Carbon Black.

CONNECT

POWER OF YOU

Monday June 3, 2019

Developer Day

dev:~$ _

Getting to "Done"
Faster and with Less Effort with Carbon Black APIs

Carbon Black.
CONNECT
POWER OF YOU

Follow along @ https://github.com/redcanaryco/cbconnect-2019

Follow along @ https://github.com/redcanaryco/cbconnect-2019

red canary Carbon Black.

Follow along @ https://github.com/redcanaryco/cbconnect-2019

Bad Thing Happens

1. Receive alert
2. Find process
3. Find endpoint
4. Enrich with external info
5. Isolate endpoint
6. Remediate threat

→ Bad Thing Remediated

Follow along @ https://github.com/redcanaryco/cbconnect-2019

Bad Thing Happens

1. Receive alert
2. Find process
3. Find endpoint
4. Enrich with external info
5. Isolate endpoint
6. Remediate threat

Bad Thing Remediated

Carbon Black Process Search!

Carbon Black Endpoint Isolation!

Carbon Black Live Response!

first_try.rb

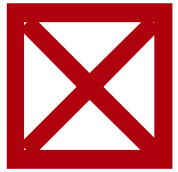
```ruby
#! /usr/bin/env ruby
AlertReceiver.new.when_alert_received do |alert|

  alert_process_name = extract_process_name_from_alert(alert)
  alert_hostname = extract_hostname_from_alert(alert)

  process_info = Actions::FindProcess.call process_name: alert_process_name, hostname: alert_hostname

  endpoint_info = Actions::FindEndpoint.call hostname: process_info['hostname']

  process_info = Actions::EnrichProcessWithPrevalenceInfo.call process_info: process_info

  endpoint_os = endpoint_info['os_environment_display_string'].to_s.downcase
  endpoint_type = if endpoint_os.include?('server') || (endpoint_os.include?('linux') && !endpoint_os.include?('desktop'))
                    'server'
                  else
                    'workstation'
                  end

  case endpoint_type
  when 'server'
    Actions::RemediateProcess.call process_name: process_info['process_name'], sensor_id: endpoint_info['sensor_id']

  when 'workstations'
    Actions::IsolateEndpoint.call sensor_id: endpoint_info['sensor_id']

    Actions::RemediateProcess.call process_name: process_info['process_name'], sensor_id: endpoint_info['sensor_id']
  end
end
```


red canary Carbon Black.

Bad Thing Happens

1. **Receive alert**
2. **Find process**
   a. Can't find it yet!
3. **Find endpoint**
4. **Enrich with external info**
5. **Isolate endpoint**
   a. It's offline!
6. **Remediate threat**
   a. It's still offline!

Bad Thing Remediated



Bad Thing NOT Remediated

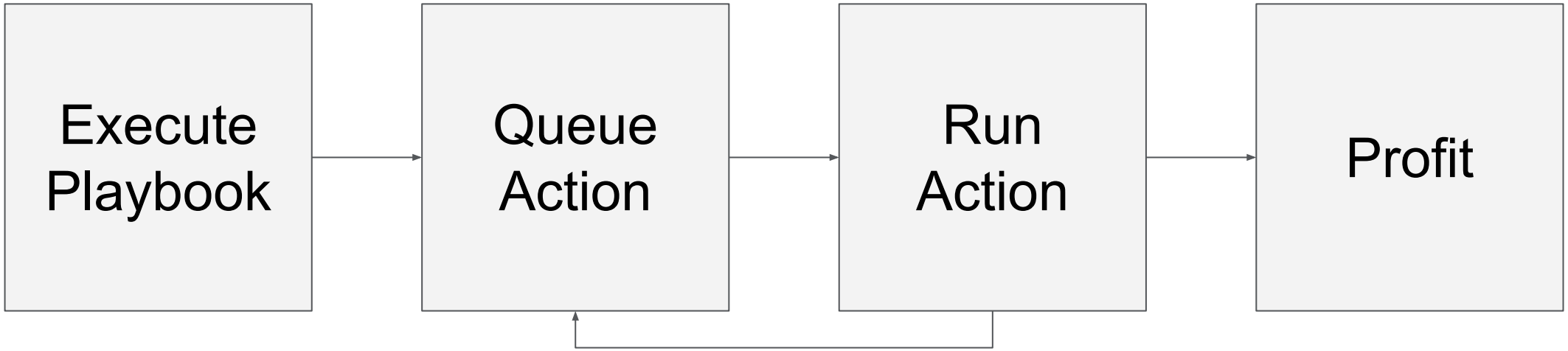
red canary Carbon Black.

Key requirements for our solution

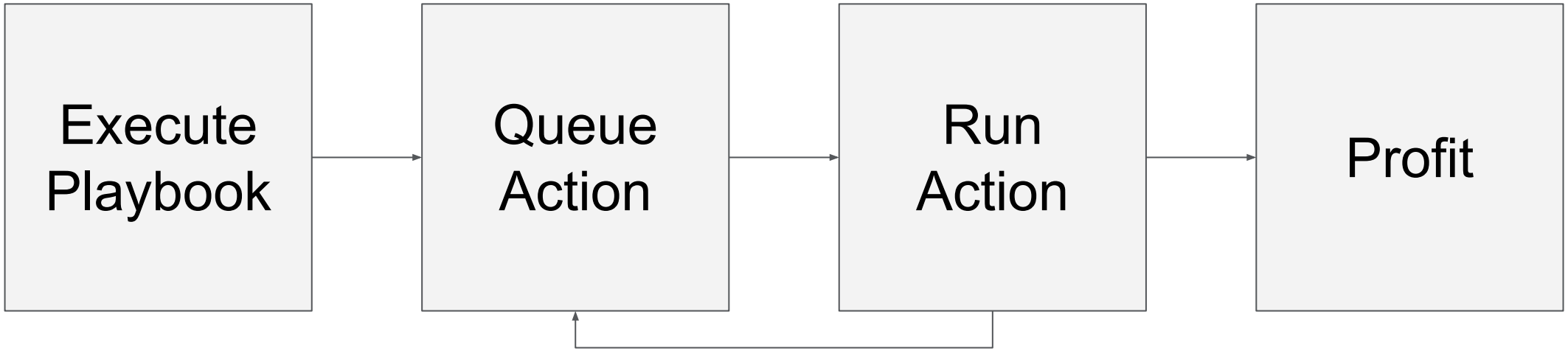
- Run code
- Expect failure
- Highly resilient
- Easy to deploy

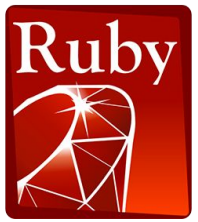
red canary Carbon Black.

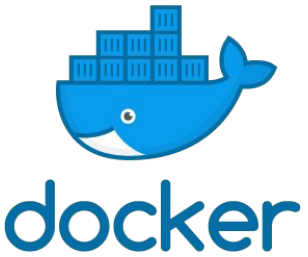
Solve with a simple architecture



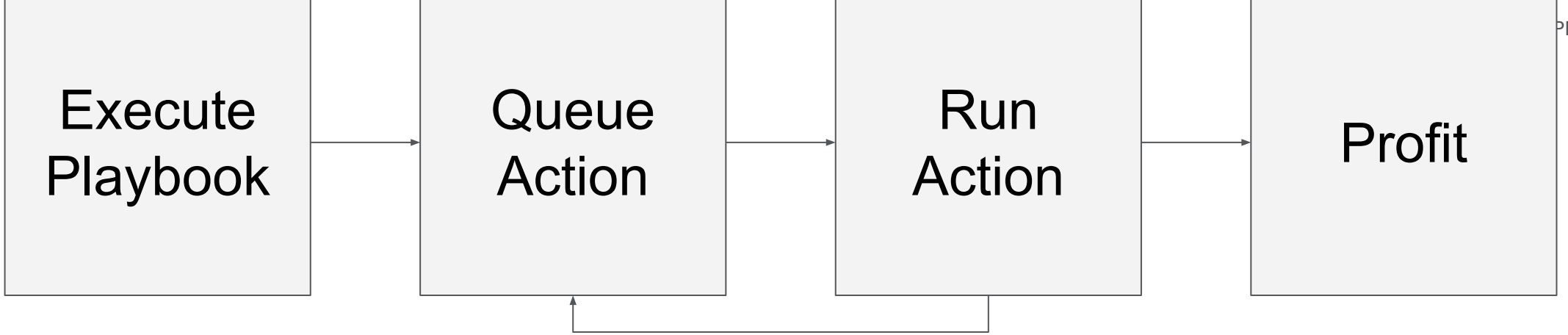
Solve with a simple architecture… all open source!

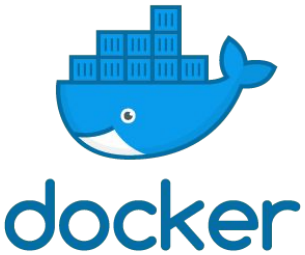






PER DAY dev:~$ _

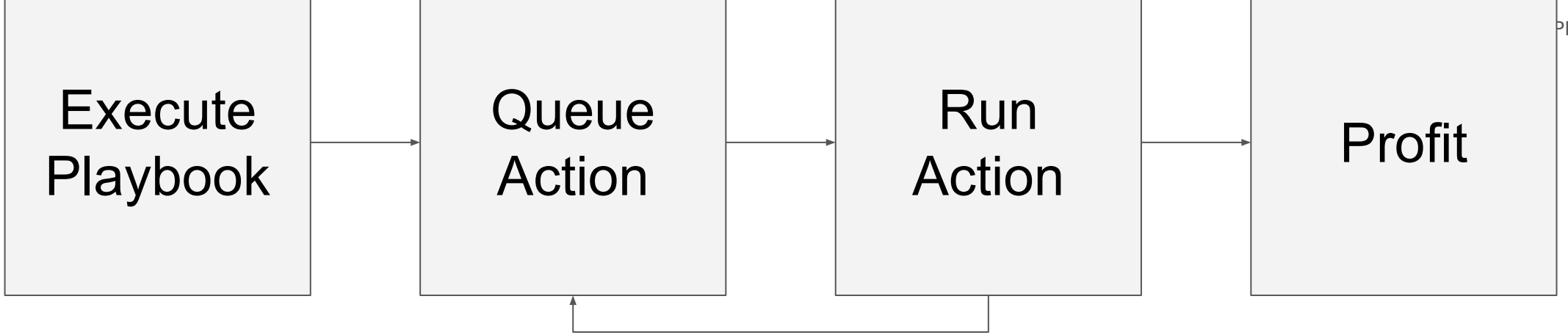


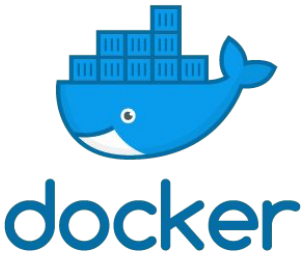


Highly readable

Easy to learn

PER DAY dev:~$ _



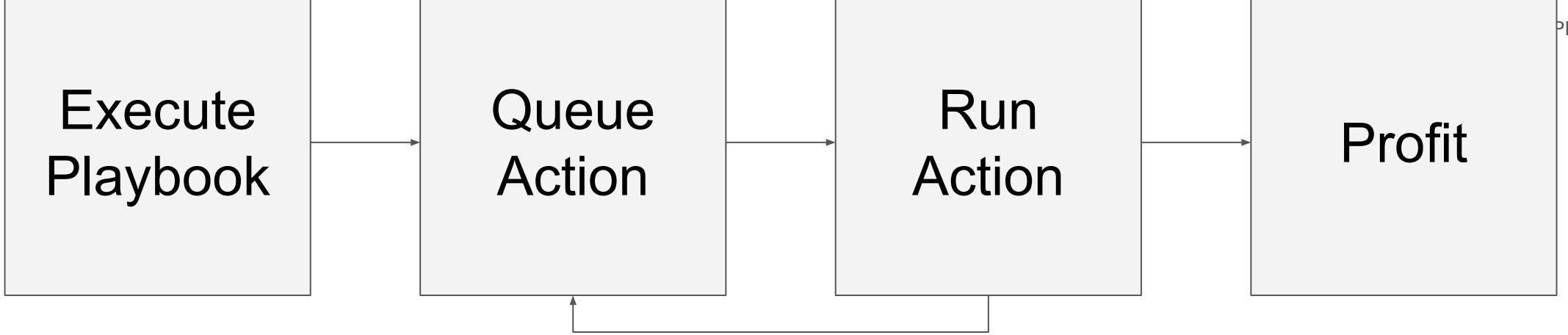


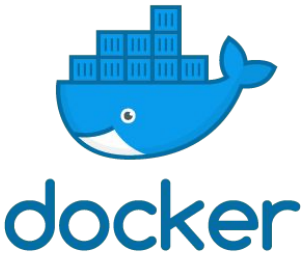
Fast key/value store

Lightweight

red canary Carbon Black.

PER DAY dev:~$ _

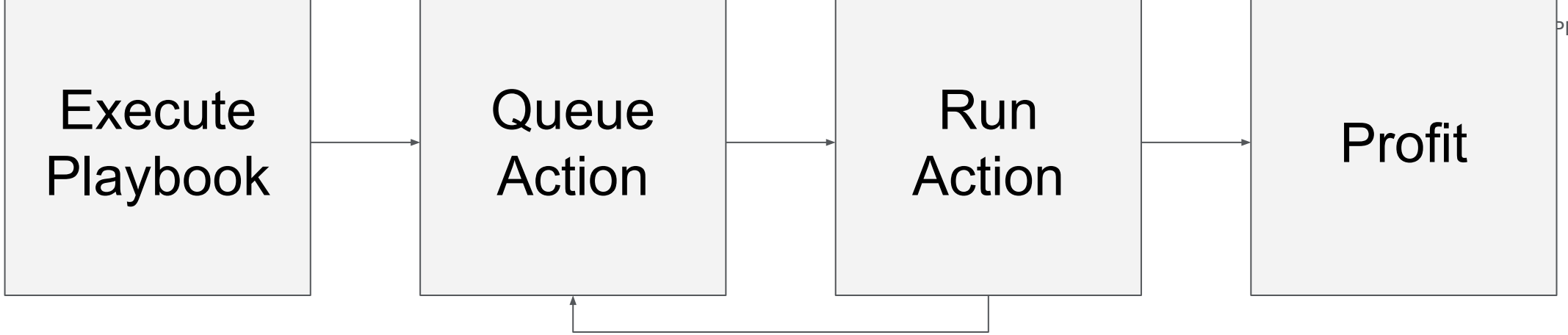


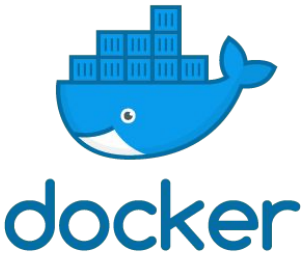


Job runner

Production grade

PER DAY dev:~$ _

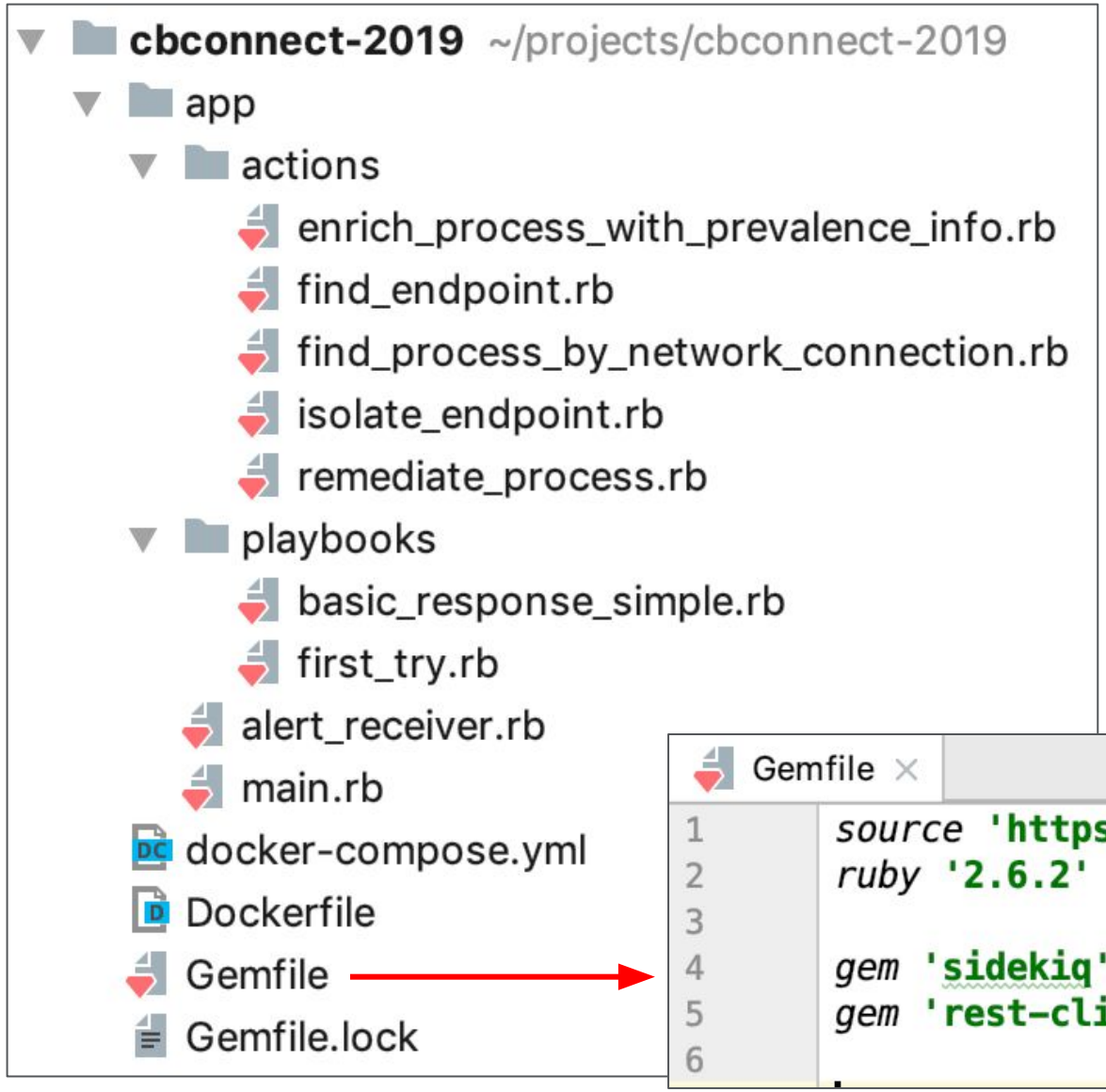




Dead simple deployments in dev AND production

red canary Carbon Black.

Step 0: Setup our project




```
~/projects/cbconnect-2019 $ bundle install
Fetching gem metadata from https://rubygems.org/.........
Fetching gem metadata from https://rubygems.org/.
Resolving dependencies...
Using bundler 1.17.2
Using unf_ext 0.0.7.6
Using mime-types-data 3.2019.0331
Using netrc 0.11.0
Fetching connection_pool 2.2.2
Fetching redis 4.1.1
Fetching rack 2.0.7
Using unf 0.1.4
Using mime-types 3.2.2
Using domain_name 0.5.20180417
Using http-cookie 1.0.3
Using rest-client 2.0.2
Installing connection_pool 2.2.2
Installing redis 4.1.1
Installing rack 2.0.7
Fetching rack-protection 2.0.5
Installing rack-protection 2.0.5
Fetching sidekiq 5.2.7
Installing sidekiq 5.2.7
Bundle complete! 2 Gemfile dependencies, 14 gems now installed.
Use `bundle info [gemname]` to see where a bundled gem is installed.
~/projects/cbconnect-2019 $
```

Gemfile

```
1  source 'https://rubygems.org'
2  ruby '2.6.2'
3
4  gem 'sidekiq'
5  gem 'rest-client'
6
```

Step 1: Define our actions

```ruby
module Actions
  class FindProcessByNetworkConnection
    def call(sensor_id:, destination_ip:, destination_port:)
      puts "  ** FindProcessByNetworkConnection"
      query = {
          'q' => ["ipaddr:#{destination_ip} ipport:#{destination_port} sensor_id:#{sensor_id}"],

          'sort' => 'last_update desc',
          'facet' => ['false', 'false'],
          'rows' => 10,
          'cb.urlver' => ['1'],
          'start' => 0,
          'timeAllowed' => 60000
      }

      url = "#{cb_url}/api/v1/process"
      response = RestClient::Resource.new(url, headers: {'X-Auth-Token' => cb_auth_token, accept: :json}).
          post query.to_json, content_type: :json

      results = JSON.parse response.body
    end
  end
end
```

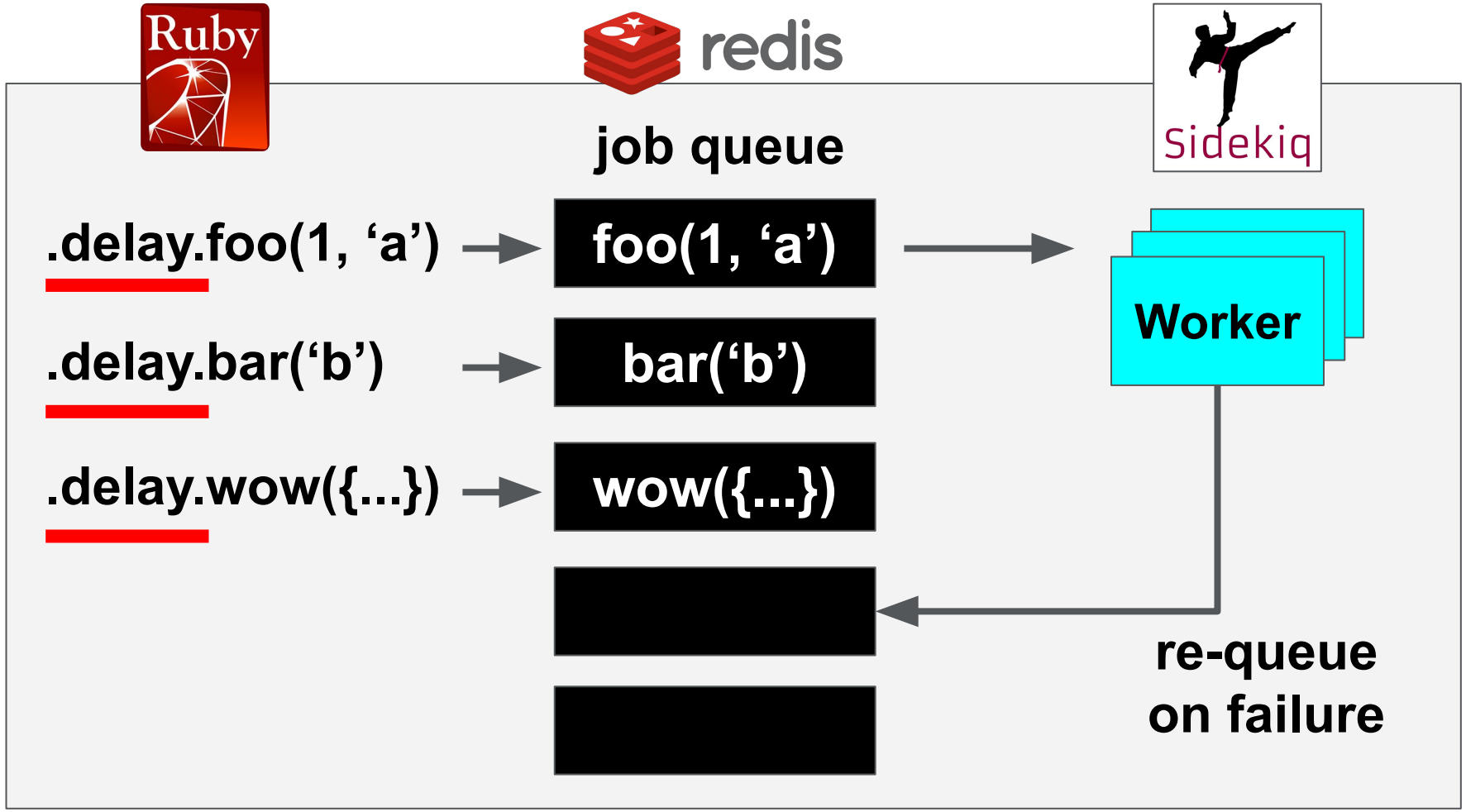
Step 1: Define our actions (cont)

```ruby
module Actions
  class IsolateEndpoint
    def call(cb_url:, cb_auth_token:, sensor_id:)

      # get current information about the sensor
      url = "#{cb_url}/api/v1/sensor/#{sensor_id}"
      response = RestClient::Resource.new(url, headers: {'X-Auth-Token' => cb_auth_token, accept: :json}).get
      sensor_info = JSON.parse response.body

      # set isolation flag to true
      sensor_info['network_isolation_enabled'] = true

      # apply it
      RestClient::Resource.new(url, headers: {'X-Auth-Token' => cb_auth_token, accept: :json}).
          put(sensor_info.to_json, content_type: :json)
    end
  end
end
```

Step 2: Execute playbook

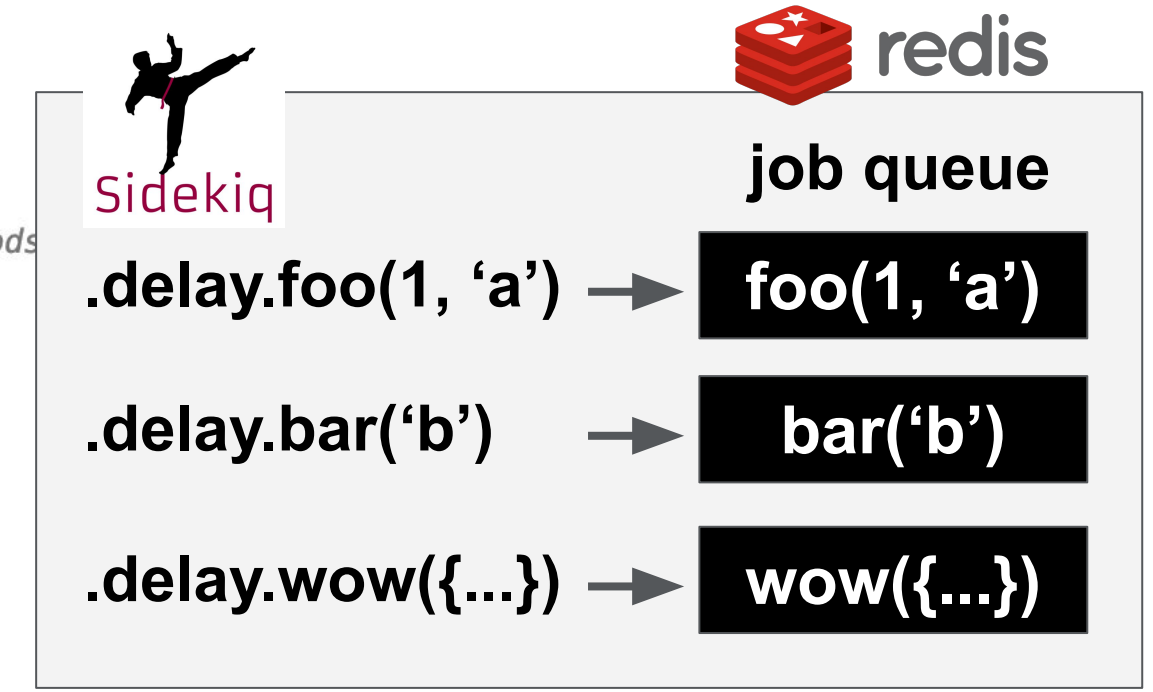
```
 9  module Playbooks
10    class BasicResponseSimple
11      def run!
12        puts "Starting playbook BasicResponseSimple"
13        AlertReceiver.new.get_alerts.each do |alert|
14          puts "- Processing alert #{alert['id']}"
15          self.class.delay.step0_parse_alert(alert: alert)
16        end
17      end
18
19      def self.step0_parse_alert(alert:) ... end
30
31      def self.step1_find_endpoint(source_hostname:, alert_ip_connection:) ... end
40
41      def self.step2_find_process(endpoint_info:, src_ip:, dest_ip:, dest_port:) ... end
51
52      def self.step3_enrich_process(endpoint_info:, process_info:) ... end
59
60      def self.step4_isolate_and_remediate(endpoint_info:, process_info:) ... end
87    end
88  end
```

Step 3: Queue action



Step 3: Queue action

```ruby
def run!
  # we want simpler code by calling `.delay` on methods
  Sidekiq::Extensions.enable_delay!

  puts "Starting playbook BasicResponseSimple"
  AlertReceiver.new.when_alert_received do |alert:|
    puts "- Processing alert #{alert['id']}"
    self.class.delay.step0_parse_alert(alert: alert)
  end
end

def self.step0_parse_alert(alert:)
  puts "- Step0", alert, alert.keys
  delay.step1_find_endpoint source_hostname: alert_source_hostname, alert_ip_connection: alert_ip_connection
end

def self.step1_find_endpoint(source_hostname:, alert_ip_connection:)
  puts "- Step1"
  endpoint_info = Actions::FindEndpoint.new.call hostname: source_hostname

  delay.step2_find_process endpoint_info: endpoint_info, src_ip: alert_ip_connection['src_ip'],
                           dest_ip: alert_ip_connection['dest_ip'], dest_port: alert_ip_connection['dest_port']
end
```



Step 4: Run action

```
sidekiq-container_1 | 2019-06-03T05:48:19.851Z JID-4dd7c9cd52ad38d0505c1938 INFO: start
sidekiq-container_1 | - Step0
sidekiq-container_1 | 2019-06-03T05:48:19.856Z JID-8c6db9c67c91fd9c1f64614a INFO: start
sidekiq-container_1 | - Step1
sidekiq-container_1 |   ** FindEndpoint hostname=ChrissMacBook2
sidekiq-container_1 | 2019-06-03T05:48:19.862Z JID-4dd7c9cd52ad38d0505c1938 INFO: done: 0.011 sec
sidekiq-container_1 | 2019-06-03T05:48:19.862Z JID-8c6db9c67c91fd9c1f64614a INFO: done: 0.007 sec
sidekiq-container_1 | 2019-06-03T05:48:19.864Z JID-3c5535a9a68d405416f9192d INFO: start
sidekiq-container_1 | - Step2
sidekiq-container_1 |   ** FindProcessByNetworkConnection sensor_id=123 destination_ip=192.168.1.64
sidekiq-container_1 | 2019-06-03T05:48:19.867Z JID-c902321f24ca202e7c104418 INFO: start
sidekiq-container_1 | 2019-06-03T05:48:19.867Z JID-3c5535a9a68d405416f9192d INFO: done: 0.004 sec
sidekiq-container_1 | - Step3
sidekiq-container_1 |   ** EnrichProcessWithPrevalenceInfo
sidekiq-container_1 | 2019-06-03T05:48:19.870Z JID-c902321f24ca202e7c104418 INFO: done: 0.003 sec
sidekiq-container_1 | 2019-06-03T05:48:19.871Z JID-2957c78b50b77206fcd9c5fa INFO: start
sidekiq-container_1 | - Step4
sidekiq-container_1 |   ** IsolateEndpoint isolating sensor_id=123
sidekiq-container_1 |   ** RemediateProcess
sidekiq-container_1 |     - terminating process_pid=374 on sensor_id=123
sidekiq-container_1 |     - banning md5=7c1a00c878eb89cb03be9b8133141b1b
sidekiq-container_1 | 2019-06-03T05:48:19.873Z JID-2957c78b50b77206fcd9c5fa INFO: done: 0.002 sec
```

Step 5: Run it!

Dockerfile

```
1  FROM ruby:2.6.2
2
3  RUN gem install bundler
4
5  ENV LC_ALL=C.UTF-8 \
6      LANG=en_US.UTF-8 \
7      LANGUAGE=en_US.UTF-8 \
8      APP_HOME=/app
9
10 RUN mkdir $APP_HOME
11 WORKDIR $APP_HOME
12
13 COPY Gemfile Gemfile.lock $APP_HOME/
14 RUN bundle install
15
16 # bring over our app
17 COPY . $APP_HOME
18
19 CMD ["bundle", "exec", "sidekiq", "-r",
```

```
~/projects/cbconnect-2019 $ docker build .
Sending build context to Docker daemon  20.99kB
Step 1/9 : FROM ruby:2.6.2
 ---> 8d6721e9290e
Step 2/9 : RUN gem install bundler
 ---> Using cache
 ---> 145410a55739
Step 3/9 : ENV LC_ALL=C.UTF-8     LANG=en_US.UTF-8     LANGUAGE=en_US.UTF-8
APP_HOME=/app
 ---> Using cache
 ---> a4905dd469a8
Step 4/9 : RUN mkdir $APP_HOME
 ---> Using cache
 ---> b8e357c39f46
Step 5/9 : WORKDIR $APP_HOME
 ---> Using cache
 ---> 136d4f0912d6
Step 6/9 : COPY Gemfile Gemfile.lock $APP_HOME/
 ---> Using cache
 ---> 0e4533c9fbe6
Step 7/9 : RUN bundle install
 ---> Using cache
 ---> a96e777325e1
Step 8/9 : COPY . $APP_HOME
 ---> aac5e00d559d
Step 9/9 : CMD ["bundle", "exec", "sidekiq", "-r", "/app/app/main.rb"]
 ---> Running in a1da45f0435f
Removing intermediate container a1da45f0435f
 ---> b5855186c3c5
Successfully built b5855186c3c5


~/projects/cbconnect-2019 $ docker run b5855186c3c5
Starting playbook BasicResponseSimple
```

Step 5: Run it!

docker-compose.yml

```
1   version: '3'
2   services:
3     sidekiq-container:
4       build:
5         context: .
6       command: ["bundle", "exec", "sidekiq", "-r", "/app/app/main.rb"]
7       environment:
8         - REDIS_PROVIDER=REDIS_URL
9         - REDIS_URL=redis://redis-container
10      volumes:
11        - .:/app
12      depends_on:
13        - redis-container
14
15    redis-container:
16      image: redis:3.2.8
17      expose:
18        - 6379
```

```
redis-container_1    | 1:C 03 Jun 04:33:14.932 # Warning: no config file specified, using the default config. In order to specif
er /path/to/redis.conf
redis-container_1    |
redis-container_1    |                 _.-``__ ''-._
redis-container_1    |            _.-``    `.  `_.  ''-._           Redis 3.2.8 (00000000/0) 64 bit
redis-container_1    |        .-`` .-```.  ```\/    _.,_ ''-._
redis-container_1    |       (    '      ,       .-`  | `,    )     Running in standalone mode
redis-container_1    |       |`-._`-...-` __...-.``-._|'` _.-'|     Port: 6379
redis-container_1    |       |    `-._   `._    /     _.-'    |     PID: 1
redis-container_1    |        `-._    `-._  `-./  _.-'    _.-'
redis-container_1    |       |`-._`-._    `-.__.-'    _.-'_.-'|
redis-container_1    |       |    `-._`-._        _.-'_.-'    |           http://redis.io
redis-container_1    |        `-._    `-._`-.__.-'_.-'    _.-'
redis-container_1    |       |`-._`-._    `-.__.-'    _.-'_.-'|
redis-container_1    |       |    `-._`-._        _.-'_.-'    |
redis-container_1    |        `-._    `-._`-.__.-'_.-'    _.-'
redis-container_1    |            `-._    `-.__.-'    _.-'
redis-container_1    |                `-._        _.-'
redis-container_1    |                    `-.__.-'
redis-container_1    |
redis-container_1    | 1:M 03 Jun 04:33:14.933 # WARNING: The TCP backlog setting of 511 cannot be enforced because /proc/sys/ne
 lower value of 128.
redis-container_1    | 1:M 03 Jun 04:33:14.933 # Server started, Redis version 3.2.8
redis-container_1    | 1:M 03 Jun 04:33:14.933 # WARNING you have Transparent Huge Pages (THP) support enabled in your kernel. T
mory usage issues with Redis. To fix this issue run the command 'echo never > /sys/kernel/mm/transparent_hugepage/enabled' as ro
.local in order to retain the setting after a reboot. Redis must be restarted after THP is disabled.
redis-container_1    | 1:M 03 Jun 04:33:14.933 * The server is now ready to accept connections on port 6379
sidekiq-container_1  | Starting playbook BasicResponseSimple
sidekiq-container_1  | Waiting for alerts
sidekiq-container_1  | .
sidekiq-container_1  | .
sidekiq-container_1  | .
sidekiq-container_1  | Got an alert!
sidekiq-container_1  | - Processing alert
sidekiq-container_1  | 2019-06-03T04:33:18.997Z  INFO: Booting Sidekiq 5.2.7 with redis options {:id=>"Sidekiq-server-PID-1", :u
sidekiq-container_1  | 2019-06-03T04:33:19.002Z  INFO: Running in ruby 2.6.2p47 (2019-03-13 revision 67232) [x86_64-linux]
sidekiq-container_1  | 2019-06-03T04:33:19.002Z  INFO: See LICENSE and the LGPL-3.0 for licensing details.
sidekiq-container_1  | 2019-06-03T04:33:19.002Z  INFO: Upgrade to Sidekiq Pro for more features and support: http://sidekiq.org
sidekiq-container_1  | 2019-06-03T04:33:19.003Z  WARN: Sidekiq 6.0 will require Redis 4.0+, you are using Redis v3.2.8
sidekiq-container_1  | 2019-06-03T04:33:19.003Z  INFO: Starting processing, hit Ctrl-C to stop
sidekiq-container_1  | 2019-06-03T04:33:19.011Z JID-2e9b14c5697e9909c42577d7 INFO: start
sidekiq-container_1  | - Step0
sidekiq-container_1  | 2019-06-03T04:33:19.022Z JID-a1300474dd06dc57af3d5585 INFO: start
sidekiq-container_1  | 2019-06-03T04:33:19.023Z JID-2e9b14c5697e9909c42577d7 INFO: done: 0.012 sec
```


Carbon Black.

www.CarbonBlack.com

Thank you.

brian@redcanary.com
@redcanaryco

Carbon Black.