MICHIGAN STATE
UNIVERSITY

Alpha Presentation
Detecting Security Threats from User Authentication 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

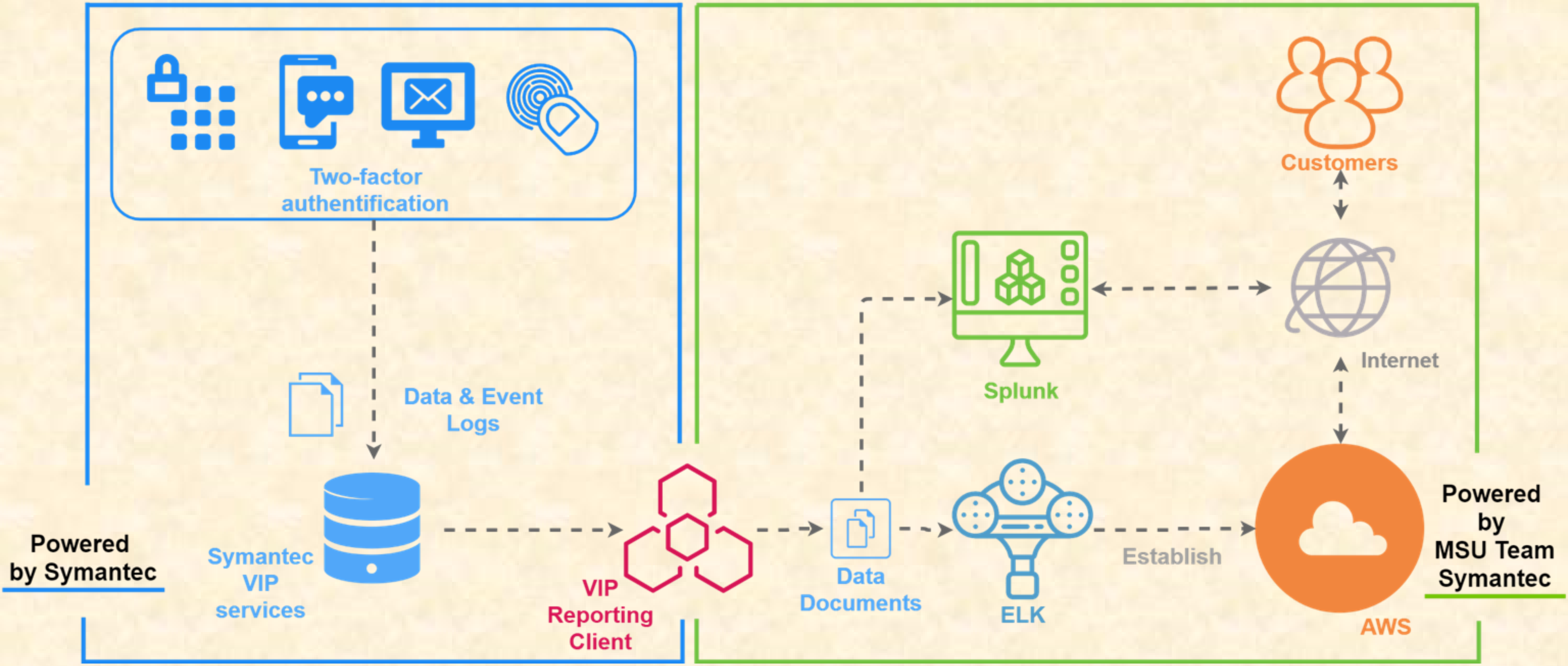
Spring 2018

From Students…
…to Professionals

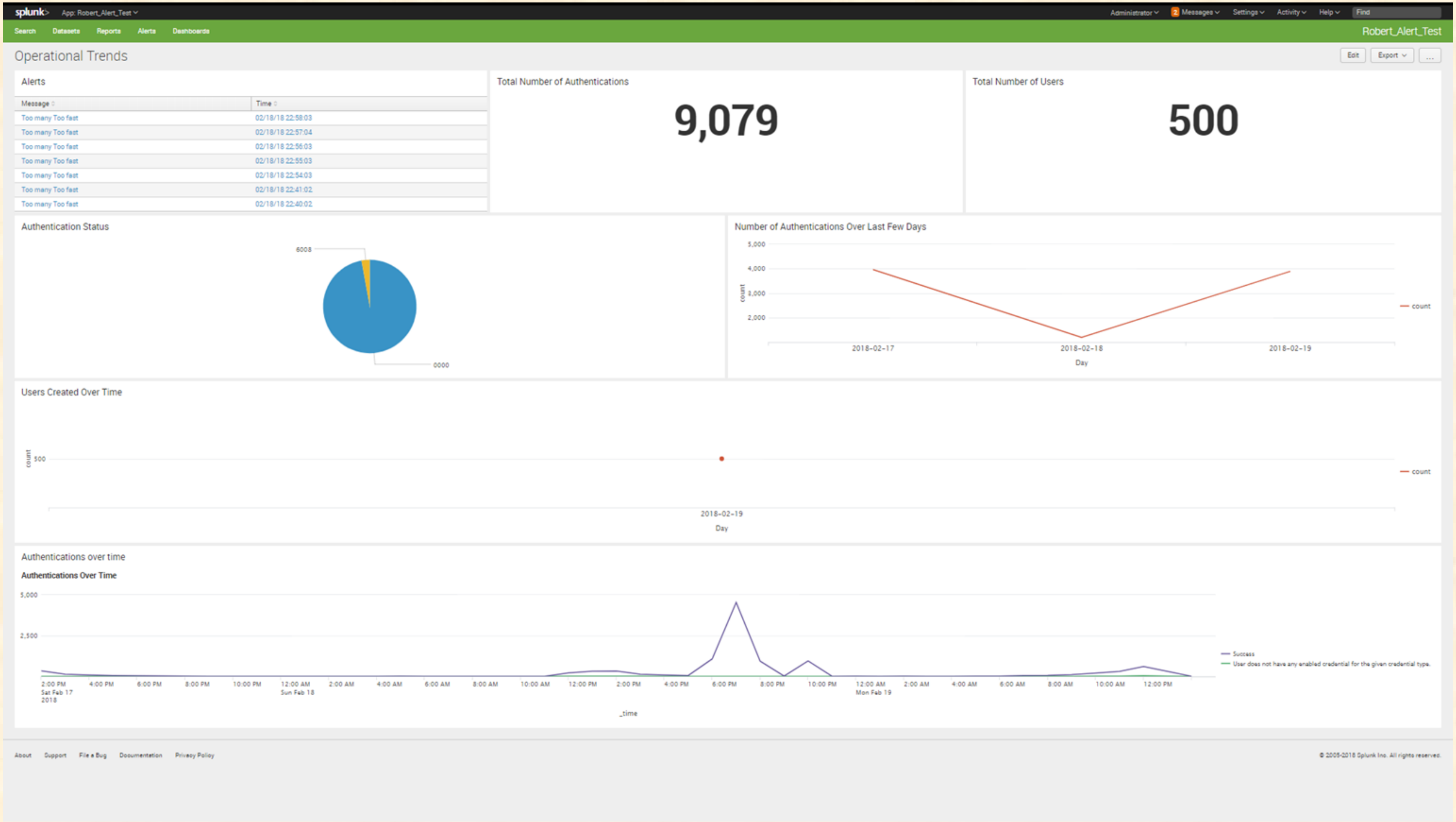
Project Overview

- 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 Dashboard



Operational Trends

Alerts

Message	Time
Too many Too fast	02/18/18 22:58:03
Too many Too fast	02/18/18 22:57:04
Too many Too fast	02/18/18 22:56:03
Too many Too fast	02/18/18 22:55:03
Too many Too fast	02/18/18 22:54:03
Too many Too fast	02/18/18 22:41:02
Too many Too fast	02/18/18 22:40:02

Total Number of Authentications

9,079

Total Number of Users

500

Authentication Status

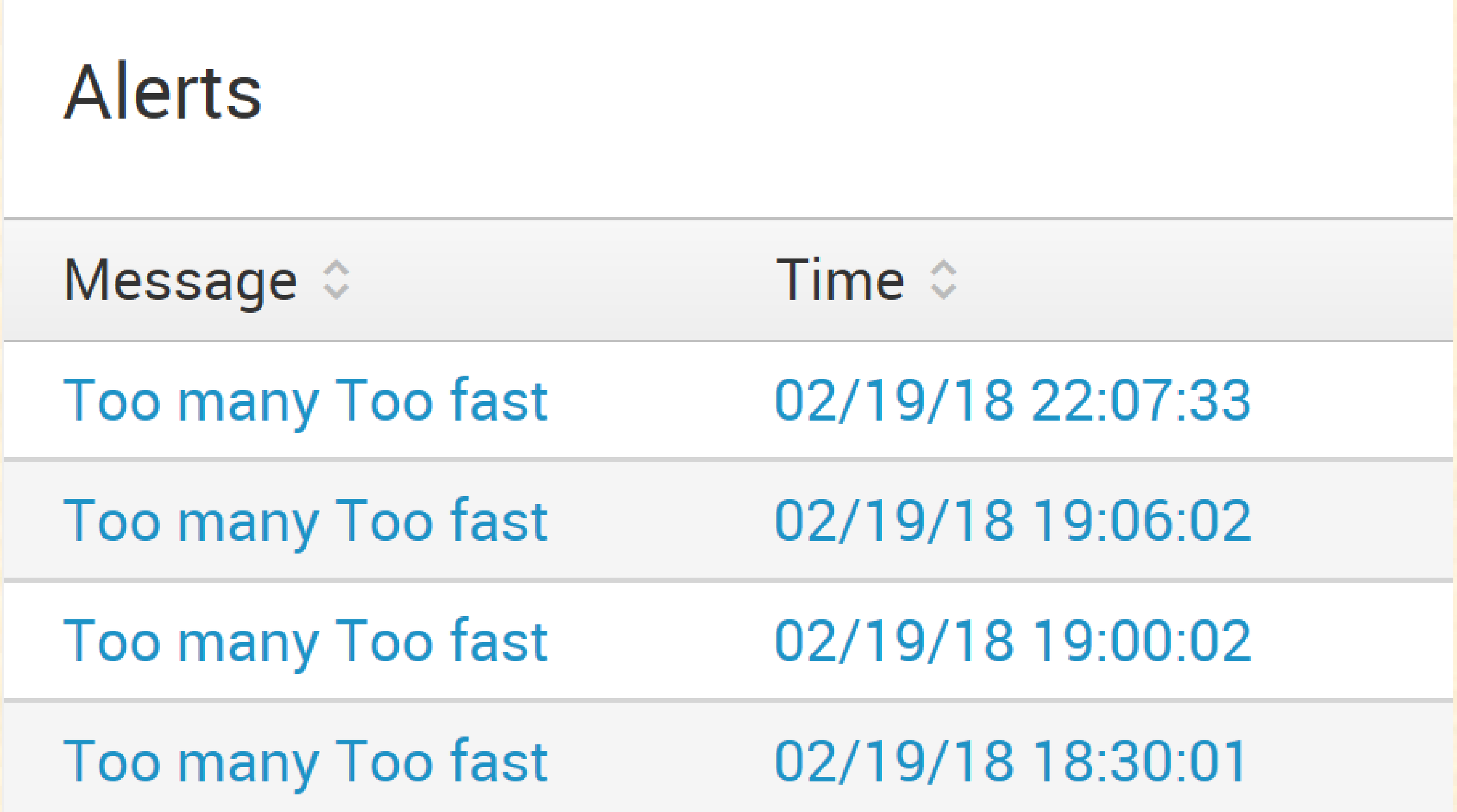
Number of Authentications Over Last Few Days

Users Created Over Time

Authentications over time

Authentications Over Time

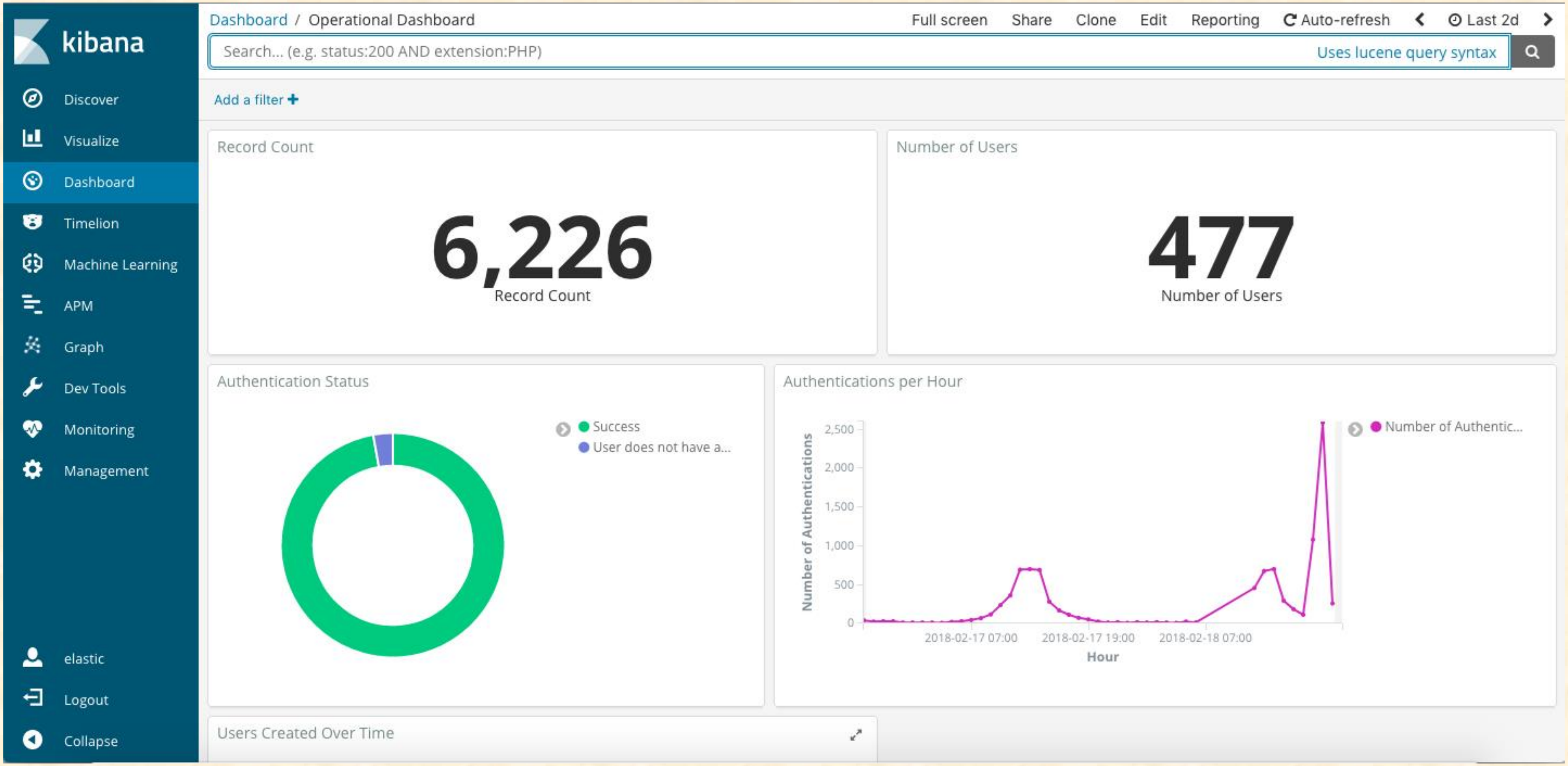
Splunk Alerting Panel



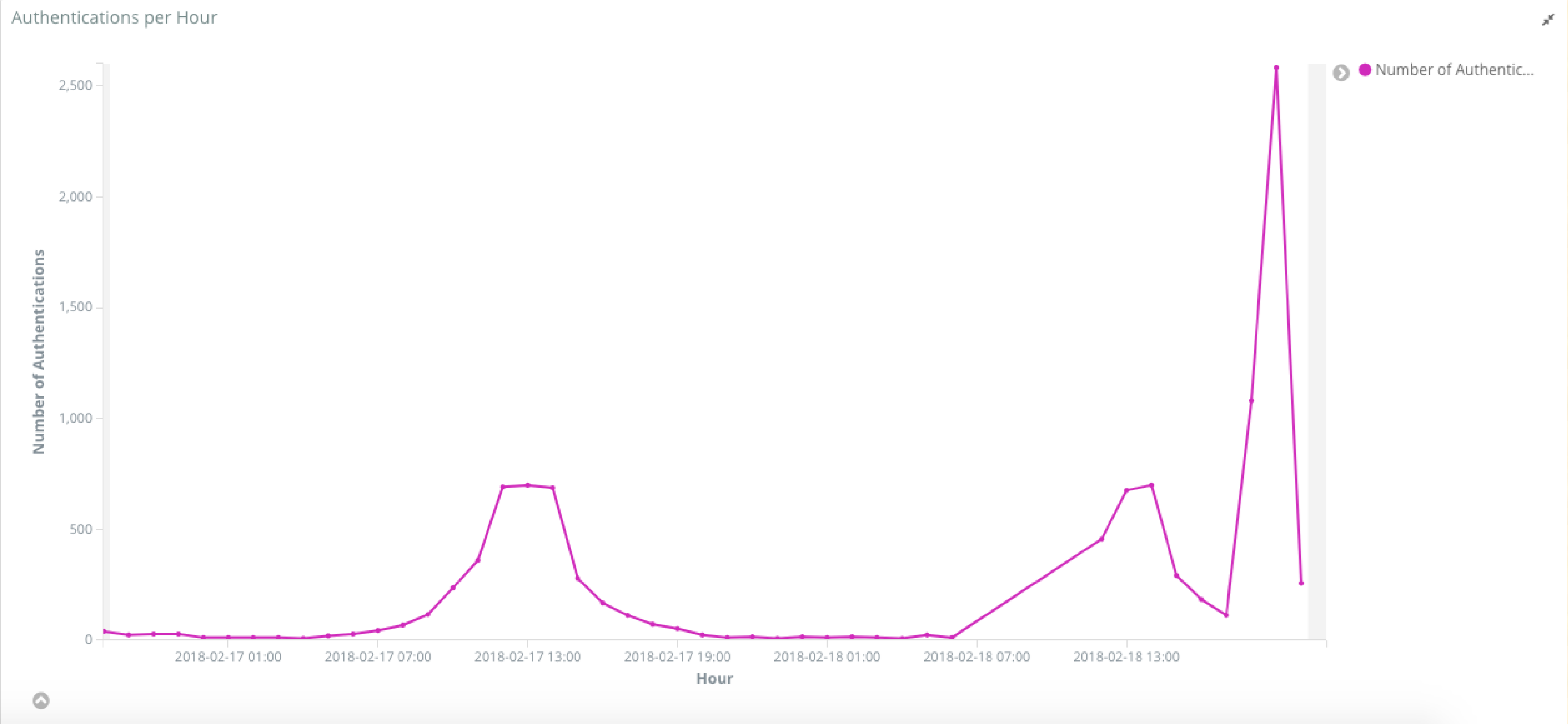
Alerts

Message	Time
Too many Too fast	02/19/18 22:07:33
Too many Too fast	02/19/18 19:06:02
Too many Too fast	02/19/18 19:00:02
Too many Too fast	02/19/18 18:30:01

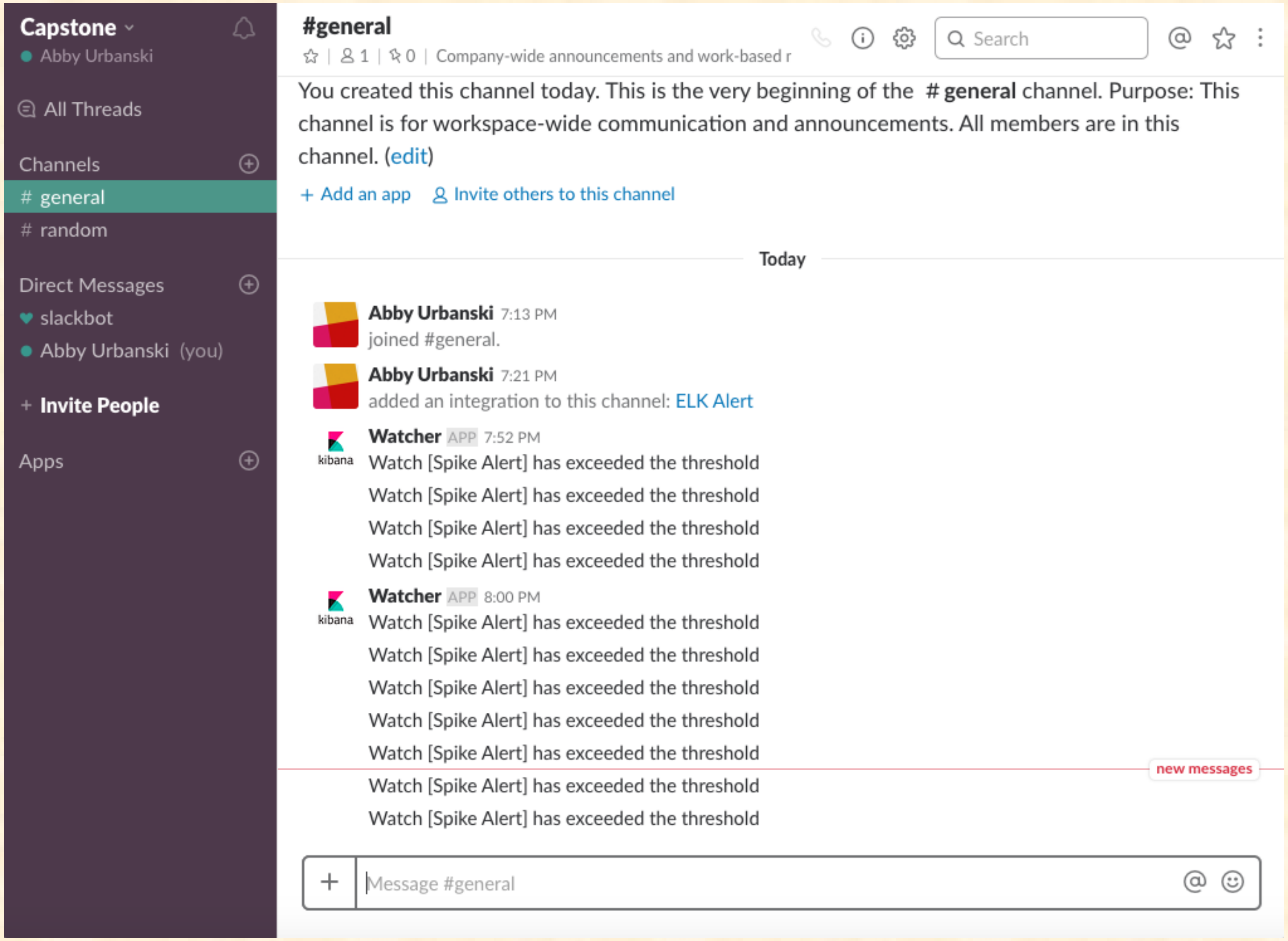
ELK Dashboard



ELK Spike on Graph



ELK Alerting on Slack



You created this channel today. This is the very beginning of the # **general** channel. Purpose: This channel is for workspace-wide communication and announcements. All members are in this channel. (edit)

Abby Urbanski 7:13 PM
joined #general.

Abby Urbanski 7:21 PM
added an integration to this channel: ELK Alert

Watcher APP 7:52 PM
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold

Watcher APP 8:00 PM
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold
Watch [Spike Alert] has exceeded the threshold

What’s left to do?

- Solidify the dashboards with more trends and patterns
- Identify more security related trends and have them be alerted
- Integrate input of user certificate within the applications

Questions?

? ? ? ?

? ?

? ? ?