Information Technology | Criminal Investigation (CI) Cybersecurity

Cybersecurity Dashboard on a Shoestring Budget

May 16, 2017

Metrics Quote

"Most consumers don't have a good metric for deciding on whether the dictionary they want to use is a good one... so they flip the book over, then go to the back, and it says, 'Over 250,000 entries.' And they go, 'Great, this dictionary must be awesome!'"

—Erin McKean

Briefing Agenda

- What is the CI Cybersecurity Dashboard?
- Data is key, tools are just tools
- Requirements development & stakeholder participation is a must
- Great program management is the glue

What is the CI Cybersecurity Dashboard: *Purpose*

- The CI Cybersecurity Dashboard was developed to display the status of Criminal Investigation's (CI) Cybersecurity FISMA reports, continuous monitoring, Risk Based Decision (RBD), and Plan Of Action & Milestones (POA&M) efforts in one snapshot at the lowest cost possible.

- The dashboard was designed to educate and provide CI leadership, the CI Technical Operations Center (TOC) and Program/Project Managers a high-level view of their Cyber risk areas in one snapshot.

- It provides management with guided, educated mitigation decisions based on the dashboard snapshot before Continuous Diagnostics & Mitigation (CDM) was operational.

What is the CI Cybersecurity Dashboard: *Source*

The source data of the dashboard will originate from the output of several cyber monitoring tools.

- The addition of new out files into data repository in SharePoint Intranet will trigger an event that will invoke Extract Transform & Load (ETL) packages in SQL Server
- The data will be extracted from the source output files and transported to respective tables in SQL. SQL Report Builder will transform the data in tables to organized visualization using charts and graphs
- The dashboard will use charts and graphs built from the SQL Report Builder tool and implemented using SharePoint Performance Point.
- The dashboard is a 50% customized application based on data driven custom charts and components of Performance Point.

What is the CI Cybersecurity Dashboard: *Charts*

- **Tripwire (Vulnerabilities Compliance)**

  SharePoint will display in two charts—the average number of vulnerabilities by host and per count

- **SCAP (Workstation Compliance)**

  SharePoint will display in two charts—the total number of workstation compliance

- **Windows Policy Checker (Server Compliance)**

  SharePoint will display from WPC data—a percentage passing score based on the server devices listed contained in monthly reporting

- **HPNA (Network Device Compliance)**

  SharePoint will display in two charts—the percentage passing score on routers and switches

What is the CI Cybersecurity Dashboard: *Charts*

- **Guardium (Data Base Compliance)**

  SharePoint will display from Guardium data—a percentage passing score based on previously selected categories.

- **Plan of Action & Milestones (POA&M)'s**

  SharePoint will display in 2 charts—the total number of open, closed, and overage POA&Ms, for each month for 5 years.

- **Archer (Incident Response)**

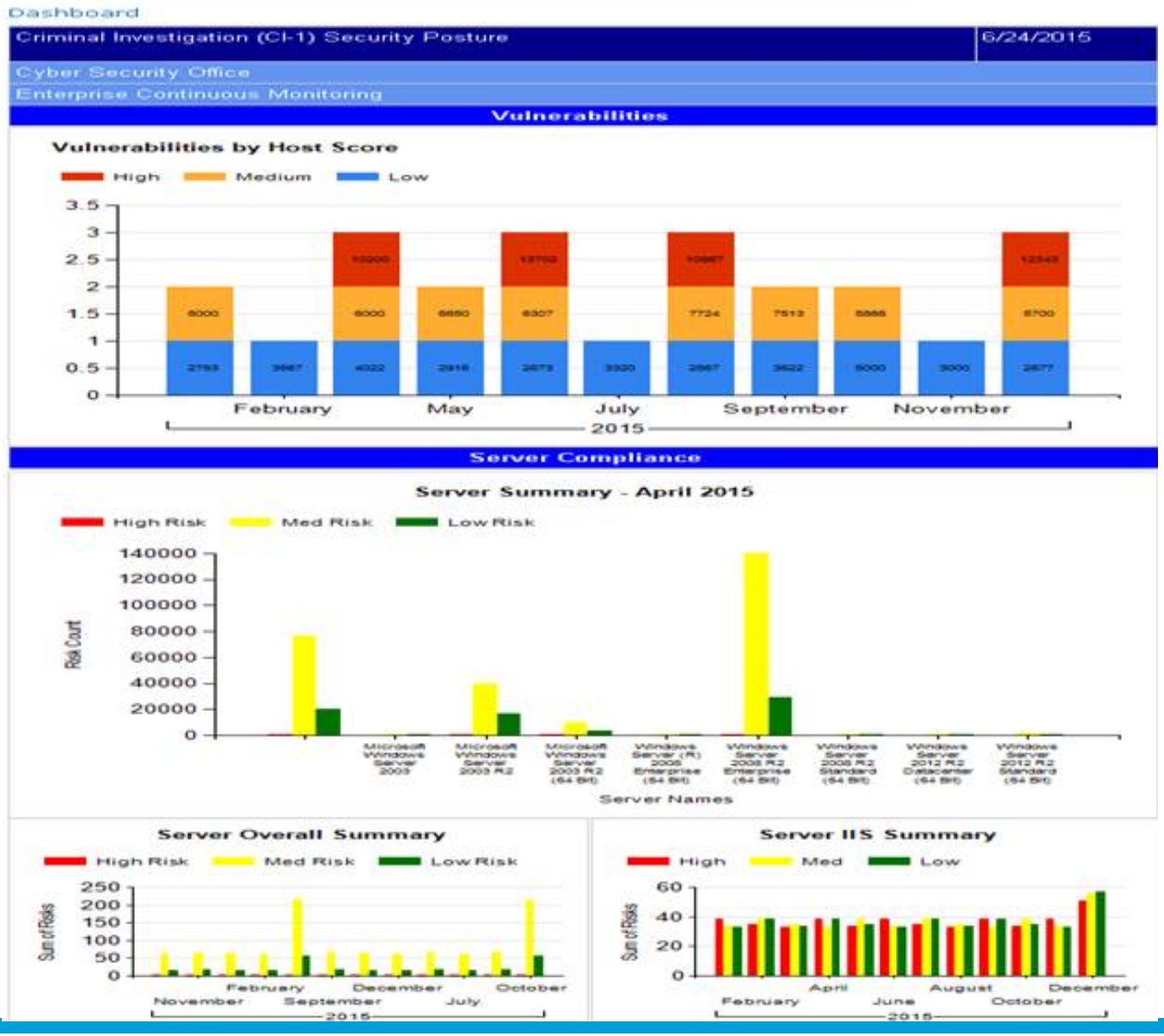
  SharePoint will display Archer data—SharePoint will open an Archer .csv file and manipulate the .csv file to display graphically CI incidents for the year.

What is the CI Cybersecurity Dashboard: *Files for Upload*

Files for certain tools **must** follow certain naming and formatting conventions. Below are file format references:

- *Archer - .csv*
- *Guardium - .xls*
- *HPNA - .xlsx*
- *POAM - .csv*
- *SCAP - .xls*
- *Tripwire - .csv*
- *WPC - .xlsx*

What is the CI Cybersecurity Dashboard: *Picture*



What is the CI Cybersecurity Dashboard: *Results*

- Finished product met requirements
- Project finished 9 months before schedule
- Project finished significantly under budget
- Currently the status of the dashboard is red or on hold due to lack of O&M funding

Data is Key, *tools are just tools*

Vision

Simplify management decision making

- →Understanding & involvement
- →Quick decisions
- →Support

Metrics to support the vision

- Never focus on a tool

Funding

- Development
- O&M

Requirements Development & Stakeholder Participation: *Requirements*

Requirements

- **Traceability**
  - Requirements, Design, & Test – Science
  - Non ELC Security deliverables & SSP - Art
- **Base lining**
- **Change Management**
- **Test must be based on the requirements**
- **Deliverables must be delivered**

Requirements Development & Stakeholder Participation: *Traceability*

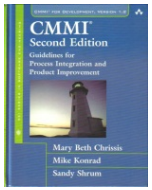
A relationship between two items

"A traceability relationship reflects the source, derivation, dependency, or other relationship between two traceability items"

BSR → DSR → STP ~ SSP

Requirements Repository Management Guide, Version 1.0

"A discernable association among two or more logical entities such as requirements, system elements, verifications, or tasks"



Capability Maturity Model Integration (CMMI) for Development, Version 1.2

Requirements Development & Stakeholder Participation: *Base lining*

Number	Req #	Requirement	Ability to export to .csv
1.	R-01	Control Impact Chart for GSS-1 and GSS-2	Derived
2.	R-02	Application vulnerability score per each tool	Derived
3.	R-03	RBD – manual	Yes
4.	R-04	POAM – manual	Yes
5.	R-05	Project Milestones – Manual	No
6.	R-06	Archer Metrics	Not Used

Requirements Development & Stakeholder Participation: *Base lining*

Number	Req #	Requirement	Ability to export to .csv
7.	R-07	Tripwire Metrics	Yes
8.	R-08	Guardium Metrics	Yes
9.	R-09	Windows Policy Checker (WPC)	Yes
10.	R-10	Unix Policy Checker (UPC)	Yes
11.	R-11	Hewlett Packard Network Automation (HPNA)	Yes
12.	R-12	Application Scanner (Appscan)	Not Used
13.	R-13	Web Scanner (Webscan)	Not Used
14.	R-14	Airwatch	Not Used

Requirements Development & Stakeholder Participation: *Change Management*

1) Tripwire
2) Network Patch Status
3) WPC
4) UPC
5) SCAP
6) SCCM
7) Guardium
8) AirWatch
9) RBDs
10) POA&Ms
11) Control Impact Chart
12) Application Vulnerability Chart
13) Web Scan
14) App Scan
15) HPNA
16) Archer

Requirements Development & Stakeholder Participation: *Deliverables Must be Delivered*

CI Dashboard – User Guide

Internal Revenue Service Criminal Investigation

THIS GUIDE IS INTENDED FOR USERS WHO HAVE ACCESS TO THE CI DASHBOARD.

Good Program Management

Program Management

- Roles & Responsibilities
- Dashboard Development
  - Set rhythm
- Stakeholder involvement
- Shared Engineering and Design
- Software Development
- SharePoint PM
- Metric Development Teams OT&E
- Lessons Learned

Roles & Responsibilities

SharePoint Business System Development (BSD)

- Robert Warren — CI – Project Manager, BSD
- Terry Lee — CI – IT Specialist, BSD
- Tim Whittle — CI – MS SharePoint Administrator, TOC

Roles & Responsibilities

Booze Allen Hamilton (BAH) Developers

• Anureet Singh	BAH – Project Manager
• Myo Sithu	BAH – Development Manager
• Mayura Solow	BAH – Developer
• Michael Wu	BAH – Developer
• Tina Arista	BAH – Functional Manager
• Michael Daly	BAH – Test Manager
• Justin Watanabe	BAH – Functional Analyst

Roles & Responsibilities

CI-Cybersecurity User Stakeholders

• Brett Manning	CI - Director Cybersecurity
• Kevin Colin	IT/C – Supervisory IT Specialist, Cybersecurity Security Engineer
• Janine Heard	IT/C – IT Security Specialist, Cybersecurity Dashboard Program Manager, RBD & POAM SME
• Paul Husman	IT/C – IT Security Specialist, Cybersecurity HPNA SME
• Samuel Buhlig	IT/C – IT Security Specialist, Cybersecurity Incidence Response SME
• Randy Christoffersen	IT/C – IT Security Specialist, Cybersecurity Tripwire SME

Questions/Comments