SCIT LABS

13834 Springstone Drive #200

Clifton, VA 20124

www.scitlabs.com

info@scitlabs.com

CCF: SCIT BASED

CONTINUOUS MONITORING,

COMPROMISED SERVER HANDLING &

FORENSIC ANALYSIS

SCIT Labs, a leading provider of cyber security product and services, presents a new approach to continuous monitoring, compromised server handling and forensic analysis (CCF). This suite of software tools called CCF provides improved security workflows, reduced operating cost, and enhanced flexibility in managing high risk security alerts. CCF offers a proactive set of automated tools that can be easily integrated into your existing infrastructure without requiring modification of existing security infrastructure to manage these three functions more effectively and more efficiently.

Using a representative enterprise and the experience of a large financial services firm, this white paper discusses how CCF can be incorporated into an enterprise security architecture, how CFF works, and the benefits it offers over current cyber security solutions.

TODAY'S CYBER SECURITY CHALLENGE

Large enterprises use virtualization and virtual machines to maximize the utility of their information technology infrastructure. Virtualized systems and the cyber security defenses used to protect them are extensive and complex. A typical corporate enterprise has 2,000 virtual machines (VM) and 30,000 or more instances of these VMs. Each standard VM can have several replications running at one time. Typically, all replicates of a standard are equally valuable so they are all monitored at the same frequency. In this representative environment, web servers are saved once a day with a monitoring period of one day.

Large enterprises make significant investments in cyber defense products and then customize these products to support the specifics of their business operations and security requirements. Large virtualized environments usually include the following products and associated support and business processes:

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Web Application Firewalls
- User Authentication Software
- Anti-Virus Software
- Database Security Tools
- Fraud Detection Software
- Forensic Analytics
- Security Incident and Event Management software (SIEM)

Throughout the day these products analyze netflow, full packet, web logs, router logs, and host and application logs. The anti-virus software, IDS/IPS, web application firewalls, database security tools, web content filtering and fraud detection software all generate log files and event details. The combination of these products and the event management software that interrogates and evaluates security events generate high risk alerts that need to be investigated by corporate security personnel.

The experience of a large financial services firm provides the background to understand the impact of high security alerts on large enterprises. The financial services firm has deployed a complex, interconnected and layer security infrastructure using a combination of commercial off the shelf products and custom software that address the firm's specific threat profile. The firm records about 150 Million individual events per 24 hour day. This, in turn, results in the creation of over 700,000 security alerts that are interrogated and evaluated by the SIEM software. The SIEM creates 70 high risk alerts each day. These 70 high risk alerts need to be investigated and resolved by the firm's security personnel. Resolution of these alerts can take between 30 minutes up to five hours with an average of 1.5 hours per event. If all of the high risk alerts could be resolved at the low end of the time scale, it would take 35 hours to resolve the 70 alerts each 24 hour business day. This requires that the enterprise employ multiple security analysts to cover their 24/7/365 operation.

Analysis and resolution of high risk alerts is reactive meaning that as soon as the systems administrators and security analysts are aware of the alert they being the process of analyzing and resolving the problem. This situation is complicated by the fact that security analysts can only resolve security threats they are aware of - situations where they have a priori knowledge of the signature of the threat. At the same time, the number of false positives is also growing.

Trained cyber security analysts are in high demand and represent a significant cost to the enterprises that hire them. According to a November 2010 report by Salary.com, the median annual salary for a Web Security Administrator is $80,553. Half of all web

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

security experts have an annual salary of between $74,497 and $100,00 with 10% who earn the highest wages having salaries that exceed $117,705. In organizations requiring extensive background checks and security clearances these salaries often exceed $150,000 or more. In addition to base salaries, large enterprise benefit costs of 35% of salary are typical with overhead of 50% or more depending on the enterprise and business sector.

The financial services firm's 70 alerts require 35 hours to resolve. Using a low end salary of $49 per hour and a loaded cost of $100 per hour for each hour spent resolving alerts the table below shows that the cost to the organization are considerable.

	Low Option	Loaded Option
Hourly Salary	$49.00/hour	$100.00/hour
70 Transactions/Day 30 Minutes Each 35 Hours Per Day	$1,715/day	$3,500/day
365 Days/Year	$625,975	$1,277,500

The cost of continuous monitoring are expected to continue to rise. The growing complexity of systems and the rising cyber threat coupled with recent high visibility intrusions and the associated economic and reputational damages experienced by firms whose systems have been compromised is resulting in practices that dictate moving to more extensive and more frequent monitoring.

THE SCIT LABS CCF SOLUTIONS

CCF provides a new approach to continuous monitoring and compromised server handling support requirements of large enterprises. CCF ensures execution of defined pre-processing steps to increase the effectiveness of forensic analysis providing improved and more flexible methods for managing analysis of the compromised servers. CCF reduces costs by supporting more efficient processes resulting in considerable cost reductions. CCF changes the operating paradigm by automating current manual steps; expediting the process of taking compromised servers off-line; and facilitating a more dynamic resilient recovery faster than current cyber security manual event handling processes.

CCF can be implemented without change to existing security infrastructures including those that require conformance and compliance with FISMA, NIST, and Authority to Operate certification requirements.

CCF supports three function:
1. Continuous Monitoring based on user defined frequency;
2. Compromised Server Handling to isolate, remove, and replace compromised servers; and,

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

3. Forensic Analysis support by archiving compromised servers and executing a set of pre-defined operations suitable for forensic analysis.

CCF uses SCIT techniques to deliver the continuous monitoring, compromised server handling and enhanced forensic analysis support. CCF has two deployment options. The first is an added capability to SCIT servers. The second is a software only approach where CCF is added to the existing virtualized environment.

SCIT technology is a moving defense paradigm that allows systems to deter an attack by constantly changing the attack surface. Using virtualization, SCIT rotates pristine virtual servers and applications at a predetermined timeframe or in the case of CCF, on awareness of the existence of a compromised server. The timing of SCIT rotations can be configured at intervals that address the threat with rotations occurring as frequently as every minute if warranted by the value of the server asset. Systems are able to continue working through an attack, with automatic and rapid recovery to a clean slate. SCIT technology continuously replaces the operating system, device drivers, and applications with a new pristine server. This approach removes the residue from errors and cyber attacks without human intervention.

HOW SCIT-BASED CCF WORKS

CCF takes advantage of the SCIT architecture to support continuous monitoring. Each standard VM monitoring frequency that is set by the user at the time the VM is launched. SCIT Labs' implementation set the frequency of monitoring using the recommendations of NIST 800-37 and agile defense strategies defined in NIST 800-39. CCF supports user defined configuration of the frequency of monitoring, rules for examination of the health of the servers, deviations from compliance and definition of deviation from the pristine state of a VM.

Continuous Monitoring Workflow -- Continuous monitoring for each VM involves the following steps:

1. A frequency of monitoring is set
2. A time to monitor signal is generated when the server hits the monitoring frequency
3. Take a snapshot of the monitored VM.
   {User may choose to launch a new VM that is a pristine clone of the VM that is being monitored. CCF then stops the old VM}

4. CFF archives the differences between the monitored VM and the standard VM
5. CCF then launches a pre-processing script to compare the monitored VM to other VMs in the archive and processing the log files.
6. CCF examines the results and compares the results to the prescribed performance requirements for the VM
7. If this process detects abnormal results, CCF signals the analyst

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

8. The VM and the results of the analysis are transferred to the analyst workbench where the analyst performance forensic analysis and generates the appropriate report.

Compromised Server Workflow -- Once a compromised server is identified CFF executes the following tasks:

1. CCF takes over and automatically isolates the server
2. If CCF is authorized, it starts a replacement server.
3. Archives the compromised server and the associated logs.
4. CCF then executes a script incorporating a series of pre-processing steps to support forensic analysis. Such steps includes comparing the compromised VM to other VMs in the archive and processing the log files.

Forensic Analysis Workflow -- CCF creates the package that is used by the security analyst to resolve issues found on the compromised server.

1. The VM and the results of the analysis are transferred to the analyst workbench where the analyst performance forensic analysis and generates the appropriate report.
2. If authorized, CCF will launch a new clone of the pristine VM, and the system continues to operate with the new VM.

Replacing Manual Steps With Automated Steps -- CCF replaces manual processes with automated processes that facilitate a rapid response to security event management without analyst intervention each time an alert is received. Current protocols incorporate a variety of manual steps including:

The analyst stopping the VM
When the service is stopped, the analyst notifies the IT department
The VM is transferred to the analyst's workbench for investigation
The active VM is archived for future use
The analyst collects the information from the event manager and pre-process the VM.
These steps are estimated at taking about 30 minutes per high risk alert incident.

By automating manual steps, CCF improves analyst visibility into high risk alerts by enabling the analyst to focus on the alert rather than on the mitigation steps to remove the compromised server from the environment. This facilitates faster response time to individual events. CCF automation ensures consistent handling of alerts and compromised servers across the enterprise rather than relying on the processes manually executed by each security analyst. This dramatically reduces the time and complexity of resolving the high risk alert process by shifting the focus to investigation and resolution from the process of stopping servers and collecting evidence.

Side by Side Comparison -- The table that follows compares the CCF process with current continuous monitoring and compromised server resolution processes:

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

Processing Step	With CCF	Current
IDS or other log analysis generates an alert.	No Change	
SIEM collects the evidence and validates the alert.	No Change	
High Risk signal is sent.	To the SCIT interface.	To the analyst.
The High Risk signal is put into the analyst queue.	No queue required. VM is automatically stopped.	In queue for 2 hours or more. Night alert results in more delays. More losses.
Analyst stops the VM.	Automatic.	
Service is halted and IT department is informed.	New VM is automatically launched.	Instructions may be in queue at IT desk for 2 hours. VM is launched.
VM is transferred to the analyst workbench.	Automatic.	Analyst action required
VM is archived for later use.	Automatic.	Analyst action required
Analyst collects the info and pre-processes VM.	Automatic.	Analyst action required.
Analyst performs forensic analysis, generates report.	No Change.	15 minutes to 5 hours.

CFF BENEFITS

CFF reduces manual effort and the time needed to stop and replace a compromised server and to assemble the resources needed to analyze and resolve security alerts.

CFF supports automatically bringing the compromised server off-line and replacing it with a new pristine server. This delivers system resilience and unattended recovery more efficiently and at a lower cost.

The automated process enables organizations to implement tighter and more frequent monitoring without adding resources to handle management of compromised servers and creation of information and associated assets to enable a security analyst to investigate and resolve an alert.

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

Business processes shift from being reactive to proactive by enabling security analysis to occur when it's optimal for the organization rather than at the time the analyst becomes aware of an alert.

Significant cost savings can be achieved by automating the process of isolating compromised servers and facilitating forensic analysis. Using the loaded and low cost estimates presented above, SCIT Labs estimates that a representative enterprise can achieve savings of $600,000 to $1.3 million by implementing CCF.

ABOUT SCIT LABS

SCIT Labs designs, develops and deploys advanced cyber security products and solutions built on its patented Self Cleaning Intrusion Tolerance (SCIT) technology. The firm's principals are leading experts in cyber security, threat analysis and deterrence, agile and resilient cyber strategies and frameworks, and emerging computer architectures.

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