CONOP for SCIT Project

SCIT LABS

13834 Springstone Drive #200

Clifton, VA 20124

www.scitlabs.com

info@scitlabs.com

I. What are the customer problems?

- Ensure reliable Configuration Management on app servers/file servers/database servers/etc.
- Remediate compromises in as close to real time as possible.
- Prevent a compromised system from being a launch point within the organization.
- Eliminate the "persistence" of attacks – enemy must redeploy initial compromise technique/vector multiple times which provides tremendously greater visibility to their attack.
- Preserve evidence of compromise for future analysis.
- Compromised server can be stopped, isolated, and delivered to Forensic Analyst workbench – thus the analyst can focus on forensics rather than set up.
- Provide an additional source of information to identify false positives – since false positives could be 75% of the alerts, this dramatically reduces SOC cost.

II. Why is SCIT different than other host integrity tools?

- Existing tools such as McAfee/Tripwire/Symantec/… are reactive. These tools can help when the threat is well understood and well known. SCIT is proactive, and threat independent.
- Reactive tools provide no protection against zero day attacks. Reactive tools are in-effective while newly discovered vulnerabilities are going through the fix cycle – identify vulnerability; manufacture develops a patch; patch is distributed; user tests the patch in staging area; patch is applied. SCIT contains losses for zero days and during the fix cycle.
- SCIT puts an upper bound on the losses incurred because of a successful intrusion. This provides managers the flexibility in scheduling patch application.
- SCIT does not generate false positives.
- Reactive system properties are compared with SCIT in Table 1.

Table 1: Current Systems Compared with SCIT

	Firewall, IDS, IPS	SCIT: 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.

III. Comparison with Other Approaches - Cyber Risk Management Viewpoint

Cyber Risk is characterized as the product of three variables: Threats, Vulnerabilities and Consequences.

$$\text{Cyber Risk} = \text{Threat} \times \text{Vulnerabilities} \times \text{Consequences}$$

Cyber Risk can be reduced to zero if any one of the terms is driven to zero. The current reactive approaches attempt to reduce the vulnerabilities. Fixing of vulnerabilities involves the manufacturer and the fix cycle can take weeks or months. SCIT focus is on significantly reducing the consequences of an attack – we reduce the window of opportunity in which the adversary can do damage. We also reduce the impact of the threat by increasing the adversary work factor.

Most of the current reactive approaches are driven by detection and prevention paradigms, which in turn focus on vulnerability elimination (Table 2). In contrast, the SCIT focus is on reducing the consequences of a successful attack – SCIT does not eliminate vulnerabilities but makes it more difficult to exploit the vulnerabilities. By choosing lower exposure times, SCIT reduces the time the adversary has to do damage and thus forcing the adversary to make repeat attempts. For example, many organized and targeted attacks are aimed at stealing intellectual property – and reducing the connection duration makes this ex-filtration more difficult.

We note that in Table 2, the Threat column is blank. This simply emphasizes the obvious - the commercial users do not have the authority to launch cyber counter attacks. Typically threats are reported to law enforcement for further action. While SCIT is a

SCIT the digital vaccine
SCIT LABS
13834 Springstone Drive #200
Clifton, VA 20124
www.scitlabs.com info@scitlabs.com

defensive tool, it indirectly impacts on reducing the impact of all threats. One way we do this is by increasing the adversary work factor, i.e. we increase the work the adversary has to do to achieve success. This property is explicitly included as the right most columns in Table 2. The Moving Target approach of SCIT makes the adversary work harder: (1) the connection to the adversary is broken at regular intervals thus requiring repeat attempts; and (2) the servers are restored to a well known state in each rotation. Both these factors increase the adversary work factor. In comparison, consider the example of IDS and IPS. As the probability of detection is increased, the probability of false positive increases, and the work load on the SOC team increases – we characterize this as an undesirable increase in the defender work factor.

Table 2: Cyber Risk Assessment for Current Technology Approaches

Technology Approach	Threat	Vulnerabilities	Consequences	Work Factor A	Work Factor D
Intrusion Detection / Prevention		X			+
Firewall		X			+
Malware detection		X			+
Incoming Packet Monitoring		X			+
Packet Analysis		X			+
SSL Proxy		X			+
SIEM		X			+
Forensics		X			+
SCIT - Recovery + Intrusion Tolerance + Forensic Support			X	+	
Outgoing Packet Monitoring (DLP)			X	+	

IV. Definition and project implementation

- Review of the overall opportunity
  - Produce draft case study
- Select the tier to SCITize: webserver, application, database and data storage tiers will be considered.
  - DMZ is likely to be the first to be SCIized. Identify the webserver suite; requirements of persistent data
- Review the requirements to save the images
- Review the forensic requirements
- Develop a pilot project
  - SCIT software
  - Integration requirements

SCIT LABS
13834 Springstone Drive #200
Clifton, VA 20124
www.scitlabs.com info@scitlabs.com

    - Test plan
    - Training plan
    - Roll out plan
- Refine case study for release and distribution

V. What can SCIT do?

- We delete malware without detecting it.
- We make the lateral move of malware to other tiers of the architecture more difficult - because the guiding hand has limited time to act.
- Assuming a bi-weekly (20,160 minutes) server maintenance and a 10 minute exposure time for SCIT server, the volume of data lost is reduced by a factor of 2000.
- Repeated attempts by the determined malicious hacker, will expose the hacker, and thus act as deterrent.
- Volume of alerts is very large and many are false positives. There is a funnel that reduces the data to be processed. A FS company gets 1,000,000 packets per day, resulting in 10,000 IDS and log analysis alerts and the SIEM producing 100 events marked as requiring resolution. Two-thirds to three-fourth of these are false positives. Each investigation takes 0.5 to 5 hours with an average time of 1.5 hours. Thus 150 hours of highly qualified personnel is required 365 days a year, just to handle the high security risk alerts. This translates to a staff requirement of about 30 people – this is much more than the current staffing of this function. We also note that in this scenario, more than 100 hours per day is spent on resolving false positives SCIT strategy resolves false positives quickly. Since current staffing levels do not permit resolving all the alerts, we need to minimize the damage done in each attack – this is the focus of SCIT.
- Capturing the VM soon after the compromise is discovered reduces the set up cost for forensic analysis. The manual processes introduce a time lag. In some environments the data collection process is very time consuming. If the compromised VM is saved soon after it is identified, the data will remain secure and the VM itself will provide substantial information. We automate the set up process – stop compromised VM, copy and move the compromised VM. If required a new VM can be brought up in its place.

SCIT the digital vaccine
SCIT LABS
13834 Springstone Drive #200
Clifton, VA 20124
www.scitlabs.com info@scitlabs.com