

38th Engineering Squadron

Plan, engineer, implement, assess, and restore

AF cyber capabilities throughout the cyberspace domain



"We're both paying for the same system!"

Ben Griffith

The Overall Classification of this briefing is:

UNCLASSIFIED





Before We Start



All of the following statements apply specifically to NIPRnet and SIPRnet.

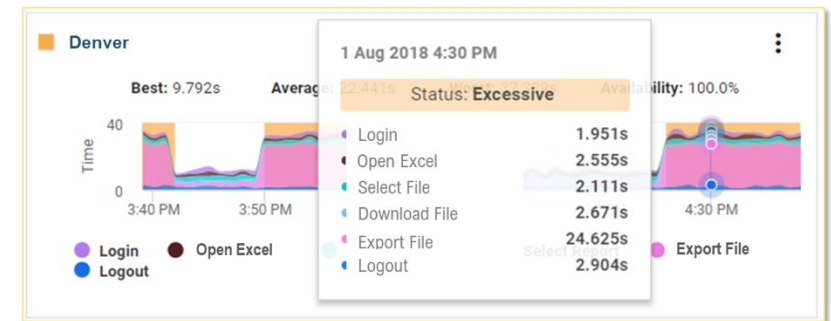
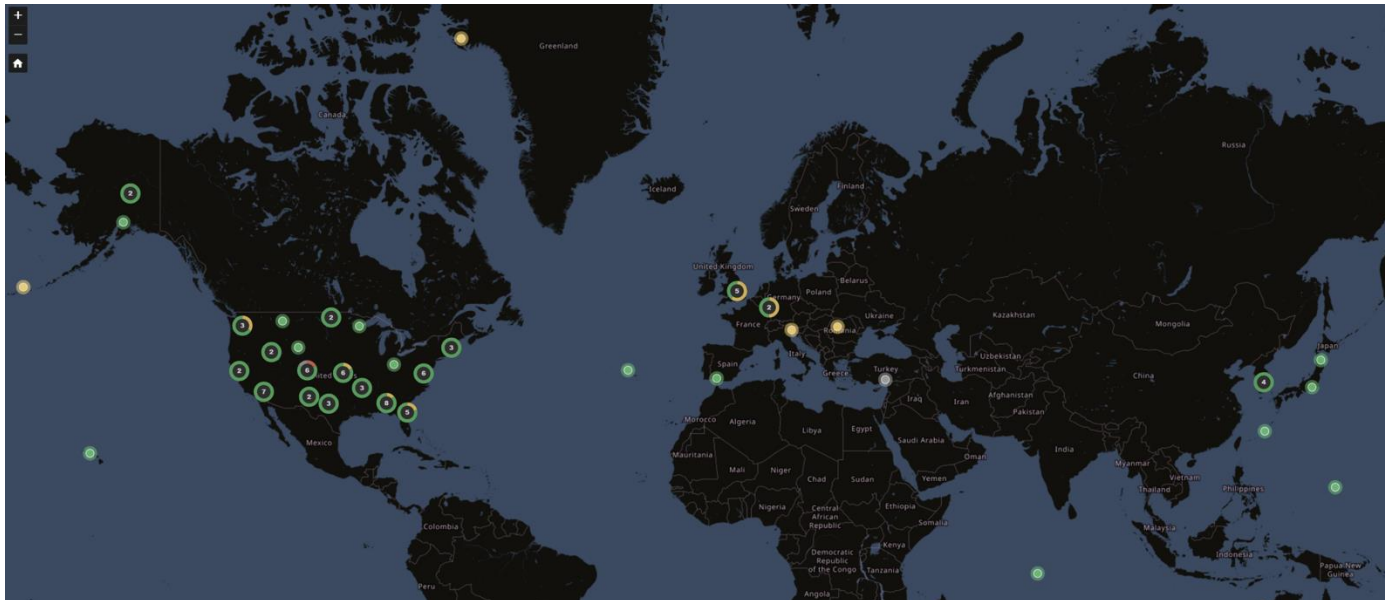
This discussion does NOT concern air-gapped environments or mission systems.

The intent of this presentation is to provide a framework for data acquisition that satisfies all parties concerned with the general information technology ecosystem of the Air Force, NOT your super-niche mission.





Who's The Guy





Lines of Effort We All Can See



LOE 1 (Collapsing Tools): “We’re paying for disparate systems that don’t talk to each other, our airmen aren’t trained on, and this leaves us less prepared when we rotate.”

The Air Force, pretty much unanimously: “Yep! We see the same thing occurring on our end. Let’s get on the same page.”

The Air Force’s Action: Establish colocated PMOs and begin tool consolidation. Ref: IDCS, EPMS, etc.





Lines of Effort We All Can See



LOE 1 (Collapsing Tools): “We’re paying for disparate systems that don’t talk to each other, our airmen aren’t trained on, and this leaves us less prepared when we rotate.”

The Air Force, pretty much unanimously: “Yep! We see the same thing occurring on our end. Let’s get on the same page.”

The Air Force’s Action: Establish colocated PMOs and begin tool consolidation. Ref: IDCS, EPMS, etc.

LOE 2 (Data Ops & “Single Source of Truth”): “We’ve got multiple tools monitoring the same things- which tool do I listen to and how do I cross-correlate?”

The Air Force, pretty much unanimously: “Yep! We need to join the data and begin data analysis at once.”

The Air Force’s Action: Begin data consolidation into clouds, enforce cloud migrations. Ref. CloudOne, PlatformOne, etc.





Enter: Your Requirements vs. My Requirements



PMO1: Our 1067 requirements list BAN NetFlow and Packet Feed data as a requirement

PMO Actions:

- *Review, accept requirements*
- *Investigate multiple contenders for COTS/GOTS that can fulfill 1067 requirements*
- *Build budget for acquisition, sustainment, maintenance*
- *R&D, acquire, continuously improve on PMO1 system*





Enter: Your Requirements vs. My Requirements



PMO1: Our 1067 requirements list BAN NetFlow and Packet Feed data as a requirement

PMO Actions:

- *Review, accept requirements*
- *Investigate multiple contenders for COTS/GOTS that can fulfill 1067 requirements*
- *Build budget for acquisition, sustainment, maintenance*
- *R&D, acquire, continuously improve on PMO1 system*

PMO2: Our 1067 requirements list BAN NetFlow and Packet Feed data as a requirement

PMO Actions:

- *Review, accept requirements*
- *Investigate multiple contenders for COTS/GOTS that can fulfill 1067 requirements*
- *Build budget for acquisition, sustainment, maintenance*
- *R&D, acquire, continuously improve on PMO2 system*





Enter: Your Requirements vs. My Requirements



PMO1: Our 1067 requirements list BAN NetFlow and Packet Feed data as a requirement

PMO Actions:

- *Review, accept requirements*
- *Investigate multiple contenders for COTS/GOTS that can fulfill 1067 requirements*
- *Build budget for acquisition, sustainment, maintenance*
- *R&D, acquire, continuously improve on **PMO1 system***

PMO2: Our 1067 requirements list BAN NetFlow and Packet Feed data as a requirement

PMO Actions:

- *Review, accept requirements*
- *Investigate multiple contenders for COTS/GOTS that can fulfill 1067 requirements*
- *Build budget for acquisition, sustainment, maintenance*
- *R&D, acquire, continuously improve on **PMO2 system***

~~SYSTEMS~~

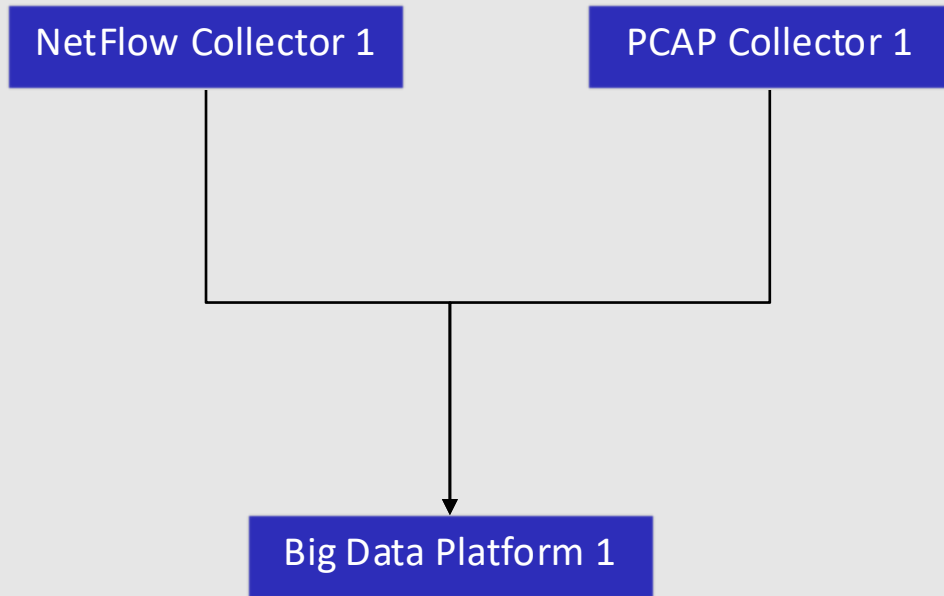
DATA



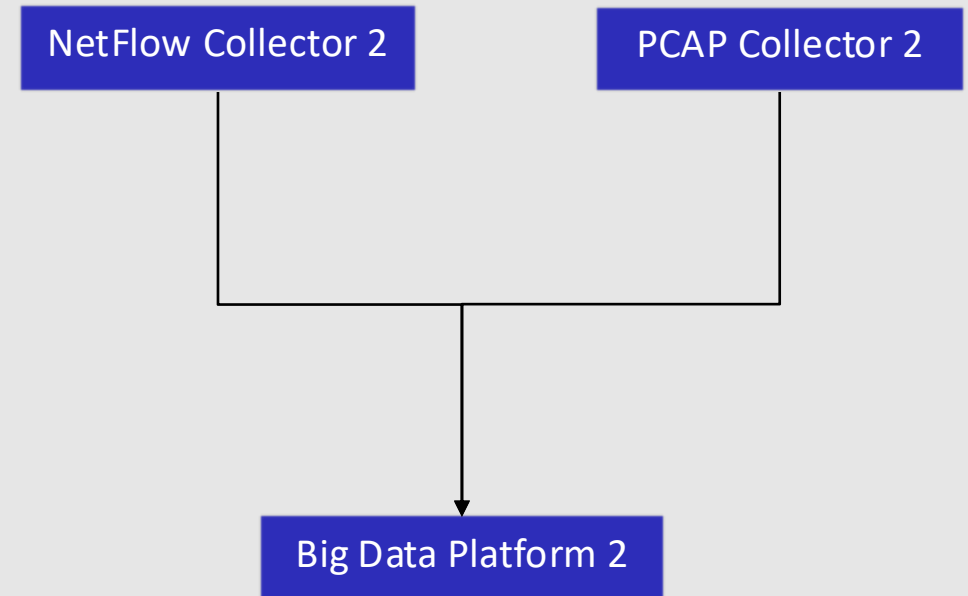


Result of System-Centric Thinking

PMO1 SYSTEM

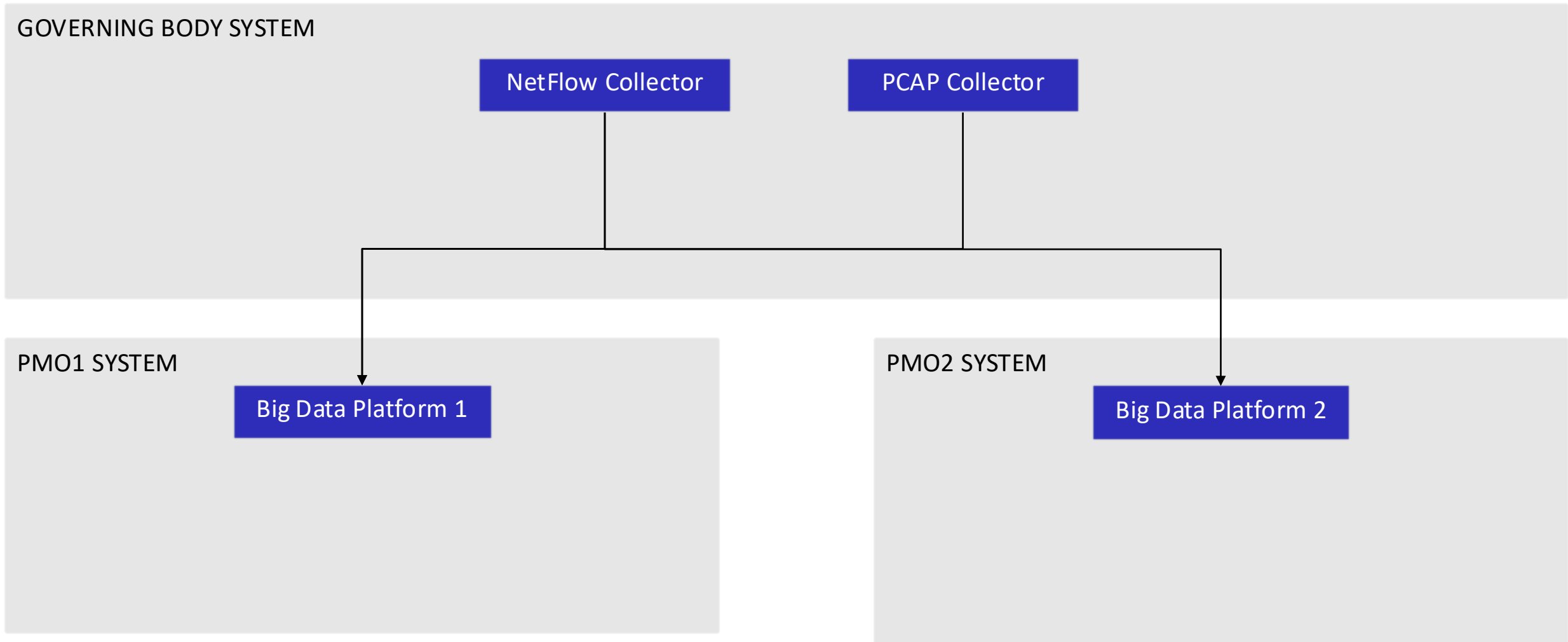


PMO2 SYSTEM





Result of Data-Centric Thinking

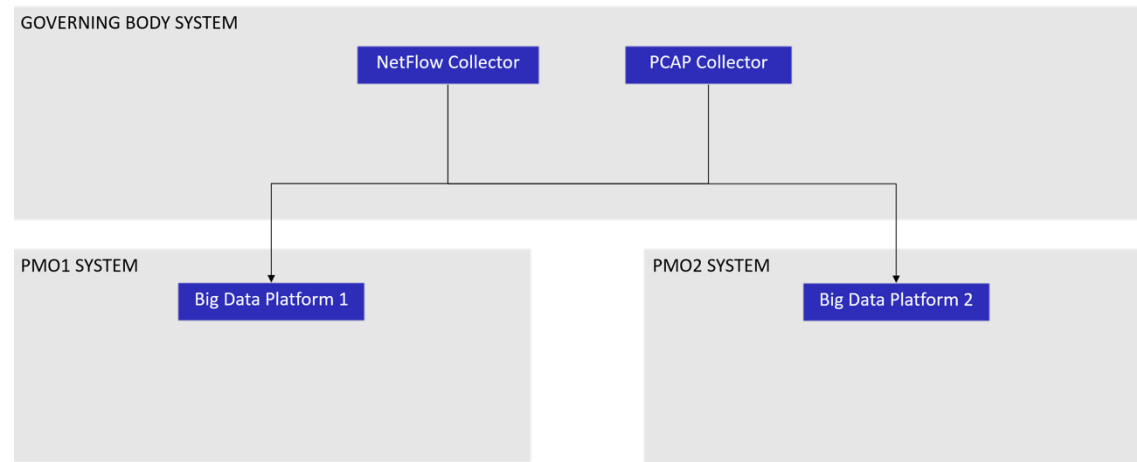


1067: BAN NetFlow and Packet Feed

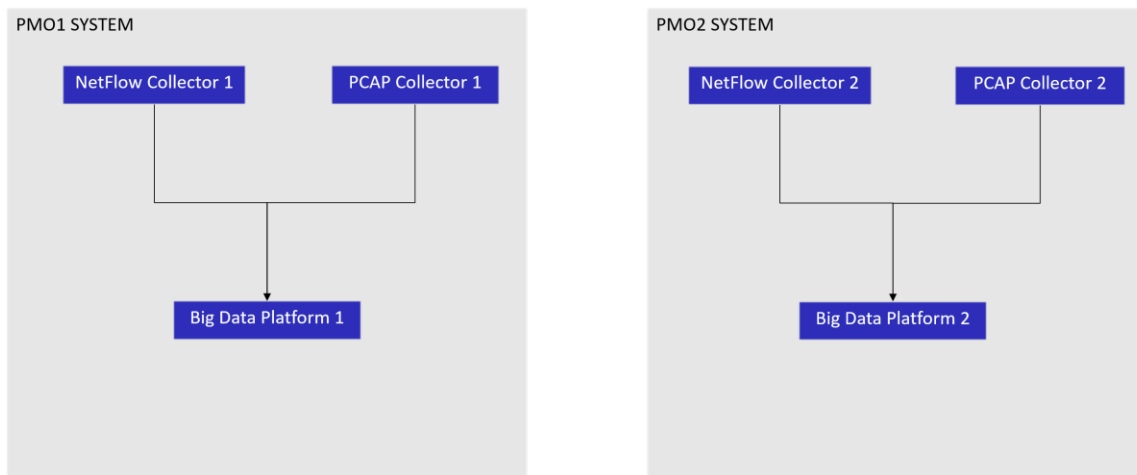




Air Force Assumption 1



Most system owners care less about how precisely the data is coming to their doorstep, and more about the data not changing

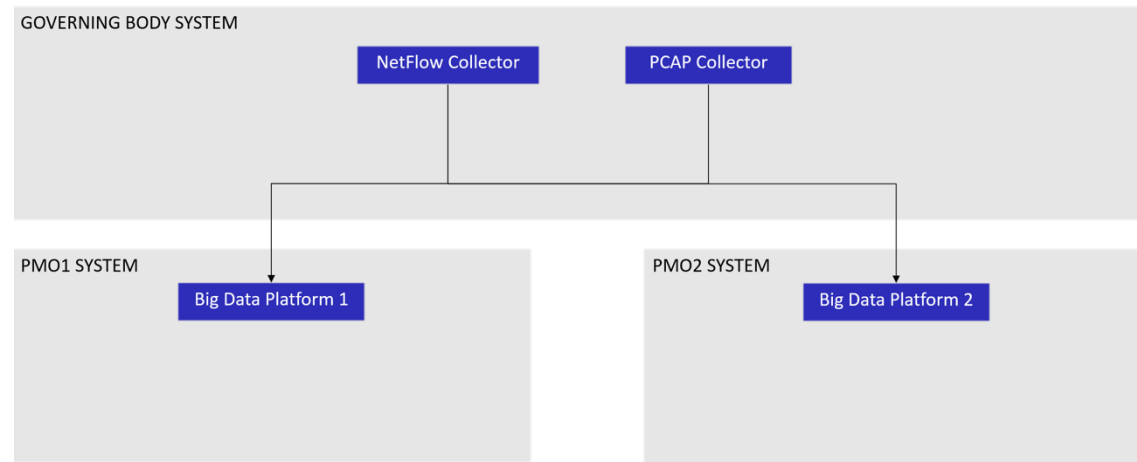


“If you let my system continue working as is, I don’t care!”

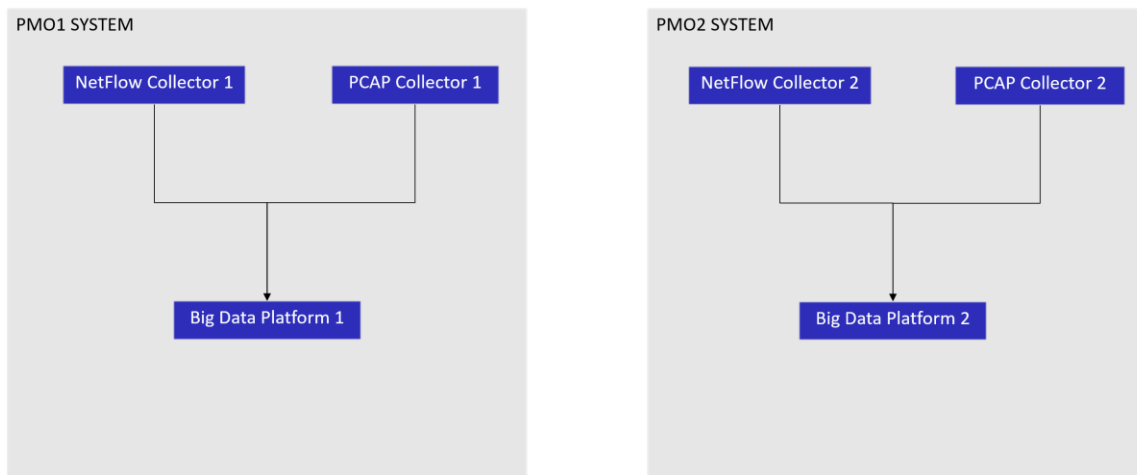




Air Force Assumption 2



In the event that multiple PMOs are able to converge on a solution for strictly data collection, then the Air Force at large will, with a fixed budget, be capable of leveraging more capabilities against the data.

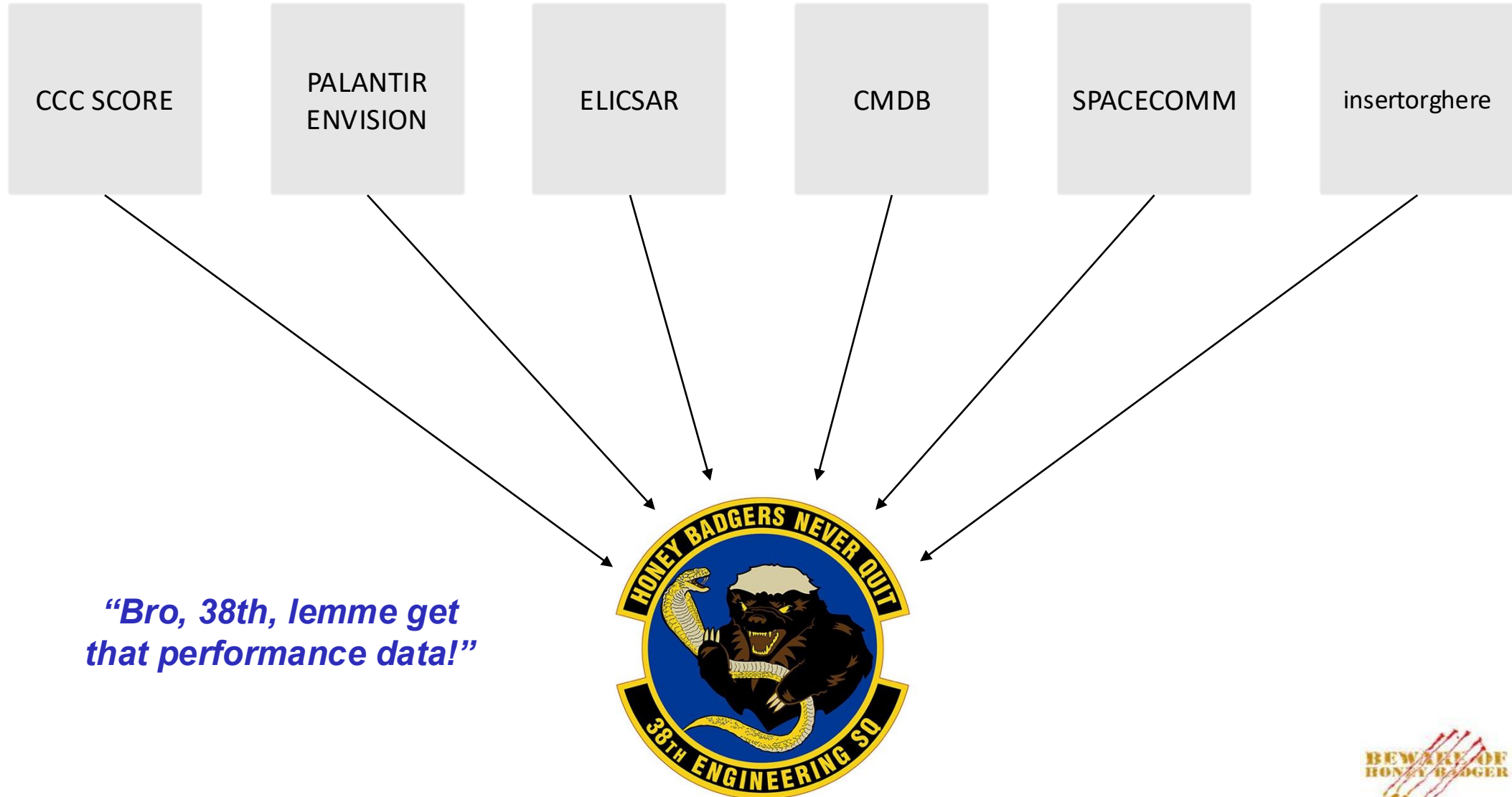


“Vendor X, good news and bad news: You’re selling bigger stuff to us, but now there’s fewer customers.”



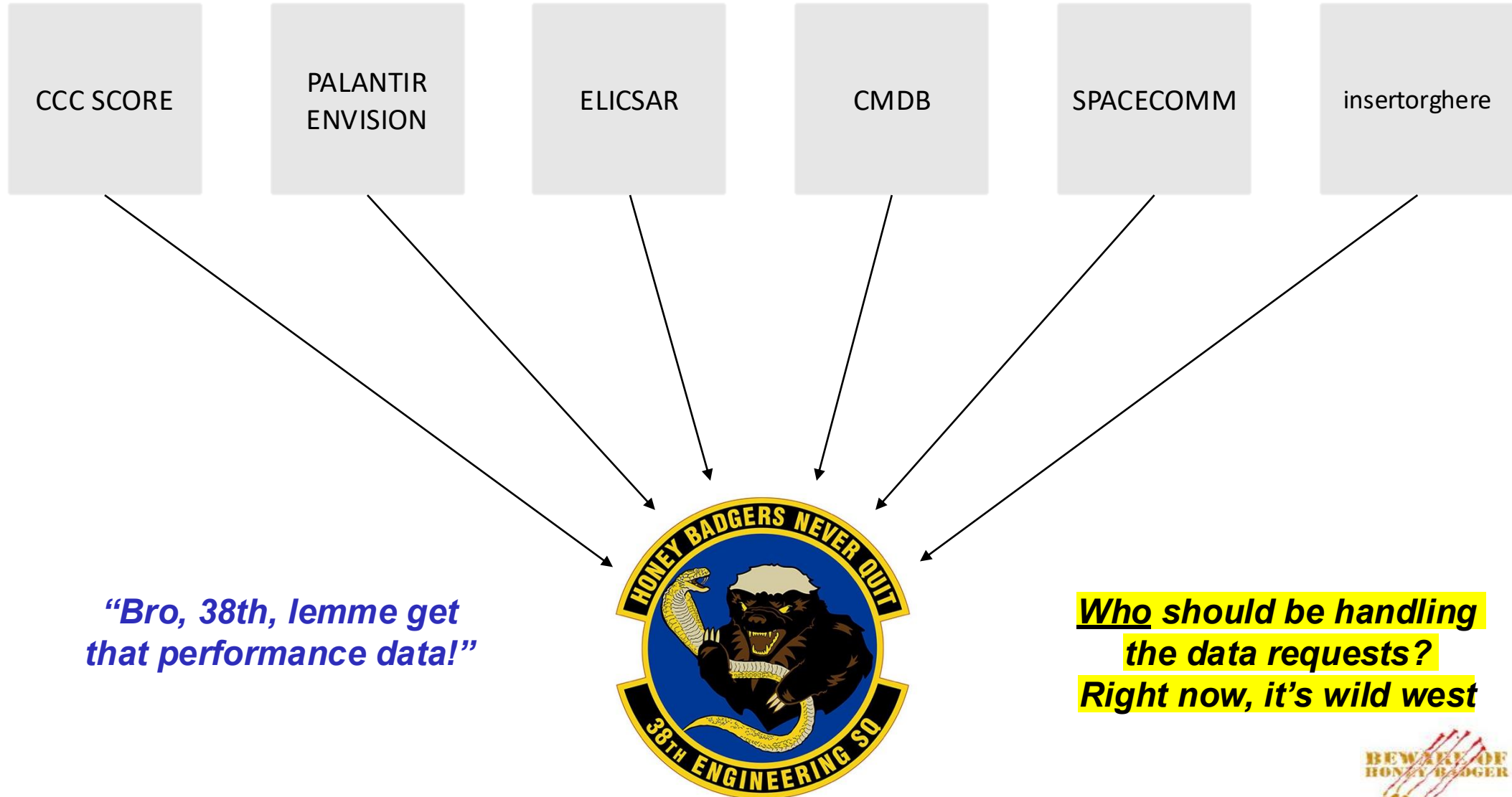


The Bro-net is already starting to do this...



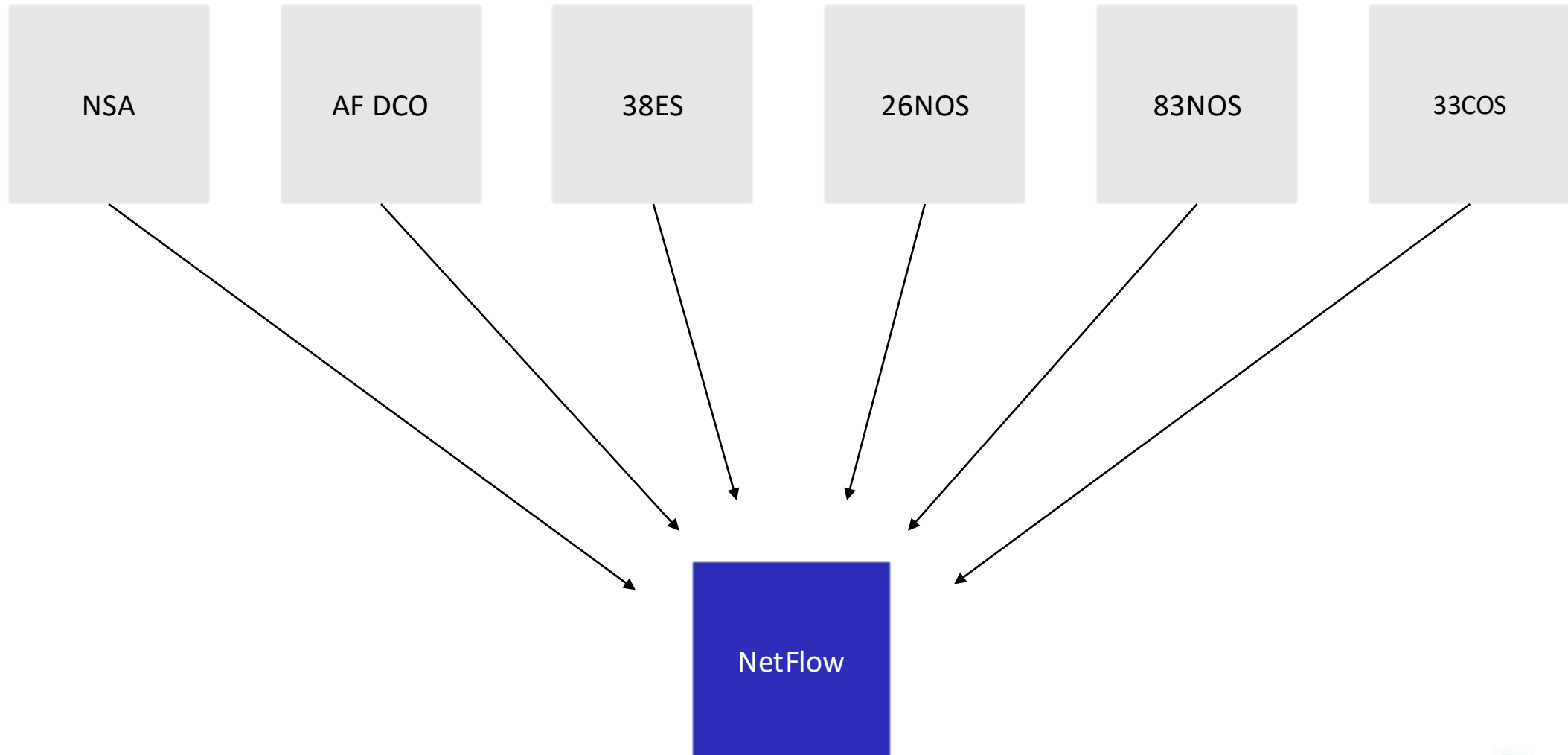


The Bro-net is already starting to do this...



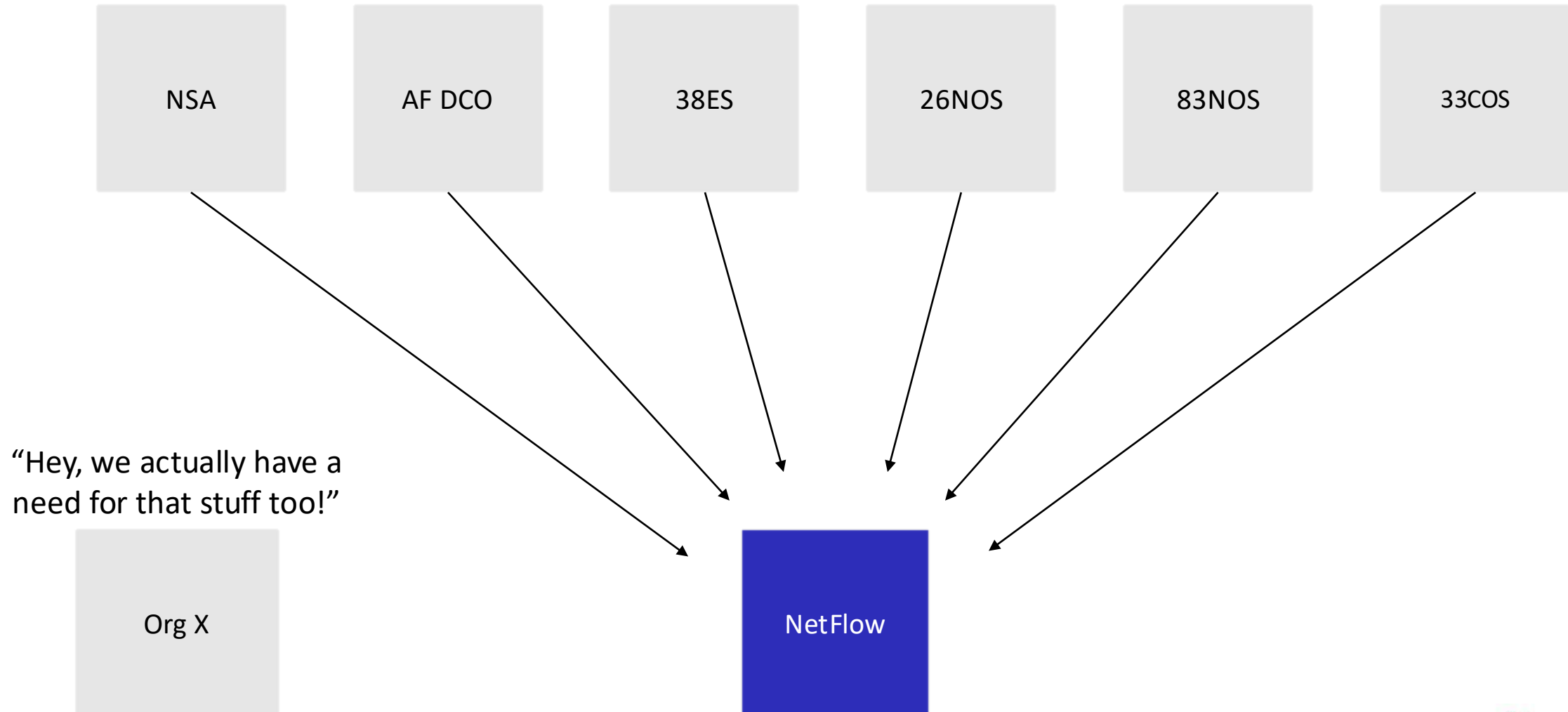


Fully Operational Capability



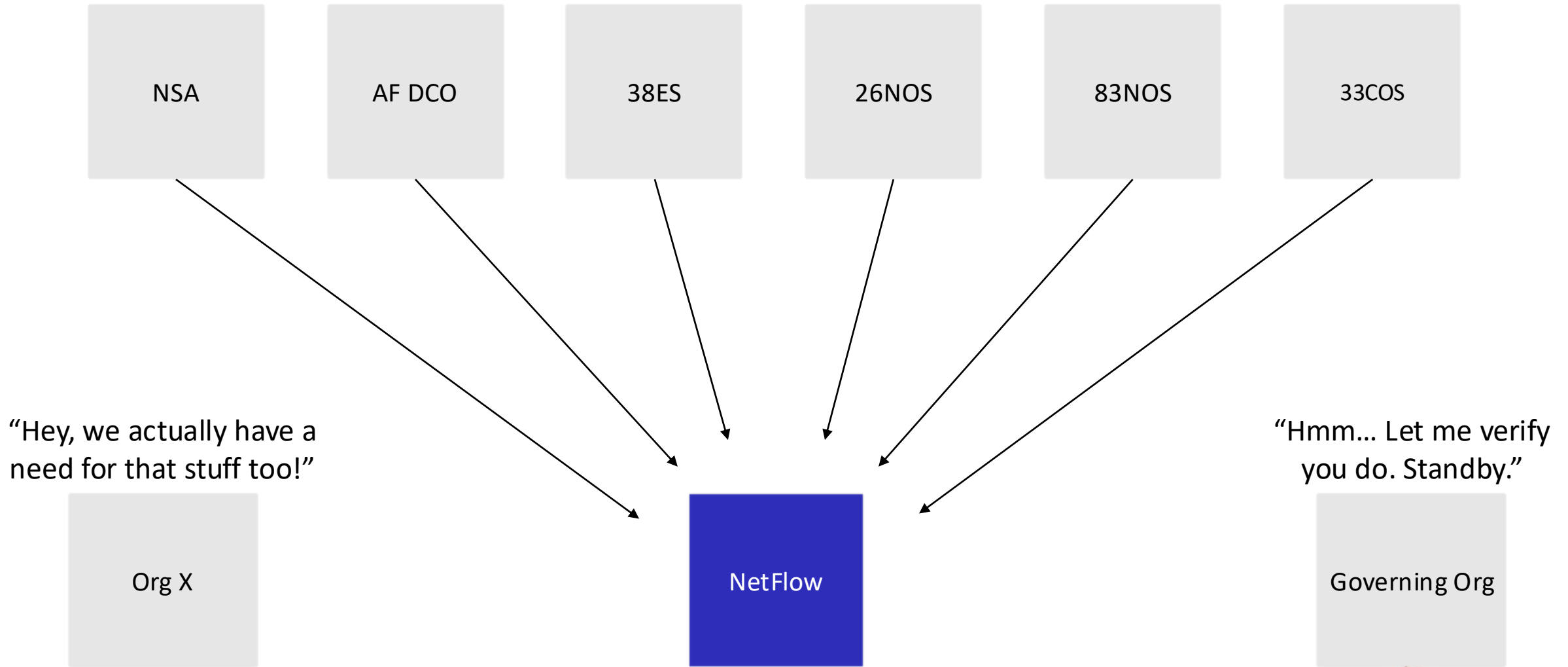


Fully Operational Capability



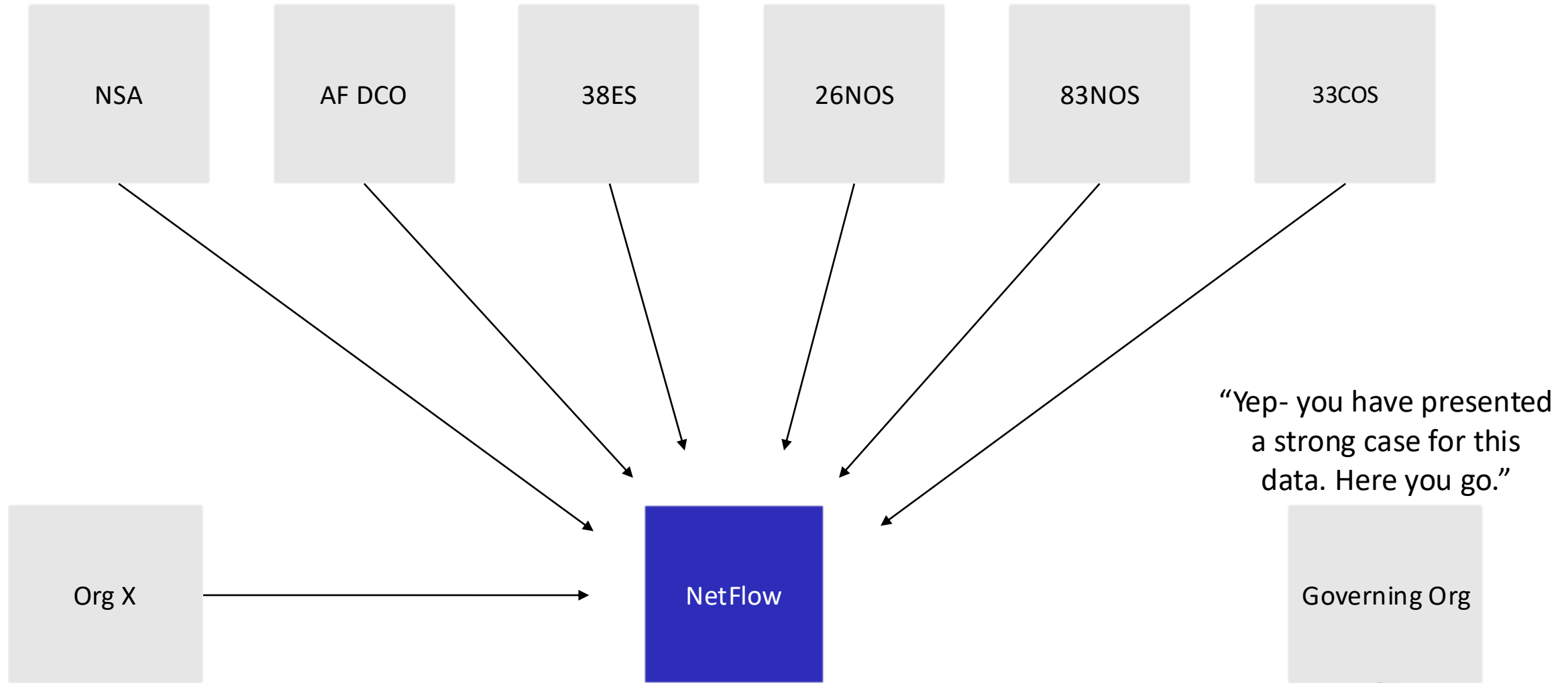


Fully Operational Capability





Fully Operational Capability

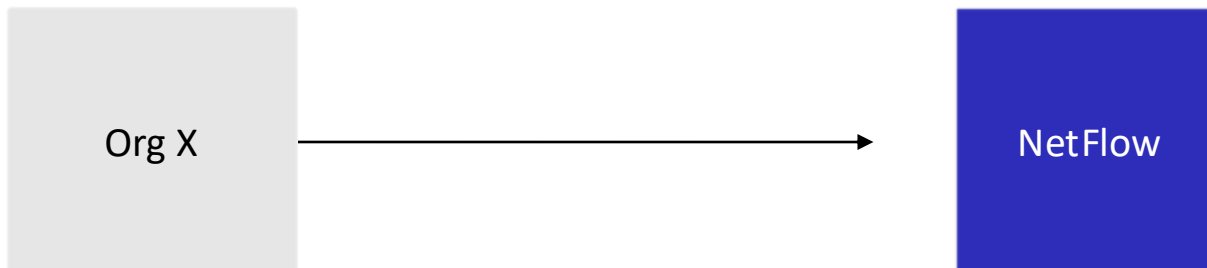




Fully Operational Capability



**0 new data collection systems funded
(unless specs of data collector now
require an upgrade)**





Rolling This Out



1. General query, one data type/protocol at a time: *Who is collecting X data source at this time?*





Rolling This Out



1. General query, one data type/protocol at a time: *Who is collecting X data source at this time?*
2. Receive an insane number of responses, begin sorting
 1. Enclave
 2. Classification
 3. AOR





Rolling This Out



1. General query, one data type/protocol at a time: *Who is collecting X data source at this time?*
2. Receive an insane number of responses, begin sorting
 1. Enclave
 2. Classification
 3. AOR
3. Aggregate each respective PMO's current funding used for the data collection





Rolling This Out



1. General query, one data type/protocol at a time: *Who is collecting X data source at this time?*
2. Receive an insane number of responses, begin sorting
 1. Enclave
 2. Classification
 3. AOR
3. Aggregate each respective PMO's current funding used for the data collection
4. RFI to private industry for a single system capable of supporting this data plane





Rolling This Out



1. General query, one data type/protocol at a time: *Who is collecting X data source at this time?*
2. Receive an insane number of responses, begin sorting
 1. Enclave
 2. Classification
 3. AOR
3. Aggregate each respective PMO's current funding used for the data collection
4. RFI to private industry for a single system capable of supporting this data plane
5. R&D





Rolling This Out



1. General query, one data type/protocol at a time: *Who is collecting X data source at this time?*
2. Receive an insane number of responses, begin sorting
 1. Enclave
 2. Classification
 3. AOR
3. Aggregate each respective PMO's current funding used for the data collection
4. RFI to private industry for a single system capable of supporting this data plane
5. R&D
6. PMOs shift budget to governing body. Savings go back to PMOs! (minus additional funding for manpower to support the governing body)





Limiting Factors



1. Requires a governing body... CDAO? HNXX? Personally vote CDAO





Limiting Factors



1. Requires a governing body... CDAO? HNXX? Personally vote CDAO
2. Does not extend to tools that leverage the data for visualizations, SIEM, SOAR, etc.
 1. Could in theory, however the argument loses considerable footing to do so (Less overlap in organizations' requirements, e.g. visualizations)





Limiting Factors



1. **Requires a governing body... CDAO? HNXX? Personally vote CDAO**
2. **Does not extend to tools that leverage the data for visualizations, SIEM, SOAR, etc.**
 1. Could in theory, however the argument loses considerable footing to do so (Less overlap in organizations' requirements, e.g. visualizations)
3. **EITaaS & Data Ownership: Still a very large unknown**
 1. **Not a kick at EITaaS! It's simply a question we haven't figured out an answer to yet. If a vendor says "we can sensor, monitor, and operate our own site tyvm", what happens next?**





Limiting Factors



1. Requires a governing body... CDAO? HNXX? Personally vote CDAO
2. Does not extend to tools that leverage the data for visualizations, SIEM, SOAR, etc.
 1. Could in theory, however the argument loses considerable footing to do so (Less overlap in organizations' requirements, e.g. visualizations)
3. EITaaS & Data Ownership: Still a very large unknown
 1. Not a kick at EITaaS! It's simply a question we haven't figured out an answer to yet. If a vendor says "we can sensor, monitor, and operate our own site tyvm", what happens next?
4. There may be more! What do you think?





Continue Discussion



38ES & HeptagonIT Bakeoff occurring right now: Baselineing NetFlow and PCAP

- Elastic
- ExtraHop
- Gigamon
- NetScout
- Riverbed
- Splunk

Minimum Goal: Evaluate products in tandem to save time, effort, and disseminate information regarding these COTS vendors

Hopefully and Probably: Discover mission partner organizations have very similar data needs as us at the 38ES UX/PM COE

Ideally: Come to an agreement between our respective PMOs and joint-fund a system to collect PCAP and/or NetFlow





Presentations < Discussion



If you represent an Air Force entity and would like to pursue opportunities in joint efforts regarding data acquisition as opposed to system acquisition, please speak to me offline.

