
# Metric Driven Development in SECDEVOPS

**Charles Herring**
Co-Founder, CTO

CharlesHerring.com
@charlesherring
Charles@WitFoo.com

# About Charles

**1995-2002**: Forward Deployed US Navy Hornet Avionics Tech

**2002-2005** US Naval Postgraduate School
Network Security Group Division Officer
*sk3wl 0f r00t* team member

**2003-2008**: InfoWorld Test Center
Contributing Product Reviewer – Network and Information Security

**2005-2012** DoD Security, Data & Workflow Consultant

**2012-2016**: Consulting Security Architect for Lancope then Cisco Systems

**2016** CTO & co-founder at WitFoo

# Agenda

- Unit Tests
- System Tests
- SAST
- Vulnerability Scans
- Containerization
- Custom Builds
- Application Performance Monitoring
- Automated Metric Analysis

# WitFoo Precinct Development Goals

- Comprehensive Security Operations Platform
- Turn-key usability (no professional services or maintenance)
- “Always up” Architecture
- Secure Platform
- Deploy Software on-prem, cloud, hosted or hybrid
- Infinite data ingest, processing and retention
- Simple (single SKU) pricing

# WitFoo DEVOPS Components

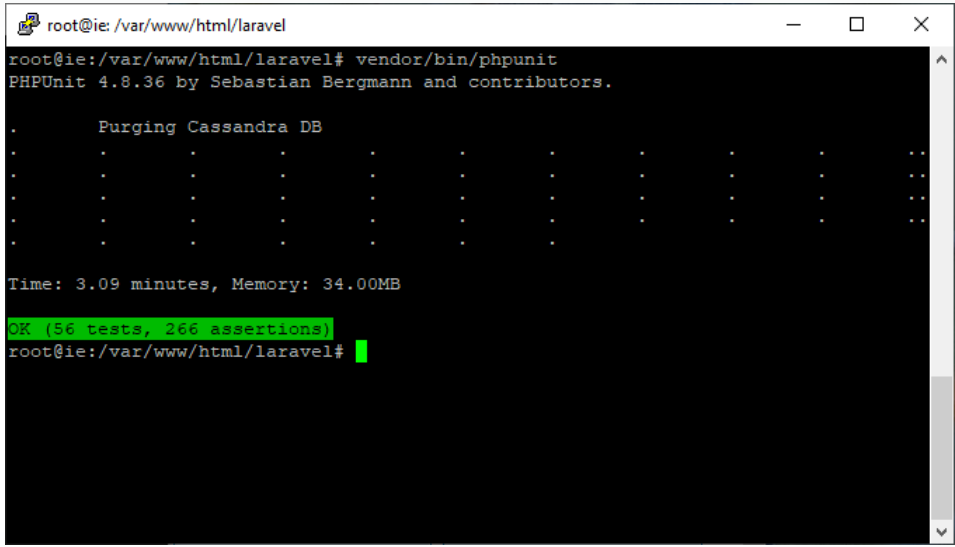




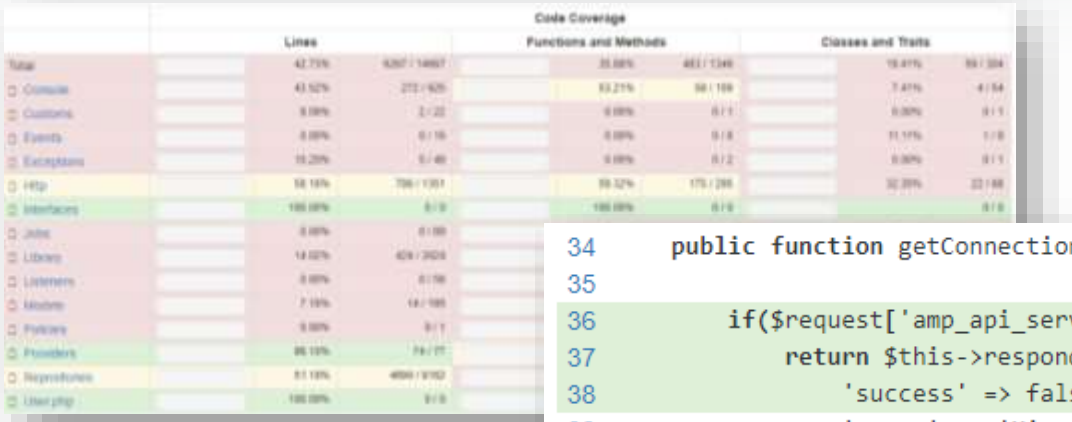
Library.witfoo.com
Registry.witfoo.com
WitFoo Superintendent

# Unit Tests

```php
public function testRegisterUser(){
    $data = array(
        'name' => 'Jimmy McNulty',
        'password' => 'F00theN0ise!',
        'email' => 'jimmy@thewire.com',
        'auth_type' => 'Local',
        'display_theme' => 'dark-theme',
        'function_role' => 1,
        'data_role' => 1,
    );
    $response = $this->call('POST', 'register',$data);
    $this->assertEquals(200, $response->status());
    $response = $this->call('GET', 'api/users');
    $this->assertEquals(200, $response->status());
    $data = $response->getData();
    $this->assertEquals(1, count($data->users->active));
    $user = $data->users->active[0];
    $this->assertEquals('Jimmy McNulty',$user->name);
    $this->assertEquals('jimmy@thewire.com',$user->email);
    $this->assertEquals('Local',$user->auth_type);
    $this->assertEquals('dark-theme',$user->display_theme);
    $this->assertEquals(1,$user->function_role);
    $this->assertEquals(1,$user->data_role);
}
```

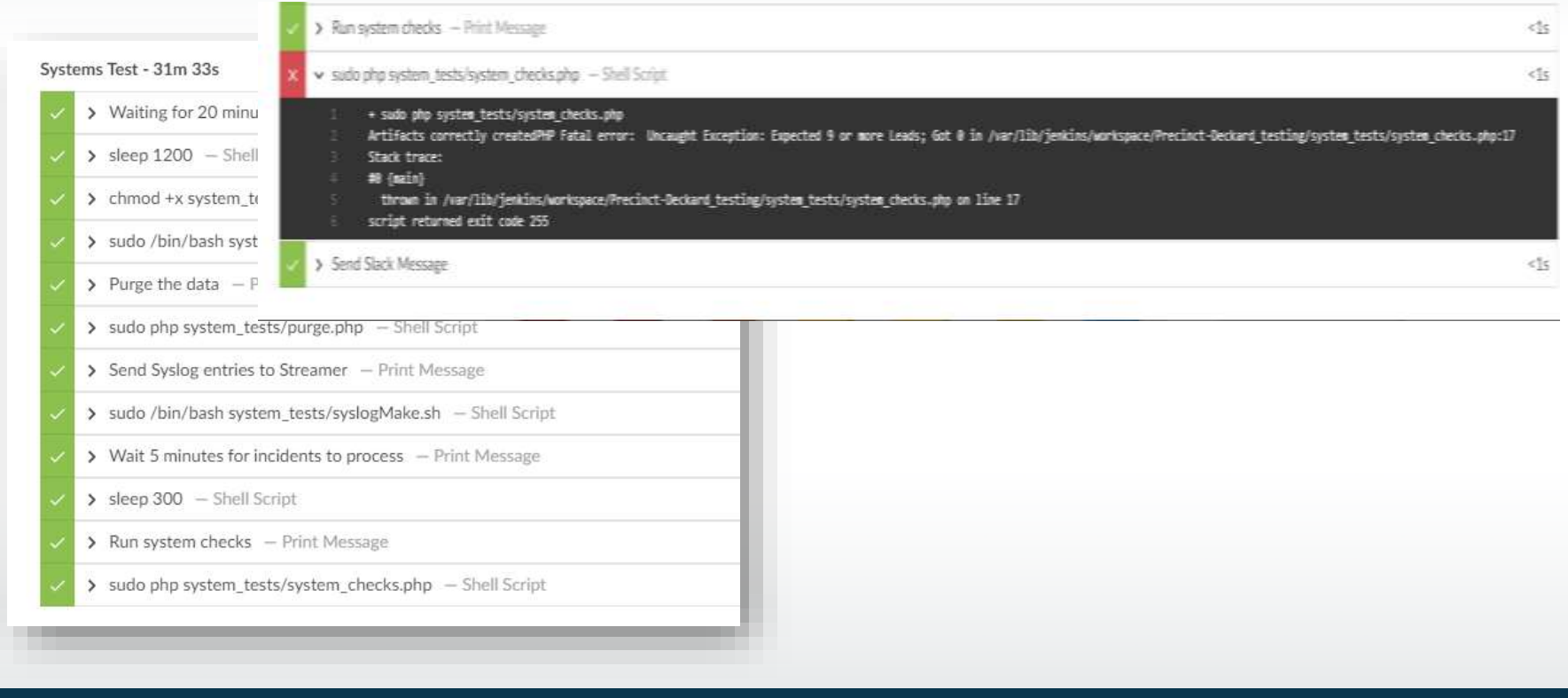


# Code Coverage

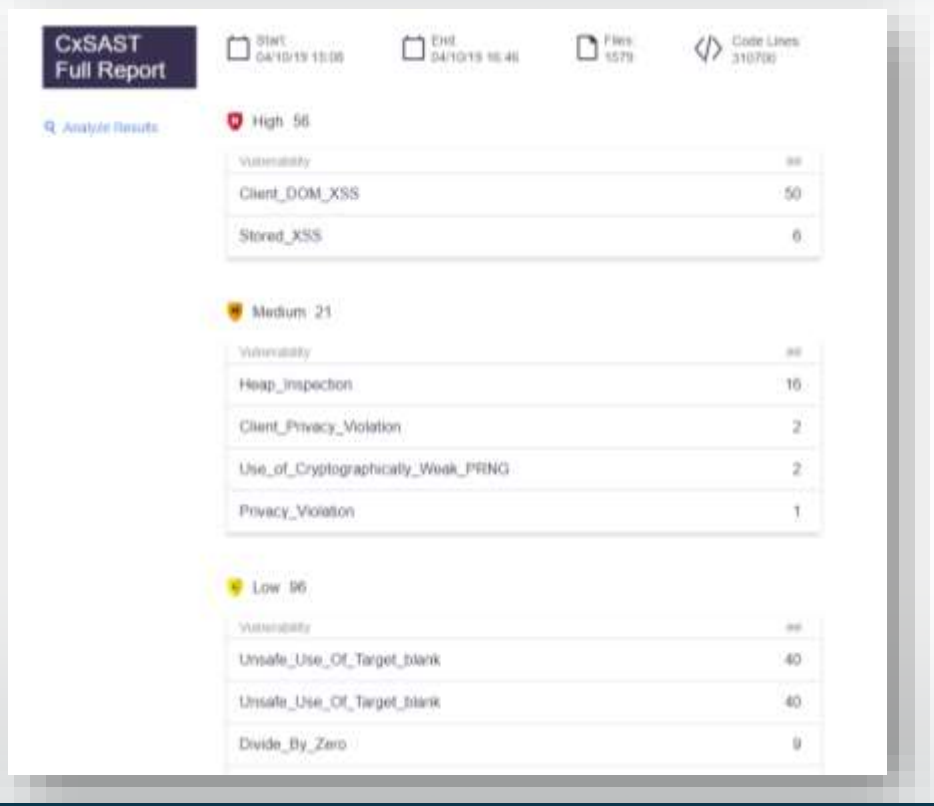



```
34      public function getConnectionStatus(Request $request){
35
36          if($request['amp_api_server'] == '' || $request['amp_api_key'] == '' || $req
37              return $this->respond(array(
38                  'success' => false,
39                  'error' => 'Missing the URL, key, or client ID'
40              ), 400);
41          }
42
43          $request['amp_api_server'] = Formatter::prependHttps($request['amp_api_serve
44          $connection_status = AMPApi::getConnectionStatus(filter_var($request['amp_ap
45          $status_code = $connection_status['success'] === true ? 200 : 400;
46          return $this->respond($connection_status, $status_code);
```

# System Tests



# Static Application Security Testing



# Vulnerability Scans / App Penetration

# Jenkins


```
pipeline {
  agent any
  stages {
    stage('Compile') {
      steps {
        sh 'cp config_files/laravel/var/www/html/laravel/.env ie/laravel/.env'
        sh 'cp ie/laravel/env_appliance_development.php ie/laravel/env.php'
        sh 'cp config_files/laravel/etc/apache2/sites-enabled/000-default.conf
        ie/000-default.conf'
        sh 'cp config_files/laravel/etc/apache2/sites-enabled/100-api.conf
        ie/100-api.conf'
        dir('ie/laravel') {
            sh '/usr/bin/composer update'
            sh '/usr/bin/composer install'
            sh '/usr/bin/composer install --optimize-autoloader'
            sh '/usr/bin/composer dump-autoload -o'
        }
        dir('ie/ngx') {
          sh 'yarn'
          sh 'ng build --prod'
        }
        sh 'cp ie/ngx/.htaccess ie/ngx/dist/'
      }
    }
    stage('Unit Tests') {
    when { not { branch 'perftesting' } }
```

# Docker Containers

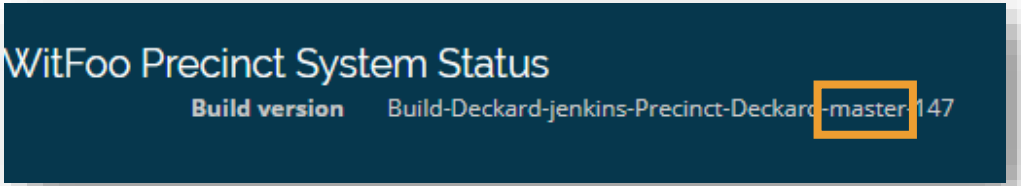
```
FROM ubuntu:xenial
LABEL maintainer "developers@witfoo.com"

USER root

ENV DEBIAN_FRONTEND noninteractive
ENV INITRD No
ENV PATH=$PATH:/usr/share/elasticsearch/bin
ENV NR_INSTALL_KEY=e3ca107ea775cc3198f51b9129af95f8572db479
ENV NR_INSTALL_SILENT=true

RUN apt-get update && apt-get install -y \
    cron \
    curl \
    apache2 \
    libapache2-
    mysql-clie
    php-fpm \
    php php-cli
```

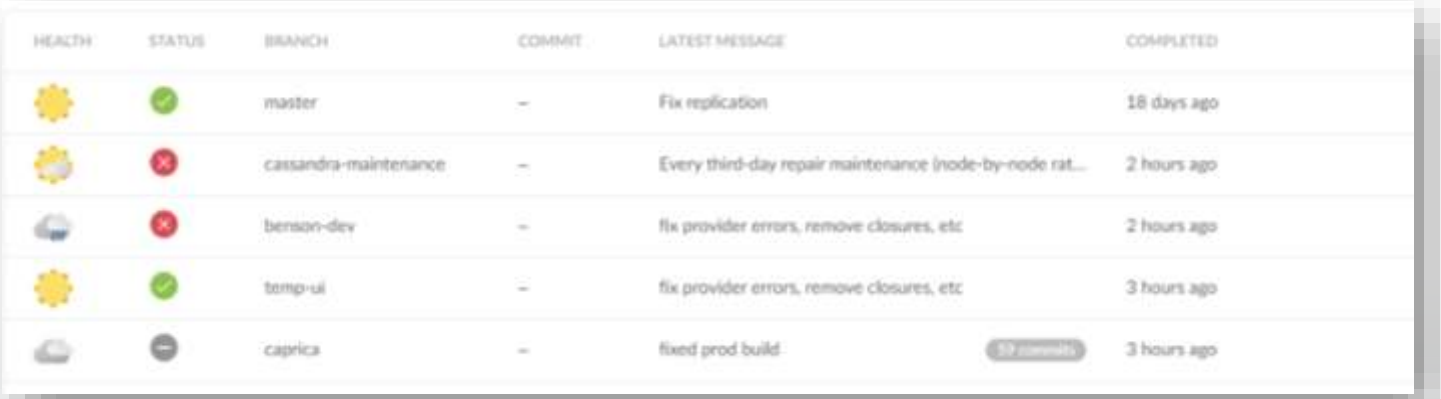
```
root@dev-charles:~# docker pull ubuntu:xenial
xenial: Pulling from library/ubuntu
a1298f4ce990: Extracting   23.4MB/44.11MB
04a3282d9c4b: Download complete
9b0d3db6dc03: Download complete
8269c605f3f1: Download complete
```

root@dev-charles: ~

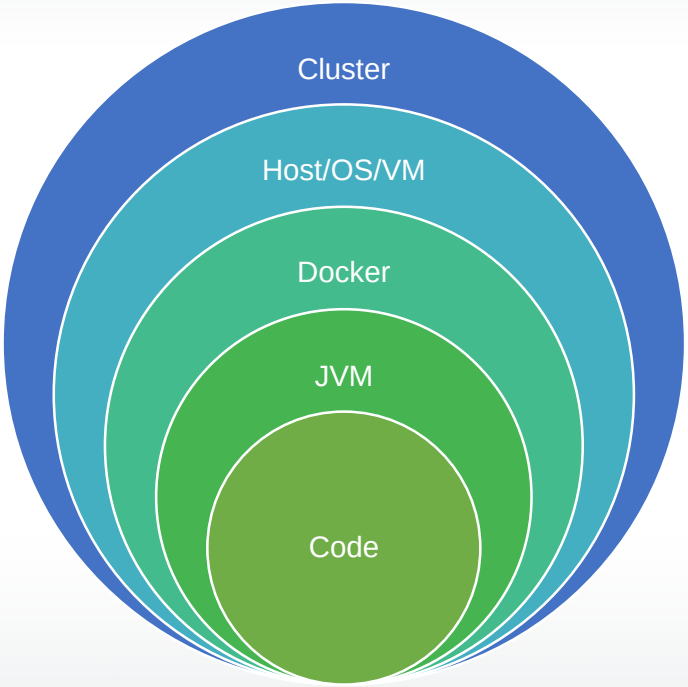
```
root@dev-charles:~# docker ps
CONTAINER ID        IMAGE                                          COMMAND                  CREATED             STATUS
a46a51d1f3a0        registry.witfoo.com/witfoo/streamer:temp-ui    "start-streamer"         2 hours ago         Up 2 hours
5e0829fd2a66        registry.witfoo.com/witfoo/logstash:temp-ui    "start-logstash"         2 hours ago         Up 2 hours
f65f0a3e3c2c        registry.witfoo.com/witfoo/ie:temp-ui          "/usr/bin/start-witf…"   2 hours ago         Up 2 hours
fc508863e15a        registry.witfoo.com/witfoo/cassandra:temp-ui   "docker-entrypoint.s…"   2 hours ago         Up 2 hours
a28858949882        registry.witfoo.com/witfoo/mysql-cluster:temp-ui   "/entrypoint.sh mysq…"   2 hours ago         Up 2 hours (healthy)
4703c3873db7        registry.witfoo.com/witfoo/metricbeat:temp-ui  "/bin/sh -c metricbe…"   2 hours ago         Up 2 hours
4e0c418e9c1c        registry.witfoo.com/witfoo/kafka:temp-ui       "start-kafka.sh"         2 hours ago         Up 2 hours
04ae03818dd7        registry.witfoo.com/witfoo/zookeeper:temp-ui   "/bin/sh -c '/usr/sb…"   2 hours ago         Up 2 hours
root@dev-charles:~#
```

# Custom(er) Builds

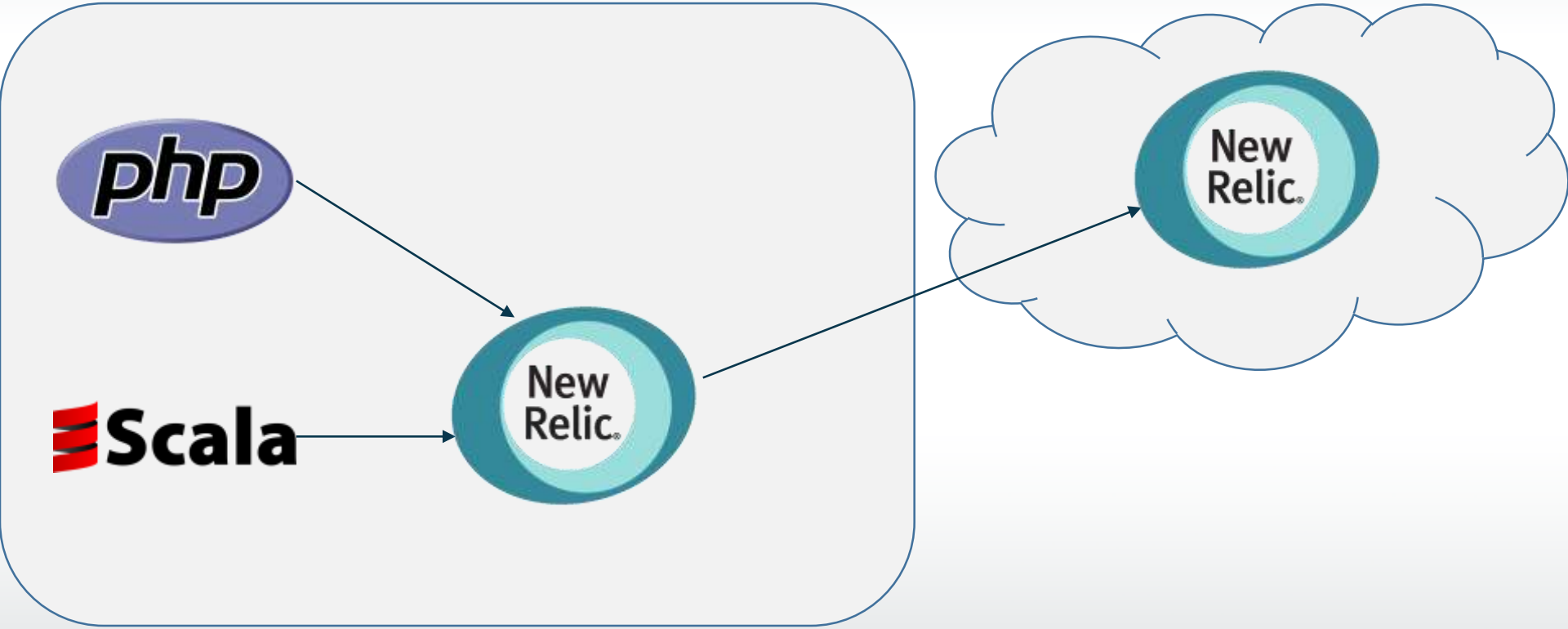


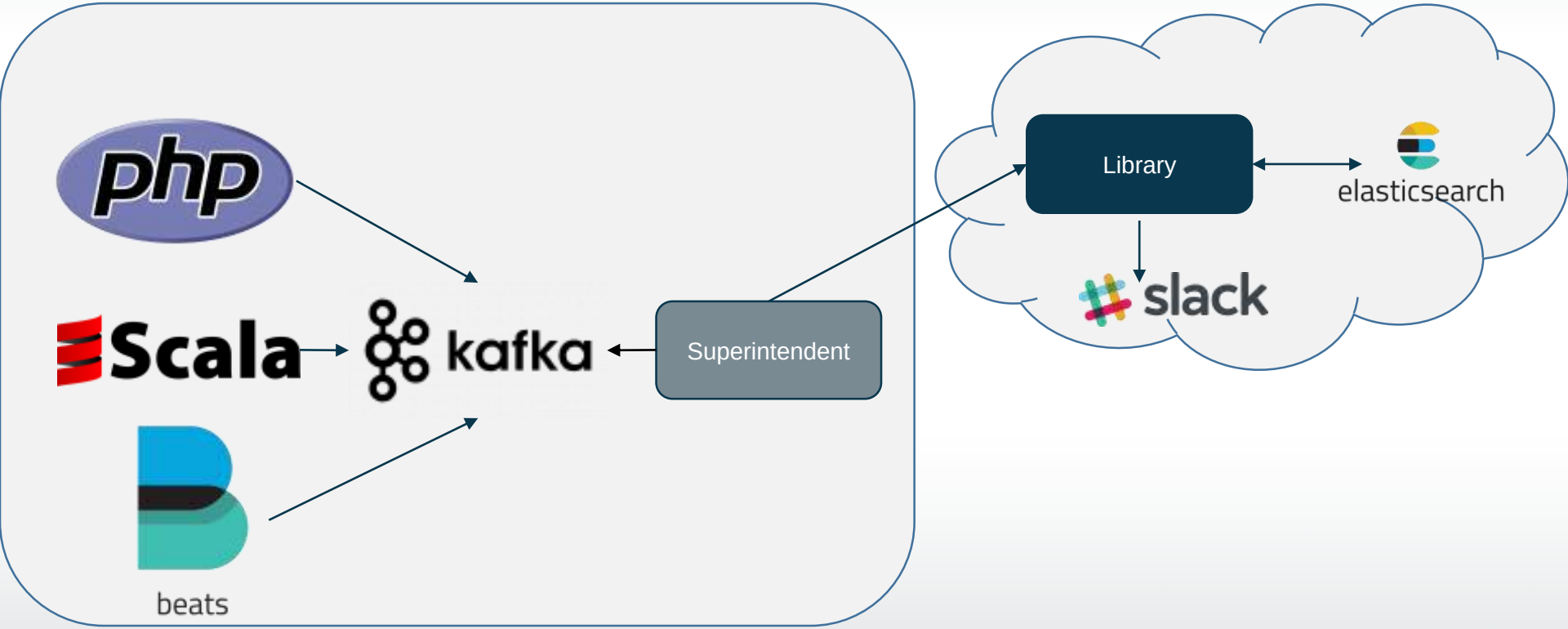
# Russian Doll of Metric Components



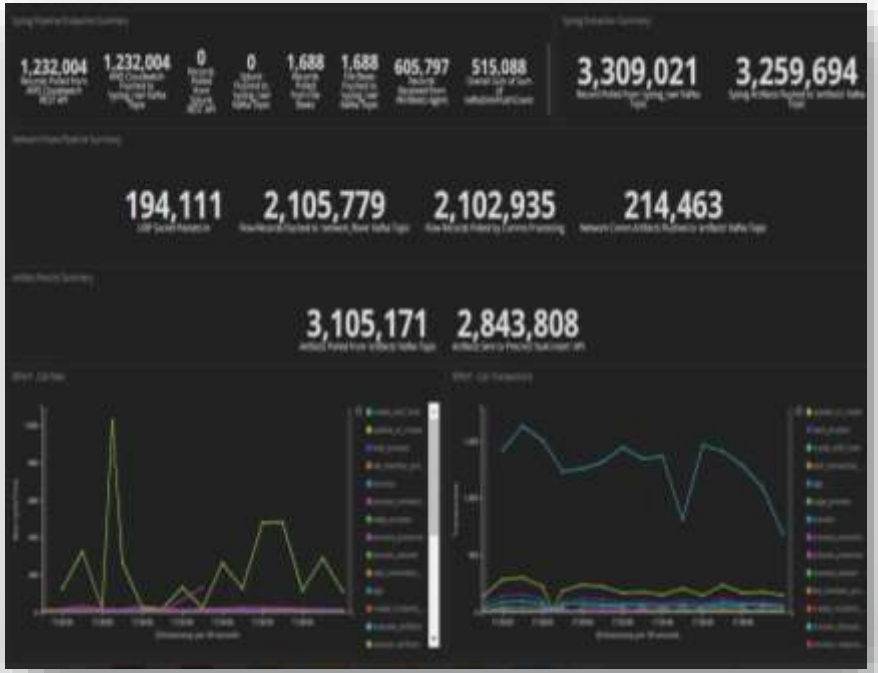
# Commercial APM Collection



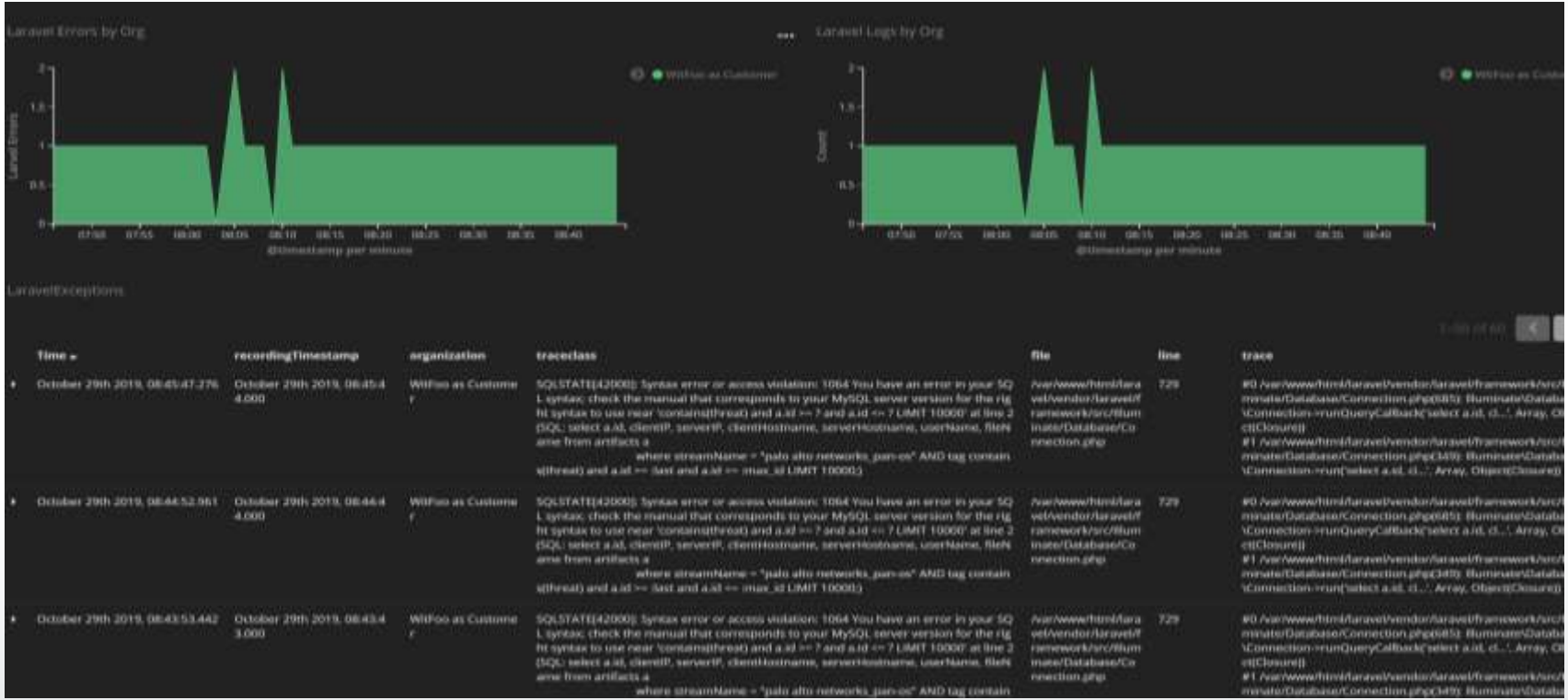
# Custom Metric Collection Pipeline



# Metrics and More Metrics



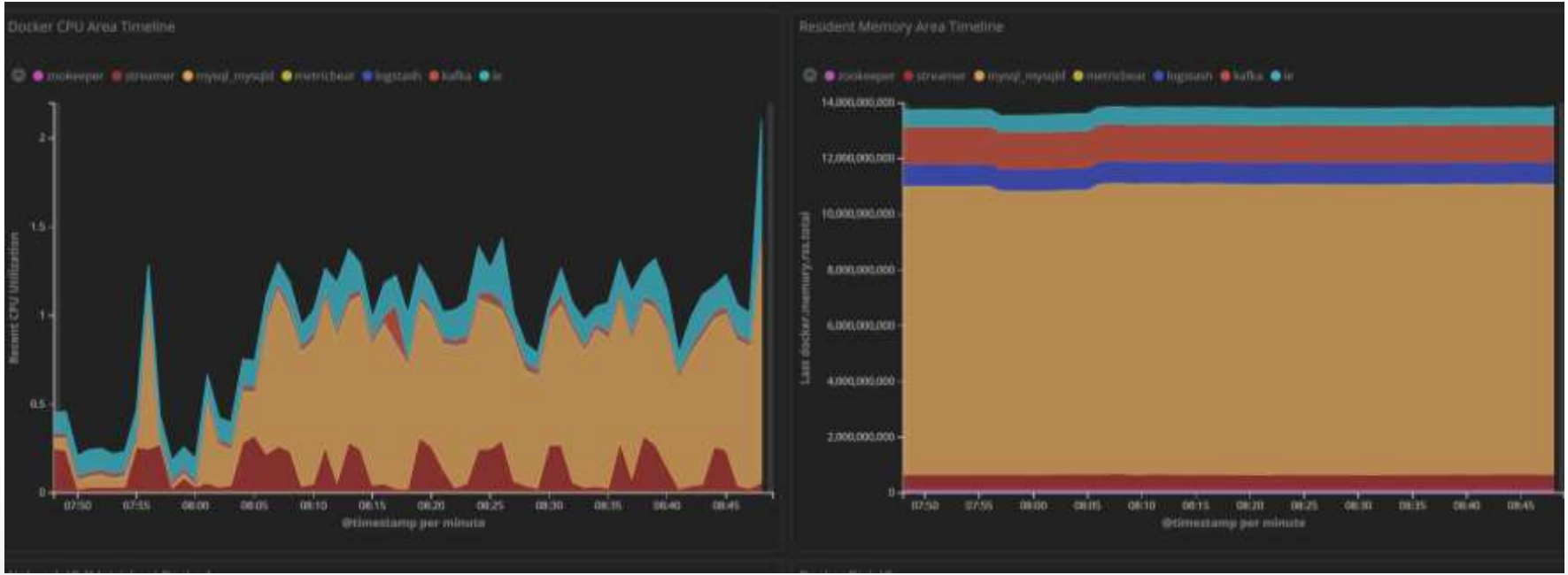
# Error Catching



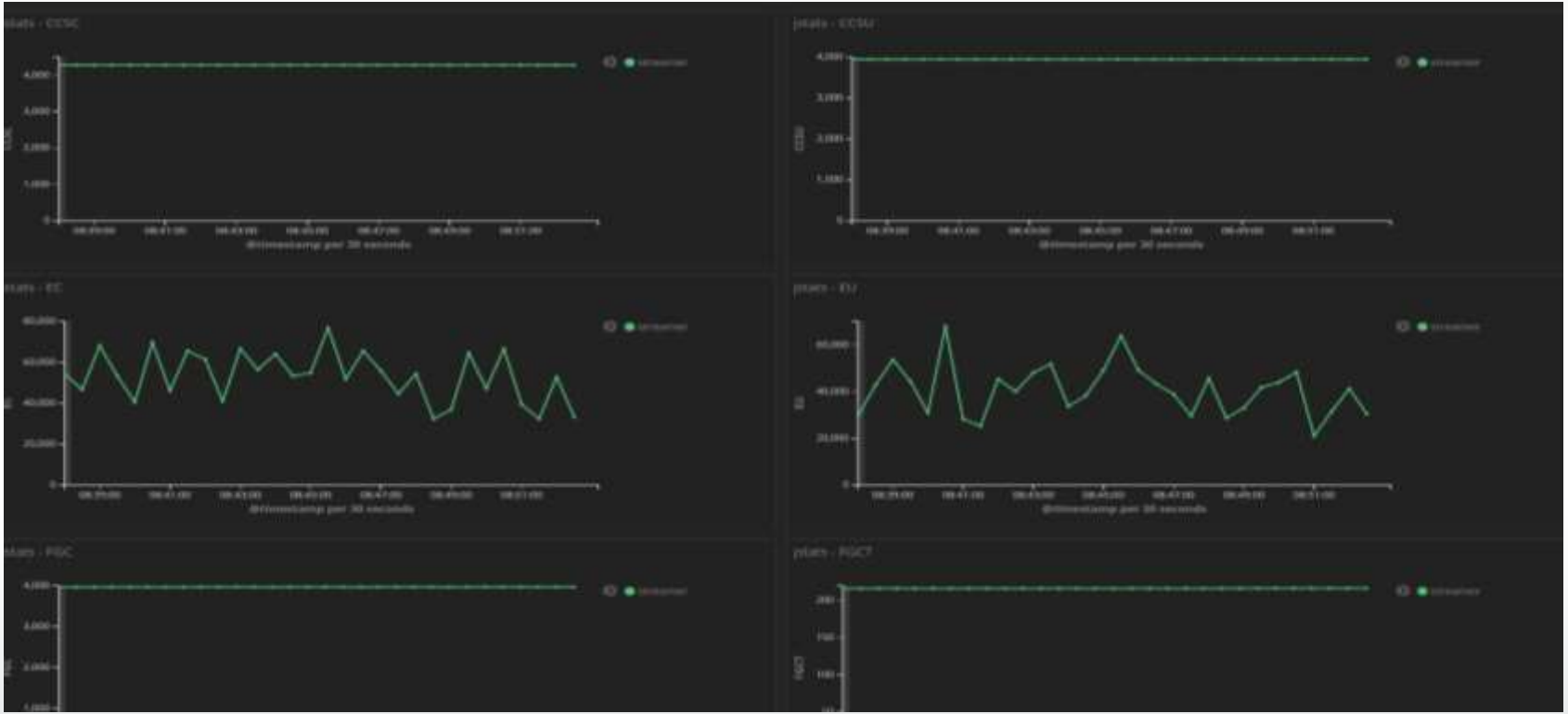

witfoo

# System Performance

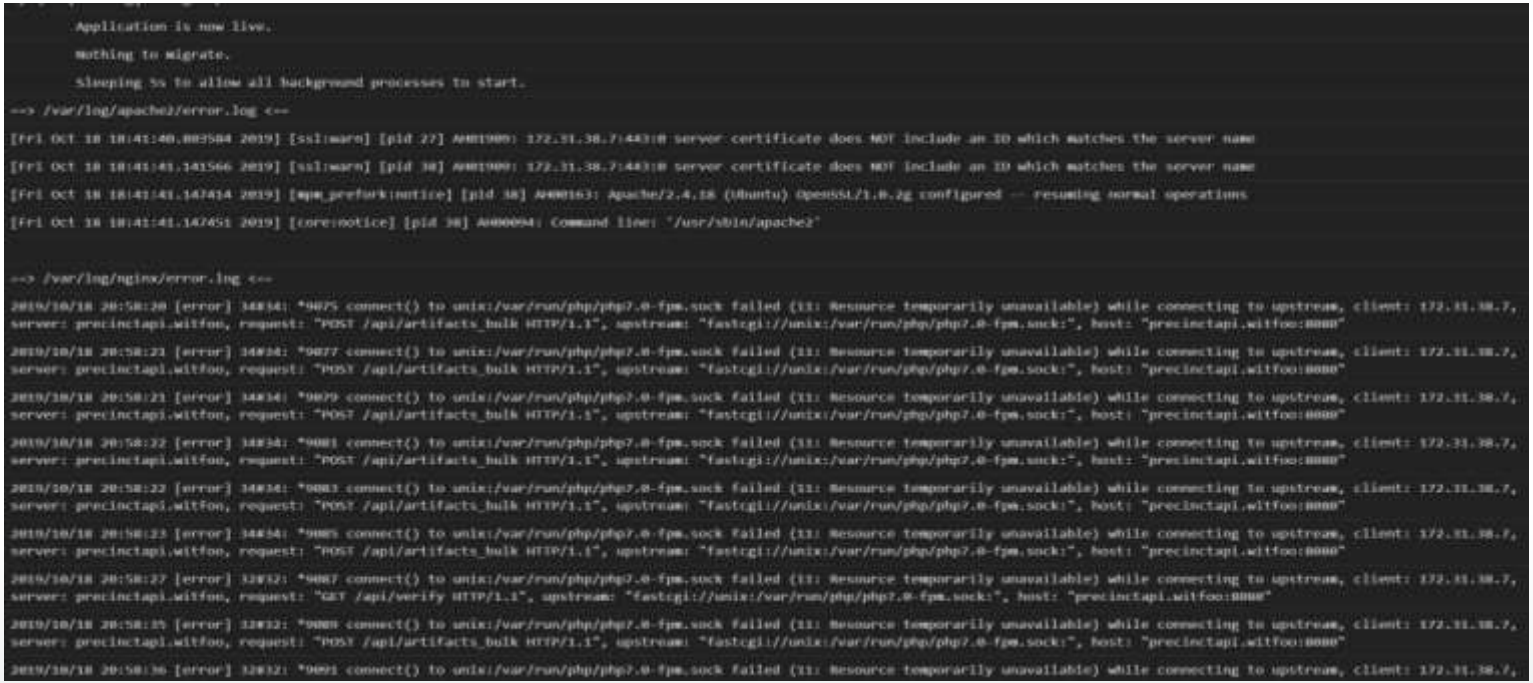
# Docker Container Performance



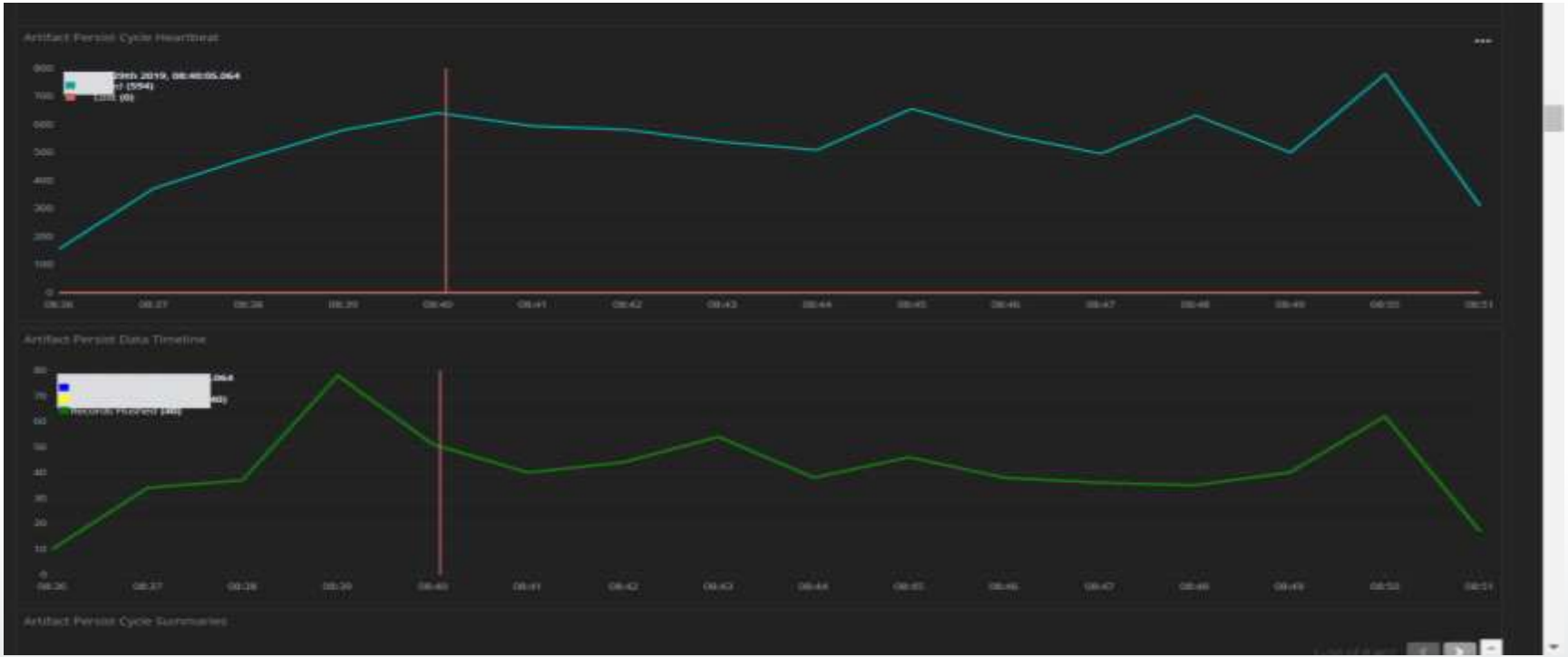
# JVM Health



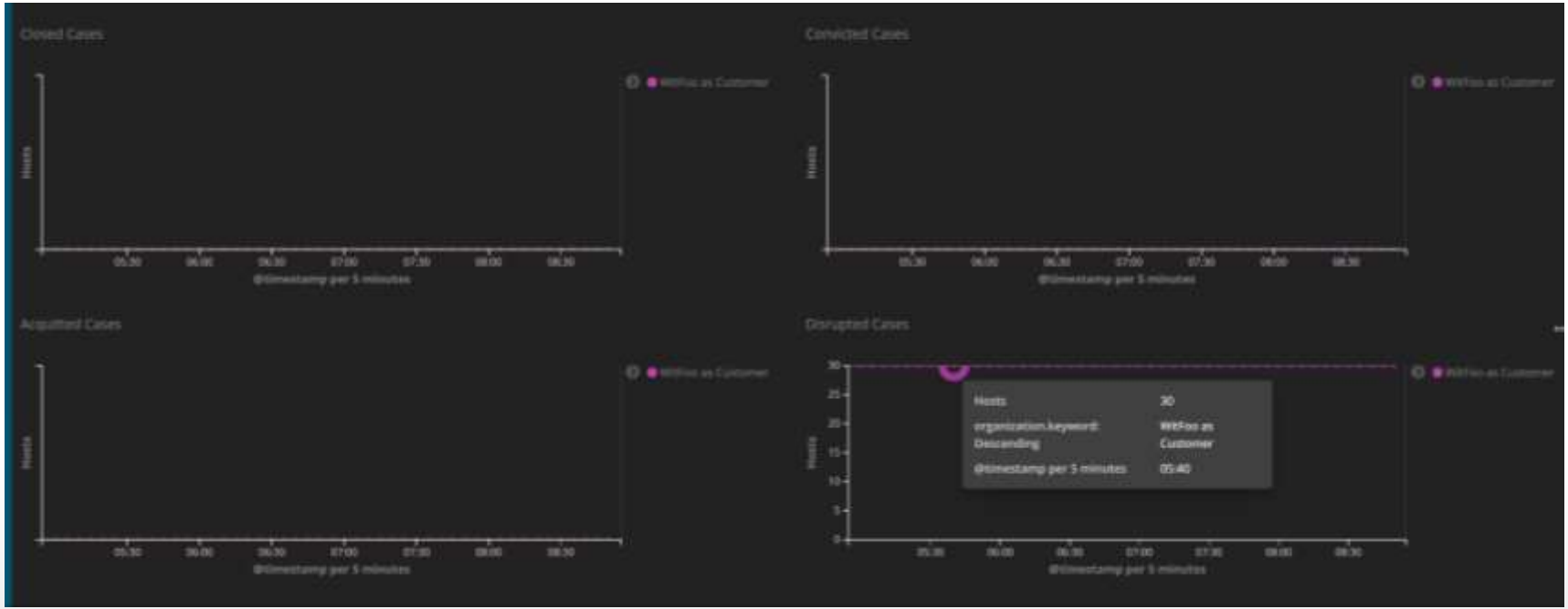
# Logging


Application is now live.
Nothing to migrate.
Sleeping 5s to allow all background processes to start.
==> /var/log/apache2/error.log <==
[Fri Oct 18 18:41:40.803504 2019] [ssl:warn] [pid 27] AH01909: 172.31.38.7:443:0 server certificate does NOT include an ID which matches the server name
[Fri Oct 18 18:41:41.141566 2019] [ssl:warn] [pid 38] AH01909: 172.31.38.7:443:0 server certificate does NOT include an ID which matches the server name
[Fri Oct 18 18:41:41.147414 2019] [mpm_prefork:notice] [pid 38] AH00163: Apache/2.4.18 (Ubuntu) OpenSSL/1.0.2g configured -- resuming normal operations
[Fri Oct 18 18:41:41.147451 2019] [core:notice] [pid 38] AH00094: Command line: '/usr/sbin/apache2'
==> /var/log/nginx/error.log <==
2019/10/18 20:58:20 [error] 34#34: *9075 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:21 [error] 34#34: *9077 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:21 [error] 34#34: *9079 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:22 [error] 34#34: *9081 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:22 [error] 34#34: *9083 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:23 [error] 34#34: *9085 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:27 [error] 32#32: *9087 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "GET /api/verify HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:35 [error] 32#32: *9089 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7, server: precinctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "precinctapi.witfoo:8080"
2019/10/18 20:58:36 [error] 32#32: *9091 connect() to unix:/var/run/php/php7.0-fpm.sock failed (11: Resource temporarily unavailable) while connecting to upstream, client: 172.31.38.7,

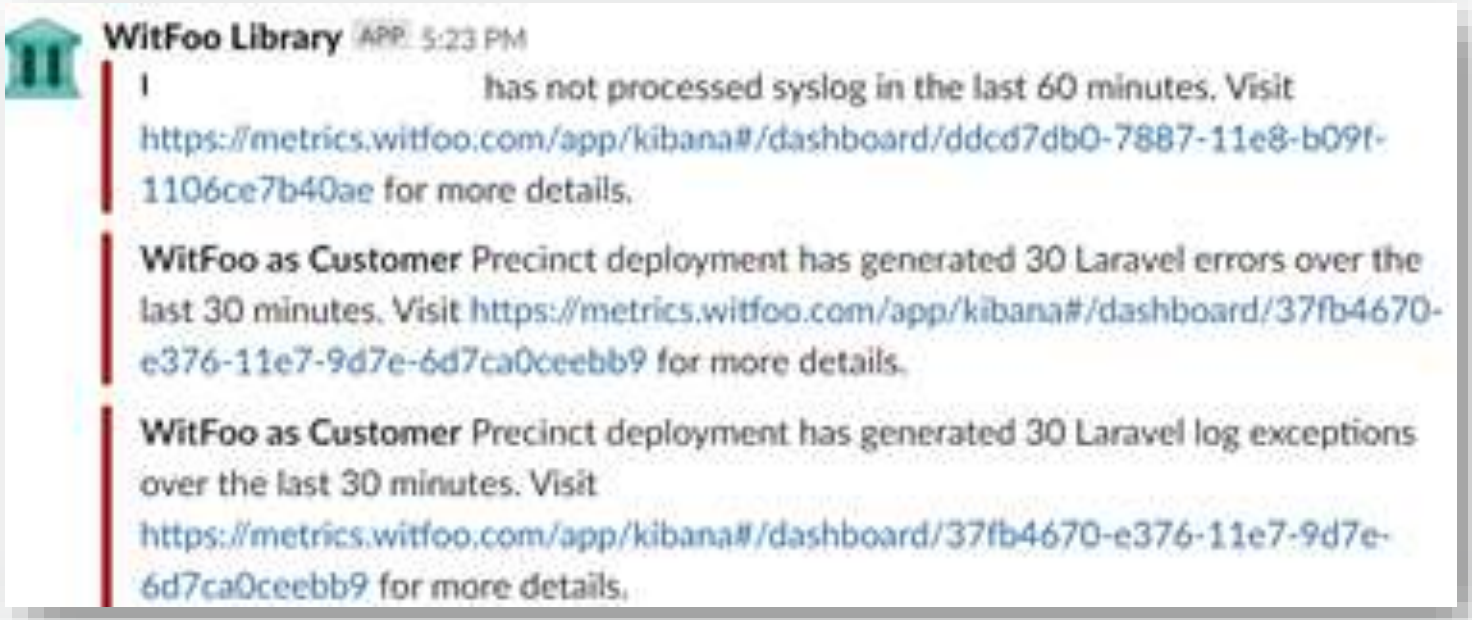
# Cycle Metrics



# User Interaction



# Automate Metric Analysis



# Assertions

- Field Metrics can drive better test writing
- Field Metrics provide for more secure code
- Containerizing provides flexibility to quickly fix issues
- Confidents can be gained from actual metrics
- Speed of development can improve with better metrics


# Secure Development Operations (SECDEVOPS)

**Charles Herring**
Co-Founder, CTO

CharlesHerring.com
@charlesherring
Charles@witfoo.com