CS-Solutions

MANAGING CYBERSECURITY

Platinum CS Protection

PLATINUM CS PROTECTION (PCSP)

CS-Solutions, Inc
Cybersecurity
Whitepaper - 2011
Contact Info: Gabriel Raia - CEO
Phone: 760-550-1050
Email: graia@CS-SI.us

Table of Contents

Preface

Malicious cyber activity has caused hundreds of billions of dollars in lost revenue every year along with disruptive operations to critical infrastructures extending to the computing platforms. Maintaining today's mission critical infostructure (information infrastructure consisting of the computing platforms) has become center stage for industry, the Department of Defense (DoD) along with Federal agencies particularly DHS, NSA, DIA and the like. The recent formulation of Cyber Commands across federal agencies and DoD are resultant to the importance and awareness that cyber warfare is a reality and threat to our national security, economy and nation that must be addressed immediately. Today's cybersecurity model is to formulate measures to repel and protect the communications infrastructure against constant attack; this whitepaper provides the reader an approach to addressing the infostructure in a similar model.

This Cybersecurity Whitepaper is intended to provide technical and functional information regarding CS-Solutions' Platinum CS Protection™ (PCSP) solution, which provides essential components to Cybersecurity architectures not readily addressed in current approaches. The methods discussed in the whitepaper are not hypothetical, they are deployed in various stages providing immediate mission assurance capabilities now realized in Federal and DoD areas of Cybersecurity concern. More importantly, this Whitepaper will address the necessary information to adopt cybersecurity best practices and integration methodologies, to utilize when integrating the PCSP solution with currently deployed security and network point solutions within a cybersecurity infrastructure. Moreover, PCSP will provide the path to maintain the necessary information assurance (IA) accreditations, which form the foundational element to security on the computing platforms, without compromising the resources of the organization.

Cyber Infrastructure Defined:

Maintaining the communication (network) infrastructures has been the primary focus in many organizations by deploying solutions that perform network layer backups, redundancy, multi-path (satellite, LOS) and self-healing mesh capabilities. Securing communication infrastructures has matured in many aspects by providing industry, DoD and federal agencies with a number of technologies and methodologies that enable continuous communications from point A to point B in the event of network failures. As critical to maintaining these levels of redundancy for the communications platforms, the same level of importance should be given to the continuity of operations for the computing platforms, i.e., servers, VM server, desktop/laptops and mobile systems. This policy is not currently employed and yet is equally as critical. The computing platforms (information infrastructure) is a key mission assurance element to the cybersecurity architecture because without the computing platforms being operational, the packets of information, commands and/or data that are delivered via the communications infrastructure to the servers or to the end-point systems would be rendered useless if the computing platform was inoperable. It is this added layer of protection that can be gained using the Platinum CS Protection™ solution.

The PCSP Solution Adds a Level of Protection to the Cybersecurity Environment

If a contagious malware such as "Melissa" or "I Love You" crashes an operating system or one of the installed applications, it can be devastating to an enterprise or to a mission. How does an enterprise or mission recover from such an event? Could Tier 2 support be deployed in a timely manner such that there is no disruption of Operations? More than likely the operations of the mission would be disrupted for hours and in some instances for days. CS-Solutions' provides a holistic approach to protecting the computing platforms by integrating its PCSP Solution, which provides an immediate recovery capability of the computing platforms and thus maintaining 99.999% continuity of operations. This approach of integrating PCSP solution would minimize or eliminate the infostructure as a cyber weapons platform.

Architecture Considerations to Computing Platforms:

The enterprise consists of a network layer (communications infrastructure) providing communication between computing platforms. In the context of this section, we define computing platforms (infostructure) as any computer system (server or VM server, desktop, laptop, mobile device) with a Windows® Operating System, x86 platforms. In most cases, the infostructure is the entry point for cyber warfare. The essential elements below provide the focus areas to mitigate cyber warfare entry points. CS-Solutions' instantiates best practices for computing platforms and infostructure with its solution integration of Platinum CS Protection™. The elements to providing a secure and recoverable infostructure are as follows:

- Lockdown Information Assurance directives
- Maintain computing platforms baseline integrity and compliance
- Ensure computing platforms entering the enterprise are compliant
- Provide an automated, cyber situational awareness and immediate computing platform remediation capability

Information Assurance

Computing platforms that are not within Information Assurance (IA) compliance levels and standards have a higher risk to becoming the entry point for a cyber warfare attack. PCSP provides essential components to these first steps in securing the computing platforms to maintain highest levels of Information Assurance standards along with providing pristine software baselines that are locked down. The importance of maintaining strict IA controls in maintaining accredited software baselines should be a primary focus towards cybersecurity and security compliances on computing platforms for mission critical operations. CS-Solutions' PCSP software leverages its solution architecture to accomplish this capability for computing platforms on both classified and unclassified operating environments. PCSP has received numerous ATO's (Authority To Operate) and certifications to operate within these classified environments.

Below are the Department of Defense Information Assurance (DoD IA) controls that are met by using the PCSP solution:

DoDI 8500.2 IA Controls
Platinum CS Protection meets the following DoD Information Assurance Controls.

DCPA-1 *Partitioning the Application--User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.*

DCPR-1-1 *Configuration Management Process - Ensures that a configuration management (CM) plan has been developed to include detailed CM roles, test processes for the changes requested, and processes to verify and validate the effectiveness of the CM process.*

DCSS-2 *System State Changes--System initialization, shutdown and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.*

DCSS-2-1 *System State Changes – Shutdown and Initialization - Ensures that the system initialization, shutdown, and aborts are configured to verify that the system remains in a secure state.*

COB 1-3 *Technical Security Controls - Ensures that appropriate technical security controls are employed for protection of backup and restoration assets.*

CODP-2-1 *Disaster Recovery – 24 hours Verifies that a disaster plan exists to provide for the resumption of mission or business essential functions within 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)*

COTR-1-1 *Trusted recovery - Verifies that recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner, and that circumstances that can inhibit a trusted recovery are documented and that appropriate mitigating procedures have been put in place.*

ECSD-2 *Software Development Change Controls--Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.*

Baseline Integrity:

The key to Information Assurance is maintaining the software baseline integrity by ensuring that no matter the event, the computing platform can restore to its certified baseline. By incorporating the PCSP solution (Freeze Mode) into a Computing Platform's software baseline, compliance levels to software baseline image integrity is assured. Regardless of end-user rights, new software cannot be added to the existing baseline. Each time a computer is restarted, the system reverts to the certified and accredited compliant software baseline, removing newly installed programs.

Moreover, in the event malicious malware payloads install within critical OS or application system files, upon reboot, these changes, modifications and or additions will no longer exist or be functional, thus providing the ultimate pristine and true integrity compliant baseline management capability.

Network Access Control

One of the major areas of concern regarding cyber attacks is the insider threat. Enterprises today have invested millions of dollars to guard against cyber attacks coming in from the exterior of the network. A firewall will not guard against a laptop, for example, that is infected outside of the network, which then enters into the network and begins infecting the other computing platforms. To mitigate against the insider threat, CS-Solutions leverages Network Access Control (NAC). NAC capabilities integrated with the PCSP solution provide an essential capability; computing platforms entering the enterprise are guaranteed that they are within IA compliance standards and virus free. The PCSP solution provides an elegant approach to this integration. Before the computing platform enters the enterprise, the NAC issues a reboot command, which reboots the computing platform to its authorized clean compliant baseline.

PCSP (Freeze Mode) ensures that upon restart, malicious code is erased regardless of antivirus definitions or functionality. Further, it provides no path for internet-based malicious code to re-establish a connection to the computer system, because at system restart the computer is brought into a new certified and accredited compliant baseline leaving no residue of internet compromise or vulnerabilities associated with these connections (e.g., botnets, spyware, keystroke loggers, backdoors, etc.).

Cyber Situational Awareness

Maintaining and protecting the infostructure is the ability to have both cyber situational awareness and the capability to remediate or take action based on security analytics information. Today, enterprises leverage SIEM (Security Information Event Manager) solutions that provide essential enterprise security information to security administrators so to deploy enterprise corrective INFOCON policy levels congruent to particular threat levels. CS Solutions' integration of the PCSP solution with SIEM solutions provides the added ability to leverage an intelligent security automated architecture combining network security analytics with the ability to immediately remediate the computing platforms based on an event threat level without the deployment of IT personnel and with minimal disruption to the operation. If a contagious malware with destructive payloads that crash Operating Systems (OS) and/or corrupts applications has entered the enterprise and starts to propagate through a network segment, the enterprise SIEM could issue a command set to the PCSP solution residing on the computing platforms to disable the malware propagation and clean all compromised computing platforms, rendering them virus free in the time it takes to reboot the computing platform.

The underlying goals are to minimize the cyber threat on the computing platforms and to have the ability to immediately recover and remediate from a cyber event that would otherwise disrupt the continuity of operations. To maintain 99.999% mission assurance at the infostructure level, this is best accomplished by employing the PCSP solution

coupled with best practices, integrated security solutions and processes that dictate levels of redundancy and remediation.

Platinum CS Protection solution defined:

PCSP is a software-based application that operates on the Hard Disk Drive (HDD) or VM platform of the client computer, server or VM server (computing platform) with special control mechanisms that reside in the boot sector. The operating functionality and architecture of PCSP affords the IT system administrator assurances that the accredited software baseline that complies with the organization's compliance directives (e.g., DOD, FISMA, DIACAP, GLBA, SOX, HIPAA, etc.) are maintained upon the rebooting of the end-device - every time. Moreover, rebooting the system brings the computing platform to a pristine (virus free) system in the event it was targeted by a cyber attack.

The system administrator is provided the ability to systematically control and enforce the organization's application license controls; the administrator can apply and enforce Change / Configuration Management controls as it pertains to Compliance application access and software baseline management. Most important, PCSP provides IA compliance controls without the need for any additional IT support or any additional network enterprise appliances, because the computing platform does not need to be connected to the organization's network to maintain compliance directives for both enterprise and remote devices.

Benefits:

- Immediately restore computing platforms to a virus free state with a simple reboot or power reset
- Manage and guarantee a certified compliant baseline on all PCSP enabled systems
- Ability to seamlessly update compliant software baselines through existing software delivery methods in a fraction of the time (e.g., SMS, SCCM, BIGFIX)
- Ensures that the compliant baseline integrity is not compromised by an end-user loading personal applications or a malicious virus payload that reconfigures system files
- Continuity of Operations – maintain 99.999% availability to OS, applications and data
    - End user computing platforms that experience a software system error can immediately recover by simply restarting their computer.
    - Servers and VM servers – any OS application errors caused by a bad patch, virus attack and/or OS/application failure, the administrator reboots the server to backup, or pre-patch operating snapshot, using Standard Mode or just power cycles the server in Freeze mode

Modes of Operation:

PCSP can be initialized to operate in two different modes; Freeze Mode and Standard Mode. Both modes offer similar capabilities and are described in the following paragraphs. Freeze mode is the preferred method of operation because it requires no intervention form the administrator or end-user.

Freeze Mode:

Computing platforms operating in the PCSP Freeze Mode have a very low risk of corruption, or infection. At every system restart the system boots into a pristine snapshot containing the compliant application baseline and operating system files along with current data. In the background, the previously booted snapshot is entirely incrementally rewritten to include the accredited applications and OS layers. With each and every reboot, the user is presented with the approved and intended operating environment – all other changes are removed.
Furthermore, regardless of end-user rights, access to PCSP's administrative interface is restricted by a complex password created and maintained by the System Integrator (SI) or system security administrator.

For those systems attached to the network, the process of updating a baseline is done in an automated fashion using current SMS, SCCM or end-point management system on the market. The SMS system, as an example, must authenticate to validate it as an authorized system allowed to provide an update to the baseline. The update process only updates the software baseline; the end-user data is not part of that baseline. Thus if a problem exists with the update by means of an interoperability problem causing a system crash, the end-user boots to a pre-patch/ pre-updated environment with all user data intact.

For those systems not connected to the enterprise that require security updates, many hours may be spent to completely re-image a computer system every three months with security updated base loads and patches. With PCSP, this same process can be done in minutes without having to completely re-image the computer system, because only the changes to the baseline need to be applied; this process avoids the risk of sensitive data loss often associated with a complete re-image and greatly increases the ease of maintaining a DIACAP complaint software image baseline.

Standard Mode:

Computing platforms operating in the PCSP Standard Mode function very similar to those computing platforms operating in the PCSP Freeze Mode. The main difference is that when utilizing PCSP Standard Mode the end-user or administrator initiates the restoring of their computer system back to the certified compliant software baseline. In contrast, when operating in the Freeze Mode, the restoration of the snapshot occurs automatically at every system reboot.

The PCSP Standard Mode may be the best choice when end-users have a requirement to load non-certified or non-accredited software applications. The operating environment that they create can be restored upon any system restart, or it can continue to be used as long as they have a need. It is important to note that even when the environment is restored to compliant levels, the end-user's data will remain intact. This mode offers a tremendous amount of flexibility while still providing fail-safe recoverability and compliance.

Avoiding Data Loss:

A unique feature incorporated into the PCSP solution is its ability to ensure important data is not lost even when restoring the computer system to the certified and accredited complaint software baseline. This process is accomplished by preserving data files and folders within PCSP utilizing a process called Data Anchoring.

When operating PCSP in either the Freeze or Standard Mode, data contained within these anchored folders/files will be available regardless of which snapshot is being used. These anchored locations are defined by the administrator and can be configured to specific needs. In this respect, all anchored data files are made "globally available" to all snapshots. This feature enables end-users the ability to retain important data even when a computing platform experiences critical system failures and must be restored to the original baseline, and when system administrators install updated baselines, IAVAs or security patches to ensure intended compliance standards (e.g., corporate, DIACAP, DoD, etc).

Security:

PCSP offers several layers of security controls both for the end-user and the Systems Integrator. A few of the more important security features are detailed below.

Boot Security:

PCSP incorporates an option that allows a boot password to be entered prior to being granted access to the Computing platform's operating system. This password capability renders many current password technologies obsolete, because several of the common methods for bypassing system passwords require access to the operating system files which allow for an attack on local OS accounts.[i]

Unlike a Basic Input Output System (BIOS) password, or a HDD password that is enabled within the BIOS menu, the PCSP boot password cannot be compromised by a BIOS flash or a BIOS kill attack. Furthermore, a PCSP-enabled boot password does not break DoD policy regulating access to BIOS commands and functions.

Security - at the Administrative and System Level:

PCSP administrative features can only be accessed with a unique PCSP application password. This feature limits interaction with PCSP to only an approved system, SMS, SCCM, System Integrator and or system administrators. This control ensures that enabled PCSP security features, including attempts to modify the baseline, cannot be maliciously or inadvertently altered without appropriate password authentication. This feature enables ease of use for end-users, but ensures that only approved personnel or authorized systems, SMS, SCCM, are permitted to access PCSP administrative features. All changes made from the previous operating environment are logged to provide an appropriate audit trail.

[i] This password capability is useful when accessing the HHD through the system as intended, and it should be noted that this product does not replace the need for encryption. Files on the hard disk remain in the same state (encrypted or non-encrypted) as they were prior to product installation. Because of this, the access of systems files are not prevented by this product from attacks involving the mounting by another operating system.