Message

From: Chao, Henry (CMS/OIS) NotResp
Sent: 9/22/2013 5:36:38 PM
To: Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp; Lyles, Darrin V. (CMS/OIS) NotResp NotResp
CC: Outerbridge, Monique (CMS/OIS) NotResp NotResp Grothe, Kirk A. (CMS/OIS) NotResp NotResp
Subject: Re: SCA Finding Analysis

So using the BDC or an EDC to illustrate an analogous situation of which I am certain there are historical precedences even just in the tenure of Teresa, combining what the XOSC found with the final SCA would be similar to saying that current high open findings anywhere in a data center would translated as a lack of confidence in any one system that is in that data center. To take it a step further that means we should apply the 17 findings to CALT, MIDAS, Hub, zONE, HIOS, EIDM, and Healthcare.gov.

Or am I mixing things up?

I want you to go find me similar situation where we would apply the 17 findings from a global test to a single ATO for a single system. For example CMSNet high findings, BDC high findings,any of the VDCs or any other data center High Findings that then is applied to each systems ATO evaluation.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244
301-492-4100 (Pri)
410-786-1800 (Alt)
(b)(6) (BB)

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Sunday, September 22, 2013 01:16 PM
To: Chao, Henry (CMS/OIS); Lyles, Darrin V. (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: RE: SCA Finding Analysis

Henry,

Cheryl's response shows the feedback to the MITRE/Blue Canopy test that occurred during the week.

What Monica has been given is the list of findings that have been compiled and provided each night over the past five weeks to the test team. The findings come from the testing by the XOC security team. They are all contained in the Sat 12:56 PM file that I sent over to you. These findings are not part of the SCA report, but Teresa is factoring these in as independent testing upon which she is making her decision to recommend that an ATO not be authorized. I had no idea

until Friday that she was going to take this stance. I talked with Monica and Eric on Thursday before I left Herndon and Eric was going to have an updated stats on all the high items. To help expedite things, I am planning to have Adam Willard report on Monday to Herndon to work with Eric to confirm the status of each of these.

Does that help clarify? If not I can call you.

Tom

From: Chao, Henry (CMS/OIS)
Sent: Saturday, September 21, 2013 6:25 PM
To: Schankweiler, Thomas W. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: Re: SCA Finding Analysis

Tom,

To answer your earlier email Cheryl's response is based on you asking me to follow up with Monica on the 17 high findings the XOSC has on the books and you made it sound like they will be part of the report.

So give me the full story. What are we actually signing off on and what finding are indicated by whom. Seems confusing that the recent FFM SCA and accompanying report can have input from other security testing sources?

Bottom line is on Monday Marilyn and Michelle want the clean and simple explanation--what is the risk we are assuming--facts, not what someone feels.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244
301-492-4100 (Pri)
410-786-1800 (Alt)
(b)(6) (BB)

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Saturday, September 21, 2013 05:59 PM
To: Chao, Henry (CMS/OIS); Lyles, Darrin V. (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: RE: SCA Finding Analysis

Henry,

This matches what I would expect from the SCA audit. However, this is not the response to the High items though. I have arranged for Adam Willard of FGS to come to Herndon on Monday and Tuesday to work with Eric (CGI) about reviewing and closing out the items from his list. I have to be in Baltimore for some security meeting with Tony and George. When I get done there I'll head to Herndon for the evening.

Darrin is working with the SCA team on Monday for the Adobe Live Cycle (Digi-Docs) review.

I have a request in to Teresa to have Kevinand a guy named Jason Patterson to come up to Baltimore on Tue/Wed to sit with someone on her POAM team to work through and close out as many findings as possible. Part of the challenge is getting everything documented just-so in the CFACTS system so it will be acceptably closed. Hopefully a side by session will result in a 35-40% reduction in overall findings which are actually resolved, but still need to pass the CFACTS POAM audit process.

Finally, Kirk and I had a discussion with Teresa on Friday, and after Oct 1, we are going to sit down collectively with OAGM to find out how to mod the Blue Canopy contract so that we can get a dedicated test team for the next year to work in line on FFM and DSH testing. The constraints of having to test within a rigid timreframe and with limited scopes has been a barrier for getting testers to support the ad-hoc nature of the build process we have been and will continue to operate in. Folks have worked hard to be flexible but to stay within the contract boundaries. The best thing we can do is address the restrictions around the barrier so that we have the freedom to perform more ad-hoc testing on demand.

In regards to tools, we will continue to work with Peter, and Mark Orlando and I will be there to talk about the tools. I am not sure we have much in the way of overlap, like Splunk and Akamai, the tool and service can support bother operations and security. Splunk has logs being fed to it which are not duplicative of other logs being captured elsewhere. Hope to explain more of that approach later this week.

Thanks,

Tom

From: Chao, Henry (CMS/OIS)
Sent: Saturday, September 21, 2013 5:02 PM
To: Campbell, Cheryl (CGI Federal); Schankweiler, Thomas W. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)
Cc: Ramamoorthy, Balaji Manikandan (CGI Federal); Martin, Rich (CGI Federal); Outerbridge, Monique (CMS/OIS)
Subject: RE: SCA Finding Analysis
Importance: High

Tom,

Does this match what you were expecting?

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services

Centers for Medicare & Medicaid Services
410-786-1800

From: Campbell, Cheryl (CGI Federal) [mailto:Cheryl.Campbell@cgifederal.com]
Sent: Saturday, September 21, 2013 4:51 PM
To: Chao, Henry (CMS/OIS)
Cc: Ramamoorthy, Balaji Manikandan (CGI Federal); Martin, Rich (CGI Federal)
Subject: FW: SCA Finding Analysis

Henry,

As per our discussion earlier today, Balaji has provided an update on the 2 High and 17 Moderate findings identified and CGI's mitigation/action.

As part of the latest round of Mitre and Blue Canopy SCA Testing that was completed on Friday, September 20th, there were a total of 2 High and 17 Moderate findings identified. These finding can be grouped into 5 different categories:

Category	High	Moderate
Access Control	1	5
Session Management	1	
Documentation		3
Contingency & Planning		1
System and Communication Protection		6
System and Information Integrity		2
Total Findings	**2**	**17**

An initial analysis is attached with tentative target dates. As part of our initial review and planning, four of the findings have already been closed (2 high / 3 moderate) and two others are pending a review by Mitre. Of the remaining, there are seven moderate findings that are still outstanding and we have developed a tentative plan as to when these findings will be addressed. However, there are five moderate findings that cannot be closed due to limitations based upon CMS requirements or the way in which the system has been architected. These findings will need to be reviewed with CMS to determine the risk threshold and next steps. The table below summarizes the status of 2 High and 17 Moderate Findings

Status	High	Moderate
Closed	2	3
Outstanding		7
Pending		2
Limitation		5
Total Findings	**2**	**17**

Attached is the SCA Testing Report Summary with detailed information on each finding.

Balaji is here today in Herndon and is prepared to discuss at your convenience.

Let him know if you want to meet today.

Cheryl