DRIVING CYBER CAPABILITIES THROUGH RSA ARCHER

on the Department of Homeland Security's Continuous Diagnostics And Mitigation (CDM) Program

Presented By Matt House
Director, Cybersecurity Services
January 24, 2017

INFORELIANCE

AGENDA

1. What is Continuous Diagnostics & Mitigation
2. RSA Archer as the Platform
3. Unique Challenges…
4. … and Unique Solutions
5. What's Next for CDM?

+

RSA

+

IR

INFORELIANCE

SECTION
01

What is

CONTINUOUS DIAGNOSTICS & MITIGATION?

A quick primer

CDM GOALS, OBJECTIVES, AND PHASES

- Provide Executive Branch leaders with a standardized way to identify, score, prioritize, and report on cyber performance

- Promote a common understanding of organizational risk to support
  - Prioritization of risks
  - Effective risk-based decision making, per the risk management framework

- Enable local operators to address cyber hygiene more effectively using a “worst problems first” approach

- Capabilities will be implemented in (roughly) three phases
  - Phase 1: What’s on my network?
  - Phase 2: Who’s on my network?
  - Phase 3: What’s happening on my network?

MOTIVATION

Other than the obvious

- OMB* Identified cybersecurity as a Cross Agency Priority (CAP)
- Current cybersecurity posture varies widely across the Federal Government
- Need a clear understanding of organizational risk to support
  - Prioritization of risks
  - Effective risk-based decision making, per the risk management framework
- Need a standardized way to identify, score, prioritize, and report on risks at a Federal level

** OMB M-14-03, "Enhancing the Security of Federal Information and Information Systems",*
OMB M-15-01, "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices"

SECTION
02

RSA ARCHER AS THE PLATFORM

Why was Archer the right choice?

HOW WAS ARCHER SELECTED?

Exploring the Alternatives

- Initially, DHS expected the dashboard to be a custom solution
  - Based upon earlier market research
  - InfoReliance conducted an alternatives analysis to survey the marketplace and evaluate potential solutions
- We examined functionality across five areas, which directly aligned to DHS's requirements
  - Analysis Engine, Extract/Transform/Load (ETL), Presentation and Reporting, Data Repository, Task Orchestration
- Solutions were measure to determine which could meet requirements with lowest level of effort and risk along a spectrum:

Out of the Box (OOTB)  **Complex Customization**

- RSA Archer offered several significant advantages over other COTS products and a custom approach
- Flexible architecture, data model, and straightforward technology stack

WHAT IS THE DASHBOARD?

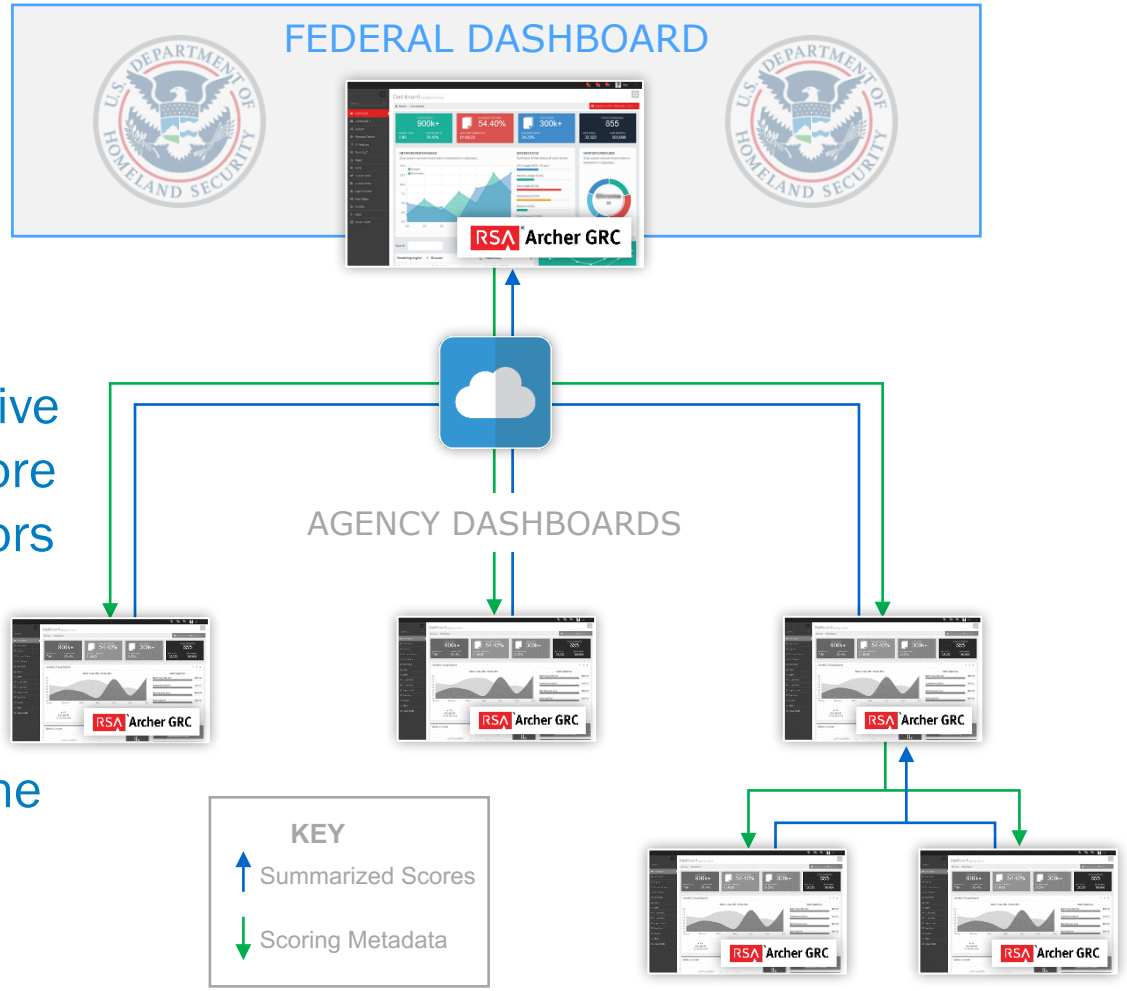
- Two flavors of Dashboard
  - Agency Dashboard
    - Captures data locally from network sensors
    - Scores data and shows “worst problems first” for operators
  - Federal Dashboard
    - Aggregates scores from Agency Dashboards
    - Provides command & control that supports centralized governance

- Modules included
  - Enterprise Management
  - Continuous Monitoring
  - Assessment & Authorization
  - On-Demand Applications

CONCEPT OF OPERATIONS

How does it come together?

- Federal Dashboard passes metadata, configuration data, and scoring parameters down to subscribing instances
- Agency Dashboards deployed locally and receive this data and use it to score data collected from sensors
- Agency Dashboards summarize scores and report those back up to the Federal Dashboard



SECTION
03

We’re facing some

UNIQUE CHALLENGES...

Some are familiar, some are new

CDM PRESENTS SOME UNIQUE CHALLENGES

Dashboarding is ***hard!***

- Scale
  - This will be the ***largest*** federated Archer implementation ever
  - Approximately 150 instances of the Agency Dashboard to be deployed
  - Multi-tiered architecture with Agency Dashboards reporting to other Agency Dashboard
- Federation/Distribution
  - Dashboards will live on networks maintained by local staff, yet they need to federate with at least the Federal Dashboard
  - Local concerns are not necessary the same as enterprise ones
- Summarization
  - Detailed data collected within an Agency Dashboard must be summarized before transmission to the Federal Dashboard
- Governance
  - How do you keep all of the cats herded?

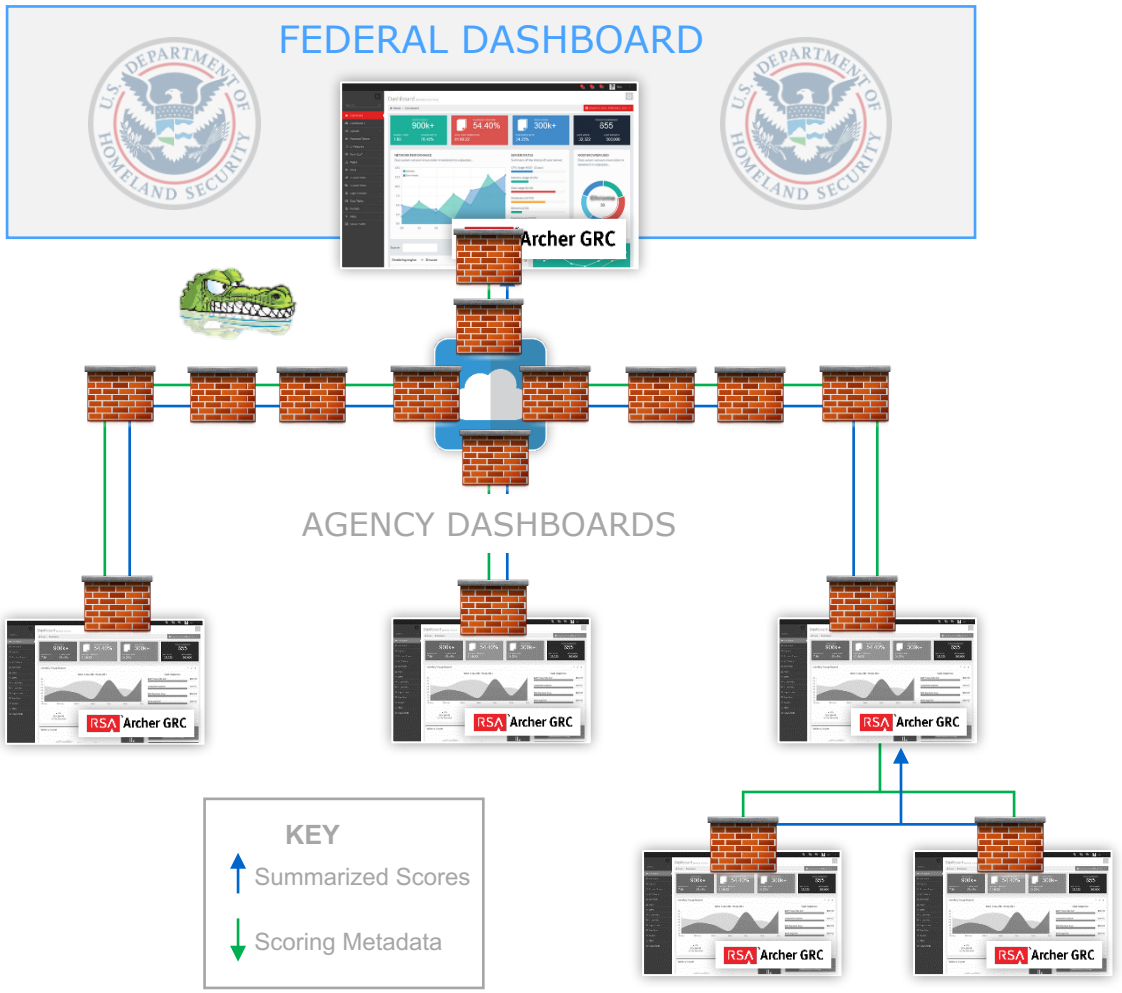
INSTANCE TO INSTANCE COMMUNICATION

- How it should work…

  … and reality

- Getting Dashboards to talk to each other consistently is ***hard!***

- But, we seemed to have figured it out with email



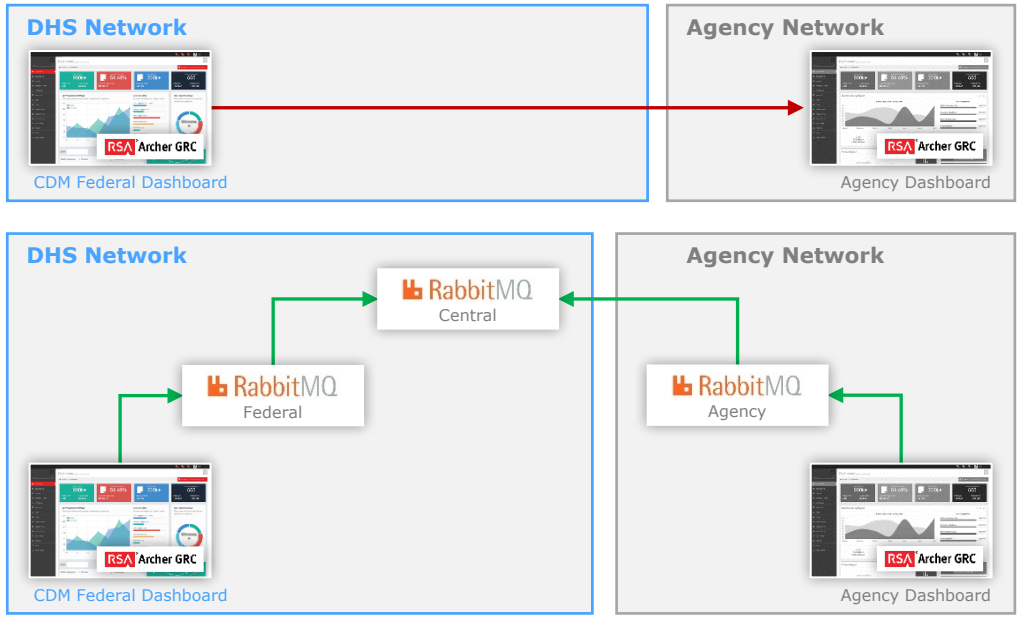
SECTION
04

But we’ve come up with some interesting approachs

… AND UNIQUE SOLUTIONS

MESSAGE QUEUING TO THE RESCUE!

- We've adopted messaging queuing to pass data between instances
  - Built upon RabbitMQ and some custom .NET utilities
  - Removes point to point communication
  - Bi-directional
  - Passive store and forward
  - Allows Dashboards to be hierarchy agnostic
- RabbitMQ acts solely as a store and forward message broker
- Integration applications act as the publisher and consumer of messages between the Agency Dashboard and RabbitMQ
- Integration actions
  - SOAP and REST API calls
  - Remote data feed execution
  - SQL Server stored procedure executions



STRONG AUTHENTICATION IN FEDERATED WORLD

- Users of the Federal Dashboard will span multiple agencies
  - There is no single LDAP data source for all potential users
- Need strong authentication using PIV cards
- The solution… have someone else do it
  - The Office of Management and Budget (OMB) offers authentication services through the MAX platform
    - 173,000+ Users, 180 Agencies, 45,000+ PIV/CAC Cards at 110 agencies
    - Automatic registration for federal users by email domain • HSPD-12 PIV / DOD CAC cards and SMS 2-factor for sensitive activities • Enterprise Federated Partner Automated Login (i.e. single sign-on) with agencies
- We've built some custom code to consume SAMLv2 tokens produced by MAX for use within Archer

LOCAL AND FEDERAL RISK SCORING

- The OOTO scoring mechanism works well, but doesn't allow for local users to score data differently from the Federal method

- Ok… so we copied it
  - Introduced the concept of parallel implementations, the Local Risk Scoring Algorithm (LRSA) and the Federal Risk Scoring Algorithm (FRSA)
  - Schema for scoring parameters is identical
  - Local operators can introduce different scoring parameters and values in the LRSA
  - Role based access control enforces standardization of FRSA parameters

OBJECT CONTAINERS

- Need a flexible way to summarize detailed data for reporting to Federal Dashboard
- Custom ODA – found in Organizational Hierarchy solution
  - Provides the ability to group and assign CDM hardware objects to logical containers
  - Traces overall cybersecurity risk and exposure
- Multiple types of hierarchies
- Settings and impact
  - Exclusive/Exhaustive
  - Mutually Exclusive Field – Calculation
  - Container Owner Field
  - Created By Field
  - Root Container Field
  - Hide Local Scoring

Container Type	Description
Org Hierarchy Container	Organization containers represent the organization hierarchy of the US government and individual agencies
FISMA Container	FISMA containers represent individual FISMA systems
Object Role Container	Object role containers represent
Additional Containers	Custom local hierarchies

SECTION
05

WHAT'S NEXT FOR CDM?

So what else ya got?

CURRENT STATUS AND WHAT'S COMING

- Agency Dashboard
  - Release 2.1 available for deployment
- Federal Dashboard
  - Release in deployment
- Scoping Wave 3 releases now
  - Targeting early Spring 2017 completion
  - We expect to produce at least two full releases for Agency and Federal Dashboards in CY 2017
- Based upon version 5.5, transitioning to 6.x in Release 3
- Addressing Section 508 compliance
- CyberScope replacement
- Phase 2 and 3 requirements

QUESTIONS?