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.

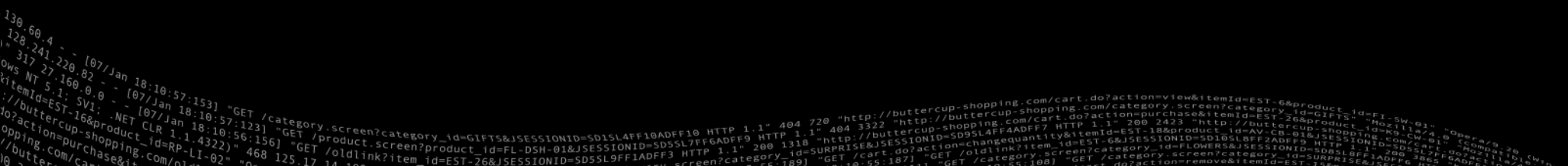
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements 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> .conf18

Introduction

Who We Are

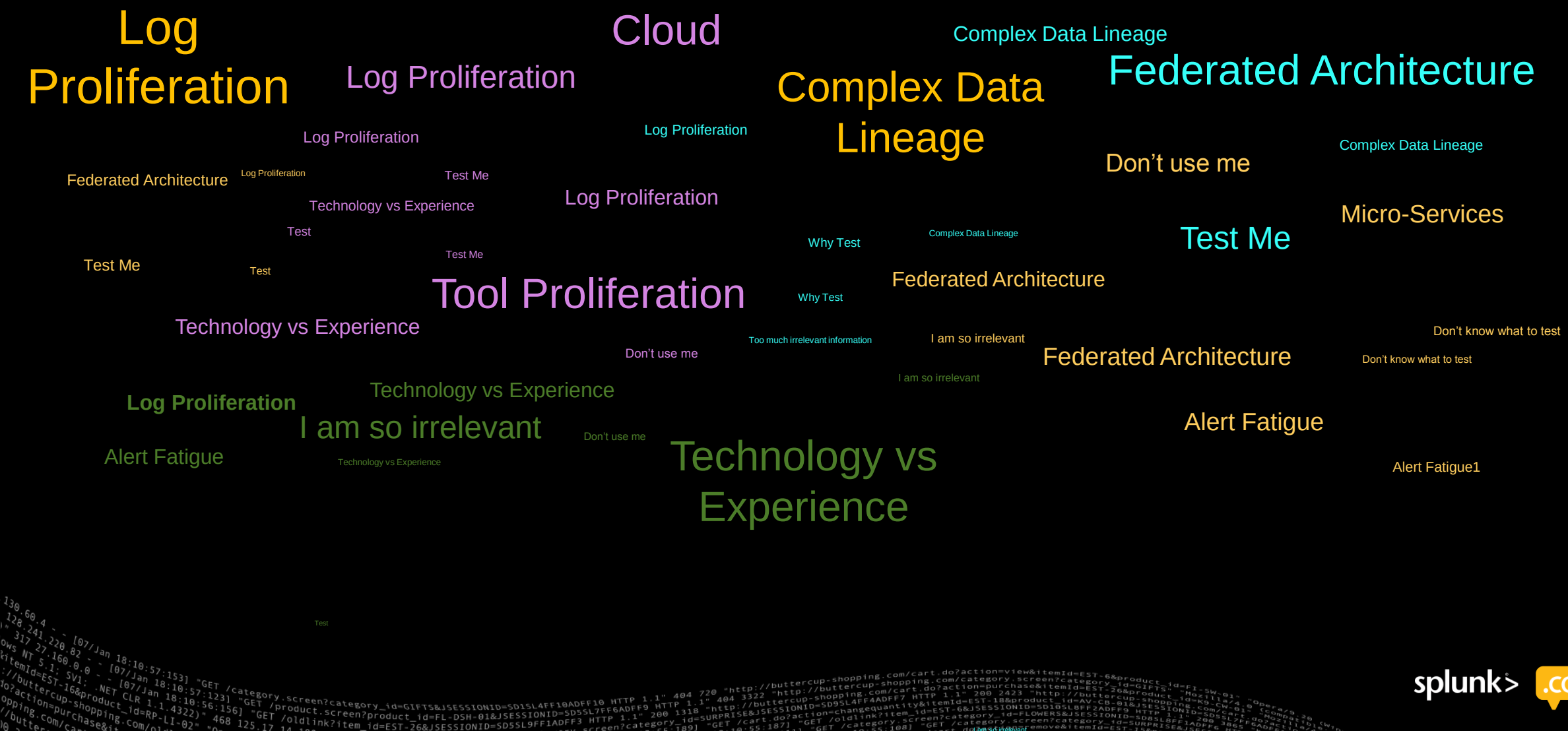
- Suman Ojha
  Sr. Data Engineer
  Capital One
- Geethanjali Gopal
  Director of Software Engineering
  Capital One



Ensuring High Reliability of Identity Services is critical to our business

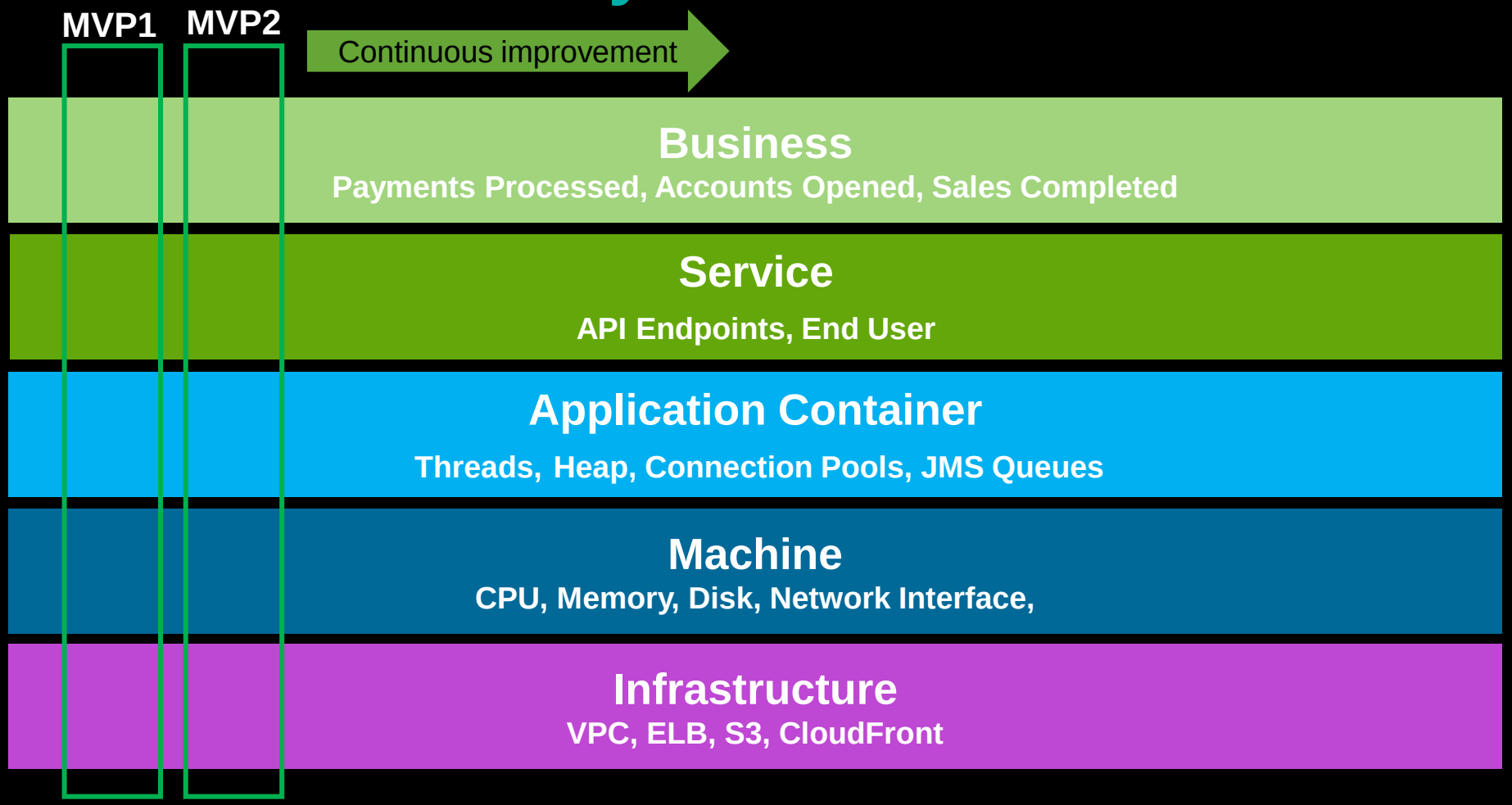
splunk> .conf18

Technology advancement brings new challenges



splunk> .conf18

Business-Oriented approach focuses on delivering value early and often



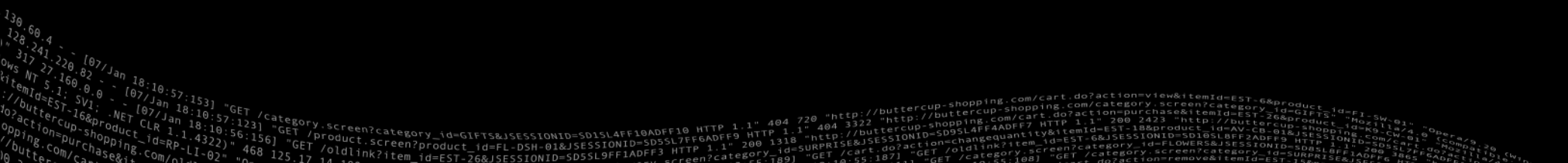
Unified drillable dashboards, actionable metrics, high-fidelity alerts

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

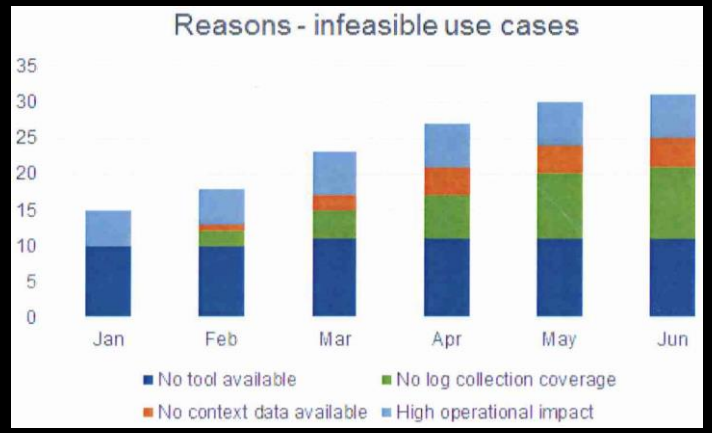
Use Case Design Template - Example	
Use Case Name	PCI DSS Data accessed from outside the Cardholder Data Environment (CDE)
Use Case Description	Database of payment data is accessed by hosts external to the Cardholder Data Environment
Use Case Driver	PCI DSS Compliance
Required Data	Payment data database 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**

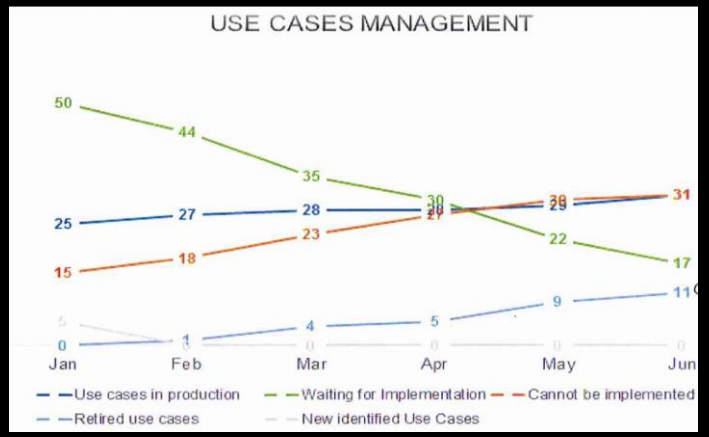
splunk> .conf18

Understand and improve monitoring by actively managing monitoring use cases

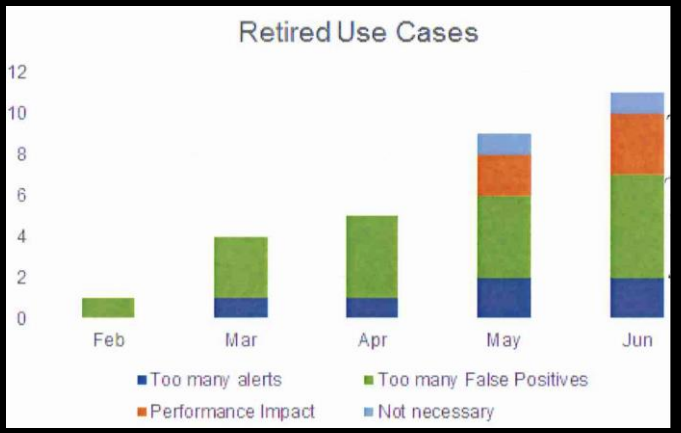
Reason infeasible use cases and fix critical issues



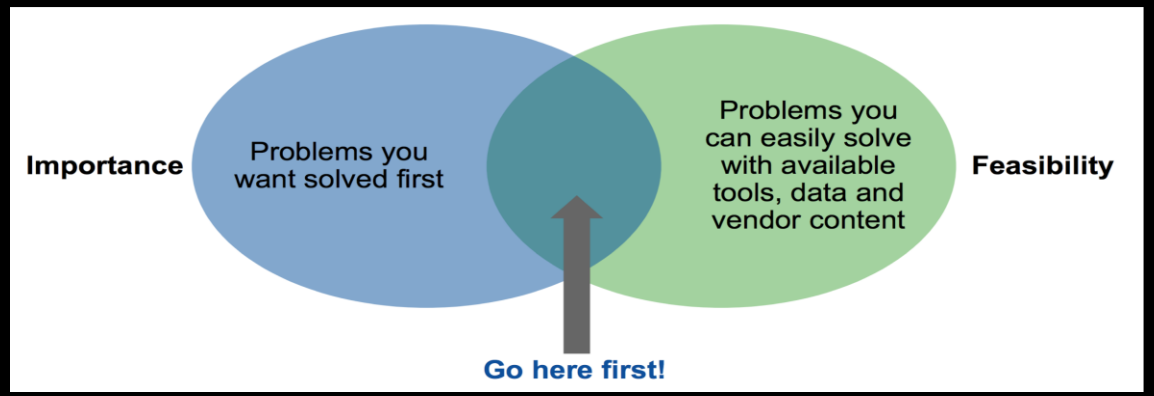
Actively manage security monitoring use cases



Actively retire use cases and manage them as defects



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

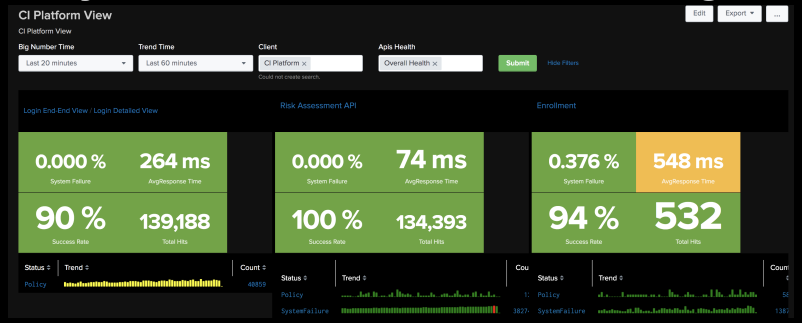


Ref: Gartner use case management framework

splunk> .conf18

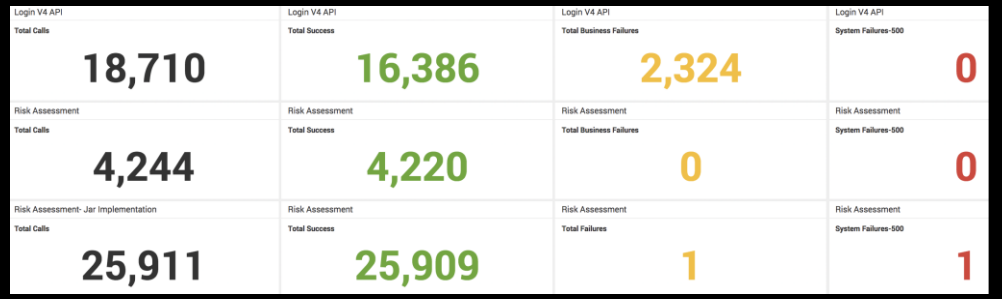
Business oriented approach with end to end drillable view

Are my business features meeting SLAs?



Business metric view

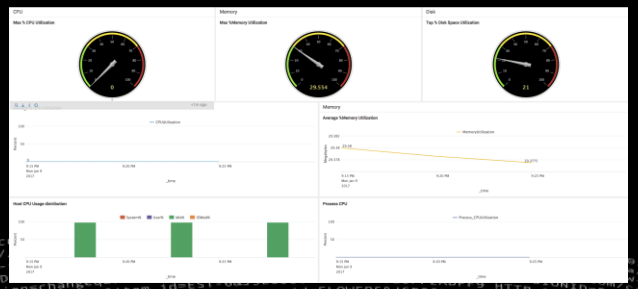
API view of a business feature



Deep Dive into one business feature

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

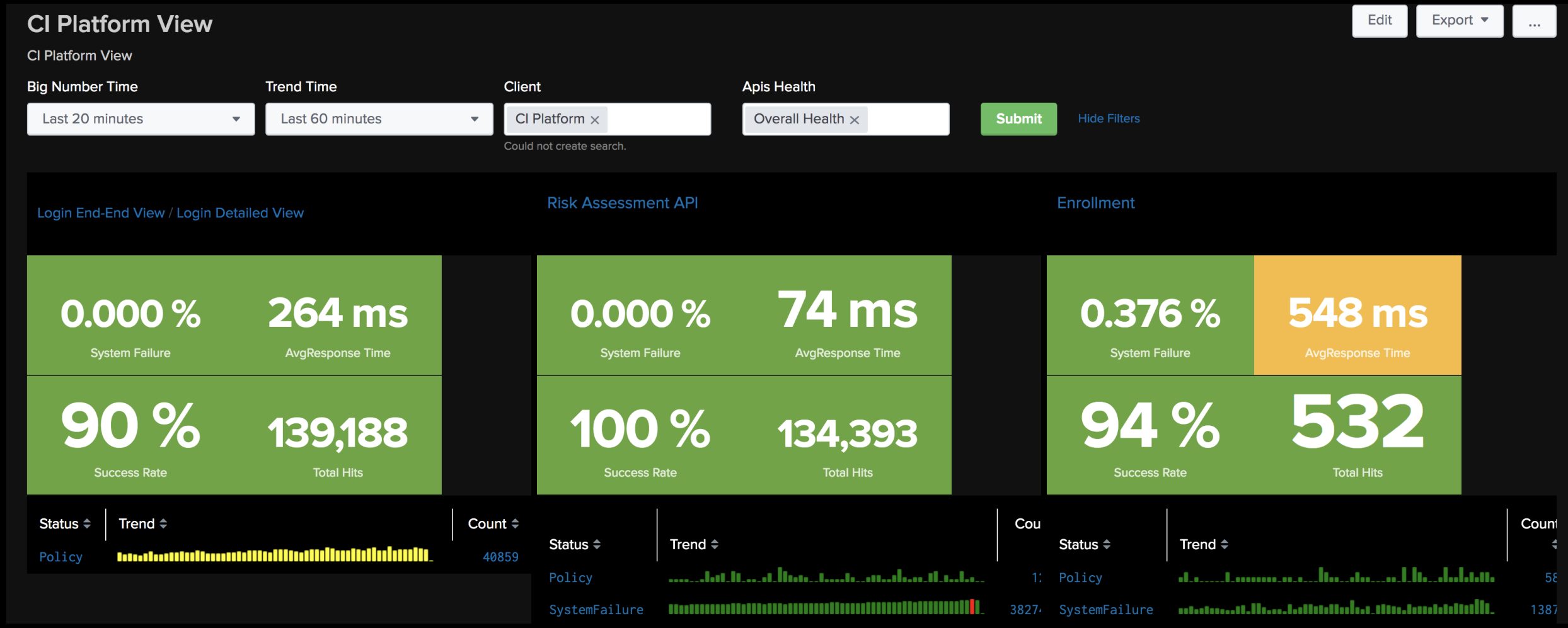
Is my stack Healthy - One Page view of environment health of the entire stack



Deep Dive into one service

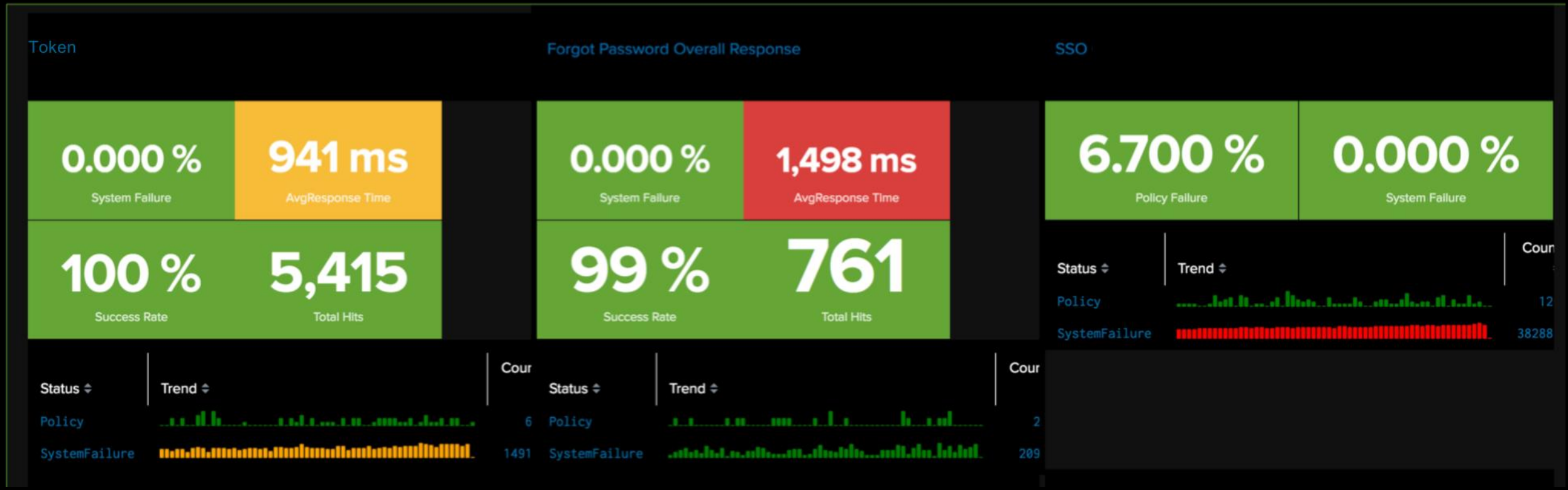
splunk> .conf18

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



splunk> .conf18

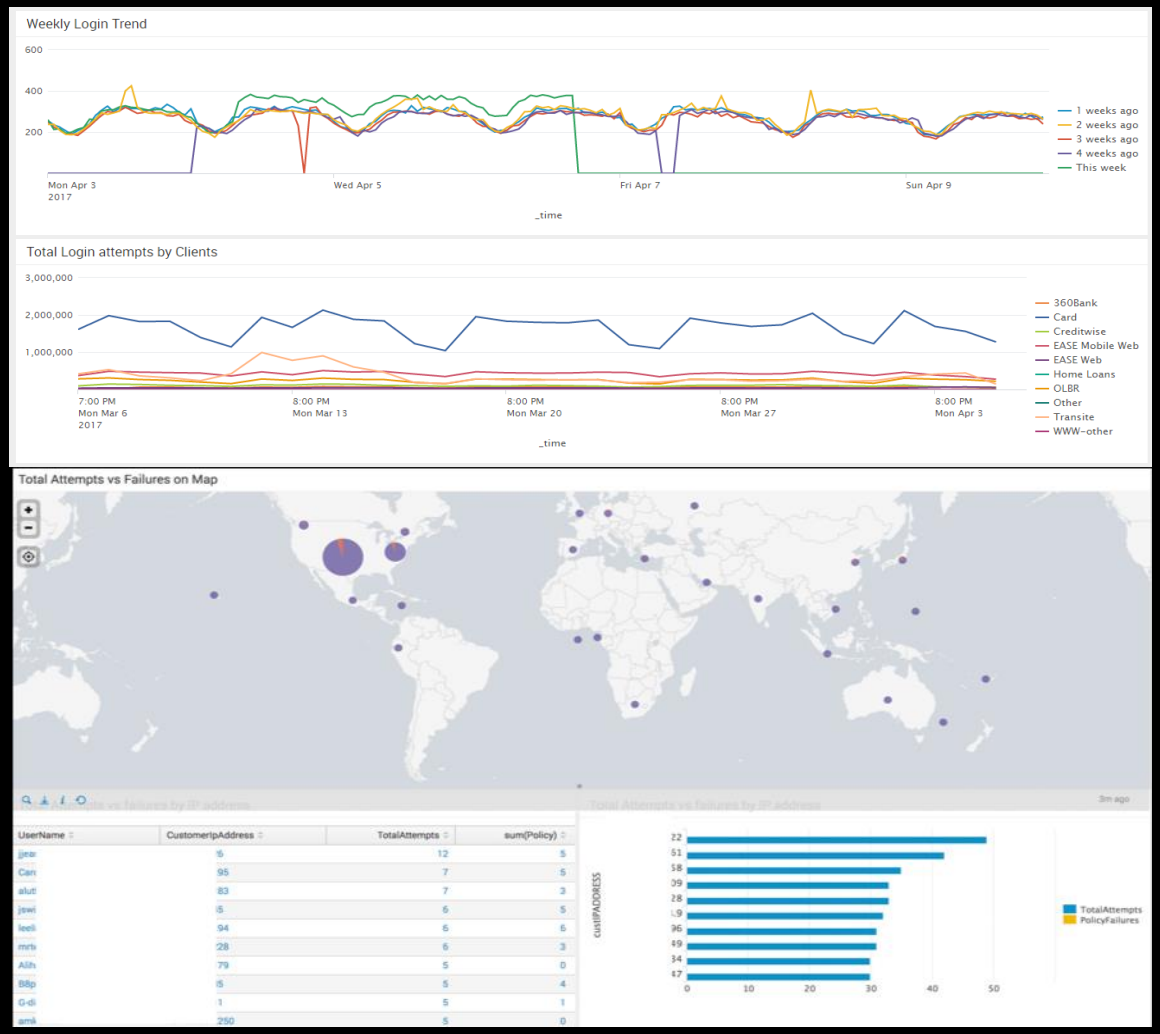
Bird's-eye view of end-to-end business performance (contd.)



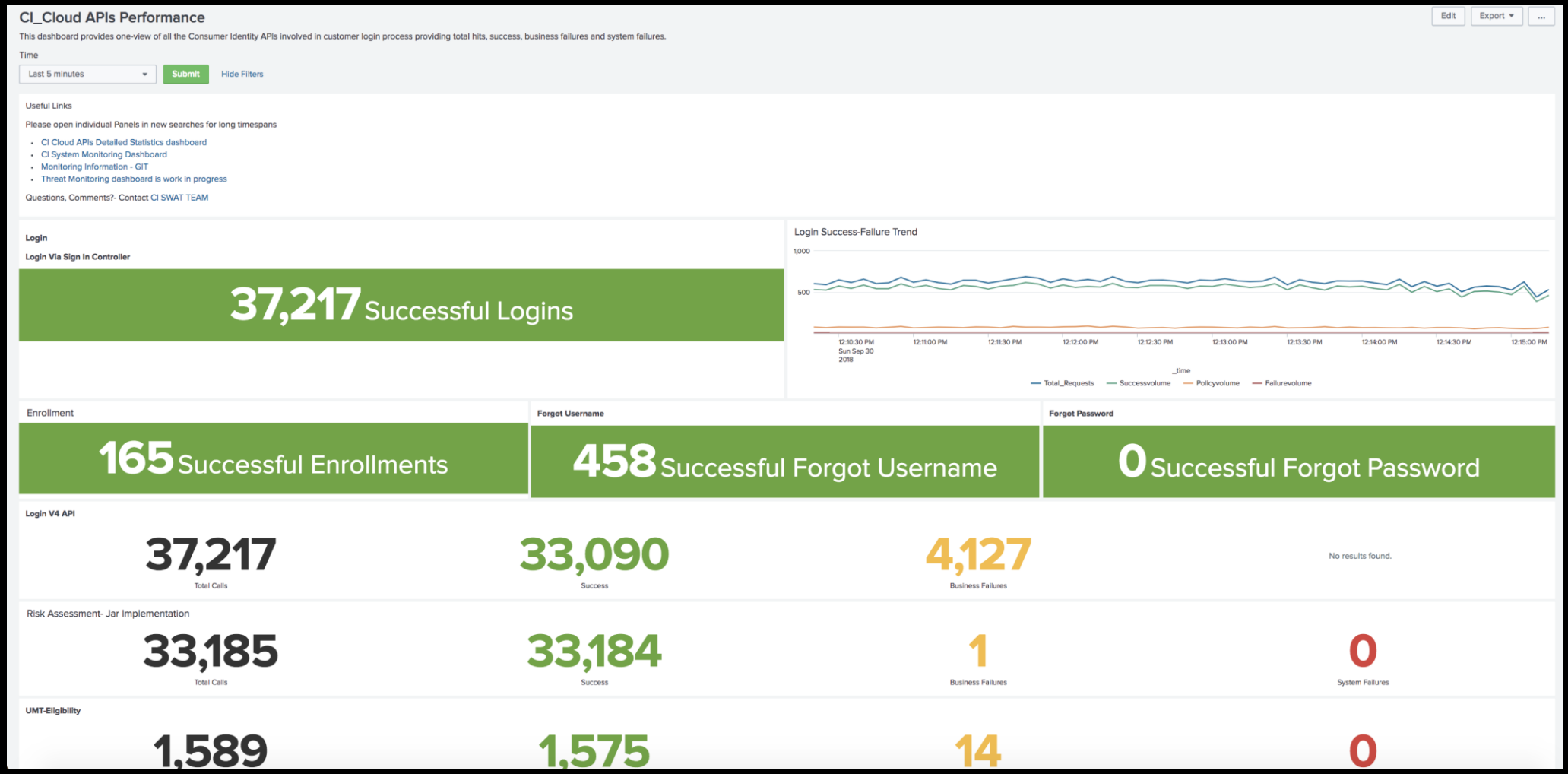
Drill-down view of business performance of one business feature

Business Performance View

Geo View

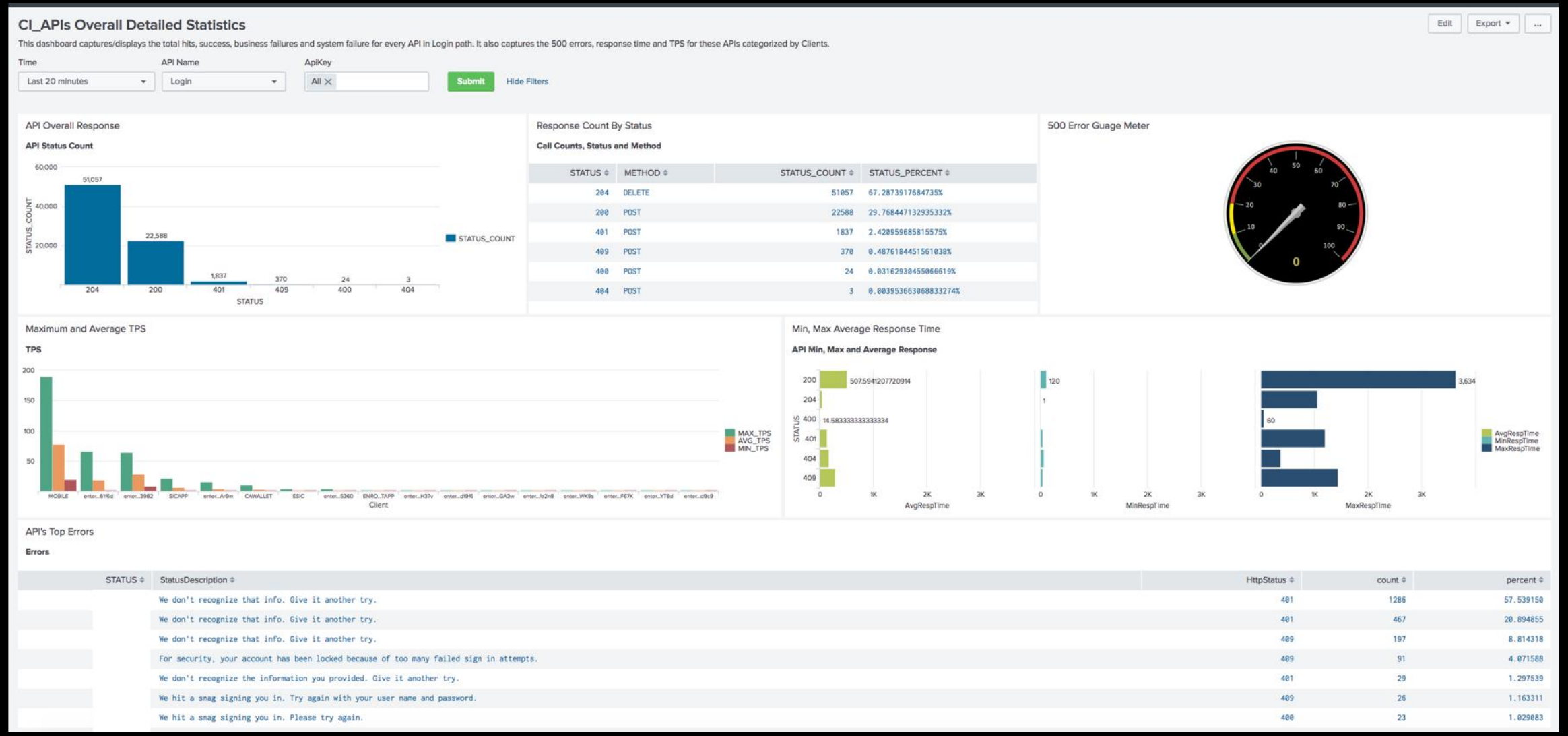


Central API view of all services that make up a business feature



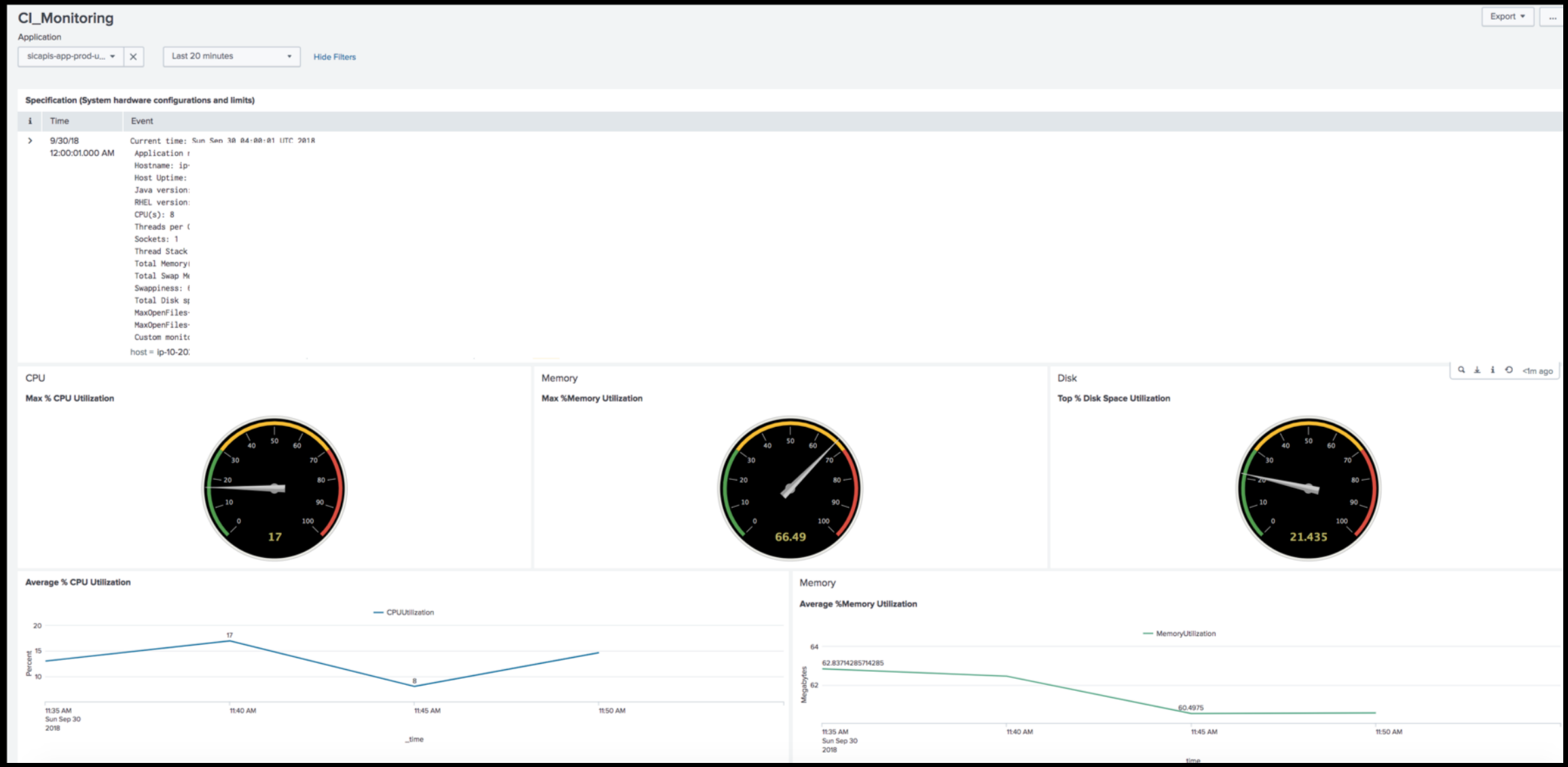
splunk> .conf18

Detailed view of API performance – standardized view



splunk> .conf18

Systems view of an entire stack that hosts a service



Systems view contd.

splunk> .conf18

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

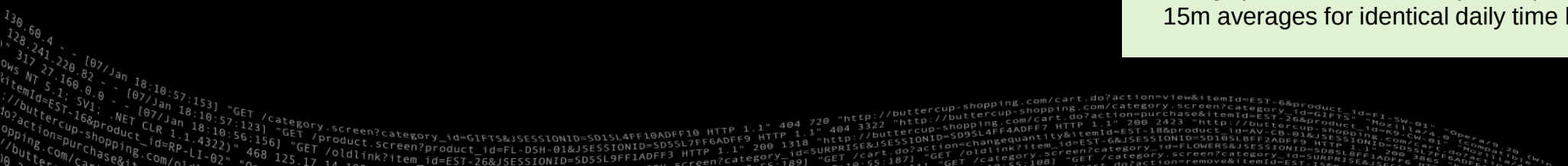
login trend changes through out the day so hard coding did not work

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)))



splunk> .conf18

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