SATURN 2017

13th Software Engineering Institute Architecture Technology User Network Conference

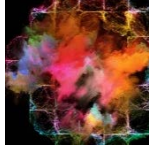
DevOps, Architecture, and Security in a Cloud

Greg Shevchenko

Paul Dudeck,

UPMC Enterprises

UPMC at a Glance



$14 billion integrated global health enterprise

More than 25 academic, community, and regional hospitals

UPMC Health Plan: 3.1 million members; network of 125+ hospitals, 11,500+ physicians

Affiliated with the University of Pittsburgh

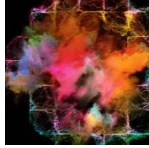
317,100 inpatient admissions, 200,000 surgeries performed annually

3.9 million outpatient visits, 870,000 emergency visits

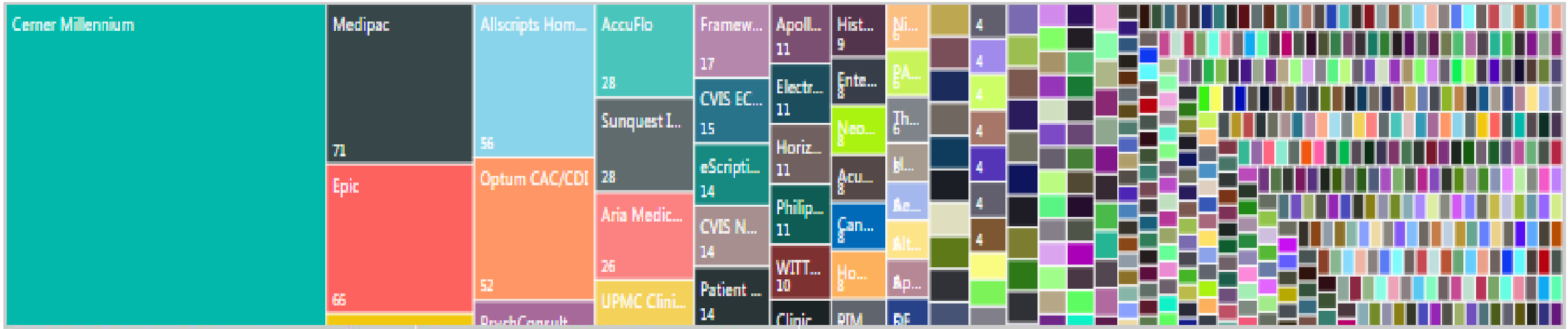
650 transplants annually

Pennsylvania's largest employer: 65,000 employees

BEST HOSPITALS U.S.News HONOR ROLL 2015-16



UPMC at a Glance

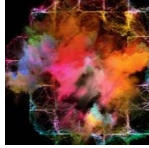


Total Number of Apps

1102

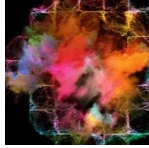
Data Domains of Top 20 Apps

Application Name	Count of Application Name
Cerner Millennium	573
Medipac	71
Epic	66
Horizon Home Care	64
Centricity RIS-IC	63
Allscripts Homecare	56
Total	**1263**



Introduction to UPMC Enterprises

- UPMC Enterprises roles in UPMC:
  - Health care innovation and development center
  - Partnerships with existing and emerging companies
  - Delivering new models of care to UPMC
- UPMCE's four focus areas:
  - Translational science
  - Improving outcomes
  - Infrastructure and efficiencies
  - Consumer

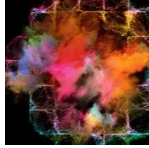


UPMC Enterprises: Portfolio & Strategic Partners

CAVULUS	Member management software and services for health plans
cernostics — PROVIDING DEEPER TISSUE INSIGHTS	Oncology diagnostics and precision medicine
CURAVI HEALTH	Reducing avoidable hospitalizations from nursing homes
evolent HEALTH	Value-based care and IDFS development
FABRIC GENOMICS	Automated clinical interpretation of genomes
HealthCatalyst — ignite outcomes improvement	Cost management
HF HEALTH FIDELITY	Risk adjustment transformation
ImPACT	Neurocognitive/concussion assessment
lantern	Online mental health wellness tool
medCPU	Clinical decision support and data acquisition
ovation — Revenue Cycle Services	Comprehensive HIM and revenue cycle services
PENSIAMO	Health care supply chain
Prodigo SOLUTIONS	Supply chain efficiency
RxAnte — Know the future. Then change it.	Medication adherence on behalf of health plans
3SCAN	3D computational pathology
via oncology	Clinical pathways decision support for cancer
vincent PAYMENT SOLUTIONS	Centralized control over decentralized payments
vivifyhealth	Remote patient monitoring

SATURN 2017

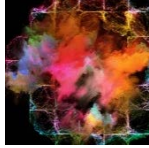
Project Voltron at UPMC Enterprises



Initial State in Jan 2016

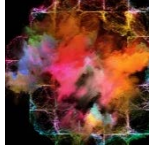
Baseline:

- Extensive experience in SCRUM process
- Architecture standards consistently maintained by the Architecture team
- Infrastructure dependencies on UPMC ISD
- Successful completion of POC projects in AWS and Azure
- Pilot projects built in AWS
- Growing expertise in Docker
- Some knowledge of Kubernetes
- Use of Jenkins, Artifactory, GitHub, SVN
- Variety of collaboration tools including MS SharePoint, 2 Wikis
- Issue tracking in JIRA and MS SharePoint
- Operations performed by development teams
- Client Services team focused on pilot software implementations inside UPMC and externally
- Client Services team has no representation in sprint planning and stand-up meetings



DevOps Initiative – Planning Phase

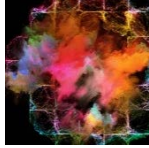
- Main emphasis on the transition of operations to Client Services team to increase the velocity of the development teams and start migration towards DevOps model
- Formulated collaboration between operations, architecture, and software engineering
- Initial plan included 5 areas:
  - Application Infrastructure Management
  - Infrastructure Monitoring
  - Application Lifecycle Management
  - Cloud Infrastructure Optimization
  - Information Management, Security, and Governance
- 4 levels of task priorities
- Proposed services, required tools and solutions, mapped technical and soft skills
- Gap analysis
- Planning phase took 4 iterations and approximately 4 weeks



DevOps Initiative – Planning Phase

Top priorities in **Application Infrastructure Management**:

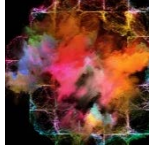
- Infrastructure planning
- Configuration management tools
  - Template development, testing, deployment
  - Provisioning and decommissioning processes
- Managing infrastructure in environments including storage, databases, middleware components, networks and VPN gateways
- User accounts, roles, privileges, and key management
- Collecting operational data and its visualization
- Dashboards and reports describing daily operations, workloads, and environment status
- Environment migration, promotion processes and procedures



DevOps Initiative – Planning Phase

Top priorities in **Infrastructure Monitoring**:

- Service monitoring and SLA enforcement
- Event management and intrusion detection
- Maintenance of a knowledge base
- Incident management and change management
- Security management in application environments



DevOps Initiative – Planning Phase

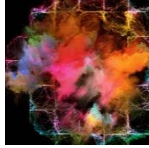
Top priorities in **Application Lifecycle Management**:

- Assistance in change management and code deployment
- Help in definition of application security and compliance

Top priority in **Information Management and Governance**:

- Perform data transition to the cloud, propagation to higher environments, secure data distribution to end-users
- Maintain data access roles and policies
- Manage HIPAA log files
- Report discrepancies between security standards and their implementation and uphold BAA requirements

No cloud infrastructure optimization goals



Proposed Roles and Responsibilities

Project: DevOPS and Infrastructure Automation

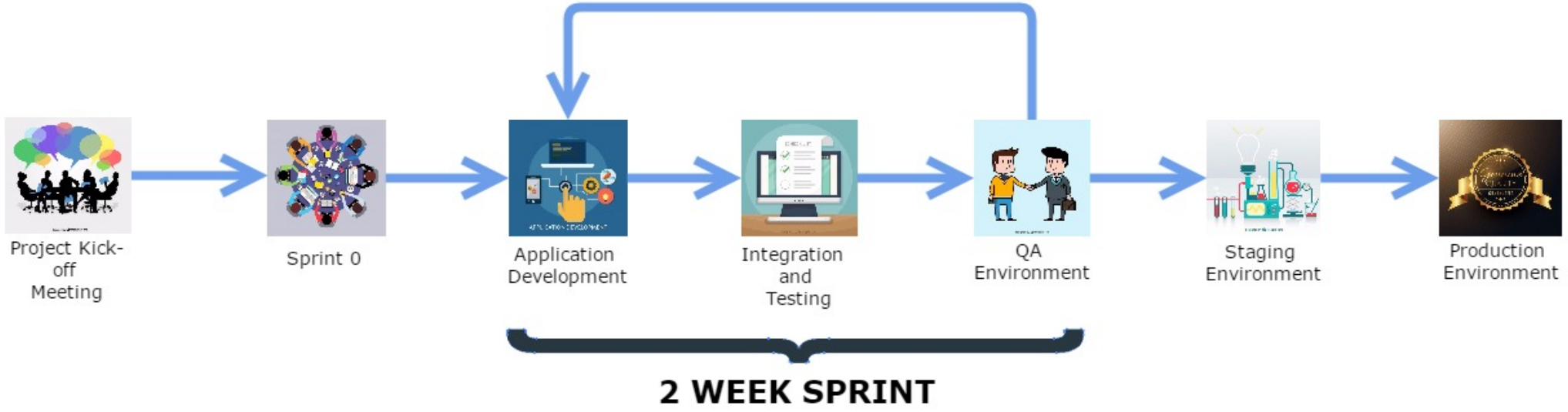
PROCEDURE	Automated Infrastructure Provisioning
DEPARTMENT	Client Services
UPDATED	5/9/2016

Entity	DESCRIPTION	Cloud Infrastructure Engineer	Architect	Dev Engineer	QA Engineer	TPM	CS Mgmt
1	Infrastructure/Compute environment in AWS (EC2, Docker containers)	A/R	C/I/R			I	I
2	Infrastructure/Storage (S3, Glacier) and Content Delivery (data import/export, data migration)	A	C/I	R		I	I
3	Infrastructure/Database (RDS)	A	C/I	R		I	I
4	Infrastructure/Networking (private and public networks, VPN, DNS, ELB)	A/R	C/I			I	I
5	DP & OPS/Dev Tools(Artifactory, Git, EMMI?, testing and automated testing frameworks, deployment tools)	I	C/I	A/R	C	C/I	I
6	DP & OPS/Management Tools(configuration and deployment management, CloudWatch, CloudTrail, automation tools)	A/R	C/I			I	C/I
7	DP & OPS/Security and Identitiy(directory services, KMS, identity management)	A/R	C/I	R	C/I	I	I
8	DP & OPS/Application Svcs (SNS, Queue services, search service)	I	C/I	A/R	C	C/I	I
9	Platform Services (ALL)	I	C/I	A/R	C	C/I	I
10	DevOps tool support	I	C/I	C/I	C	I	A/R

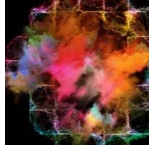
SATURN 2017

Development and DevOps collaboration

Development Process



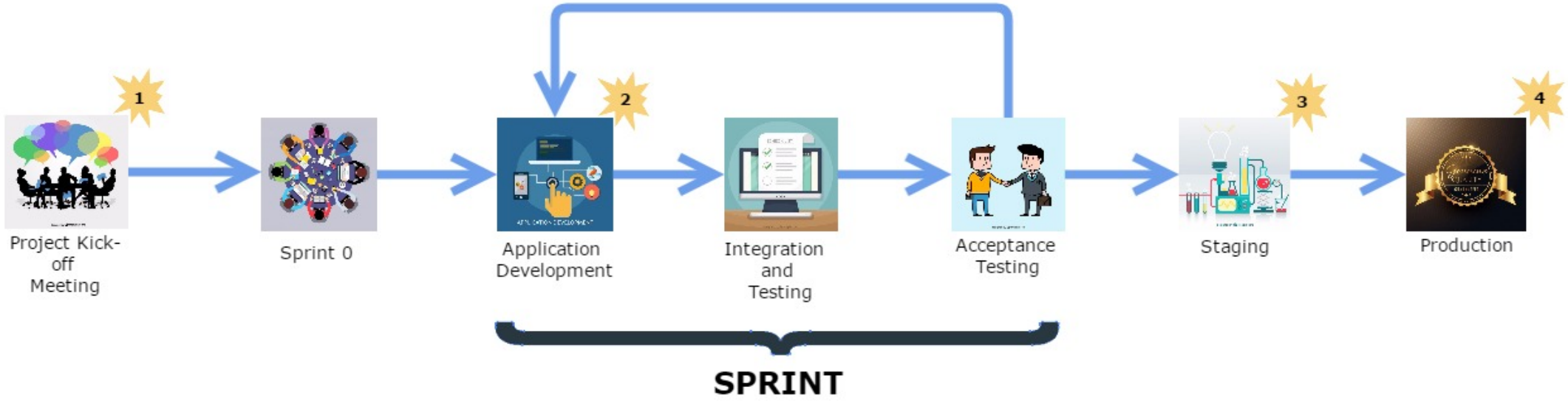
1. Project initiation and resource planning
2. Planning user stories in sprint 0
3. Development, unit tests, container build in subsequent sprints; code versioning and sharing via locally installed GitHub and Artifactory
4. Container deployment in Dev/Test
5. Automated functional and integration testing using Cucumber, Protractor + Jasmine framework, Supertest API testing
6. Container deployment in QA (optional), manual user acceptance testing
7. Automated minimal viable product deployment in Stage; automated volume testing using scripts, JMeter, Locus
8. Release deployment in Production



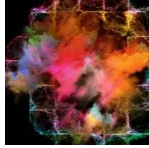
Automated Deployments

- Configuration management based on CloudFormation and bootstrap scripts for propagation of infrastructure components
- Custom build scripts for building Kubernetes clusters
- Jenkins jobs for building Docker container images for continuous integration
- ECR as a container repository
- Docker container deployments at scale on Kubernetes clusters
- Minor footprint of Elastic Container Service
- Key quality attributes for selection of container management tool:
  - **Non-functional requirements**: elasticity, load balancer triggers, triggers based on utilization of VM resources, local high availability, support for multi zone deployment, disaster recovery, cloud portability, software maintenance, support services, deployment process, cluster performance
  - **Functional requirements**: port management, health checks, storage management, integration with AWS AIM roles and policies, service recovery, load balancing, management UI

Client Services Contribution – Infrastructure as Code

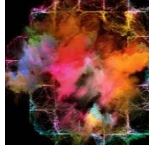


1. Participating in the infrastructure resource planning
2. Building infrastructure offerings and their maintenance in Service Catalog
3. Automated deployment
4. Support services to UPMCE development teams as well as portfolio companies
   - Managing accounts, roles, and policies
   - Event management
   - Monitoring resource utilization with CloudWatch metrics during volume testing
   - 24x7 monitoring of application and infrastructure
   - Incident response and change management
   - Managing non-production costs by parking unused compute instances



Event and Incident Monitoring

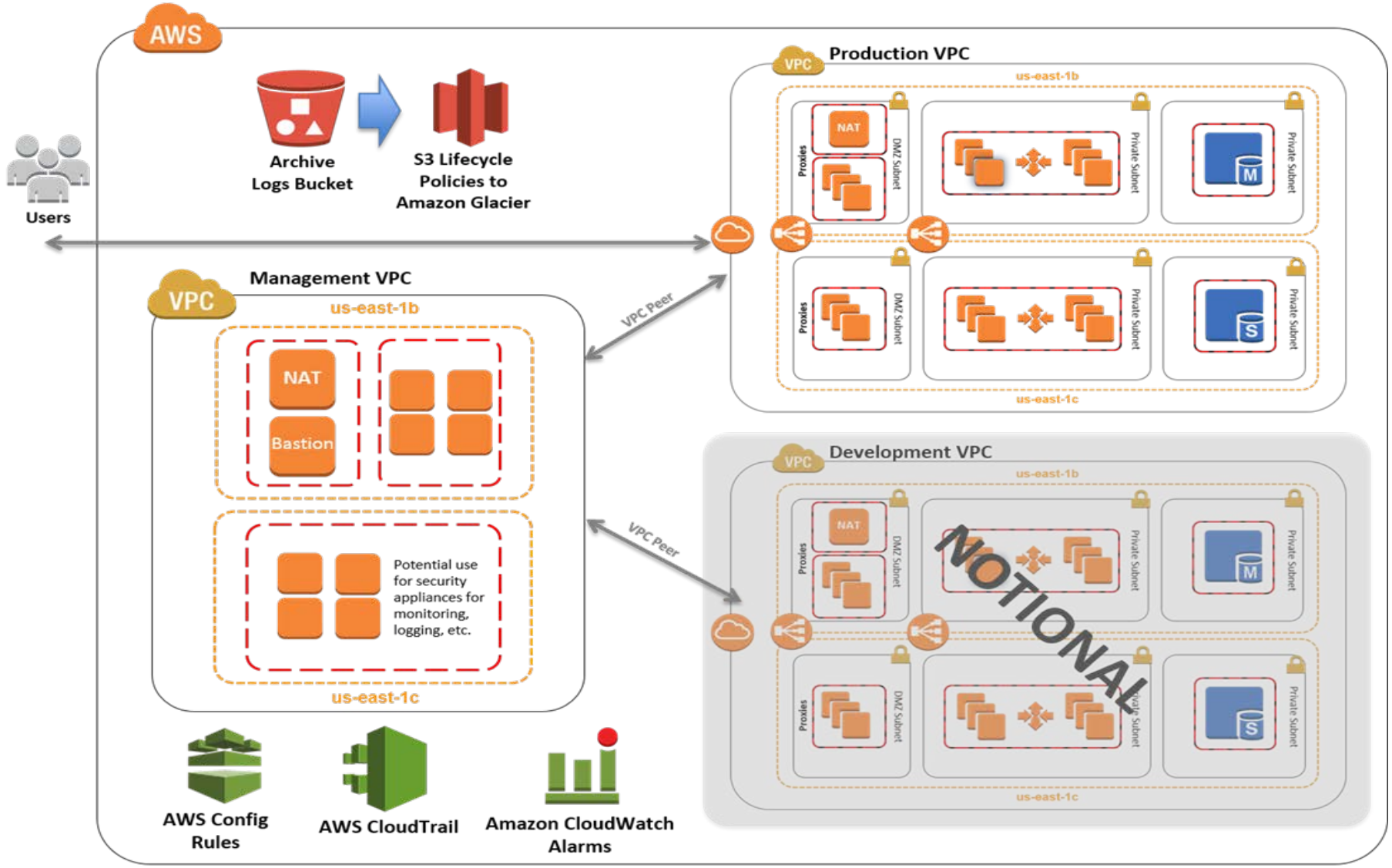
- Monitoring all AWS administrative events i.e. building EC2 instances, managed services, network and security groups changes via CloudTrail
- Application and managed services log files stored in S3 buckets with restricted access for further processing
- Filtering major application events in CloudWatch sending error notifications via SMS to 1st level support
- Reporting on resource utilization with CloudWatch dashboards and charts as well as ELK stack
- Regular updates of knowledge base maintained as private pages in Confluence
- *Work in progress: outsourcing the analysis of security related events*



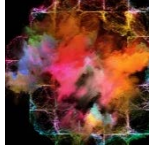
Security Considerations

- AIM user accounts, roles, access policies on all resources
- Weekly account reports and reviews
- Network security and access controls in compliance with AWS best practices based on NIST SP 800-53 and SP 800-171 standards
- Bastion servers for accessing resources on private subnets with SSH tunneling
- User access keys and 2048 bit RSA keys to log in to EC2 instances
- Centralized key management in KMS
- Encrypted EBS volume, S3 buckets with server side encryption
- Limited access to queue, CloudWatch, CloudTrail, and database services
- AWS Shield services deployed on public endpoints
- TLS encryption enabled on data in transit
- Endpoint protection on EC2 instances
- HIPAA log files being processed daily

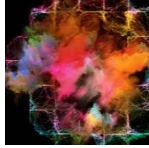
Example of supported environment



Challenges



- Vulnerability analysis and penetration test on Docker containers deployed on Kubernetes clusters and CoreOS
- Single sign on in heterogeneous cloud-based environment integrating multiple open source and vendor products
- Some cloud services are not HIPAA compliant that pushed our development toward PaaS based solutions and increased the scripting work
- Organization culture and concerns about data privacy demanded additional efforts to secure data, applications, and services
- Event correlation, alerting, and incident response

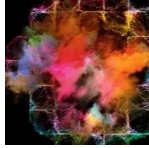


Benefits of new DevOps practices

- Configuration management practices reduced operator's errors, operational and infrastructure costs up to 60%
- Configuration management practices make it easy to replicate the production environment in Stage
- Automated deployments reduced infrastructure provisioning and application deployment time Rationalized collaboration and change management tools reduced the support costs by 5%
- Improved continuity planning, capacity planning, and services availability in the cloud
- Delineation of application development and operations increased the developers productivity

SATURN 2017

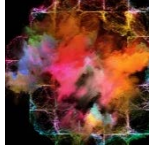
Current State and Roadmap for 2017



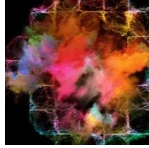
Current State

- Strong commitment to agile processes
- GitHub is single code repository for source code
- Artifactory is a repository for 3rd party and reusable libraries
- ECR includes all container images that can be deployed in Stage and PROD
- All documentation and articles are maintained in Confluence Wiki
- JIRA is used for all types of Requests For Change including user access requests, configuration changes, new development, enrollment of service candidates in Service Catalog, code progression, and issue tracking
- 24x7 monitoring is based on CloudWatch metrics and alerts
- Slack is a standard collaboration tool with SSO based on AD accounts

Current State



- Client Services team :
  - Provides continuous delivery of infrastructure components tightly integrated with the technology stack
  - Maintains Service Catalog and develops new offerings in collaboration with development teams
  - Facilitates continuous deployment of applications by automating container and services deployment in Stage and Prod environments
  - Maintains user accounts, roles, policies, and data access rules
  - Participates in capacity planning as consultants
  - Conducts environment optimization reviews based on automated metrics collection and analysis of resource utilization
  - Generates reports and decommissions unused resources
  - Coordinates building VPN gateways with UPMC ISD
  - Provides automated deployments of Kubernetes clusters and Docker container
  - Facilitates all data governance processes and internal audits, meeting with stakeholders, and coordinate meetings with AWS and MS solution architects



Roadmap for 2017

- Improve security by introducing Web Application Firewall in all application environments
- Harden our security posture for container defense by implementation of a product similar to TwistLock
- Complete PoC project and implement log analytics
- Conduct penetration testing and automate it
- Turn on AWS Inspector to capture user errors in configuration of roles, privileges, security groups, and other service configurations
- Collect requirements for establishing dedicated network connections to UPMC data centers via AWS Direct Connect
- Complete evaluation of WSO2 Identity server as SSO solution integrated with Health and Insurance Services
- Explore Terraform as alternative tool for composing infrastructure resources independently from cloud providers
- Introduce new cloud service provider in order to be more platform agnostic