EMBIT
Building Innovative Technical Solutions

Securing data from the inside out™

Multinational Information-Centric Security Strategy to Task (MICSS2T)

Edward Ballanco
EMB Information Technology, Inc.

Greg Sullivan
Global Velocity, Inc.

Christopher “Jake” Jacobson, PhD
Chief Technologist, IBM Systems and Technology Group, U.S. Federal

August 19, 2015

Introduction

Today's reality is that the United States will rarely, if ever, conduct unilateral military operations where the US "goes it alone" on the battlefield. Recent history has shown we will be part of a coalition of nations that varies in terms of friendship and capabilities. In the past this has forced us to accommodate the lowest common denominator in terms of military prowess as well as Command and Control technology. Further, the degree of "friendship" directly impacts our willingness to share information with coalition partners for fear of security leaks and risk of divulging advanced capabilities to future potential adversaries. Examples abound from operations in Bosnia, Serbia, Iraq, and Afghanistan. Relationships between our coalition partners also affect our ability to share information as evidenced by the multiple caveats to the releasability of information to different nations in any given theater.

These factors cause us to segregate information into different networks and systems, which serve to protect but does not support sharing of information sometimes even with ourselves. US-only systems and networks are physically separated where even the presence of foreign nationals prevent their use. Information residing on one system cannot be easily shared with other systems and information protection in the combined environment defaults to the most restrictive sharing protocols. These circumstances stand in the way of operating in a truly collaborative fashion with our coalition partners.

These challenges are recognized at all levels throughout the DoD from the Joint Chiefs of Staff, DISA, the Combatant Commands (COCOM) down to the unit level. Effectively sharing information is a critical capability as evidenced by DoD Instruction DoDI 8110.01, November 25, 2014, the Joint Chief's instructions CJCSI 6285.01C, DISA's Strategic plan that specifies information sharing with coalition partners, and the national interest realigning priorities toward the Pacific theater. All of these emphasize building an improved ability to share information with our Coalition Mission Partners in a secure cyber environment. Full participation with our Mission Partners starts with the strategic planning and this document will examine the need and our proposed solution – the Multinational, Information-Centric Security, Strategy to Task (MICSS2T) tool that facilitates coalition participation in building, executing, and assessing strategies.

Background

The planning process for major operations can be an arduous process to take the commander's guidance and intent, and transform it into the essential tasks required to accomplish the mission. Having tools to make that process easier is extremely helpful especially when they come with templates to help guide the process and automation that provides pull down selections, filters information, and creates documents. Anything that speeds the procedure and eases the drudgery of putting together the details of the plan will help in the end to keep our decision-making inside our adversary's decision loop.

Joint planning guidance addresses the need to weave a method of assessment into the planning process to objectively measure progress toward mission accomplishment. Having a tool that incorporates an assessment process whereby measures of effectiveness and measures of performance, along with a scoring mechanism and analytical rollup, is essential for this process.

Since this planning occurs in a coalition environment, we need to make these tools available to our mission partners while at the same time securing the planning environment from compromise. In some cases the risk of compromise could come in different ways. Not all our mission partners will be "friends" to the same degree and we have varied security agreements and relationships with different countries that will be on our team. In addition our partners will have their own relationships among themselves, which will complicate the sharing environment. What is needed is a fully functional, accredited information-centric security solution that allows access by credentialed users based on securely tagging of the data. This is needed today, not several years in the future.

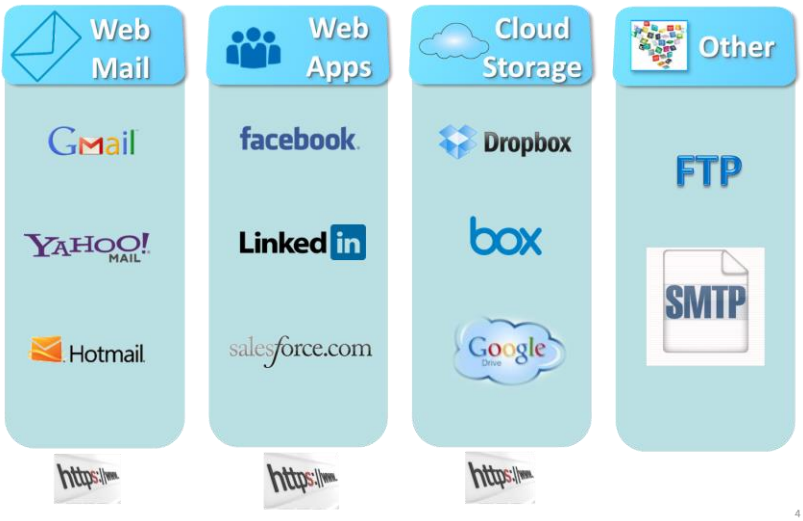
Our Solution

Our team has developed Multinational Information-Centric Security Strategy to Task (MICSS2T) on the IBM SoftLayer Federal Information Security Management Act (FISMA) secure cloud using proven Commercial Off the Shelf Technology (COTS) products. The combined capabilities of IBM's Collaborative Lifecycle Management (CLM) applications coupled with the security features of IBM's "System Z" and Global Velocity's "Securio™" provides an information-centric security solution to support almost any multinational situation. MICSS2T is scalable to meet theater level or smaller scale needs and is available immediately.

The MICSS2T foundation is IBM's System Z, a trusted and accredited cross domain solution. IBM achieved multi-level mode accreditation with this platform for the Air Force Space Command, and has retained a Common Criteria certification at Evaluation Assurance Level (EAL) 5 under the Common Criteria Evaluation and Certification Scheme. Currently IBM is working with DISA to implement a Cross Domain Information Sharing (CDIS) service using System Z to support military customers.

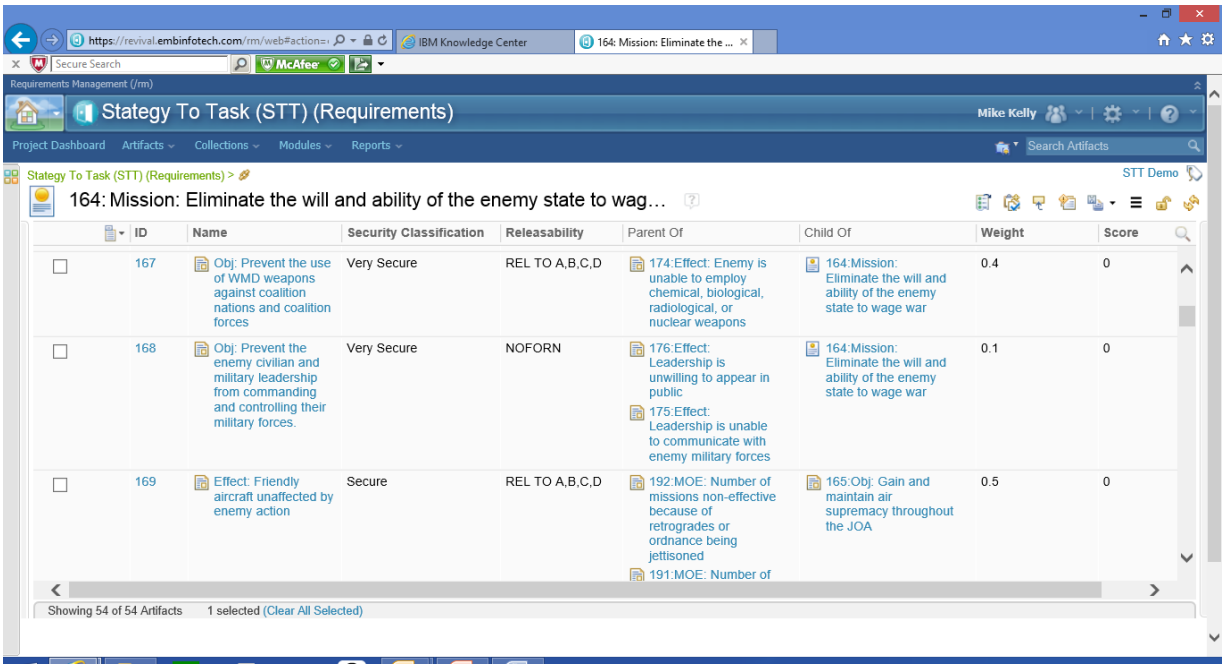
Global Velocity's Securio™ adds additional security by inspecting and scanning information content at rest and in motion. Securio™ provides information-centric security visibility and control. Key Policy components include pattern matching, customizable dictionary keywords terms and phrases, digital fingerprints and file types as shown below:

Securio™ Protect monitors and controls HTTP / HTTPS traffic of both trusted insiders and potential covert operators. Additional protected protocols include SMTP and Clear FTP. Policy actions include log, Block and Block / Notify.

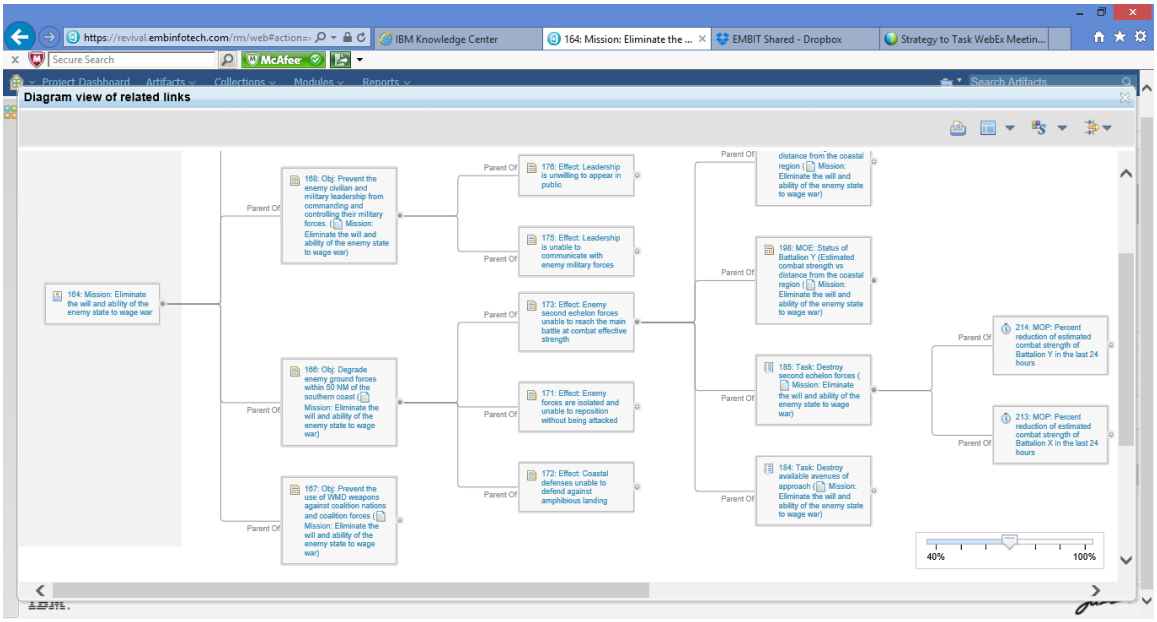


Securio™ Discover scans file shares once or continuously. Discover detects confidential information in an unauthorized location on the file share. This Securio™ feature can thus for example reveal an honest mistake by a trusted insider or a "file" staging area on a compromised server awaiting extraction.

Through our expert configuring, IBM's CLM applications create an ideal strategy to task planning capability. We leverage the ability to use templates of pre-formatted plans. The template includes links to items that are associated with each other in a parent-child relationship such as a "Mission" to "objectives" and "objectives" to "tasks", etc. The screen shot below illustrates those linkages. It also shows the security attributes that allow System Z and Securio to limit access to the data based on login credentials. The desired assessment attributes are shown under the "Weight" and "Score" headings where the measures of effectiveness and measures of performance can be evaluated and rolled up for scores on mission success that is compiled from mission reports within the database. This data structure provides a future capability to link to mission analysis tools that can assist in optimizing the plan.



The parent-child relationships allow some interesting ways of viewing the relationships between the items within the plan. The following snapshot shows a network view of the linkages that include selectable links to trace back to the actual item in the plan.



The CLM tool will also automatically produce documents that have a table of contents that can show the hierarchy of the plan along with links to the actual artifacts within the CLM tool. The excerpt below is a portion of a document produced by the CLM tool.

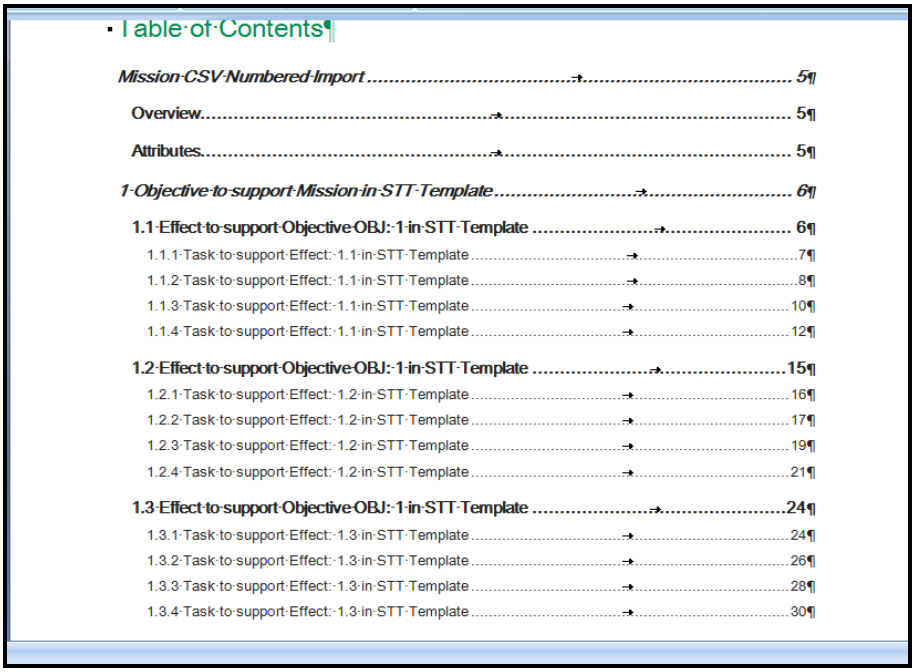


Table of Contents

Way Ahead

If you could use these capabilities, we welcome the opportunity to present a MICSS2T demonstration. Our team has the expertise and experience to help you take the necessary steps to simplify mission planning in a multinational environment and can tailor MICSS2T to your needs.

Points of Contact

Edward “Victor” Ballanco
EMB Information Technology Inc.
757-810-1751
edward.ballanco@embinfotech.com

Greg Sullivan
Global Velocity, Inc.
314-588-8555
gsullivan@globalvelocity.com

Christopher “Jake” Jacobson, PhD
IBM Systems and Technology Group, U.S. Federal
757-240-8630
christopher.jacobson@us.ibm.com