

Cyber Command and Control (Cyber – C2) Whitepaper

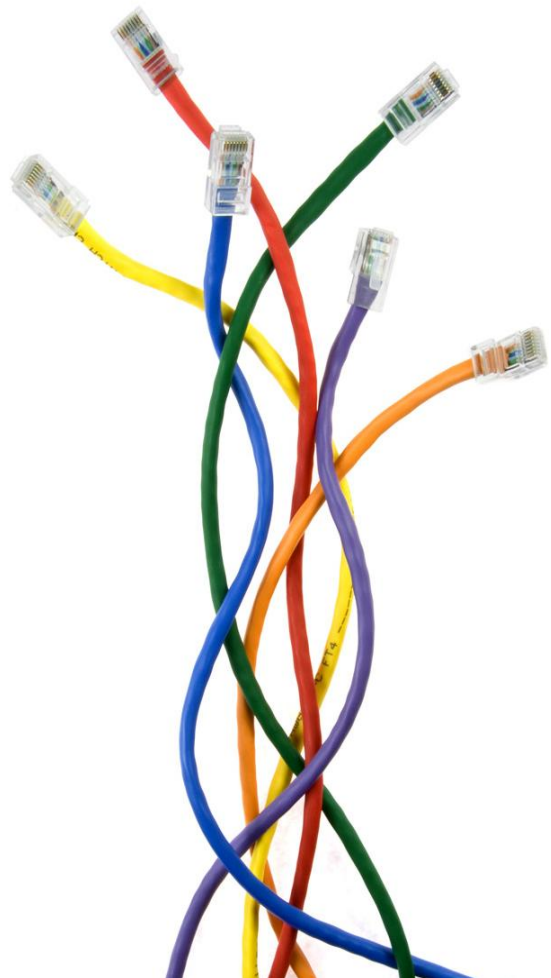


Table of Contents

- Introduction..... 2**
 - Background 2
 - The Problem 2
 - Deloitte Solution and Approach..... 3

- Cyber Security – What’s missing?..... 4**
 - Mechanisms to identify a real Cyber Attack 4
 - Monitoring at different levels using a defined Process..... 5
 - Collaboration and Trust 5
 - Cyber Security layers 5
 - Analysis and situational awareness 5
 - Social Networking Aspect 5

- Deloitte’s Cyber Command and Control (Cyber-C2) Solution..... 6**
 - Cyber Command and Control Conceptual Architecture..... 6

- Deloitte’s Technical Framework (CSADM) 9**
 - Situation Awareness Services..... 9
 - Collaborative Workflow or Business Process Management 9
 - Web 2.0 technologies such as Wikis as Knowledgebase 10
 - Instant Messaging/ Incidence specific secure chat rooms..... 10
 - Analytical Services 10
 - Data Fusion and Integration Services 10
 - Infrastructure Services 10

- Conclusion 10**

Introduction

While it is important to develop secure products to defend and protect our cyber assets, it is just as important that the cyber space that is monitored systematically and even traces of cyber threats are tracked, analyzed and shared for effective actions against them. This paper describes an approach and a solution for Cyber Collaborative Situational Awareness and decision making to government agencies and the private sector entities that can implement it not only to protect their own digital assets but to also help in identifying, collaborating with national level cyber agencies and responding to cyber threats at the highest level.

Background

The growth of cyber crime, identity thefts, and intrusions into many government networks, sophisticated social networking techniques to attack the cyber assets and wide spread vulnerabilities through the public and private networks has led President Obama to announce Cyber Security as Nation's top security priority. The report by CSIS commission on Cyber Security for the 44th presidency included 25 recommendations and highlighted the need for government to rebuild partnership with private sector to handle this mammoth problem.

The US government has taken this problem of cyber security at three different levels.

- a. National Cyber Command to monitor and protect nation's military cyber assets and if required engage in offensive cyber warfare
- b. Department of Homeland Security - National Cyber Security Division (NCSD) responsible to build an effective nationwide cyber response system
- c. Cyber law enforcement responsible for monitoring and investigations of cyber crimes, prosecute the cyber criminals and also prevent cyber crimes.

The forth element of this structure includes cyber security divisions of state and local government agencies, private sector companies etc. who are engaged in efforts to protect their own cyber assets.

The Problem

It is clear that with the wide spread nature of cyber resources of the nations, it is practically impossible for a centralized agency to monitor every single cyber threat. While partnership between public and private entities is important in developing more secure products, it is also important that Public and private sector entities collaborate and share information on critical cyber security among them and with nation's centralized cyber security organization in a trusted environment. In other words, these entities must have a cyber security infrastructure in place that will

allow them to collaborate with other entities and with our nation's centralized agency responsible for cyber security.

In a 38-page report released May 29, 2009 on the government's 60-day review of cyberspace policy, the Administration said the nation is at a "crossroads," where digital information permeates national life, but that it's also using infrastructure which is inherently insecure and vulnerable to attacks that can cause devastating disruptions.

Excerpt from President's Report on Cyber Security

The government needs to integrate competing interests to derive a holistic vision and plan to address the cyber security related issues confronting the United States. The Nation needs to develop the policies, processes, people, and technology required to mitigate cyber security-related risks.

To overcome these weaknesses, the report calls for closer cooperation and more robust *information-sharing* between itself and private industry. While the government has the responsibility to protect and defend the country against attacks, it's the private sector that builds and operates most of the systems, from computers and the software running on them to the telecommunications networks that connect them.

Sharing information related to cyber threats and vulnerabilities is one challenge. Identifying a real cyber threat is another challenge. Identifying a cyber threat from the huge amount of data in terms of security logs, network traffic is like finding a needle in the hay stack.

Each organization, whether it is a private entity, a local, state, federal or defense government agency, needs to prepare itself to participate in a large information sharing network specifically to exchange information related to cyber threats and vulnerabilities in real-time. The problem is – not many organizations are ready with infrastructure in place to exactly that or perhaps they have the infrastructure but not really integrated in a manner to participate in this information exchange this bigger problem of cyber security demands.

Deloitte Solution and Approach

This paper addresses the issues resulting from insufficient collaboration, information sharing and analysis with respect cyber incidents. Distinction of real threats to the cyber assets from sporadic hacking incidents is a big challenge. Unless these cyber incidents are gathered, visualized, analyzed, disseminated and correlated with other incidents at different levels, it is quite possible that some of the real threats may go unnoticed causing harm of enormous magnitude.

In this paper, Deloitte presents a Cyber Command and Control solution that can be implemented at many levels within the government and the private sector entities leveraging their existing investments in cyber security operations. The solution will provide standards based, open architecture framework to allow information sharing

and collaboration across multiple security operations centers (private and public) in a trusted environment.

Cyber Security – What’s missing?

For each individual organization monitoring and protecting its cyber assets, there is an additional responsibility to share the information in order to protect higher level national cyber interests.

Very rightly, many organizations have been focusing on patching every system for known vulnerabilities and monitoring the cyber activity for known patterns. The real cyber threat however, comes from unknown vulnerabilities and unknown patterns of cyber activities. In addition to the monitoring and patching activities, unfortunately, not enough attention is given to the following aspects of cyber security.

Mechanisms to identify a real Cyber Attack

With cyber attacks getting more and more sophisticated, it is not enough to simply monitor the network traffic, keep the anti-virus updated, and configure firewalls to the tightest possible security.

A random cyber attack attempt on its own may not be flagged as a real cyber threat by the security analysts monitoring it but it may really be a threat if looked at in coordination with other security incidents. These other security incidents could be taking place in a different organization monitored by a completely different set of people. Unless these incidents are correlated it may not be possible to detect a true threat. Imagine going through 360 million attempts in a year against Pentagon, i.e. 1 million attempts a day. How many analysts are required to monitor a million attempts flagged by security operations software?

For example, a port scan of other servers from a server within the same enterprise may be treated as legitimate. At the same time, information exchange with a trusted partner is also considered legitimate. It may be a spybot scanning the other servers periodically. Specific information is sent via the same secure channels to the other trusted agencies and ultimately may be leaked through the most vulnerable port using another spybot running in a completely different organization. Although this scenario is totally hypothetical, it is quite a possibility in today’s interconnected cyber world.

Cyber Attacks - Some Facts

- 360 million attempts were made against Pentagon computers last year.
- Computers in Estonia and Georgia, which have had recent conflicts with Russia, were subject to denial-of-service attacks.

Monitoring at different levels using a defined Process

Layers of monitoring capabilities are required to ensure none of the suspicious activities go unnoticed. Well defined yet flexible and dynamic processes must exist to handle unanticipated situations.

Collaboration and Trust

Currently, organizations have security operations centers (SOCs) working as silos, monitoring and resolving patterns of cyber activities without collaborating with other organizations, agencies who may have a bigger impact than just their IT systems. The Cyberspace policy review report cited above struck the same old finding of how to foster trust among participating agencies and private entities.

Cyber Security layers

The problem of cyber security exists at the company level, small and big organization, government agencies, enterprises, big enterprises and at national level. Is traditional top-down, traditional command and control organization and operational structure going to work to solve the problem of cyber security? - Probably not. So how does one approach to solve this problem and even extend and scale to the national level? In addition to monitoring the threats and patching the vulnerabilities one requires a completely distributed, collaborative cyber situational framework to get a clear view of the Cyber situation at any level at any point in time.

Analysis and situational awareness

Metrics such as number of cyber attempts in a year are important to collect to assess the overall security situation (via cyber dashboards, intelligent after the fact analysis using historical information). However, due to the nature cyber attacks where a potent cyber attack can produce enormous harm to an Organization's will, business, nation's economy, infrastructure that it is important to have a real-time situational awareness and analysis of the cyber incidents as they are taking place.

Social Networking Aspect

Cyber attackers consider themselves the smartest people in the cyber world and typically like to boast their achievement and want to be ahead of the major technology companies spending millions of dollars in making their hardware and software more secure. Computer Network Exploitation social networking groups are on the rise where these people share information, though not necessarily revealing their identity. However, intelligence gathering and analysis through these and various other hacker forums can provide meaningful information ahead of time to protect the cyber assets from potential cyber attacks. There have been cases where such analyses have led to the capture of the attackers.

Deloitte's Cyber Command and Control (Cyber-C2) Solution

Deloitte addresses all of the above facets of the Cyber Security problem in its Cyber-C2 solution. It includes -

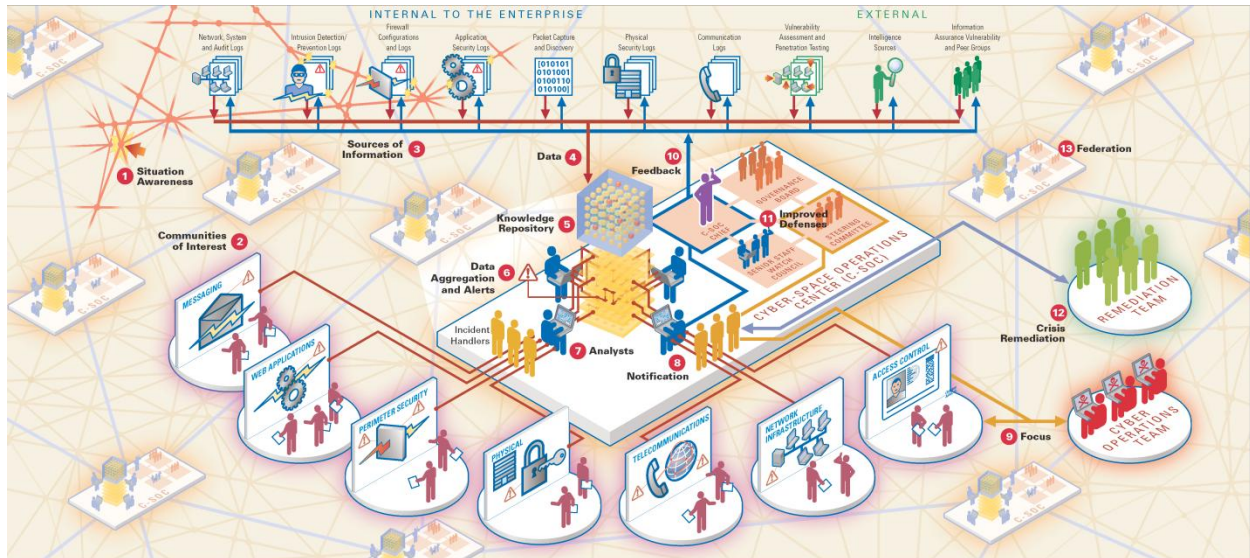
- a) Strategy for collecting, analyzing and collaborating on cyber incidents,
- b) Implementation of an already established technology framework
- c) Implement the strategy using a well defined Cyber Security methodology.

This paper focuses on the technical framework of the solution.

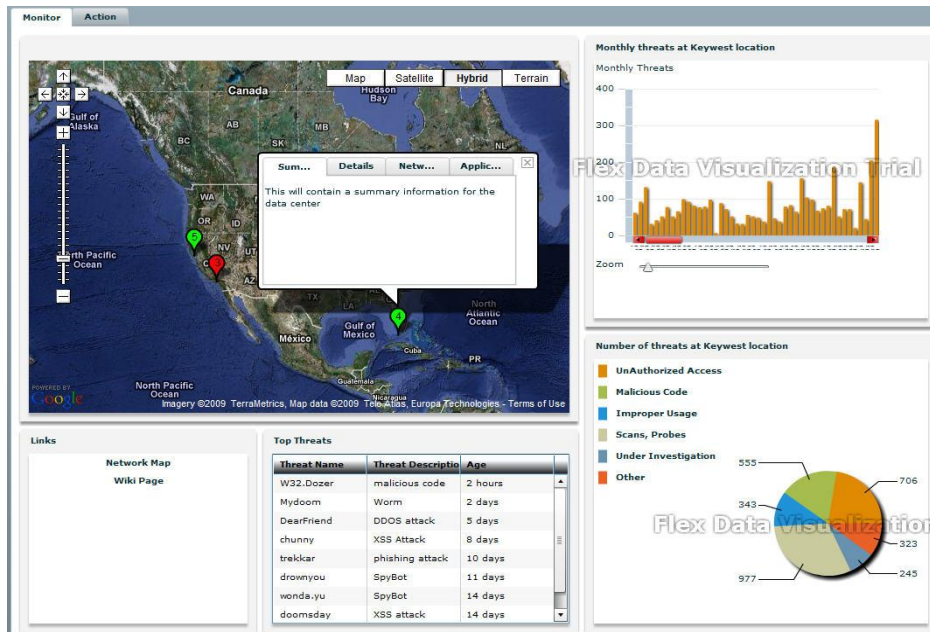
Cyber-C2 Conceptual Architecture

The following diagram shows the federated concept of our Cyber Command and Control (Cyber-C2) solution

At the center of this diagram is the Security Operations Center (SOC). The SOC collects information from firewalls, intrusion detection devices, network appliances and a host of other network sentinels, normalizes it and uses it to construct a common operating picture (COP) of the cyberspace in relation to the data centers it is monitoring. Industry leading security operations software products and incident collection products are typically used to maintain a state of continuous situational awareness by processing millions of events in real time. Geographic and network map views provide visualization of the cyberspace. Deloitte's Cyber-C2 solution adds a Collaborative Situational Awareness and Decision Making (CSADM) framework on top of the existing SOC infrastructure to provide the missing elements of Cyber security solution described above. Deloitte's CSADM framework (described later in the section) provides different means of collaboration, streamlined processes, analysis and integration of Cyber data, all within the context of a given Cyber threat. Each SOC can collaborate with other such SOCs within the enterprise or even outside the enterprise in a trusted environment using Federated Identity Management and Cross Domain Information Sharing components of the solution.



The SOC analyst recognizes anomalies in Cyber activity and generates an alert for the senior security analysts, SOC chief and other stakeholders. Stakeholders outside of the SOC, overseeing the overall operation of multiple SOCs monitor a higher level Cyber Situational View as shown in the following diagram below.



This high level Cyber dashboard provides information related to the affected SOC or data center on a geo-spatial display. Zooming into or clicking on any of the affected SOCs provide a network map of the cyber assets monitored by the SOC. One can further drill down to get information about impacted servers, applications etc.

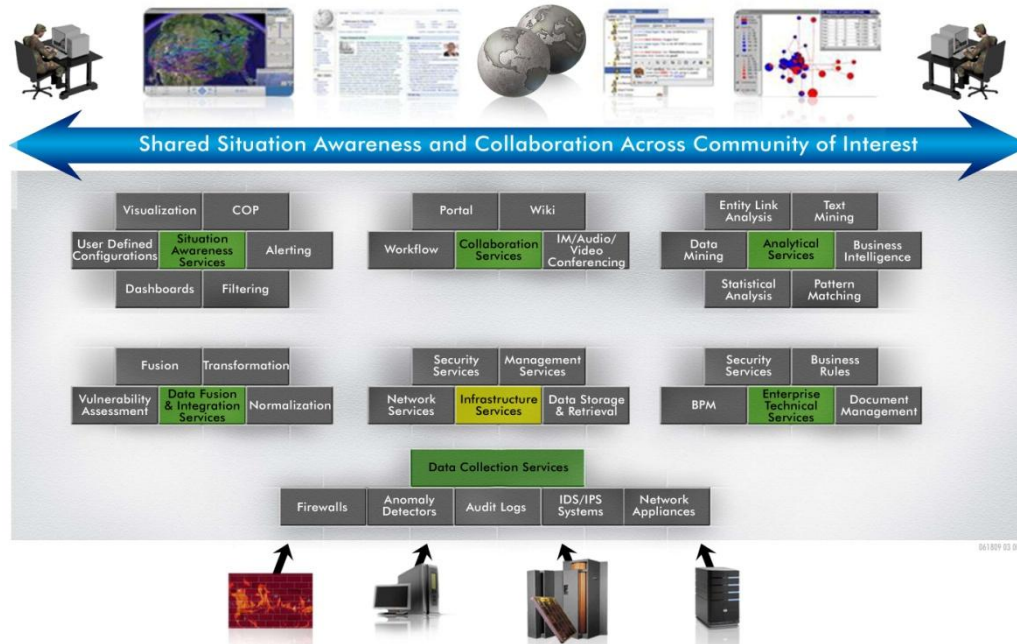
The integrated CSADM platform automatically creates a Wiki page for the identified threat as soon as the alert is generated. The Wiki page acts as a shared knowledgebase for recording and sharing information related to the cyber threat. Automatic search through wiki also identifies any related incidents similar to this event. At the same time, an intelligent and automated routing takes place through a well defined business process to route this incidence to appropriate experts by creating tasks for them, notifying them via email, voicemail or text message depending on the severity of the event. Skills based routing can also be achieved using the information captured related to the Cyber incidence. The process preserves the context of the incident throughout all the notifications, tasks and Wiki pages.

The different communities of interests such as the incident handlers, Cyber operations team, the remediation team, the system administrators, the application owners, the SOC chiefs and governance councils all participate at different times through the incident handling process. These users collaborate using many different collaboration channels (For example, secure chat, and email and portal tasks). The integrated CSADM environment pulls all the information exchanges onto the Wiki pages so as to create a true shared knowledgebase of the incident.

Cyber-C2 is not just about capturing the cyber incidence data and acting upon it. Today's cyber threats can originate from terrorist cells, state sponsored hacker units, coordinated attacks from multiple hackers. Entity Link Analysis of information from Open Source Intelligence (OSI) related to such incidents, their signatures of cyber threats, known vulnerabilities databases such as the NVD (National Vulnerabilities Database), Information exchanges on hacker forums, information related to known hackers etc can lead to some serious discoveries of potential links between two or many threats occurring at the same time. This provides additional information, which in some cases distinguishes individual hacker attacks vs. coordinated cyber attacks. As courses of actions are developed, a constant context aware collaboration keeps the stakeholders and users with area of responsibility informed of the actionable tasks they need to carry out. As different experts provide inputs using their perspectives, the decision makers have valuable information to make accurate and informed decisions. The decision may spawn multiple sub-actions related to different threats based on the link analysis and how different threats may be related. Users receive these sub-actions as workflow tasks, through email notifications and collaborate again via Chat, discussion forums, audio/video conferences, email, Wikis etc.

The following section briefly describes Deloitte's CSADM framework.

Deloitte's Technical Framework (CSADM)



CSADM is based on strong architectural foundation using Deloitte's SOA Framework. It is developed using proven, production tested, standards based COTS components as opposed to custom developed components. Many of the components are already in use in many of the DoD and Federal agencies. Web 2.0 technologies such as Wikis, Social Networking, Bookmarking and Chats provide new ways of Net Centric, Web enabled collaboration. CSADM also provides context sensitive analysis of the situation for better and informed decision making. All of these capabilities are integrated in CSADM within a context of a situation or an event. The architecture contains the following set of services.

Situation Awareness Services

The Situation Awareness Services include the graphical visualization of a situation and of objects and events surrounding the situation, using dashboards or by integrating with geospatial information where required. Real time visualization of information has been a significant challenge and recent advances in technology permit us to combine this capability along with analysis, alerting, and anomaly detection.

Collaborative Workflow or Business Process Management

Guided processes through automation can certainly improve the coordination required among security personnel from different organizations. At the core of the CSADM solution is a Business Process Management (BPM) engine that choreographs and coordinates the actions that human users need to perform in order to achieve the mission goals in efficient manner.

Web 2.0 technologies such as Wikis as Knowledgebase

CSADM uses Wiki as a shared knowledgebase where information can be shared freely by users yet controlled by access controls on who can edit, view certain information. Wikis provide the flexibility to users on how they would like to organize the information as opposed to the traditional content management tools. Although Wikis aren't replacement for the traditional content management tools, they are excellent platform for collaboration without any delay. Wiki facilitates communication and augments the business process flows for ad-hoc collaboration.

Instant Messaging/ Incidence specific secure chat rooms

Instant Messaging integrated with portals and BPM along with a context services described below provides meaningful "context aware" chats that can help prevent human errors due to information sharing without a meaningful context.

Analytical Services

Integrated analysis of enormous amount of information, both structured and unstructured is important to key decision makers. While situation awareness and collaboration when combined provide a strong foundation for mission effectiveness, analytical tools add another valuable dimension to problem solving and decision making. As more and more information is made available to the end users and decision makers, it becomes time consuming to wade through it to make sense and its applicability to the situation at hand. By providing a suite of well integrated analytical tools, the quality of decisions improves significantly.

Data Fusion and Integration Services

Data Fusion is a vast topic and can range from combining information from multiple sources to achieving inference by linking the new information thus available.

Infrastructure Services

CSADM is built on SOA Foundation and therefore fits right into any existing SOA infrastructure.

Conclusion

Employing secure software and hardware products, monitoring the cyber traffic and patching the vulnerable assets are some of the necessary actions to secure the cyber assets. Despite these, the impact of a single cyber threat can be devastating and therefore a quicker detection, if possible prevention of potential cyber threat, quicker action to minimize the impact is required. Information and analysis on the cyber threat therefore must be available at the finger tips of the decision makers. It is only possible through collaboration across multiple stakeholders, federated SOCs and with other public/private sector organizations, along with a precise situational awareness view on cyber threats. Deloitte offers a comprehensive strategy, a scalable and extensible Cyber-C2 solution framework and the methodology required for a complete Cyber Security solution for any organization.