On Demand Cloud Infrastructure

GSA IT Security Engineering Division

Bo Berlas- Chief Information Security Officer

CIVIC DIGITAL FELLOWSHIP

GSA

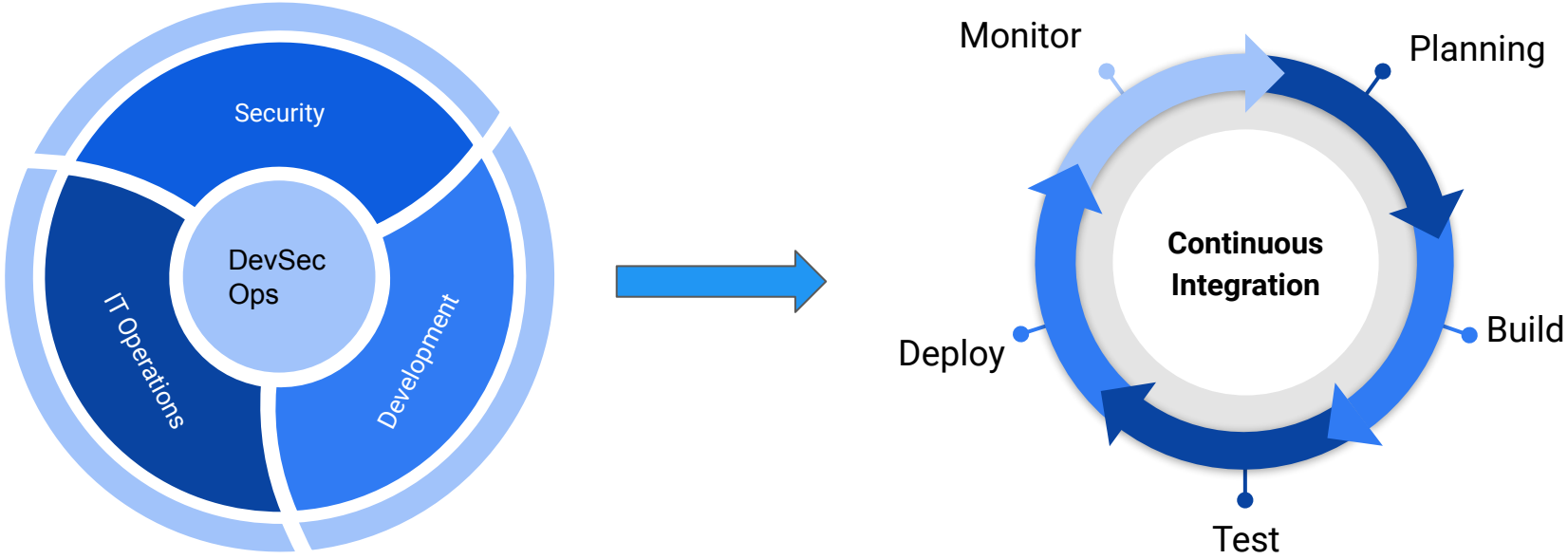
JOSHUA WOLKOFF
University of Rochester
Computer Science, Philosophy

Outline

1. Background
2. The problem
3. The solution
4. What was built
5. Live demo

CIVIC DIGITAL FELLOWSHIP

BACKGROUND: DevSecOps



CIVIC DIGITAL FELLOWSHIP

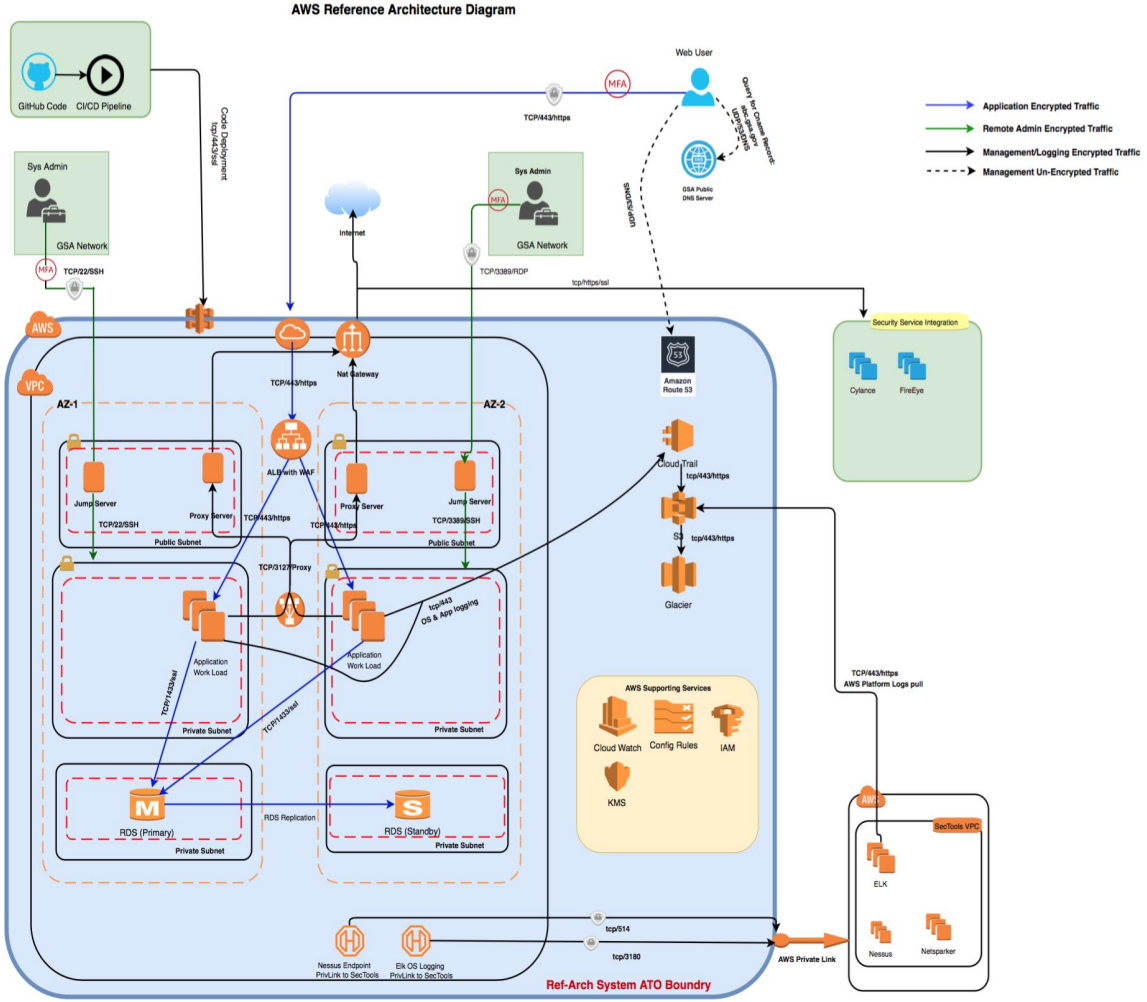
THE PROBLEM

- **How do you make sure that development teams have the proper infrastructure required for security integration?**

CIVIC DIGITAL FELLOWSHIP

THE SOLUTION

- Integrate with security team from the beginning, Security bolted in design and development
- Create a pre-made piece of reusable infrastructure that each new development team can build off of which is designed with security integration in mind.
- Pre-build code, pipe-lines and automation that teams can use with little or no changes



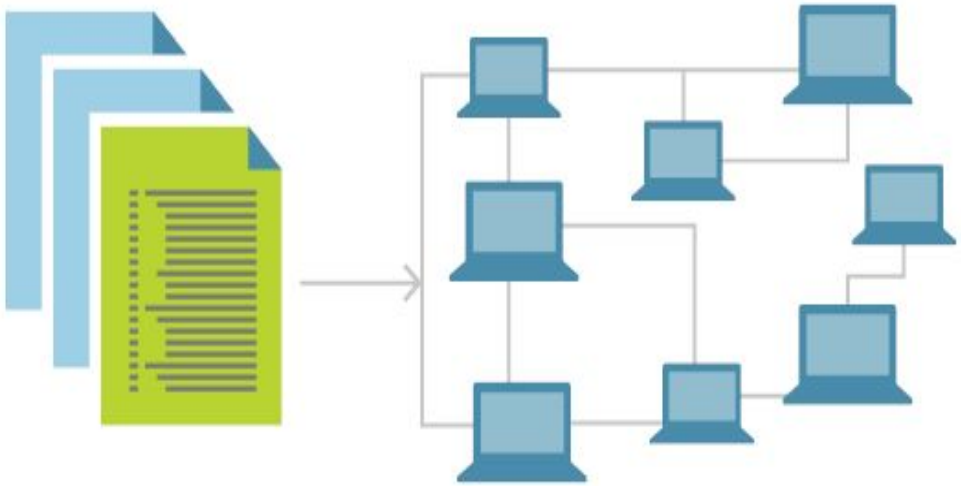
CIVIC DIGITAL FELLOWSHIP

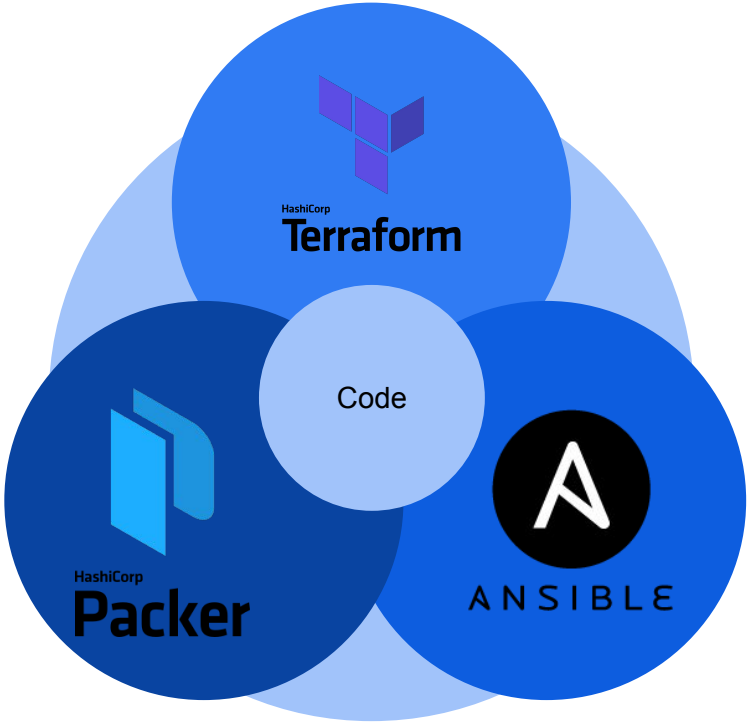
BUT WAIT...

- **How do we make it easy to reproduce this infrastructure to any given team and allow for modifications as necessary?**

CIVIC DIGITAL FELLOWSHIP

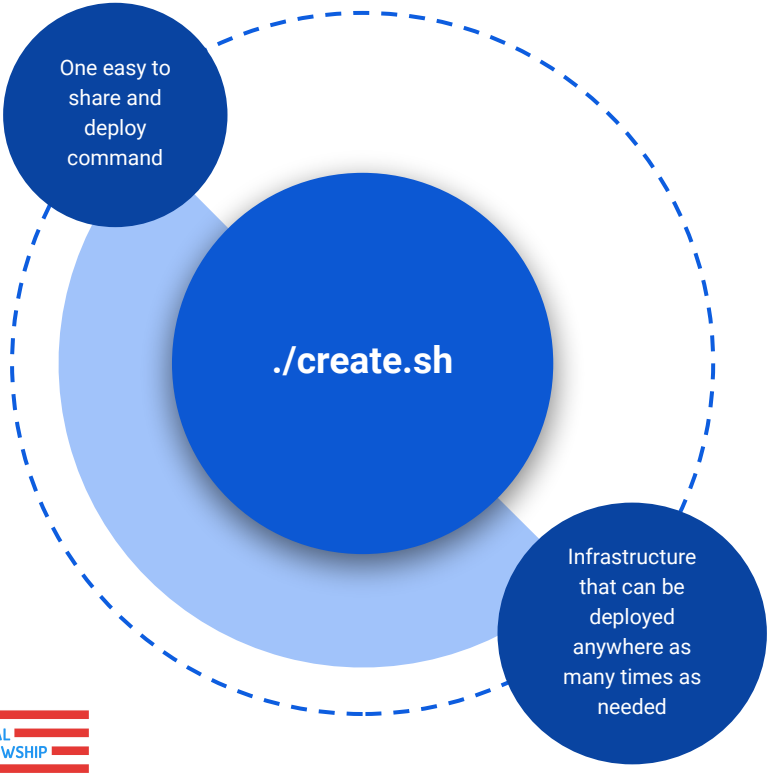
INFRASTRUCTURE AS CODE





CIVIC DIGITAL FELLOWSHIP

THE RESULT




```
- downloading role 'nginx', owned by nginxinc
- downloading role from https://github.com/nginxinc/ansible-role-nginx/archive/0
.12.0.tar.gz
- extracting nginxinc.nginx to /Users/joshuawolkoff/.ansible/roles/nginxinc.ngin
x
- nginxinc.nginx (0.12.0) was installed successfully
amazon-ebs output will be in this color.

==> amazon-ebs: Prevalidating AMI Name: odp-rhel-private
    amazon-ebs: Found Image ID: ami-02eac2c0129f6376b
==> amazon-ebs: Creating temporary keypair: packer_5d474d1f-2df1-b9e4-f6c5-f246a
028db1d
==> amazon-ebs: Creating temporary security group for this instance: packer_5d47
4d24-d803-1c6e-d171-e4d78fba9606
==> amazon-ebs: Authorizing access to port 22 from [0.0.0.0/0] in the temporary
security groups...
==> amazon-ebs: Launching a source AWS instance...
==> amazon-ebs: Adding tags to source instance
    amazon-ebs: Adding tag: "Name": "Packer Builder"
    amazon-ebs: Instance ID: i-06363be25a737cc7c
==> amazon-ebs: Waiting for instance (i-06363be25a737cc7c) to become ready...
==> amazon-ebs: Using ssh communicator to connect: 18.212.137.62
==> amazon-ebs: Waiting for SSH to become available...
```

CIVIC DIGITAL FELLOWSHIP

IT'S LIVE!

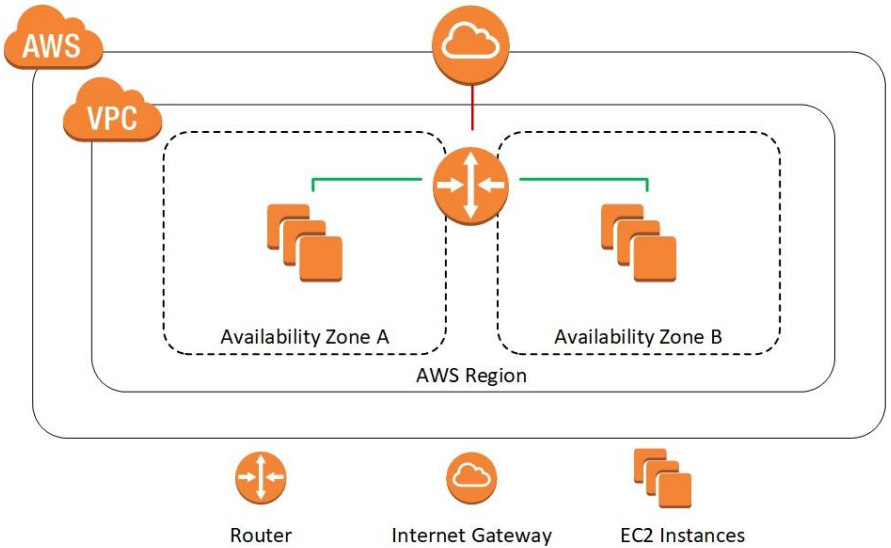
DEMO TIME

CIVIC
DIGITAL
FELLOWSHIP

WHAT IS BUILT

Network Configuration

- VPC
- Private/Public Subnet
- Internet Gateway
- NAT Gateway
- Route Tables



CIVIC DIGITAL FELLOWSHIP

WHAT IS BUILT

Network Configuration

- VPC
- Private/Public Subnet
- Internet Gateway
- NAT Gateway
- Route Tables

IAM Account Configuration

- Pre-configure security groups
- Provide security policies
- Detail user permissions

Group Name	Users
securityOperations-sandbox	0
securityAssessment-sandbox	0
finance-sandbox	0
userManagement-sandbox	0
incidentResponse-sandbox	0
fullAdmin-sandbox	0
devsecops-sandbox	0
default-sandbox	0

CIVIC DIGITAL FELLOWSHIP

WHAT IS BUILT

Network Configuration

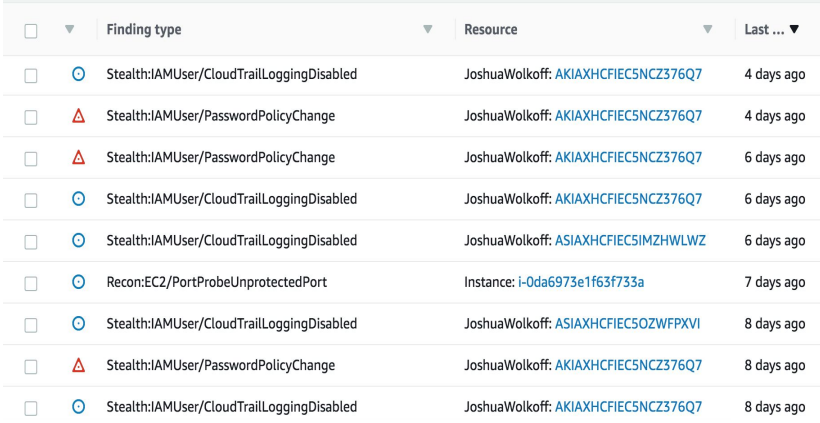
- VPC
- Private/Public Subnet
- Internet Gateway
- NAT Gateway
- Route Tables

IAM Account Configuration

- Pre-configure security groups
- Provide security policies
- Detail user permissions

Architecture Security Configuration

- GuardDuty
- Config rules
- VPC flow logs
- Secure, encrypted logging
- Pre-made logging storage structure
- Forced MFA



Finding type	Resource	Last ...
Stealth:IAMUser/CloudTrailLoggingDisabled	JoshuaWolkoff: AKIAXHCFIEC5NCZ376Q7	4 days ago
Stealth:IAMUser/PasswordPolicyChange	JoshuaWolkoff: AKIAXHCFIEC5NCZ376Q7	4 days ago
Stealth:IAMUser/PasswordPolicyChange	JoshuaWolkoff: AKIAXHCFIEC5NCZ376Q7	6 days ago
Stealth:IAMUser/CloudTrailLoggingDisabled	JoshuaWolkoff: AKIAXHCFIEC5NCZ376Q7	6 days ago
Stealth:IAMUser/CloudTrailLoggingDisabled	JoshuaWolkoff: ASIAXHCFIEC5IMZHWLWZ	6 days ago
Recon:EC2/PortProbeUnprotectedPort	Instance: i-0da6973e1f63f733a	7 days ago
Stealth:IAMUser/CloudTrailLoggingDisabled	JoshuaWolkoff: ASIAXHCFIEC5OZWFPXVI	8 days ago
Stealth:IAMUser/PasswordPolicyChange	JoshuaWolkoff: AKIAXHCFIEC5NCZ376Q7	8 days ago
Stealth:IAMUser/CloudTrailLoggingDisabled	JoshuaWolkoff: AKIAXHCFIEC5NCZ376Q7	8 days ago

CIVIC DIGITAL FELLOWSHIP

WHAT IS BUILT

Network Configuration

- VPC
- Private/Public Subnet
- Internet Gateway
- NAT Gateway
- Route Tables

IAM Account Configuration

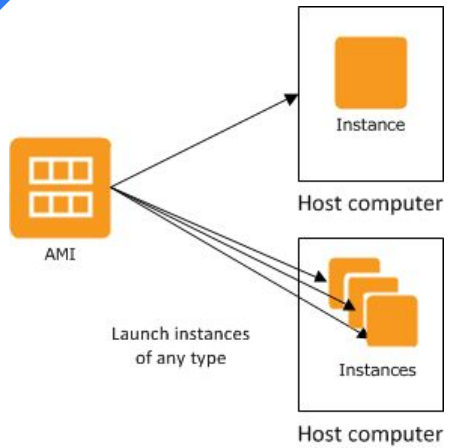
- Pre-configure security groups
- Provide security policies
- Detail user permissions

Architecture Security Configuration

- GuardDuty
- Config rules
- VPC flow logs
- Secure, encrypted logging
- Pre-made logging storage structure
- Forced MFA

Configure Custom AMI

- CentOS machine
- Install and configure NGINX
- Harden using GSA ansible roles
- Copy .pem authentication files



CIVIC DIGITAL FELLOWSHIP

WHAT IS BUILT

Network Configuration

- VPC
- Private/Public Subnet
- Internet Gateway
- NAT Gateway
- Route Tables

IAM Account Configuration

- Pre-configure security groups
- Provide security policies
- Detail user permissions

Architecture Security Configuration

- GuardDuty
- Config rules
- VPC flow logs
- Secure, encrypted logging
- Pre-made logging storage structure
- Forced MFA

Configure Custom AMI

- CentOS machine
- Install and configure NGINX
- Harden using GSA ansible roles
- Copy .pem authentication files

Deploy EC2 Instances

- Launch two web servers
- Launch one jump host
- Configure load balancer between two servers

CIVIC DIGITAL FELLOWSHIP

IT'S LIVE!

What was built?

CIVIC DIGITAL FELLOWSHIP

WHAT NEXT?

- Further integration with security tools
    - Nessus Scanning
    - Code scanning
    - Web Url scanning
    - Pipeline for hardening gold images
    - Integration logging platform etc and other security integrations

CIVIC DIGITAL FELLOWSHIP

THANKS

- Manoj Chalise
- Robert Lupinek
- Douglas Sillex

CIVIC DIGITAL FELLOWSHIP