



Business Oriented Proactive Monitoring at Capital One

Geethanjali Gopal
Suman Ojha

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.



Introduction

- ▶ **Suman Ojha**
Sr. Data Engineer
Capital One
 - ▶ **Geethanjali Gopal**
Director of Software Engineering
Capital One

Ensuring High Reliability of Identity Services is critical to our business

Log Proliferation

Complex Data Lineage

Complex Data Lineage

Federated Architecture

Log Proliferation

Test Me

Log Proliferation

Test Me

Test

Tool Proliferation

Complex Data Lineage

Don't use me

Complex Data Lineage

Micro-Services

Test Me

Federated Architecture

Why Test

Technology vs Experience

Don't use me

Too much irrelevant information

I am so irrelevant

Federated Architecture

Don't know what to test

Don't know what to test

Log Proliferation

Technology vs Experience

I am so irrelevant

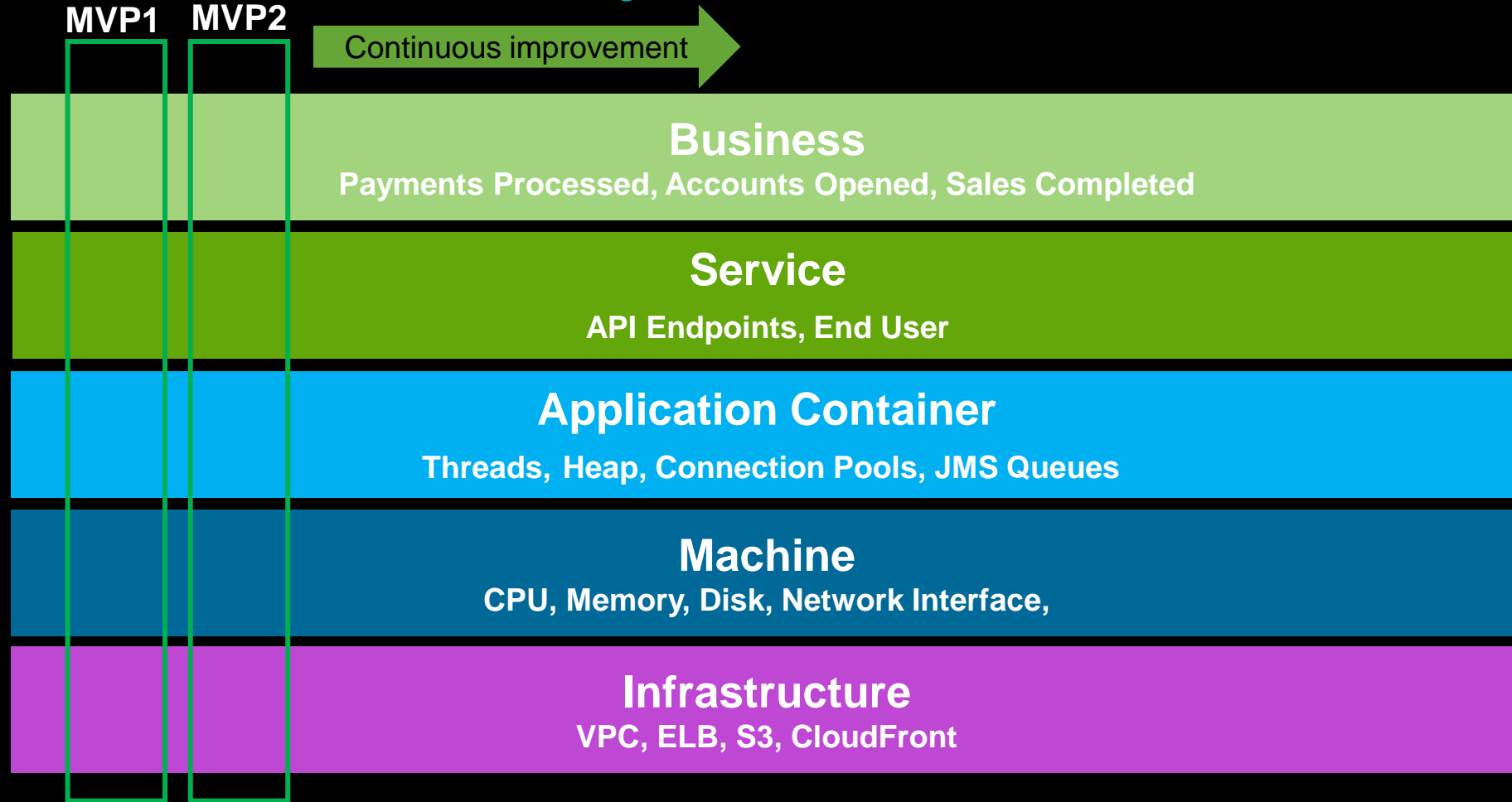
Alert Fatigue

Alert Fatigue

Technology vs Experience

Alert Fatigue1

Business-Oriented approach focuses on delivering value early and often



Unified drillable dashboards, actionable metrics,
high-fidelity alerts

Methodical approach to monitoring using Gartner use case management framework

Ref: Gartner use case management framework

- Identify use cases
- Prioritize use cases (log inventory, tool inventory)
- Implement use cases
- Review use cases -> Optimize or Retire

Treat use cases that are not actionable as defects

Use Case Template

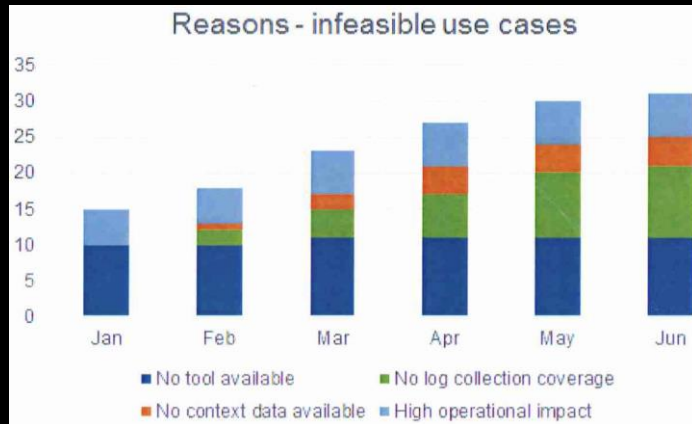
Ref: Gartner use case management framework

Use Case Design Template - Example	
Use Case Name	PCI DSS Data accessed from outside the Cardholder Data Environment (CDE)
Use Case Description	Database of payment data is accessed by hosts external to the Cardholder Data Environment
Use Case Driver	PCI DSS Compliance
Required Data	Payment data database access logs
Required Context Data	Information about CDE IP ranges, whitelists related to DBA activity (jump servers)
Time View	Real-time alerts
Candidate Tool for Implementation	SIEM
Processes Affected	SOC playbook, DBA activities
Teams Affected	SOC, DBAs

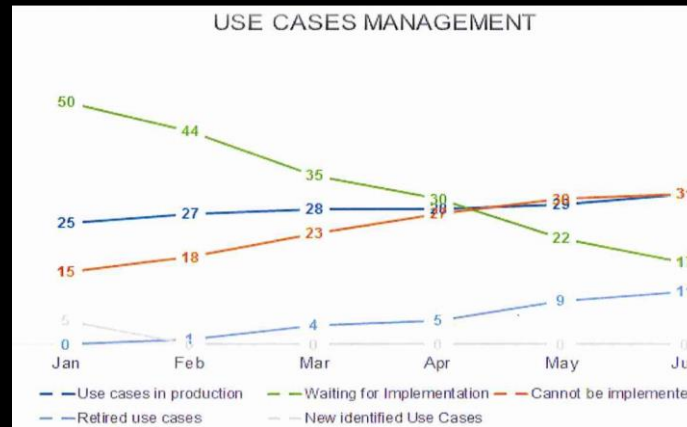
- Log Inventory
- Tool Inventory

Understand and improve monitoring by actively managing monitoring use cases

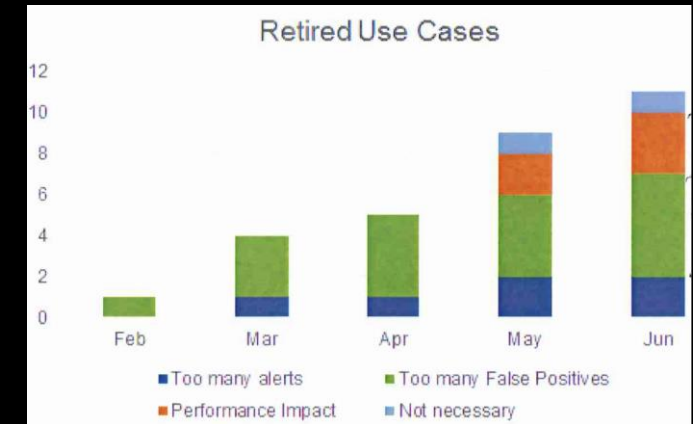
Reason infeasible use cases and fix critical issues



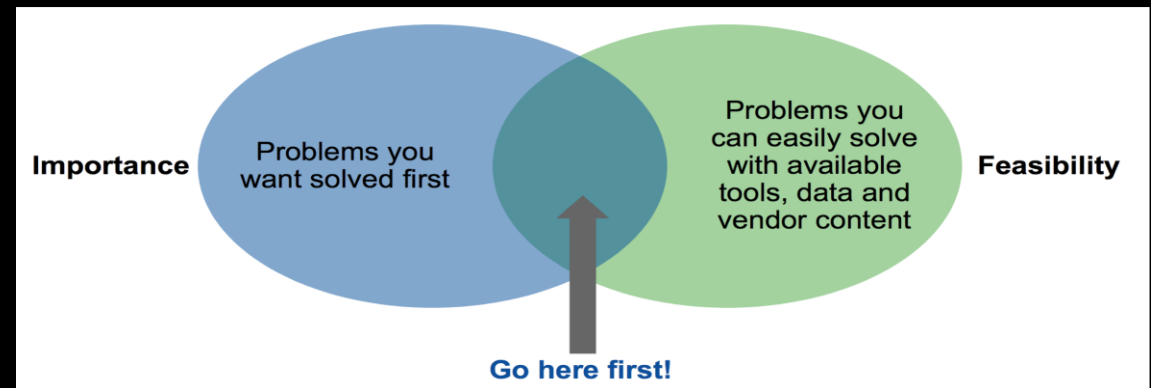
Actively manage security monitoring use cases



Actively retire use cases and manage them as defects



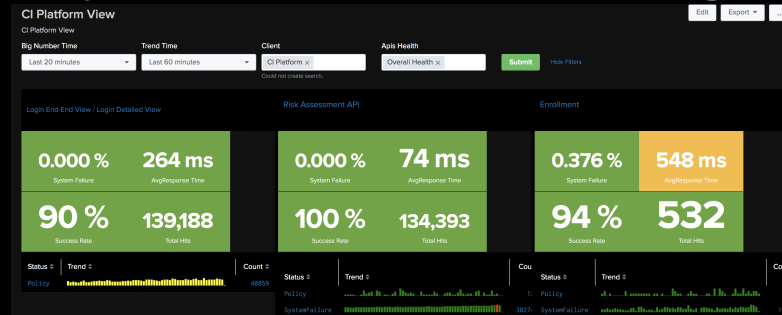
- Develop use cases
- Conduct feasibility exercise
- Implement/optimize/update



Ref: Gartner use case management framework

Business oriented approach with end to end drillable view

Are my business features meeting SLAs?



Business metric view

API view of a business feature

Deep Dive into one business feature

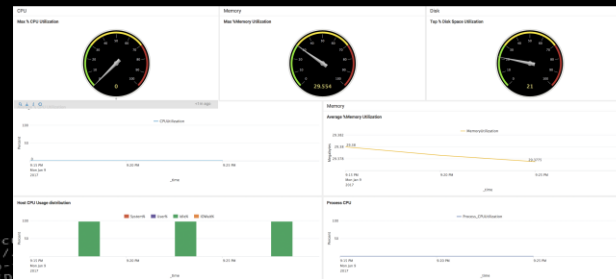
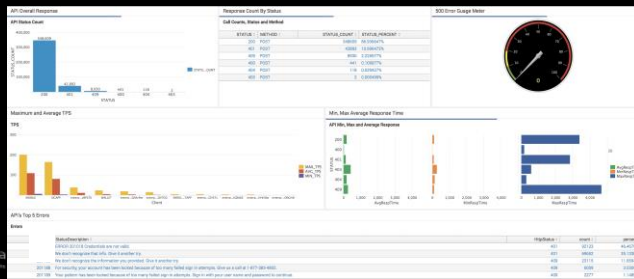


Is my API healthy – one page view of business health of an API

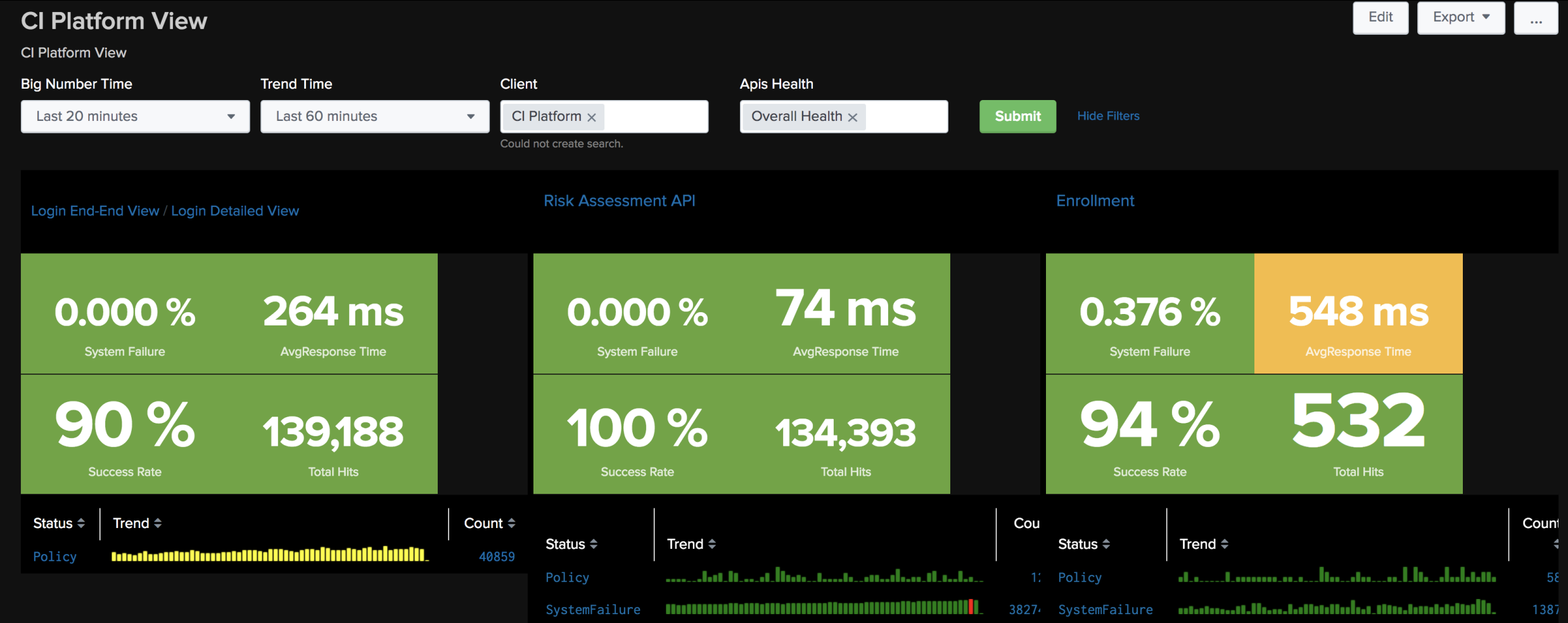
18,710 Total Calls 4,244 Risk Assessment 25,911 Risk Assessment - Jar Implementation	16,386 Total Success 4,220 Risk Assessment 25,909 Risk Assessment	2,324 Total Business Failures 0 Risk Assessment 1 Risk Assessment	0 System Failures-500 0 Risk Assessment 1 System Failures-500
--	---	---	---

Is my stack Healthy - One Page view of environment health of the entire stack

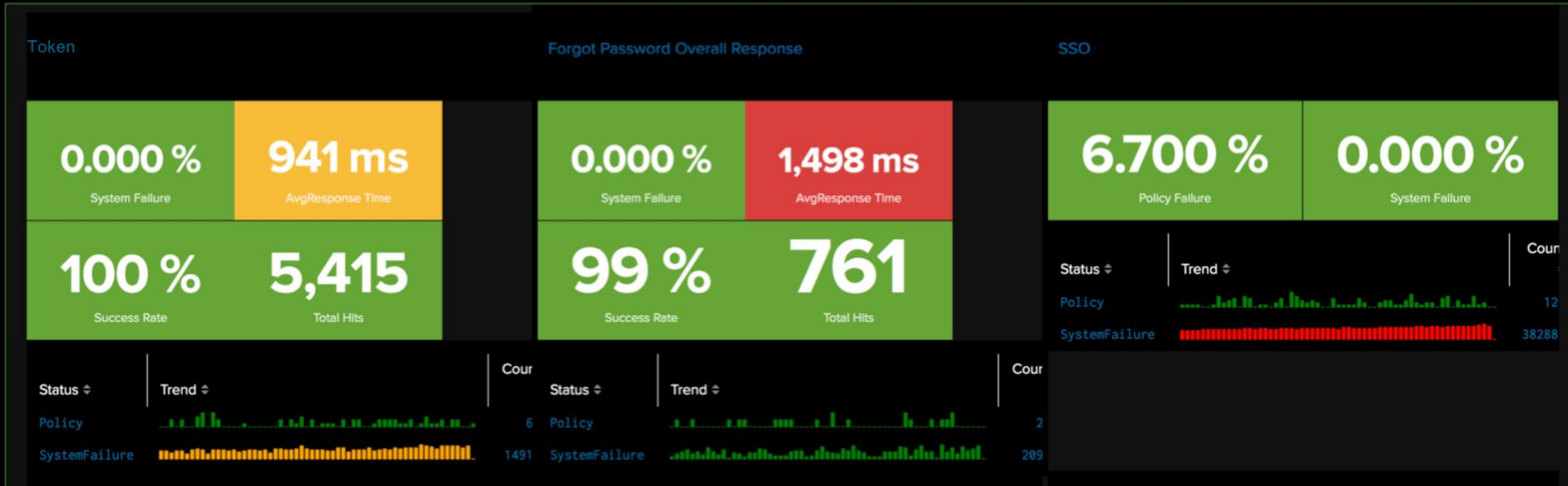
Deep Dive into one service



Bird's-eye view of end to end business performance of all business features



Bird's-eye view of end-to-end business performance (contd.)

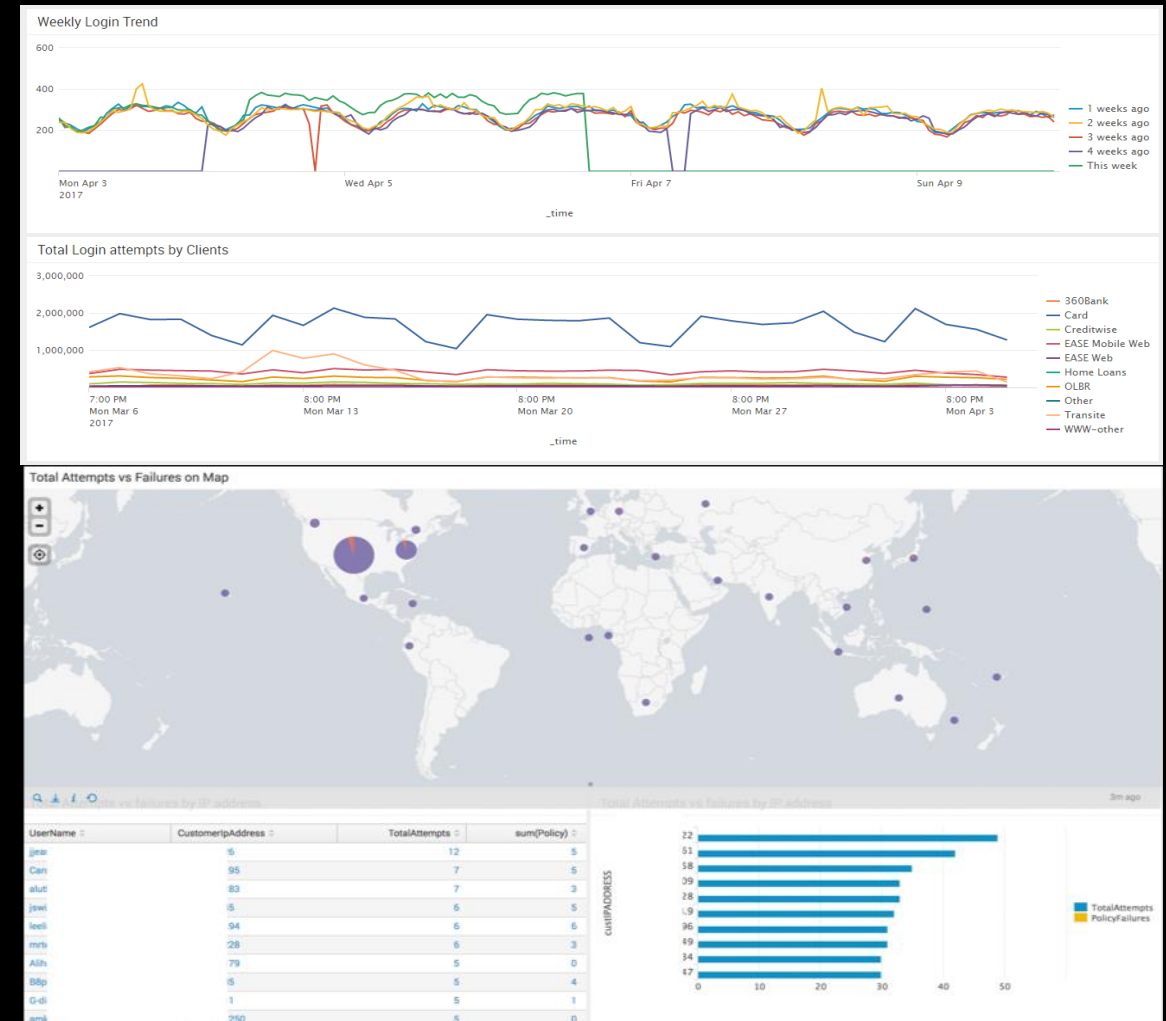


Drill-down view of business performance of one business feature

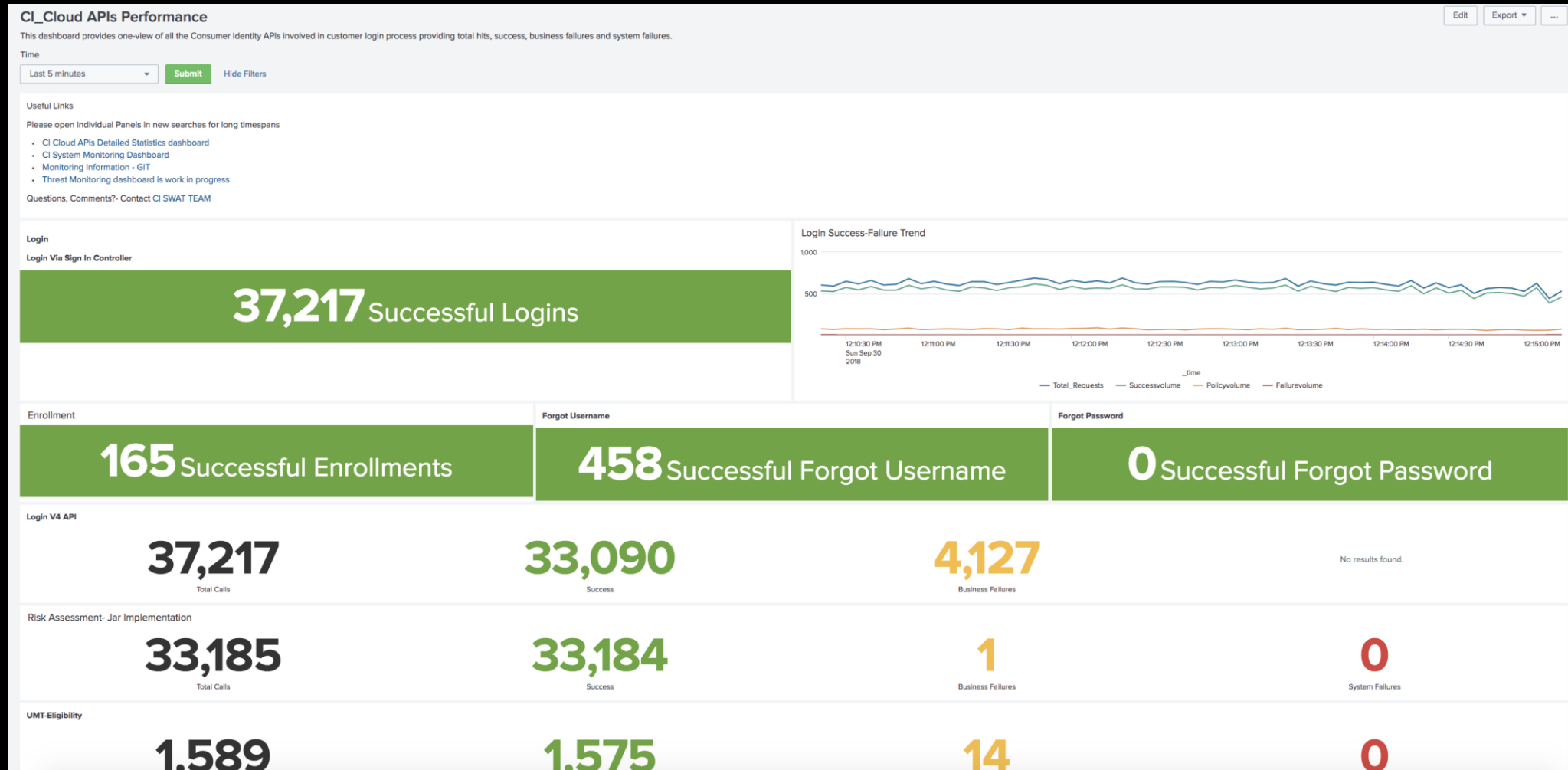
Business Performance View



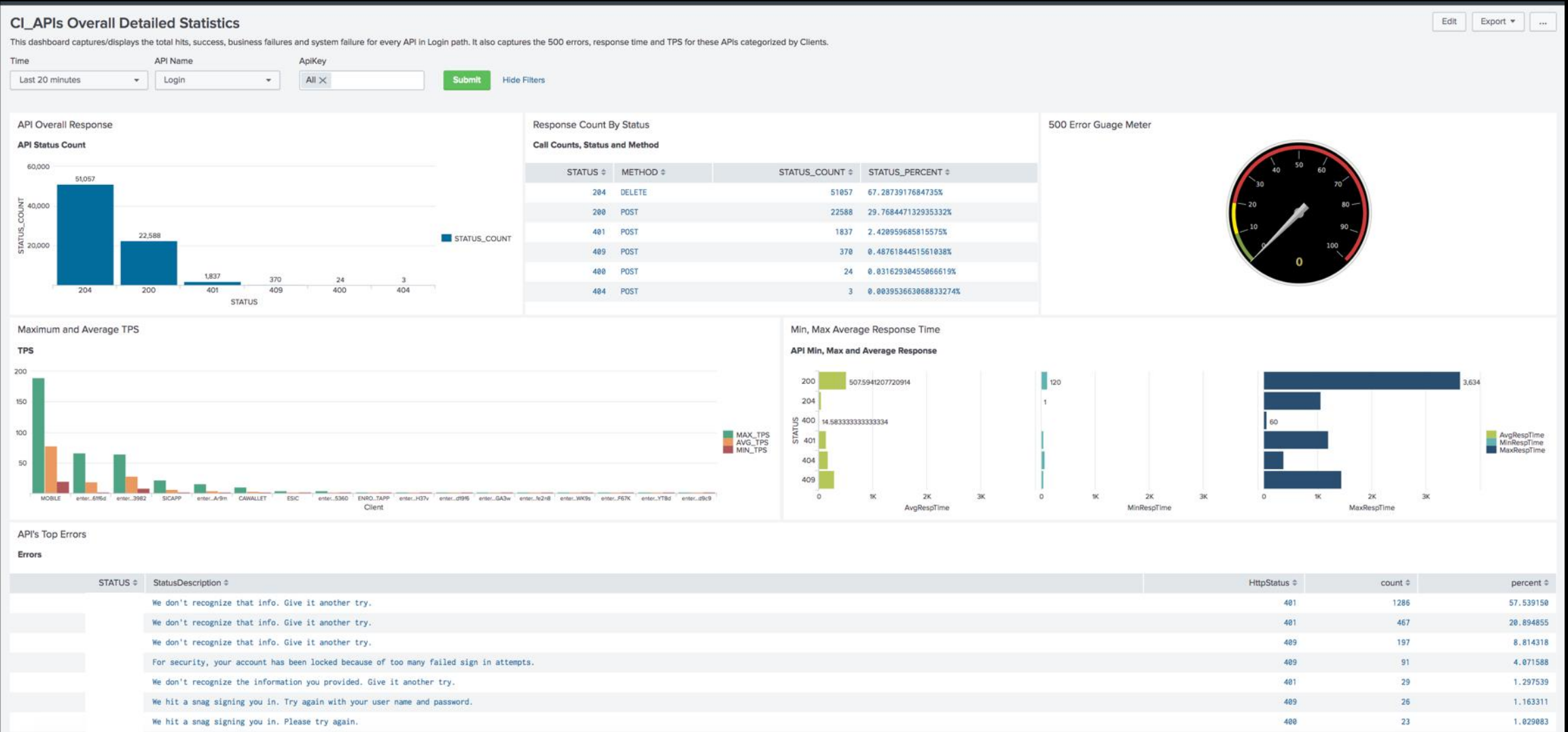
Geo View



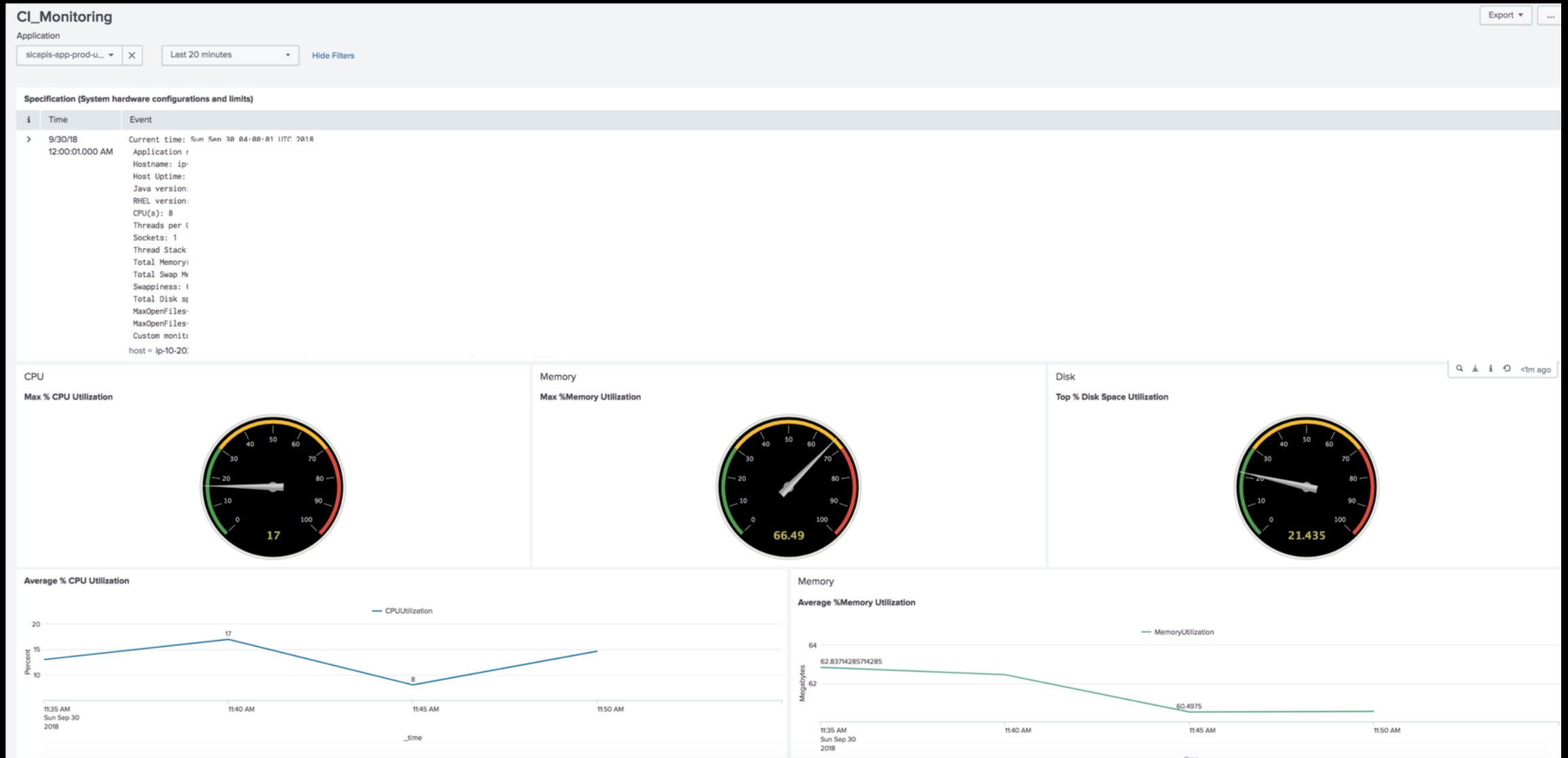
Central API view of all services that make up a business feature



Detailed view of API performance – standardized view

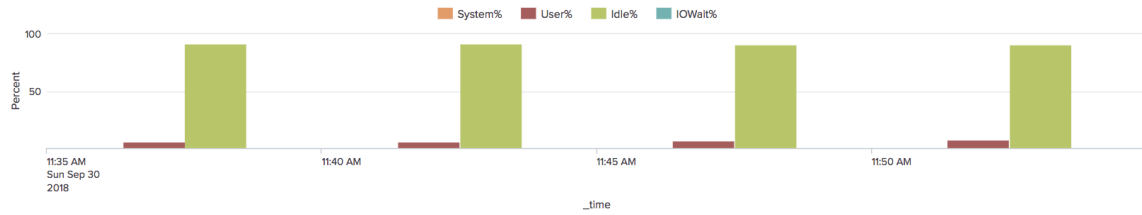


Systems view of an entire stack that hosts a service

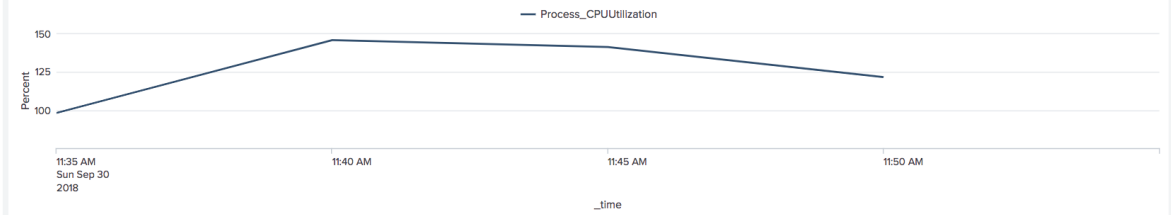


Systems view contd.

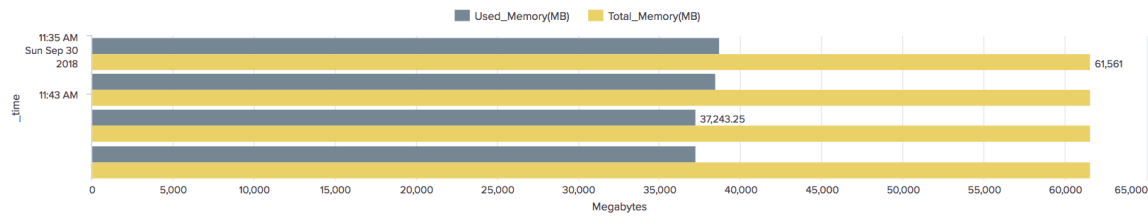
Host CPU Usage distribution



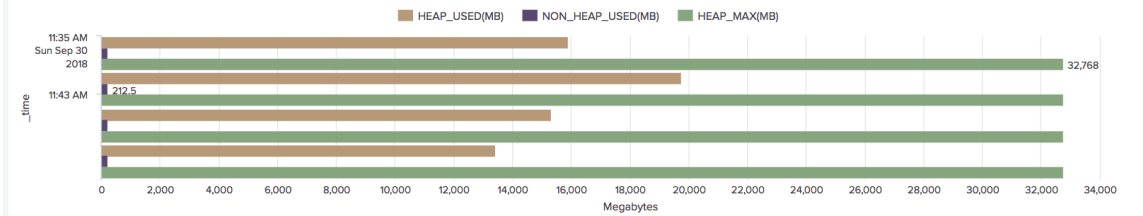
Process CPU



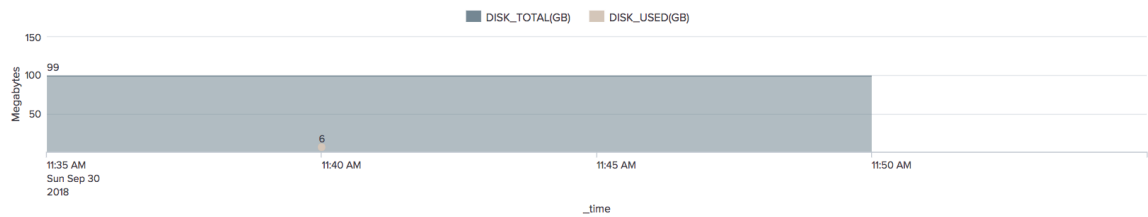
Host Memory



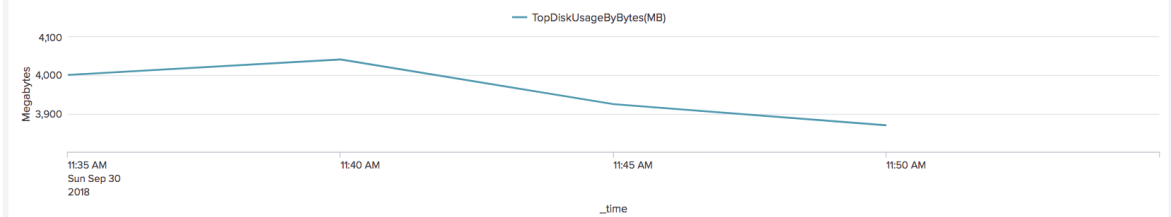
JVM Memory



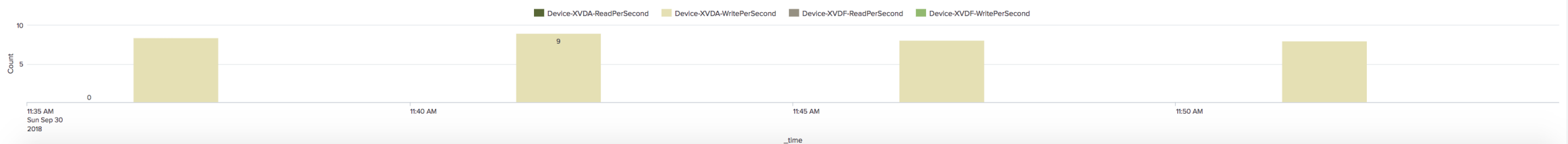
Disk Space Utilization



Top Disk Space Utilization



Disk IO



Decisioning actions can be automated on High Fidelity Alerts

- ▶ **Learn the threshold with data**
- ▶ **Review the pattern for similar datasets over a period of time**
 - Comparison over 90 days time period and remove outliers
- ▶ **Follow multi-prong approach to automate decisioning/action**
 - No. of prongs based on business needs

Hard Code Threshold

login trend changes through out the day so
hard coding did not work



Previous Day Comparison

Trend changes through out the week so comparison
with previous day did not work



Comparison over 90 days time period and remove outliers

Average(count over last 15m) > 1.2(95th percentile (data set of
15m averages for identical daily time block (prior 90 days)))

Key Takeaways

- ▶ **Make your system observable** starting with selected metrics
- ▶ **Succeed by applying a business oriented approach** to monitoring
 - Deliver value early and often
 - Avoid tools/infra rabbit holes
 - Create standards/spec
- ▶ **You don't have to break the bank** to build next generation monitoring
 - Maximize usage of existing tools/data
 - Build unified, drillable dashboards with actionable metrics
 - Create high fidelity alerts
- ▶ **Bake monitoring use cases into feature delivery**
 - Use Gartner framework

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10404; rv:1.9.1.10404; like Gecko; Chrome/28.0.1467.111 Safari/537.6" 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD9SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:53.0) Gecko/20100801 Firefox/53.0" 317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-108" 130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10404; rv:1.9.1.10404; like Gecko; Chrome/28.0.1467.111 Safari/537.6" 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD9SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:53.0) Gecko/20100801 Firefox/53.0" 317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-108" 130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10404; rv:1.9.1.10404; like Gecko; Chrome/28.0.1467.111 Safari/537.6" 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD9SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:53.0) Gecko/20100801 Firefox/53.0" 317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-108"