SECURE360

CELEBRATING

15 Years

2020

SECURE360

Metric Driven SECDEVOPS

Charles Herring

CTO, WitFoo

Ryan Self

Chief Data Researcher, WitFoo

Slides: www.witfoo.com/blog/S360-2020

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

About Ryan

- **1999-2007** – Plankowner Electronics Technician for the USS Ronald Reagan, and forward deployed during Operation Enduring Freedom onboard the USS Theodore Roosevelt. Worked alongside Charles at the Naval Postgraduate School doing security automation.
- **2007-2010** - Studied Computer Science and Philosophy at the University of California, Santa Cruz.
- **2010-2016** - Frontend Engineer and Data Scientist for product recommendations startup, Baynote.
- **2016 –** WitFoo Chief Data Researcher

Agenda

- Project Scope Context
- DEVOPS Basics
- Automating DEVOPS
- Metrics in DEVOPS

Project Scope Context

What’s a WitFoo??

WitFoo Goals – Diagnostic SIEM

Provide tools & data that improve the maturity of Cyber Security Operations

1. Investigators Understand Data
2. Supervisors Understand what Investigators need
3. Business Executives Understand what Security needs
4. Organizations hold Security Vendors Accountable
5. Organizations safely share threat information with each other
6. Organizations and Law Enforcement collaborate
7. Law Enforcement has evidence to prosecute crimes

WitFoo Precinct Business Constraints

- 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

Metric Driven Philosophies

- Maximize Metrics
- Sustainable, Enduring Development
- Write Unit/System tests from learned lessons
- Reduce Risk in Experiments (Fail faster and safer)
- Validate assertions quickly (More Experiments)
- Precision in Decision Making
- Skip writing unnecessary tests
- Adjust platform on data results
- Reduce customer effort (& exhaustion)

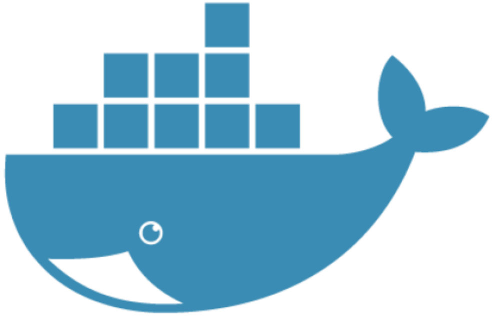
DEVOPS Basics

Unit tests, System Tests, Code Coverage and other boring hygiene stuff

WitFoo DEVOPS Components

CHECKMARX

elasticsearch



slack

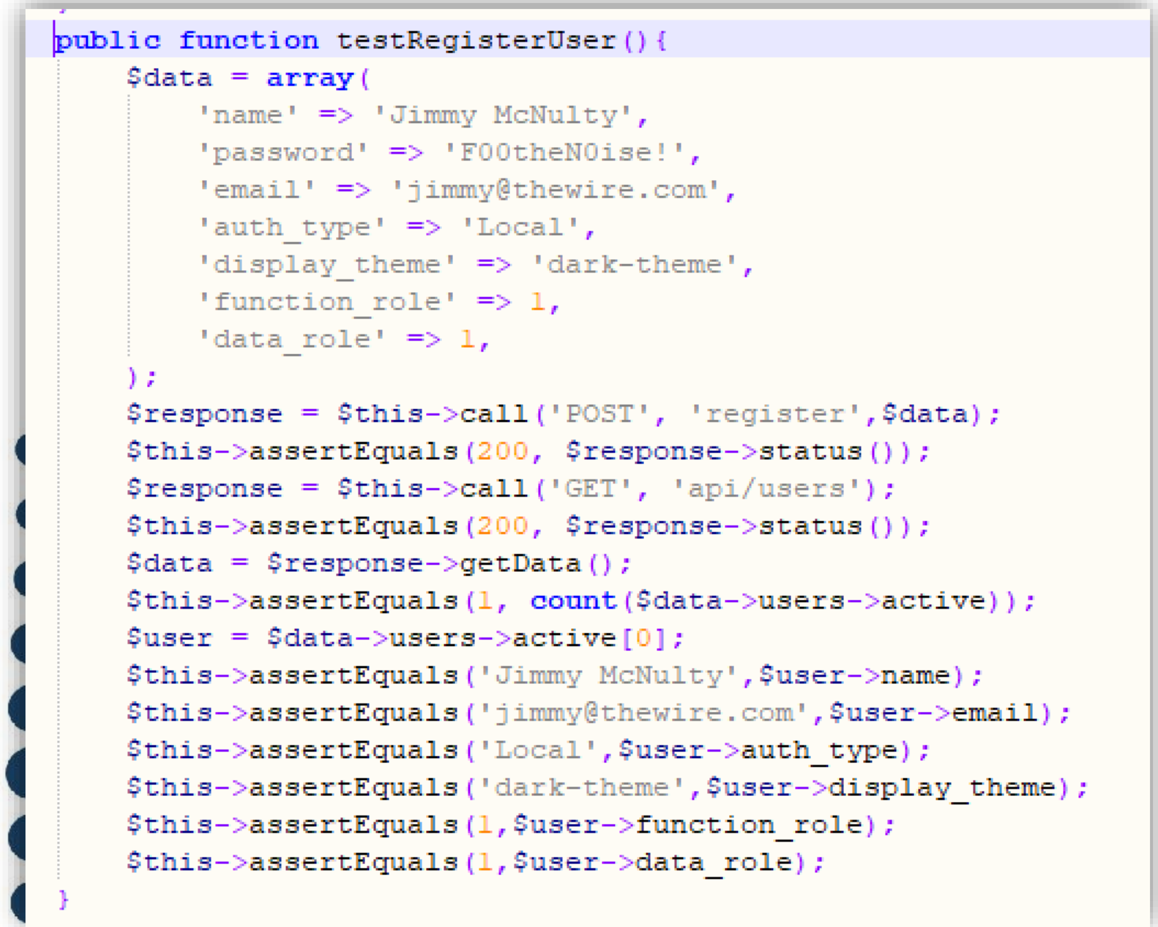
aws

Qualys.

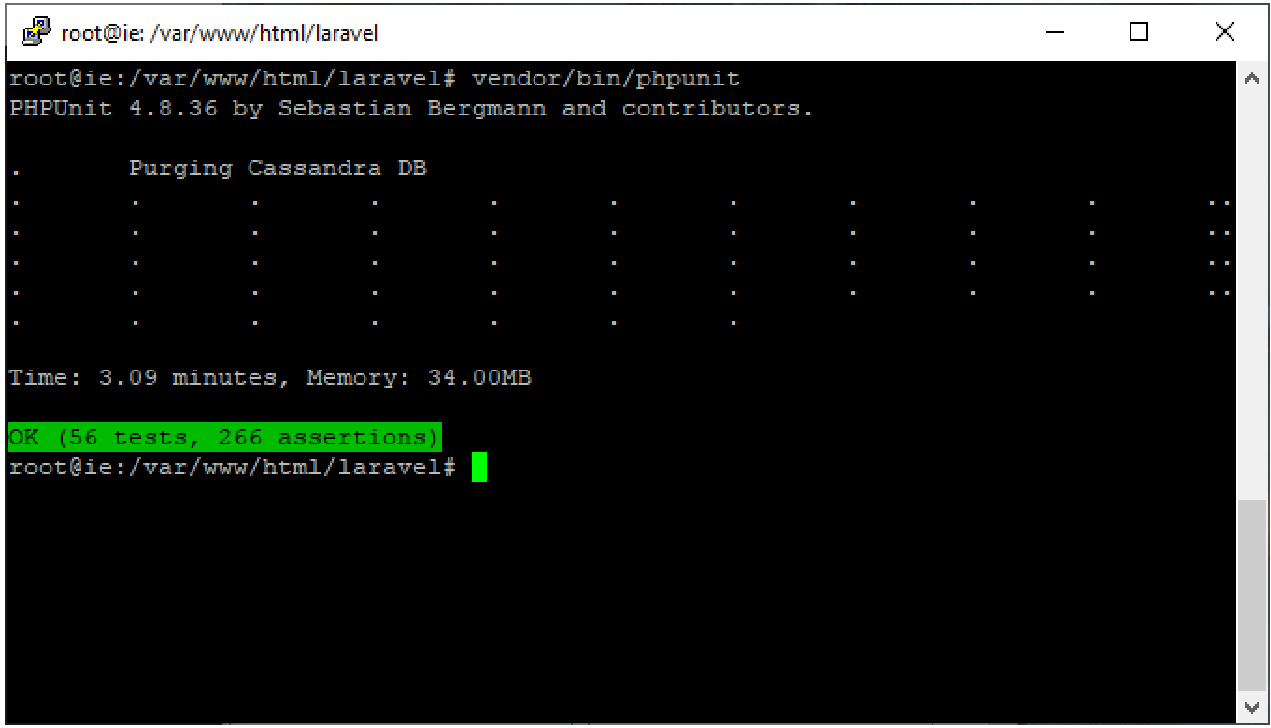
Continuous Security

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

Unit Tests

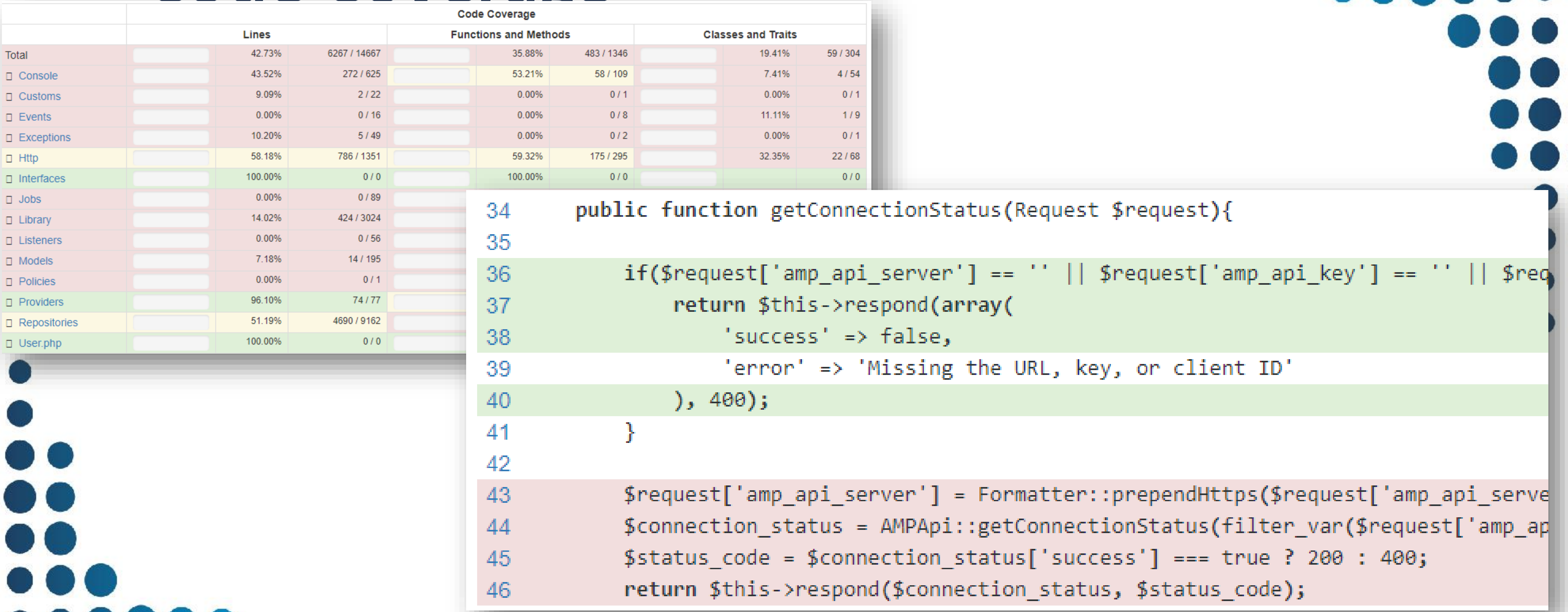


```
public function testRegisterUser(){
    $data = array(
        'name' => 'Jimmy McNulty',
        'password' => 'F00theN0ise!',
        'email' => 'jimmy@thewire.com',
        'auth_type' => 'Local',
        'display_theme' => 'dark-theme',
        'function_role' => 1,
        'data_role' => 1,
    );
    $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);
}
```



```
root@ie:/var/www/html/laravel# vendor/bin/phpunit
PHPUnit 4.8.36 by Sebastian Bergmann and contributors.

.       Purging Cassandra DB
.       .       .       .       .       .       .       .       .       .       ..
.       .       .       .       .       .       .       .       .       .       ..
.       .       .       .       .       .       .       .       .       .       ..
.       .       .       .       .       .       .       .       .       .       ..
.       .       .       .       .       .       .

Time: 3.09 minutes, Memory: 34.00MB

OK (56 tests, 266 assertions)
root@ie:/var/www/html/laravel#
```

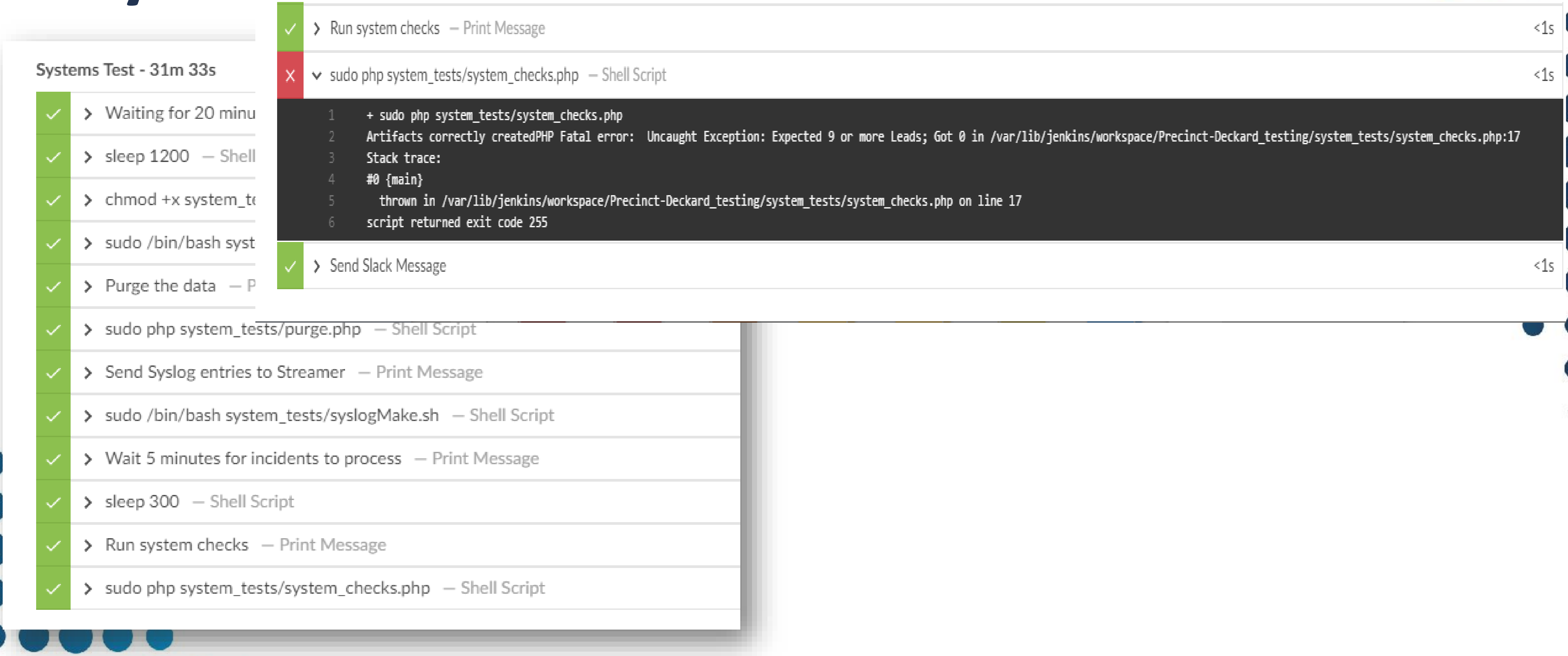
Code Coverage



	Code Coverage								
	Lines			Functions and Methods			Classes and Traits		
Total		42.73%	6267 / 14667		35.88%	483 / 1346		19.41%	59 / 304
□ Console		43.52%	272 / 625		53.21%	58 / 109		7.41%	4 / 54
□ Customs		9.09%	2 / 22		0.00%	0 / 1		0.00%	0 / 1
□ Events		0.00%	0 / 16		0.00%	0 / 8		11.11%	1 / 9
□ Exceptions		10.20%	5 / 49		0.00%	0 / 2		0.00%	0 / 1
□ Http		58.18%	786 / 1351		59.32%	175 / 295		32.35%	22 / 68
□ Interfaces		100.00%	0 / 0		100.00%	0 / 0			0 / 0
□ Jobs		0.00%	0 / 89						
□ Library		14.02%	424 / 3024						
□ Listeners		0.00%	0 / 56						
□ Models		7.18%	14 / 195						
□ Policies		0.00%	0 / 1						
□ Providers		96.10%	74 / 77						
□ Repositories		51.19%	4690 / 9162						
□ User.php		100.00%	0 / 0						

```
    public function getConnectionStatus(Request $request){

        if($request['amp_api_server'] == '' || $request['amp_api_key'] == '' || $req
            return $this->respond(array(
                'success' => false,
                'error' => 'Missing the URL, key, or client ID'
            ), 400);
        }

        $request['amp_api_server'] = Formatter::prependHttps($request['amp_api_serve
        $connection_status = AMPApi::getConnectionStatus(filter_var($request['amp_ap
        $status_code = $connection_status['success'] === true ? 200 : 400;
        return $this->respond($connection_status, $status_code);
```

System Tests



Systems Test - 31m 33s

✓ › Waiting for 20 minu

✓ › sleep 1200 — Shell

✓ › chmod +x system_te

✓ › sudo /bin/bash syst

✓ › Purge the data — P

✓ › 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

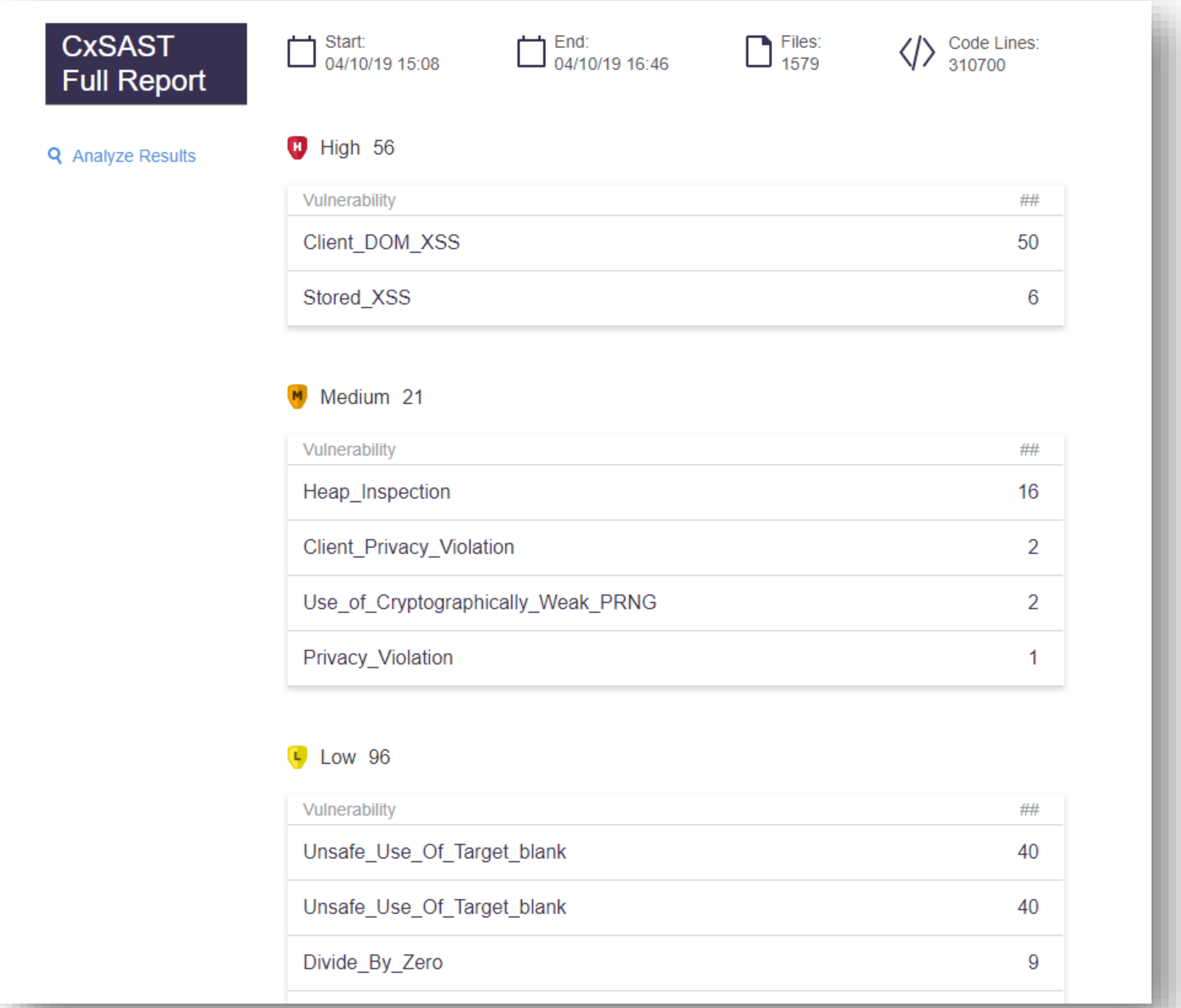
✓ › Run system checks — Print Message <1s

X ⌄ sudo php system_tests/system_checks.php — Shell Script <1s

```
+ sudo php system_tests/system_checks.php
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
Stack trace:
#0 {main}
  thrown in /var/lib/jenkins/workspace/Precinct-Deckard_testing/system_tests/system_checks.php on line 17
script returned exit code 255
```

✓ › Send Slack Message <1s

Static Application Security Testing



CxSAST Full Report

Start: 04/10/19 15:08

End: 04/10/19 16:46

Files: 1579

Code Lines: 310700

Analyze Results

H High 56

Vulnerability	##
Client_DOM_XSS	50
Stored_XSS	6

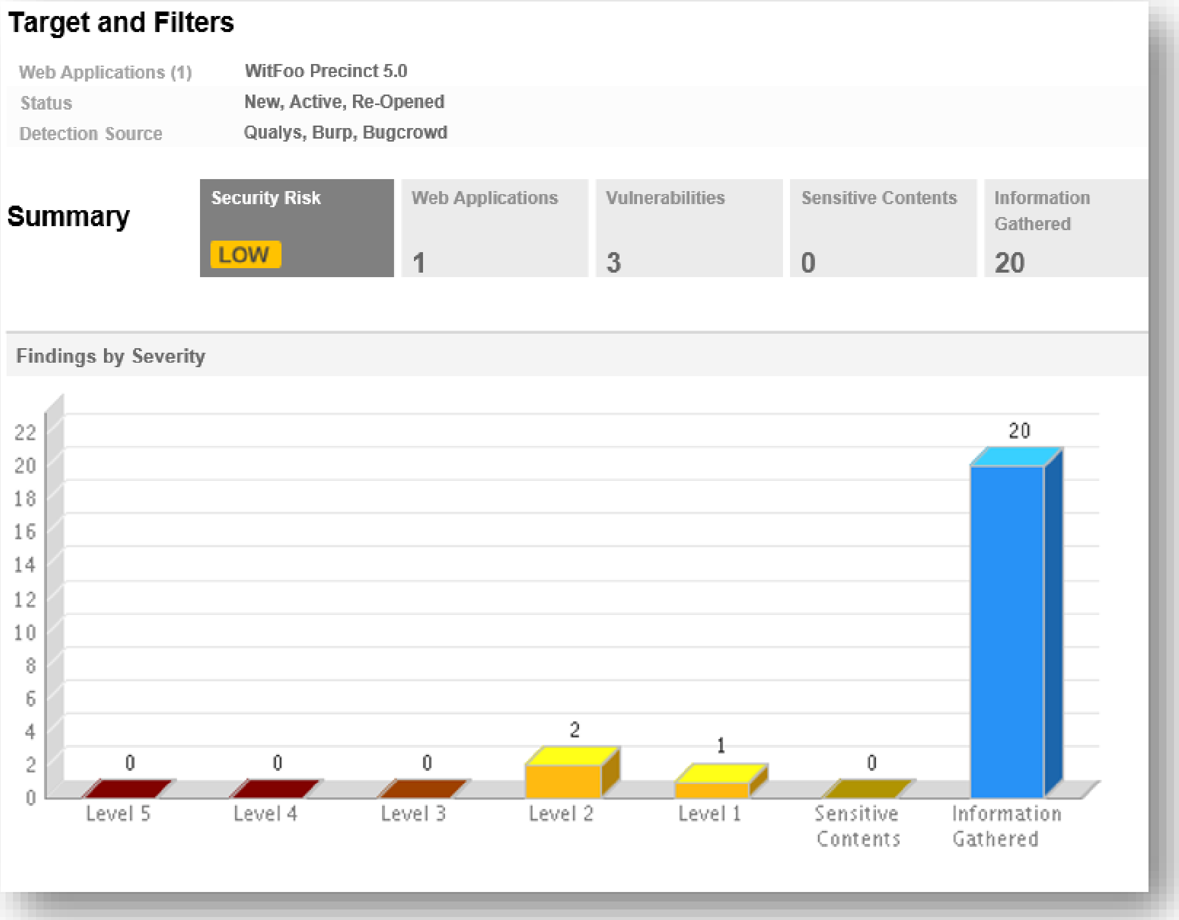
M Medium 21

Vulnerability	##
Heap_Inspection	16
Client_Privacy_Violation	2
Use_of_Cryptographically_Weak_PRNG	2
Privacy_Violation	1

L Low 96

Vulnerability	##
Unsafe_Use_Of_Target_blank	40
Unsafe_Use_Of_Target_blank	40
Divide_By_Zero	9

Vulnerability Scans / App Penetration



Target and Filters

Web Applications (1)	WitFoo Precinct 5.0
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

Summary

Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
LOW	1	3	0	20

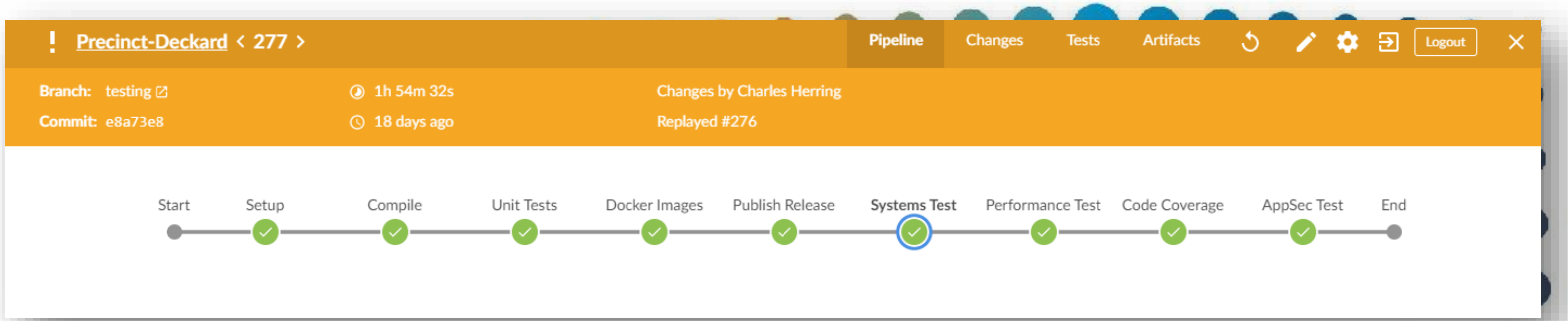
Findings by Severity

SECURE360

Automating DEVOPS

Blocking and Tackling of Builds

Jenkins



Branch: testing

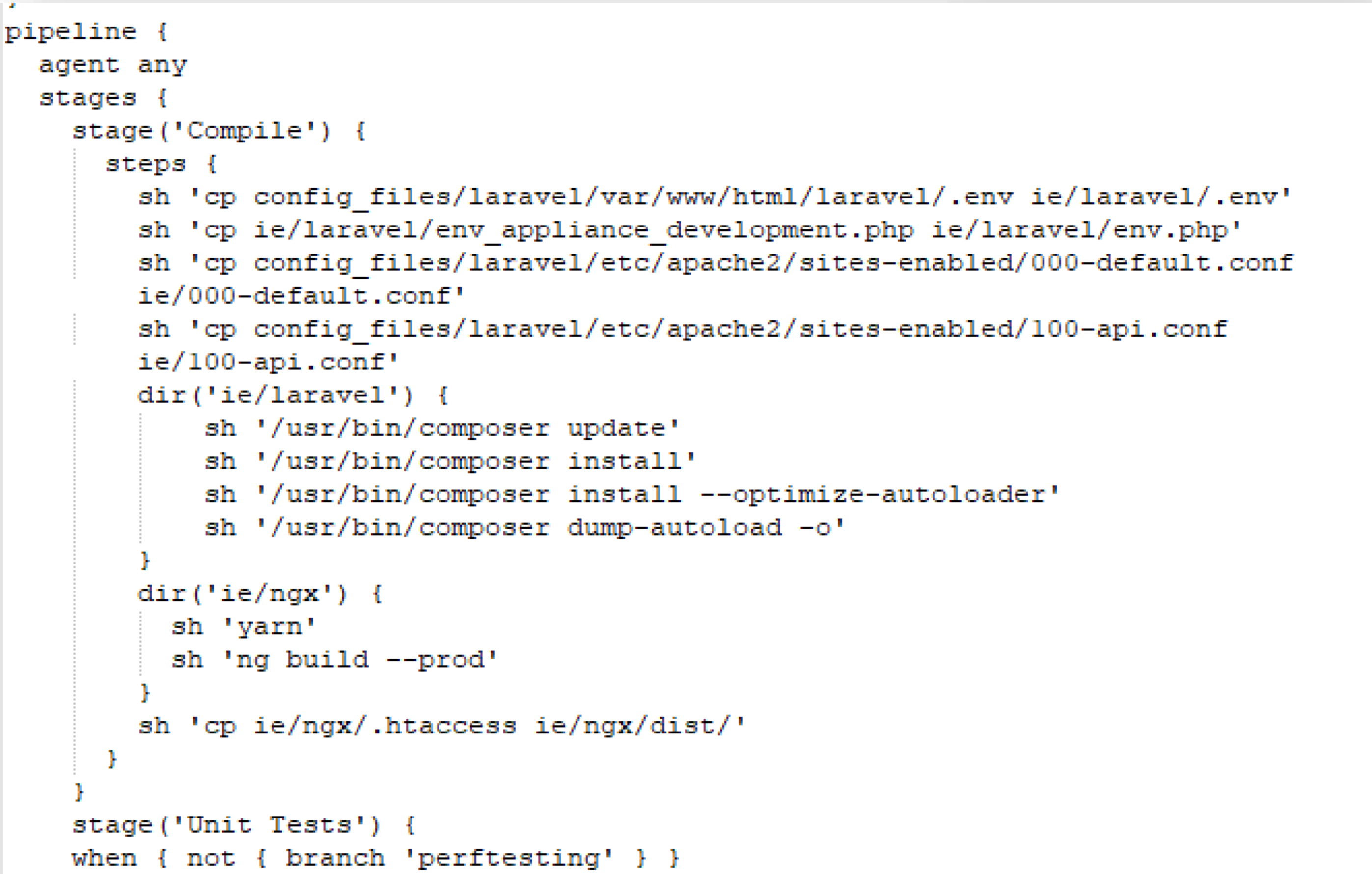
Commit: e8a73e8

1h 54m 32s

18 days ago

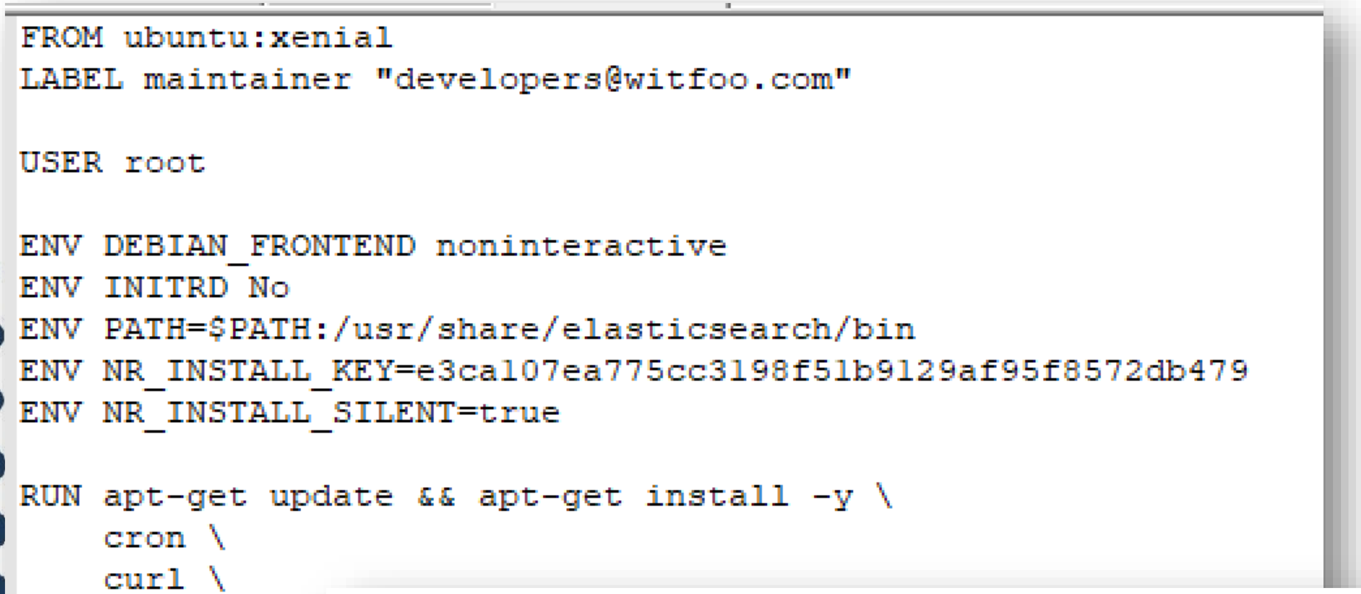
Changes by Charles Herring

Replayed #276

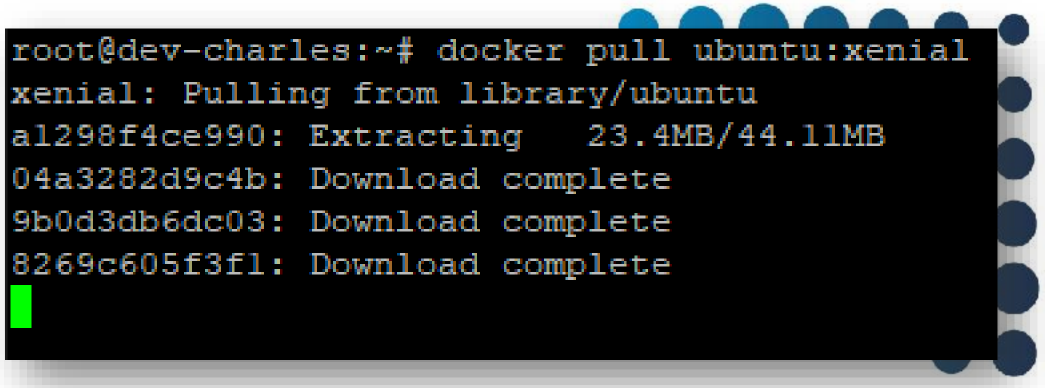


```
pipeline {
  agent any
  stages {
    stage('Compile') {
      steps {
        sh 'cp config_files/laravel/var/www/html/laravel/.env ie/laravel/.env'
        sh 'cp ie/laravel/env_appliance_development.php ie/laravel/env.php'
        sh 'cp config_files/laravel/etc/apache2/sites-enabled/000-default.conf
        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' } }
```

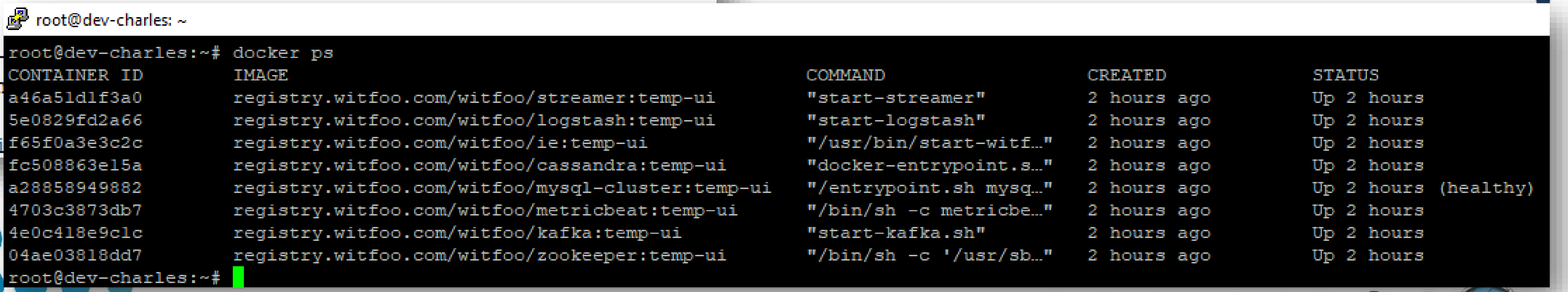
Docker Containers



```
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-clien
    php-fpm \
    php php-cli
```

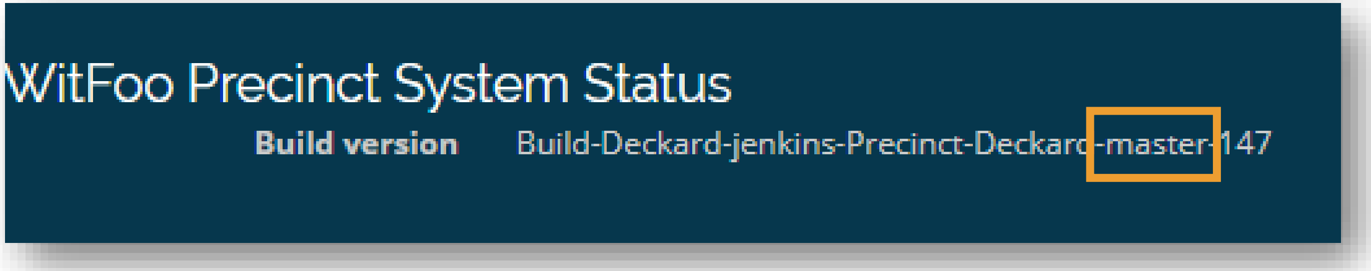


```
root@dev-charles:~# docker pull ubuntu:xenial
xenial: Pulling from library/ubuntu
a1298f4ce990: Extracting   23.4MB/44.11MB
04a3282d9c4b: Download complete
9b0d3db6dc03: Download complete
8269c605f3f1: Download complete
```



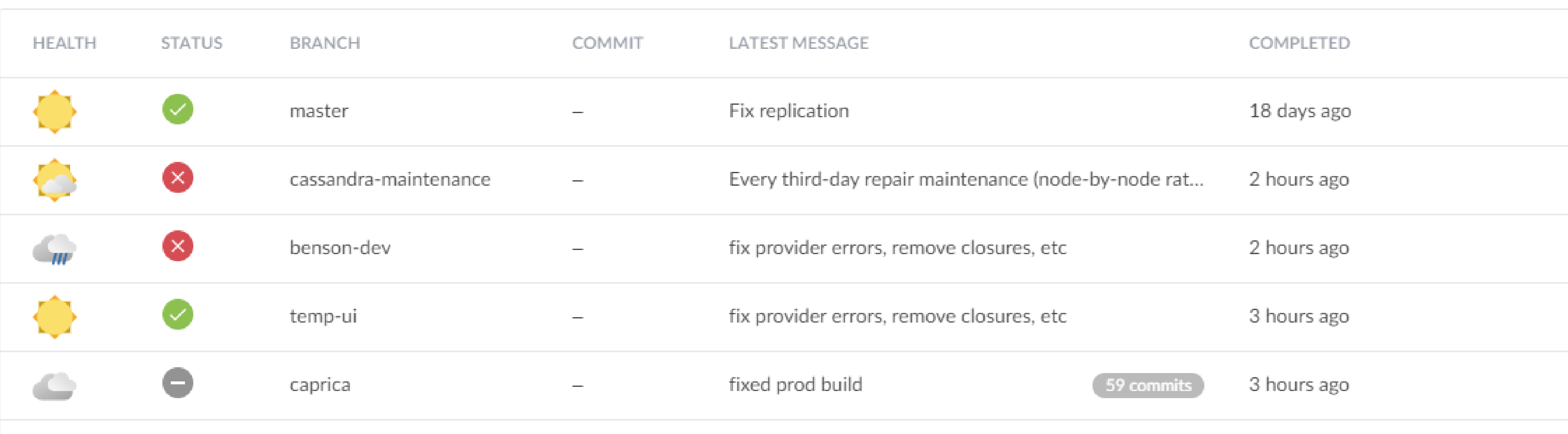
```
root@dev-charles:~# docker ps
CONTAINER ID        IMAGE                                              COMMAND                  CREATED             STATUS
a46a51d1f3a0        registry.witfoo.com/witfoo/streamer:temp-ui        "start-streamer"         2 hours ago         Up 2 hours
5e0829fd2a66        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

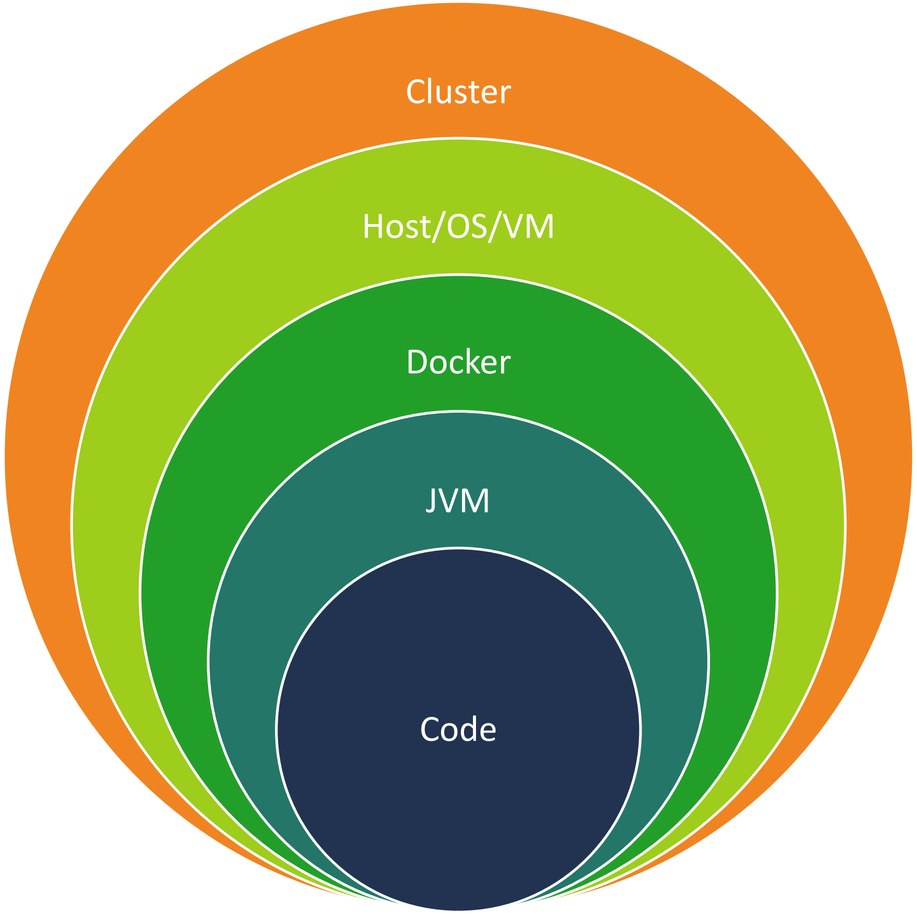


HEALTH	STATUS	BRANCH	COMMIT	LATEST MESSAGE		COMPLETED
☀	✓	master	–	Fix replication		18 days ago
⛅	✗	cassandra-maintenance	–	Every third-day repair maintenance (node-by-node rat...		2 hours ago
🌧	✗	benson-dev	–	fix provider errors, remove closures, etc		2 hours ago
☀	✓	temp-ui	–	fix provider errors, remove closures, etc		3 hours ago
☁	⊖	caprica	–	fixed prod build	59 commits	3 hours ago

Understanding Metrics

Collection, Analyze and Alert

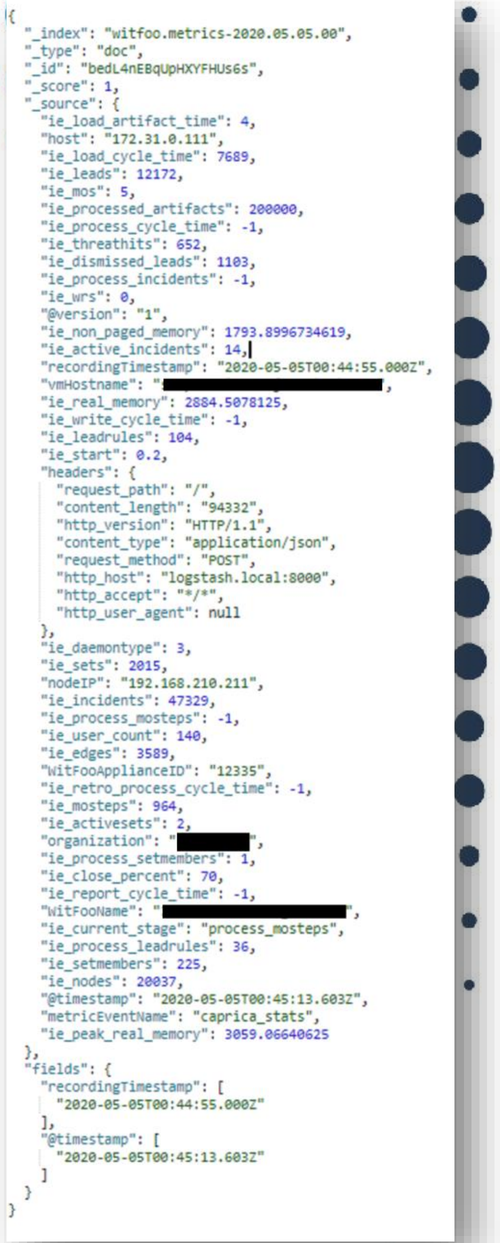
Russian Doll of Metric Components



Customer/Cluster Name

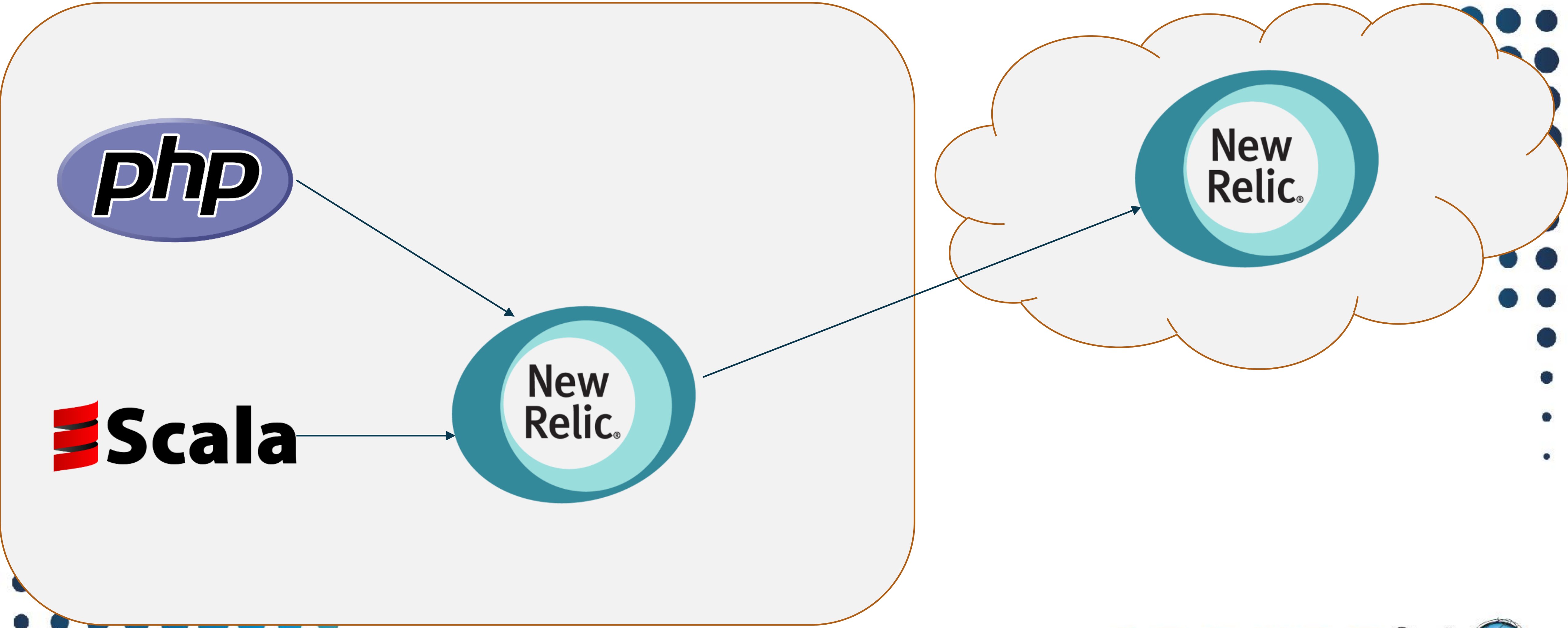
Node Name
Architecture Type (ESX, AWS, etc)
CPU, MEM, IOPS, Network, Error
Container Name
CPU, MEM, IOPS, Network, Error
Application Name
GC, MEM, CPU

Method/Function
Cycle Time
Counters
Human Interactions
Error

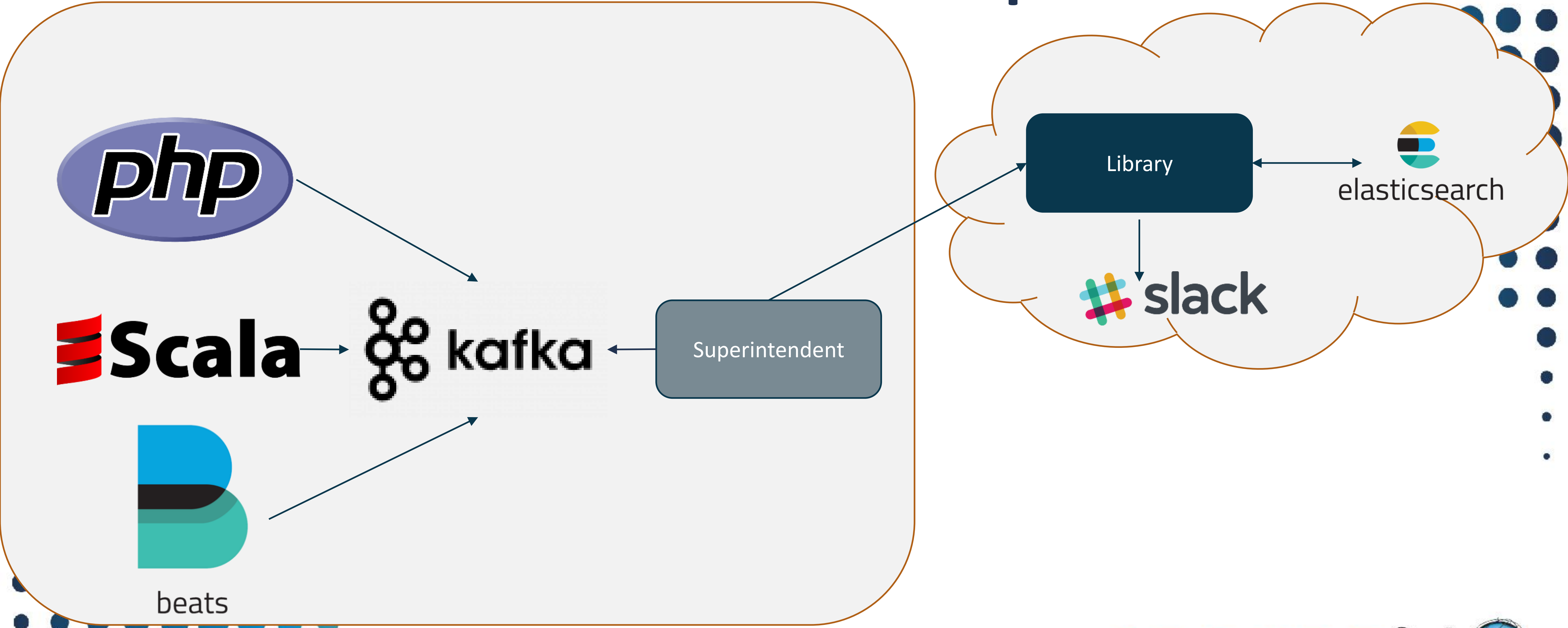


```
{
  "_index": "witfoo.metrics-2020.05.05.00",
  "_type": "doc",
  "_id": "bedL4nEBqUpHXYFHUs6s",
  "_score": 1,
  "_source": {
    "ie_load_artifact_time": 4,
    "host": "172.31.0.111",
    "ie_load_cycle_time": 7689,
    "ie_leads": 12172,
    "ie_mos": 5,
    "ie_processed_artifacts": 200000,
    "ie_process_cycle_time": -1,
    "ie_threathits": 652,
    "ie_dismissed_leads": 1103,
    "ie_process_incidents": -1,
    "ie_wrs": 0,
    "@version": "1",
    "ie_non_paged_memory": 1793.8996734619,
    "ie_active_incidents": 14,
    "recordingTimestamp": "2020-05-05T00:44:55.000Z",
    "vmHostname": "[redacted]",
    "ie_real_memory": 2884.5078125,
    "ie_write_cycle_time": -1,
    "ie_leadrules": 104,
    "ie_start": 0.2,
    "headers": {
      "request_path": "/",
      "content_length": "94332",
      "http_version": "HTTP/1.1",
      "content_type": "application/json",
      "request_method": "POST",
      "http_host": "logstash.local:8000",
      "http_accept": "*/*",
      "http_user_agent": null
    },
    "ie_daemontype": 3,
    "ie_sets": 2015,
    "nodeIP": "192.168.210.211",
    "ie_incidents": 47329,
    "ie_process_mosteps": -1,
    "ie_user_count": 140,
    "ie_edges": 3589,
    "WitFooApplianceID": "12335",
    "ie_retro_process_cycle_time": -1,
    "ie_mosteps": 964,
    "ie_activesets": 2,
    "organization": "[redacted]",
    "ie_process_setmembers": 1,
    "ie_close_percent": 70,
    "ie_report_cycle_time": -1,
    "WitFooName": "[redacted]",
    "ie_current_stage": "process_mosteps",
    "ie_process_leadrules": 36,
    "ie_setmembers": 225,
    "ie_nodes": 20037,
    "@timestamp": "2020-05-05T00:45:13.603Z",
    "metricEventName": "caprica_stats",
    "ie_peak_real_memory": 3059.06640625
  },
  "fields": {
    "recordingTimestamp": [
      "2020-05-05T00:44:55.000Z"
    ],
    "@timestamp": [
      "2020-05-05T00:45:13.603Z"
    ]
  }
}
```

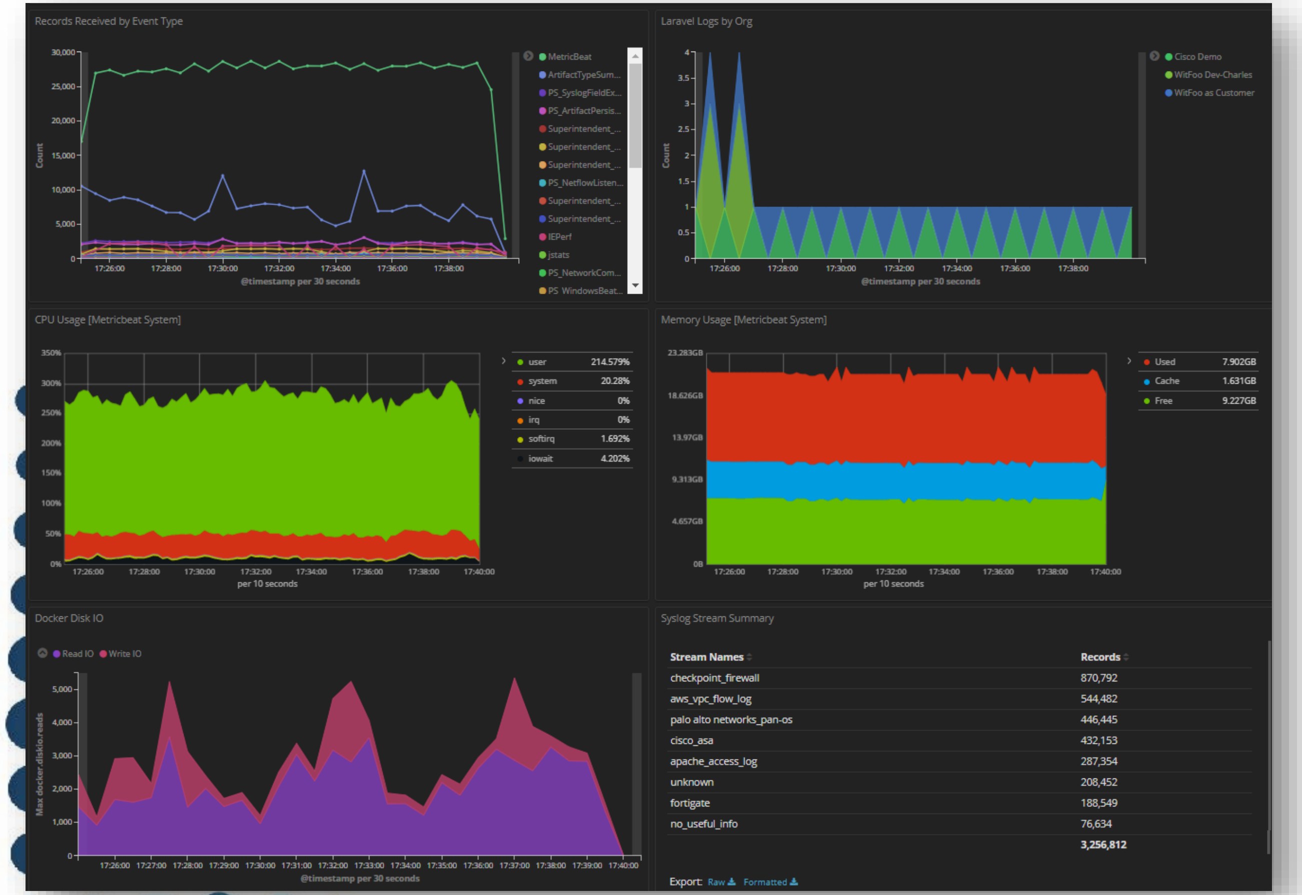
Commercial APM Collection



Custom Metric Collection Pipeline



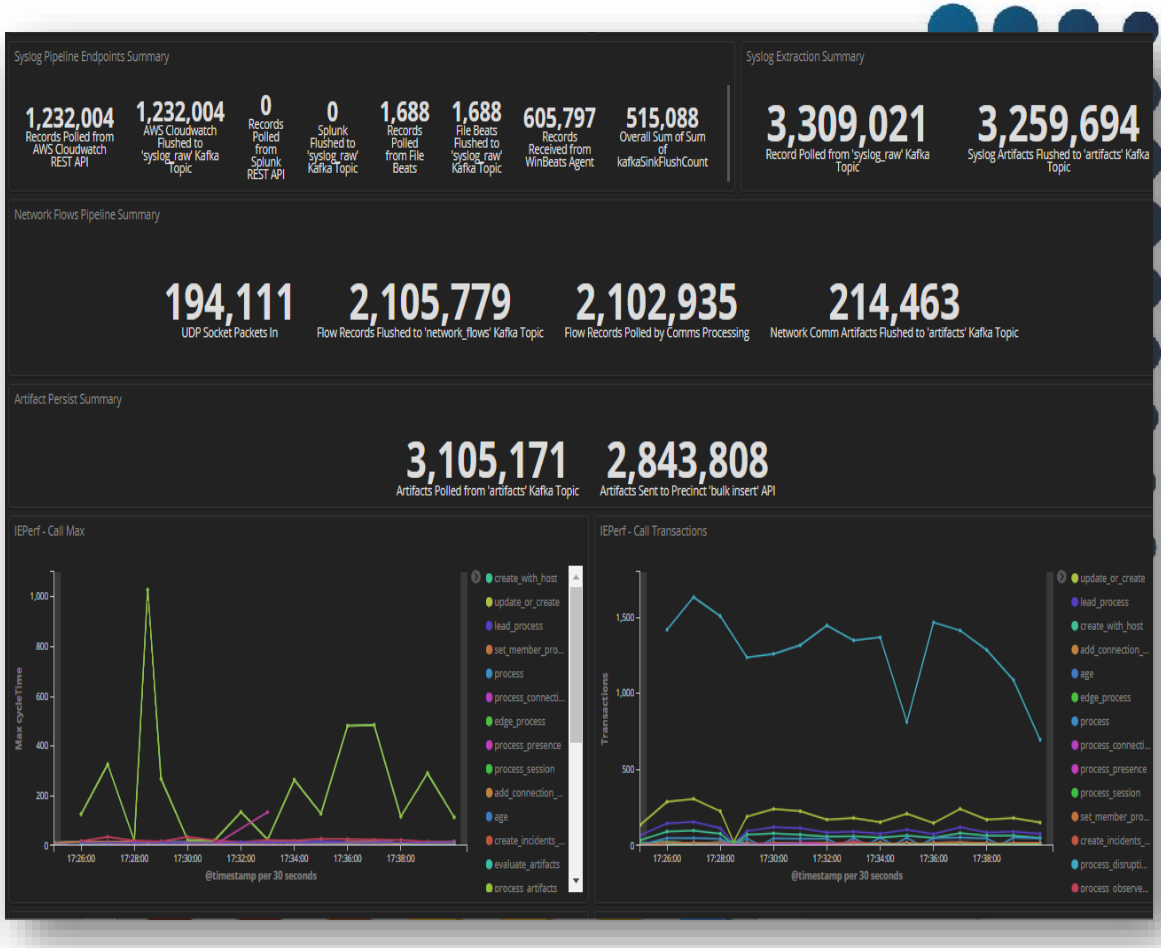
Metrics and More Metrics



Syslog Stream Summary

Stream Names	Records
checkpoint_firewall	870,792
aws_vpc_flow_log	544,482
palo alto networks_pan-os	446,445
cisco_asa	432,153
apache_access_log	287,354
unknown	208,452
fortigate	188,549
no_useful_info	76,634
	3,256,812

Export: Raw Formatted



Syslog Pipeline Endpoints Summary

1,232,004 Records Polled from AWS Cloudwatch REST API

1,232,004 AWS Cloudwatch Flushed to 'syslog_raw' Kafka Topic

0 Records Polled from Splunk REST API

0 Splunk Flushed to 'syslog_raw' Kafka Topic

1,688 Records Polled from File Beats

1,688 File Beats Flushed to 'syslog_raw' Kafka Topic

605,797 Records Received from WinBeats Agent

515,088 Overall Sum of Sum of kafkaSinkFlushCount

Syslog Extraction Summary

3,309,021 Record Polled from 'syslog_raw' Kafka Topic

3,259,694 Syslog Artifacts Flushed to 'artifacts' Kafka Topic

Network Flows Pipeline Summary

194,111 UDP Socket Packets In

2,105,779 Flow Records Flushed to 'network_flows' Kafka Topic

2,102,935 Flow Records Polled by Comms Processing

214,463 Network Comm Artifacts Flushed to 'artifacts' Kafka Topic

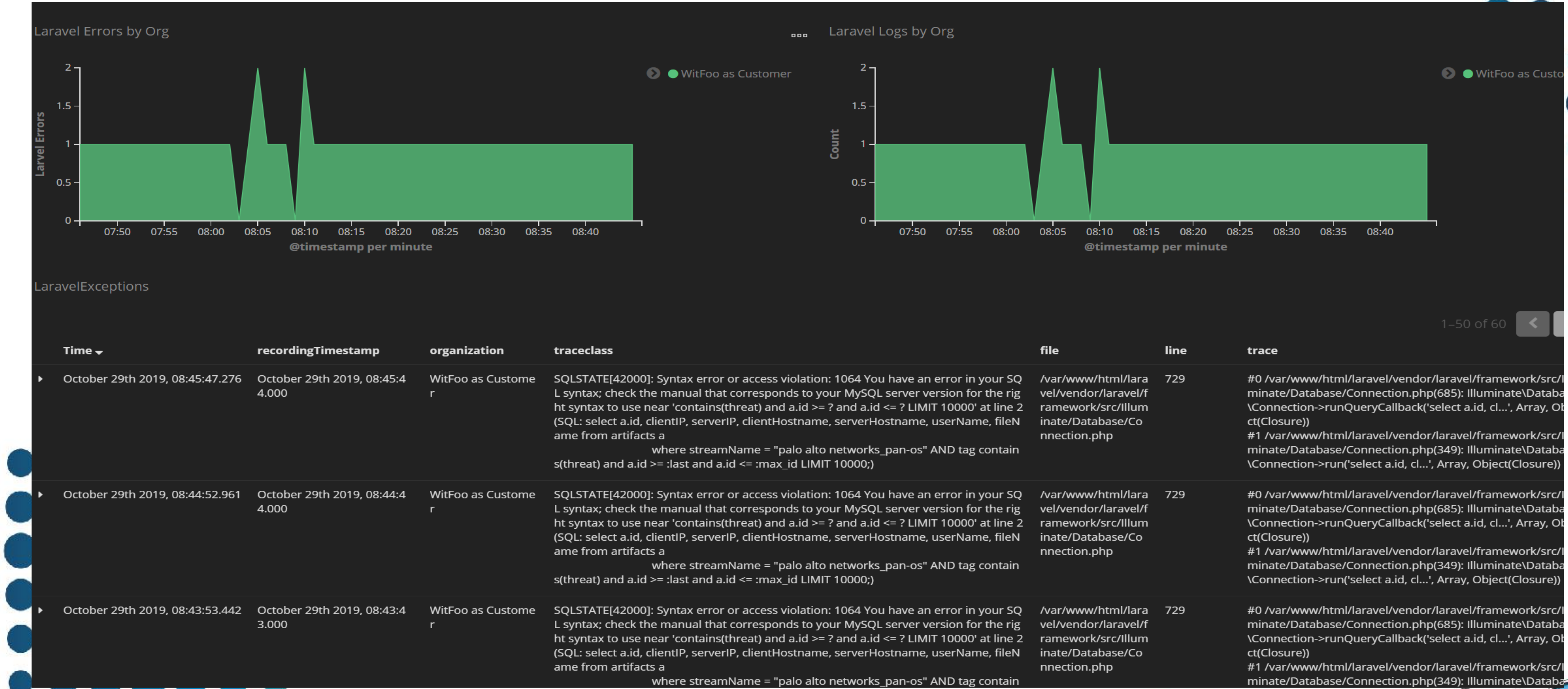
Artifact Persist Summary

3,105,171 Artifacts Polled from 'artifacts' Kafka Topic

2,843,808 Artifacts Sent to Precinct 'bulk insert' API

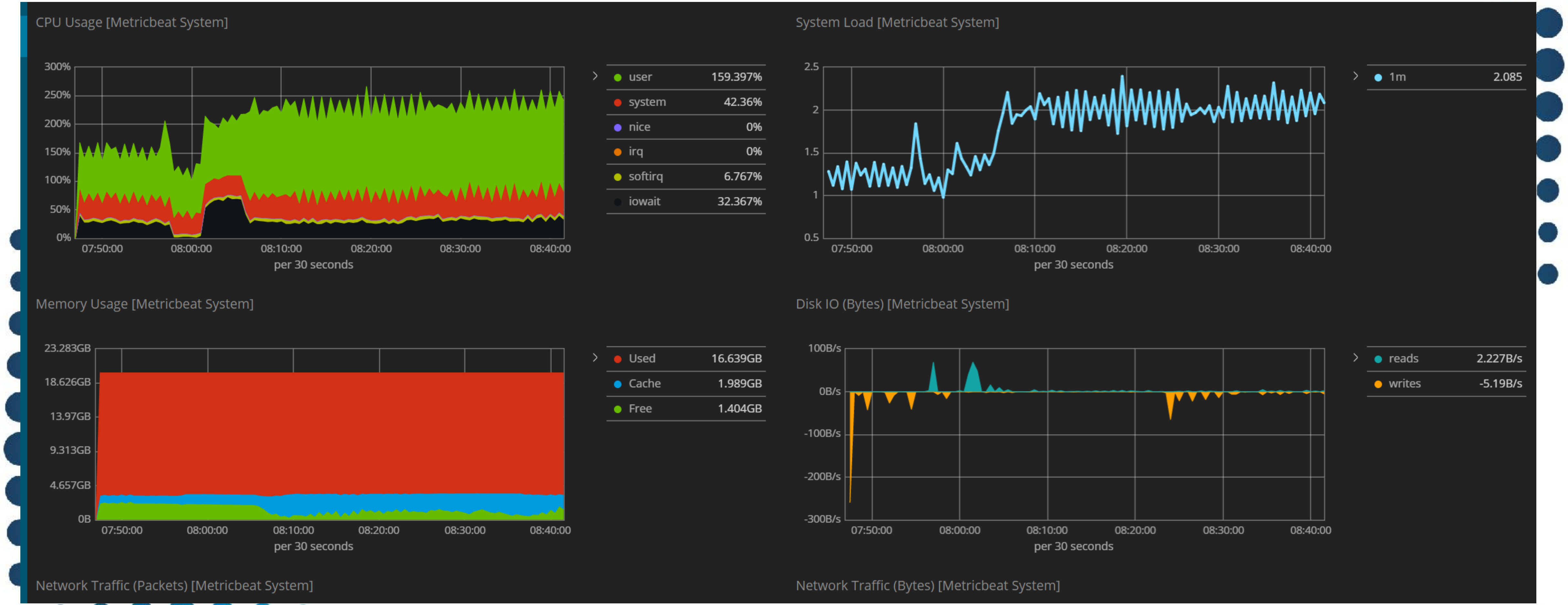
SECURE360

Error Catching



Time	recordingTimestamp	organization	traceclass	file	line	trace
October 29th 2019, 08:45:47.276	October 29th 2019, 08:45:44.000	WitFoo as Customer	SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'contains(threat) and a.id >= ? and a.id <= ? LIMIT 10000' at line 2 (SQL: select a.id, clientIP, serverIP, clientHostname, serverHostname, userName, fileName from artifacts a where streamName = "palo alto networks_pan-os" AND tag contains(threat) and a.id >= :last and a.id <= :max_id LIMIT 10000;)	/var/www/html/laravel/vendor/laravel/framework/src/Illuminate/Database/Connection.php	729	#0 /var/www/html/laravel/vendor/laravel/framework/src/I minate/Database/Connection.php(685): Illuminate\Databa \Connection->runQueryCallback('select a.id, cl...', Array, Ob ct(Closure)) #1 /var/www/html/laravel/vendor/laravel/framework/src/I minate/Database/Connection.php(349): Illuminate\Databa \Connection->run('select a.id, cl...', Array, Object(Closure))
October 29th 2019, 08:44:52.961	October 29th 2019, 08:44:44.000	WitFoo as Customer	SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'contains(threat) and a.id >= ? and a.id <= ? LIMIT 10000' at line 2 (SQL: select a.id, clientIP, serverIP, clientHostname, serverHostname, userName, fileName from artifacts a where streamName = "palo alto networks_pan-os" AND tag contains(threat) and a.id >= :last and a.id <= :max_id LIMIT 10000;)	/var/www/html/laravel/vendor/laravel/framework/src/Illuminate/Database/Connection.php	729	#0 /var/www/html/laravel/vendor/laravel/framework/src/I minate/Database/Connection.php(685): Illuminate\Databa \Connection->runQueryCallback('select a.id, cl...', Array, Ob ct(Closure)) #1 /var/www/html/laravel/vendor/laravel/framework/src/I minate/Database/Connection.php(349): Illuminate\Databa \Connection->run('select a.id, cl...', Array, Object(Closure))
October 29th 2019, 08:43:53.442	October 29th 2019, 08:43:43.000	WitFoo as Customer	SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'contains(threat) and a.id >= ? and a.id <= ? LIMIT 10000' at line 2 (SQL: select a.id, clientIP, serverIP, clientHostname, serverHostname, userName, fileName from artifacts a where streamName = "palo alto networks_pan-os" AND tag contain	/var/www/html/laravel/vendor/laravel/framework/src/Illuminate/Database/Connection.php	729	#0 /var/www/html/laravel/vendor/laravel/framework/src/I minate/Database/Connection.php(685): Illuminate\Databa \Connection->runQueryCallback('select a.id, cl...', Array, Ob ct(Closure)) #1 /var/www/html/laravel/vendor/laravel/framework/src/I minate/Database/Connection.php(349): Illuminate\Databa

System Performance



CPU Usage [Metricbeat System]

● user	159.397%
● system	42.36%
● nice	0%
● irq	0%
● softirq	6.767%
● iowait	32.367%

System Load [Metricbeat System]

● 1m	2.085

Memory Usage [Metricbeat System]

● Used	16.639GB
● Cache	1.989GB
● Free	1.404GB

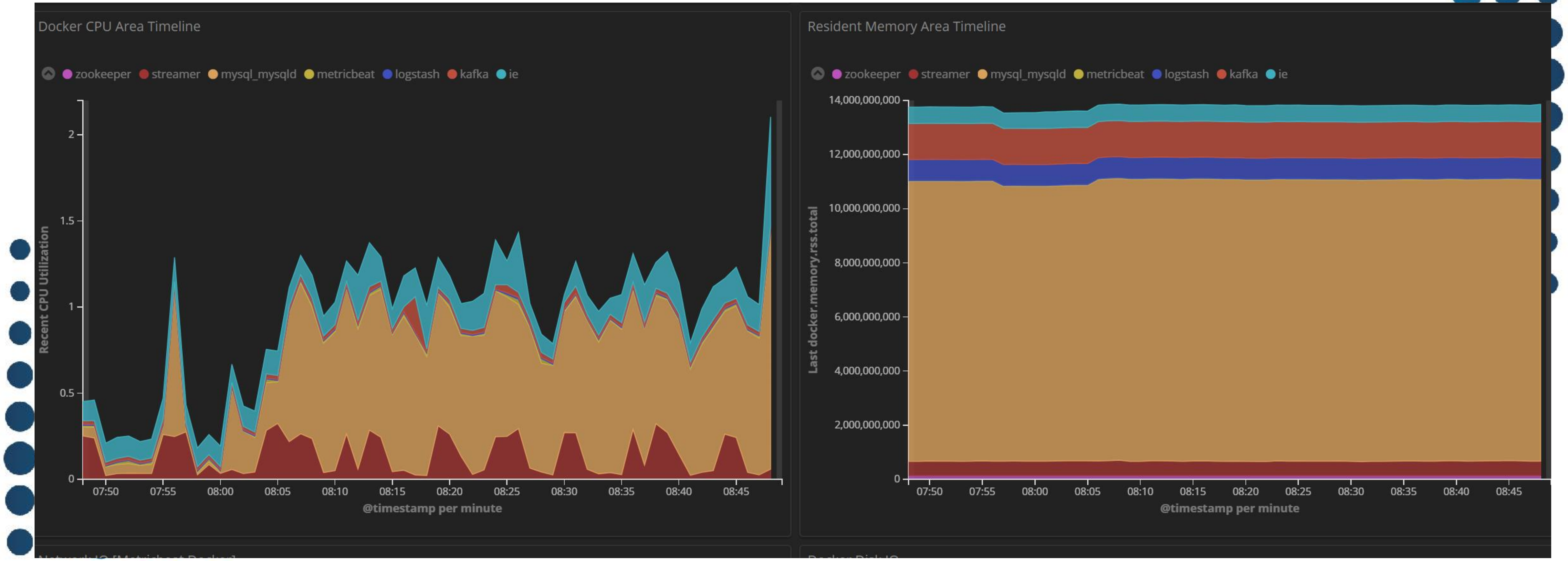
Disk IO (Bytes) [Metricbeat System]

● reads	2.227B/s
● writes	-5.19B/s

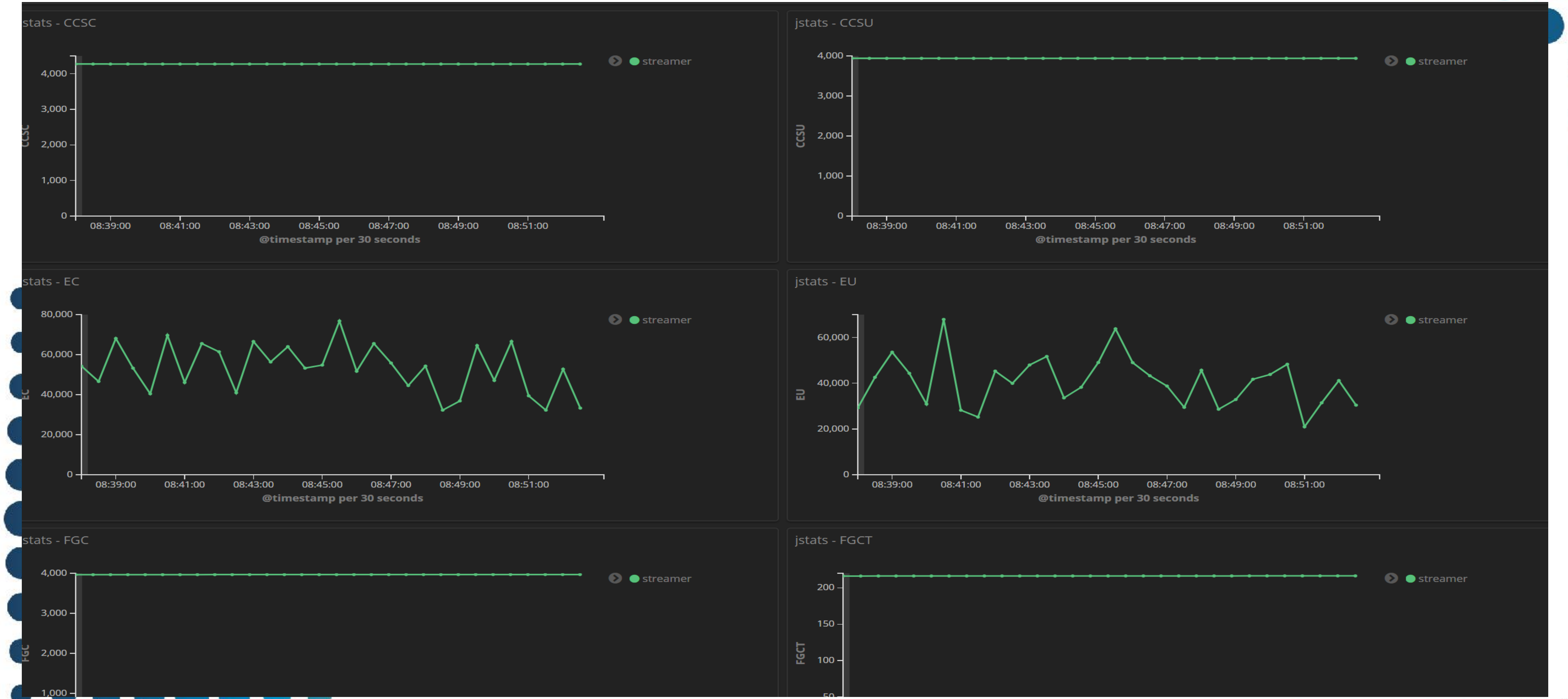
Network Traffic (Packets) [Metricbeat System]

Network Traffic (Bytes) [Metricbeat System]

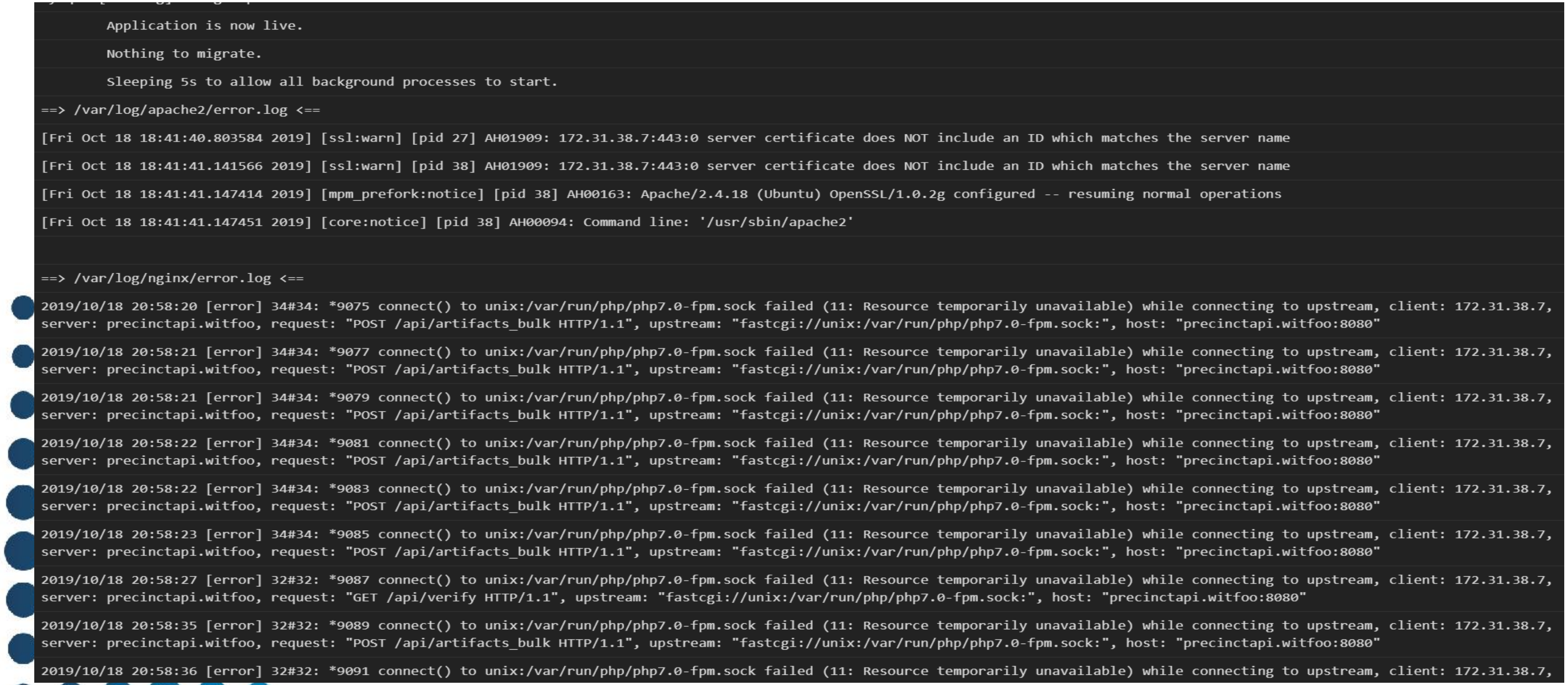
Docker Container Performance



JVM Health

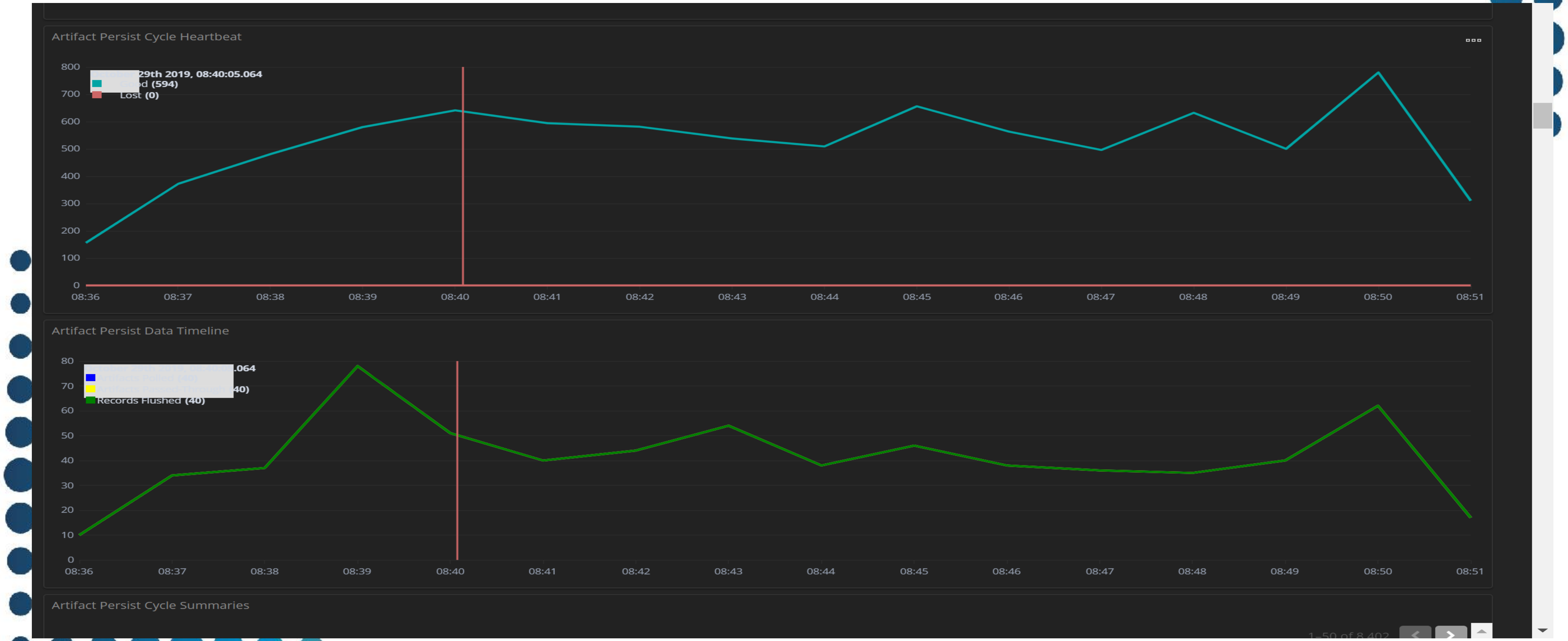

stats - CCSC
4,000
3,000
2,000
1,000
0
CCSC
08:39:00
08:41:00
08:43:00
08:45:00
08:47:00
08:49:00
08:51:00
@timestamp per 30 seconds
streamer
jstats - CCSU
4,000
3,000
2,000
1,000
0
CCSU
08:39:00
08:41:00
08:43:00
08:45:00
08:47:00
08:49:00
08:51:00
@timestamp per 30 seconds
streamer
stats - EC
80,000
60,000
40,000
20,000
0
EC
08:39:00
08:41:00
08:43:00
08:45:00
08:47:00
08:49:00
08:51:00
@timestamp per 30 seconds
streamer
jstats - EU
60,000
40,000
20,000
0
EU
08:39:00
08:41:00
08:43:00
08:45:00
08:47:00
08:49:00
08:51:00
@timestamp per 30 seconds
streamer
stats - FGC
4,000
3,000
2,000
1,000
FGC
streamer
jstats - FGCT
200
150
100
50
FGCT
streamer

Logging

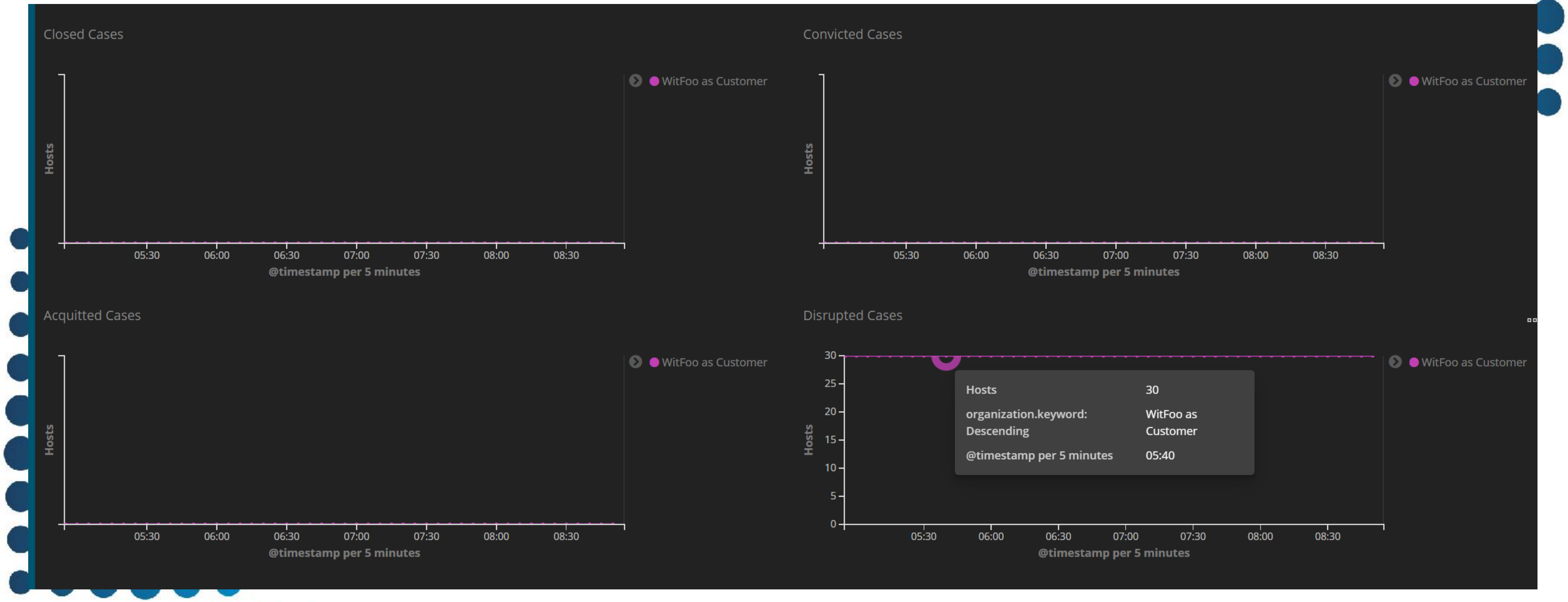


```
        Application is now live.
        Nothing to migrate.
        Sleeping 5s to allow all background processes to start.
==> /var/log/apache2/error.log <==
[Fri Oct 18 18:41:40.803584 2019] [ssl:warn] [pid 27] AH01909: 172.31.38.7:443:0 server certificate does NOT include an ID which matches 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

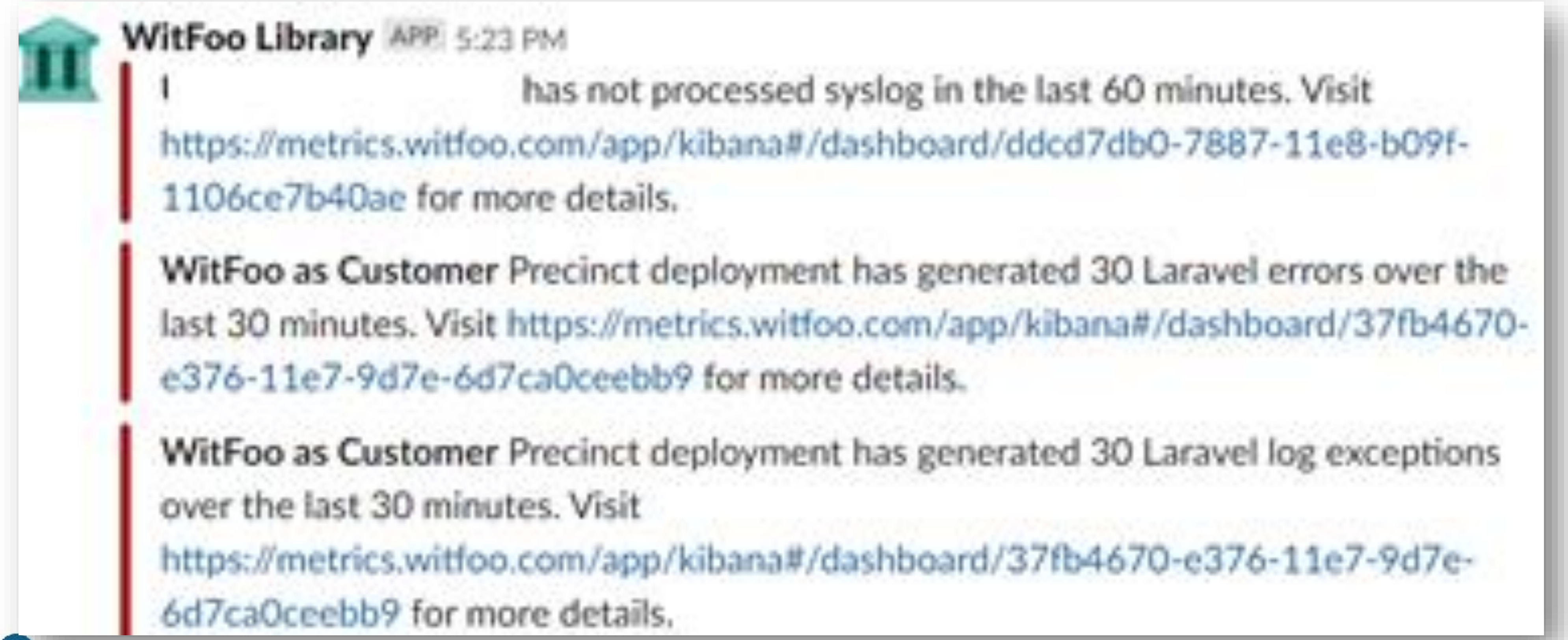


User Interaction



Hosts	30
organization.keyword: Descending	WitFoo as Customer
@timestamp per 5 minutes	05:40

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.

Metric Driven Philosophies

- Maximize Metrics
- Sustainable, Enduring Development
- Write Unit/System tests from learned lessons
- Reduce Risk in Experiments (Fail faster and safer)
- Validate assertions quickly (More Experiments)
- Precision in Decision Making
- Skip writing unnecessary tests
- Adjust platform on data results
- Reduce customer effort (& exhaustion)

SECURE360

Metric Driven SECDEVOPS

Charles Herring
CTO, WitFoo

Ryan Self
Chief Data Researcher, WitFoo

Slides: www.witfoo.com/blog/S360-2020