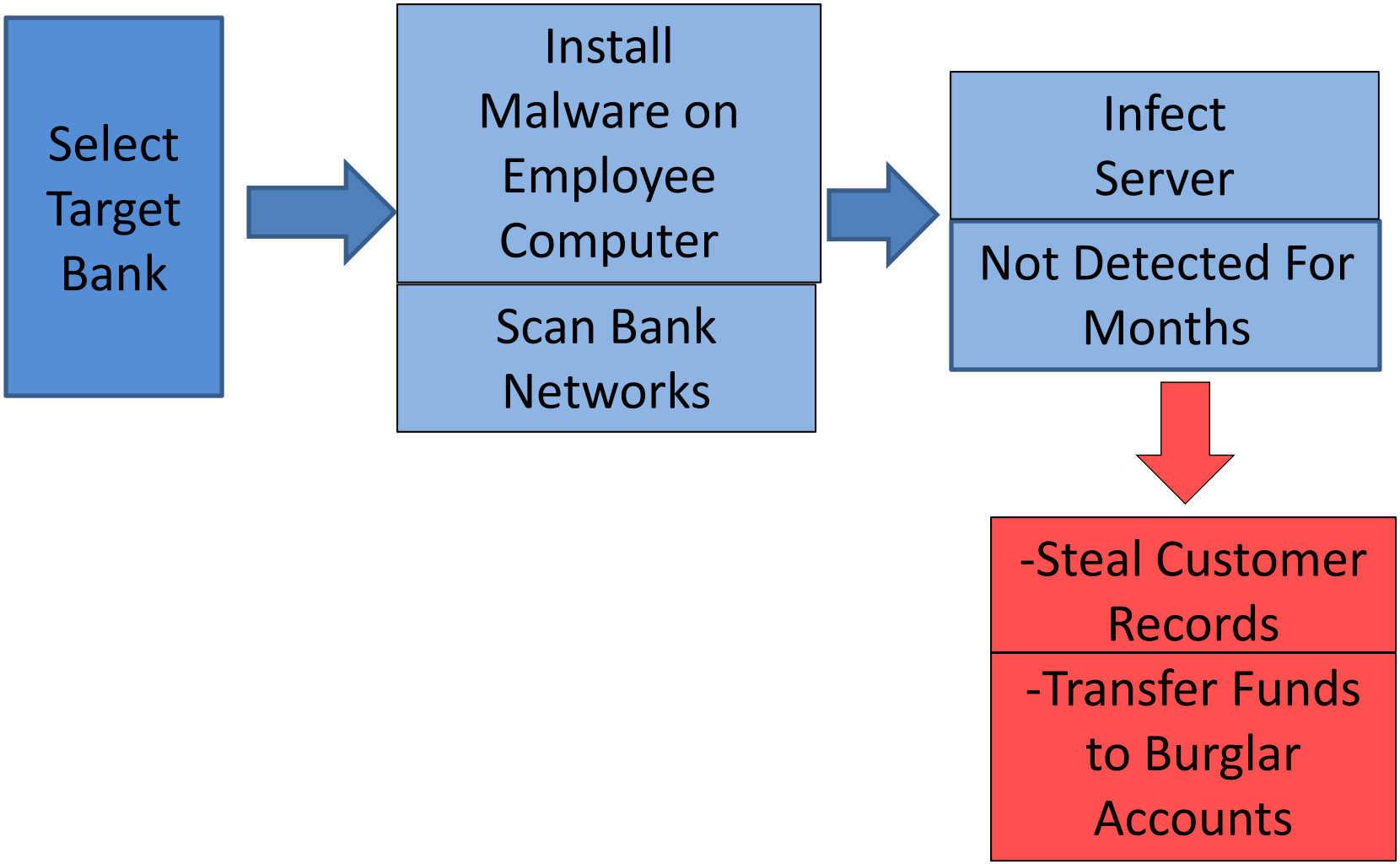
- Founded in 2007 as a George Mason University spin-off
- Accomplished executive team of business and technology leaders
- Achievements and Awards
  - 2008 – Winner of the TIE-DC Elevator Pitch Competition
  - 2009 – 2nd place award for the Global Security Challenge (GSC) SC Cyber Security Challenge
  - 2010 – 1st place award for the Global Security Challenge (GSC) Security Technologies of Tomorrow Challenge
  - 2012 – NSA Corporate Technology Challenge – short listed by technical experts
- Patented Technology
  - 5 patents issued, 1 patent in Notification of Allowance

SCIT Cyber Resilience

- Regularly restore application to pristine state
- Continues to function in presence of intruder
  - Uninterrupted service
  - Provide max functionality
- Limits performance degradation
  - Define from a customer viewpoint
- Return to normal operation
  - ASAP


RSA Timeline
Source: Jeffery Carr http://jeffreycarr.blogspot.com/2011/06/18-days-from-0day-to-8k-rsa-attack.html
Feb 28 2011: The attacker acquires yuange1975's flash 0-day
Attacker identifies privileged users and moves laterally through the network
Attacker used FTP to upload the encrypted files to a compromised FTP server
RSA Discovers the intrusion and reports findings to executives
Day 1
Day 18
Attacker sends 2 different emails over 2 day period to rank and file RSA personnel
Established "staging" servers where stolen info was compressed and encrypted
Attacker deletes the files from the FTP server
March 17 2011: EMC Lawyers publish customer letter and SEC 8-K notification

Cyber Burglary



Intruder Residence Time in Months

WYNDHAM

5 months (Average at hotels 156 days)

network solutions

2 months

Michaels THE ARTS AND CRAFTS STORE

3 months

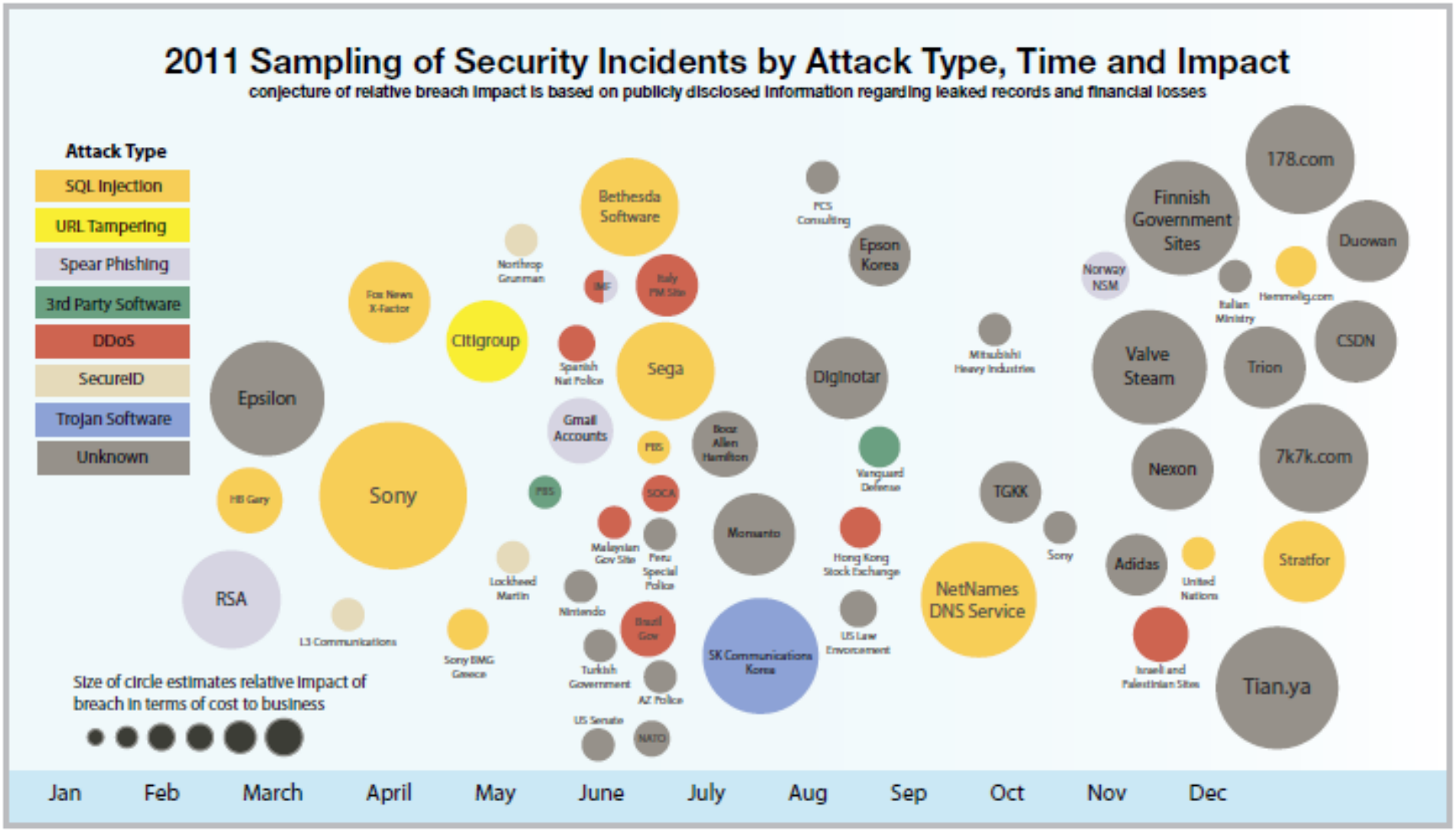
U.S. Chamber of Commerce
Standing Up for American Enterprise

6 weeks to 1 year

NORTEL

10 years

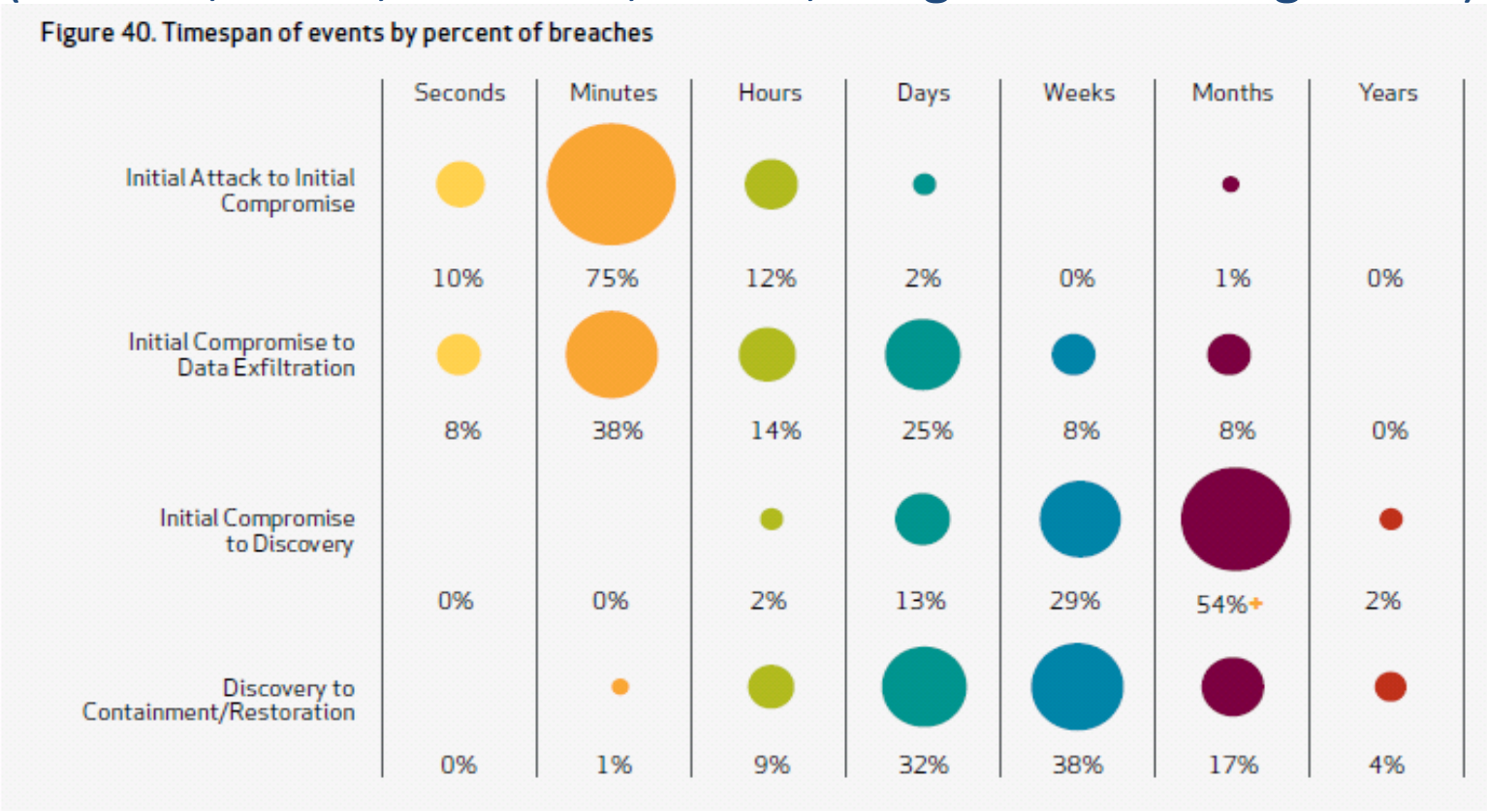
SCIT Labs Confidential and Proprietary



Source: IBM Xforce Report 2012

Intruder Residence Time

Verizon DBIR 2012: 855 breaches 174 M records compromised (Verizon, US SS, Australia, Dutch, UK government agencies)



Compromise to Discovery: 98% more than 1 day; Discovery to Containment: 90% more than 1 day

SCIT Goal: Reduce Compromise to Restoration to 1 minute.

SCIT Technology

Cyber Security Threat

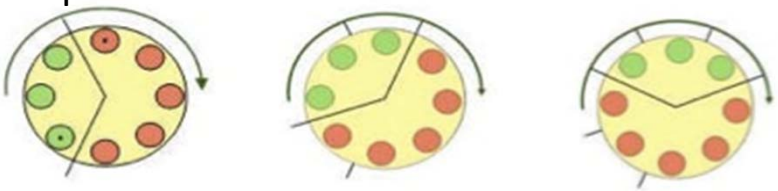
I. Intrusions are inevitable

II. Bad guys stay in systems for days, weeks, months

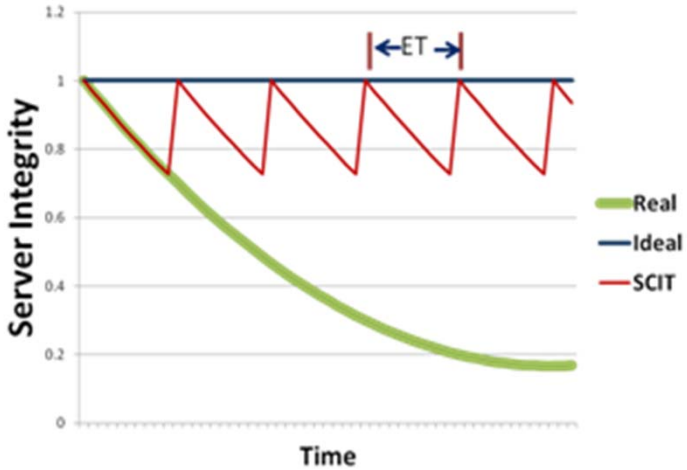
III. Current servers are sitting ducks

How SCIT Works

- **Online servers are assumed compromised. Offline servers are restored to pristine state..**
- SCIT reduce exposure to bad guys; and restores serves to pristine state every minute.
- Example: **5 online** and **3 offline** servers.



Restore System Integrity



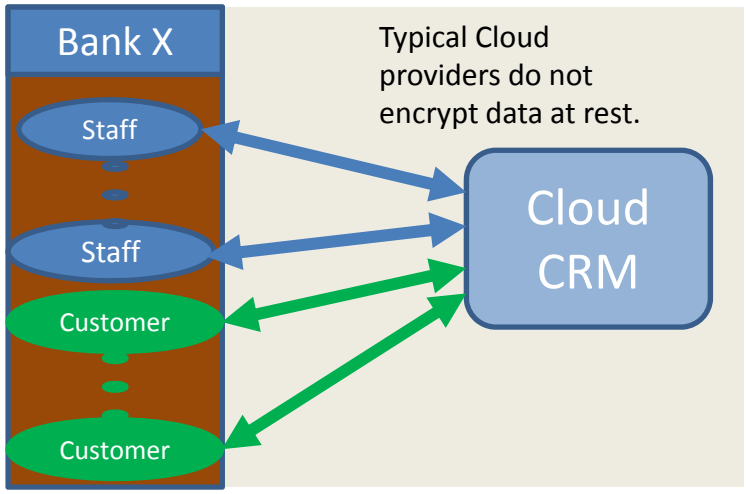
From Verizon Business DBIR 2012

- For 90% Breaches Compromise to Restoration > 2 days
- SCIT would restore systems to pristine state in 1 minute

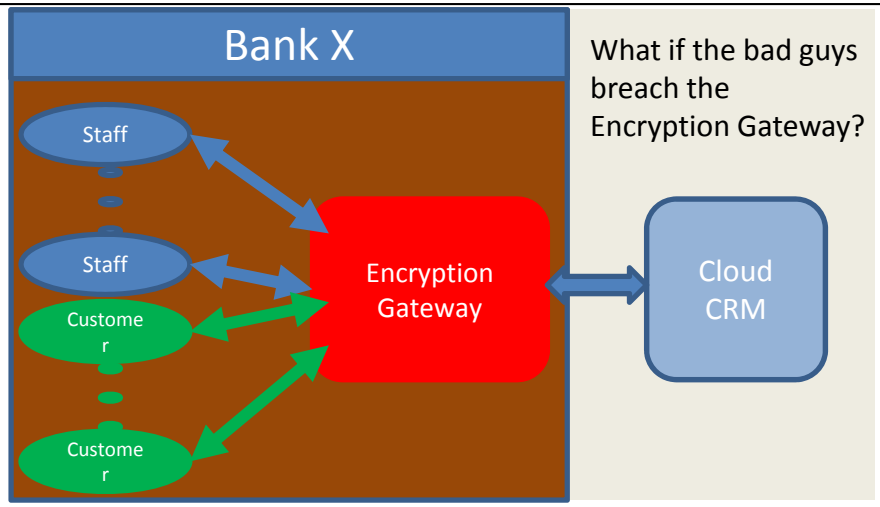
Ecommerce Demo Video

Illustrative Use Case: Secure Gateway

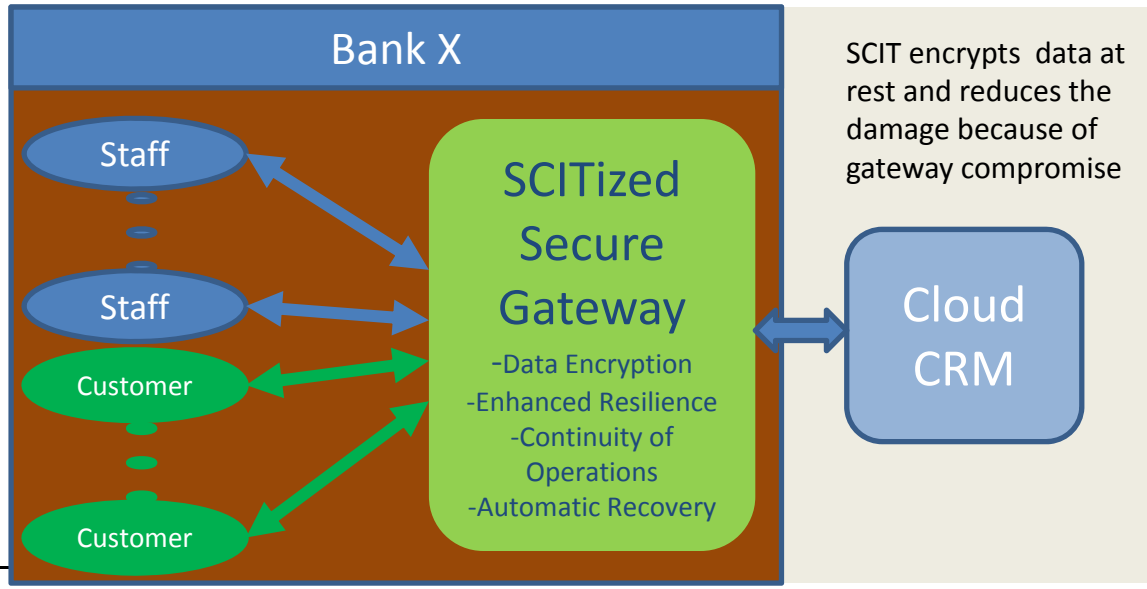
PCI DSS requires data at rest encryption, and host IDS. An Encrypted Gateway can achieve the former. SCITized Secure Gateway provides a compensating control and achieves both requirements.



Typical Cloud providers do not encrypt data at rest.



What if the bad guys breach the Encryption Gateway?



SCIT encrypts data at rest and reduces the damage because of gateway compromise

Evolving Security Standards

CISOs focus on Compliance. Budgets are constrained and compliance is job one. Compliance occurs at one point in time, and is inadequate. NIST has formulated additional security standards.

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

- " Many organizations are concerned about advanced persistent threats, so we added new organizations to use different strategies to combat those types of threats, " Ross, NIST http://www.nist.gov/itl/csd/sp800-022812.cfm 800-53 Rev 4 **Non-Persistence control (SI-14)**

SCIT meets these needs and focuses on 5 goals.

Resilience

Monitoring

Tolerance

Recovery

Forensics

SCIT Value Proposition

Value Proposition

- **SCIT** makes hackers work harder.
- **SCIT** ensures continuity of operations.
- **SCIT** reduces cost of security operations.
- **SCIT** increases availability & reduces CAPEX.
- **SCIT** operational resilience reduces OPEX.

SCIT Advantages

- **SCIT** reduces ex-filtration risk.
- **SCIT** deletes malware without detecting it.
- **SCIT** reduces support cost – no false positives; load and forget software.
- **SCIT** adapts to threat intensity.
- SCIT supports continuous monitoring and compromised VM handling
- **SCIT** eliminates memory leak losses.
- **SCIT** hot patches – no server reboots

SCIT is a Robust Solution

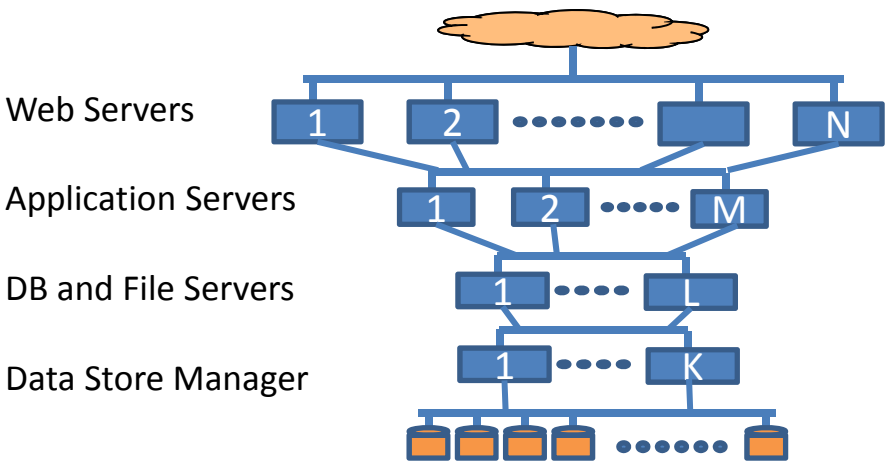
- Cyber Risk = Threats **X** Vulnerabilities **X Consequences**

  Current systems focus on eliminating vulnerabilities. SCIT focuses on consequence reduction.

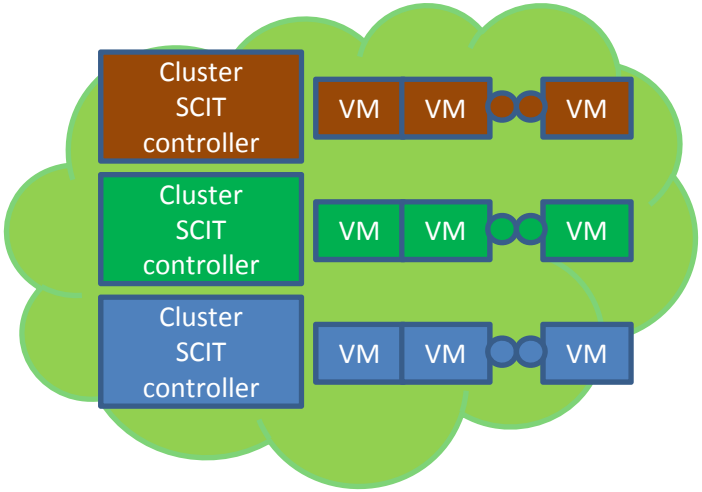
- Reliability Measures: MTTF, MTTR

  Current systems increase MTTF. SCIT reduces MTTR (R=Recovery)

SCIT Applies to Each Layer of Multi-tier Architecture



Market Assessment

Customer Segments	Key Activities
• Government: DOD, IC, Civil • Corporate: Domestic, International, Large, Medium • Professional: Legal, Accounting • Cloud Service Providers and Hosting Services: SaaS, PaaS , IaaS • Mobile Apps • Independent Software Vendors (ISV)	• Recognition of SCIT: Participate in Challenges (GSC, GCV, NSA). Presentations. Interviews and Publications • Proposals funded: Army – CERDEC, DHS – S&T, Sub Contracts: NHS, DOL • Proposals selected: DHS – Protecting the Smart Grid – not currently funded • Proposals in process: SPAWAR: C4ISR /ET: Source Selection Completed; NSA:CND R&T • Other Proposals: SPAWAR Energy, USDA, USDOT, Wilmington Port, Northrop Grumman (ES)/ET • Recent presentations: NSA Global Mitigation; Cyber Command Dynamic Defense; National Nuclear Security Agency
SCIT Scalability •Thousands of VMs. Many applications. Variety of exposure times. •Interface SCIT to key commercial security products: HP Fortify RTA; Guidance Encase Forensics; Alien Vault SIEM. This approach combines the properties of reactive and proactive approaches. •Port to cloud. •Validate in DHS SBIR Phase I.	Private Cloud 

Combining SCIT & RTA functionality

SCIT and RTA have complementary properties. Combining the two approaches, provides a mixture of reactive and proactive cyber defense.

Type of Attack	No SCIT No RTA	RTA No SCIT	SCIT No RTA	SCIT and RTA
SQL Injection	Attack Successful	Protected Zero Loss	Losses Limited	Protected Zero Loss
Cross Site Scripting	Attack Successful	Protected Zero Loss	Losses Limited	Protected Zero Loss
Trojan installation	Attack Successful	Attack Successful	Trojan Deleted Losses Limited	Trojan Deleted Losses Limited
Zero day malware	Attack Successful	Attack Successful	Malware Deleted Losses Limited	Malware Deleted Losses Limited
Stealing Intellectual Property	Attack Successful	Attack Successful	Losses Limited	Losses Limited

Combined Cumulative Benefits

	Fortify Runtime	**SCIT**
A priori information required	Attack models. Software vulnerabilities.	Exposure time. Length of longest transaction
Protection approach	Protect listed vulnerabilities	Limit losses
Programming Environment	Java, .NET	Any
Applying patches	Must be applied immediately	Can be planned
Threats mitigated	Web Apps	Web, DNS, SSO, ….
Memory leaks	Not addressed	Eliminated

SCIT HP Runtime Video

http://www.youtube.com/watch?v=JgPp_5JUqb4

PROACTIVE CYBER ATTACK DEFENSE

Arun Sood, Ph.D.

asood@scitlabs.com

+1 703.347.4494