

*Innovative. Open. Agile.*

TechFlow, Inc. Response to  
Request for Quotation (RFQ)  
4QTFHS150004  
Agile Delivery Services (ADS I)

# Continuous Monitoring

July 7, 2015



**TABLE OF CONTENTS**

1.0 Overview ..... 1

2.0 Continuous Monitoring ..... 1

3.0 Initial Configuration..... 1

**LIST OF FIGURES**

Figure 1. CloudCheckr Best Practice Recommendations ..... 2



## 1.0 Overview

Our approach to continuous monitoring incorporates preventive (robust configuration management practices) and detective (independent assessment) controls using appropriate tools found in either the Amazon Web Service (AWS) or GitHub market places. The National Institute of Standards and Technology (NIST) Publication 800-37 outlines the five components of effective continuous monitoring, which include:

- Configuration Management
- Security Impact Analysis on Changes
- Assessment of Security Controls
- Security Status Reporting
- Active Management of Security Risks

## 2.0 Continuous Monitoring

We setup and used the version of CloudCheckr integrated with AWSConfig and AWSCloudtrail for continuous monitoring for the TechFlow DARI product. This combination provides:

- Vulnerability, configuration, and asset management based on best practices.
- Near real time visibility into the system security posture through regular monitoring and analysis of security metrics through AWSConfig Reporting.
- Threat intelligence through alerts and visibility using AWSCloudtrail Reporting to ensure linkage to events related environment changes. This supports the timely mitigation of system risks and ultimately will result in a more secure operating environment.

Through the setup and use of CloudCheckr and the associated AWS tools we are able to monitor and prevent inappropriate or unauthorized changes to the security baseline. Our technical architecture documentation describes the Virtual Private Cloud (VPC) separation between the management (i.e., Puppet and Jenkins) and application (i.e., DARI app) layers of the architecture.

## 3.0 Initial Configuration

We conducted an initial security baseline for our DARI product using CloudCheckr, which provided recommendations for our product development team to implement based on best practice results. Figure 1, illustrates a subset of the results provided by CloudCheckr. Another output we used from CloudCheckr is the inventory analysis to verify:

- Running instances
- Storage used
- Identity and Access Management (IAM) groups and users
- Hosted zones and health checks
- Number of VPCs and subnets

















 <b>15 EC2-VPC Security Groups Outbound Rules Set To All Ports</b>	
Group: APP   ID: sg-2adf284e   IP Range: 0.0.0.0/0   Resources using this security group: 1   Region: US West (Oregon)	
Group: app-loadbalancer   ID: sg-03cb3c67   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: US West (Oregon)	
Group: CentOS 6 -x86_64- - with Updates-6 - 2014-09-29-AutogenByAWSMP-   ID: sg-3a12e65e   IP Range: 0.0.0.0/0   Resources using this security group: 3   Region: US West (Oregon)	
Group: default   ID: sg-5222d636   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: US West (Oregon)	
Group: default   ID: sg-aeab4dc9   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: US East (N. Virginia)	
Group: default   ID: sg-b928dcdd   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: US West (Oregon)	
Group: default   ID: sg-434ec326   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: US West (N. California)	
Group: default   ID: sg-48ac922d   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: EU (Ireland)	
Group: default   ID: sg-2f79f04a   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: Asia Pacific (Singapore)	
Group: default   ID: sg-9aa1c7ff   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: Asia Pacific (Tokyo)	
Group: default   ID: sg-e7d16882   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: South America (S?o Paulo)	
Group: default   ID: sg-107eec75   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: Asia Pacific (Sydney)	
Group: default   ID: sg-148f277d   IP Range: 0.0.0.0/0   Resources using this security group: 0   Region: EU (Frankfurt)	
Group: HAProxy   ID: sg-d8f80ebc   IP Range: 0.0.0.0/0   Resources using this security group: 1   Region: US West (Oregon)	
Group: Web   ID: sg-b01febd4   IP Range: 0.0.0.0/0   Resources using this security group: 2   Region: US West (Oregon)	

Figure 1. CloudCheckr Best Practice Recommendations