



Impact of Digital Transformation to Existing Air Force Structures

DAFITC Education & Training Event
August 2023

Presented by:

Colonel Michael Medgyessy
AF Intelligence Community (IC)
Chief Information Officer (CIO)





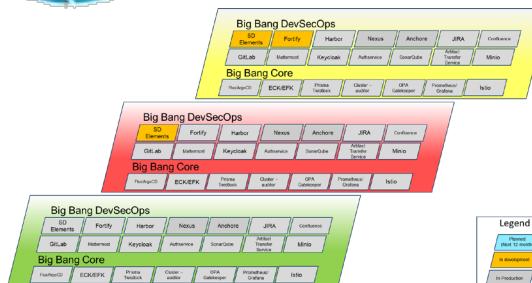
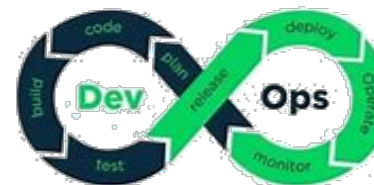
Non-Endorsement

Reference to any specific contractor, company, products, processes, or services by trade name, trademark, manufacturer, non-government entity or otherwise in the presentation does not constitute or imply its endorsement, recommendation, or favoring by the Government.

What is Digital Transformation?



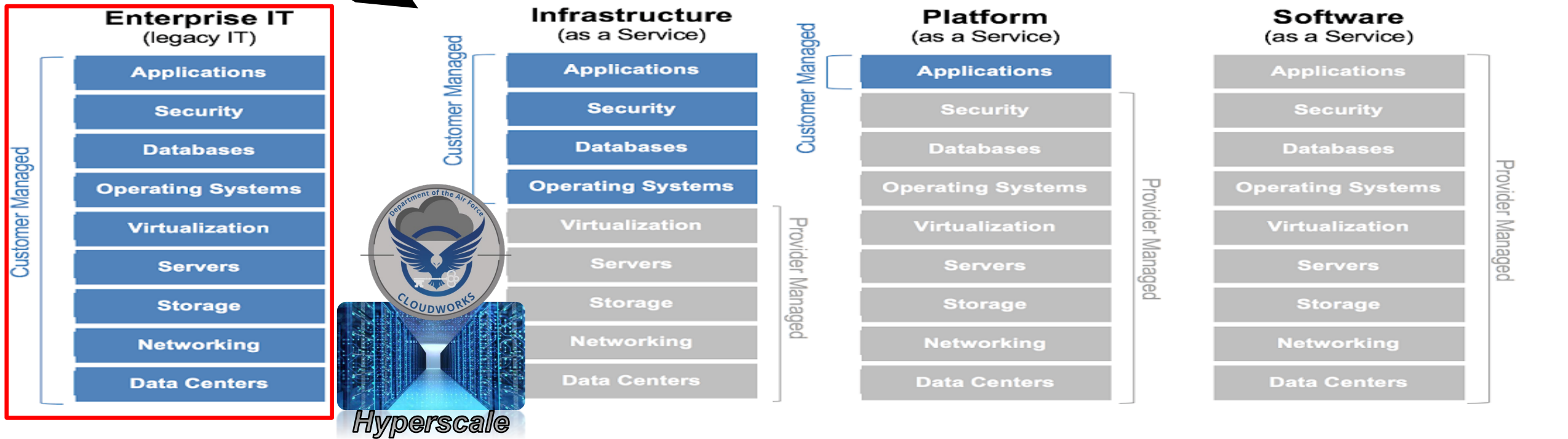
Infrastructure as Code (IaC)



Software Defined



Msn Apps



What is Digital Transformation?



Transformation is NOT an Iterative Improvement for Information Technology



- IT Workforce Roles
- IT Finance Methods
- IT Acquisition Methods
- AF IT ORG Structure Roles
- IT Delivery Processes
- IT Security Processes

What Has Been Done Different in Your Org



...the Department of Defense's (DoD's) ability to adapt and respond to these threats is now determined by its ability to develop and deploy software to the field rapidly.

-Defense Innovation Board, 21 March 2019

Executive Order 14028, directing accelerated movement to secure cloud services and emphasizing the importance of commercial relationships.

“Unless the requirements, budgeting and acquisition processes are aligned to permit faster and more targeted execution the US will fail to stay ahead of our adversaries.” (Taken from the article ‘**Why DoD is so bad at buying software**’
– Lauren C. Williams Nov 08, 2021 NSCAI report) -

DoD must provide reusable automated design patterns, such as Infrastructure as Code, Compliance as Code, and hardened software containers, to ease the burden required in standing up and configuring virtual development environments. –DoD Software Modernization Strategy

*‘Agencies are struggling with how to utilize existing acquisition methods to acquire cloud services that use consumption and rate-based business models. Cloud computing presents an enormous paradigm shift from the usual acquisition model for acquiring traditional Information Technology (IT) services. The current mechanisms of **Federal funds systems** work directly against the intended business advantages of cloud computing. **This is the most impactful issue facing the Federal Government with cloud computing.** While there are other disadvantages in the current Federal structures, they generally have a much lower impact than funding constraints*

-Excerpt for the DoD Cloud Acquisition Guidebook for reference

What is Digital Transformation?



Democratization Phase Shift



By 2024, 80% of Technology Products and Services Will Be Built by Those Who Are Not Full-Time Technical Professionals.

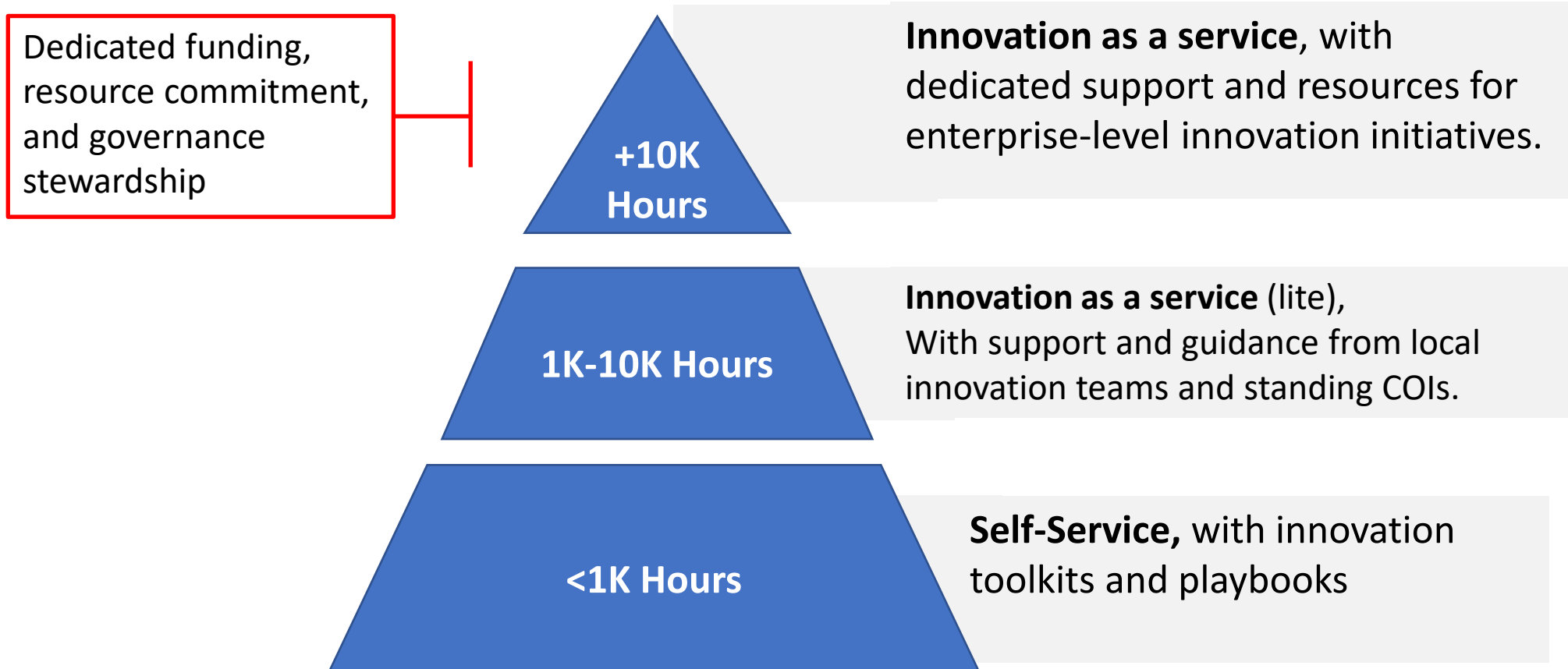
Gartner

What is Digital Transformation?



Right-size Central IT Support for Business-led Innovation

Tier IT Participation by Level of Business Effort- Example model from a major US bank below:



Workforce Trends



- IT was for IT specialized people to work with - Military was where you went to work on expensive hard to find things like mainframes for skills
- Most jobs started to require use of IT and tech skills especially white collar
- Tech skills become general education to include coding for young students
- Use of computers starts in single digits of life and integrated into adult daily living
- Workers expect to be able to automate their work themselves
- Low Code/No Code spreads development of capability to average users
- Average new hires are familiar with building applications and use of cloud services to solve problems
- IT professionals look for challenging new tech usage not challenges with running old tech in a modern world



What Does this New IT Service Delivery Look Like? (compared to how we do it now ‘piece by piece’)

By 2024, nearly 60% of IT spending on application software will be directed toward cloud technologies.

(2022 Tech Trends)
Gartner

IT Delivery Process



Start: Mission Area has a Funded IT Capability Requirement

Legacy IT:

- Leadership support send requirement to MAJCOM for validation and prioritization in 1067 requirement process
- Study done by PMO, engineering, and units affected for O&M to decide scale, priority, and resourcing requirement
- Placed in queue for PMO acquisition and change management process
- Acquisition strategy, contract creation, security team involvement for accreditation
- Hosting location identified and delivery of hardware, install, configure, secure
- Build virtual machines, Network IPs, add to VLAN, DNS, certificates, add security products, STIG, patch, join to domain, add security groups, adjust firewalls, integrate logging
- Accreditation work
- Troubleshoot, test, maintain
- **~Years** from requirement to capability

Digital Infrastructure:

- Funded requirement owner onboards at cloud office with requirement- ~days
- Hardware needed already delivered, configured, accredited and ready providing full development, test, and production environments once accounts are built ~a day
- IATT after short 30 questions answered ~ a day
- Full access to over 60 cloud provider enterprise services at all classifications, numerous cloud office provided enterprise services, inherited accreditations – 0 time
- Automated processes to bring in commercial software of newly created software capabilities- team will help ~depends on complexity ~weeks
- Using max available already accredited services on the platform a new capability can be put in production in as short as **~2 weeks** post MIPR or Form 9 money transfer given strong tech team for the project
- Capability and security updates **measured in hours** some with multiple a day changes put into production- on customer team
- CI/CD



As a Service Model



Acquisition Issues Continued

- **ACC A2 Tools Teams**
– partial answer,
best practice
 - **Smoke Jumpers, Unicorns**
 - **Mission depends on apps which can come and go-how to deal with this reality**



Finance Changes Needed



All
money, is
not good
money...

Sorry wrong color!

The Money Is No Good

Organizational Structure Challenges



Corporate ORG Structure Roles Change **We are Talking Transformation not Simply Evolution**

- Impact of DevSecOps model and software vice hardware
 - No handoff to a sustainment unit or O&M squadron
 - Developers are the support for the production products
 - Environment is constantly changing, can be multiple times a day even constantly
 - Continuous Integration and Continuous Delivery automated pipelines remove most human involvement in deploying changes to the environment
 - Outsourced as a service cloud model means the military no longer does that work
 - No ISS, No NOSC involvement in providing underlying comms which have been outsourced
 - There is no military training pipeline or one being developed to support this work
 - AFMC not ACC is lead for outsourced comms through acquisition program offices
 - Responsibilities and roles shift from the traditional organizations to new ones
 - Some orgs like AFRL are uniquely suited to perform the mission where no other unit can for numerous reasons

How we always did things in the past is no reason to shoe-horn our future into that old way

Traditional Org Structure



- HQ: POM-Strategy-Architecture-Policy –Congress sends IT dollars with Program funding not centralized under CIO control
- Lead MAJCOM: OT&E, Requirements, Operational Oversight
- AFMC: PMO- Sustainment – Procurement
- NAF: Wing-Group- Squadrons Operate and Maintain

Breaks Down with Agile DevSecOps and metered as-a-service Cloud Service Delivery

Why Traditional Org Structure Doesn't Work



- DevSecOps- No Handoff to sustainment or operational orgs
 - Dev team is the production operations O&M team as well
 - Cycles go between dev and prod multiple times a day
 - RDT&E to O&M constant mix, mostly funded with RDT&E
- Shift from ACC to AFMC providing preponderance of IT capabilities
 - Outsourced IT provided as a Service means we no longer do those things ie. OT&E
 - Software Factories- provide agile mission capabilities to customers using the below
 - Cloud offices
 - Enterprise Services and Security
 - DataOps (data platforms), MLOps (AI platforms), DevOps (K8s platforms)
- HQ providing direction to enterprise service providers- Flat and Fast
 - Chief Info Officer, Chief Tech Officer, Chief Data and AI Officer, Chief Software Officer, Chief Info Security Officers direct to AFMC orgs
 - No 16th AF units and No ACC directorates really involved in service delivery

Why Traditional Org Structure Doesn't Work



Required Speed, Scale, & Agility

- Can't continue to provide IT as we have and meet the needs
- SecAF to Operational Imperative Structure –shifted from MAJCOM lead to HQ lead for POM out of necessity
- Integrating PEO C3BM direct report to Secretary
- New industry leaders injected into key HQ leadership positions to lead strategic to tactical as SMEs needed in transformation
- Capabilities provide the ability for majority of IT solutions to be produced outside the IT department control
 - Gartner-80% of IT solution across industry are now produced outside IT departments
 - Workforce shifted from IT using computers, to all jobs using computers, to all employees empowered to create IT solutions for their jobs
 - How does our structure deal with this fact of life now?

Day 2 Operations / Site Reliability Engineering



- Traditional Enterprise Service Providing units under 16th AF
 - Future decrease in mission specific networks and increase of mission on base networks
 - Due to Cloud accessibility of systems and Zero Trust
 - SaaS apps need a marketplace and tools teams
 - Track what is being used latest, how to add to funding to gain access to requirements and backlog priorities, mitigate risk to sudden disappearance
 - Integrate coders at the edge for seamless small feedback loops to the SaaS DevSecOps teams
 - Support Airmen Coders with tools and guardrails to work inside with connections to software factory teams and tools teams
 - SRE work force
 - Measuring mission application useability and constantly improving experience
 - Help Desk interface between users and developers
 - CSSP as a Service vice each having its own

Integrated vs Separated

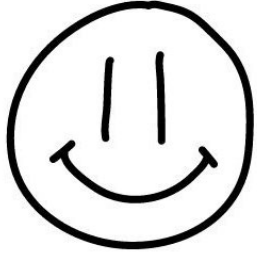


Building Solutions Together; not Passing Requirements

**USER CENTRIC VS
USER DRIVEN**

WHO IS DRIVING THE PRODUCT?

USER CENTRIC	USER DRIVEN
	
Go Somewhere New Together	Go Where The User Tells You To go
Discover Solutions Unknown End State	Limits Solutions Known End State

 USER CENTERED	VS	 USER DRIVEN
1 Talk to me about how you use...		1 What are your pain points?
2 Can I watch you use....		2 What features would you like to see?
3 How much time do you spend...		3 Can you prioritize our backlog?



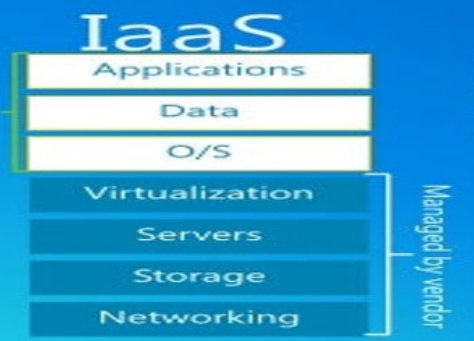
“Traditional” Waterfall vs. Agile: General Mindsets and Practices



“Traditional” Waterfall		Agile
<u>Scope</u> ; not Time and Cost	★ Fixed	Time and Cost; <u>Not scope</u>
Completely defined in detail up-front; resists change; Tries to be predictable	★ Requirements & Estimation	Iteratively refined during development; welcomes change; Accepts that total predictability in software requirements is impossible
Detailed cost estimates and full funding	Risk Reduction	Incremental releases and sprints
Early, large, and document-intensive	Reviews	Small, frequent, and often informal
Process and documentation over people	★ Emphasis	Knowledgeable, empowered teams/people and delivered code
Detailed plans freeze solution early	Baselines	Adapted to new info learned throughout development
At end of an increment (years)	Delivery	At end of a release (months)
Earned value measures and conformance against plan	Measurement	Frequent capability deliveries; value to the customer
Independent, following development	★ Testing	Daily development, integration, test
Acceptance at end of increment	★ Users	Active for continual review and feedback
Hierarchical, command-and-control, formal structures; difficult to change; IPTs	Org Structure	Flexible and adaptive structures,
Leader as keeper of vision; primary authority to act	Leadership Style	Facilitative; champion and team advocate
Top-down; documentations; indirect	Communication / Decision Making	Daily stand-up; face-to-face; retrospectives; info radiators

★ Key DoD Friction point

Agile misinterpretations: **no documentation, no process, no plan...**
...successful Agile implementations: **look for *balance*, not extremes**



Infrastructure as a Service (IaaS)



<Somebody else's computer>

Legacy IT

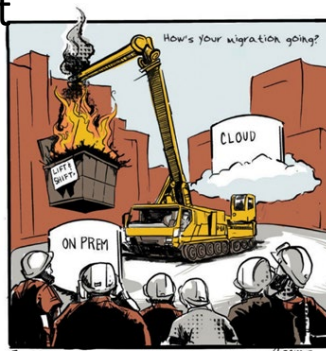
- Find empty available datacenter space with capacity
- Estimate capacity requirements to grow into over the next five years until tech refresh to procure
- Find a contract vehicle or build one to acquire capacity for network, compute, and storage or fund growth to virtual hosting cluster as needed
- Contracting timeline
- Equipment delivery timeline
- Engineering of change requests and approvals, prioritization for execution
- Install, configure, integrate, secure, test, accredit
- Add to equipment inventories, logging, add to maintenance workload
- Provide to customer for use

Start Building ~year(s)

Digital Infrastructure

- Onboard with Cloud office
- Get added to an existing task order and provide funding
 - Setup IATT or CtF for proposed work
- Done- Days
- Build new task order
- Get accounts

Start building ~4 months



Infrastructure as a Service (IaaS)



Ways to Use

Someone Else's Computer:

- Run your virtual machines in a commercial cloud provider
- Get automatic tech refresh
- Increased resilience and performance
- On demand elastic capacity
- Access to Cloud Native Services

Infrastructure as Code:

- Ruthless automation
- Serverless computing
- Usage of Cloud Native Services



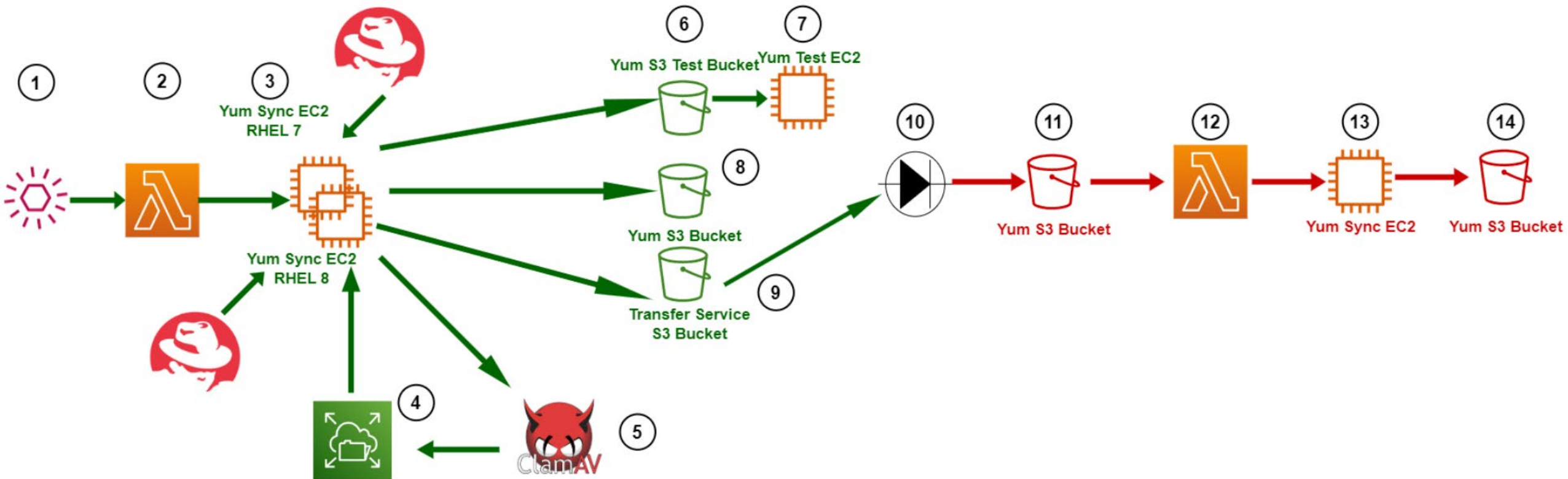


How Does That Look?

If you do something more than 3 times, make it code.

(We run on three classifications so everything actioned is worth converting to code)

Gold AMI (Windows & Linux Twice a Month)





Platform as a Service (PaaS)

What in the world is this?

- The platform is run by a team maintaining capabilities used in common across tenants vice each tenant building, securing, and maintaining those common services each time in a stack of their own- Unique services provided to Dev teams from the government cloud office
- As the platform continues to mature additional services are being added for both containerized micro service-based workloads and IaaS based monolithic legacy applications
- Inherited Common Control Packages for Accreditation, CtF pipeline and repository
- ***Common terms and functions:*** CI/CD pipelines, Gitlab runners, AGILE DevSecOps, IaaS+, Cloud native services and applications, serverless, micro-services, SaaS applications

Platform as a Service (PaaS)



Build Once, Configure, Secure, and use Pay-as-You-Go Services



Security Services

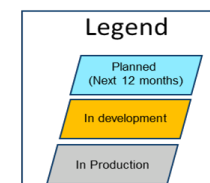
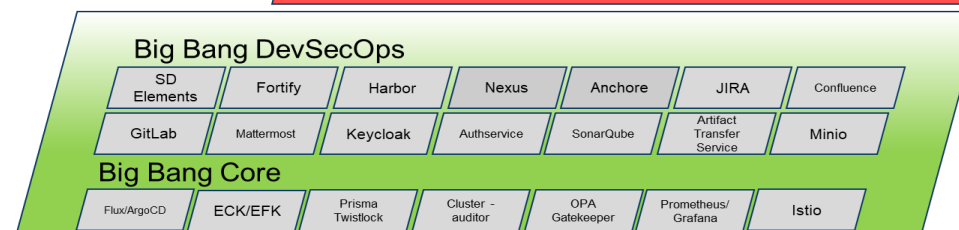
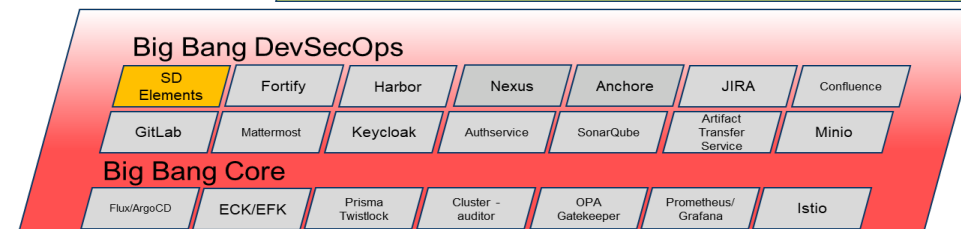
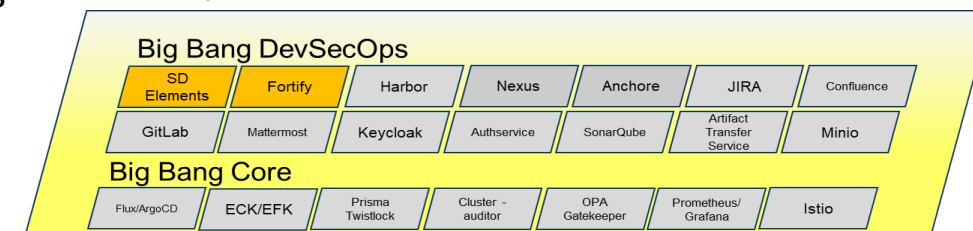
- ClamAV
- ACAS
- ECE –logging/auditing
- Gold AMI x 2 monthly
- AWS Directory Services

Enterprise Services

- YUM
- DNS (local and public)
- PKI
- ICAM (Keycloak, Geoaxis, AccessIT)

Software Factory

- Diode Transfer Service
- Collab Tools (Mattermost, JIRA, Confluence, Gitlab, etc)



ODIN Services



- | | |
|------------------------------------|--|
| • Flux/Argo CD | ✓ Automated Deployment tool |
| • ECK/EFK | ✓ Logging/monitoring aggregation of logs |
| • Prisma/Twistlock | ✓ Vulnerability Scanning |
| • Cluster Auditor | ✓ GOTS. Enforcement of OPA policies |
| • OPA Gatekeeper | ✓ Policy enforcement |
| • Prometheus/Grifana | ✓ Manage costing, sizing, limits, CPU, memory |
| • ISTIO, Kiali, Jaeger | ✓ Service mesh, routing, segmentation, mTLS |
| • Gitlab | ✓ Source code repository, CI orchestrator |
| • Keycloak, GeoAxis | ✓ Identity, and Certificate Access Manager |
| • Auth Service | ✓ Authenticates mission apps to Key Cloak |
| • Sonar Cube | ✓ Code quality, ensures good coding practices |
| • DIODE, artifact transfer service | ✓ Cross domain as a service low to high |
| • Minio | ✓ K8S storage tool- abstraction to work with all kinds of storage products |
| • Fortify | ✓ Static code analysis, dynamic, code analysis, vulnerability checker |
| • STIG enabled | ✓ OS and K8s lock down, Open SCAP |
| • Nexus | ✓ Multiple coding language libraries for classified networks |
| • Anchore | ✓ Container scanner prevents additions to Docker files post approval |
| • SD Elements | ✓ Survey tool for cyber security team checking planned app architecture |
| • Velero | ✓ Database backups |
| • Flux | ✓ Ensures apps stay running through failures |
| • D2IQ | ✓ Version of Kubernetes for container orchestration |
| • Harbor | ✓ Registry which signs secure software artifacts |

Data & AI/ML Platforms

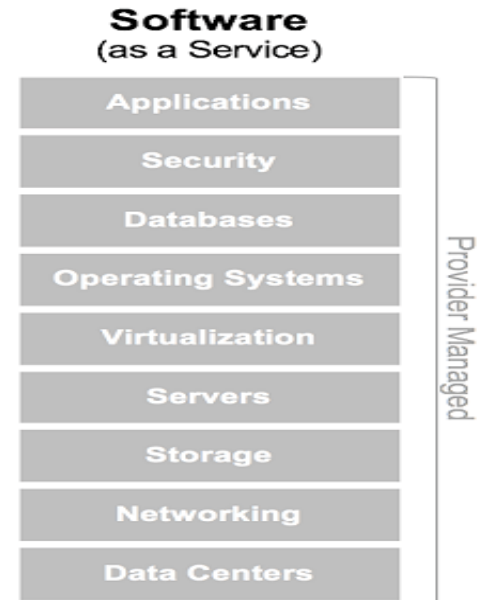


- Big Data Platforms have DevSecOps pipelines and services that focus on common data layer services and user interfaces to them using IaaS, PaaS, and SaaS internal to data services integrating with external data and applications –ie ETLs using things like HADOOP, Collibra, etc.
- MLOps platforms have DevSecOps pipelines and services harnessing IaaS, PaaS, and SaaS services which are common to AI/ML activity- ie RedForce, DragonSpell, Maven, MAGE using things like Inference engines, GPUs, Tensorflow
- Apps, Data, AI/ML all integrate together to provide modern capabilities to the warfighters and analysts with industry standards and best practices made globally available with resilient software defined networks

Software as a Service (SaaS)



- Web apps available globally through a modern browser
- No tie to a specific domain or network just classification- ~~mission-LANs~~
- Bring your own data, you just have an account
- Examples: Mission apps like Ripsaw, Radiance, C2D2, Big Data Platforms (ELICSAR, UDL), Project IKE, or collaborative tools Confluence, Mattermost, JIRA, Gitlab, m365, etc.
- This is where MAJCOMs, NAFs, functional communities, WepTac, units get involved with requirements and TTP development for use- Tools teams, unicorns, Smoke Jumpers, combat coders, Agile feedback loops



What About Networks?



- Moving to Software Defined LAN and WAN technology and black network transport is an iterative upgrade and part of the total transformation
- Underlying dependency and important activity
 - Focus for ABMS, AOC, DCGS, ACC, 16th AF
 - Why? Government owned, government integrated capability plugs right into current units and workforce doing work with some new training
 - This Line of Effort is much easier to understand for the current IT service delivery methodology
- Also being disrupted with Cloud providers Content Delivery Networks, Direct Connect Circuits, Edge as a Service
- Cloud based apps and data are accessed best direct from NIPR, SIPR, JWICS
 - NOT a mission network which used to hold apps and data required for specific computers on a specific network with specific logins
 - Along with Zero Trust implementation – **Mission specific networks are a thing of the past!!**

What About Security?



- New RACI chart where security responsibilities are broken out depending on how much you pay to have done for you vice doing yourself
- Security professionals need to understand how to read the code running in Gitlab repositories
 - Serverless compute has compute and store spun up for an instant and disappear after execution
 - Elastic infrastructure balloons and reduces on demand- no tracking assets with spreadsheets, machine names, IPs
 - Environment is so fluid that only through understanding the policies and code used to launch can you understand the security of the running environment
 - Accreditation can be as easy as a few questions or a full package depending on what is chosen by the customer to be on them
 - Inheritance and reciprocity agreements are essential
 - CSSP in the cloud needs to be as a service and scaled out with contractors
 - Completely different tooling for the vast majority of capability
 - Zero Trust technical stack is completely different than legacy on-prem architecture
 - Zero trust is a whole presentation in itself and how it works in the cloud

Questions to Ask Yourself

The world around us changes increasingly fast, so we must also change to stay relevant

- AF level org redesign required:
 - What MAJCOM has the software factories running mission applications?
 - In DevSecOps where is the handoff to an operational IT squadron for applications in production?
 - What “color” of funds do you normally get to buy new solutions?
 - How can you scale your solutions on demand up and down with funding quickly?
 - What new Cloud apps and capabilities are out there we could capitalize on as well?
- Data actually treated as a strategic asset:
 - Who are your data owners, stewards?
 - How does an external source get access to your data?
 - How do you access data you need?
- Upskilling:
 - How do you automate your routine tasks? If you perform a task 3 times automate it
 - What are Airman Coders? What is the difference in an application development and scripting?
 - When my Airmen come to me with a request to automate their work how do you support them?
 - Office products with flat files are difficult to mine for data and reuse. Flat files become obsolete in minutes. What real-time dashboards are using to contextualize your data needs for decisions and action?
- What are the new things we could never do before because we were doing the work that computers do for us now?
- As the pace of technology change increases, the generation after this will recognize our way of life less than the previous one does