FISMA Metrics

An architectural approach to data collection and measurement using security automation

Current State

- 50 SCAP validated products from 32 different vendors
  - Enables assessment of commonly available operating systems and applications
  - Standardized content provides content-level interoperability allowing the same content to be used in all SCAP products (e.g. USGCB)
- Network protocols are not standardized, preventing plug-and-play interoperability of security automation tools
- Asset management is not fully addressed

Continuous Monitoring OODA Loop

Observe

- Use of automated capabilities to ***collect data*** using sensors

Orient

- Orchestration of analysis processes to provide ***shared situational awareness***

Decide

- Exposing information to users and autonomous capabilities to inform ***decision making***

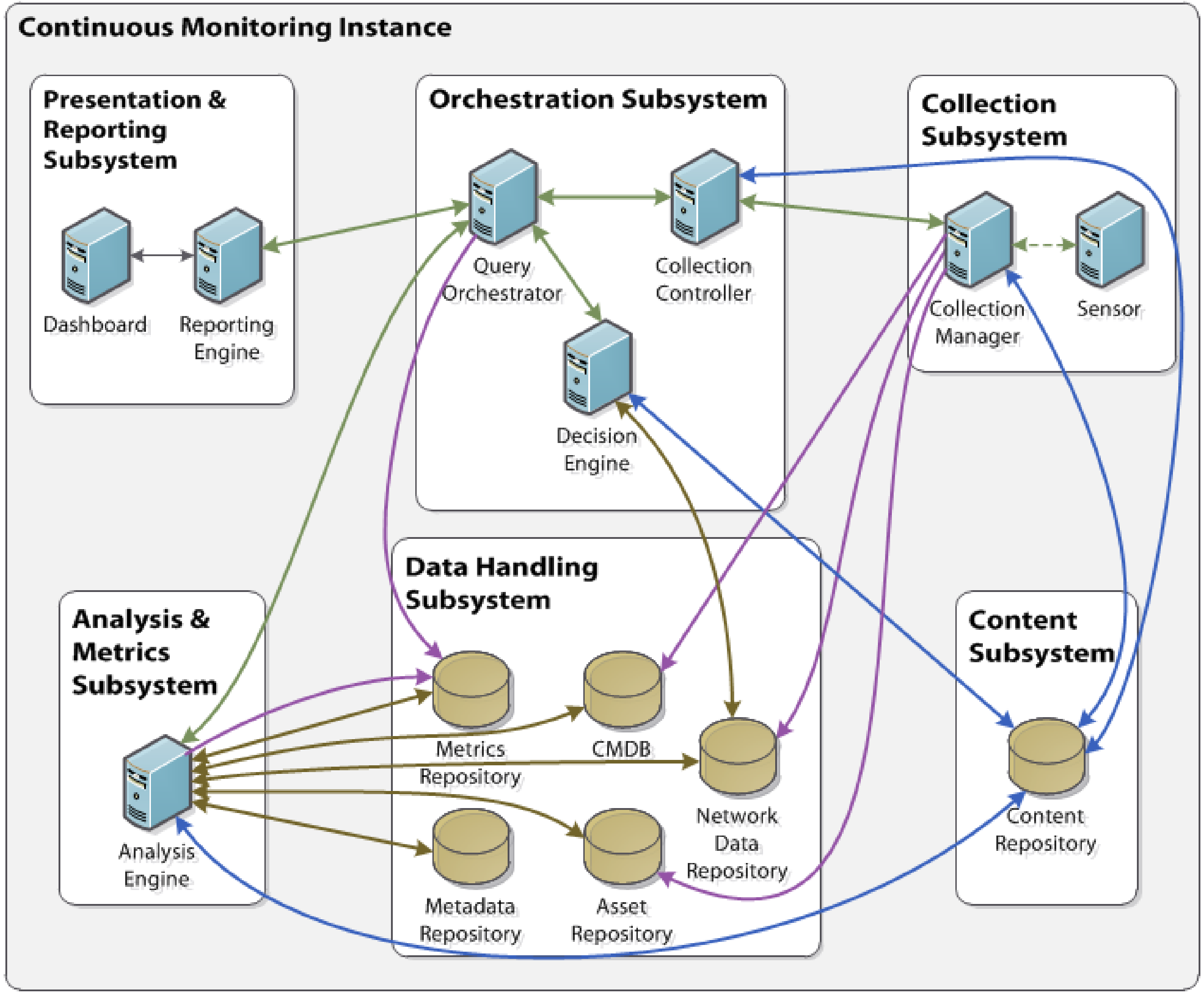
Act

- Providing information in support of taking **autonomous or technology-assisted actions**

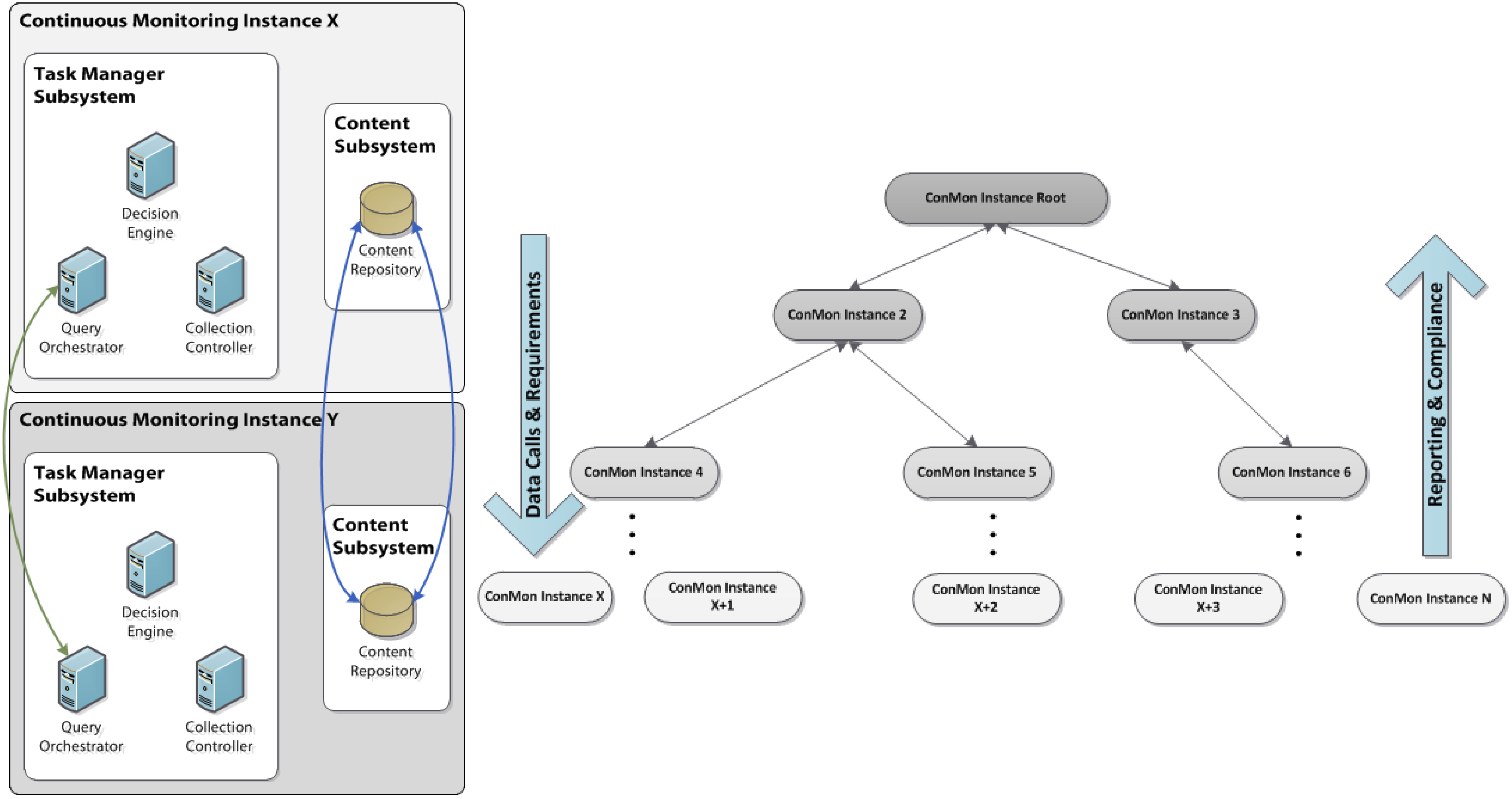
Current Work

- Development of CAESARS-FE: A Continuous Monitoring Technical Reference Architecture described by NISTIR 7756.
- Collaboration with industry and government to develop use cases and requirements.
- Outreach to Standards Development Organizations (SDOs)
  - Establishment of an IETF security automation working group focused on industry-led, international consensus standards.
  - Working with the Trusted Computing Group (TCG) and IETF to expand Trusted Network Connect (TNC) protocols to collect asset details and enforce policies.
  - Working with ISO to expand support for Software Identification (SWID) tagging standards.

CAESARS-FE Reference Architecture



Hierarchical Data Collection and Reporting



Asset Management

- Provide visibility into hardware assets using hardware and software device identities (2.1, 2.2)
- Integrate with asset repositories using CAESARS-FE to support assignment of responsible parties (2.3) and other asset metadata (e.g. FIPS199)
- Enable integration with Network Access Control (NAC) capabilities based on TNC IETF and TCG standards (2.4)
- Use of Software Identification (SWID) tags to identify installed OS, applications, and patches (2.5, 2.6)
- SWID-based capabilities can integrate with whitelist tools to block execution of unauthorized software (2.7)

Configuration Management

- Use of SCAP capabilities to support automated scanning of hardware assets using USGCB and other SCAP content.
  - OS (3.1.1 - 3.1.4)
  - Applications (3.2.1 – 3.2.4)
- Identifying methods to enable OS and applications to assert configuration settings
- Use of TNC protocols to carry SCAP data using SCAP Messages for IF-M.
- Identifying methods to expand support for network devices (3.3) and other infrastructure components.

Vulnerability Management

- Use of collected software inventory to identify vulnerabilities (4.1 – 4.2)
  - Use SWID-based software inventories collected over TNC using SWID Messages for IF-M to identify vulnerable assets.
  - Use of vendor provided SWID tags containing executable and library footprint details to generate vulnerable products list based on vulnerable executable or library

Conclusions

Government and Industry needs to work together to:

- Identify and/or facilitate the development of:
  - The **schema** to **express security information**
  - The **interfaces** to enable system components to **communicate securely**
  - The **network protocols** needed to enable **interoperable data exchange**
- Provide the necessary guidance and requirements to SDOs and vendors to **drive technical solutions and standards**.
- Build on existing work by **integrating** SCAP with **existing network protocols** (e.g. TNC).
- **Integrate existing asset and software inventory management standards** into the overall technical approach