redhat.

SECURING INTELLIGENCE IN AN OPEN HYBRID CLOUD

Stories from the DoD and IC

Shawn Wells
Chief Security Strategist
U.S. Public Sector
shawn@redhat.com

24 August 2016

FOUNDATIONAL BLOCKING & TACKLING

Key **infrastructure** themes from Jennifer Kron’s presentation:

- Functional testing for identity & access management, data protection, audit
- Perform continuous diagnostics and monitoring
  - Must have consistent measurements across multiple environments
- Standardized implementations
  - Baselines?
  - Service Catalogs?
  - Platform as a Service (PaaS)?

FEDERATED DATA ACCESS

Key **data** themes from Jennifer Kron’s presentation:

- “Build to Share, BUT securely”
- How do we ensure data contains attributes and security labels/tags, and build access restrictions from this metedata?

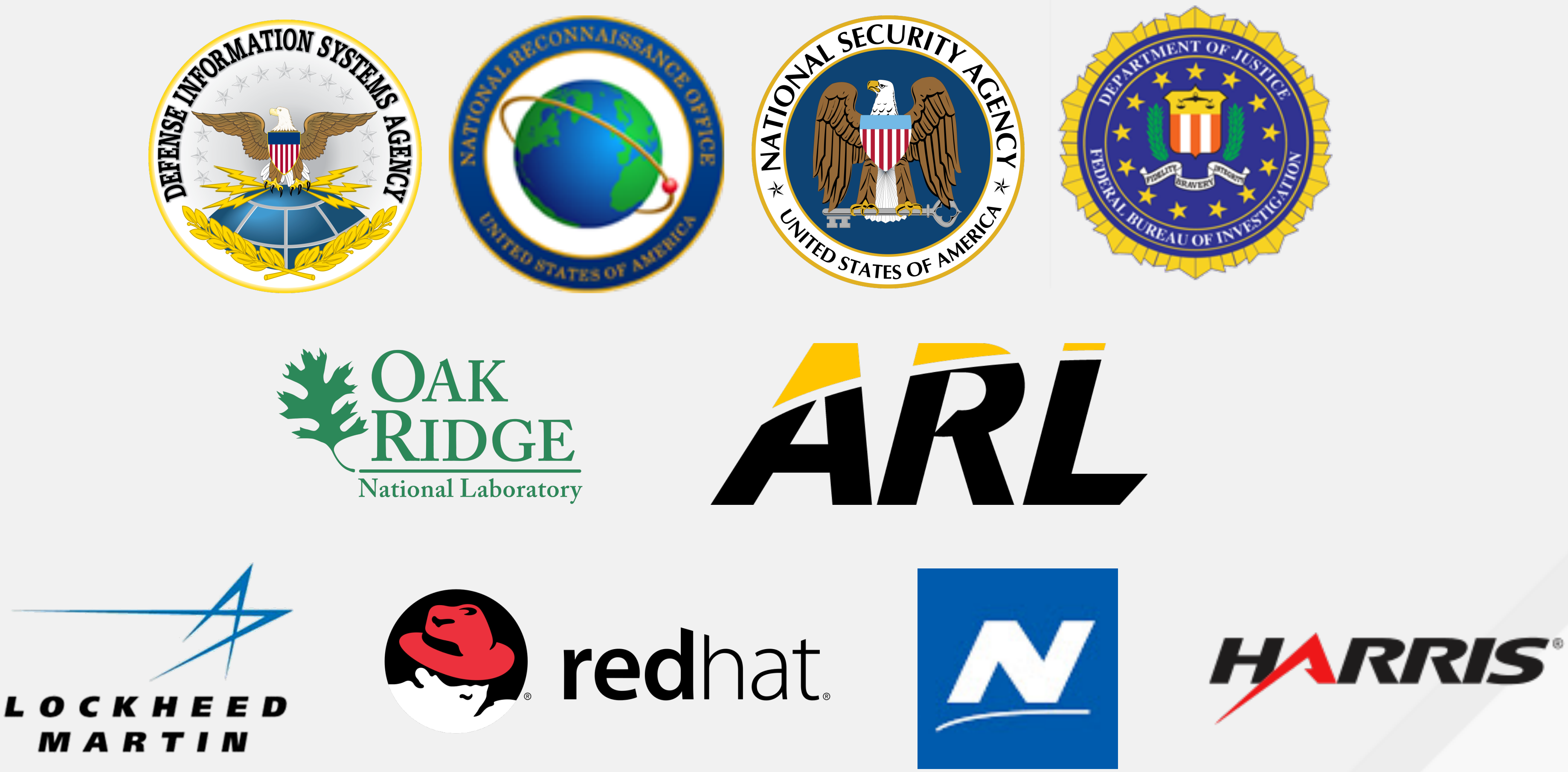
SECURITY AUTOMATION + TOOLING FOR HYBRID CLOUDS

OpenSCAP PROJECT

- Deliver practical security guidance, baselines, and associated validation mechanisms using Secure Content Automation Protocol (SCAP)

- Current upstream source for NSA, NIST, and Red Hat Configuration Guides
  - DISA JBoss Enterprise Application Platform STIG
  - DISA Red Hat Enterprise Linux 6 & 7 STIGs
  - Department of Justice CJIS Baselines
  - National Security Agency SNAC Guide

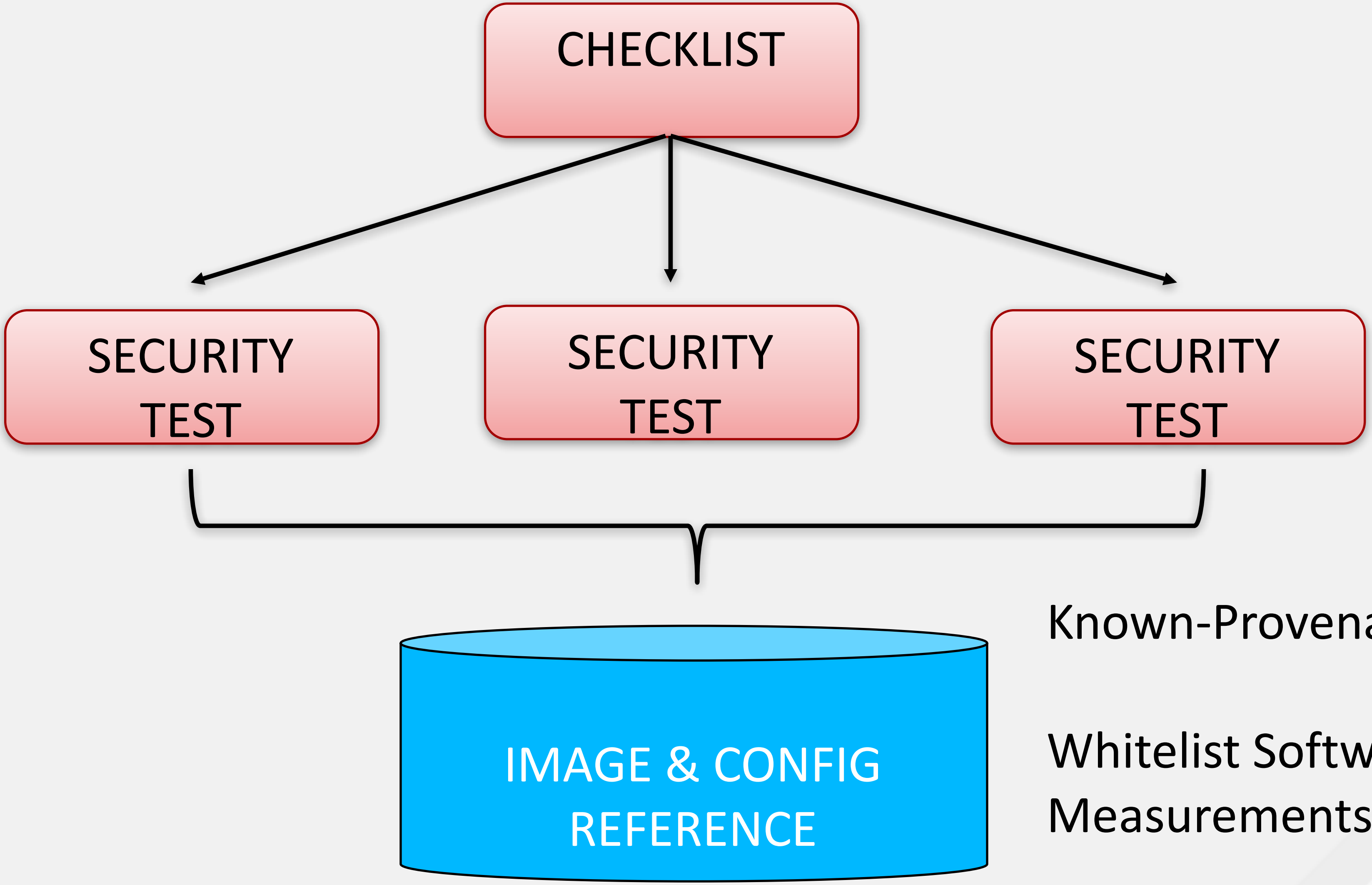
OpenSCAP PROJECT CONTRIBUTORS



OpenSCAP PROJECT

- Maps specific security tests to formalized policies
  - NIST 800-53 rev4
  - DISA Operating System SRG
  - NIST CCE

- Delivering DoD and IC Automated Baselines today!
  - DoD STIG: Joint development with NSA, DISA FSO
  - C2S: Developed for CIA C2S Linux images
  - CS2: Developed with NSA TS for GOVCLOUD systems
  - CJIS: FBI criminal justice systems


CHECKLIST

SECURITY TEST

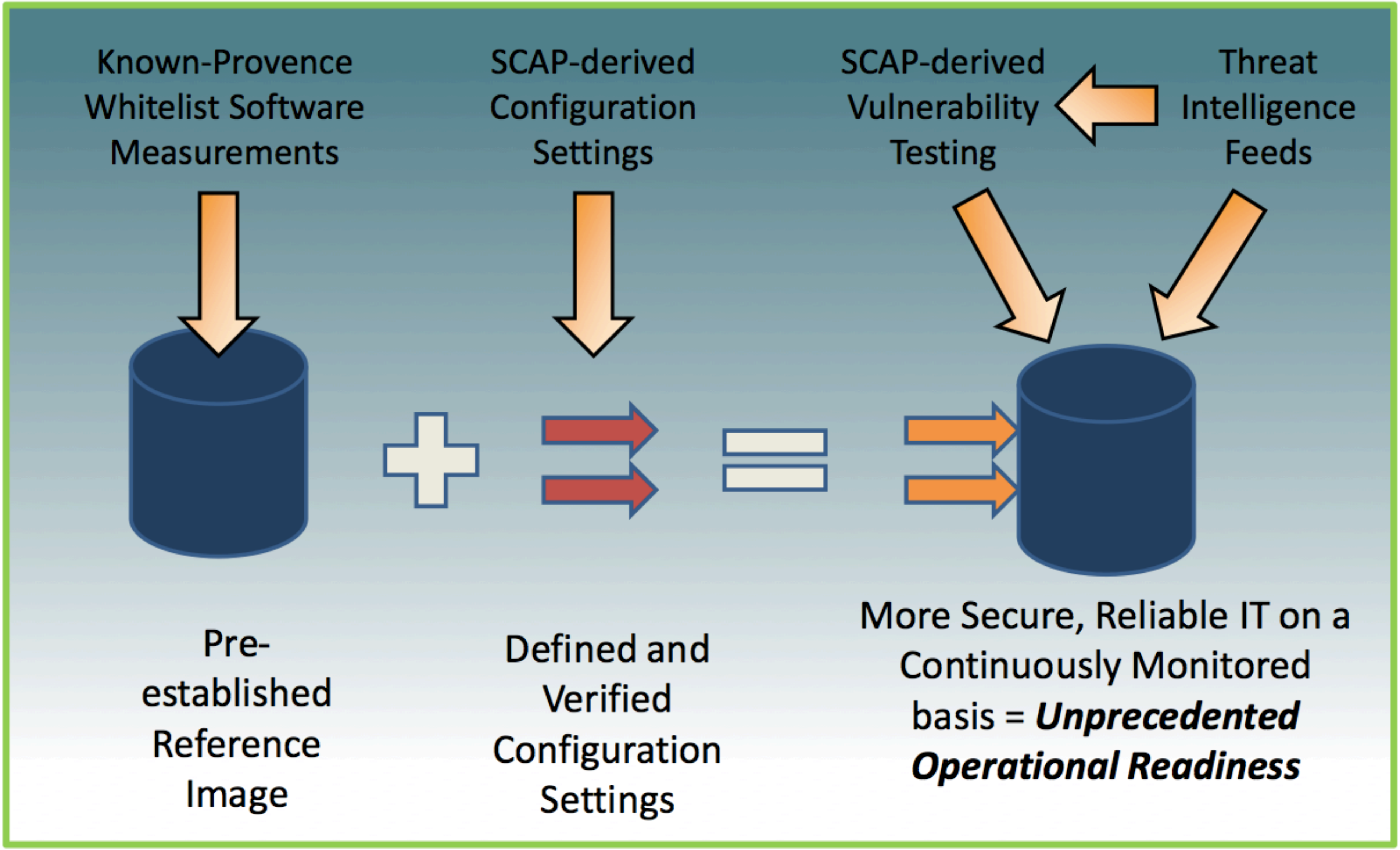
SECURITY TEST

SECURITY TEST

IMAGE & CONFIG REFERENCE

Known-Provenance

Whitelist Software Measurements



Known-Provence Whitelist Software Measurements

SCAP-derived Configuration Settings

SCAP-derived Vulnerability Testing

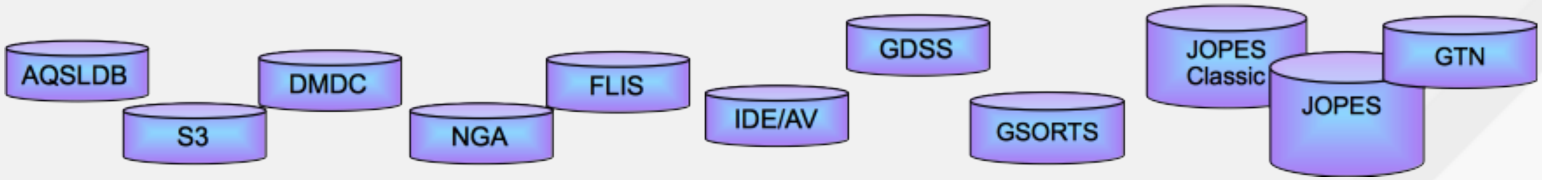
Threat Intelligence Feeds

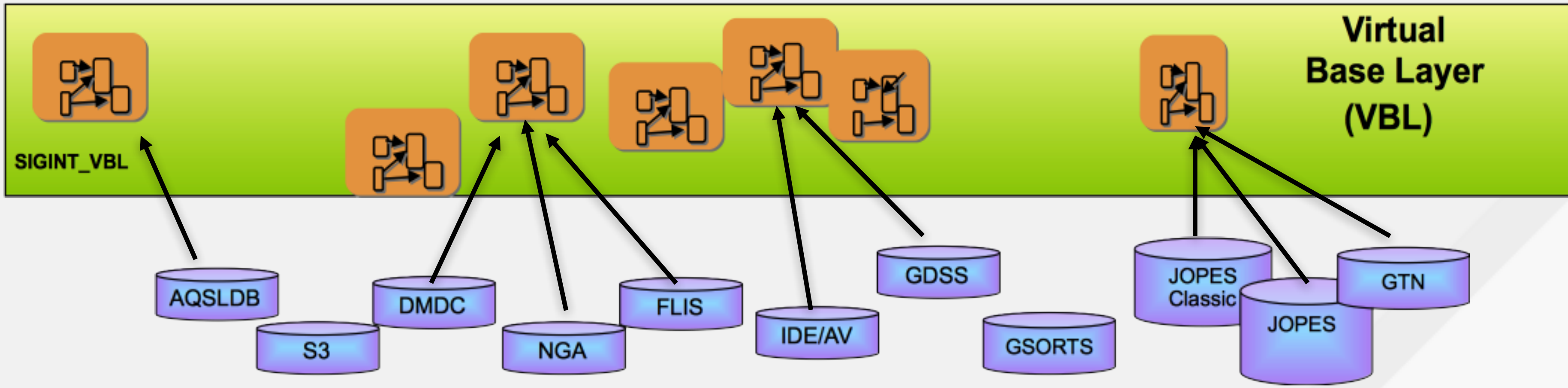
Pre-established Reference Image

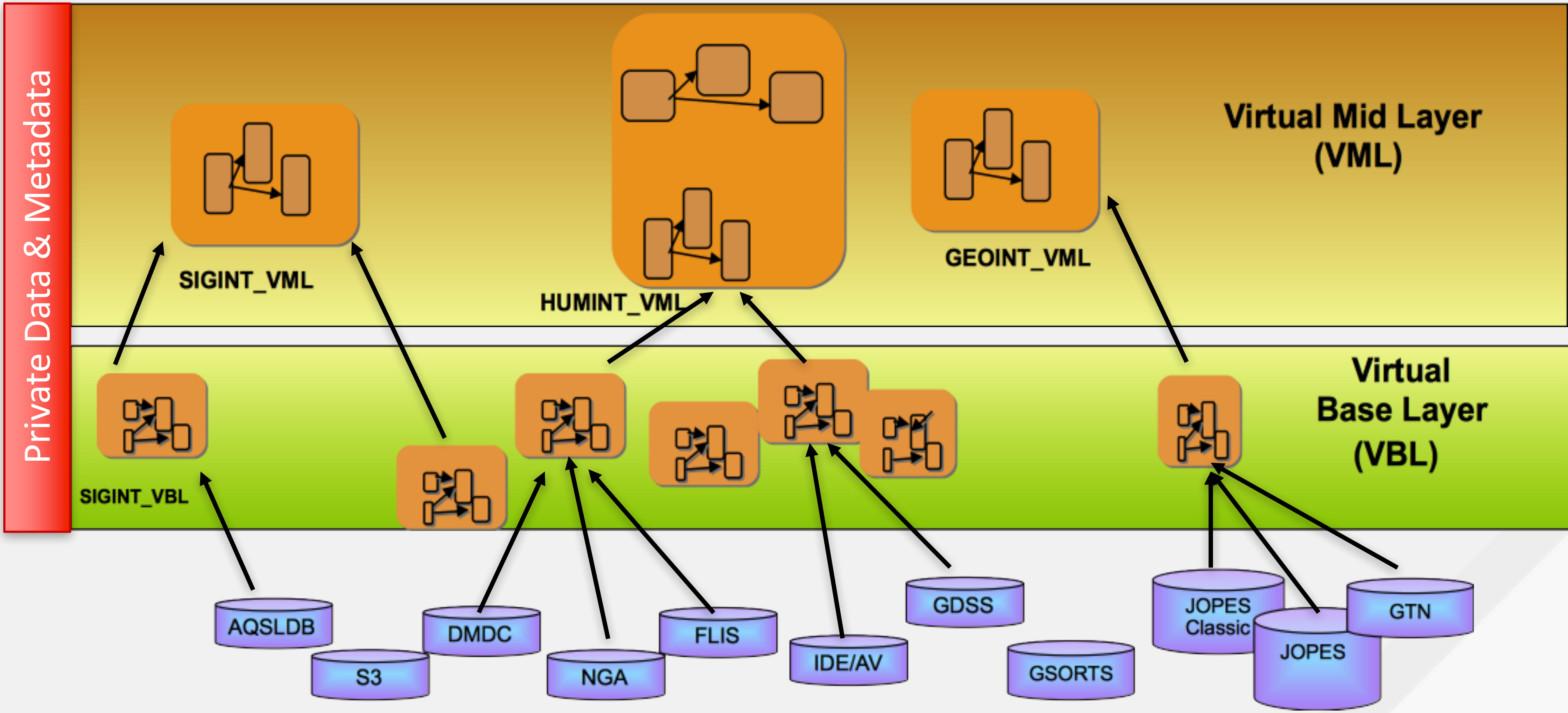
Defined and Verified Configuration Settings

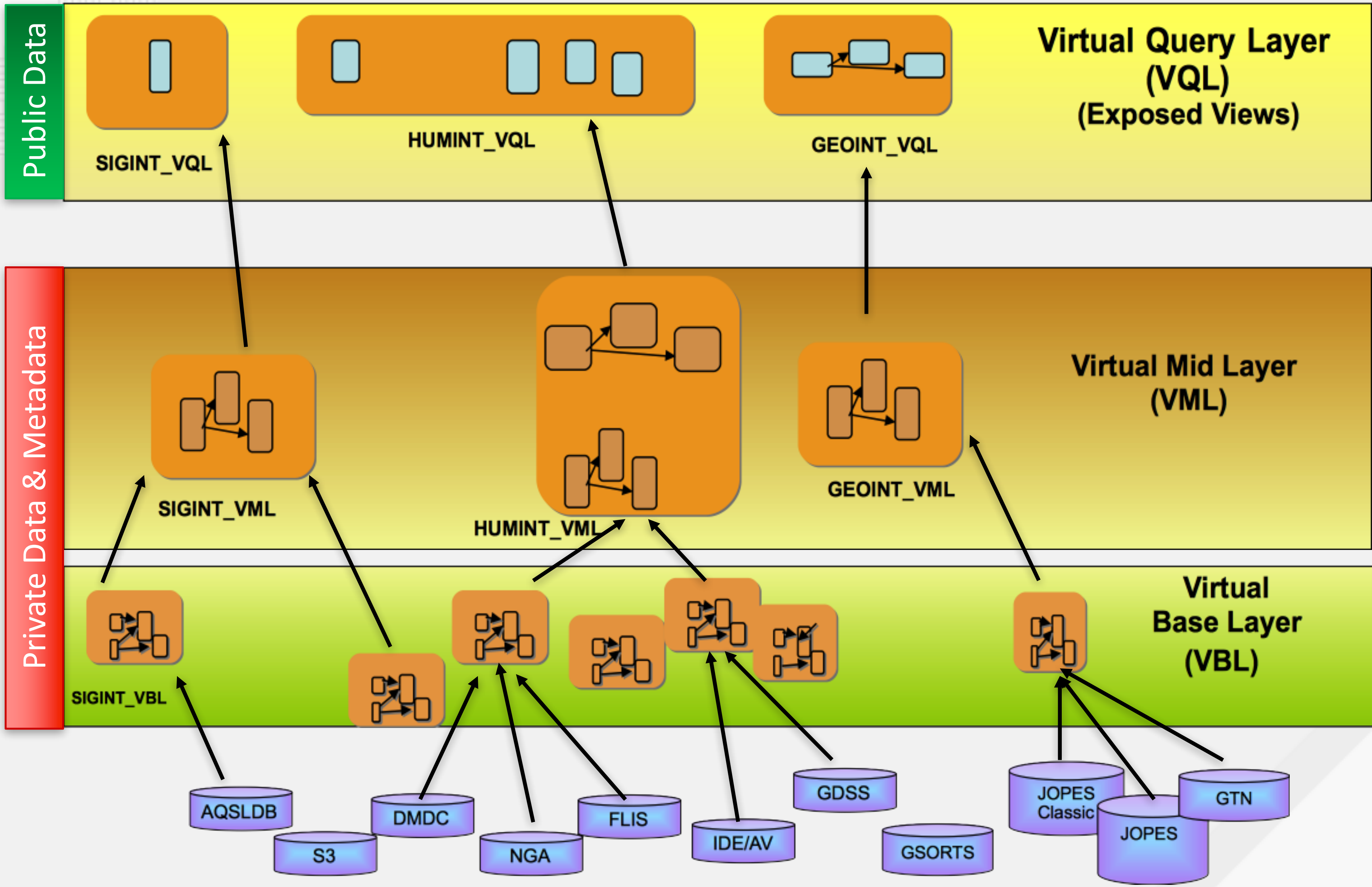
More Secure, Reliable IT on a Continuously Monitored basis = ***Unprecedented Operational Readiness***

STRUCTURED DATA SERVICES ACROSS HYBRID CLOUDS


AQSLDB
S3
DMDC
NGA
FLIS
IDE/AV
GDSS
GSORTS
JOPES Classic
JOPES
GTN


Virtual
Base Layer
(VBL)
SIGINT_VBL
AQSLDB
S3
DMDC
NGA
FLIS
IDE/AV
GDSS
GSORTS
JOPES
Classic
JOPES
GTN


Private Data & Metadata
Virtual Mid Layer
(VML)
SIGINT_VML
HUMINT_VML
GEOINT_VML
Virtual
Base Layer
(VBL)
SIGINT_VBL
AQSLDB
S3
DMDC
NGA
FLIS
IDE/AV
GDSS
GSORTS
JOPES
Classic
JOPES
GTN


Public Data
Private Data & Metadata
Virtual Query Layer (VQL) (Exposed Views)
SIGINT_VQL
HUMINT_VQL
GEOINT_VQL
Virtual Mid Layer (VML)
SIGINT_VML
HUMINT_VML
GEOINT_VML
Virtual Base Layer (VBL)
SIGINT_VBL
AQSLDB
S3
DMDC
NGA
FLIS
IDE/AV
GDSS
GSORTS
JOPES Classic
JOPES
GTN

IC PERSONS OF INTEREST

CHALLENGE

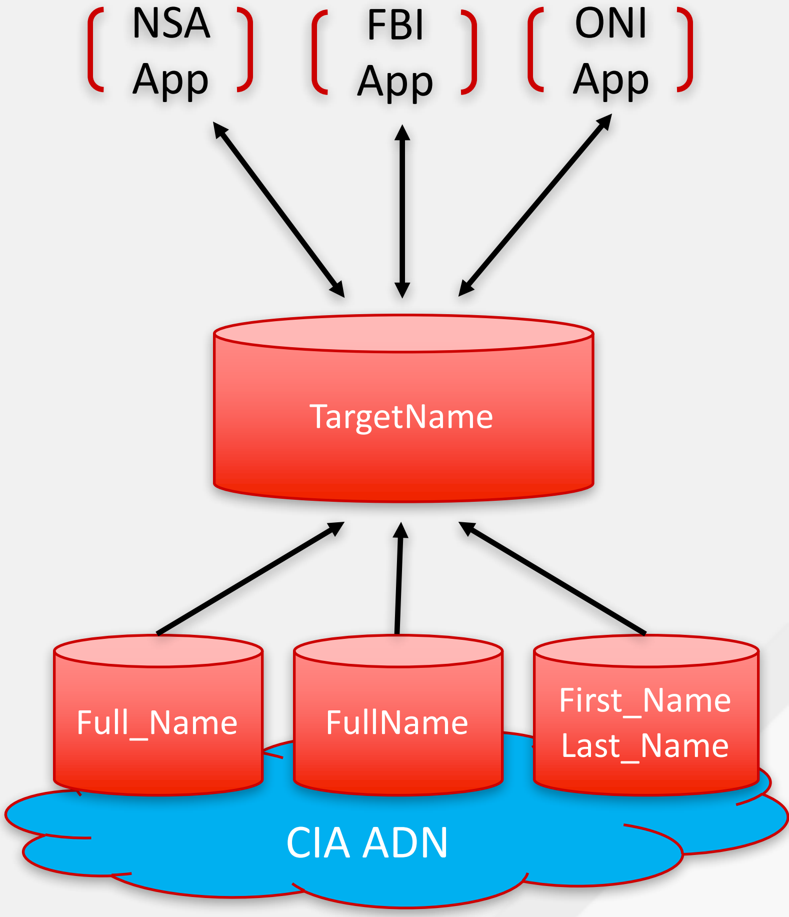
- Need to find Person of Interest across disparate IC systems
- Adherence to IC-wide common data scheme

SOLUTION

- Create abstracted view of enterprise data schema
- Facilitates data ingest/egress by creating standard data fields

BENEFIT

- Simplified data access, decoupled services and apps from the underlying complex data infrastructure



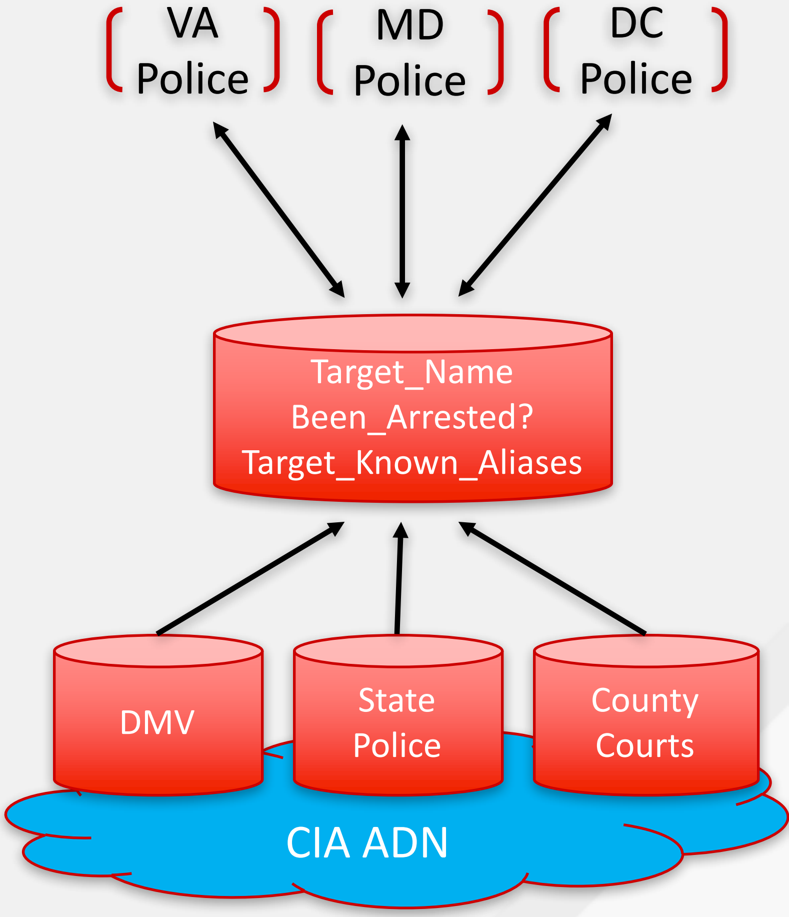
DISA ADNET: ANTI-DRUG NETWORK

CHALLENGE

- Counter-narcotics and counter-narcoterrorism
- Statutory detection and monitoring
- Data is heterogeneous & on multiple systems

SOLUTION

- Created abstracted view across multiple State/Local Law enforcement agencies
- Virtual database enables BI tools to get a complete picture of person from any history, warrants, jail, crimes, vehicles, etc
- Federated search layer looking for possible aliases given general details (cars, addresses, license, etc).



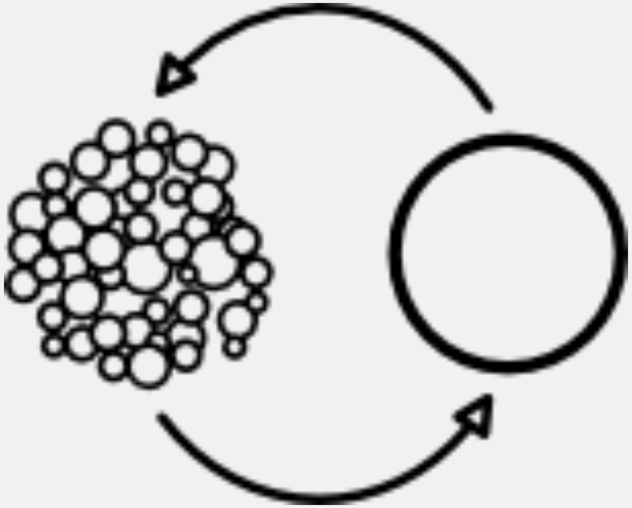
BUILDING YOUR OPEN HYBRID CLOUD

EVERYONE IS A TECHNOLOGY COMPANY TODAY.

WHEN EVERYONE IS A TECH COMPANY,

I.T. CAN BE A SOURCE OF COMPETITIVE ADVANTAGE.

THESE TECHNOLOGIES ARE DRIVEN BY OPEN SOURCE



OPEN SOURCE MEANS COMMUNITY MEMBERS CAN
SEE, LEARN FROM, IMPROVE, MODIFY, AND SHARE
THE SOURCE CODE TO SOLVE CHALLENGES AND MEET NEEDS.

THE OPEN SOURCE ADVANTAGE

Provides the interoperabilility to use a range of solutions from multiple providers.

Security developed in collaboration with the industry's experts.

Gives you access to the best technology, and contribute to its success.

Reduces time spent keeping the lights on and increases your time to innovate.

**THIS ISN'T JUST A WAY OF DOING BUSINESS.
IT'S A MODEL FOR THE FUTURE OF TECHNOLOGY.**

RED HAT MAKES OPEN SOURCE READY FOR THE ENTERPRISE

RED HAT DELIVERS THE INNOVATION OF OPEN SOURCE PROJECTS AS PREDICTABLE, RELIABLE, AND SECURE PRODUCTS.

COMMON CRITERIA – FIPS 140-2 – DoD STIGs – CNSSI 1253 redhat.

THANK YOU!

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos