MICHIGAN STATE
UNIVERSITY

Beta Presentation
Detecting Security Threats from User Patterns

The Capstone Experience

Team Symantec

Stephen Alfa
Keerthana Kolisetty
Robert Novak
Abby Urbanski
Xiaoyu Wu

Department of Computer Science and Engineering
Michigan State University

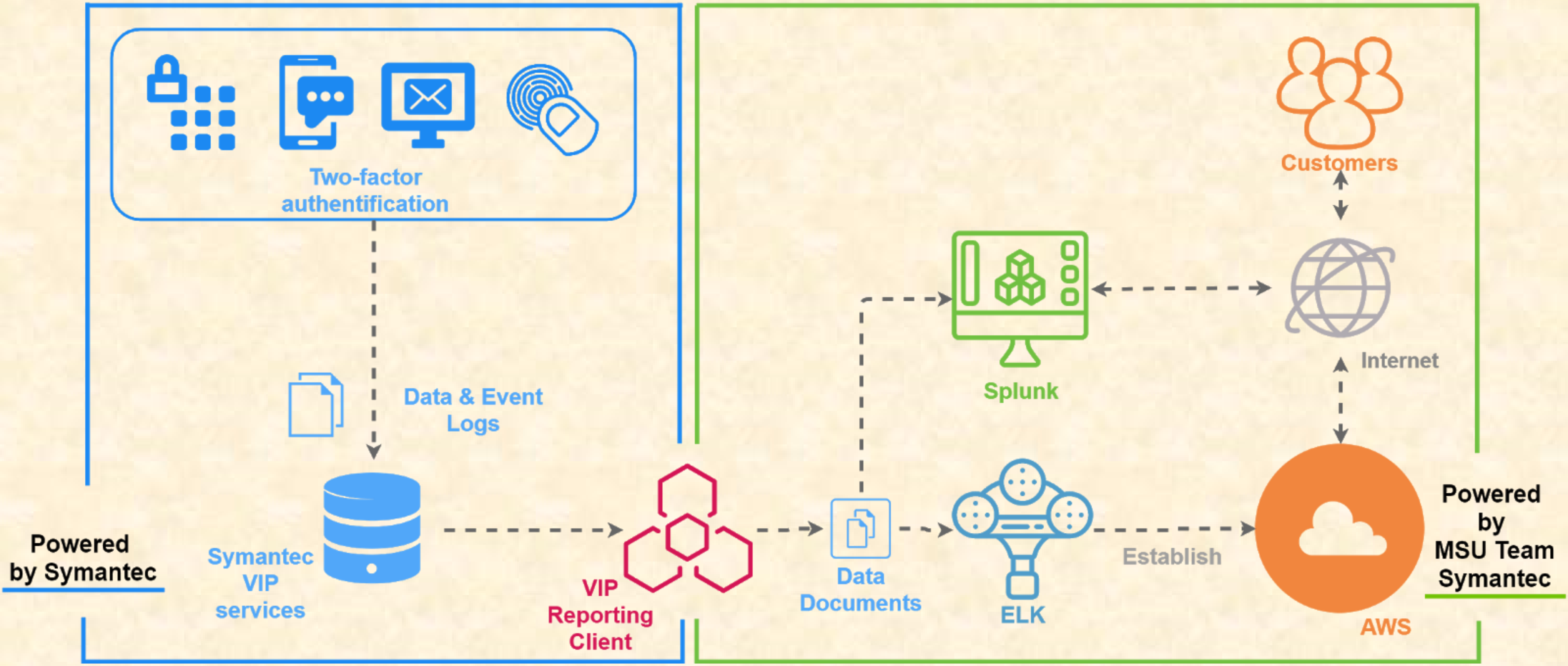
Spring 2018

From Students…
…to Professionals

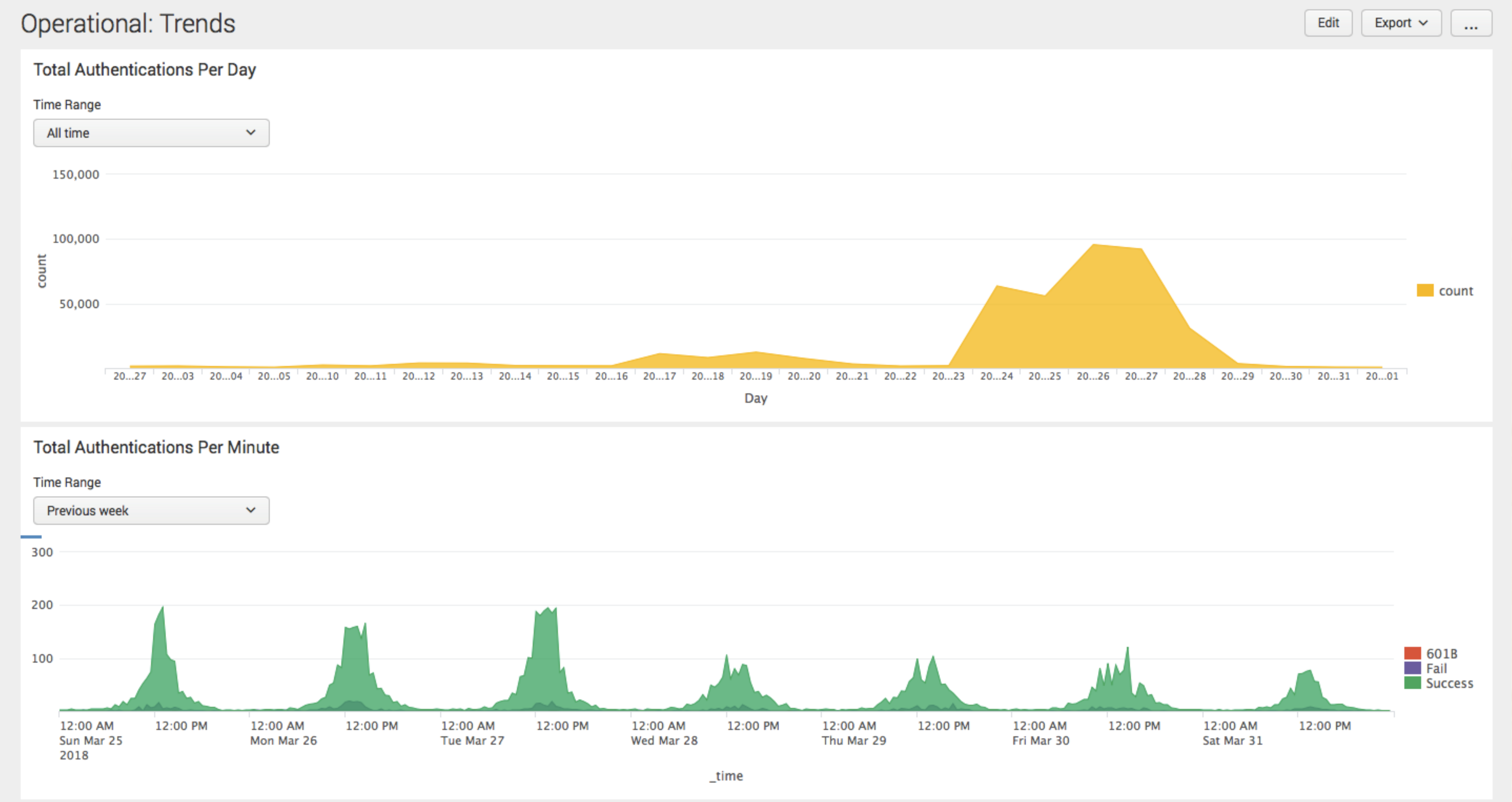
Project Overview

- The goal of the project is to provide VIP customers a Splunk add-on and an ELK application on 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

System Architecture



Splunk: Operation Trends Dashboard



Operational: Trends

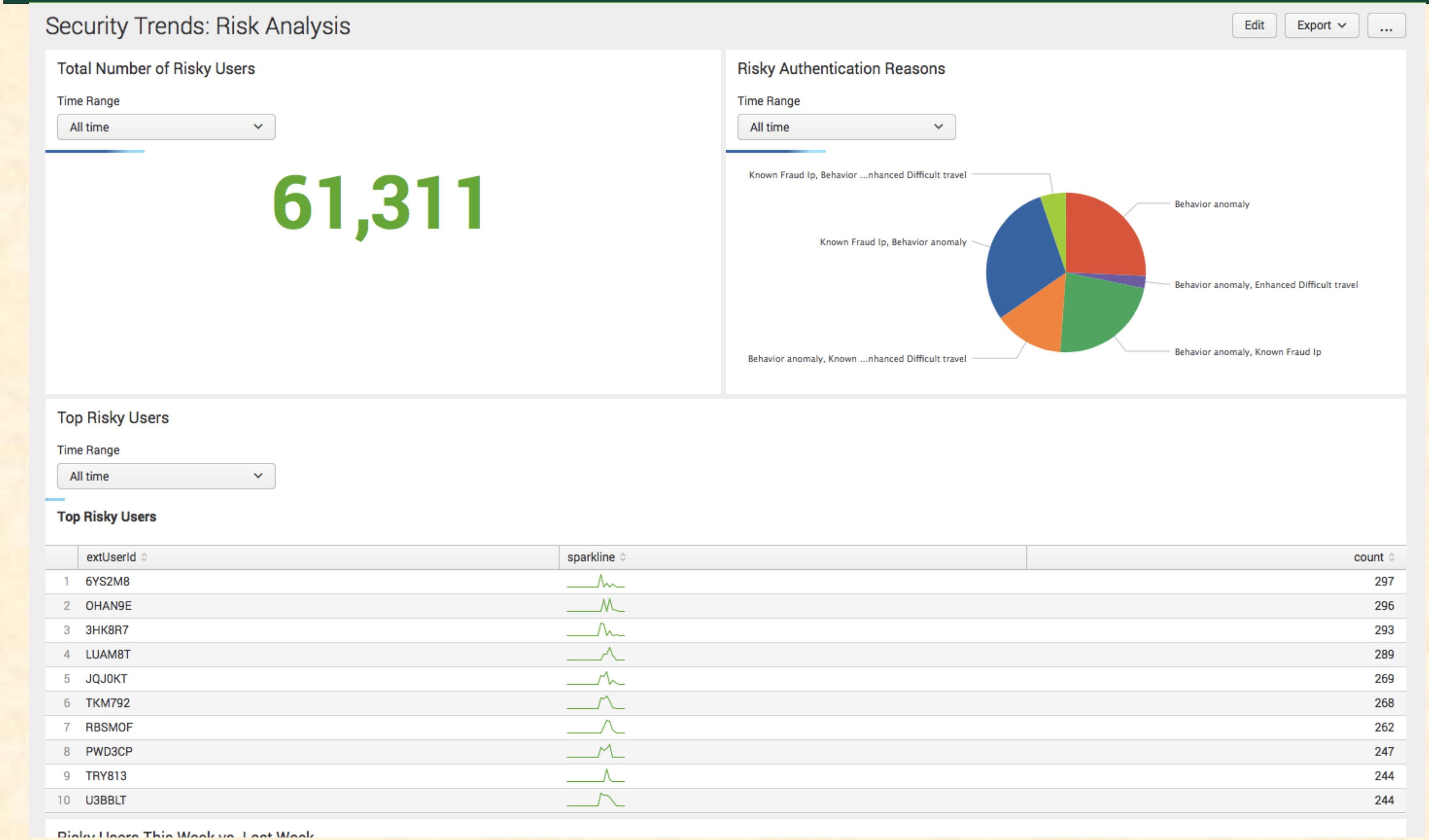
Total Authentications Per Day

Time Range: All time

Total Authentications Per Minute

Time Range: Previous week

Splunk: Risk Analysis Dashboard



Security Trends: Risk Analysis

Total Number of Risky Users

Time Range: All time

61,311

Risky Authentication Reasons

Time Range: All time

Known Fraud Ip, Behavior ...nhanced Difficult travel
Behavior anomaly
Known Fraud Ip, Behavior anomaly
Behavior anomaly, Enhanced Difficult travel
Behavior anomaly, Known Fraud Ip
Behavior anomaly, Known ...nhanced Difficult travel

Top Risky Users

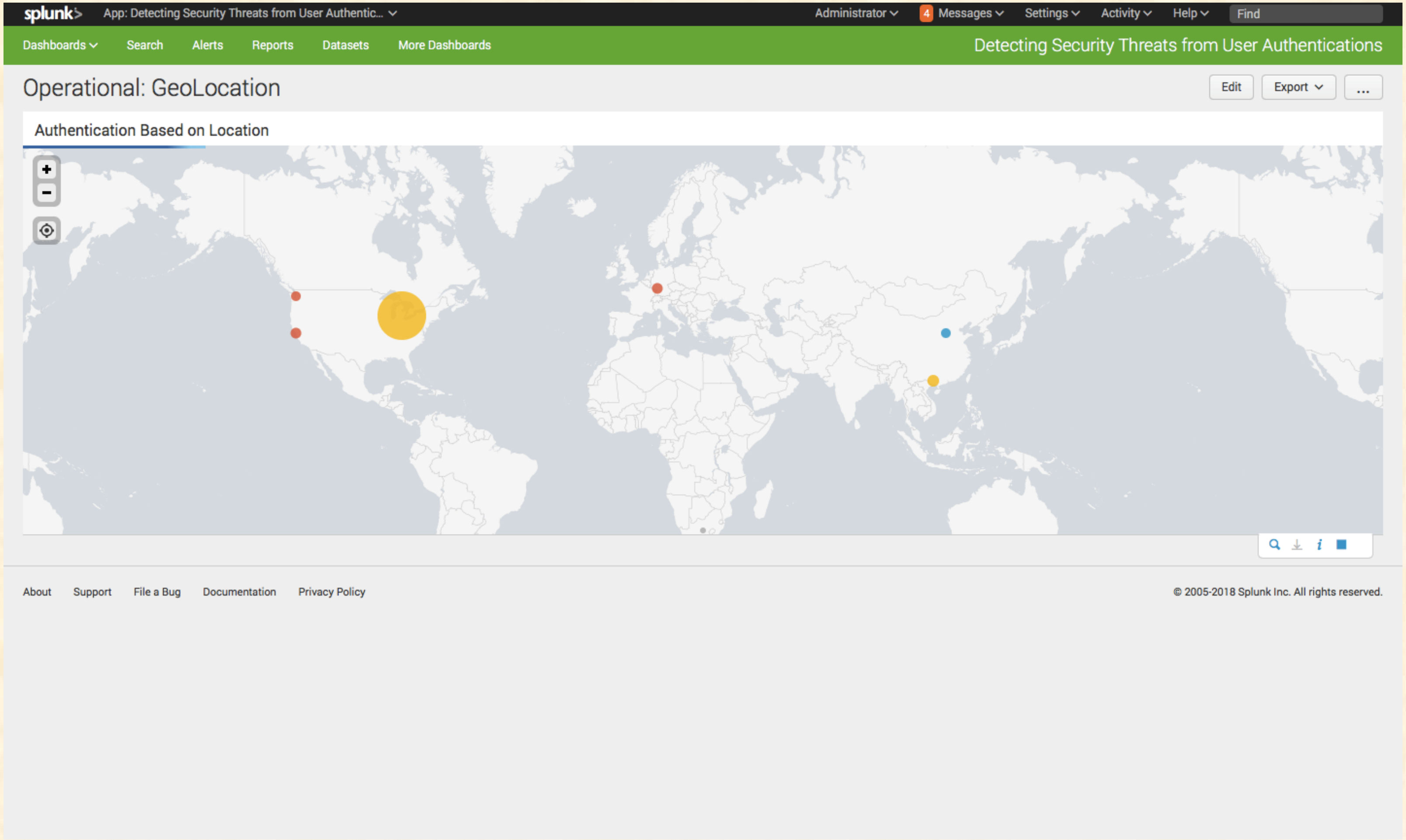
Time Range: All time

Top Risky Users

	extUserId	sparkline	count
1	6YS2M8		297
2	OHAN9E		296
3	3HK8R7		293
4	LUAM8T		289
5	JQJ0KT		269
6	TKM792		268
7	RBSMOF		262
8	PWD3CP		247
9	TRY813		244
10	U3BBLT		244

Risky Users This Week vs. Last Week

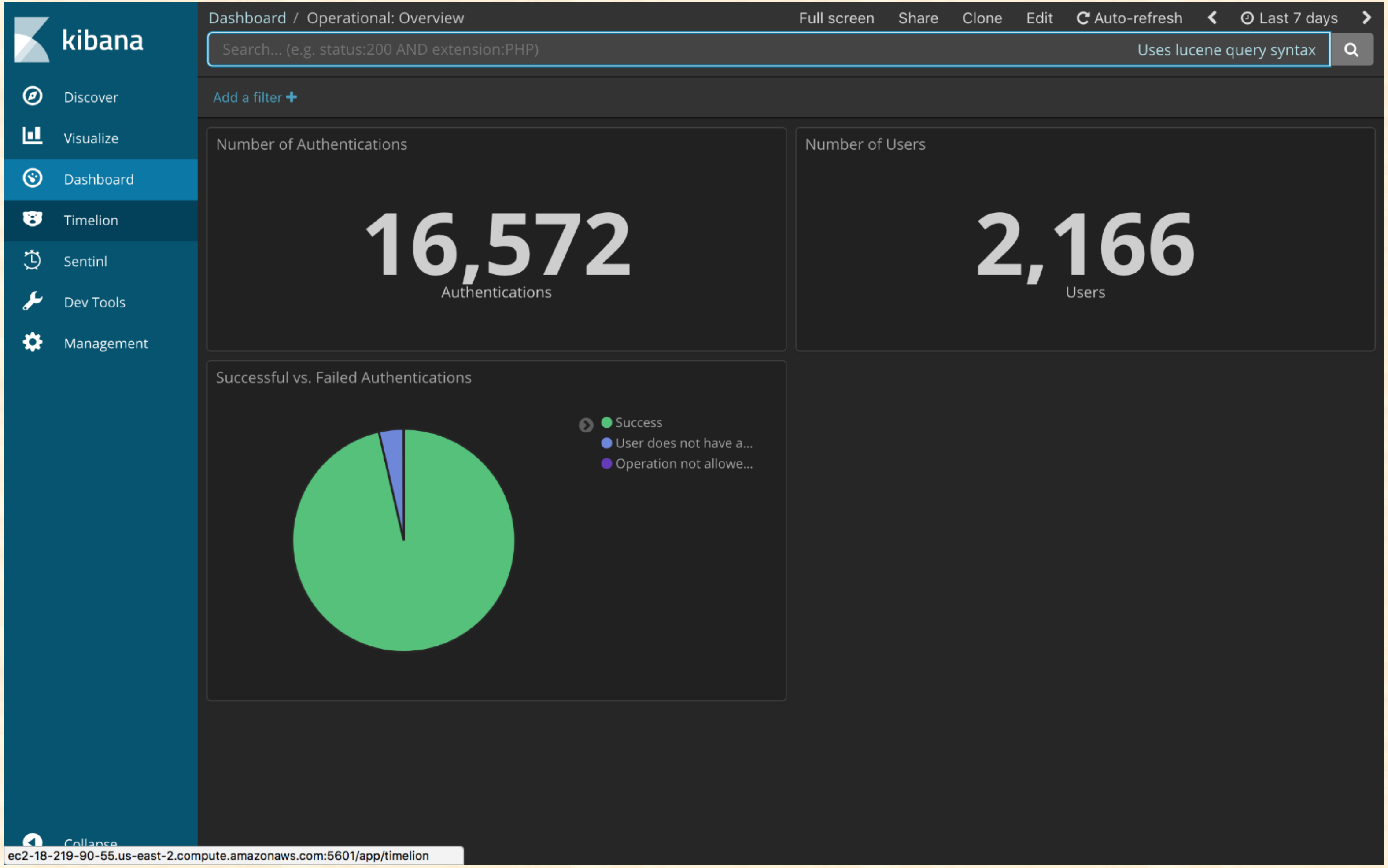
Splunk: Geolocation Dashboard



Operational: GeoLocation

Authentication Based on Location

ELK: Operational Oveview Dashboard



kibana
Discover
Visualize
Dashboard
Timelion
Sentinl
Dev Tools
Management
Collapse
Dashboard / Operational: Overview
Full screen
Share
Clone
Edit
Auto-refresh
Last 7 days
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
ec2-18-219-90-55.us-east-2.compute.amazonaws.com:5601/app/timelion

Number of Authentications

16,572
Authentications

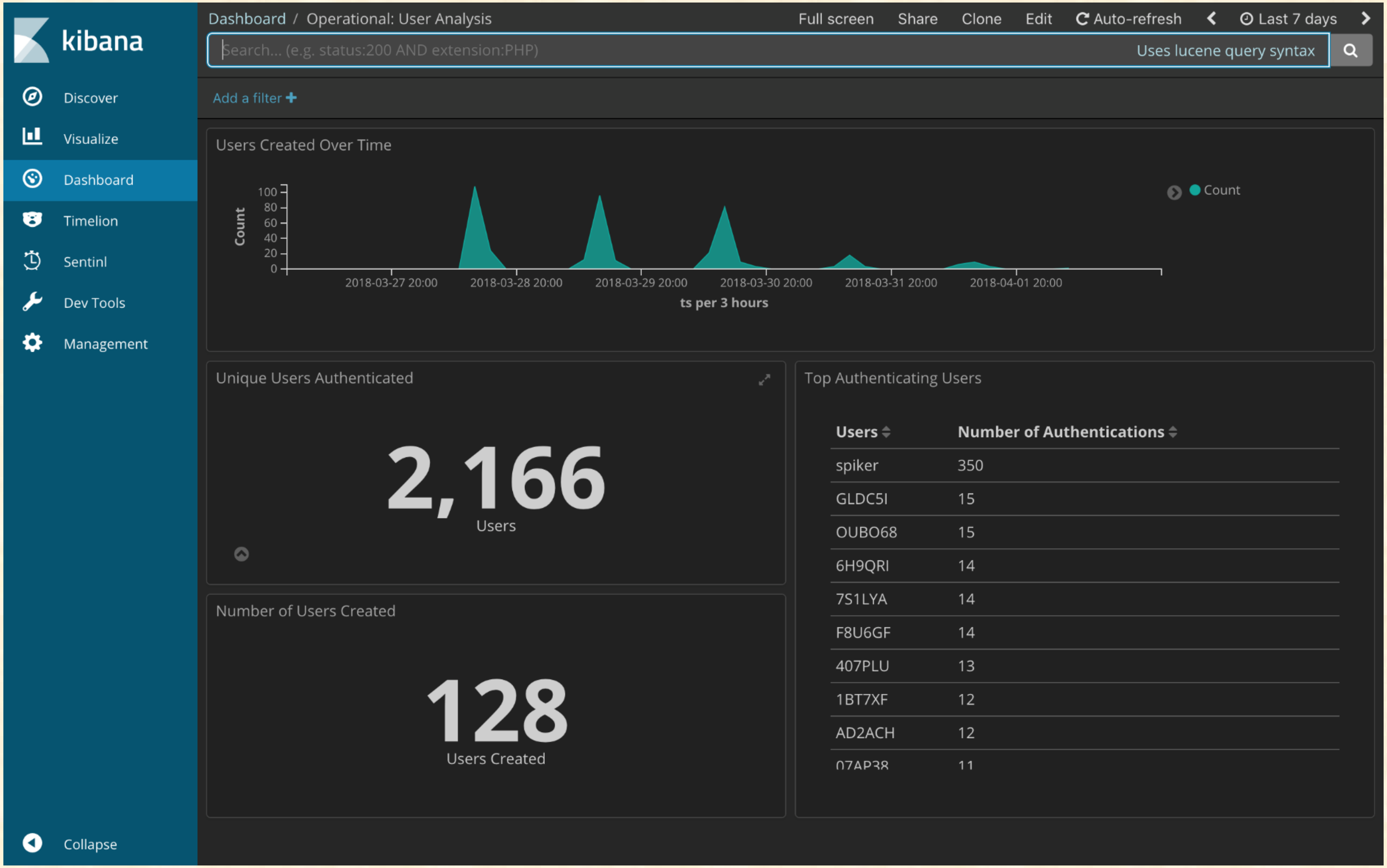
Number of Users

2,166
Users

Successful vs. Failed Authentications

● Success
● User does not have a...
● Operation not allowe...

ELK: Operational User Analysis Dashboard



Unique Users Authenticated

2,166

Users

Number of Users Created

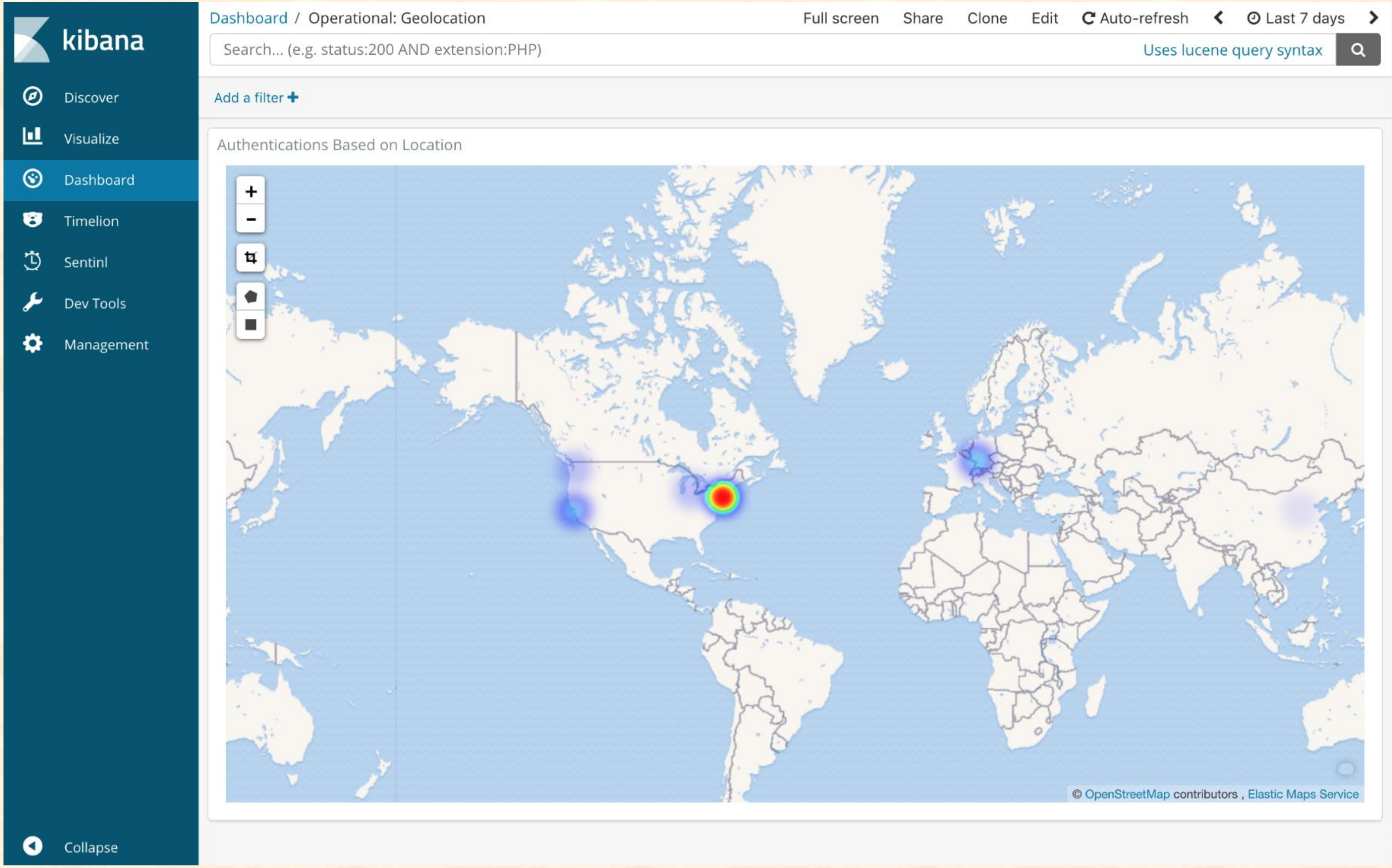
128

Users Created

Top Authenticating Users

Users	Number of Authentications
spiker	350
GLDC5I	15
OUBO68	15
6H9QRI	14
7S1LYA	14
F8U6GF	14
407PLU	13
1BT7XF	12
AD2ACH	12
07AP38	11

ELK: Geolocation Dashboard



Authentications Based on Location

What’s left to do?

- Adding any additional pre-built panels
- Clean up Splunk UI
- Packaging the applications

Questions?

? ? ? ?

? ? ?

? ?