Headquarters U.S. Air Force

Integrity - Service - Excellence

DAF IC Digital Infrastructure

Cloud Focused Presentation

Colonel Michael Medgyessy

Department of the Air Force Intelligence

Chief Information Officer
Chief Data Officer
Authorizing Official

What are these buzzwords? Why are they important?

Speed

Elastic

Hyperscale

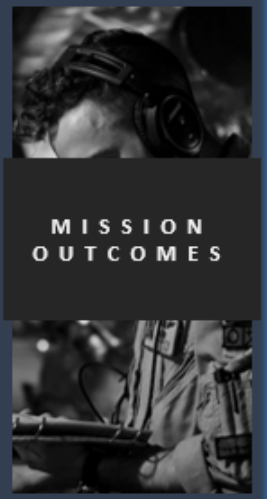
Innovation
At the edge

Enabling AI

Digital Transformation Overview

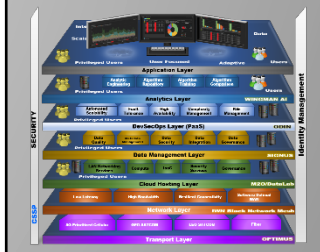
VISION

BY 2027, A SQUADRON IDENTIFIES A PROBLEM, CREATES A HUMAN-MACHINE TEAMED APPLICATION BY SELF-PROVISIONING THE COMPONENTS WITH THE BEST AI ALGORITHMS, AND OBTAINS ALL RELEVANT DATA WITH GLOBAL, FULLY ACCREDITED AND SECURE ACCESS IN LESS THAN 24 HOURS.



Data is postured for secure discovery, access, and integration between mission partners realizing data as a strategic asset	Integrated analytics and human machine teaming shorten the kill chain and improve rapid informed decision making	A mesh network suitable for DDIL operations or Agile Combat Employment (ACE) across Intel and DoD.	Commercial classified cloud platforms allow new elastic solutions as a service, deployed and used quickly, securely, and globally.	Cybersecurity risk is managed & security automation adopted to support acceleration of innovation & modernization.
SIGNUS/COGNOS/ Unified Data Library	Wingman AI	Optimus	M2O & ODIN	Cloud SOC

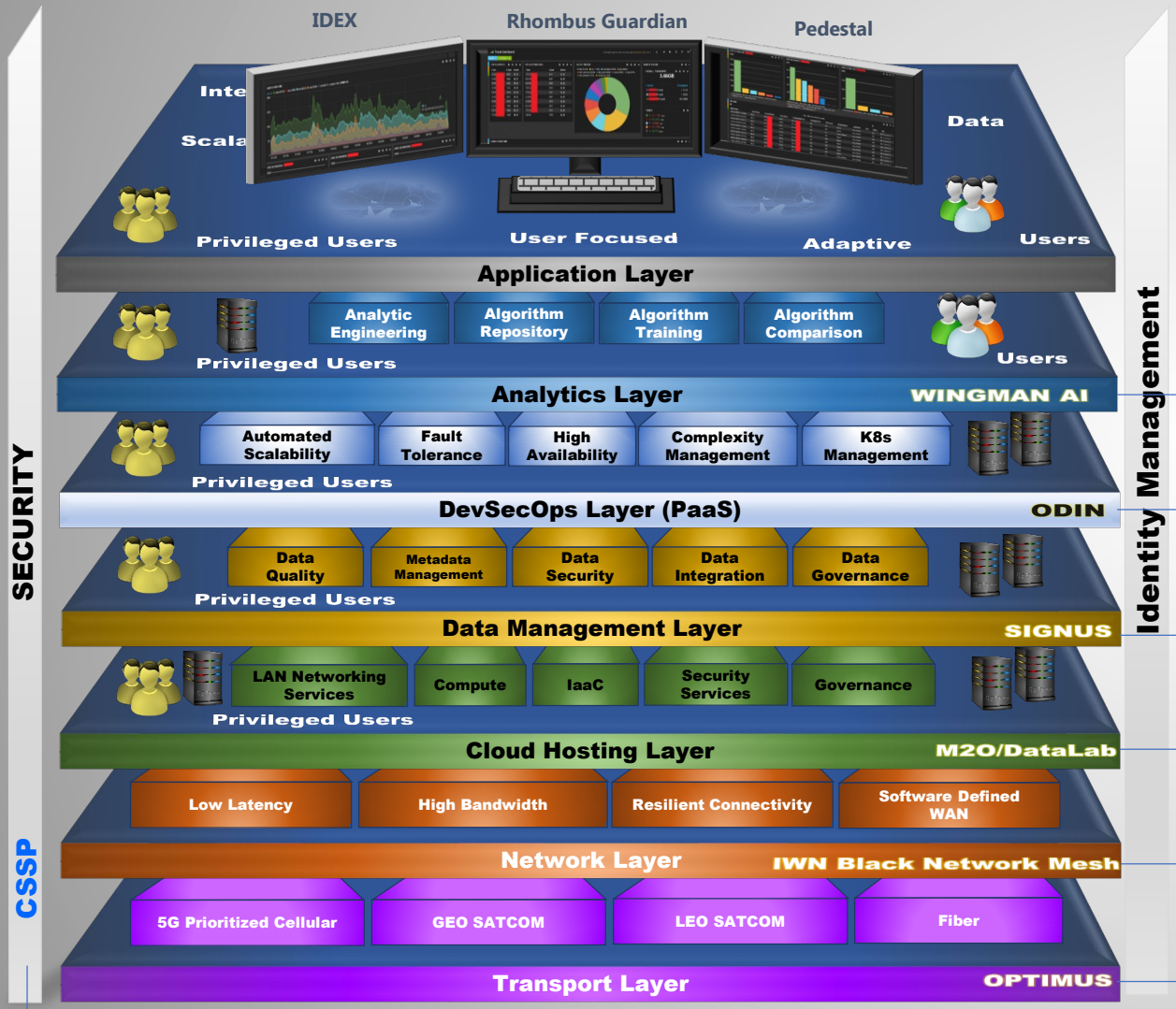
ENTERPRISE SERVICE



Current State

Data is segmented and stored in non-standardized formats. Accessibility to mission relevant data is complicated by security levels, need to know and compatibility. Interoperability shortfalls complicate enabling the decision advantage.	Independent pockets of AI/ML and pilot efforts are being leveraged to enhance portions of the mission, and significant automation/integration gaps within the intelligence process.	Network traffic is best effort, encrypted path un-optimized, quality of service not standard for real-time services, and links side by side from various owners inaccessible for sharing and inefficiency in duplicated tunnel overhead.	On-prem data centers tightly coupled behind enclave boundaries providing services organically from locally owned infrastructure purchased guessing to growth which will utilize the capacity at its fullest prior to tech refresh. Ecosystem of globally created capabilities not captured.	Reciprocity challenges lead to duplicative cybersecurity efforts to gain ATOs. Manually intensive processes demand weeks and months to secure and maintain accreditation. Visibility of cyber threats and metrics is disparate and reactive in nature.
DATA & INFORMATION	SENSE MAKING/ AAA	NETWORKS	HYBRID CLOUD	CYBERSECURITY

Enterprise Service Capabilities Today

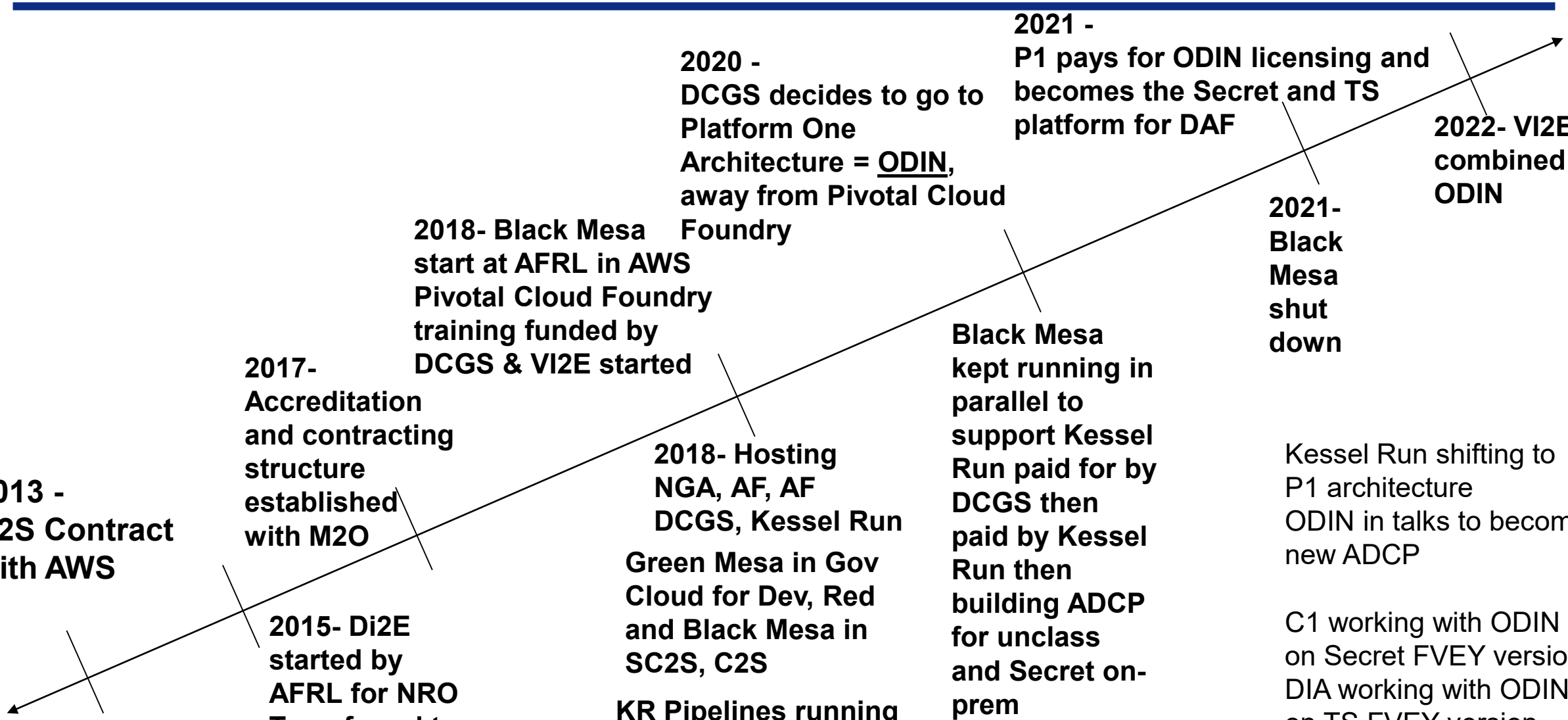


AF IC Digital infrastructure provides layers of required cloud-based services & utilities for DAF users at three classification levels

- AI/ML from Wingman AI – Platform for AI development/execution
- DevSecOps Platform from ODIN/DataLab/VI2E – Pipeline for rapid software development & operations at all classification levels
- Data Platform from SIGNUS – Brokers access to data (AF, DoD, IC) and ensures data usability by users
- C2E management by Mission Modernization Office (M2O) – Manages user access, cloud compute, & contracting for IC cloud infrastructure
- Allows shared pathways integrating IC and DAF links
- Direct Connect from Optimus – Enables source data direct connection and optimizes networks to cloud based capabilities

ATO, Cyber threat detection, prevention, & response

Where did this come from?



Kessel Run shifting to P1 architecture
ODIN in talks to become new ADCP

C1 working with ODIN on Secret FVEY version
DIA working with ODIN on TS FVEY version

DAF Cloud Digital Infrastructures

SAP EITAAS

SAF/HNJ Led

SAP Cloud Based Enterprise IT As A Service

Top Secret/SCI

HAF A2/6 Led

M2O Access to Classified Cloud
ODIN Development and Operations
Enterprise Services

Secret

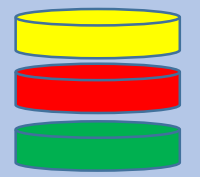
HAF A2/6 Led and SAF/CN

M2O Access to Classified Cloud
ODIN Development and Operations
Enterprise Services

Unclassified

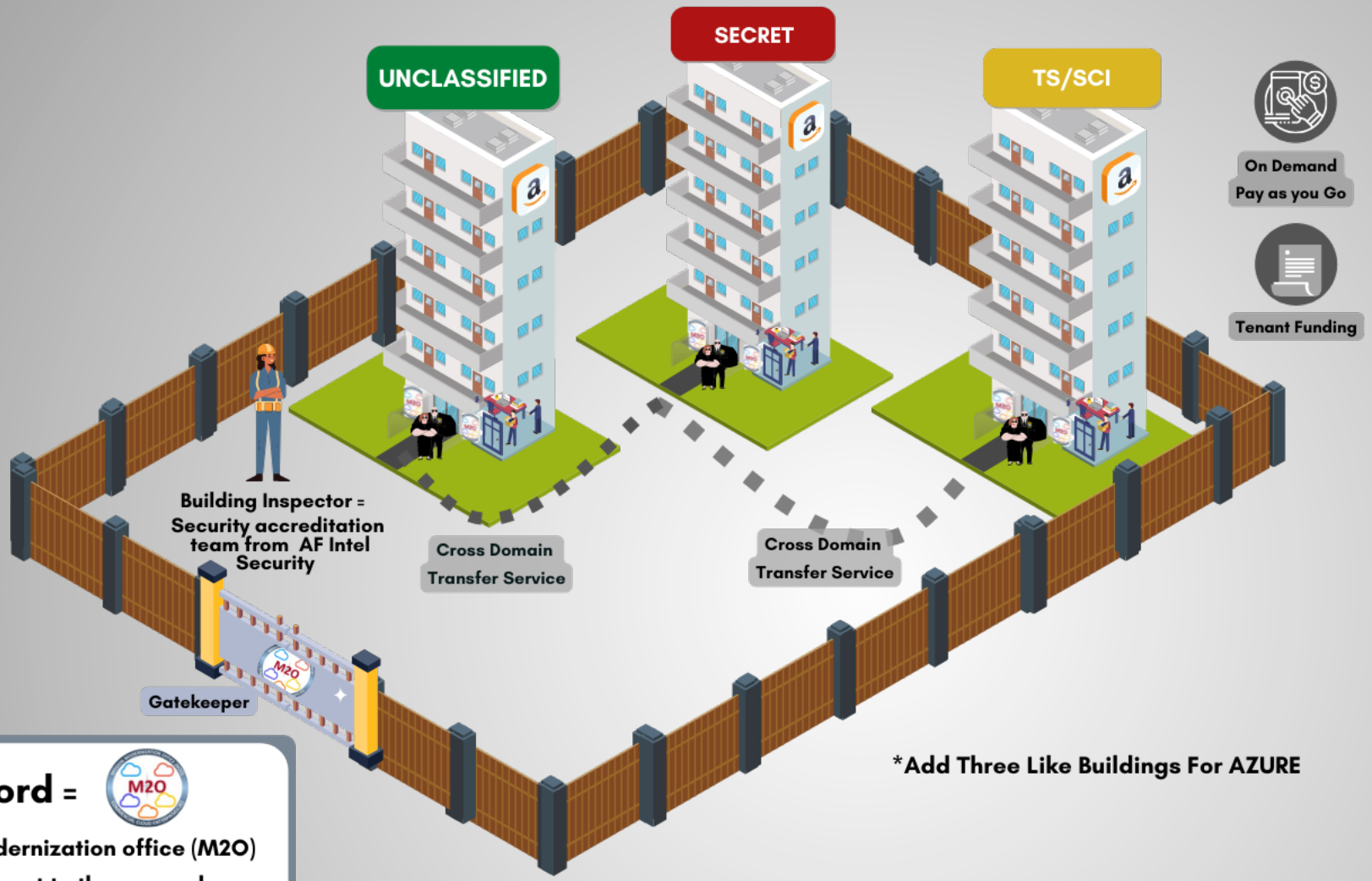
SAF/CN Led

Cloud One Access Cloud Resources
Platform One Development and Operations
Enterprise Services



Cloud Edge Multi-Tenant
Compute Nodes

*CloudOne working to build capability at Secret
**ODIN has required limited unclassified capabilities



Water & Sewer = Cloud Service Provider Services from AWS

Duke Power Electric = DevSecOps Platform from ODIN/Datalab/VI2E

Dominion Gas = Data Platform from SIGNUS

COX Cable TV = AI/ML from Wingman AI

Verizon Internet = Direct Connect from Optimus

Landlord = M2O

Mission Modernization office (M2O)

<You pay rent to these people>

Landlord → Centralized Billing → Reception → Contracting → ADT Cloud Cyber Security from 33rd NWS

Unclassified

Intelligence Community Cloud

Title 50 Cloud

Mayor DNI- IC CIO sheriff

ICD Regulations, Intel Funding

(17 Components including AF IC)

Service of Common Concern C2S contract through CIA

Department of Defense Cloud

Title 10 Cloud

Mayor SecDef –OSD CIO sheriff

DODI, DoD Funding

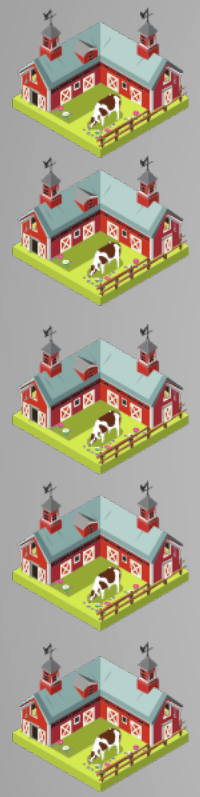
(Army, AF/Space, Navy, Marines, Coast Guard, DISA)

Enterprise Service contract JWCC through DISA

Realm of Dragons

Middle Earth

IC Data Fabric to AF Data Fabric



SIGINT

GEOINT

HUMINT

FBI

DHS

Intel Big Data Platforms X 18
Creators and Owners
(Farms)

OMNI
Central Data Catalog
(Shopping Catalog)

Common Data Fabric (CDF)
Data Broker (Supermarket)

Intel Data

DAF Data

Governance and Access
AF IC SIGNUS
(Supermarket Cooperation)

Vault
All Domain

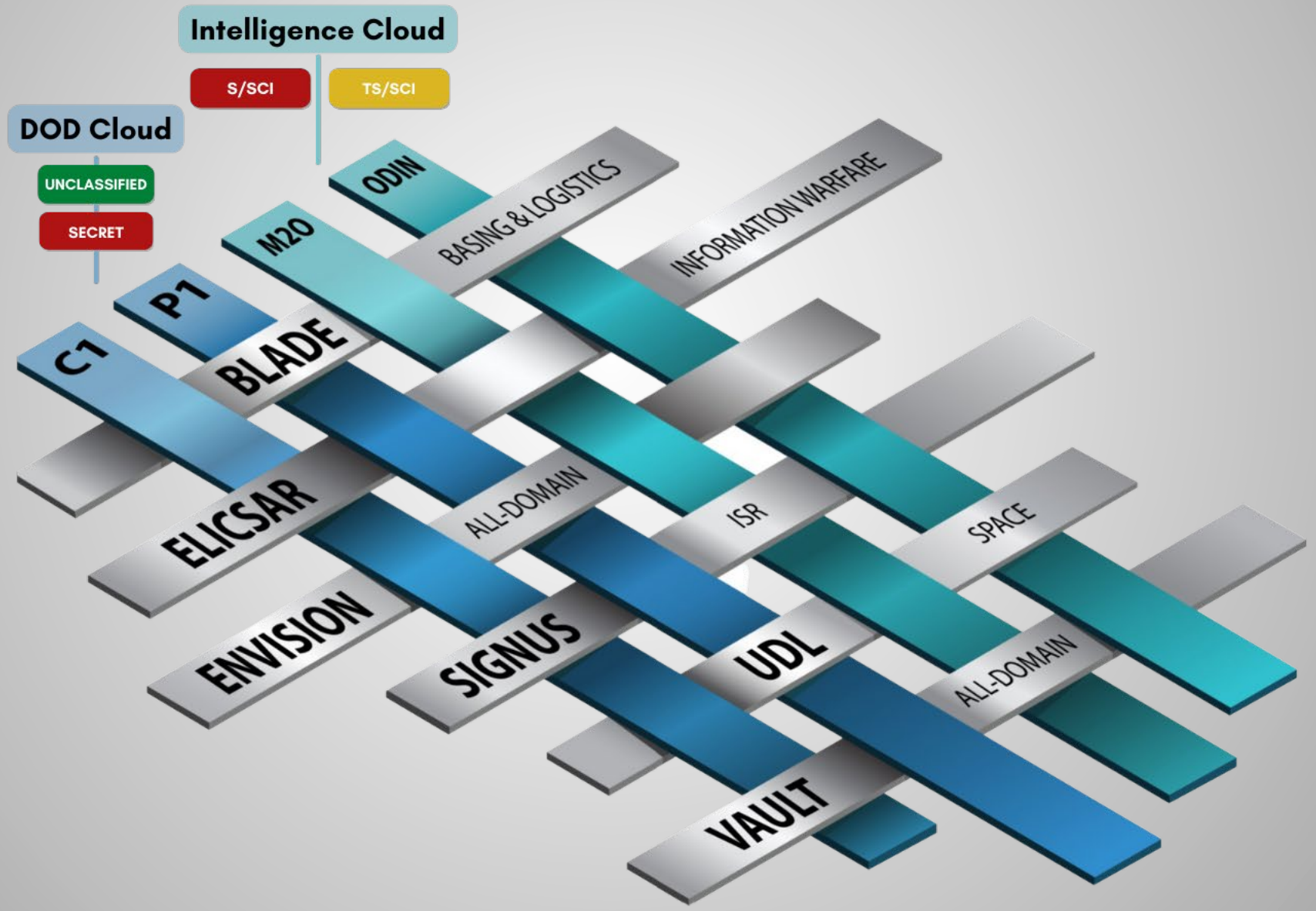
Envision
All Domain

ELICSAR
Cyber

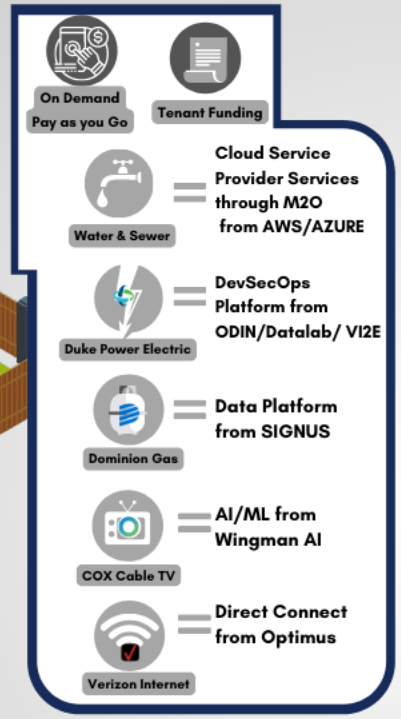
UDL
Space

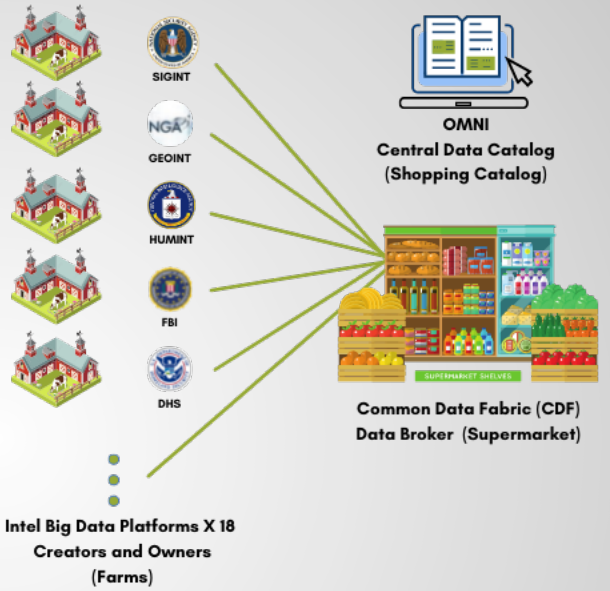
Blade
Logistics

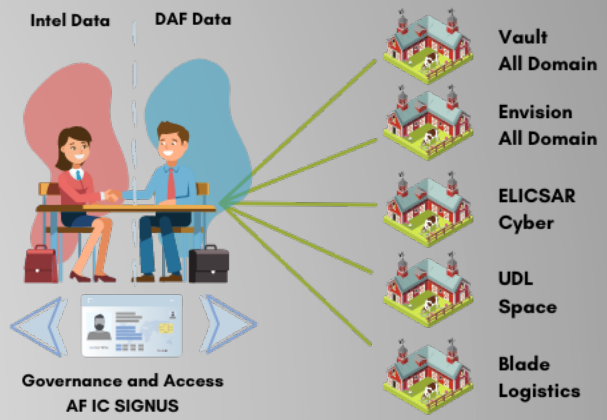
DAF Data Fabrics



Applications Analogy







NASIC is like Pizza Hut with offices in these buildings which utilize the services to produce pre-made meals which a storefront like the restaurant can provide the customers to choose from and utilize.

Warfighters and intelligence professionals utilizing capabilities from applications ready to use for their use-cases.

Deep Dive
Optimus & ODIN

- Direct Connects to Classified Commercial Cloud with Cloud Edge Nodes
- Classified Commercial Cloud DevSecOps Platform providing IaaS and PaaS

Overarching FMV Architecture Issues

- Data Quality is being degraded as it hits the ground and is transported through multiple infrastructure hops
- Algorithms are being trained to lower quality video causing confidence and accuracy issues for detections
- Enhanced technologies and data standards are not being employed across the Enterprise to meet the future requirements
- Use cases being presented today are not addressed by the current infrastructure/workflows and promotes vendor lock into legacy solutions

Project Optimus

- FMV on Secret Pilot use case:
  - Edge node processing
  - Direct data ingest to SC2S
  - Cloud-based FMV data distribution
- Architecture incorporates ML algorithms and cloud services embedded within these distributed cloud nodes across Air Force/community infrastructure
- Upstream data conditioning and direct ingest resulting in: better computer vision and the algorithms effectiveness

Future: Build on initial successes of the pilot program to expand Enterprise-wide and layer architecture with additional workflows

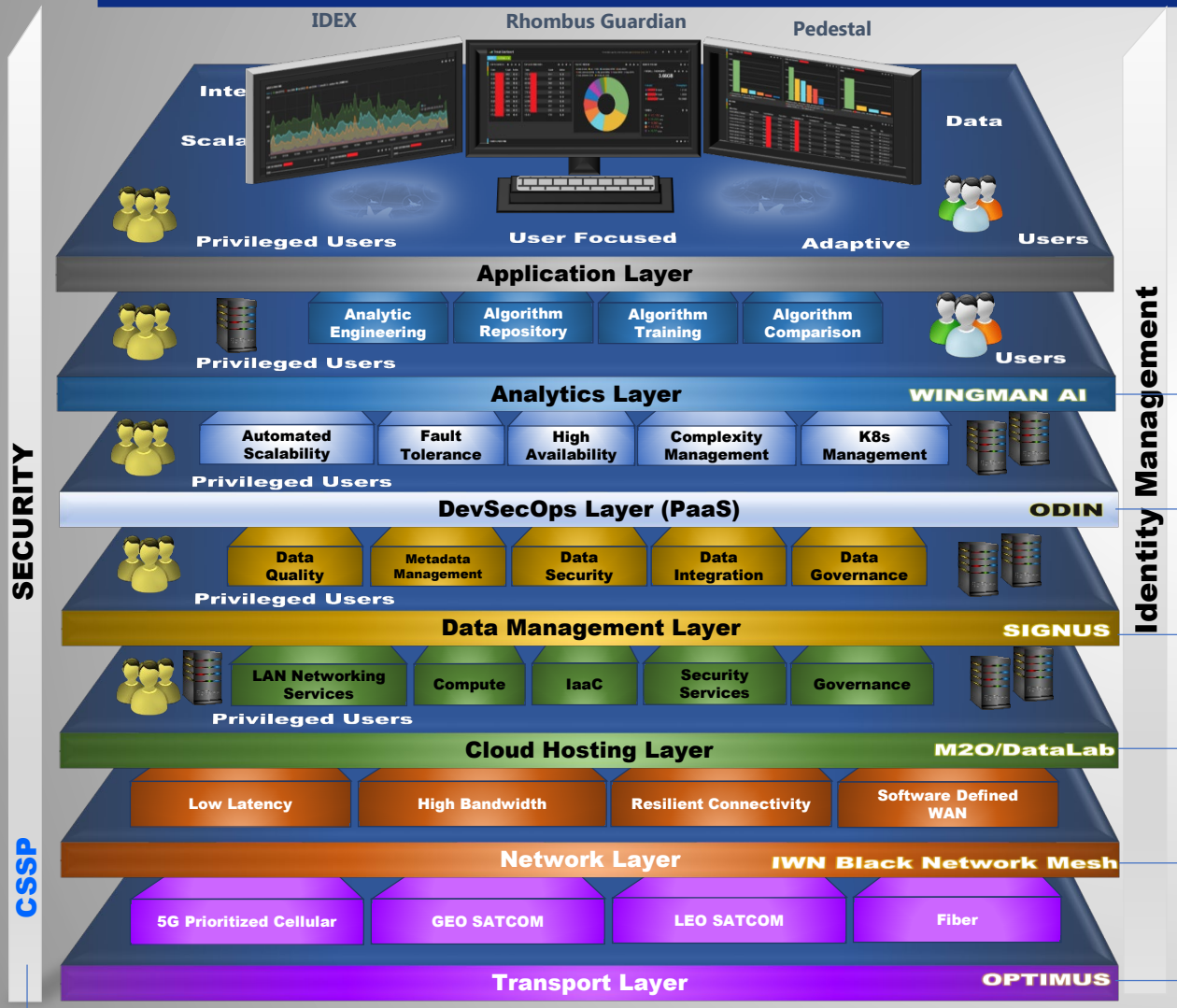
Optimus Existing Deployment and Future

- Currently a Snowball is deployed OCONUS in Europe with NGA FMV applications and Algorithms sending video across a dedicated connection into SC2S via the direct connect capability at 10Gbps
- This summer connecting in local networking to test the infrastructure disconnected from CONUS and routed to local users to continue mission in a disconnected state
- Funded to expand to Pacific this FY to stand up a similar architecture
- Next Steps:
  - Funded add TS/SCI Snowball Edge in Europe
  - Funded add Direct Connects and Edge nodes in Pacific operational by end of 2023
  - Add AF ODIN Platform at Secret and TS/SCI for multi-tenant operations of containerized applications
  - Move to a customer funded solution to deploy quickly new cases and locations
  - Integrate with AF programs and IC architectures for networks and processing (i.e. AF DCGS, AF JWICS, JREN)

Future Vision

- Bring Cloud to the Edge as a service
  - Expand edge node architecture
  - Leverage existing and emerging networks to enable global cloud connectivity to address DDIL requirements
- Utilize multi-tenancy environments to maximize integration across Services and Agencies to enable NextGen ISR mission outcomes

Enterprise Service Capabilities Today



AF IC Digital infrastructure provides layers of required cloud-based services & utilities for DAF users at three classification levels

- AI/ML from Wingman AI – Platform for AI development/execution
- DevSecOps Platform from ODIN/DataLab/VI2E – Pipeline for rapid software development & operations at all classification levels
- Data Platform from SIGNUS – Brokers access to data (AF, DoD, IC) and ensures data usability by users
- C2E management by Mission Modernization Office (M2O) – Manages user access, cloud compute, & contracting for IC cloud infrastructure
- Allows shared pathways integrating IC and DAF links
- Direct Connect from Optimus – Enables source data direct connection and optimizes networks to cloud based capabilities

ATO, Cyber threat detection, prevention, & response

U.S. AIR FORCE

USSF

Operational DevSecOps for ISR NEXGEN

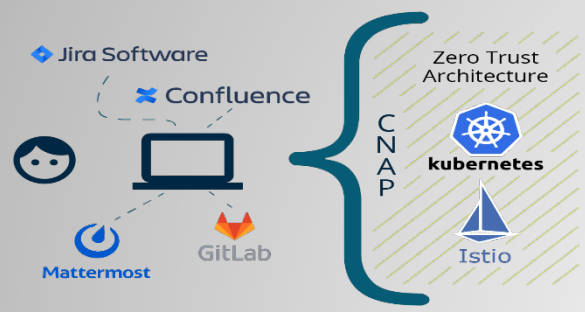
Why Is ODIN So Important?

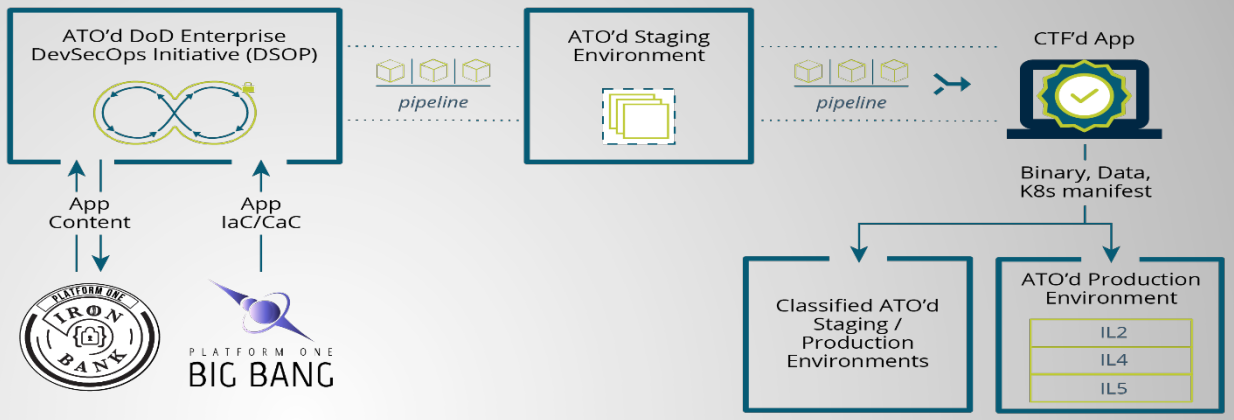
- Where does an Airman deploy new capability in classified environments using continuous integration and continuous delivery with agile methodology?
- If the US is to survive a peer conflict we must be able to harness technology and continuously integrate and deliver capability in production routinely in a day or less
  - Where do we fight? Classified environments. Where is this capability for the DAF enterprise for classified environments? ODIN
  - From requirement to solution in standard process we work measured in years, ODIN on hyperscale commercial classified cloud can bring this to minutes and hours
- Each program which could afford it was having to build and operate it's own DevSecOps platform
- There was no place a smaller effort could operate their containerized code at Secret and TS/SCI and incorporate Continuous Integration and Continuous Delivery

Where is the DAF Enterprise Platform for Secret and TS/SCI

- What Does ODIN Do?
  - ODIN is the enterprise PlatformOne based DevSecOps platform which provides IaaS and PaaS to the DAF
  - ODIN has full reciprocity with P1 Ironbank and other Dev Platforms
  - ODIN has an Unclass environment which mimicks the Secret and TS environments
  - ODIN has the transfer service to move code from low to high
  - ODIN has the ATO common controls for you to inherit
  - ODIN has common enterprise services you do not need to recreate: DNS, ICAM, Collaborative tools (Mattermost, Confluence etc), Regularly STIG'd Linux and Windows images, logging, vulnerability scanning, and more
  - ODIN has the ability to not only operate classified workloads in production but develop classified code as well
  - ODIN is moving to Snowball Edge and 3rd party Edge nodes in the near future
  - Intelligence Community ICAM integration and reciprocity agreements
  - FVEY and Zero Trust maturity coming soon

ODIN Capabilities





PaaS Environment (SIPR/JWICS)

- Platform One Party Bus
- Enables customers to focus on mission app development and delivery without worrying about infrastructure or management of hosted environment
- One-stop shop for specific mission needs with P1 architected deployed capability

IaaS Software Factory (Unclass/SIPR/JWICS)

- Leverage AWS services
- Core services for software development (Certificate to Field/Collaboration)
- Enterprise and Security services for dev/test/prod work

- Transfer Service that allows developers to *rapidly* and *securely* transfer code from Unclassified to Secret and/or Top Secret environments

Parity across TS/SCI, SECRET and UNCLASS Environments

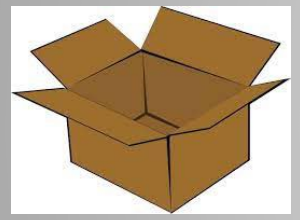
Lets Get Your Application Onboarded

"A la Carte" Bundles…Customize ODIN services for your application's needs

TCO

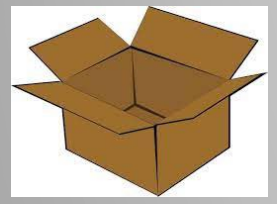
Full PaaS Bundle: Use of software development tools, software artifacts transfer service, deploy into CNCF compliant architected container-based CI/CD platform integrated with DoD and Intel Community

$



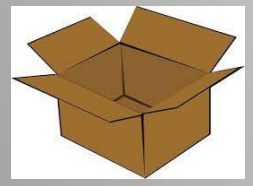
Bundle 4: Bundle 3 *plus* required software development tools

$

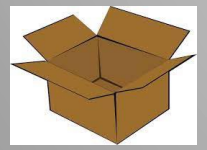


Bundle 3: Bundle 2 *plus* enterprise services, inherit all common control provider package (CCP) in Xacta

$



Bundle 2: Bundle 1 *plus* security services



Bundle 1: Use of Gold AMI and account management services (GEOAxIS/AccessIT! CAP), partial CCP inheritance in Xacta, deploy direct to AWS VPC

$

Less Enterprise Services

Enterprise & Security Services Offered Today

Unclassified

Security Services
- ClamAV- Antivirus
- ACAS –Vuln Scanning
- ECE and Endgame -Logging
- Gold AMI – Updated OS'
- AWS Directory Services
- Vault

Enterprise Services
- YUM -Patching
- DNS (local and public)
- Collaborative tools (JIRA, Confluence, Mattermost)
- Gitlab
- PKI
  - GEOAxIS & Keycloak

CI/CD Pipeline
- Diode Transfer Service
- Fortify and SonarQube
- SonaType
- OWASP ZAP
- Concourse
- ThreadFix
- Retire.js
- Anchore
- Trivy

Secret

Security Services
- ClamAV
- ACAS
- ECE and Endgame
- Gold AMI
- AWS Directory Services

Enterprise Services
- YUM
- DNS (local)
- Collaborative tools
- Gitlab

- PKI
  - GEOAxIS & Keycloak

Top Secret / SCI

Security Services
- ClamAV
- ACAS
- ECE and Endgame
- Gold AMI
- AWS Directory Services

Enterprise Services
- YUM
- DNS (local and public)
- Collaborative tools
- Gitlab

- ICITE PKI
  - GEOAxIS & ACCESSIT & Keycloak & JBLOCK

+ Enterprise Cross Domain Transfer Services
+ AWS accredited services – next slide

Classified Cloud AWS Services Accredited for Use

Services Available in Region - At a Glance

Services Currently Available in Top Secret Region		Services Currently Available in Secret Region	
Amazon API Gateway	Kinesis Data Firehose	Amazon API Gateway	AWS Key Management Service
Amazon Aurora	AWS Lambda	Application Auto Scaling	Amazon Kinesis
Application Auto Scaling	AWS License Manager	AWS Billing and Cost Management	AWS Lambda
AWS Billing and Cost Management	AWS PrivateLink	AWS CloudFormation	AWS License Manager
AWS CloudFormation	AWS Outposts	AWS CloudTrail	AWS PrivateLink
AWS CloudTrail	Amazon Redshift	Amazon CloudWatch	Amazon Redshift
Amazon CloudWatch	Amazon Relational Database Service	Amazon CloudWatch Events	Amazon Relational Database Service
Amazon CloudWatch Events	Amazon Route 53	Amazon CloudWatch Logs	Amazon Route 53
Amazon CloudWatch Logs	Amazon SageMaker	AWS CodeDeploy	Amazon Simple Storage Service
AWS CodeDeploy	AWS Secrets Manager	AWS Config	Amazon Simple Notification Service
Amazon Comprehend	Amazon Simple Storage Service	AWS Database Migration Service	Amazon Simple Queue Service
AWS Config	Amazon Simple Notification Service	AWS Direct Connect	Amazon Simple Workflow Service
AWS Database Migration Service	Amazon Simple Queue Service	AWS Directory Service	AWS Snowball
AWS Data Pipeline	Amazon Simple Workflow Service	Amazon DynamoDB	AWS Snowball Edge
AWS Direct Connect	AWS Snowball	Amazon Elastic Block Store	AWS Step Functions
AWS Directory Service	AWS Snowball Edge	Amazon Elastic Compute Cloud	AWS Systems Manager
Amazon DynamoDB	AWS Step Functions	Amazon EC2 Auto Scaling	AWS Transit Gateway
Amazon Elastic Block Store	AWS Systems Manager	Amazon Elastic Container Registry	Amazon Virtual Private Cloud
Amazon Elastic Compute Cloud	AWS Transit Gateway	Amazon Elastic Container Service	AWS Virtual Private Network
Amazon EC2 Auto Scaling	AWS Transcribe	Elastic Load Balancing	Amazon S3 Glacier
Amazon Elastic Container Registry	AWS Translate	Amazon EMR	AWS Health
Amazon Elastic Container Service	Amazon Virtual Private Cloud	Amazon ElastiCache	AWS Identity and Access Management
Elastic Load Balancing	AWS Virtual Private Network	Amazon Elasticsearch Service	Elastic Kubernetes Service (EKS)
Amazon EMR	Amazon WorkSpaces	AWS Fargate	AWS Liberty
Amazon ElastiCache	AWS Identity and Access Management	Amazon S3 Glacier	AWS Aurora
Amazon Elasticsearch Service	AWS Key Management Service	AWS Health	AWS WorkSpaces
Elastic File System (EFS)	Amazon Kinesis	Elastic File System (EFS)	AWS Resource Access Manager
AWS Fargate	Elastic Kubernetes Service (EKS)		
AWS Elemental: MediaPackage	AWS Health		
AWS Elemental: MediaLive	AWS Key Management Service		
Amazon S3 Glacier			

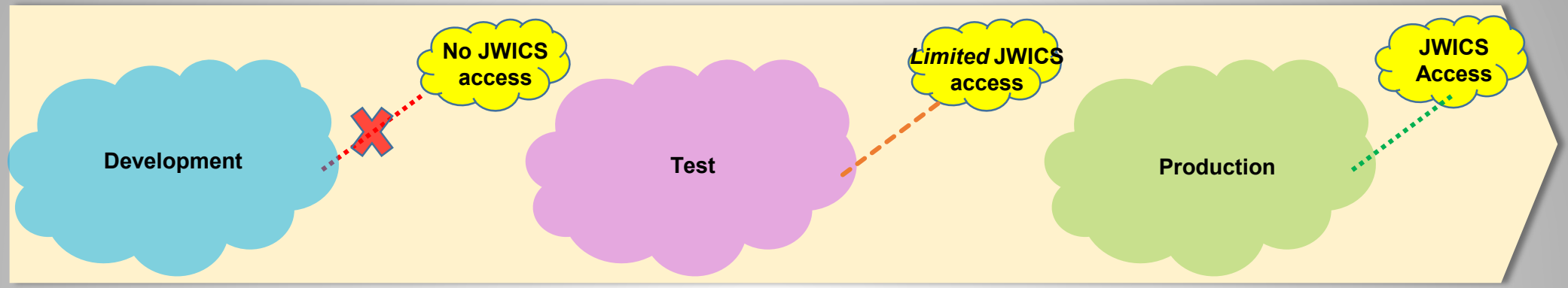
What These Tools Do

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
Kion	Multi-tenant cloud management automated billing, security auditing, dashboarding
Kubecost	Multi-tenant containerized platform management, billing, policy automation dashboarding

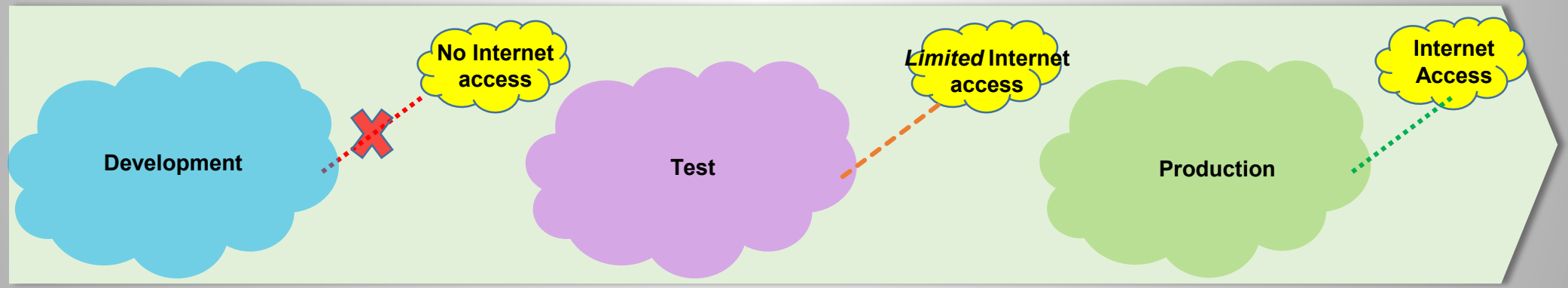
IaaS Architecture

Automation and Implementation

TC2S (*TS/SCI*) and SC2S (*Secret*) *Environments*



GovCloud *Unclassified Environment*



Development
- Software Testing
- NO access IGW (JWICS)
- Bastion/Proxy

Test
- Interim approval to test
- Limited Access IGW (JWICS)
- Bastion/Proxy

Production
- Authority to Operate
- Full Access IGW (JWICS)
- Bastion/Proxy

Cyber Security Partnership

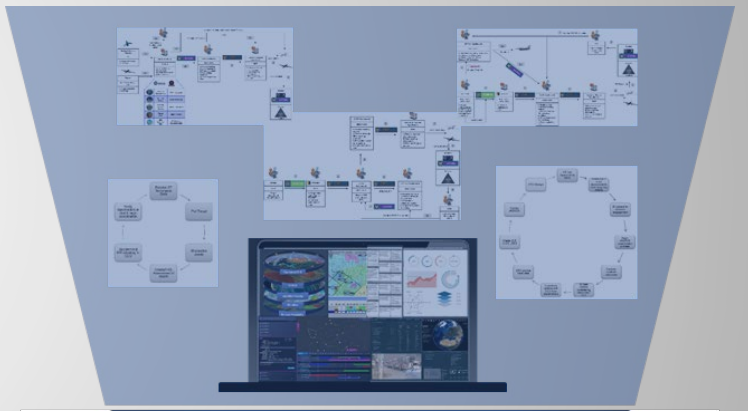
- 2021- AF Intel provided funding and training to 33rd NWS in support of their growth in Commercial Cloud Cyber Defense
- 2022- ODIN provides tools for 33rd NWS to perform Cyber Defense activities and training on the environment
- 33rd NWS to be the DAF Cloud SOC moving away from C5ISR and include TS/SCI as well
- Platform One in partnership is growing CNAP architecture to IL6 at ODIN
  - Slides to follow on the detailed plans
- Cloud One in partnership with ODIN working Secret FVEY platform plans
- DIA working with AFRL on plans for TS SCI FVEY platform

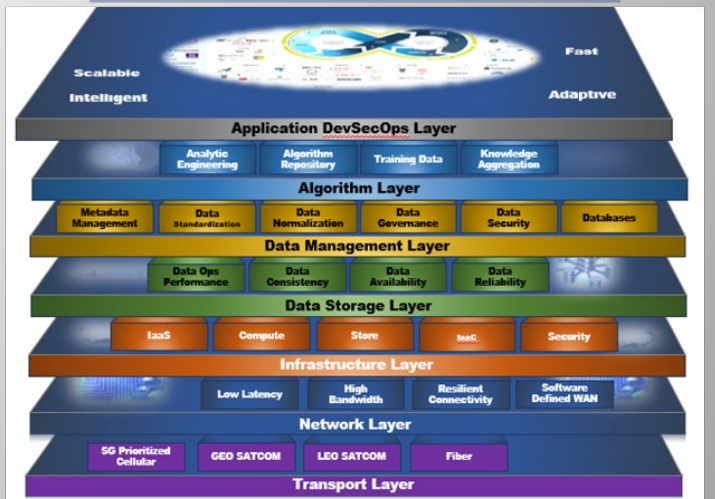
Zero Trust at TS/SCI Cloud

- Working with NASIC on piloting new ICAM and Zero Trust architecture which is compliant with IC Zero Trust architecture and interoperable with DoD
- Architecture still in development
- As applications and capability grow in the cloud the majority will retire capabilities on-prem and adopt the zero trust security with the transition to meet executive order requirements

Shorten the Kill Chain

- Multi-tenant Edge Nodes controlled by AOR MAJCOM with applications running on ODIN from NRO, NGA, NSA, DAF, and connected to JREN
  - Provides low latency and disconnected continued operation for mission critical cloud based applications
- Mission Threads for Intel supported
  - Dynamic Targeting
  - Post Strike BDA
  - ISR Feasibility
  - Collection Management AETs/PED operations



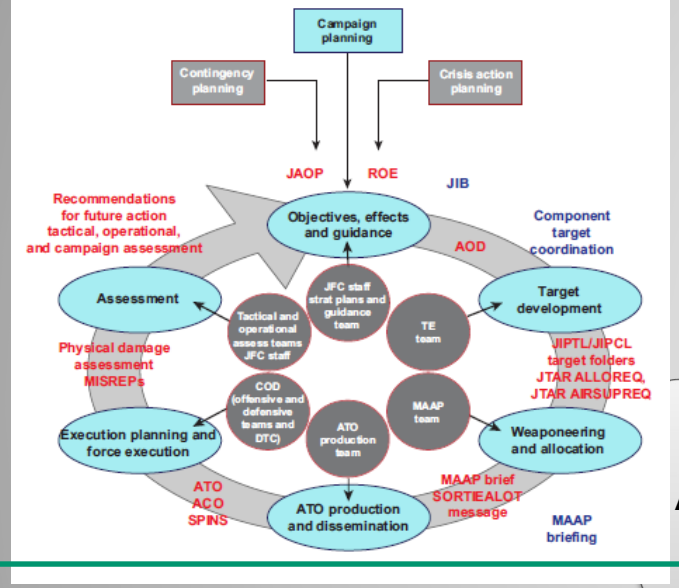


- ODIN is the Key to multi-tenant

  Commercial cloud edge hosting for

  Disparate agency and service applications

Focused Processes



Air Tasking Cycle

Commander's Objectives

Cognos

MOP / MOE Recommendations

Plans, JAOP, PIRs, AOD

Sphinx

Assessments

Dynamic Targeting

BDA, F2T2EA

Snapglass
Umami
JADOCS
Baldur
JTT

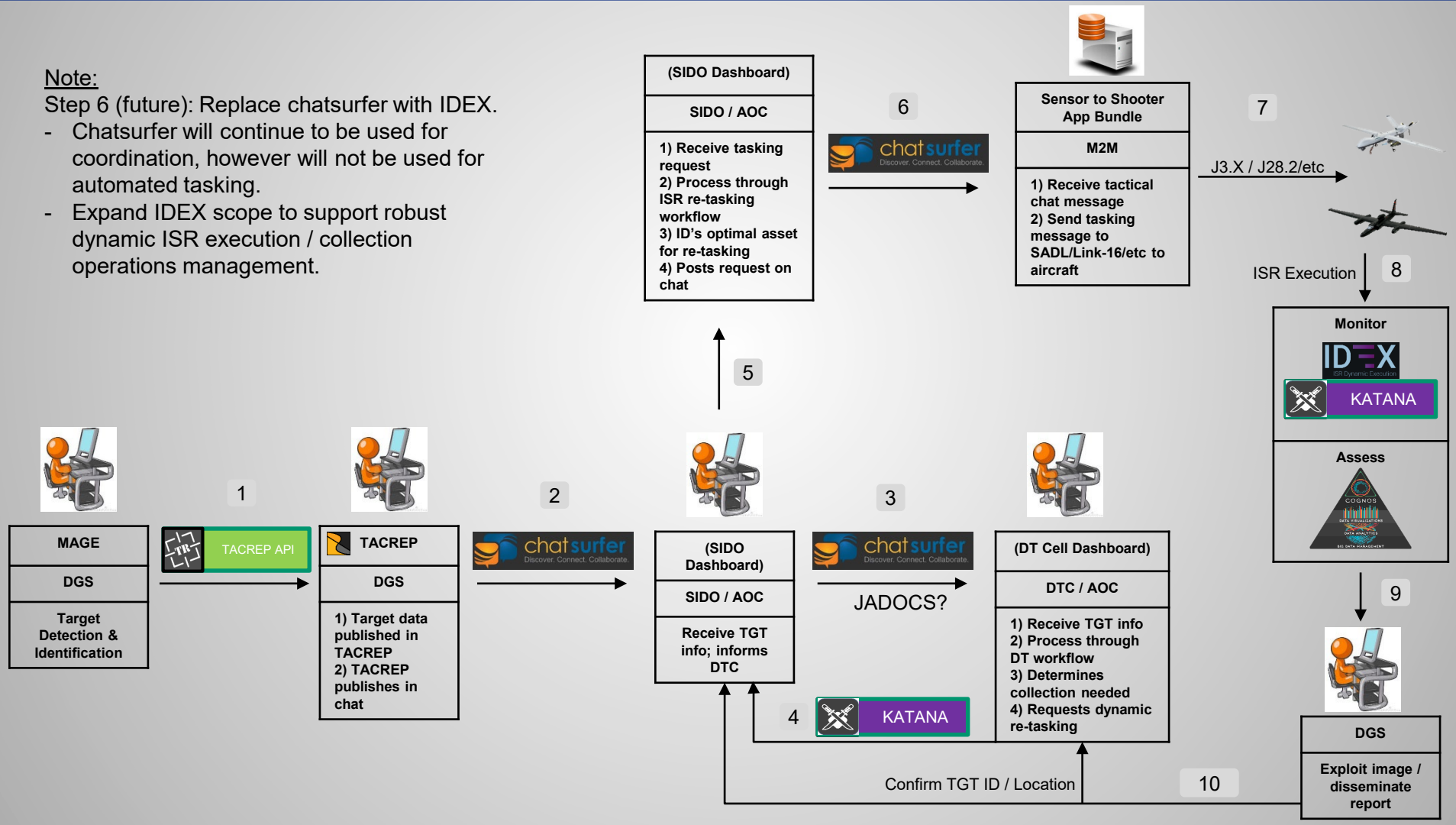
Dynamic Retasking

IGL, ISR Feasibility

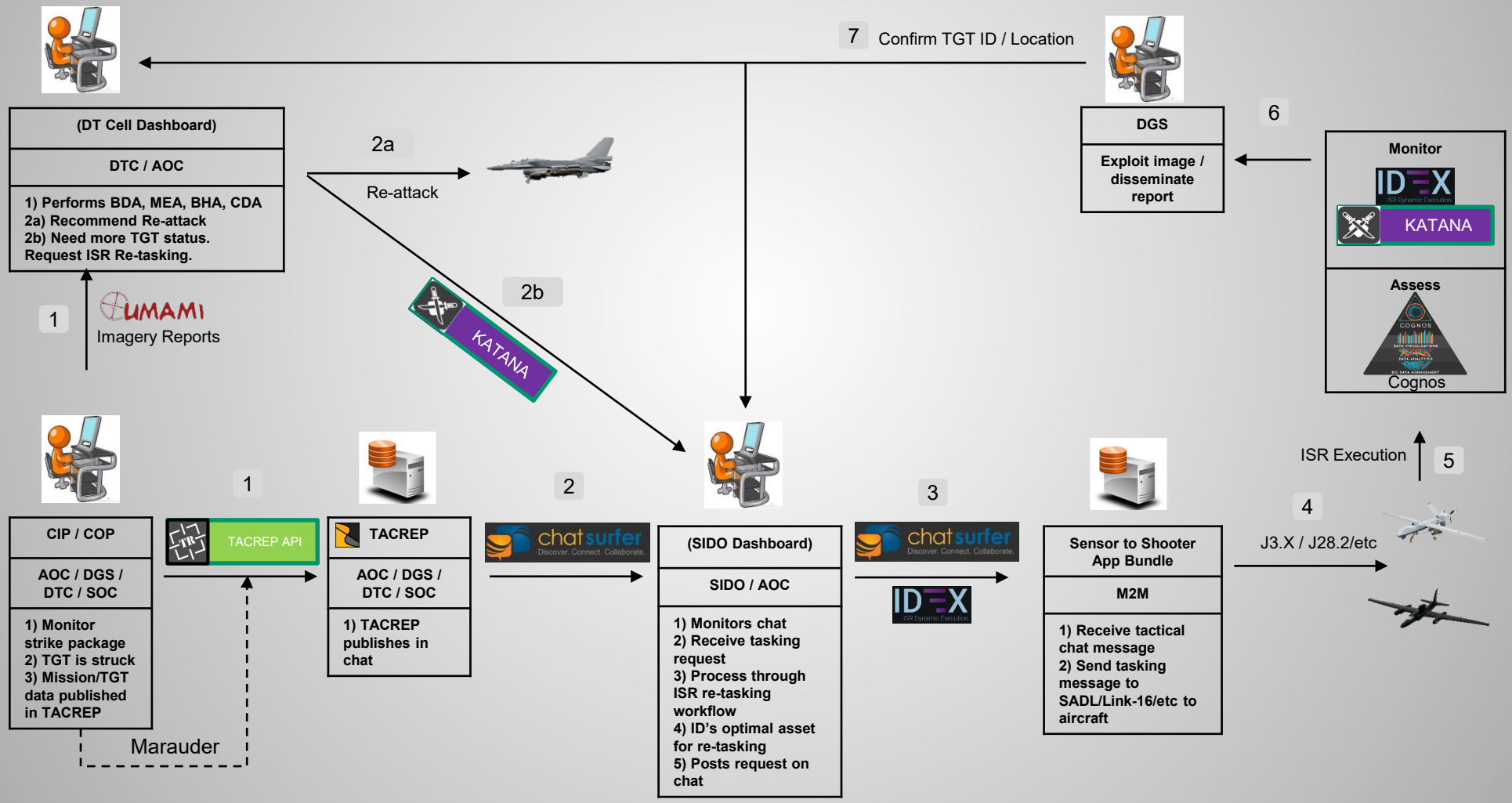
IDEX
KRAKEN
MIOS

Mission Thread 1: Target Detection

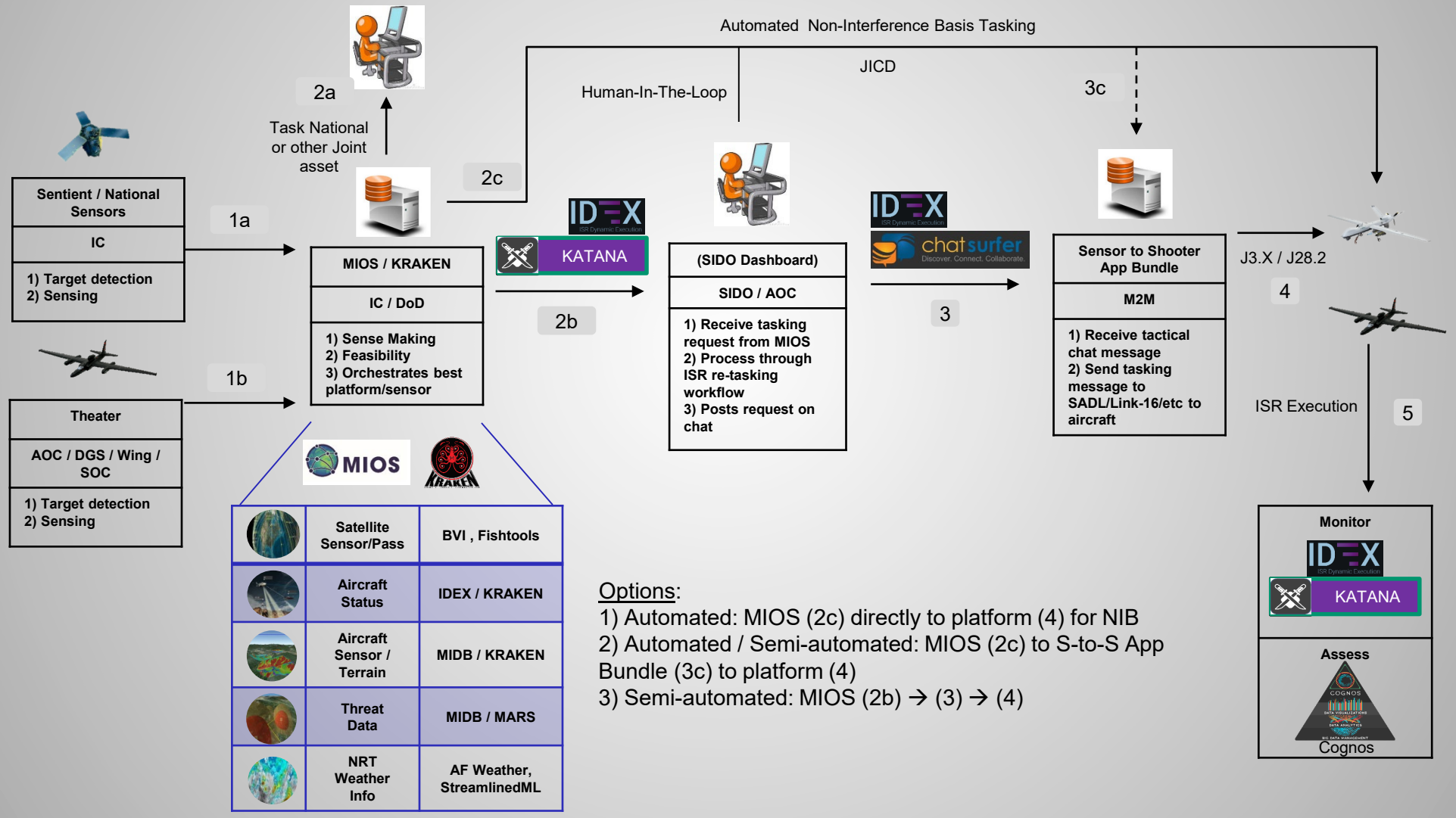
Note:
Step 6 (future): Replace chatsurfer with IDEX.
- Chatsurfer will continue to be used for coordination, however will not be used for automated tasking.
- Expand IDEX scope to support robust dynamic ISR execution / collection operations management.



Mission Thread 2 : Post-Strike

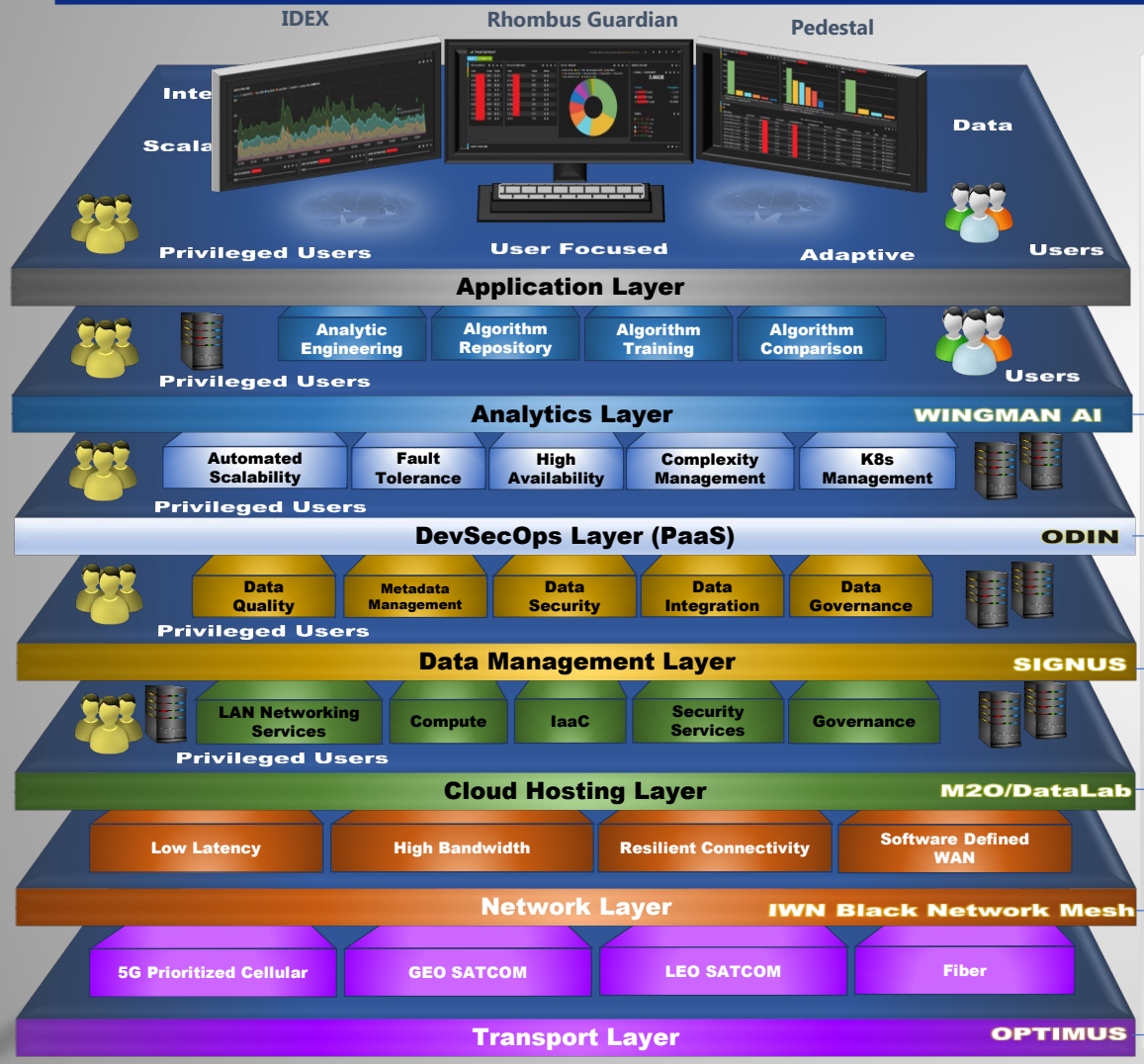


Mission Thread 3: ISR Feasibility



Options:
1) Automated: MIOS (2c) directly to platform (4) for NIB
2) Automated / Semi-automated: MIOS (2c) to S-to-S App Bundle (3c) to platform (4)
3) Semi-automated: MIOS (2b) → (3) → (4)

Enterprise Service Capabilities Today



AF IC Digital infrastructure provides layers of required cloud-based services & utilities for DAF users at three classification levels

- AI/ML from Wingman AI – Platform for AI development/execution
- DevSecOps Platform from ODIN/DataLab/VI2E – Pipeline for rapid software development & operations at all classification levels
- Data Platform from SIGNUS – Brokers access to data (AF, DoD, IC) and ensures data usability by users
- C2E management by Mission Modernization Office (M2O) – Manages user access, cloud compute, & contracting for IC cloud infrastructure
- Allows shared pathways integrating IC and DAF links
- Direct Connect from Optimus – Enables source data direct connection and optimizes networks to cloud based capabilities

ATO, Cyber threat detection, prevention, & response

Headquarters U.S. Air Force

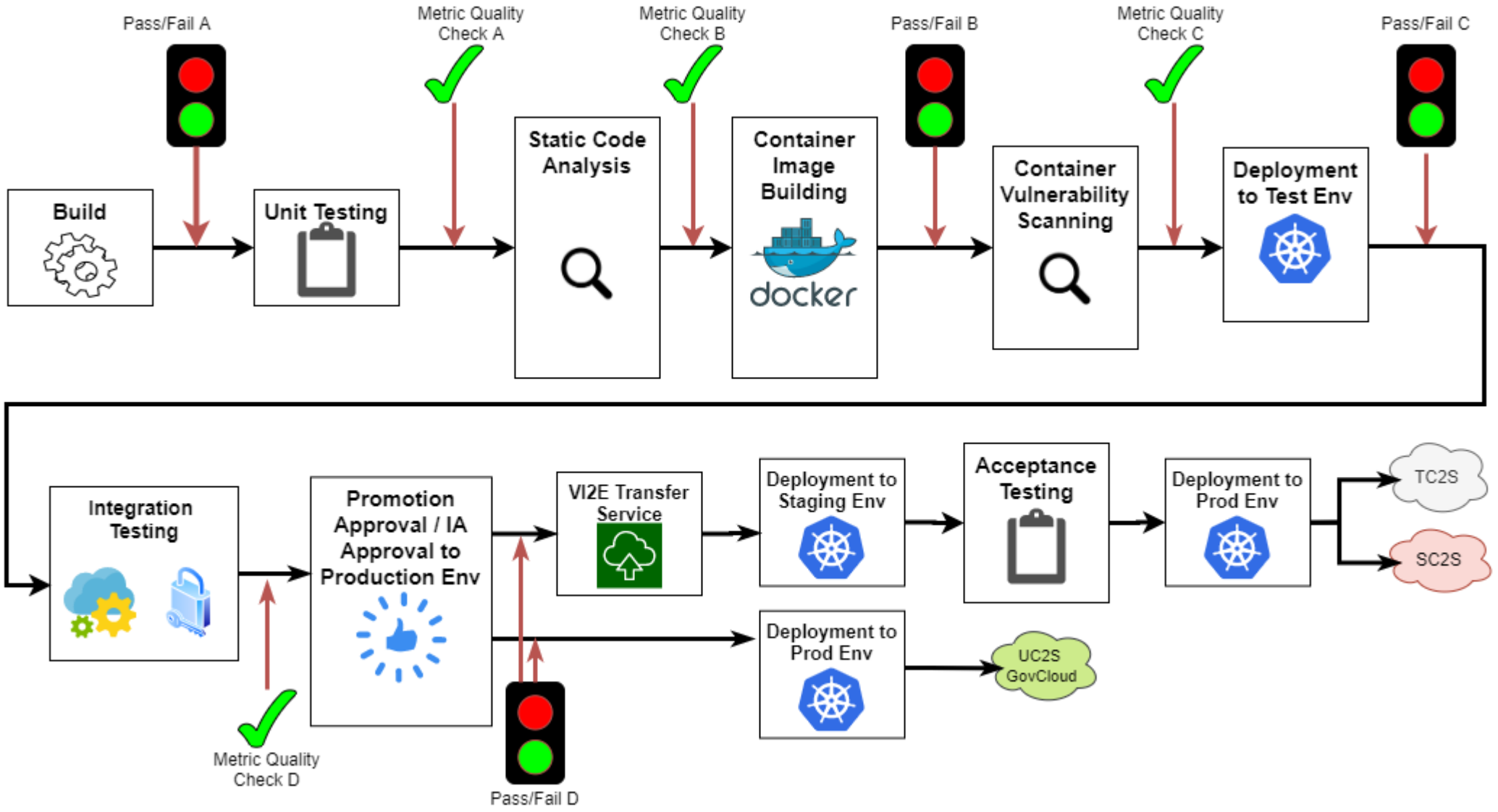
Integrity - Service - Excellence

Questions?

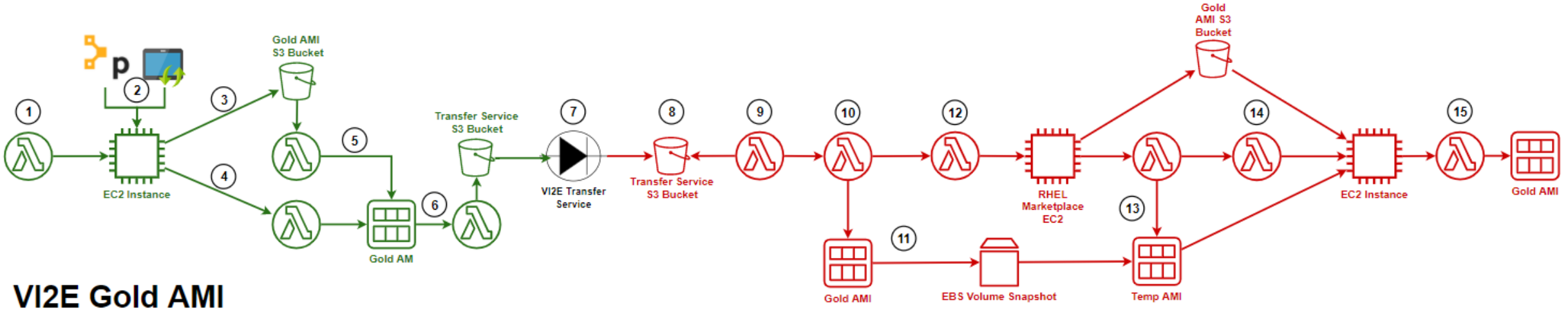
Challenges to Digital Transformation

- Valley of Death
  - Requirements validation, DOTMLPF process, PPBE POM process, addition to a program, advertising and large scale adoption into changed TTPs all non-existent
- Funding regulation
  - Cloud is based on as a service models and you need RDT&E and O&M
  - Funds expire, savings not reinvested, cost models and mechanics are not there for organizations to aggregate small dollars into large investments and split funding
- Lack of understanding on what we are transforming into
- Complete breakdown in what orgs do in the new way
  - There is no transfer to sustainment
  - There is no transfer to an ops org
  - Insourced work and owning the code base
  - Funding from customers and centrally together

CI/CD Pipeline



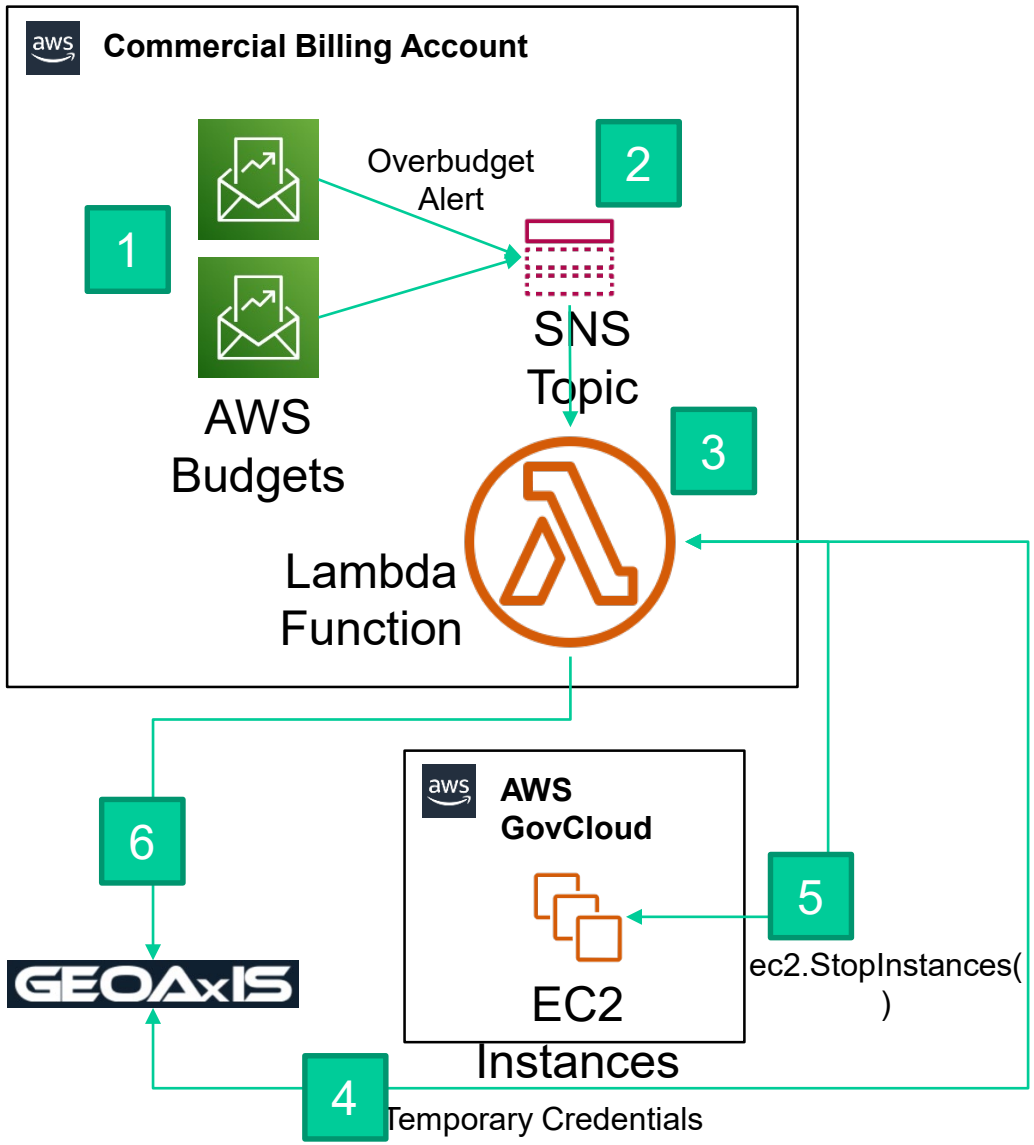
Gold AMI



VI2E Gold AMI

1. Using a cron schedule a Lambda function stands up an EC2 instance
2. After startup the EC2 instance updates all Yum installed software and uses Puppet to apply the DISA STIG
3. The EC2 instance performs a DISA STIG compliance scan, uploads the results to S3, and then shuts down
4. Lambda function snapshots the stopped EC2 instance with the appropriate Gold AMI name and date and terminates the EC2 instance
5. Lambda function checks the DISA STIG compliance scan, ensures it meets DAO requirements, and publishes the Gold AMI snapshot
6. Lambda function then exports the Gold AMI and sends the exported image to the Transfer Service S3 Bucket
7. VI2E Transfer Service transfers exported image to the high side environments
8. VI2E Transfer Service uploads exported image to the Transfer Service S3 bucket on the high side
9. Using a cron schedule a Lambda function checks for new exported images that are delivered to the Transfer Service S3 Bucket
10. When a new exported image has been identified a Lambda function imports the exported image into the high side environment
11. EBS Volume snapshot is extracted from Gold AMI
12. Lambda function stands up a Marketplace RHEL instance and uploads the CA Trusted Root certs and Yum configurations to the Gold AMI S3 Bucket and then shuts down
13. Lambda function snapshots the Marketplace RHEL instance, attaches the EBS Volume Snapshot created previously and terminates the RHEL Marketplace EC2 instance
14. Lambda function stands up a new EC2 instance using the Temp AMI, pulls down the Yum configurations and the CA Trusted Root certs from the Gold AMI S3 Bucket, installs them, then shuts down
15. Lambda function snapshots the new EC2 instance with the appropriate Gold AMI name and date, publishes the snapshot, and terminates the EC2 instance

VI2E Budget Enforcement



1. Each Pilot's approved budget amount is put into an AWS Budget. This service tracks the usage cost throughout the month. POCs are notified when the budget utilization reaches certain thresholds (50%, 75%, 90%, 95%, 100%).

2. If a monthly budget is exceeded, the budget service automatically sends a message to an SNS Topic.

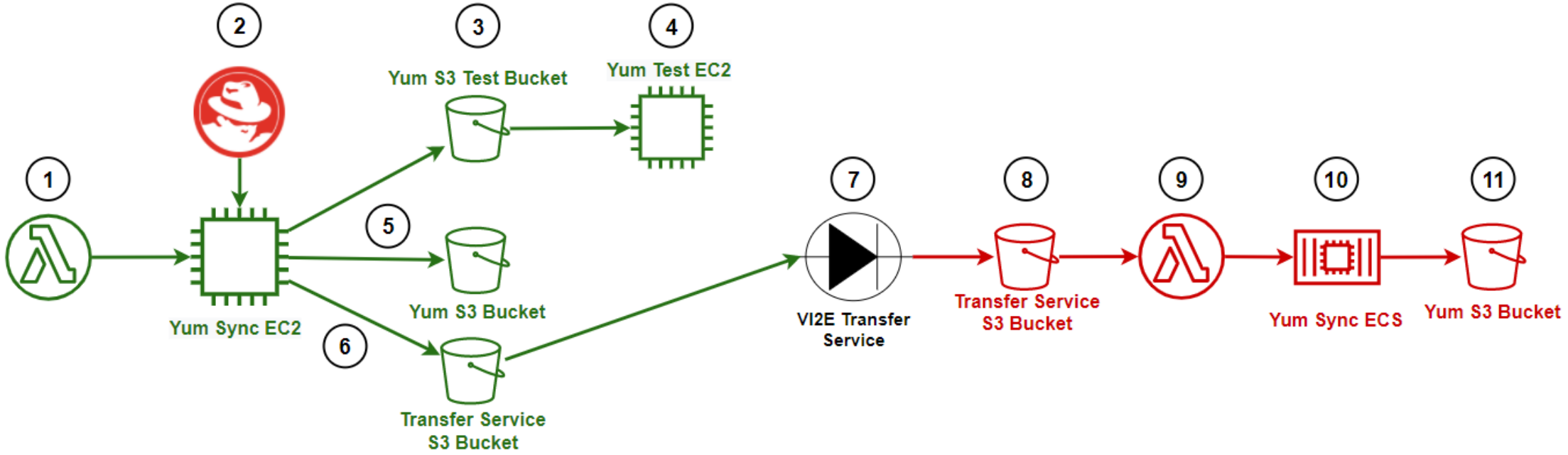
3. A Lambda function listens for these SNS Topic Notifications.

4. The Lambda function reaches out to GEOAxIS to obtain temporary credentials for the account whose budget was exceeded.

5. The Lambda function then uses those temporary credentials to authenticate to the overbudget account and stop all running compute resources.

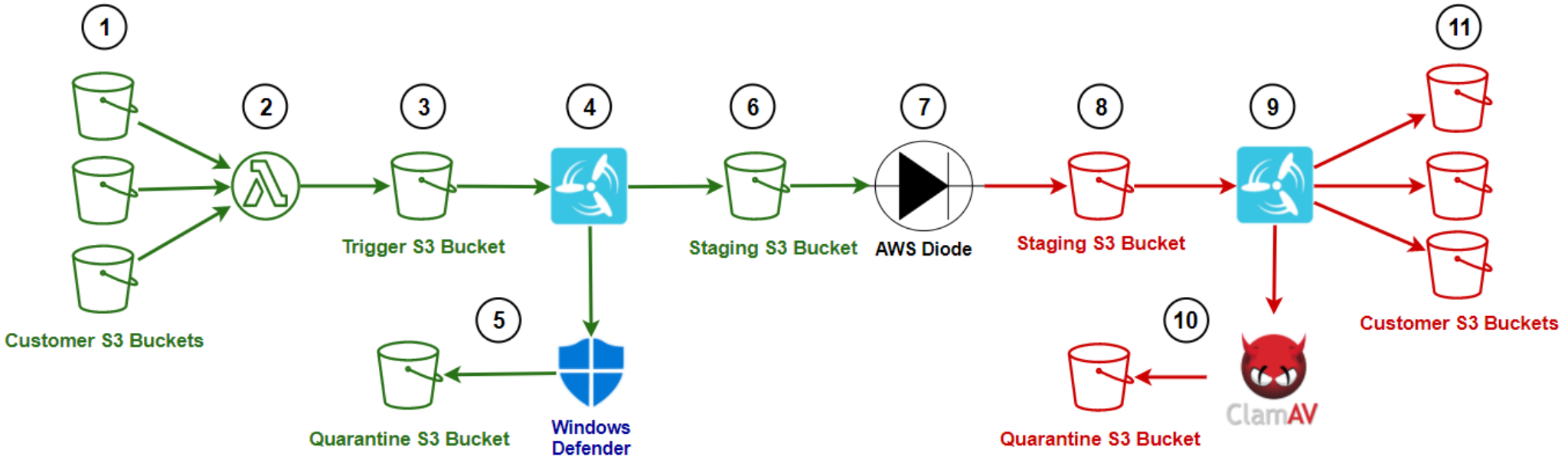
6. Finally, the Lambda function disables the account from within GEOAxIS so users cannot login and restart resources. It will be enabled at midnight on the first day of the following month.

YUM Synchronization



1. Using a cron schedule a Lambda function starts the Yum Sync EC2 instance
2. After startup the Yum sync EC2 syncs Red Hat repositories to a test file location
3. The Yum sync EC2 instance syncs Red Hat repositories to the Yum S3 Test Bucket
4. The Yum sync EC2 instance uses CloudFormation to create the Yum Test EC2 instance, which once started, uses the Yum S3 test bucket to perform Yum updates, then performs system tests. If tests fail, the pipeline is halted and engineers are notified for triage.
5. If tests pass the Yum sync EC2 instance syncs Red Hat repositories to a production file location and syncs the Red Hat repositories to the Yum S3 bucket
6. The Yum Sync EC2 instance uploads delta files from step 5 to the Transfer Service S3 bucket and then performs a shutdown on itself
7. The VI2E Transfer Service transfers delta files to the high side environments
8. The VI2E Transfer Service uploads delta files to the Transfer Service S3 bucket on the high side
9. The upload of the files to the Transfer Service S3 bucket triggers a Lambda function which sends a run task notification to the Yum Sync ECS cluster
10. The Yum Sync ECS cluster downloads the delta files from the Transfer Service S3 Bucket
11. The Yum Sync ECS cluster uploads the delta files to the Yum S3 bucket and removes any files that were removed in step 5 from the Yum S3 bucket

Transfer Service



1. A file is uploaded to a customer's S3 Bucket
2. The file upload triggers a Lambda function which gathers metadata on the file
3. The Lambda function uploads the metadata file to the Trigger S3 Bucket
4. Concourse is triggered by the upload of the metadata file, downloads the file from the customer's S3 bucket, generates a hash on the file, and digitally signs the file
5. Concourse runs a Windows Defender antivirus scan on the customer's file and quarantines the file if the scan results in a finding
6. If no finding was found in step 5 the customer's file is uploaded to the staging S3 bucket
7. The customer's file along with the metadata, hash information is sent through the AWS Diode
8. AWS Diode delivers the file, metadata, and hash information to the staging S3 bucket in the high side AWS account
9. Concourse is triggered by the upload of the customer's file to the staging S3 bucket, downloads the file from the stating S3 bucket, checks the hash generated in step 4, and checks the digital signature of the file
10. Concourse runs a ClamAV antivirus scan on the customer's file and quarantines the file if the scan results in a finding
11. If no finding was found in step 10 the customer's file is uploaded to the customer's S3 bucket in the high side AWS account