Virginia Commonwealth University
VCU Scholars Compass

Capstone Design Expo Posters

School of Engineering

2016

Application Intrusion Detection: Security for Cloud Deployments

Justin Murphy
Virginia Commonwealth University

Nick Harrison
Virginia Commonwealth University

John Taylor
Virginia Commonwealth University

Follow this and additional works at: http://scholarscompass.vcu.edu/capstone

Part of the Computer Engineering Commons

© The Author(s)

Downloaded from

http://scholarscompass.vcu.edu/capstone/117

This Poster is brought to you for free and open access by the School of Engineering at VCU Scholars Compass. It has been accepted for inclusion in Capstone Design Expo Posters by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.

Team Members: Justin Murphy, Nick Harrison, John Taylor

Faculty Advisor: Carol Fung

Sponsor: GE

Sponsor Advisor: Randy Harris

COMPUTER SCIENCE

Application Intrusion Detection

Security for Cloud Deployments

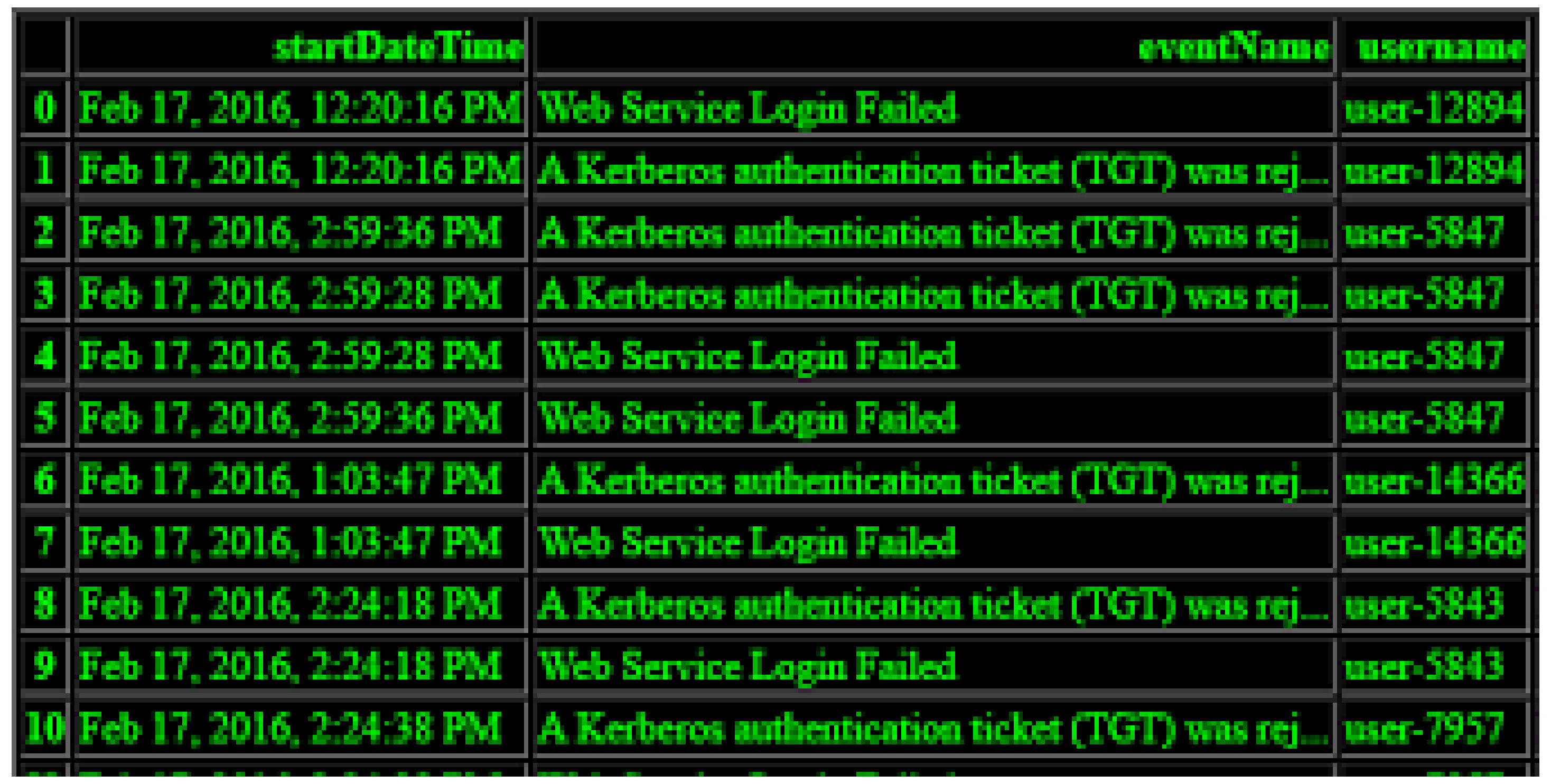
CAPSTONE DESIGN EXPO 2016

Anomaly Finder

●More and more companies are turning over to a cloud based infrastructure, there has been a lack of security measures to cover all the new threats associated with moving to the cloud.

●Our project searches through data that is generated every time a user logs into a system and organizes it into means that makes it easier for a CIRT team to understand.

●If there is a discrepancy in the data, our system will notify the user of the anomaly and which user prompted it. By doing so we could alert to possible intrusions of malicious users in the system and handle the problem before any damage can be done.



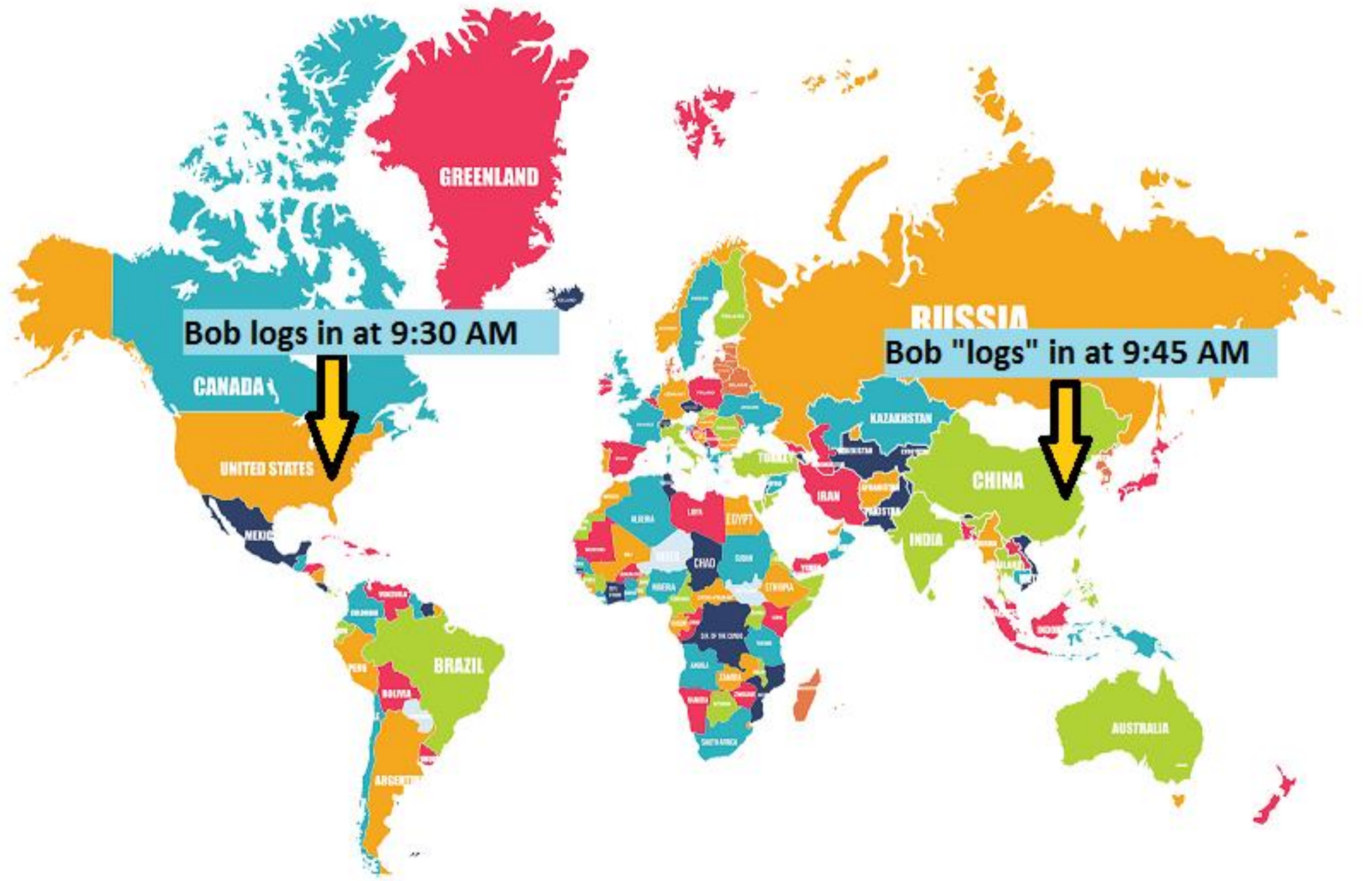
	startDateTime	eventName	username
0	Feb 17, 2016, 12:20:16 PM	Web Service Login Failed	user-12894
1	Feb 17, 2016, 12:20:16 PM	A Kerberos authentication ticket (TGT) was rej...	user-12894
2	Feb 17, 2016, 2:59:36 PM	A Kerberos authentication ticket (TGT) was rej...	user-5847
3	Feb 17, 2016, 2:59:28 PM	A Kerberos authentication ticket (TGT) was rej...	user-5847
4	Feb 17, 2016, 2:59:28 PM	Web Service Login Failed	user-5847
5	Feb 17, 2016, 2:59:36 PM	Web Service Login Failed	user-5847
6	Feb 17, 2016, 1:03:47 PM	A Kerberos authentication ticket (TGT) was rej...	user-14366
7	Feb 17, 2016, 1:03:47 PM	Web Service Login Failed	user-14366
8	Feb 17, 2016, 2:24:18 PM	A Kerberos authentication ticket (TGT) was rej...	user-5843
9	Feb 17, 2016, 2:24:18 PM	Web Service Login Failed	user-5843
10	Feb 17, 2016, 2:24:38 PM	A Kerberos authentication ticket (TGT) was rej...	user-7957

●Right now our project detects anomalies in location, repeated failures, and other red flags that coincide with the actions of a possible intruder.

●By taking in sets of authentication logs, our project is able to comb through thousands of logs over set periods of time, a process that would be time consuming and tedious for any security team to handle manually.

How is it done?

Using the data generated when logging in, we can compare the information to known patterns of intrusion and in doing so catch potential hackers. A classic example would be if User Bob logged in at the VCU student commons, but then we see 15 minutes later that Bob has logged in from somewhere China. We see this by comparing Bob's source IPs generated when his account logs in.



Obviously this is not physically possible so we would alert on Bob to see if his account was being infiltrated. By using location and several other criterion, we can alert to these anomalies to see if they were pure happenstance or intended attack. Using this amalgamated data, we can take certain fields and compare them to see if anything is subject to scrutiny. If the anomaly is too far from the norm or is suspicious, measures can be taken in order to protect private information from the unwanted trespasser.

What's the Point?

Why is it Important? :

●Big companies have thousands of login attempts every day

●It is not likely that a cyber-security team is able to review all the logs generated, thus leaving openings for intruders to work their way into the systems

●They could then steal information, damage systems, and generally cost the company money and man hours.

●With our system in place, the logs are able to be reviewed, and the cyber-security team only has to deal with the anomalies that were found, making the whole deal harder for attackers to go unnoticed.

Nothing is like it:

●The biggest attribute is the marketable potential of this product.

●No big brand product is out on the market covering the same needs as our product could lead to very promising marketability opportunities.

●It is only furthered by the fact that many companies are moving to the cloud and don't know how to handle the security aspects with the change