Continuous Improvement in System Provisioning

Dan Han
Craig Kilgo

A little about us

Dan Han is the CISO for VCU, and is responsible for the oversight of the information security program in VCU.

Craig Kilgo is a project manager in the VCU Technology Services PMO focusing on the technology project vertical.

Agenda

- What is system provisioning
- The legacy process and deficiencies
- Process re-envisioned
- Outcome of new process
- Future plans

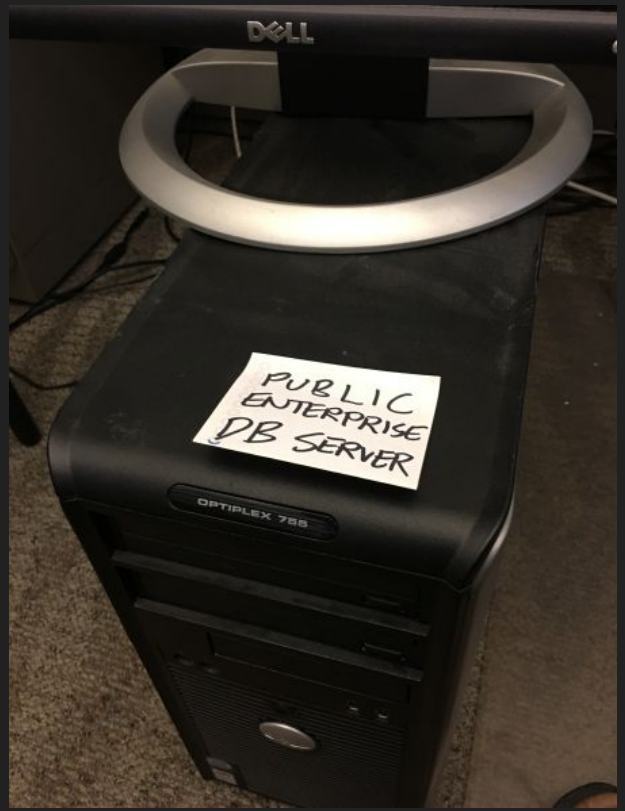
Prior to 2011...

System provisioning process #1

- Service desk ticket > Computer center
- Computer center purchases, provisions server, install OS from CD
- Configures server, assigns to system admin
- Works with network services to provision network settings / IP address
- Charges customer, hand over keys > /process

System provisioning process #2

- Service ticket > Network services
- Ask for static IP (or IP blocks) or reserved DHCP
- Specify Desired ACL
- Buy your system and self-provision



2011

Challenges

- Lack of validation of what is being provisioned
- No accurate inventory
- Customer says jump, we say how high
- Results:
    - Don’t know what we have
    - Can’t protect what we don’t know

The Infosec involvement

- Met with Networking and Data center to go over existing process
- Obtained buy-in to inject security validation into system provisioning process
- Result:
  - System Security Plan and data classification at the core of provisioning process for both network and servers
  - Systems are classified based on sensitivity
  - Network ACLs and proposed system configuration are reviewed prior to provisioning
  - Utilization of server inventory for asset tracking
  - Relocation of a large number of decentralized servers into the data center

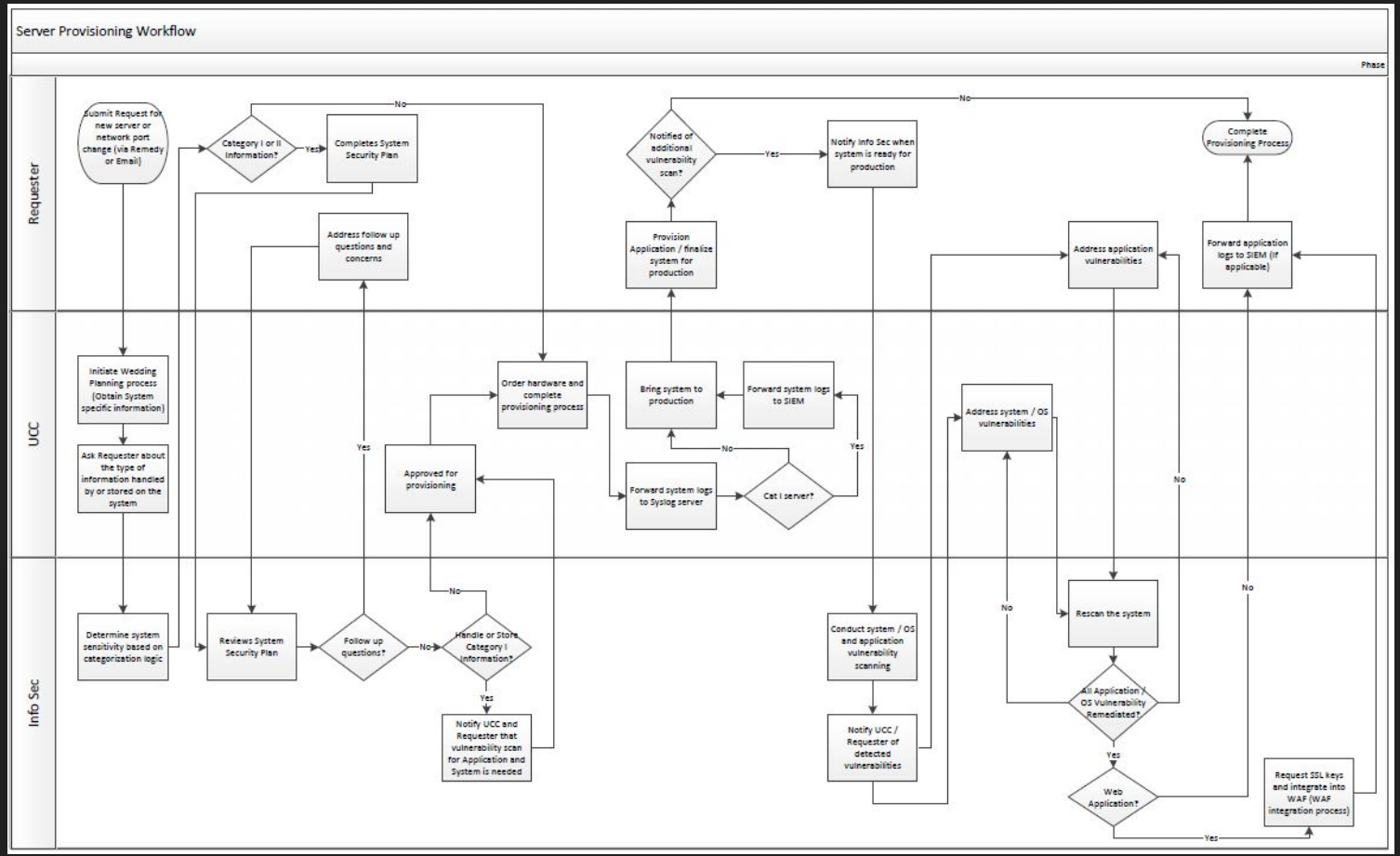
Provisioning of IT systems

- What is needed?
  - Type of system
  - Design system specs
  - System architecture
  - Purpose of system
  - Data security classification
  - Network ACL
  - Vulnerability assessment if needed
  - Monitoring configuration
  - Inventory information / System ownership information

Teams needed for provisioning

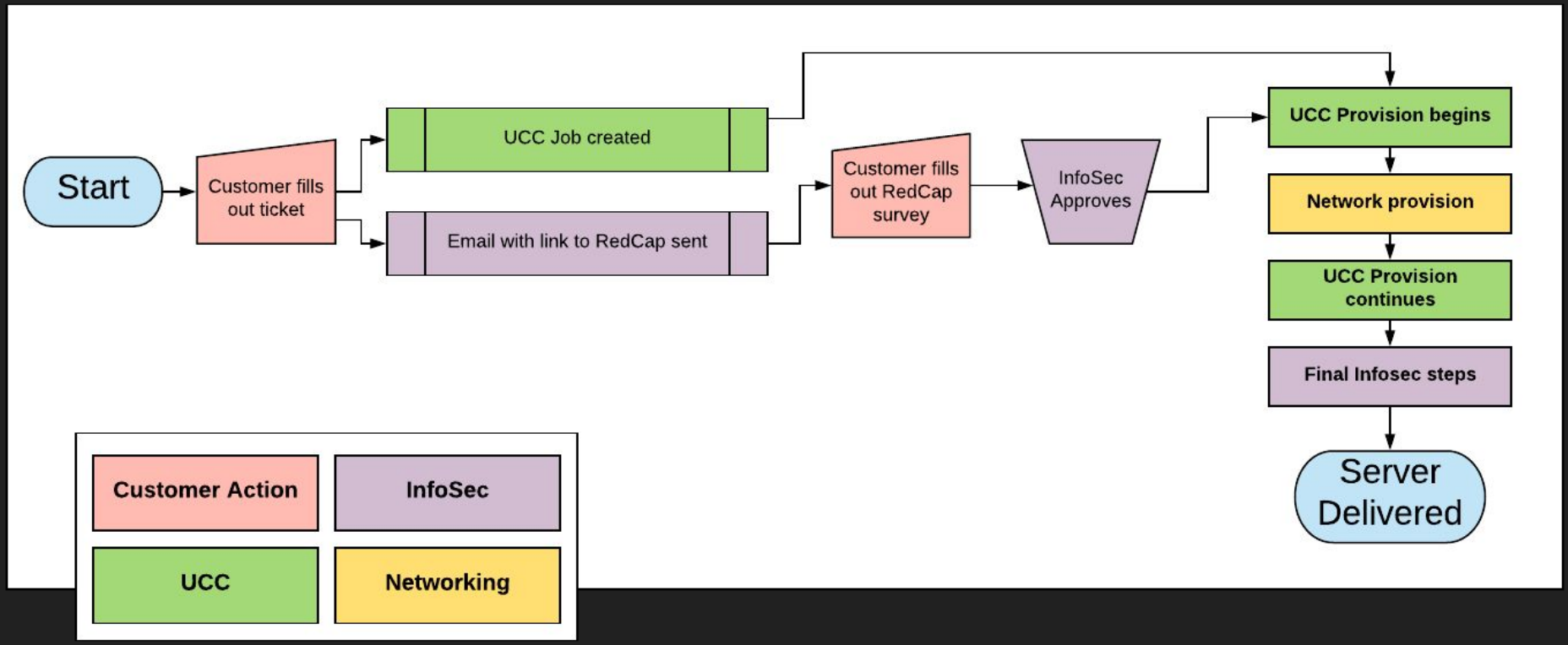
- Network
- Computer Center (Data Center)
- Information Security

The 2011 - 2017 Process



Of course, everyone can follow that, right?

Simplified version



Results: What worked

- Concierge service
- Defined process
- Security classification of systems and documented security plans for all systems provisioned through this mechanism
- Inventory & Tracking
- Centrally managed network serves as a checkpoint

But, over time problems started to become apparent.

Issues with this approach

- Slow, lengthy, and painful for the customers
  - **Average 29 days to provision a system!**
- Multiple units individually communicating with customer
- Collection of redundant data from customer
- Difficulties with coordination and orchestration of tasks
- Inaccurate records
- Inconsistent delivery of services
- Many bottlenecks in the critical path / No parallel activities
  - System security plan before anything else
  - Network provisioning before system provisioning

By the numbers

VCU PMO conducted an assessment of the process and identified that:

- 29 business days on average from request to delivery
- 6 days on average to get approved system security plan
- ~ 10 days for network provisioning / troubleshooting
- 45 minutes needed to complete the provisioning request and system security plan for a veteran IT personnel

In 2016...

Provisioning Network

- An attempt to remove network provisioning from critical path
- Provides ability to build before production IP address is assigned
  - Patching
  - Configuration of OS
  - Configuration of applications / mid-tier / DB connections
  - Limited access from and to other resources
- Allows parallel workflows between network provisioning and server preparation

Results?

- 27 business days to provision in 2016
- 23 business days in 2017

- Good news: Shaved off 6 days at the cost of a new network

- Bad news
  - We still suck
  - Many of the issues still exist

What now?

Options

- Continue to bolt on to existing process?

- New process from the ground up?

The test...

- Provisioning of 6 IAM servers
- PMO decided to test the existing provisioning process as a “model customer”
- Tester is a veteran IT staff with prior knowledge and experience with provisioning
- The results...

The gut check

Hi,

I believe all my servers within VCUNet have been taken down.

Since y'all beefed up the border and use Cisco VPN I've been putting classes up at DigitalOcean or RackSpace.

gsx.isy.vcu.edu, gsx2.isy.vcu.edu, and gsx3.isy.vcu.edu can all be taken out of the DNS...

PLMK if I need to do anything to get them off your books.

Core DevOps principles

- Flow
  - Ensure process focuses on value chain delivery from end to end
  - Minimize waste and reduce bottlenecks
  - Automate process flow from end to end
- Feedback
  - Continuous testing and validation of process
  - Build automated controls and testing into process
- Continuous Improvement
  - Continuously identify and reduce waste and bottlenecks
  - Continuous improvement through constant value stream mapping
  - Goal is to let the only bottleneck be the creativity of the human mind

But wait… Isn’t DevOps a programming thing?

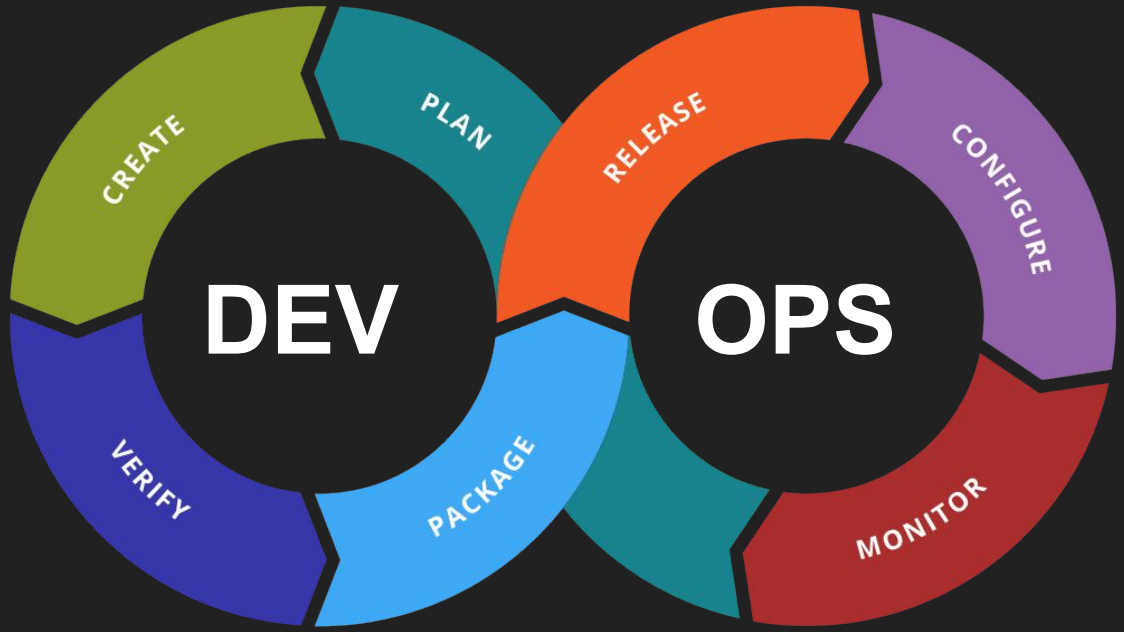
Principles of DevOps can be applied to IT operations

Dev:

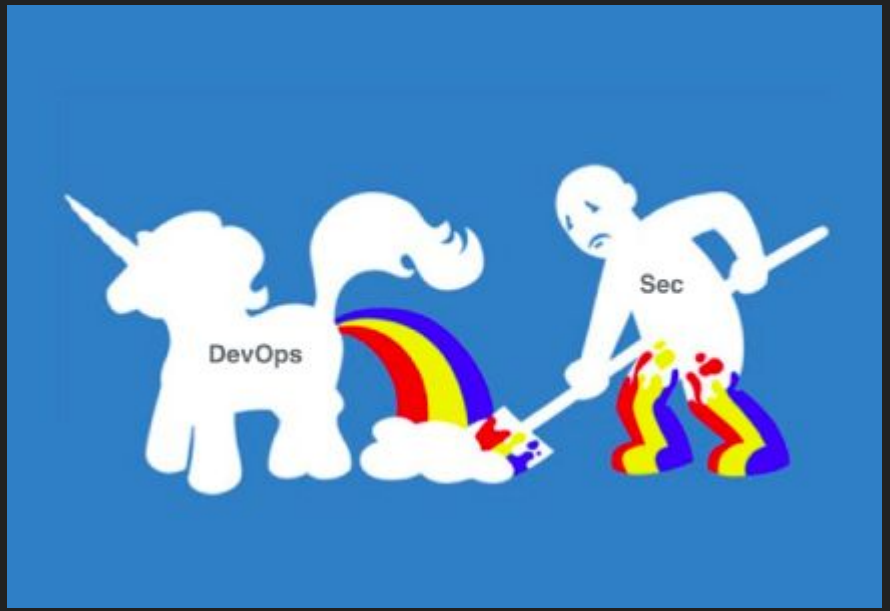
- Customers
- Infosec
- Network
- Data Center

Ops:

- Data Center
- Network
- Infosec



We need to avoid this...



Process redesign

- Start at the beginning (**Security starts at the beginning**)
- Infosec partnered with PMO to serve as project leads
- Partnered with Network services, computer center and reviewed existing processes

  Key redesign points
  - Increase efficiency and decrease the time needed to provision
  - Decrease time needed to submit a provisioning request
  - Reduce the multiple interaction points with customer
  - Collect as much information as possible before provisioning
  - Consider further parallel processing among Infosec, Networking, and Data Center

Incorporate DevOps principles into the design

- Self-service
- Automation / orchestration
- Small batch sizes and reduced bottleneck
- Continuous feedback
- Minimize waste

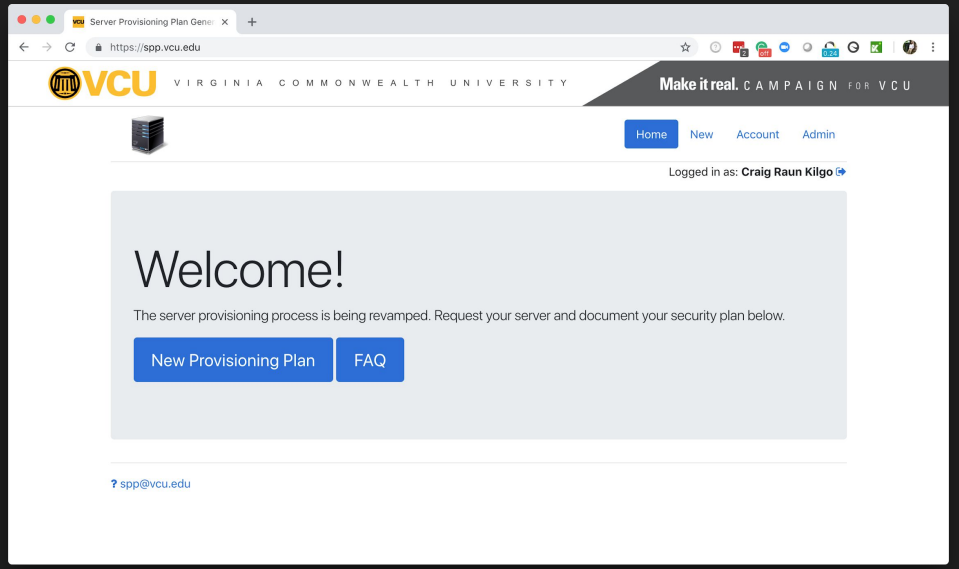
System Provisioning Plan

- Need to collect information from customers ahead of time for planning
- Need to minimize the amount of information collected to the absolute necessary to minimize time needed for completing request
- Minimize the interaction points with a customer to ensure there is one source of truth
- Provide a system which can interact with other systems for automation and orchestration capabilities
- Security review and approval done as they come in, no more batch approval

The Server Provisioning Plan

- In house “One-stop shop” app designed to collect provisioning requirements for Infosec, Computer Center, and Networking

- Ability to create request to the computer center and orchestrate security approval.



Demo

Key benefits

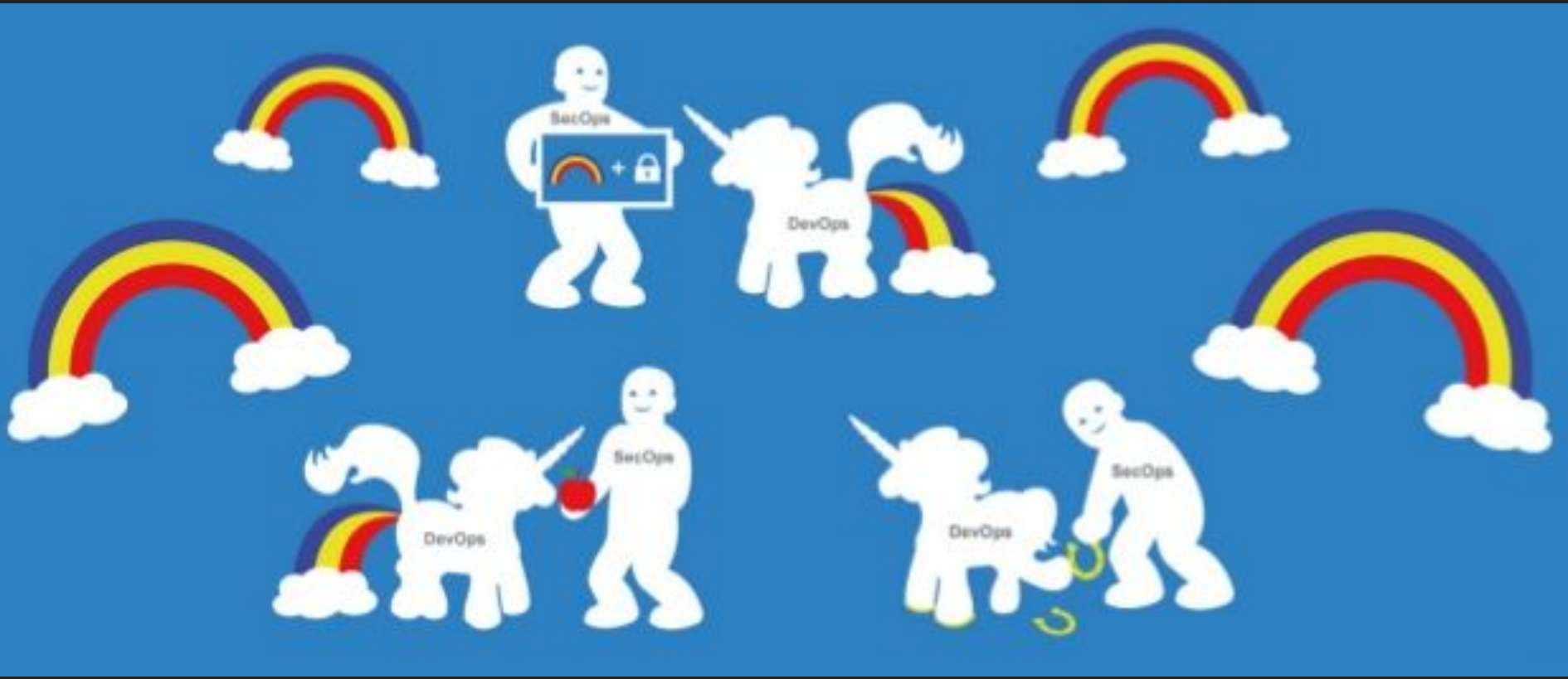
- Simple and modern interface for customers
- Reduce the need to have multiple interaction points with the customer
- Ability to orchestrate annual reviews for security plans
- Orchestration for computer center, infosec, and networking task creation and tracking
- Ability to integrate with other systems

Results

- Provisioning time reduced
  - 0.46 total days from submission to InfoSec approval
  - 12.5 business days from approval to provision
  - 13 business day total (down from 23)
- Easier way to track systems within an environment
- API endpoints available for other automation / orchestration tasks

Concepts for the future

- Private cloud and further automation / orchestration
  - Self-service
  - Rapid provisioning concept for short-term machines needed for simple tasks
  - Partial automation in ACL creation
- Increased automation in testing
  - Security validation in automated vulnerability assessment and reporting
  - Network ACL validation prior to delivery
- Move the campus IT technicians towards treating servers like cattle, not pets


SecOps
DevOps
DevOps
SecOps
DevOps
SecOps

Questions