MICHIGAN STATE UNIVERSITY

Project Plan

Detecting Security Threats from User Authentication Patterns

The Capstone Experience

Team Symantec

Stephen Alfa
Keerthana Kolisetty
Robert Novak
Abby Urbanski
Xiaoyo Wu

Department of Computer Science and Engineering
Michigan State University

Spring 2018

From Students…
…to Professionals

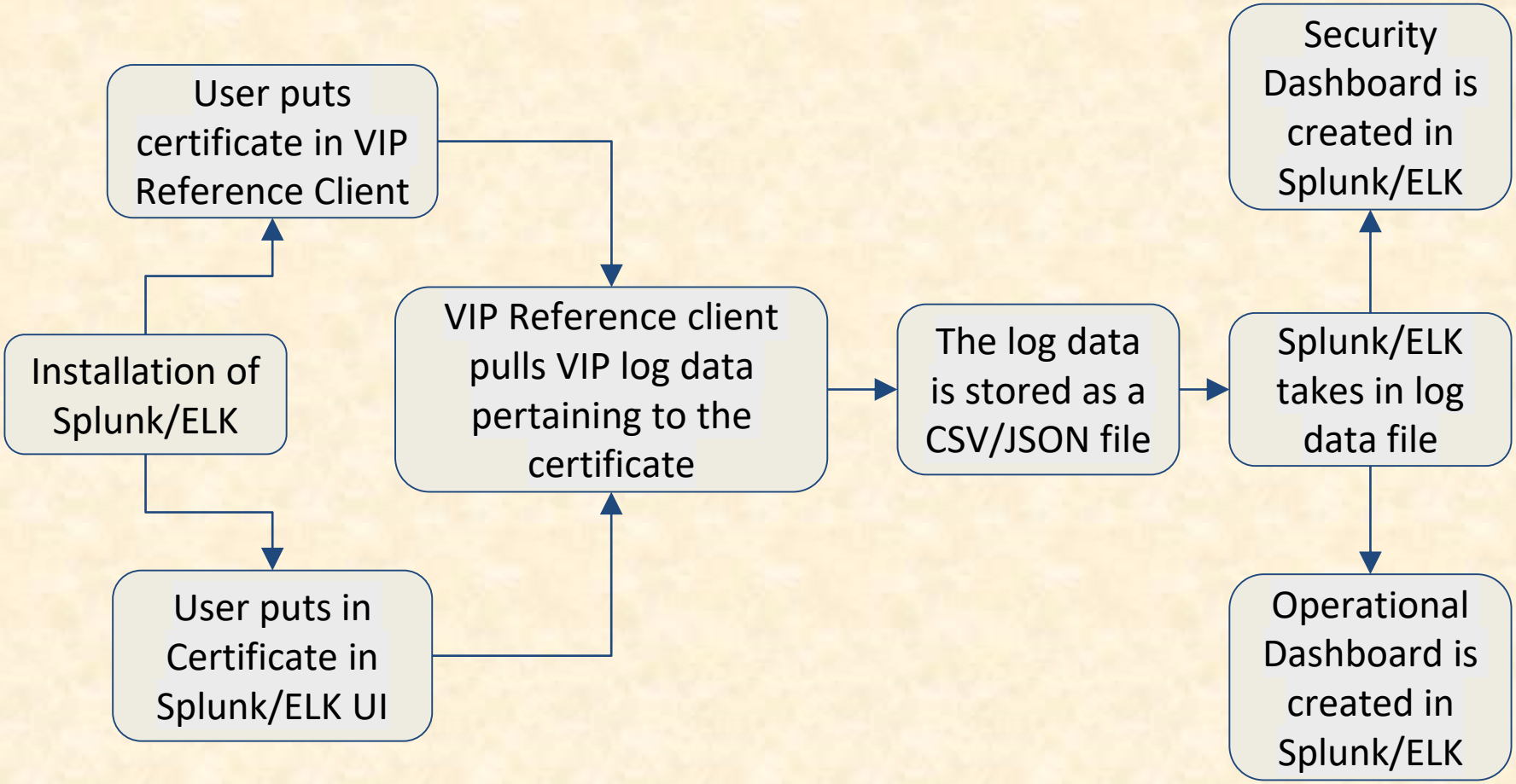
Functional Specifications

- The goal of the project is to provide VIP customers a Splunk add-on and an AWS AMI to visualize various operational and security trend information present in log data and analyze it in near real-time
- Both applications should alert users when suspicious or malicious activity is detected
- Launching and deployment of both of those applications should be frictionless

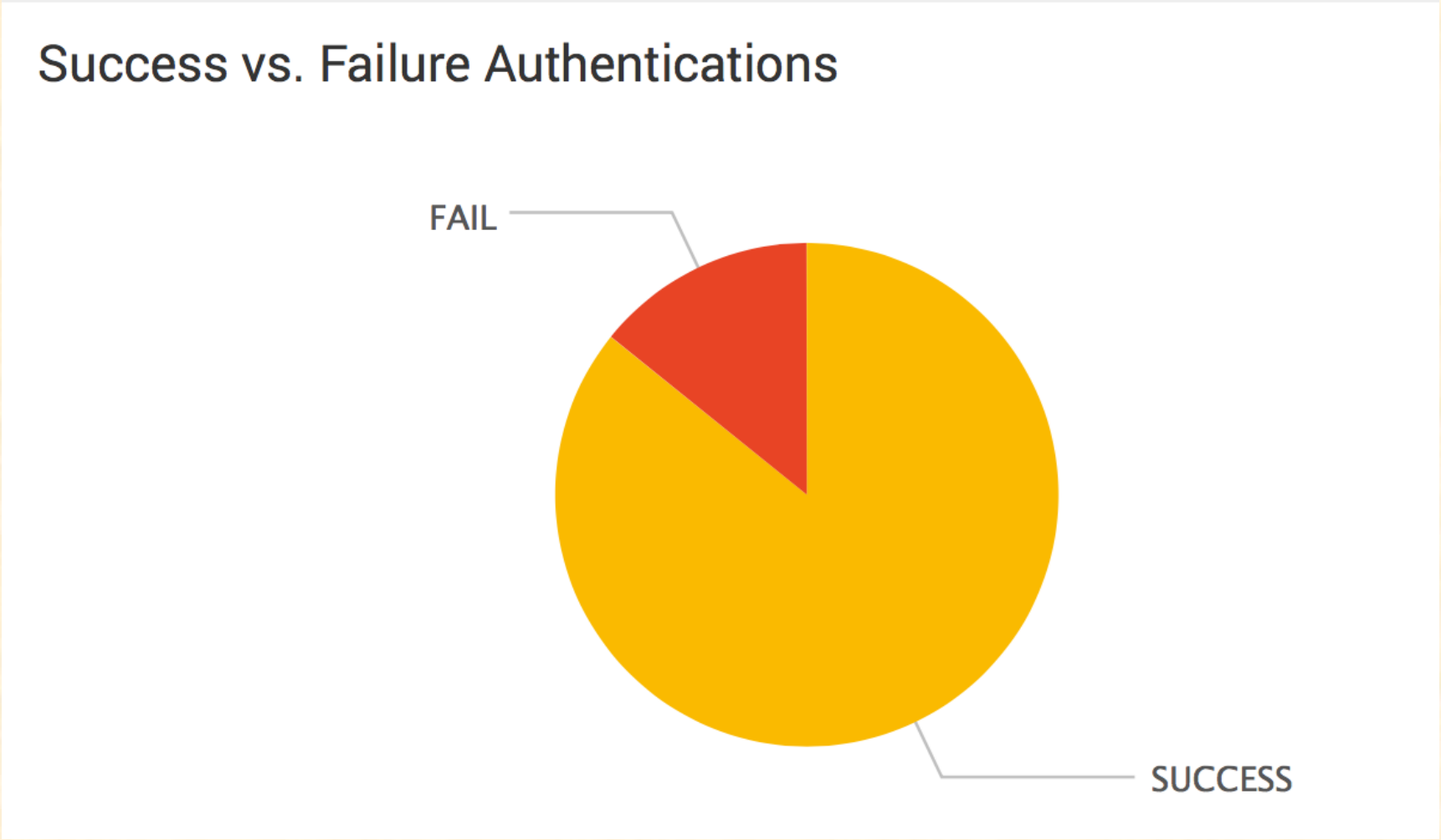
Design Specifications

- Create easy to read graphs and charts to represent authentication data
  - Successful vs Failed
  - Device Types
  - Authentications over time
- Create premade graphics and searches and allow users to choose which ones to display.
- Highlight patterns that could reveal suspicious or malicious activity

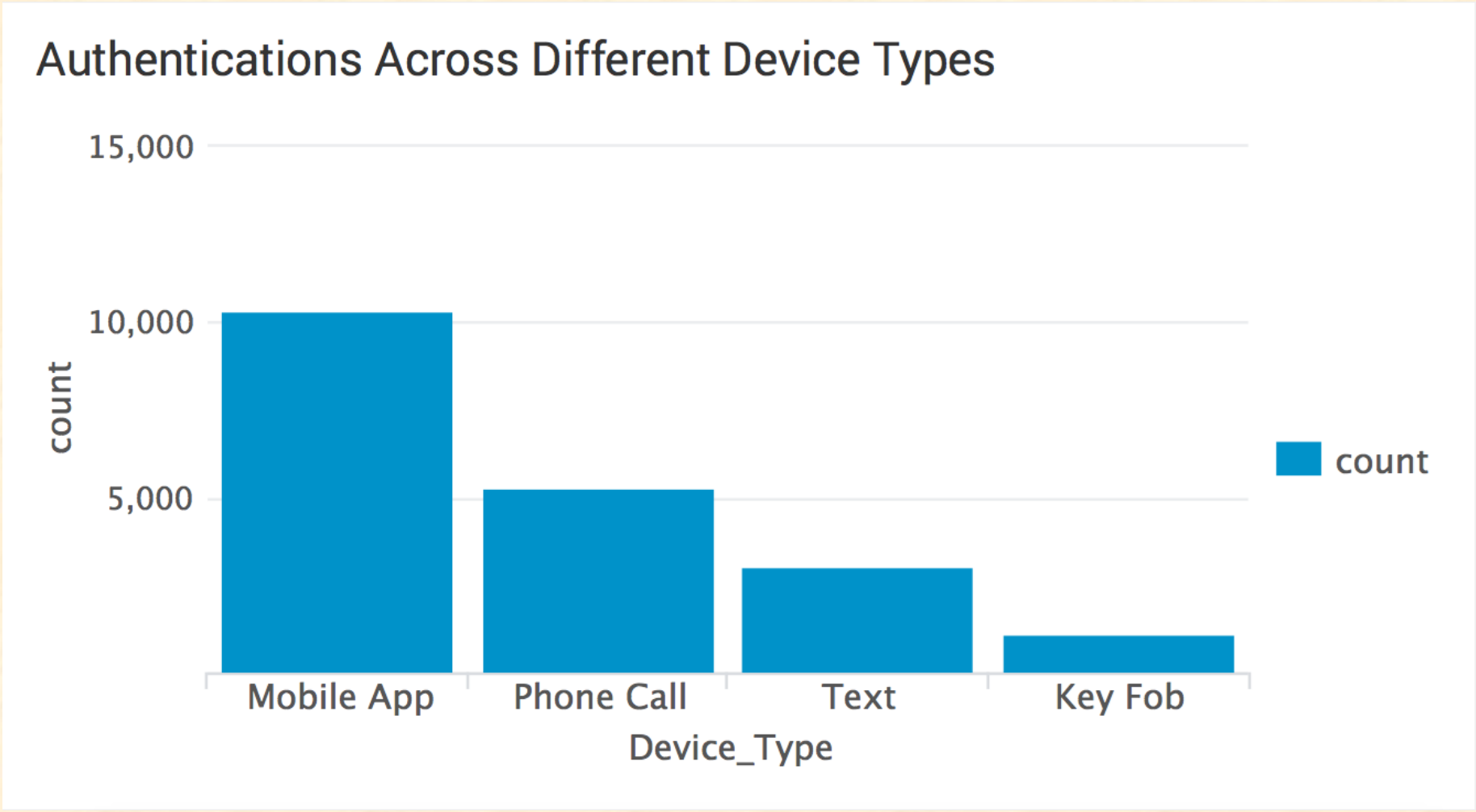
Process Flow



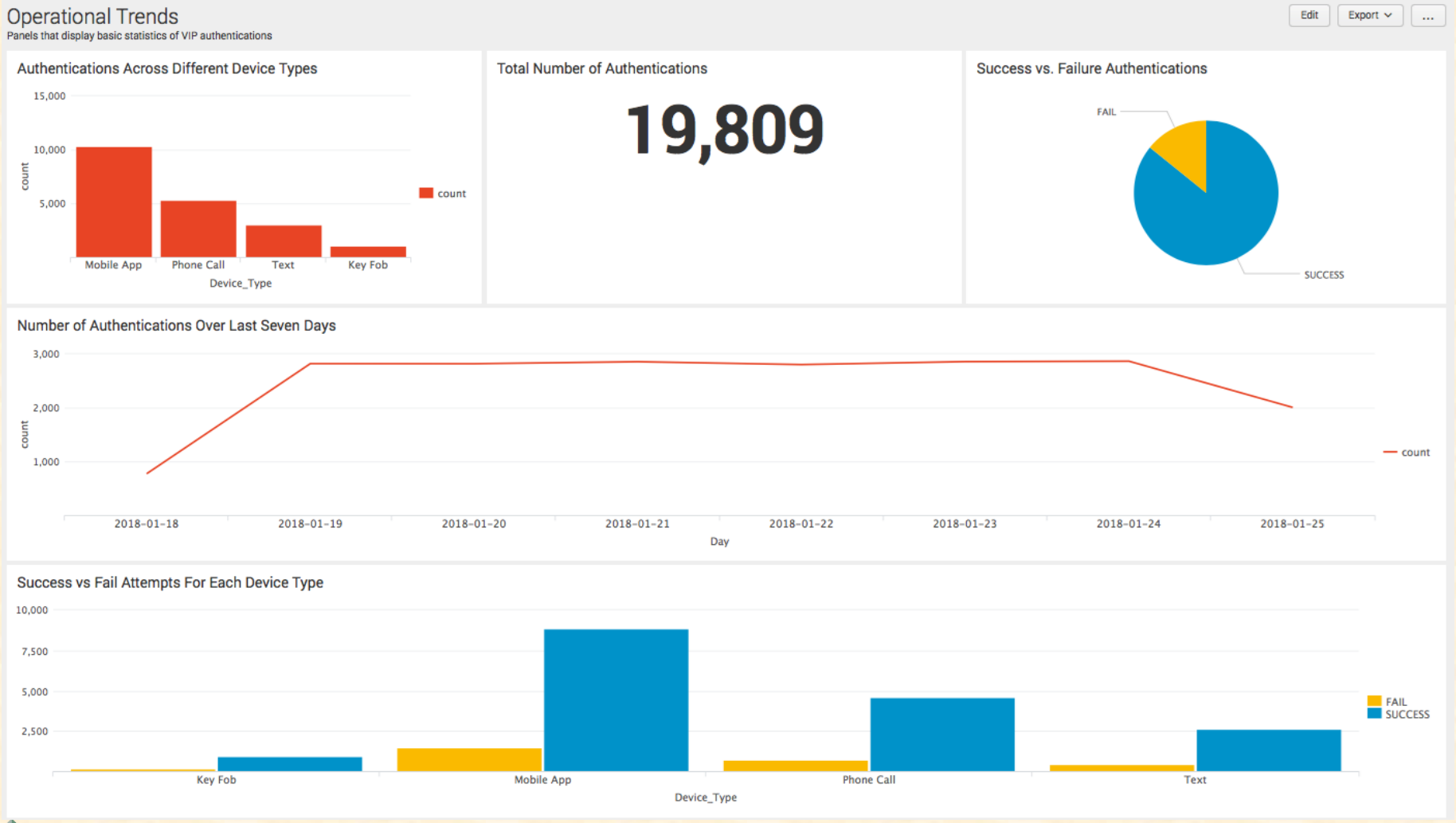
Screen Mockup: Pie Chart Panel



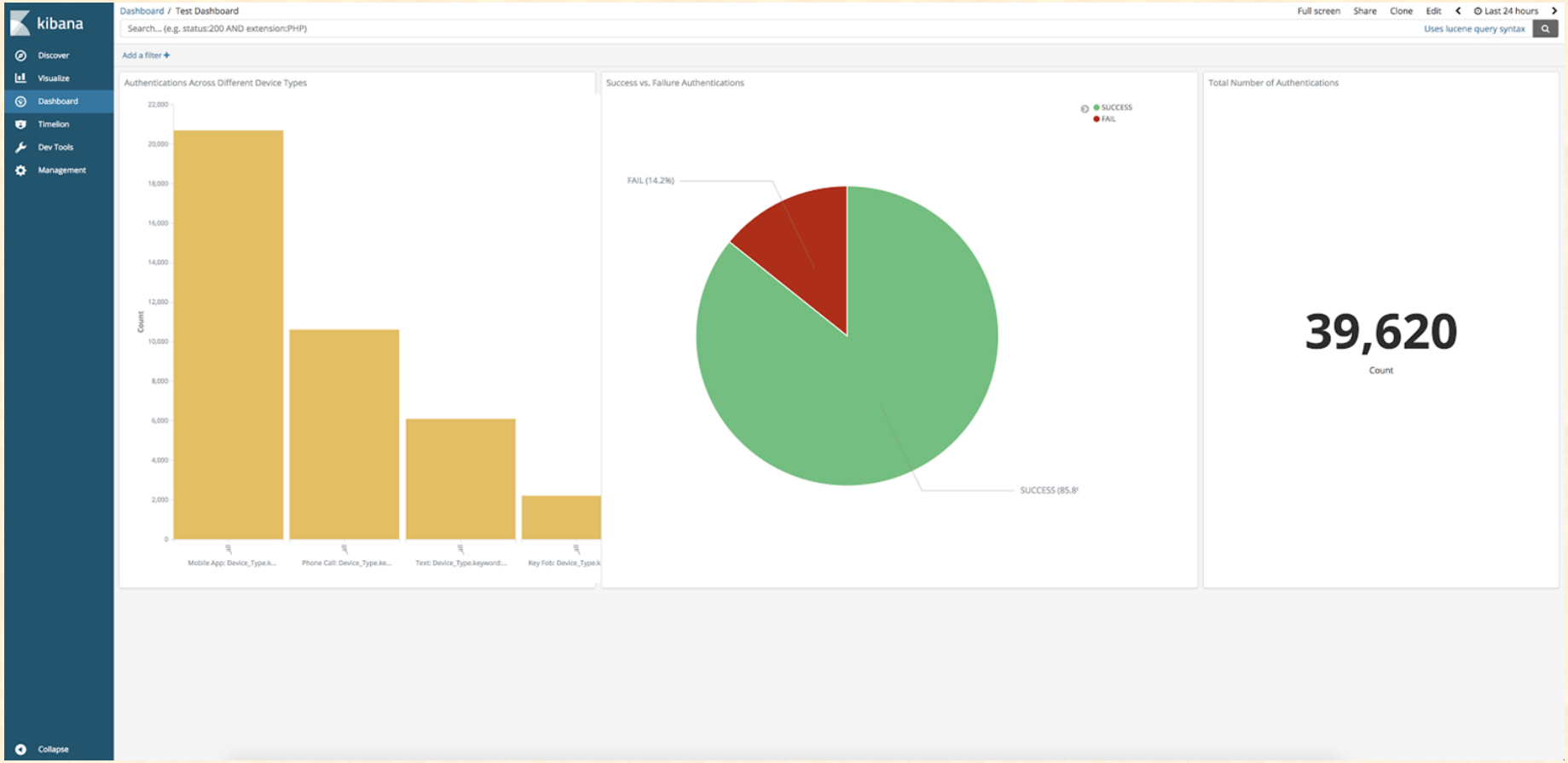
Screen Mockup: Bar Graph Panel



Screen Mockup: Dashboard in Splunk



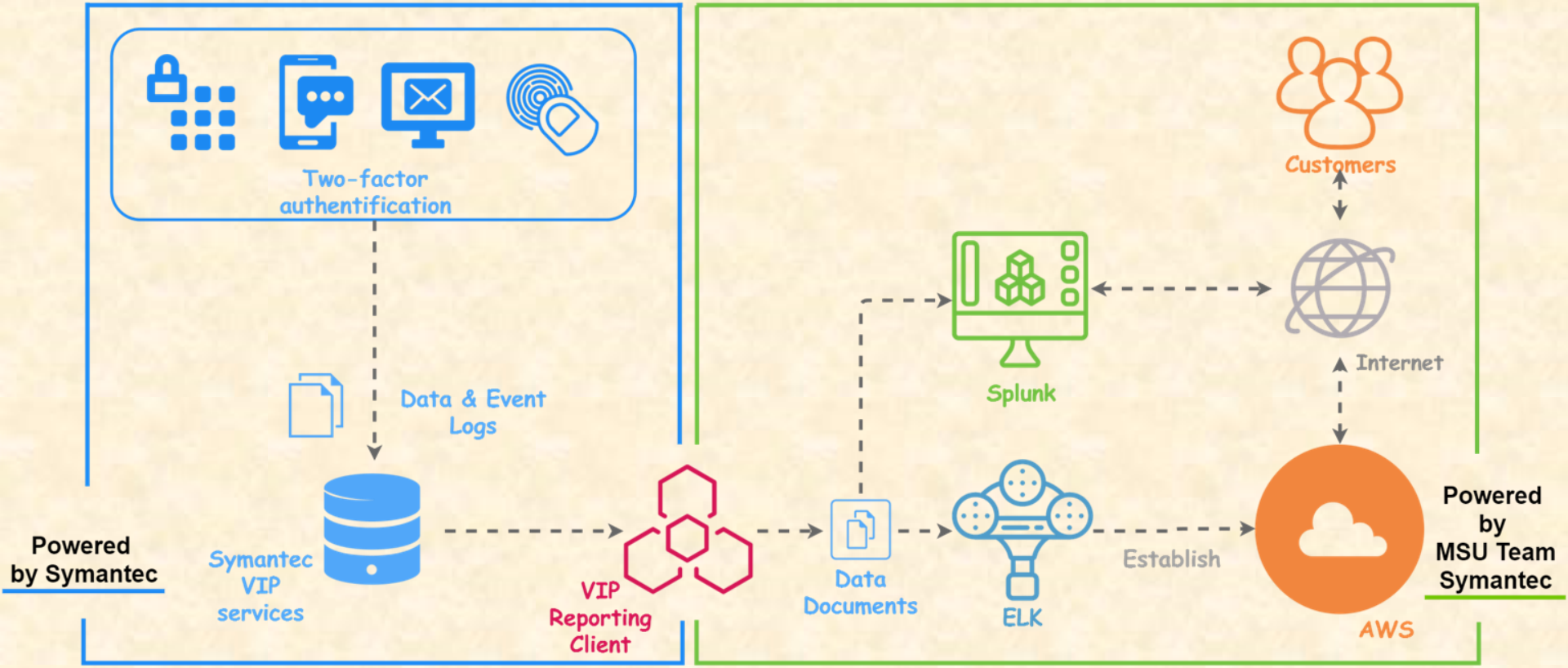
Screen Mockup: Dashboard in ELK



Technical Specifications

- SOAP (Simple Object Access Protocol) API
- Java
- VIP Reporting Service Client (REST API)
- JavaScript, HTML
- SPL (Search Processing Language)

System Architecture



System Components

- Hardware Platforms
  - Amazon Web Services
    - Amazon Machine Images
  - Software Platforms / Technologies
  - Splunk
  - Elasticsearch, Logstash, Kibana (ELK)

Risks

Risks

- Ability to Detect suspicious patterns
  - There is a wide range of threats to detect and want to avoid false flags
  - Consult with experienced security advisor and identify possible threats
- Test Data
  - Real VIP data is necessary to identify accurate threat patterns
  - Get MSU's VIP data
- Consistency between Splunk and ELK
  - Making sure that functionality is consistent between both platforms
  - Develop both applications concurrently
- AWS Servers
  - The possibility of deploying the ELK applications on the AWS server
  - Use AWS documentation and use online resources

Questions?