

MICHIGAN STATE

U N I V E R S I T Y

Alpha Presentation

Insider Threat Detection

The Capstone Experience

Team AppDynamics

Ari Kohl

Chris Kulpa

Sumanth Rudraraju

Andy Zhang



*From Students...
...to Professionals*

Department of Computer Science and Engineering
Michigan State University

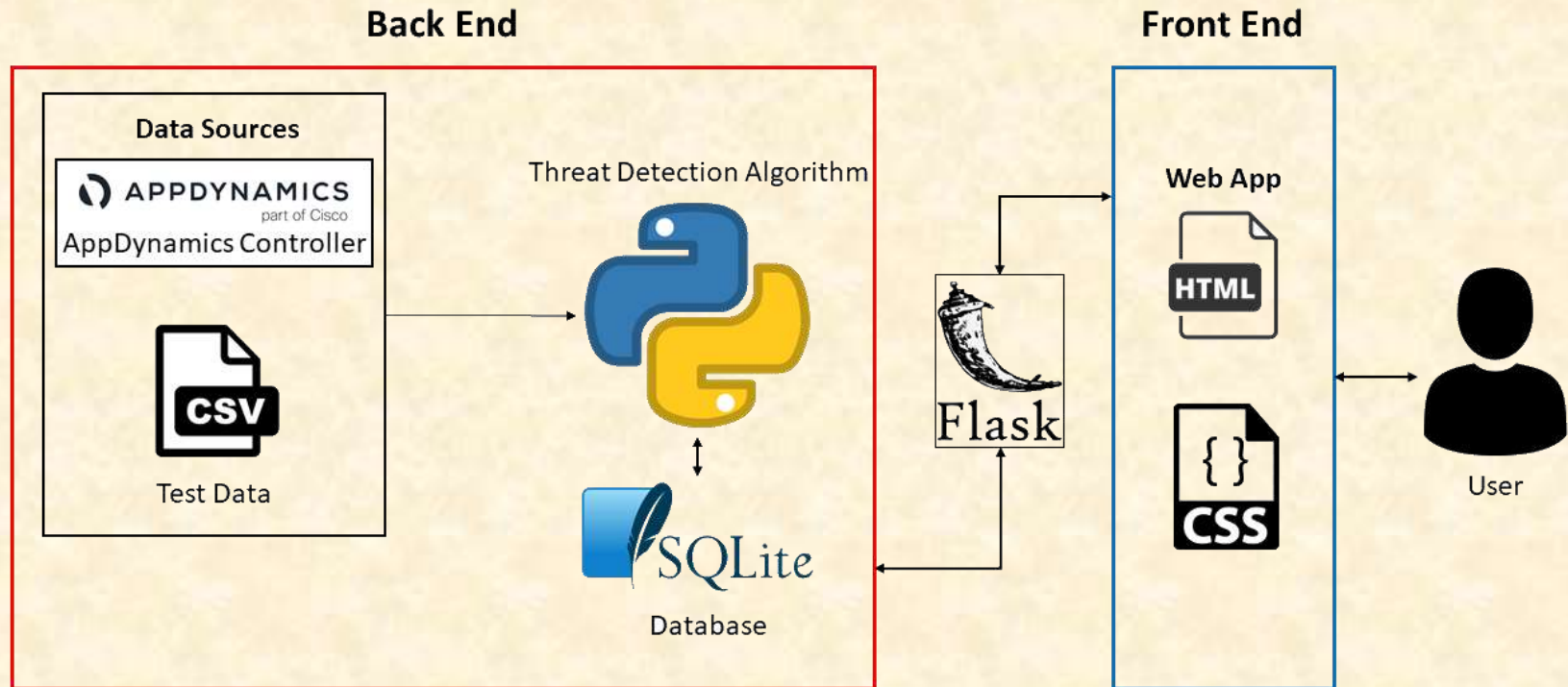
Fall 2020

Project Overview

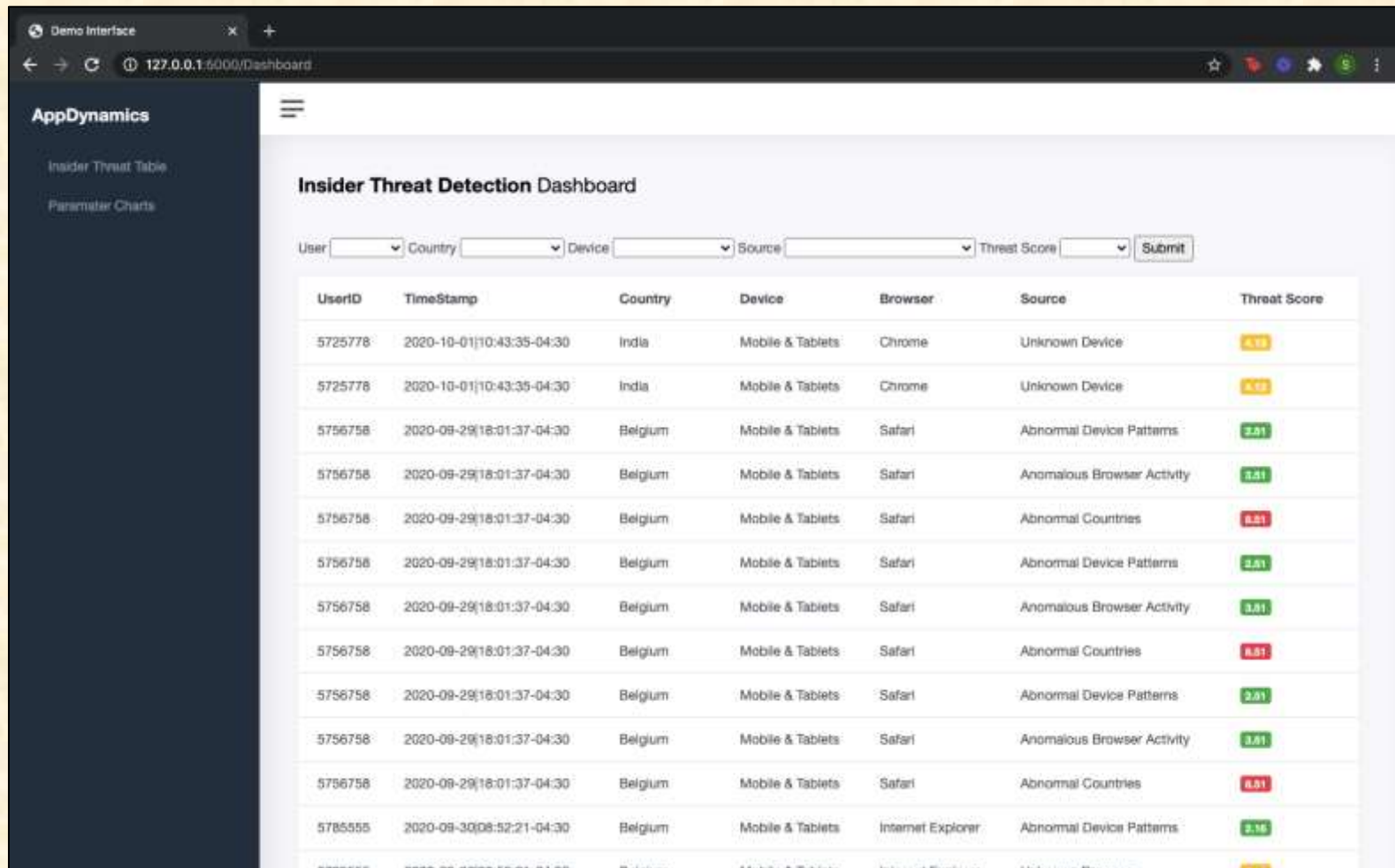
- Use AppDynamics' controller as the source of data
- Run a threat detection algorithm on the data
- The algorithm uses machine learning and kernel density estimation.
- Display the results of the algorithm on the web app
- Allow user to take action on suspicious account



System Architecture



Display of Anomalous Users



The screenshot displays the AppDynamics Insider Threat Detection Dashboard. The interface includes a navigation sidebar on the left with options for 'Insider Threat Table' and 'Parameter Charts'. The main content area features a title 'Insider Threat Detection Dashboard' and a set of filters: 'User', 'Country', 'Device', 'Source', and 'Threat Score', each with a dropdown menu, and a 'Submit' button. Below the filters is a table listing detected anomalies.

UserID	TimeStamp	Country	Device	Browser	Source	Threat Score
5725778	2020-10-01 10:43:35-04:30	India	Mobile & Tablets	Chrome	Unknown Device	4.98
5725778	2020-10-01 10:43:35-04:30	India	Mobile & Tablets	Chrome	Unknown Device	4.98
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Device Patterns	3.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Anomalous Browser Activity	3.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Countries	8.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Device Patterns	3.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Anomalous Browser Activity	3.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Countries	8.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Device Patterns	3.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Anomalous Browser Activity	3.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Countries	8.81
5785555	2020-09-30 08:52:21-04:30	Belgium	Mobile & Tablets	Internet Explorer	Abnormal Device Patterns	3.86



Filtering based on User ID

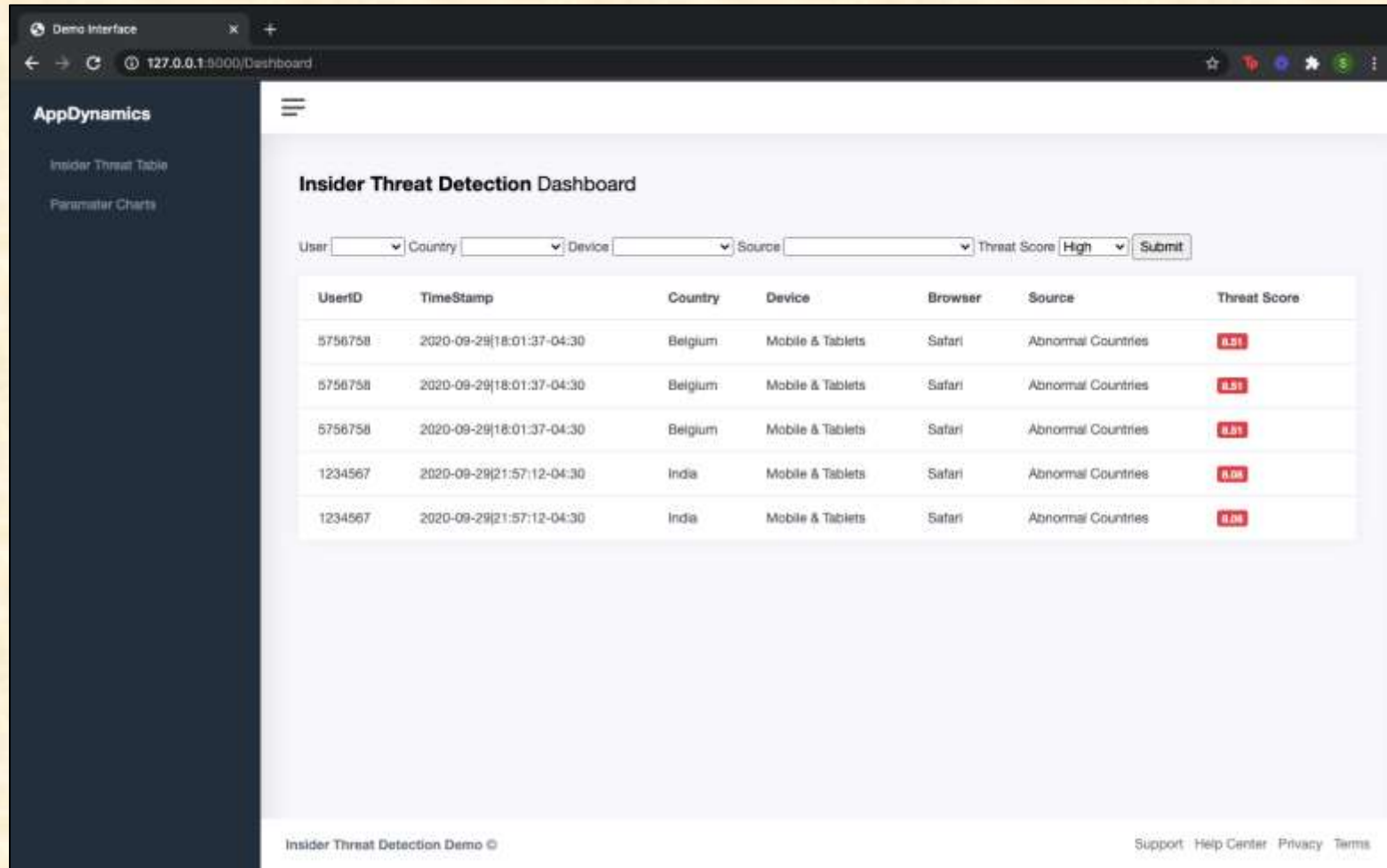
The screenshot shows a web browser window with the URL `127.0.0.1:9000/Dashboard`. The page title is "Insider Threat Detection Dashboard". On the left, there is a sidebar with "AppDynamics" and navigation links for "Insider Threat Table" and "Parameter Charts". The main content area features a filter bar with dropdown menus for "User" (set to 5872716), "Country", "Device", "Source", and "Threat Score", followed by a "Submit" button. Below the filter bar is a table with the following data:

UserID	TimeStamp	Country	Device	Browser	Source	Threat Score
5872716	2020-09-30 18:38:58-04:30	United States	Computer	Internet Explorer	Anomalous Browser Activity	2.3
5872716	2020-09-30 18:38:58-04:30	United States	Computer	Internet Explorer	Abnormal Countries	1.3
5872716	2020-09-30 18:38:58-04:30	United States	Computer	Internet Explorer	Anomalous Browser Activity	2.3
5872716	2020-09-30 18:38:58-04:30	United States	Computer	Internet Explorer	Abnormal Countries	1.3
5872716	2020-09-29 13:18:42-04:30	India	Computer	Internet Explorer	Anomalous Browser Activity	3.0
5872716	2020-09-29 13:18:42-04:30	India	Computer	Internet Explorer	Abnormal Countries	1.3

At the bottom of the page, there is a footer with "Insider Threat Detection Demo ©" on the left and "Support | Help Center | Privacy | Terms" on the right.



Filtering based on Threat Score



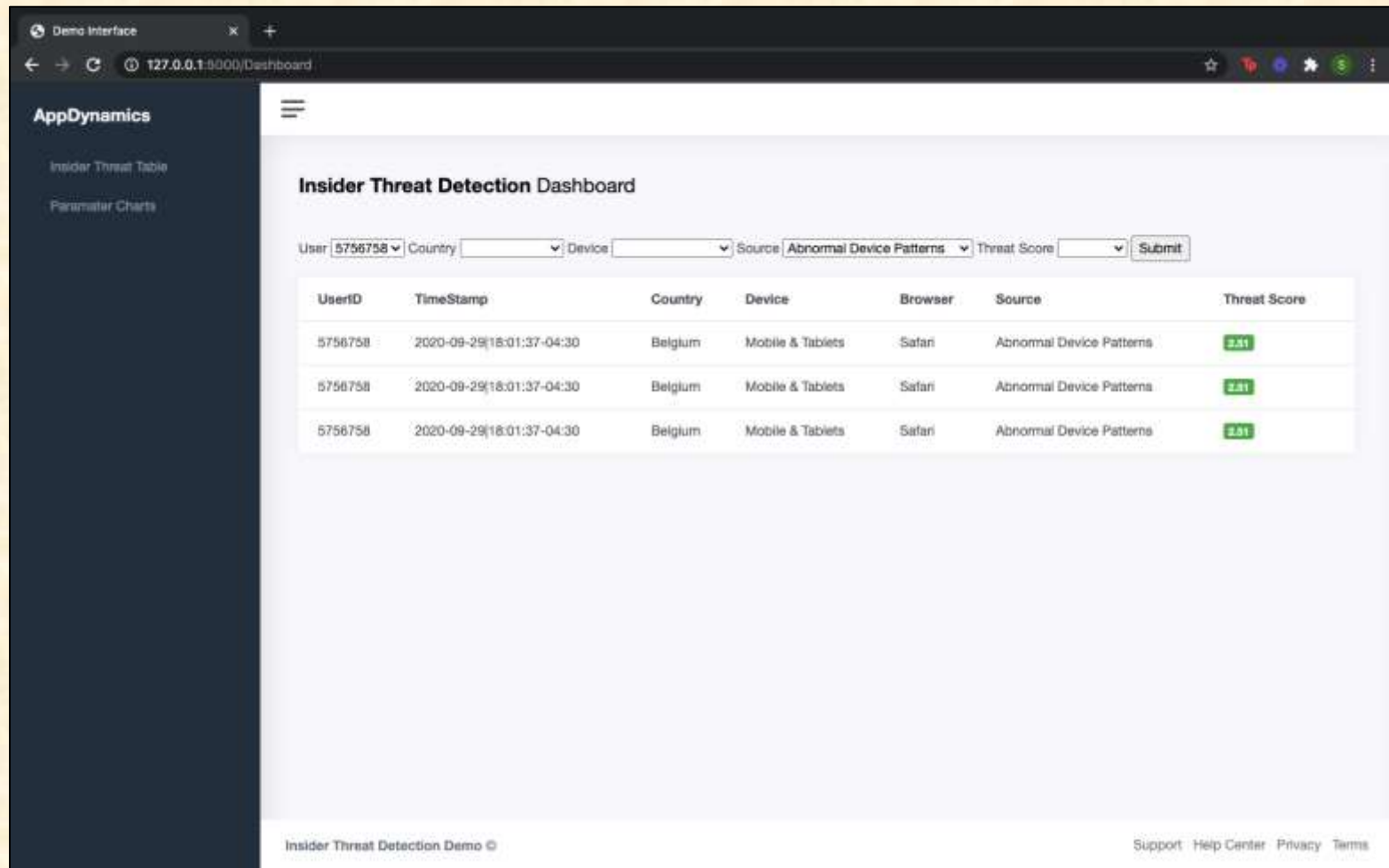
The screenshot displays the AppDynamics Insider Threat Detection Dashboard. The interface includes a navigation sidebar on the left with options for 'Insider Threat Table' and 'Parameter Charts'. The main content area features a filter bar with dropdown menus for 'User', 'Country', 'Device', and 'Source', and a 'Threat Score' dropdown set to 'High'. A 'Submit' button is located to the right of the filters. Below the filter bar is a table of threat events.

UserID	TimeStamp	Country	Device	Browser	Source	Threat Score
5756758	2020-09-29[18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Countries	8.81
5756758	2020-09-29[18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Countries	8.81
5756758	2020-09-29[18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Countries	8.81
1234567	2020-09-29[21:57:12-04:30	India	Mobile & Tablets	Safari	Abnormal Countries	8.06
1234567	2020-09-29[21:57:12-04:30	India	Mobile & Tablets	Safari	Abnormal Countries	8.06

At the bottom of the dashboard, there is a footer with the text 'Insider Threat Detection Demo ©' on the left and 'Support Help Center Privacy Terms' on the right.



Filtering based on User ID and Source of Anomaly



The screenshot displays the AppDynamics Insider Threat Detection Dashboard. The interface includes a navigation sidebar on the left with options for 'Insider Threat Table' and 'Parameter Charts'. The main content area features a filter bar with dropdown menus for 'User' (set to 5756758), 'Country', 'Device', 'Source' (set to Abnormal Device Patterns), and 'Threat Score', along with a 'Submit' button. Below the filters is a table listing detected anomalies.

UserID	TimeStamp	Country	Device	Browser	Source	Threat Score
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Device Patterns	2.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Device Patterns	2.81
5756758	2020-09-29 18:01:37-04:30	Belgium	Mobile & Tablets	Safari	Abnormal Device Patterns	2.81

At the bottom of the dashboard, there is a footer with the text 'Insider Threat Detection Demo ©' on the left and 'Support | Help Center | Privacy | Terms' on the right.



What's left to do?

- Display the results in graphs and charts
- Sorting based on a certain field
- Further develop algorithm and threat score
 - Incorporate more fields of data
 - Track the fingerprint of activity
- Act against anomalous users



Questions?

?

?

?

?

?

?

?

?

?

