RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SOP-W09

Machine Learning—The New Face of BYOD

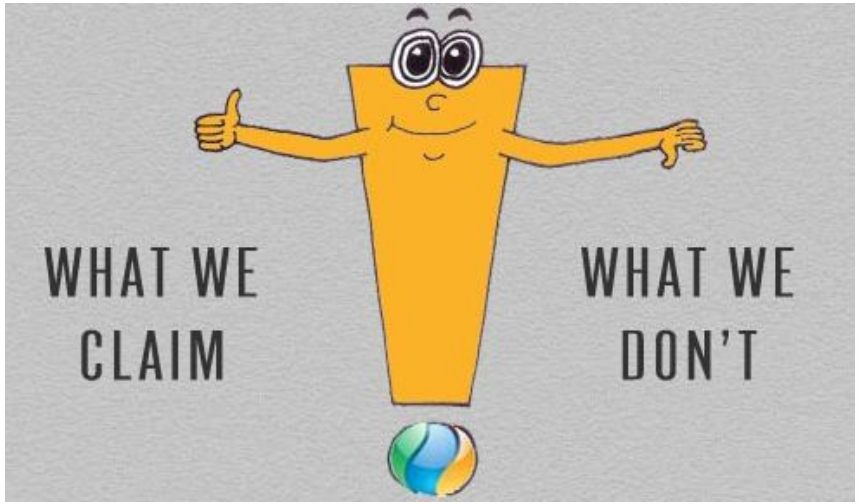
Haroot Zarger
IT Security Engineer
@harootz

Nilaykumar Kiran Sangani
IT Security Planning Analyst
@outlawzter

Disclaimer

All work mentioned in this presentation

- Is our own research/views and not those of our present and past employers.
- Does not represent the thoughts, intentions, plans or strategies of our present and past employers.



Agenda

- What is BYOD?
- Architectural Strategy
- Machine Learning
- Azane(NH_3)
- Conclusion
- Future Work

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

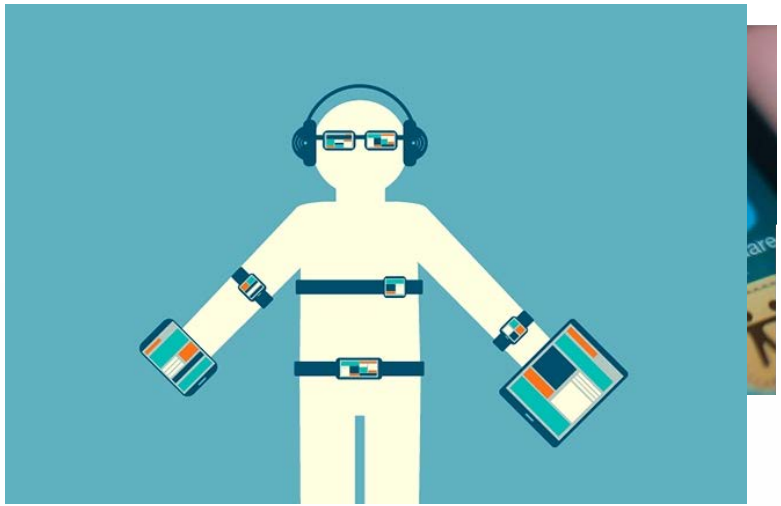
Bring Your Own Device

#RSAC

What is BYOD ?

BYOD Perception

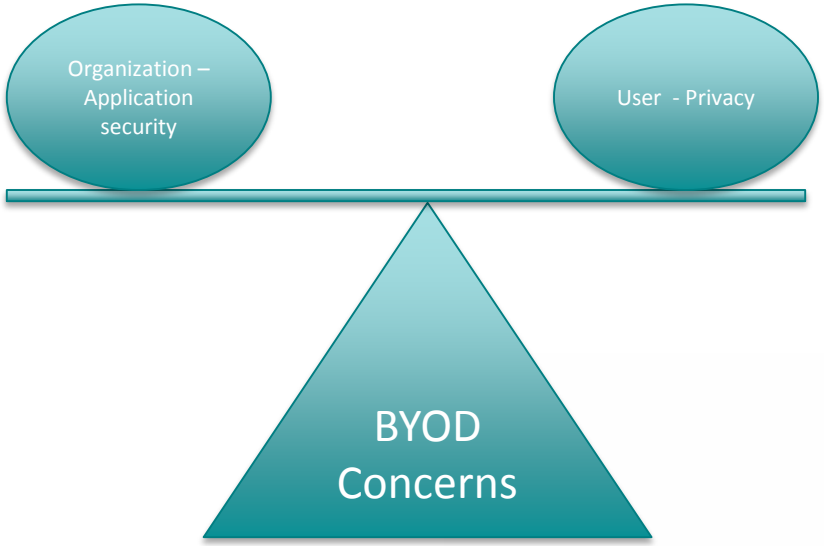
- CxO's Wish List
- Security's Nightmare
- Fashion Trend



Where does your organization stand?

- Fully implemented a bring-your-own-device (BYOD) program.
- Implemented a dual model of corporate-owned and employee-owned devices.
- Starting to consider BYOD.
- Never considered.

BYOD Concerns



Architectural Strategy

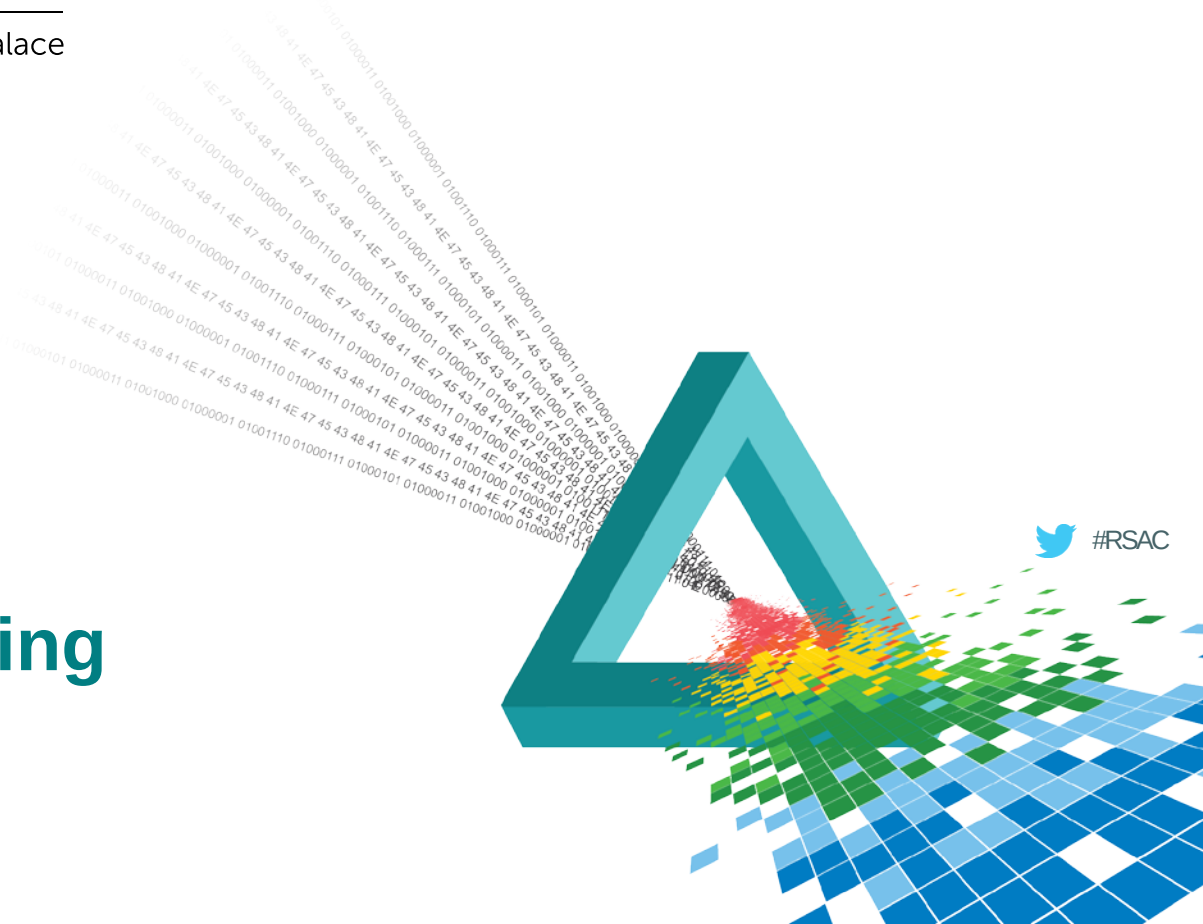
- Integrate Machine Learning (ML) at application level to analyze and differentiate between legitimate and anomalous behavior.

- Integrate ML output with centralized monitoring system (SIEM) for holistic view.

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Machine Learning

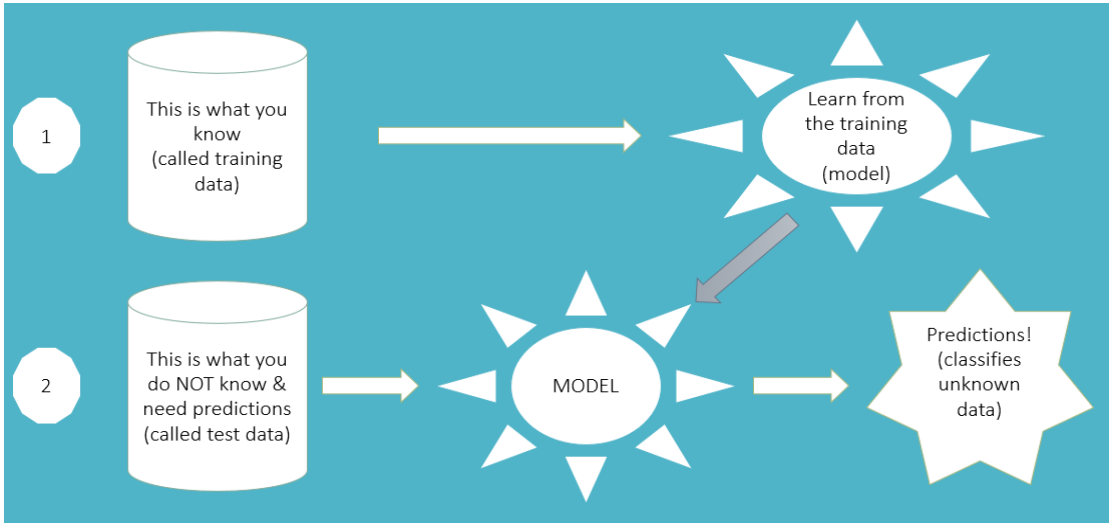


What is Machine Learning (ML)?

- “A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E”

Lets make it simple

“Field of study that gives computers the ability to learn without being explicitly programmed” - Arthur Samuel

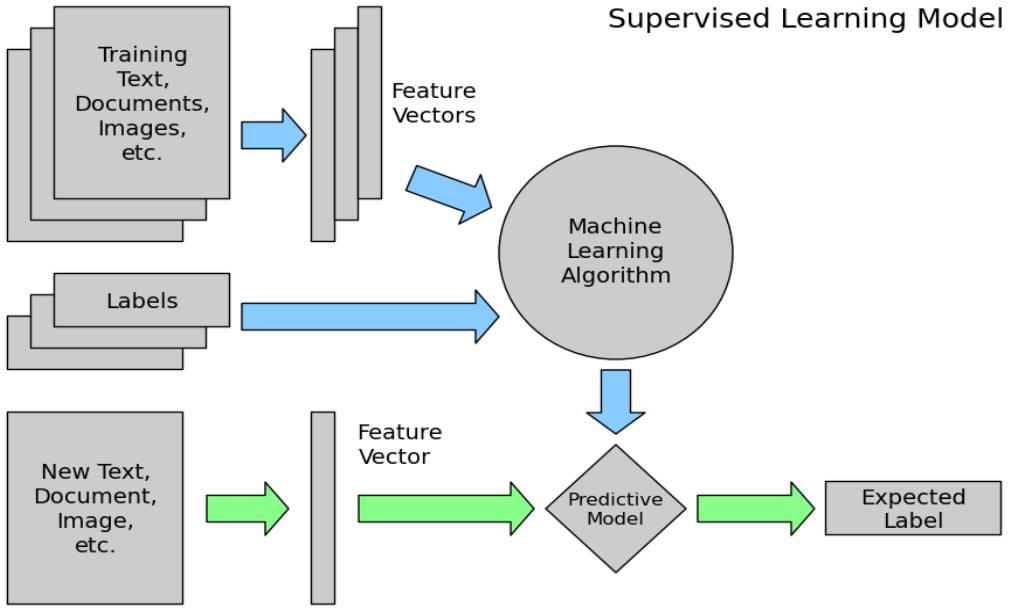


Machine Learning Models

- Supervised
- Unsupervised

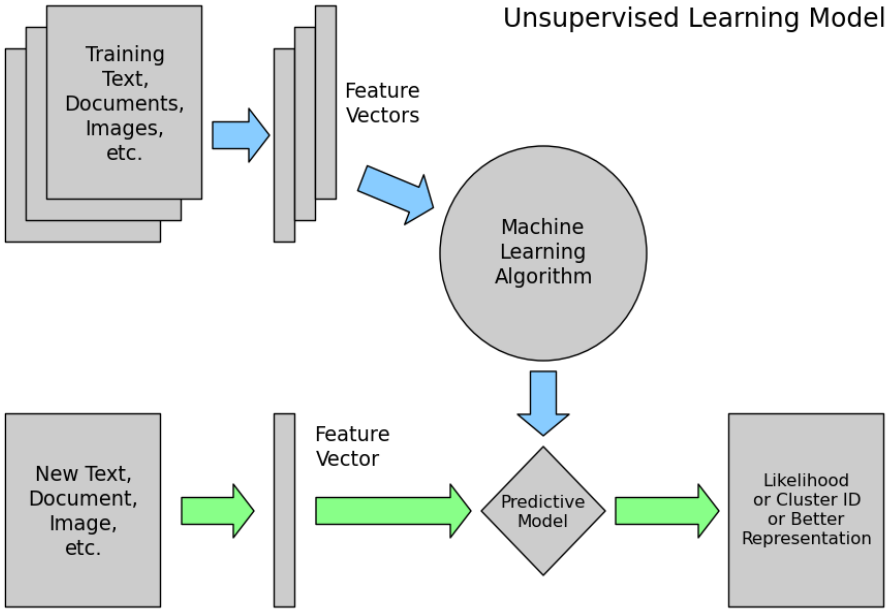
Supervised

- Datasets are provided which are used to train the machine and get the desired outputs.
  - Spam Filtering



Unsupervised

- No datasets are provided, instead the data is clustered into different classes.
  - Google News

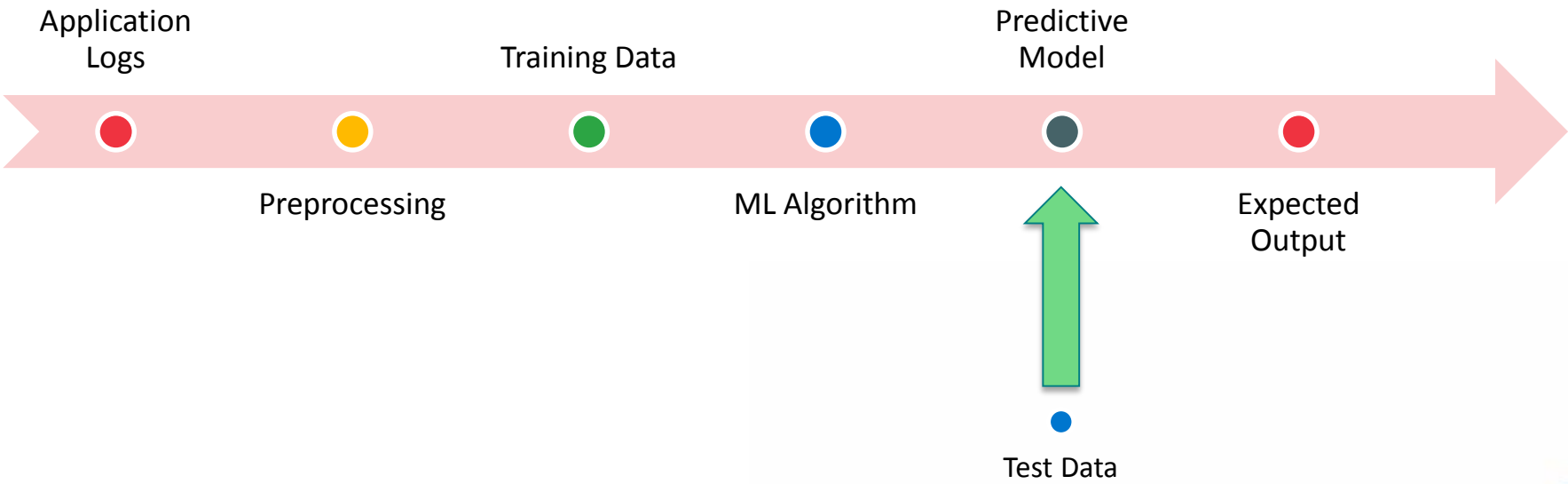


Azane (NH_3)

www.azane.io

https://github.com/sanganinilay/AzaneML

Anomaly Detection



Application Logs

Username	Authenticati	Method	Request	User Agent	Service Name	Service Function Call	Legitimate Request (Class Variables
Steve	NO	POST	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	N
Steve	No	Get	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	Y
Steve	No	POST	\Authentication.aspx	Android	SubmitAuthenticate	AuthenticateSubmit	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	DisplayPayslipMonth	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	PrintPayslipMonth	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	DisplayPayslipPastMonths	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	PrintPayslipPreviousMonth	Y
Steve	Passed	Get	\logout.aspx	Android	LogoutPayslip	SessionLogoutUserPayslip	Y
Steve123	NO	POST	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	N
Steve@gg.com	NO	POST	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	N
admin	NO	POST	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	N
Steve	No	Get	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	Y
Steve	No	POST	\Authentication.aspx	Android	SubmitAuthenticate	AuthenticateSubmit	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	DisplayPayslipMonth	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	PrintPayslipMonth	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	DisplayPayslipPastMonths	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	PrintPayslipPreviousMonth	Y
Steve	Passed	Get	\logout.aspx	Android	LogoutPayslip	SessionLogoutUserPayslip	Y
Steve	No	Get	\Authentication.aspx	Android	GetAuthenticate	AuthenticateUser	Y
Steve	No	POST	\Authentication.aspx	Android	SubmitAuthenticate	AuthenticateSubmit	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	DisplayPayslipMonth	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	PrintPayslipMonth	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	DisplayPayslipPastMonths	Y
Steve	Passed	Get	\Payslip.aspx	Android	GetPayslip	PrintPayslipPreviousMonth	Y
Steve	Passed	Get	\logout.aspx	Android	LogoutPayslip	SessionLogoutUserPayslip	Y

Preprocessing

```
-------------------------------------------------------------------------------
//Authentication
If (Authentication is No )
        { 0 }
        else
        { 1 }

Therefore : Authentication { 0,1 }
-------------------------------------------------------------------------------
//Method
If ( Method is Get )
        { 0 }
        else If ( Method is Post )
                { 1 }
        else
                { 2 }
Therefore : Method { 0,1,2 }
-------------------------------------------------------------------------------
//Request
If ( Request is Authentication.aspx )
        { 0 }
        else If ( Request is Payslip.aspx
                        { 1 }
                else If ( Request is logout.aspx )
                        { 2 }
                else
                        { 3 }

Therefore : Request { 0,1,2,3 }
```

Training data

```
1  @relation appsec
2
3  @attribute Username {0,1}
4  @attribute Authentication {0,1}
5  @attribute Method {0,1,2}
6  @attribute Request {0,1,2,3}
7  @attribute UserAgt {0,1}
8  @attribute ServiceName {0,1,2,3,4}
9  @attribute ServiceFuncCall {0,1,2,3,4,5,6,7}
10 @attribute LegitimateUser {Y,N}
11 @data
12 0,0,2,0,0,0,0,N
13 0,0,0,0,0,0,0,Y
14 0,0,1,0,0,1,1,Y
15 0,1,0,1,0,2,2,Y
16 0,1,0,1,0,2,3,Y
17 0,1,0,1,0,2,4,Y
18 0,1,0,1,0,2,5,Y
19 0,1,0,2,0,3,6,Y
20 1,0,1,0,0,0,0,N
21 1,0,1,0,0,0,0,N
```

ML Algorithm – Naive Bayes

appsecml.java

```
//-------------------------------------------------------------------------------------------------------------
//Authors : Nilay Sangani, Haroot Zarger
// Version : 0.1
// Email : sanganinilay@hotmail.com,harootz@gmail.com
// Twitter : @outlawzter,@harootz
//-------------------------------------------------------------------------------------------------------------
import java.io.BufferedReader;
import java.io.FileReader;
import java.io.IOException;
import java.util.Random;

import weka.classifiers.Evaluation;
import weka.classifiers.bayes.NaiveBayes;
import weka.core.Instance;
import weka.core.Instances;

public class appsecml {

    public static void main(String[] args) throws IOException {

        //Training
        BufferedReader objBreader = null;
        try{


        System.out.println("Supplying Training Set.................");
        System.out.println();
        objBreader = new BufferedReader(new FileReader("D:/MLNH/Trainingdata.arff"));
        Instances objTrain = new Instances(objBreader);
        objTrain.setClassIndex(objTrain.numAttributes()-1);
        objBreader.close();
        NaiveBayes objNB = new NaiveBayes();
        try {
            System.out.println("Applying Naive Bayes algorithm.... ");
            System.out.println();
            objNB.buildClassifier(objTrain); // trained
        } catch (Exception e) {
            e.printStackTrace();
        }
```

Predictive Model

```
Time taken to build model: 0 seconds

=== Evaluation on training set ===
=== Summary ===

Correctly Classified Instances          20               90.9091 %
Incorrectly Classified Instances         2                9.0909 %
```

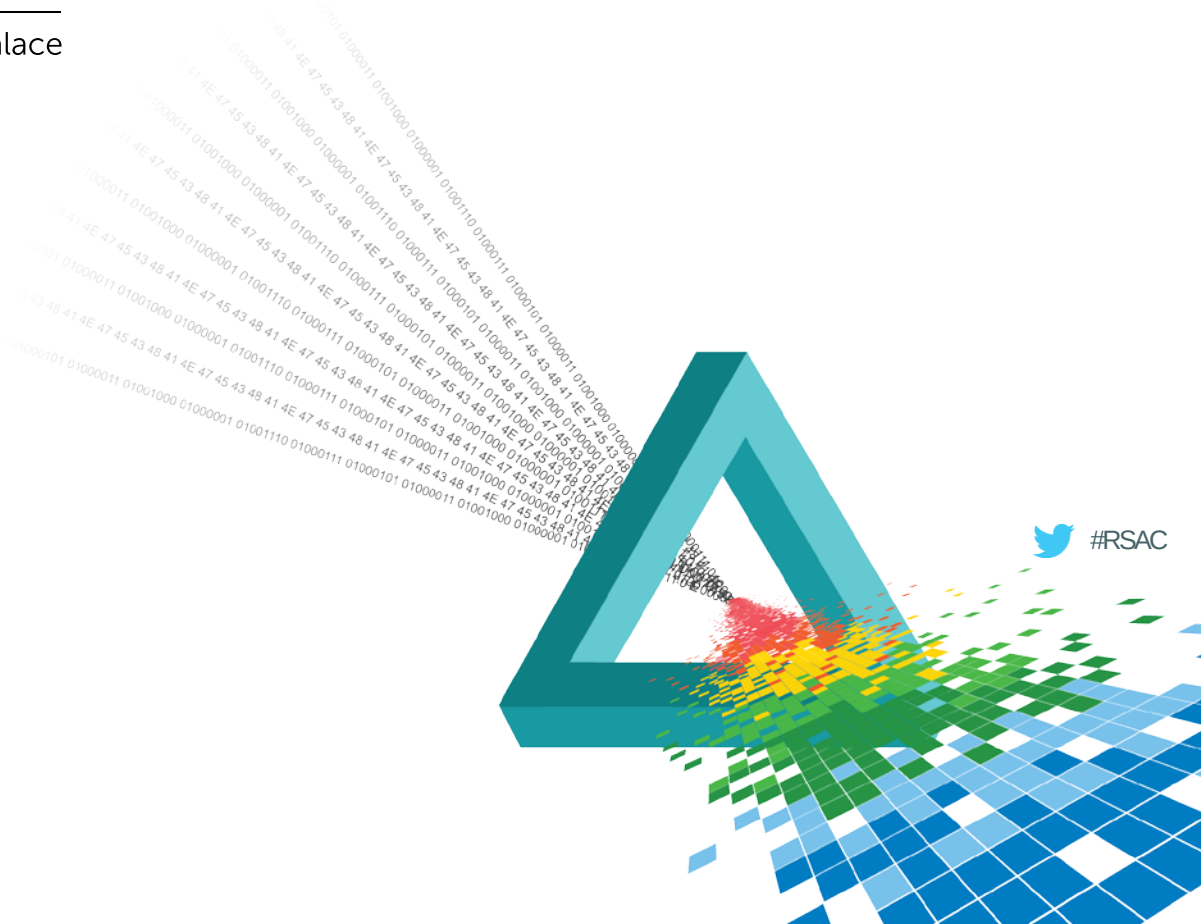
```
=== Confusion Matrix ===

  a  b   <-- classified as
 11  2 |  a = Y
  0  9 |  b = N
```

Test Data & Predicted Output

```
@relation Appsec
@attribute Username {0,1}
@attribute Authentication {0,1}
@attribute Method {0,1,2}
@attribute Request {0,1,2,3}
@attribute UserAgt {0,1}
@attribute ServiceName {0,1,2,3,4}
@attribute ServiceFuncCall {0,1,2,3,4,5,6,7}
@attribute class {Y,N}
@data
0,0,0,3,0,4,7,?
0,1,0,2,0,3,6,?
0,1,0,1,0,2,2,?
0,0,0,3,0,4,7,?
0,0,0,3,1,4,7,?
```

```
inst#,     actual, predicted,
     1          ?          1:Y
     2          ?          1:Y
     3          ?          2:N
     4          ?          2:N
     5          ?          2:N
     6          ?          2:N
```

Conclusion



Conclusion

- No additional app to be installed in the users device – privacy maintained.
- Yields better results, when huge amount of data is fed which helps to spot patterns.
- Key to ML is that it works best when the data is consistent.
- Can be Integrated with SIEM solution for centralized management
  - Single console for searching, visualizing capabilities.
  - Correlation between ML output and other infrastructure devices such as IPS, firewall etc.

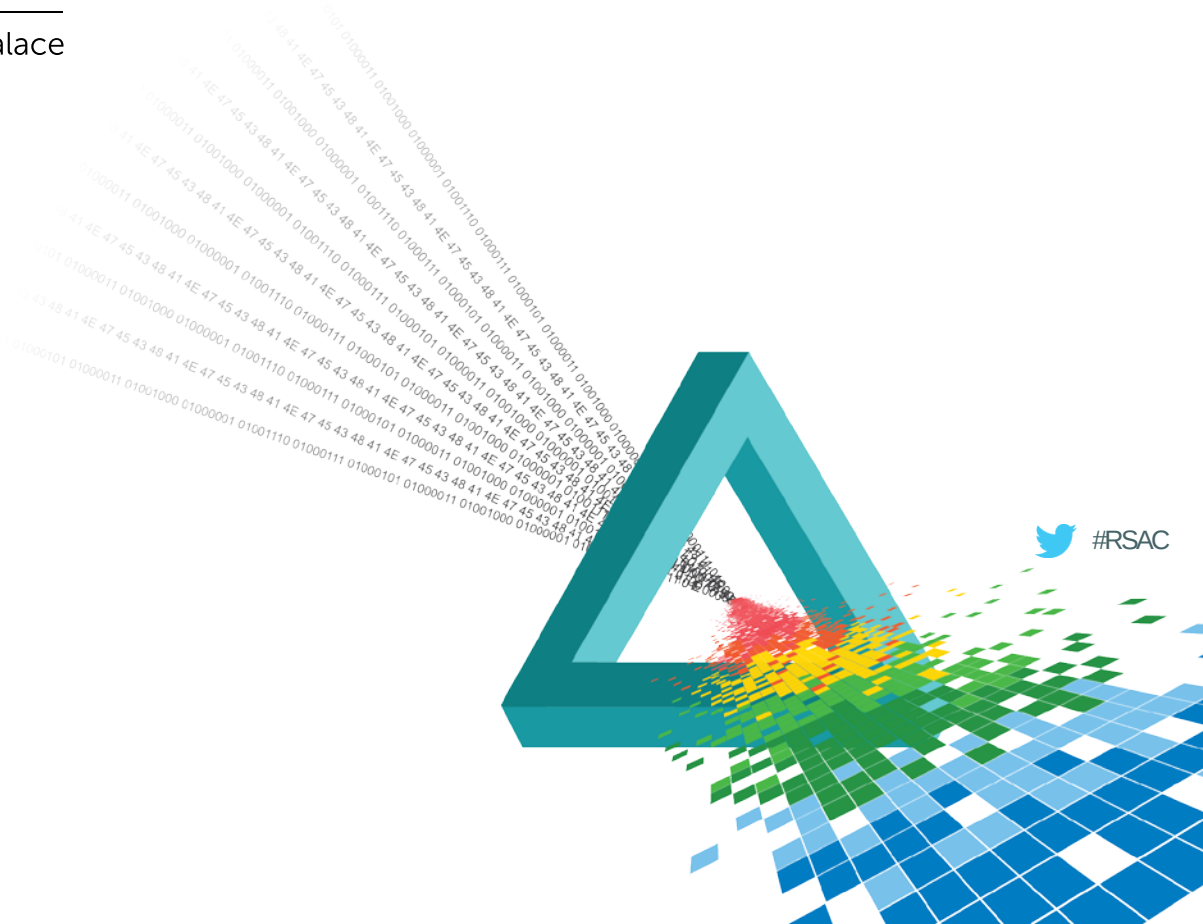
How to Apply

- Identify your organizations approach towards BYOD.
- Download the ML Engine (Azane) from github.
- Identify the attributes in your application logs.
- Create preprocessing rules as per your needs.

How to Apply

- Create training data.
- Learn the model.
- Apply test data to the predictive model.
- Analyze the output.

Future Work



Future work

- Enhancements to Azane
  - End to end integration with SIEM solution.
  - Integrating security devices.
  - Alerting and reporting modules.
  - Creation of API’s.
  - Interactive GUI.

Special Thanks

- Dr. Zeyar Aung, Associate Professor - Computing and Information Science, Masdar Institute.
- WEKA - Waikato Environment for Knowledge Analysis

Sources

- http://www.cs.waikato.ac.nz/ml/weka/
- http://www.k12blueprint.com/content/elliott%E2%80%99s-two-cents-byod-four-letter-word-parents-and-schools
- http://blogs.cisco.com/healthcare/cisco-reveals-work-your-way
- http://www.clker.com/cliparts/0/7/e/a/12074327311562940906milker_X_icon.svg.hi.png
- http://content.timesjobs.com/role-hr-needs-play-byod-implementation/
- http://sine.ni.com/cms/images/casestudies/heenaf.png?size
- http://parasdoshi.com/tag/machine-learning/

Sources

- http://www.securityweek.com/what-machine-learning-can-bring-it-security
- http://www.astroml.org/sklearn_tutorial/_images/plot_ML_flow_chart_1.png
- http://www.trackvia.com/blog/infographics/bring-your-own-devices-to-work-trend-infographic
- http://www.slideshare.net/DruvaInc/the-rise-and-risk-of-byod-infographic
- http://www.slideshare.net/ibmsecurity/2015-mobile-security-trends
- http://blogs.forrester.com/thomas_husson/14-11-11-mobile_leaders_will_break_away_from_laggards_in_2015

Sources

- http://blogs.forrester.com/julie_ask/14-11-11-mobile_predictions_the_game_will_change_in_2015
- http://www.ovum.com/press_releases/ovum-predicts-enterprise-mobility-to-be-top-of-the-cio-agenda-in-2015
- http://www.slideshare.net/ibmsecurity/2015-mobile-security-trend
- http://www.slideshare.net/LookoutInc/mobile-security-the-5-questions-modern-organizations-are-asking
- http://www.welivesecurity.com/2013/02/19/from-byod-to-cyod-security-issues-with-personal-devices-in-the-workplace

Thank You

- Nilaykumar Sangani
  - sanganinilay@hotmail.com
  - @outlawzter
- Haroot Zarger
  - harootz@gmail.com
  - @harootz

Website : www.azane.io
https://github.com/sanganinilay/AzaneML