CloudPassage Operations Document

CONFIDENTIAL This document and the information set forth herein are the proprietary property of Informatica, and are to be held in confidence. No part of this document may be copied, reproduced or disclosed to third parties without the expressed written consent of Informatica.	**DCN:** 3.13.1	**Revision**: 1.2
	Origination Date: 06/12/2015	**Revision Date:** 05/10/2016
	Author: Howard Lu/Cody Mercer	
	Status: Not Approved (DRAFT)	

Table of Contents

Events

1. CloudPassage events will be sent to Sumologic
    a) Filters will be setup in Sumologic to consume CloudPassage logs
2. The SOC respond to CloudPassage events as needed
    a) SOP's will be written regarding ticket types at a later date
        - <Bringing in 3rd party to help us on this>
    b) Tickets will be created via remedy force and assigned to the necessary parties.
3. Spin up incident response plan if necessary
    a) Refer to incident response plan for more information (link).

Granting Access

1. Console access will be granted to the people who need it
    a) Requests will need to be approved by Bill Burns

Defining Policies

1. Put all machines into specific buckets based on their intended use. Below is the list of different buckets that are currently in use. Applications with multiple tiers will have buckets based on each tier.
    a) Zabbix
    b) Domain Controllers
    c) Syslog
    d) Chef
    e) ICS Data Wizard
    f) Discovery IQ
        - Discovery IQ App
        - Discovery IQ DB
        - Discovery IQ Web
    g) REV
        - REV App
        - REV DB
        - REV Web
2. Policies are defined based on OS and applications that run on server
    a) Using default out of the box policies for OS's
    b) Additional configuration will need to be created for each of the Applications

Onboarding

1. Instances that need to be on-boarded in production and non-production environments will need to have change request associated with them. There should be no agent installs without a corresponding Change Request.

2. Each instance that needs to be on-boarded should fall under one of the following categories.
    a) Zabbix
    b) Domain Controllers
    c) Syslog
    d) Chef
    e) ICS Data Wizard
    f) Discovery IQ
        - Discovery IQ App
        - Discovery IQ DB
        - Discovery IQ Web
    g) REV
        - REV App
        - REV DB
        - REV Web
3. Application Servers will be assigned grouping automatically via tags
    a) The server startup script will need to be modified accordingly
        - sudo /etc/init.d/cphalod start --daemon-key=*your-daemon-key* --tag=*servertag*
        - Rev will have the tag REV, ICS Datawizard will have tag DW and Discovery IQ will have tag DIQ

Patching

1. Using the CP API we will import all SVA data into Keylight so it can be assigned to the correct individuals
    a) If patching needs to be done to non-management plane servers, please contact the application owners and coordinate with them for their patching cycles

Production Deployment Process

1. For servers located in the management plane in production. Instances that need to be on-boarded in production and non-production environments will need to have change request associated with them. There should be no agent installs without a corresponding Change Request.
2. All other servers will need to be QA'd with each specific app team before production deployment can happen
    a) Once QA is complete work with application owners to setup correct automation
    b) <This section needs more work, as we still don't know what the process will look like>

Troubleshooting Issues/Requests

1. If there are any troubleshooting issues please contact Cody Mercer
    a) If Cody can't answer. He will direct the user to the appropriate resource or resources

Appendix

1. CP Instance Vulnerability Script
https://informatica.app.box.com/files/0/f/7857778465/1/f_64773204117

2. CP Agent Install Script

https://informatica.app.box.com/files/0/f/7857778465/1/f_64773192053

3. CP AMI Security Assessment

https://informatica.app.box.com/files/0/f/7857778465/1/f_64773005493