



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 Of r00t team member



InfoWorld

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

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



Code Coverage

	Lines		Code Coverage		Classes and Traits	
	%	Count	%	Count	%	Count
Total	42.73%	6307 / 14807	35.00%	481 / 1348	19.41%	86 / 394
Console	43.02%	271 / 629	93.21%	98 / 105	7.41%	4 / 54
Customs	0.00%	2 / 22	0.00%	0 / 1	0.00%	0 / 1
Events	0.00%	0 / 16	0.00%	0 / 8	11.11%	1 / 9
Exceptions	16.20%	6 / 40	0.00%	0 / 2	0.00%	0 / 1
Http	58.18%	798 / 1371	99.32%	175 / 176	32.20%	22 / 68
Interfaces	100.00%	0 / 0	100.00%	0 / 0		0 / 0
Jobs	0.00%	0 / 90				
Libraries	14.00%	40 / 285				
Listeners	0.00%	0 / 16				
Modules	7.19%	14 / 195				
Policies	0.00%	0 / 1				
Providers	86.10%	74 / 85				
Repositories	81.10%	400 / 492				
Utility.php	100.00%	0 / 0				

```
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

Systems Test - 31m 33s

- ✓ > Waiting for 20 min
- ✓ > sleep 1200 — Shell
- ✓ > chmod +x system_t
- ✓ > sudo /bin/bash syst
- ✗ > sudo php system_tests/system_checks.php — Shell Script
- ✓ > Send Slack Message
- ✓ > sudo php system_tests/purge.php — Shell Script
- ✓ > Send Syslog entries to Streamer — Print Message
- ✓ > sudo /bin/bash system_tests/syslogMake.sh — Shell Script
- ✓ > Wait 5 minutes for incidents to process — Print Message
- ✓ > sleep 300 — Shell Script
- ✓ > Run system checks — Print Message
- ✓ > sudo php system_tests/system_checks.php — Shell Script

```
1 + sudo php system_tests/system_checks.php
2 Artifacts correctly createdPHP Fatal error: Uncaught Exception: Expected 9 or more Leads; Got 0 in /var/lib/jenkins/workspace/Precinct-Deckard_testing/system_tests/system_checks.php:17
3 Stack trace:
4 #0 [main]
5   throw in /var/lib/jenkins/workspace/Precinct-Deckard_testing/system_tests/system_checks.php on line 17
6   script returned exit code 255
```


Static Application Security Testing

CxSAST Full Report

Start: 04/10/19 15:08 End: 04/10/19 16:46 Files: 1579 Code Lines: 310706

[Analyze Results](#)

High 56

Vulnerability	Count
Client_DOM_XSS	50
Stored_XSS	6

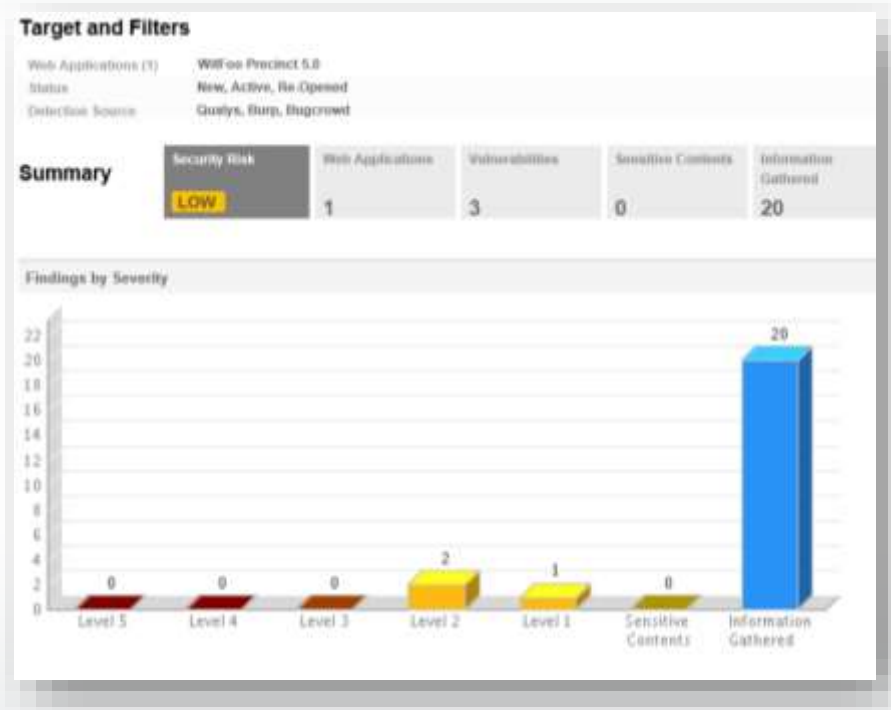
Medium 21

Vulnerability	Count
Heap_Inspection	16
Client_Privacy_Violation	2
Use_of_Cryptographically_Weak_PRNG	2
Privacy_Violation	1

Low 96

Vulnerability	Count
Unsafe_Use_Of_Target_blank	40
Unsafe_Use_Of_Target_blank	40
Divide_By_Zero	6

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/nginx') {
          sh 'yarn'
          sh 'ng build --prod'
        }
        sh 'cp ie/nginx/.htaccess ie/nginx/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-cl
```

```
root@dev-charles:~# docker pull ubuntu:xenial
xenial: Pulling from library/ubuntu
al298f4ce990: 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:~#
```

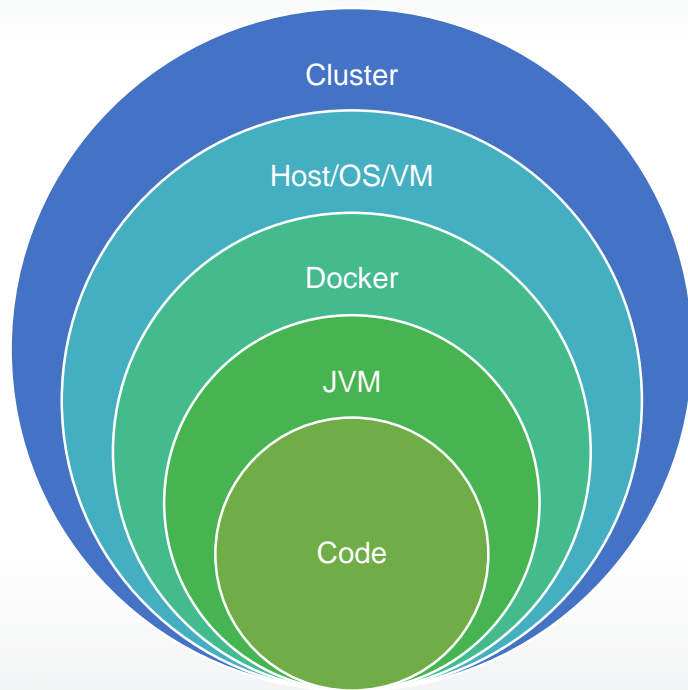
Custom(er) Builds

WitFoo Precinct System Status

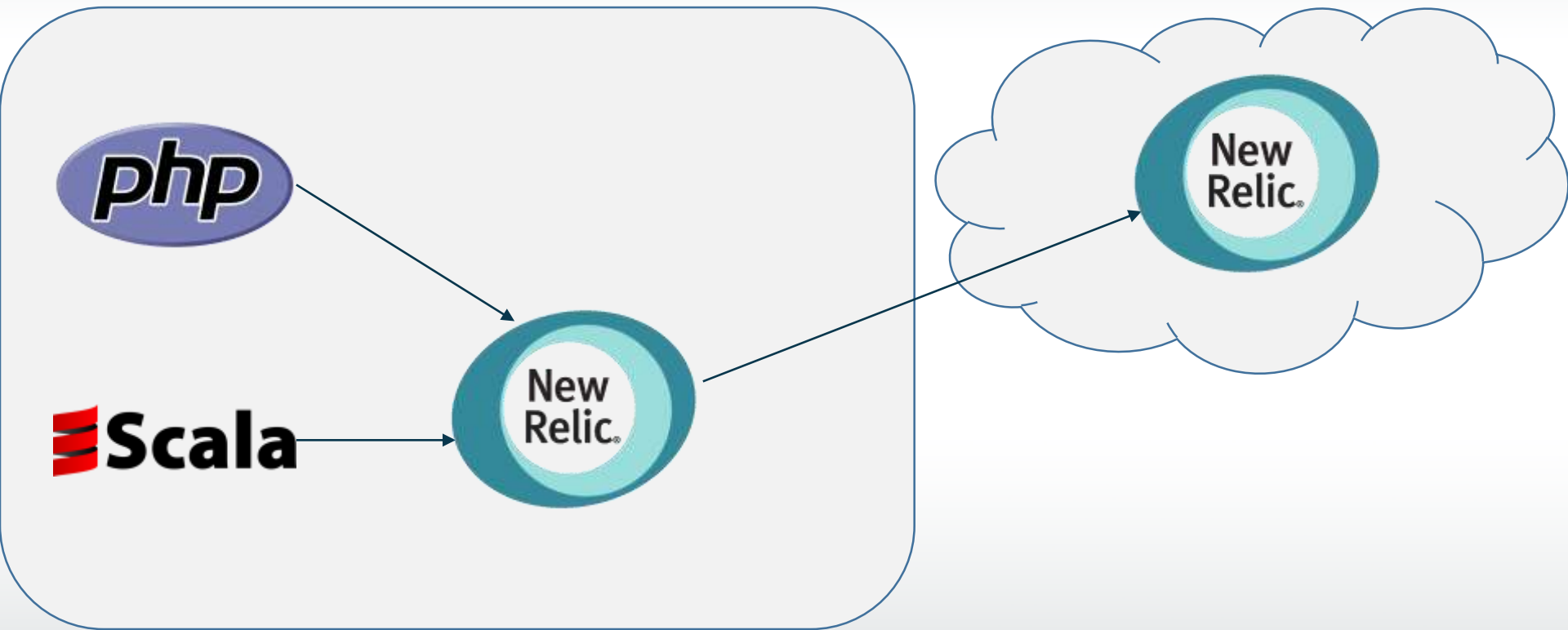
Build version `Build-Deckard-jenkins-Precinct-Deckard-master` 147

HEALTH	STATUS	BRANCH	COMMIT	LATEST MESSAGE	COMPLETED
		master	-	Fix replication	18 days ago
		cassandra-maintenance	-	Every third-day repair maintenance (node-by-node rat...	2 hours ago
		benson-dev	-	fix provider errors, remove closures, etc	2 hours ago
		tmp-ui	-	fix provider errors, remove closures, etc	3 hours ago
		caprica	-	fixed prod build	19 commits 3 hours ago

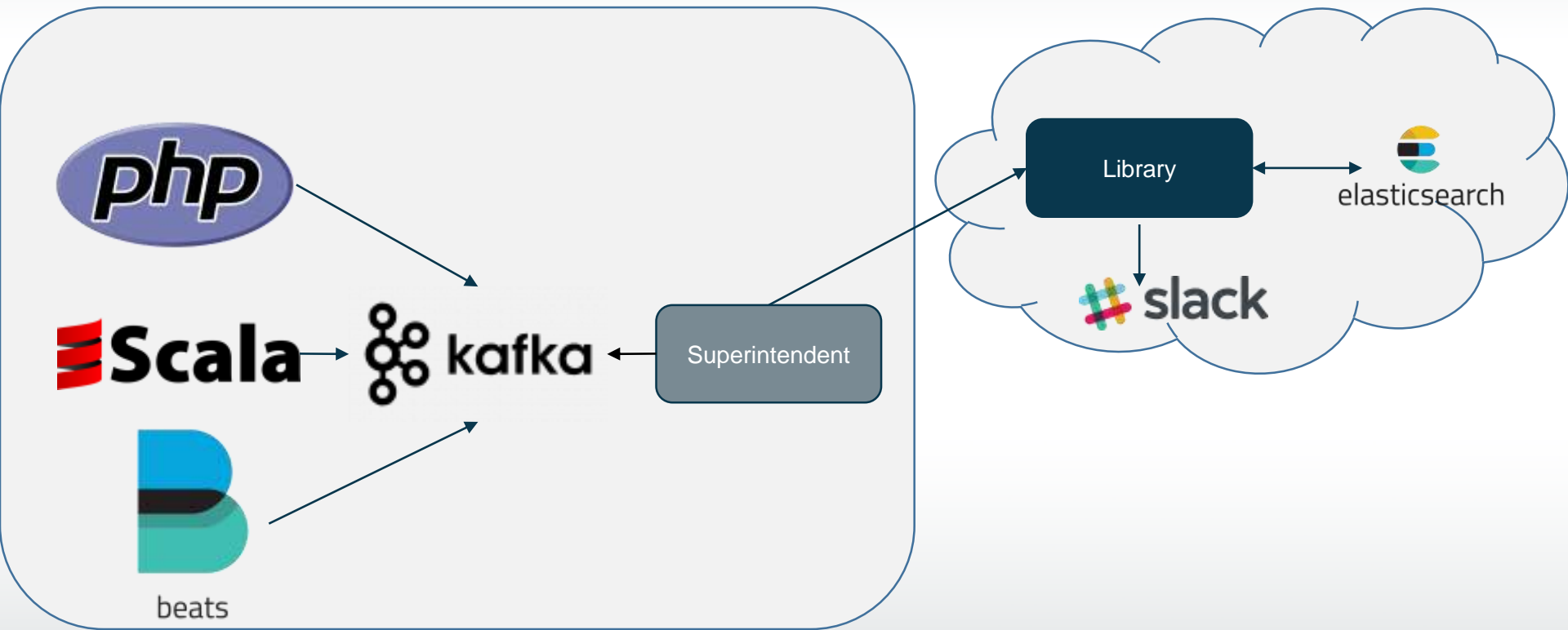
Russian Doll of Metric Components



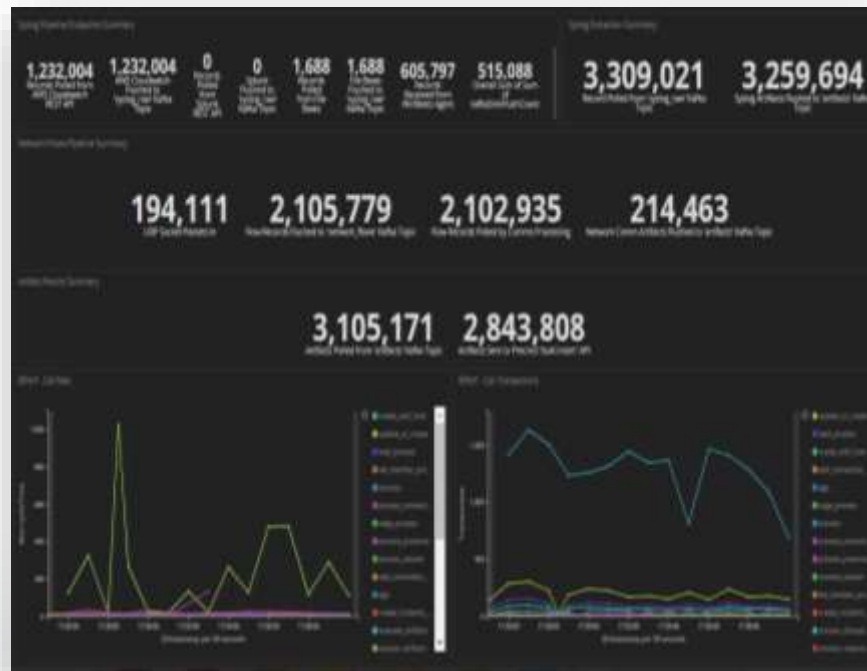
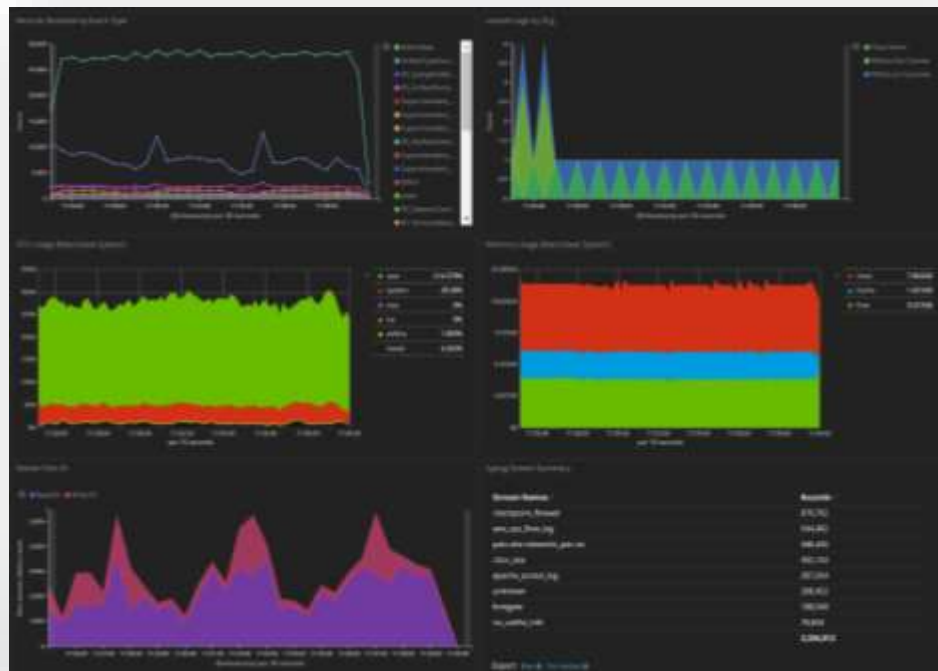
Commercial APM Collection



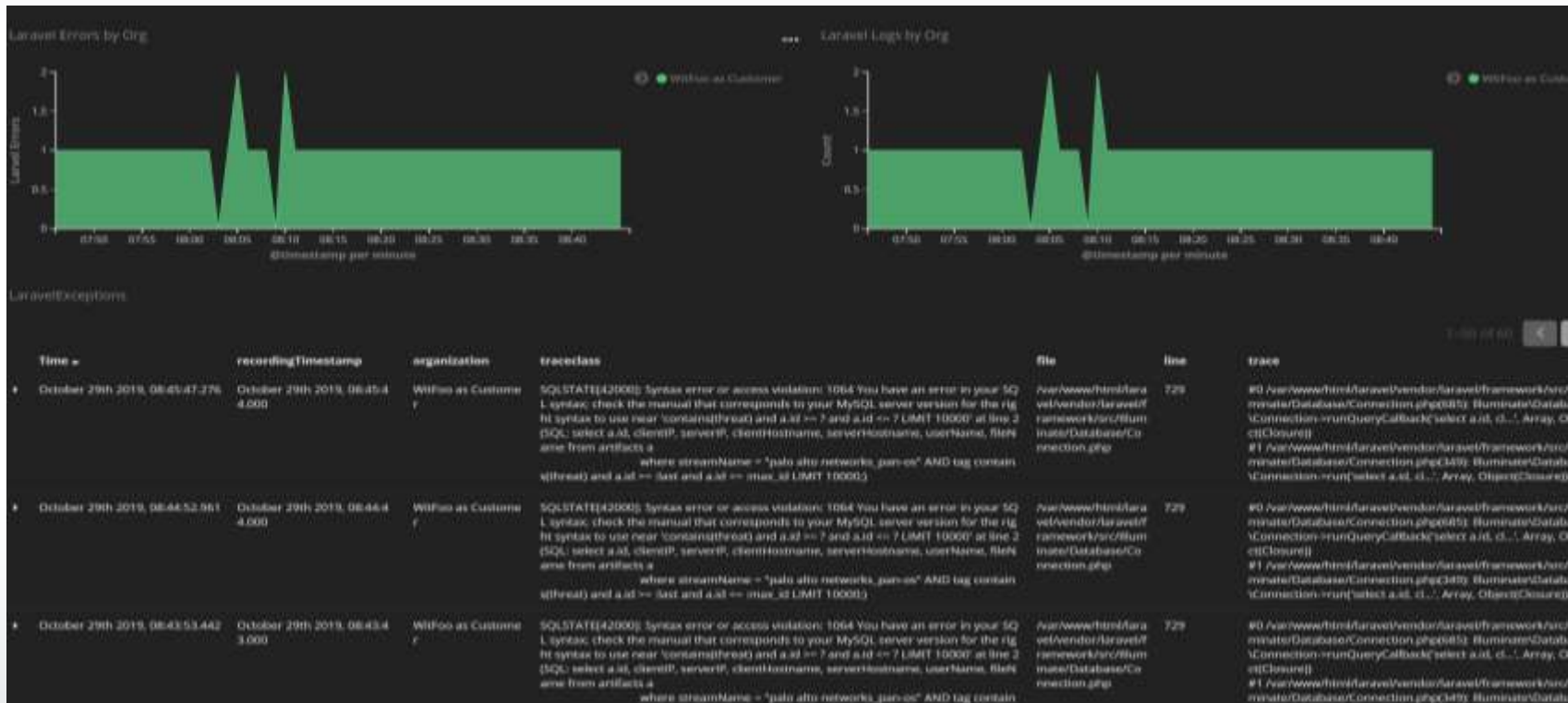
Custom Metric Collection Pipeline



Metrics and More Metrics



Error Catching



System Performance



Docker Container Performance



JVM Health



Logging

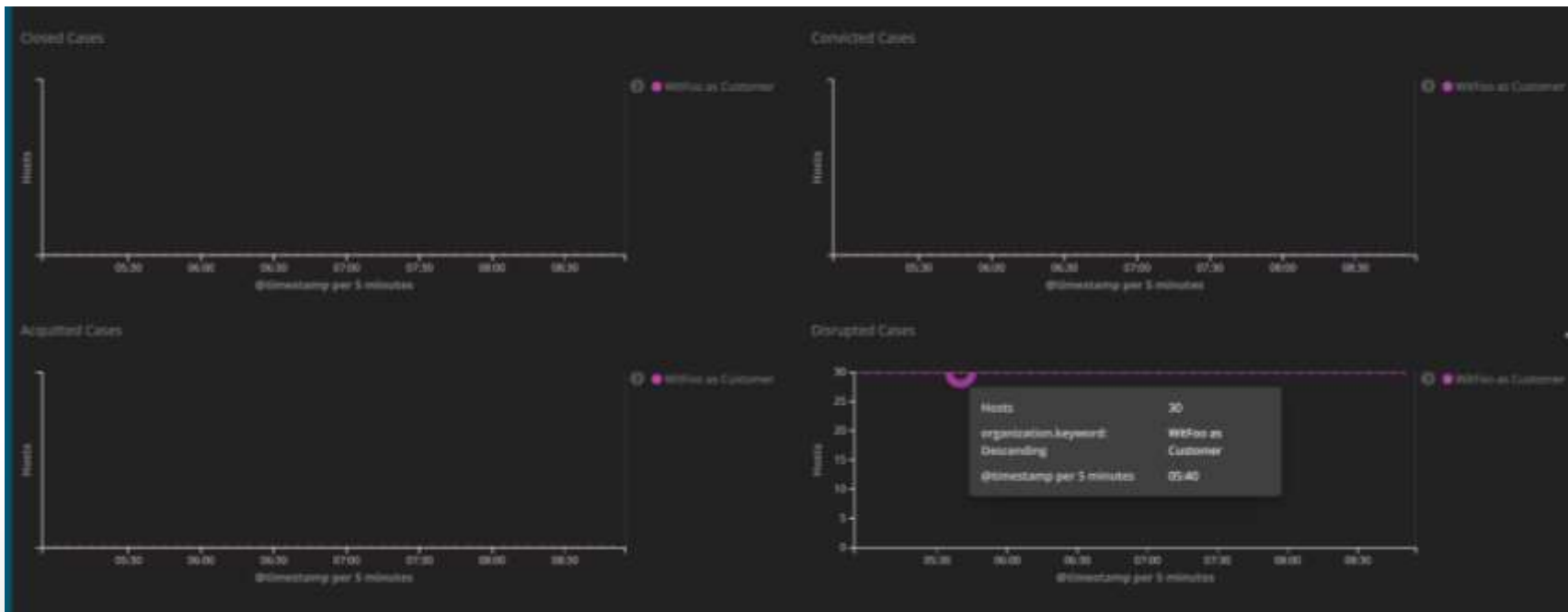
```
Application is now live.
nothing to migrate.
Sleeping 5s to allow all background processes to start.
--> /var/log/apache2/error.log <--
[Fri Oct 18 18:41:40.883584 2019] [ssl:warn] [pid 27] AH01909: 172.31.38.7:443:0 server certificate does NOT include an ID which matches the server name
[Fri Oct 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] [ajp_core:error] [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] 34834: *9875 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:21 [error] 34834: *9877 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:21 [error] 34834: *9879 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:22 [error] 34834: *9881 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:22 [error] 34834: *9883 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:23 [error] 34834: *9885 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:27 [error] 32832: *9887 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: preclnctapi.witfoo, request: "GET /api/verify HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:29 [error] 32832: *9888 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: preclnctapi.witfoo, request: "POST /api/artifacts_bulk HTTP/1.1", upstream: "fastcgi://unix:/var/run/php/php7.0-fpm.sock:", host: "preclnctapi.witfoo:8080"
2019/10/18 20:58:30 [error] 32832: *9891 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



WitFoo Library APP: 5:23 PM

I has not processed syslog in the last 60 minutes. Visit <https://metrics.witfoo.com/app/kibana#/dashboard/ddcd7db0-7887-11e8-b09f-1106ce7b40ae> for more details.

WitFoo as Customer Precinct deployment has generated 30 Laravel errors over the last 30 minutes. Visit <https://metrics.witfoo.com/app/kibana#/dashboard/37fb4670-e376-11e7-9d7e-6d7ca0ceebb9> for more details.

WitFoo as Customer Precinct deployment has generated 30 Laravel log exceptions over the last 30 minutes. Visit <https://metrics.witfoo.com/app/kibana#/dashboard/37fb4670-e376-11e7-9d7e-6d7ca0ceebb9> for more details.

Assertions

- Field Metrics can drive better test writing
- Field Metrics provide for more secure code
- Containerizing provides flexibility to quickly fix issues
- Confidants 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](https://twitter.com/charlesherring)

Charles@witfoo.com