DOP Cyber Security Service Asset

Adding speed and efficiency to the process of ensuring cyber security for a SOA infrastructure

Highlights:

- When applied to the IBM Defense Operations Platform, helps accelerate the ability to field a secure service oriented (SOA) infrastructure
- Helps reduce costs and increase the speed of getting new mission capabilities to the war fighter
- Removes known vulnerabilities and provides assistance for removing those that depend upon the user's own system environment and security policies
- Supports aerospace and defense administrators in tasks required to assure the enterprise that the system being deployed does not introduce known security risks
- Eliminates both thousands of hours of work and the need for product specialists to perform assessments and apply remediations and recommendations facilitating your cost take-out strategy

In addition to offering unprecedented advantages in defense operations, today's technologies bring interoperability and security challenges to military systems administrators and developers. Military organizations have moved beyond the concept of network-centric operations (NCO) to be focused on rapid mission onboarding. With enemies tactics evolving faster than ever, military leaders now focus on mission delivery versus networking. The ability to rapidly and securely share vital information, across the battlefield, is critical to their success. From command center to soldier, headquarters to battle group, information must be common across platforms.

Many of today's military systems operate as silos, making it difficult to achieve fully integrated end-to-end capabilities. To overcome this challenge, defense systems must come out of the box being interoperable. Technologies abound that can help resolve interoperability issues. However, it remains a complex, labor-intensive and costly process to establish and maintain a secure, reliable environment of interoperability. Furthermore, such a model can be brittle—a change in one node can break interoperability with others. The complexity and expense of customizing heterogeneous environments can greatly slow the process of getting new mission capabilities to the war fighter.

Military services need a way to dramatically accelerate the process required to field a secure mission platform — one that has been through accreditation, with cyber remediation applied during installation which removes the major known cyber vulnerabilities. remove the major known cyber vulnerabilities.

Rapid access, extended communications and reduced costs

The IBM Defense Operations Platform is a single, coherent product that incorporates support, maintenance, and ongoing development. IBM supports military IT organizations with a flexible, scalable operations environment built on significant technology and cross-industry expertise. Deploying the IBM Defense Operations Platform can help a defense department rapidly establish a control center, mobile command posts and field-level application deployments. The platform extends a shared, multichannel mission capability to all users as well as helping to reduce development and maintenance costs.

IBM has developed the platform to address NATO-specific needs for ease of installation, deployment and cyber security. The standardized technology eliminates the need to rebuild interoperability into every mission node. Because the platform supports end-to-end mission interoperability, military forces, vendors and contractors can keep their focus on mission application deployment.

DOP Cyber Security Service Asset — key to a more secure infrastructure and faster accreditation

When applied to the Defense Operations Platform foundation, the IBM Cyber Security Service Asset substantially accelerates the ability to field a secure service oriented architecture (SOA) infrastructure. The Service Asset addresses the major known vulnerabilities from the core Defense Operations Platform Command Center servers, and provides assistance in the removal of those that depend upon the user's own system environment and security policies. Once cyber remediated, the Command Center can be provided as virtual machines, with vulnerabilities already removed. Provided with these cleansed servers is documentation which identifies how each vulnerability item has been addressed in the Service Asset.

Meeting the security challenge head-on

Aerospace and defense administrators face significant challenges when required to assure the enterprise that the system being deployed does not introduce known security risks. In order to remove these security vulnerabilities and verify the system status, administrators must:

- Identify relevant vulnerabilities for each product on each server
- Apply fixes, or mitigations, to those vulnerabilities that are found on the system
- Perform regression testing for applications to verify that the fixes have not broken them
- Document the full assessment and all remediations — required for defense certification and accreditation processes
- Especially for a large system, these tasks require thousands of hours, adding significant risk to delivery schedules and profitability

Eliminating costly, complex tasks that require deep product knowledge

As an example, a web server may ship with a database which could have an existing vulnerability. Therefore the web server may have to be remediated as it is sold with a database to support the web server's configuration and run-time requirements. Even though the bundled database does not support application or user data storage needs, it still must be assessed for each potential database vulnerability. Such analysis requires deep technical knowledge of the architecture of each product on a server, its usage and its configuration options. The Cyber Security Service Asset can eliminate thousands of hours of such work and expense for users. IBM's product experts have done an extensive analysis of both end user and embedded Defense Operations Platform technology ensuring customers save thousands of hours discovering these vulnerabilities on their own.

Also, during the process of removing vulnerabilities, regression tests must be run to confirm that changes do not cause other IT infrastructure or mission applications to fail. This validation effort can greatly reduce the time required to complete the remediation effort. The Cyber Hygiene Service Asset, as delivered, has been verified for correct operation using the same calibration tools that are used to verify the installation of the Defense Operations Platform.

For defense clients, documentation of the vulnerability assessment and remediations is critical to receiving accreditation to operate on secure defense networks. For each vulnerability, an assessment of its applicability is required for each defense solution stack. If the vulnerability does not affect the solution, the reason for that decision must be documented. If the vulnerability is present, and the user repairs the problem, the remediation must be documented. Finally, if it is left open, that too must be documented, along with the reasons, and the plans for remediation or mitigation.

The Cyber Security Service asset provides this documentation for most known vulnerabilities for the Defense Operations Platform operating system, products, network configuration. System integrators presenting such documentation, to security accreditation officers, will experience greatly accelerated timelines toward certification and accreditation.

Securing the Defense Operations Platform against cyber attacks

Some of processes performed by the Cyber Hygiene Service Asset include:

- Shutdown unneeded operating system services, such as FTP, email
- Apply appropriate product maintenance so that all known product vulnerabilities have been mitigated
- Remove default user IDs
- Strengthen system passwords
- Remove sample code
- Enable sequential logging (so that log files are not overlaid)
- Establish an environment that supports "separation of concerns" — OS system administrator does not need to be the application administrator
- Ensure data and program files are on different file systems
- "Tighten" directory/file access permission's — avoid "all access" directories/files
- Turn on product auditing functions where available

Two ways to deploy

The Cyber Security Service Asset can be delivered in two ways: As a set of VMware virtual machine images that can be quickly deployed on a VMware server infrastructure; or, as an accelerator asset, which includes Cyber Hygiene remediation scripts, installation scripts and documentation for manual remediation steps.

Secure and ready for action

The IBM Cyber Security Service Asset is designed to deliver a mission platform that benefits from having previously been through an accreditation process. Experience from prior accreditation informs the remediations applied during installation to remove most known vulnerabilities. Cyber vulnerability remediation, along with documentation of the processes, accelerates the ability to field a secure mission platform—one that is ready to deliver new mission capabilities and reduce risks to the war fighter.

For more information

To learn more about the IBM Defense Operations Platform and the IBM Cyber Hygiene Service Asset, visit **ibm.com**/software/industry/defense-operations-platform/

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2011

GVS03028-USEN-00