emea ATMOSPHERE '17
THE INNOVATION EDGE

aruba
a Hewlett Packard Enterprise company

# Artificial Intelligence in Enterprise Networking

Jisheng Wang

May 9, 2017

# Me, Niara, Aruba

- **Jisheng Wang, Senior Director of Data Science in CTO Office**
  - Over 12-year experiences of applying machine learning and big data into security
  - Ph.D from Penn State – ML in network security
  - Technical Lead in Cisco – Security Intelligence Operations (SIO)
  - Lead the overall big data analytics innovation and development in Niara
- **Niara**
  - Recognized leader by Gartner in User and Entity Behavior Analytics (UEBA)
  - Re-invent enterprise security analytics for attack detection and incident response
  - Acquired by Aruba, a Hewlett Packard Enterprise company in Feb, 2017

# Outline

- ***Terms and Basics***
- Machine Learning in Practice
- Applied Machine Learning in Enterprise Networking

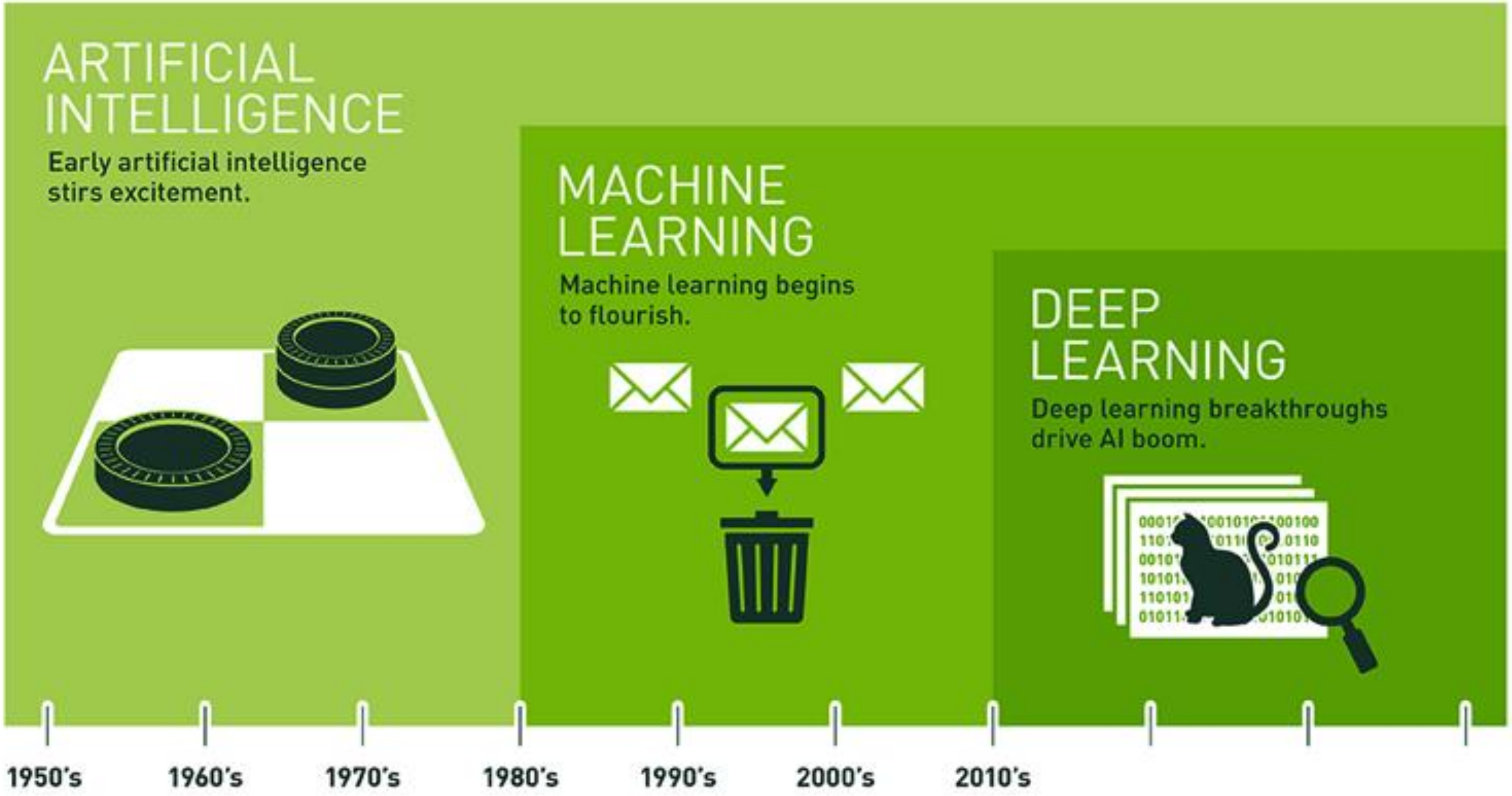
# Top Analytics Buzzwords in 2016

- Artificial Intelligence (AI)
- Machine Learning (ML)
- Deep Learning (DL)
- Business Intelligence
- Data Science
- Real-time Analytics
- Predictive Analysis
- Intelligence Decision Automation
- …………

# Top Analytics Buzzwords in 2016

- **Artificial Intelligence (AI)**
- **Machine Learning (ML)**
- **Deep Learning (DL)**
- Business Intelligence
- Data Science
- Real-time Analytics
- Predictive Analysis
- Intelligence Decision Automation
- …………

# Artificial Intelligence, Machine Learning, Deep Learning



ARTIFICIAL INTELLIGENCE

Early artificial intelligence stirs excitement.

MACHINE LEARNING

Machine learning begins to flourish.

DEEP LEARNING

Deep learning breakthroughs drive AI boom.

Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.

Image taken from nvidia

# Outline

- Terms and Basics
- ***Machine Learning in Practice***
- Applied Machine Learning in Enterprise Networking

# Machine Learning Use Case: Object Classification & Detection

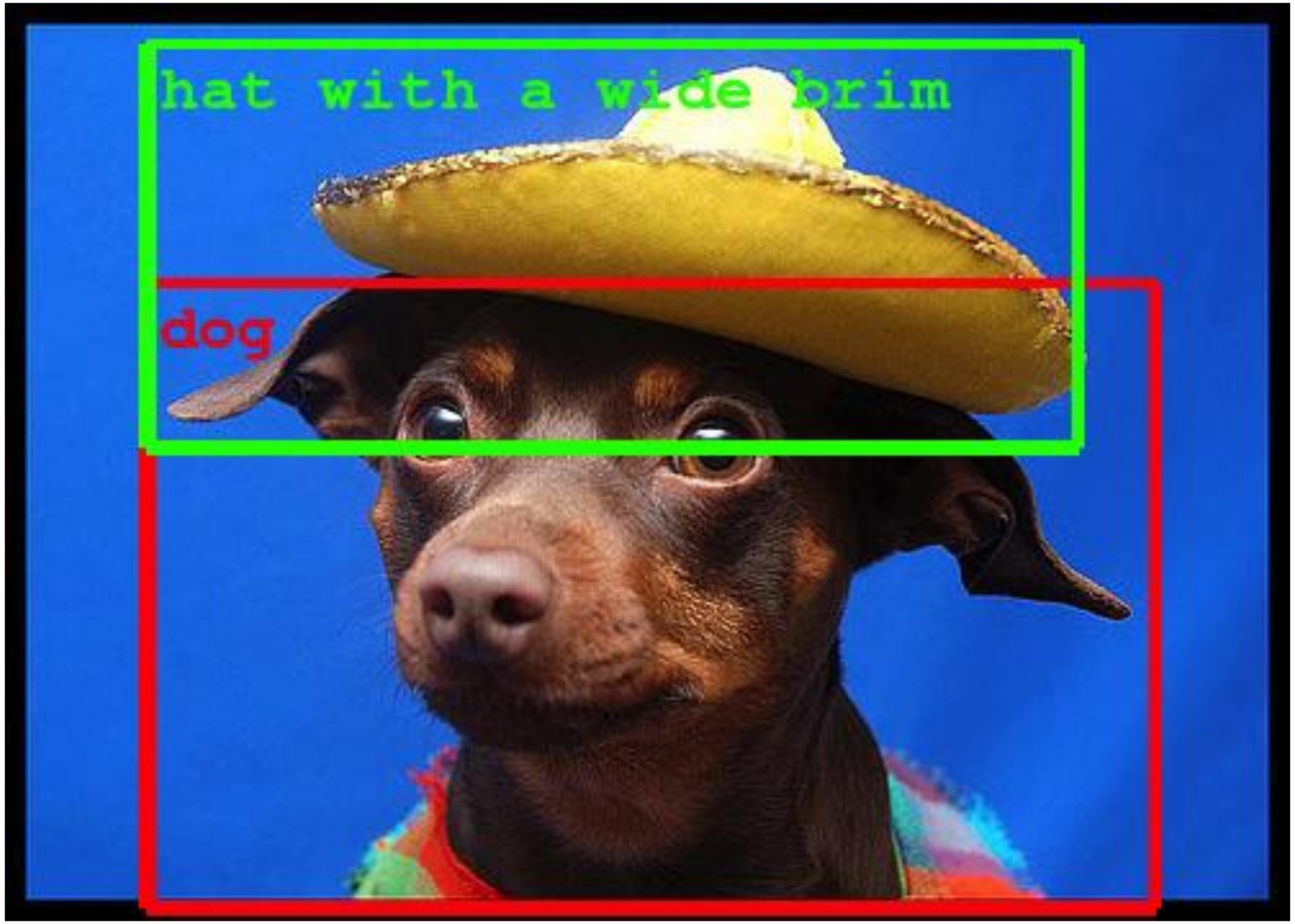


Image taken from google research

# Machine Learning Use Case: Automatic Machine Translation

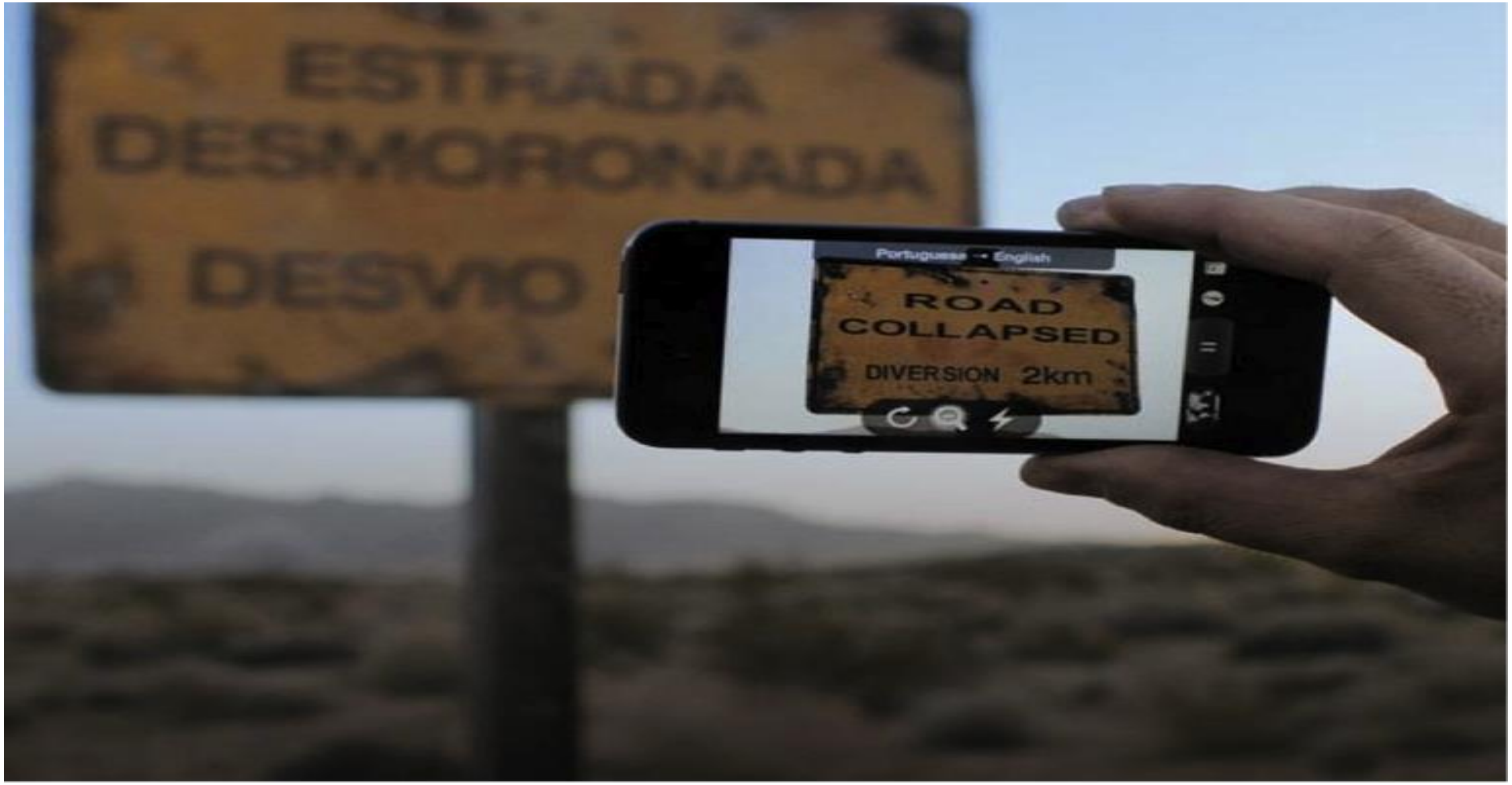
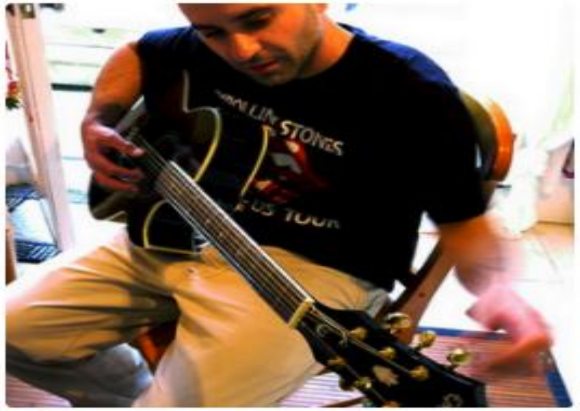
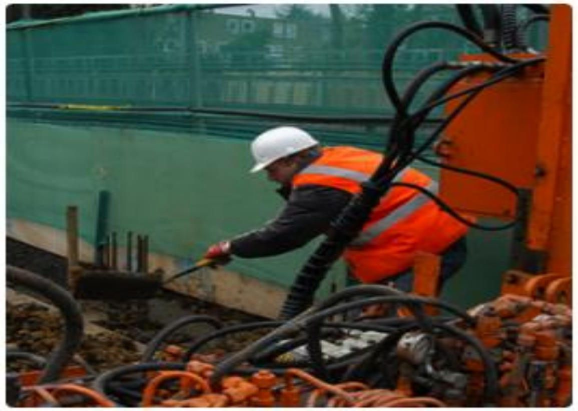


Image taken from google research

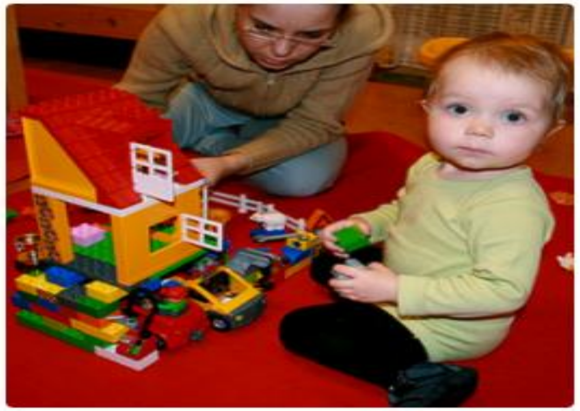
# Machine Learning Example: Automatic Image Caption Generation



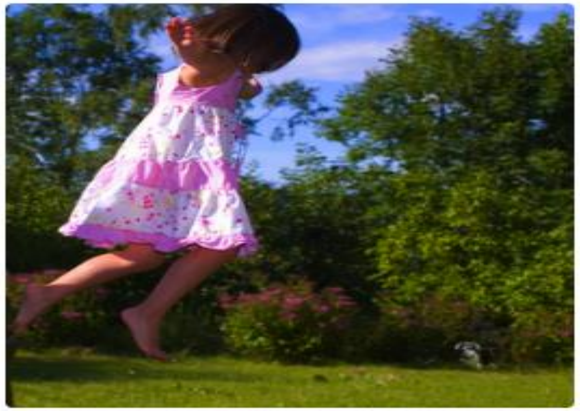
"man in black shirt is playing guitar."



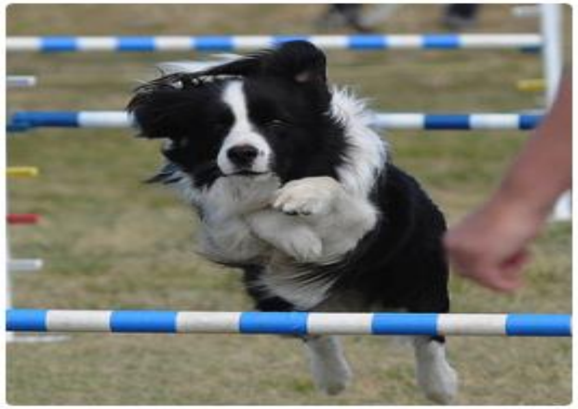
"construction worker in orange safety vest is working on road."



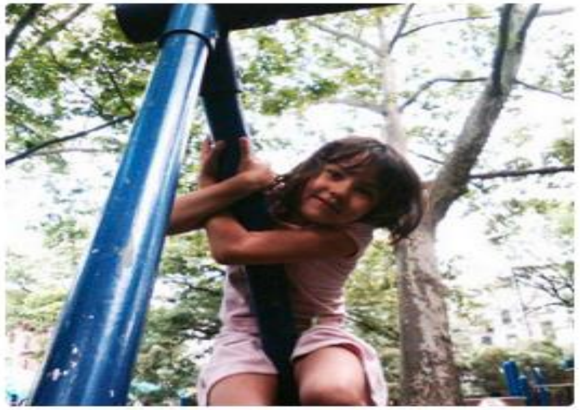
"two young girls are playing with lego toy."



"girl in pink dress is jumping in air."



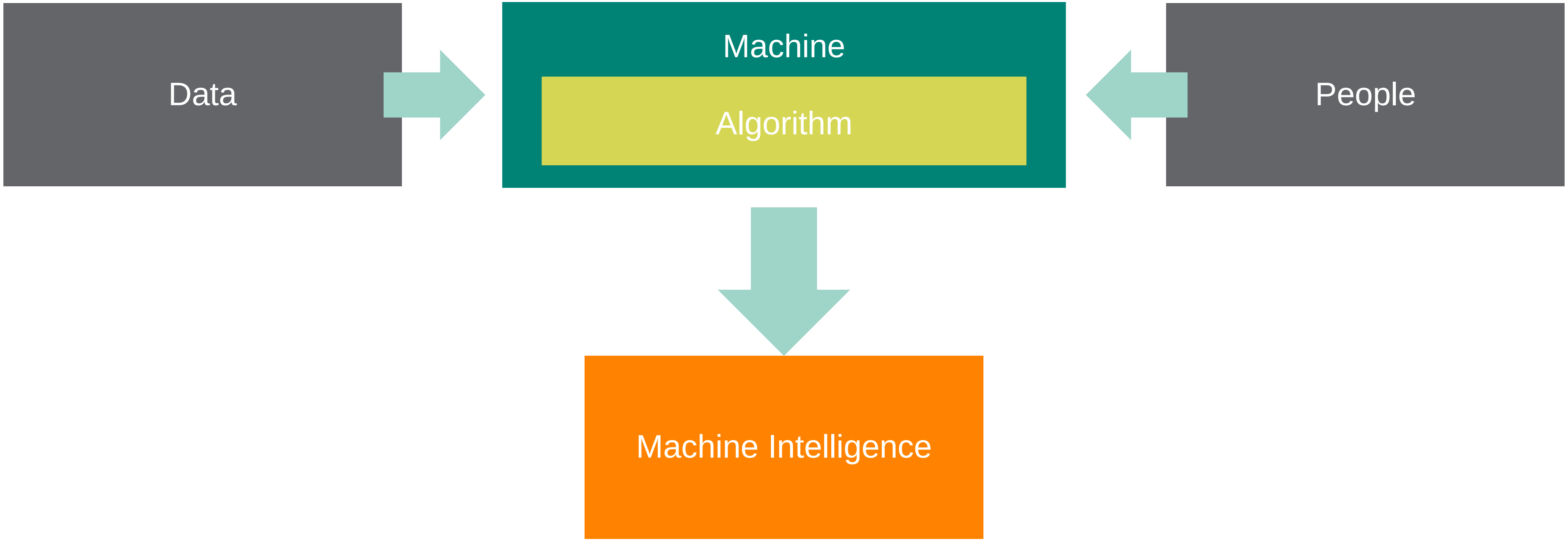
"black and white dog jumps over bar."



"young girl in pink shirt is swinging on swing."

Image taken from google research

# Machine Learning Ecosystem



Data

Machine

Algorithm

People

Machine Intelligence

# Outline

- Terms and Basics
- Machine Learning in Practice
- ***Applied Machine Learning in Enterprise Networking***

# Top Industries To Be Disrupted by Machine Learning

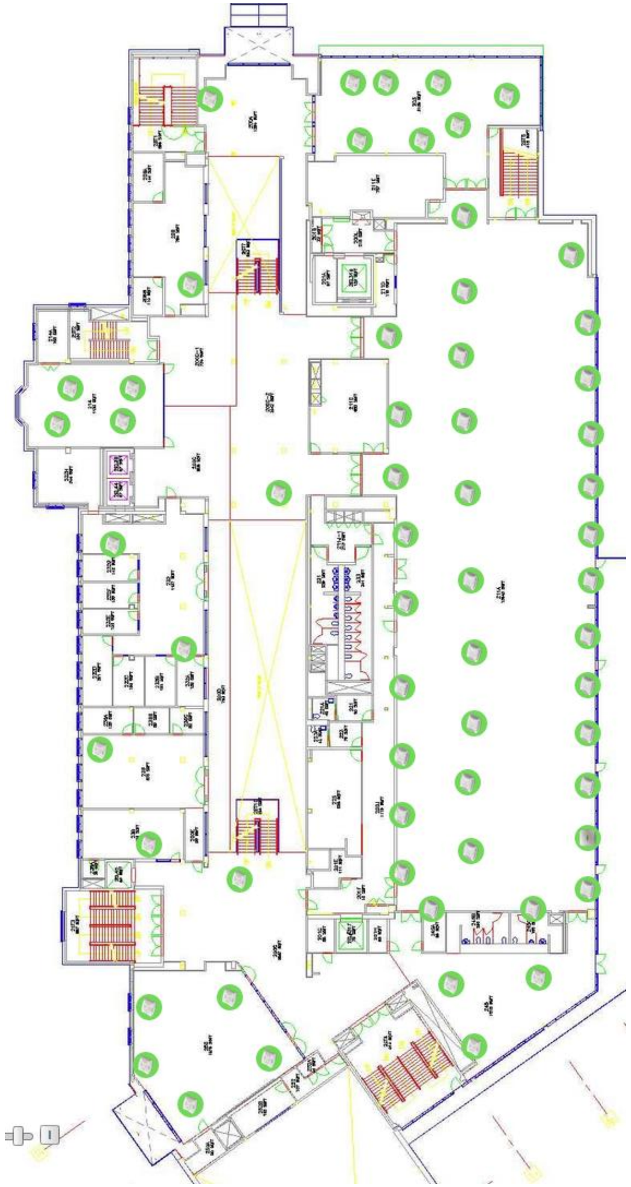
- Education
- Healthcare
- Transportation
- Financial Services
- Business and Marketing

# Top Industries To Be Disrupted by Machine Learning

- Education
- Healthcare
- Transportation
- Financial Services
- Business and Marketing
- ***Enterprise Networking***
  - ***Network Analytics: Rasa***
  - ***Security: Niara***

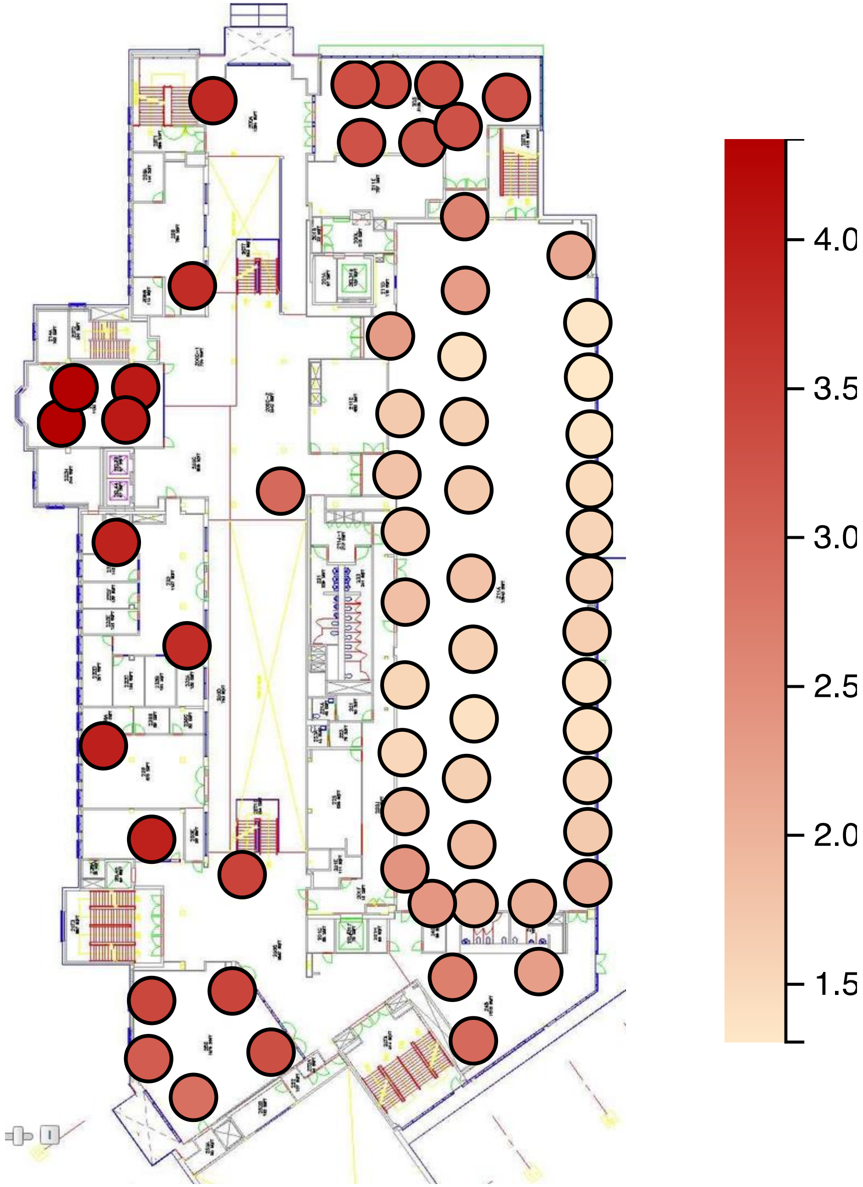
# Rasa: Environment Type Classification

# **Customer A – Building B** (Student Union)



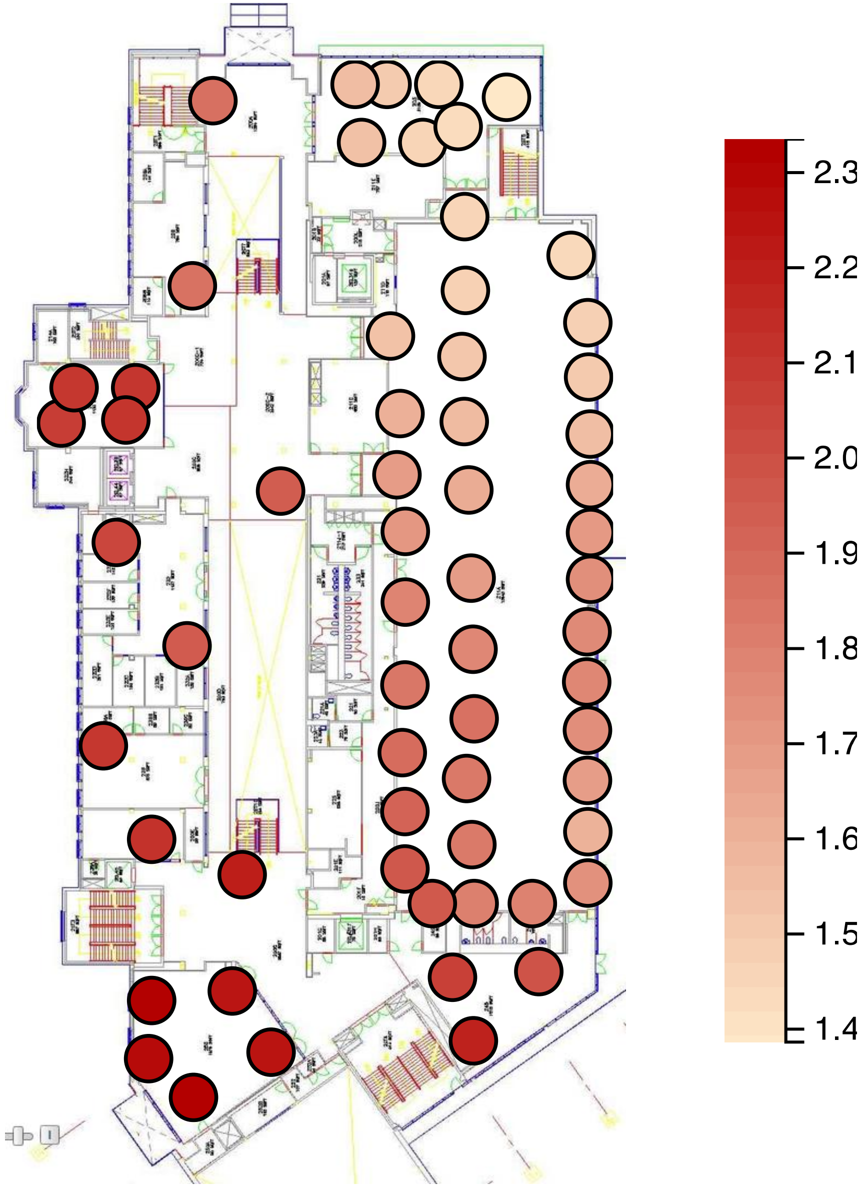
- Environment Measurements
  - Radio propagation
  - AP arrangement
  - User behavior
  - Traffic characteristics

# Customer A – Building B (Student Union)



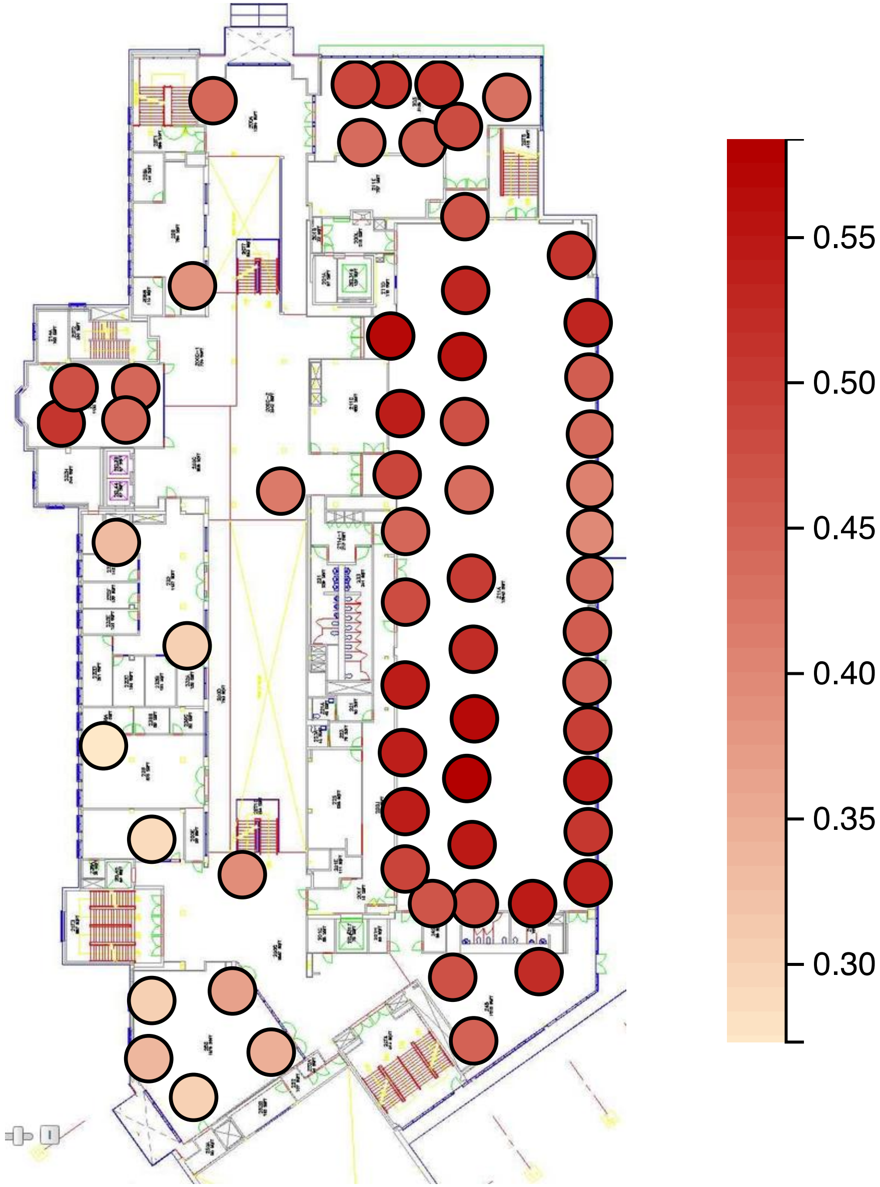
- Path loss exponent
  - Building materials
  - Room size
  - Occupancy

## **Customer A – Building B** (Student Union)



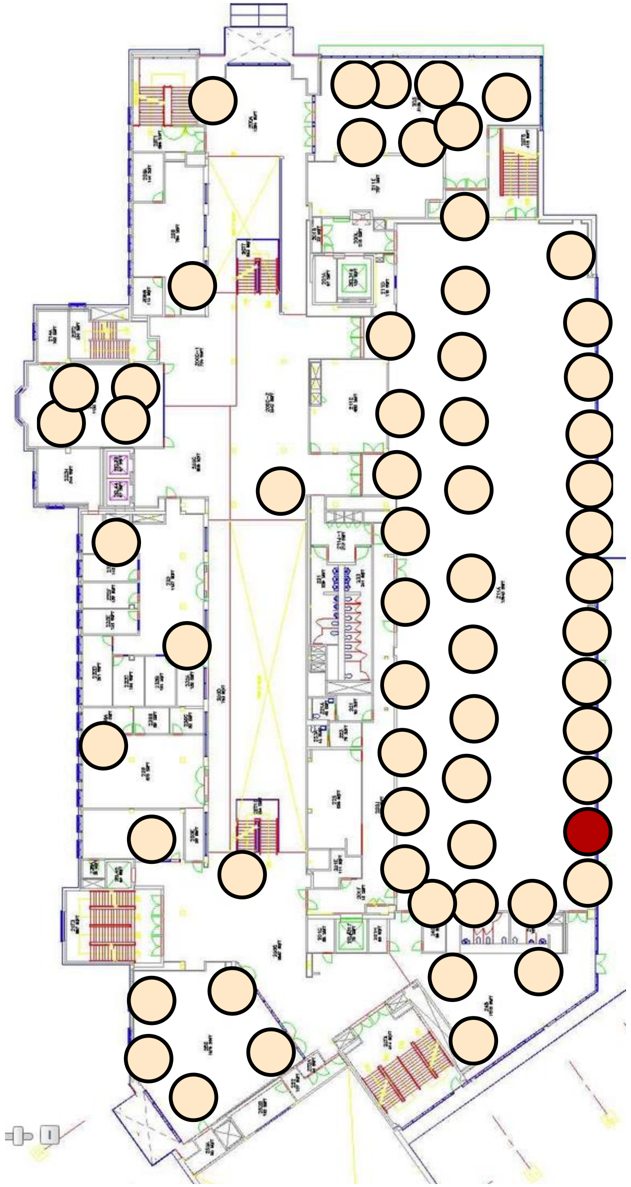
- Traffic per station
  - Application profile
  - User behavior

## Customer A – Building B (Student Union)



- Mobile ratio
  - User mobility behavior

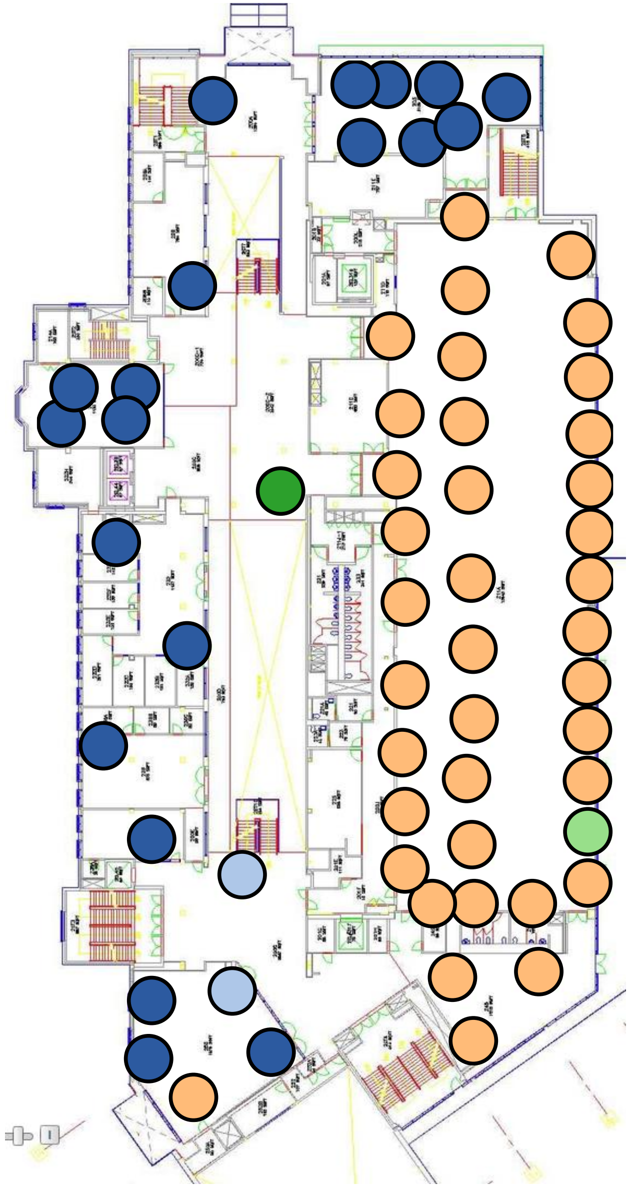
# **Customer A – Building B** (Student Union)



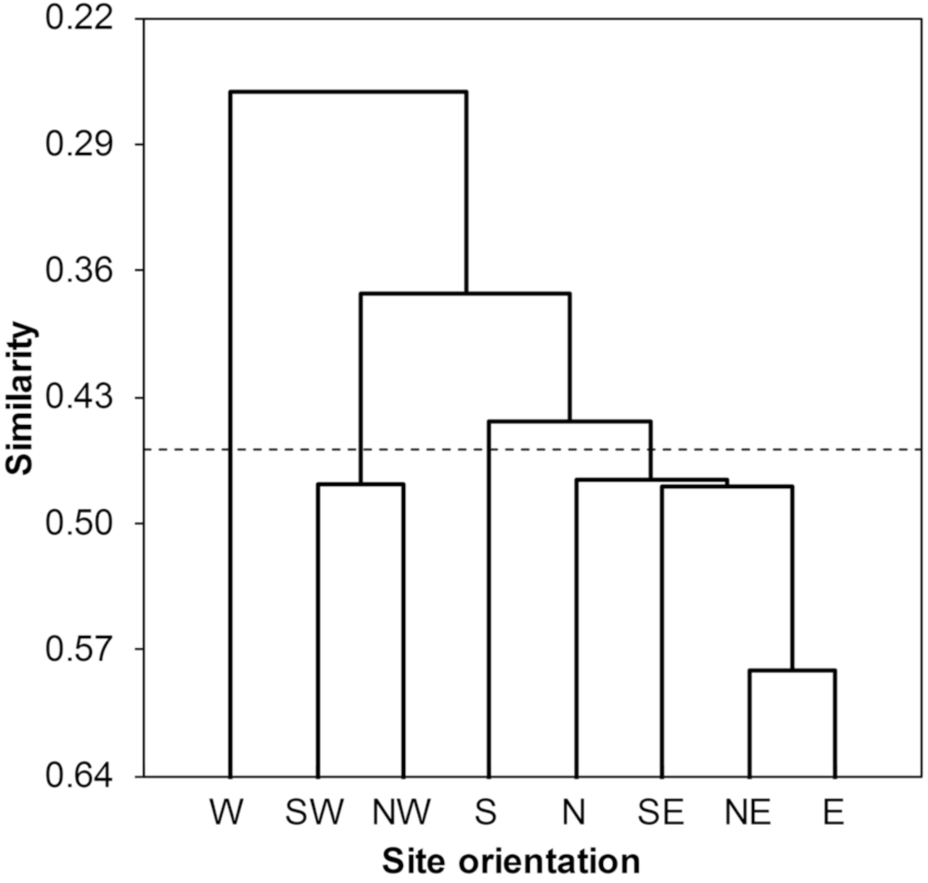
- 802.11 PHY Type
  - Deployment planning

emea atmosphere '17
THE innovation edge

# **Customer A – Building B** (Student Union)

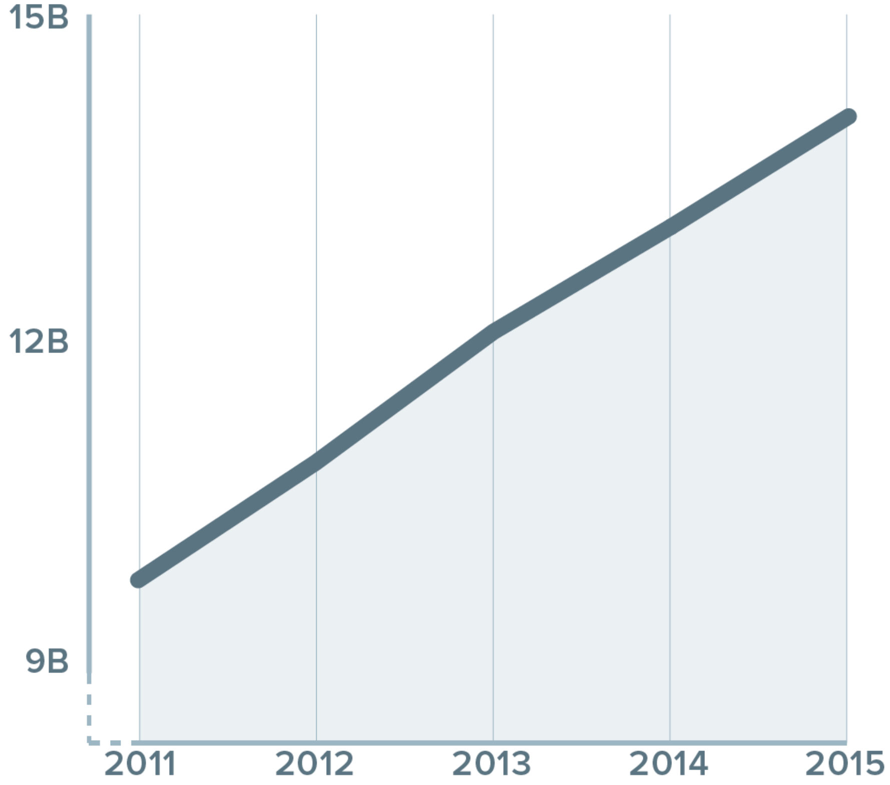


## Hierarchical Clustering



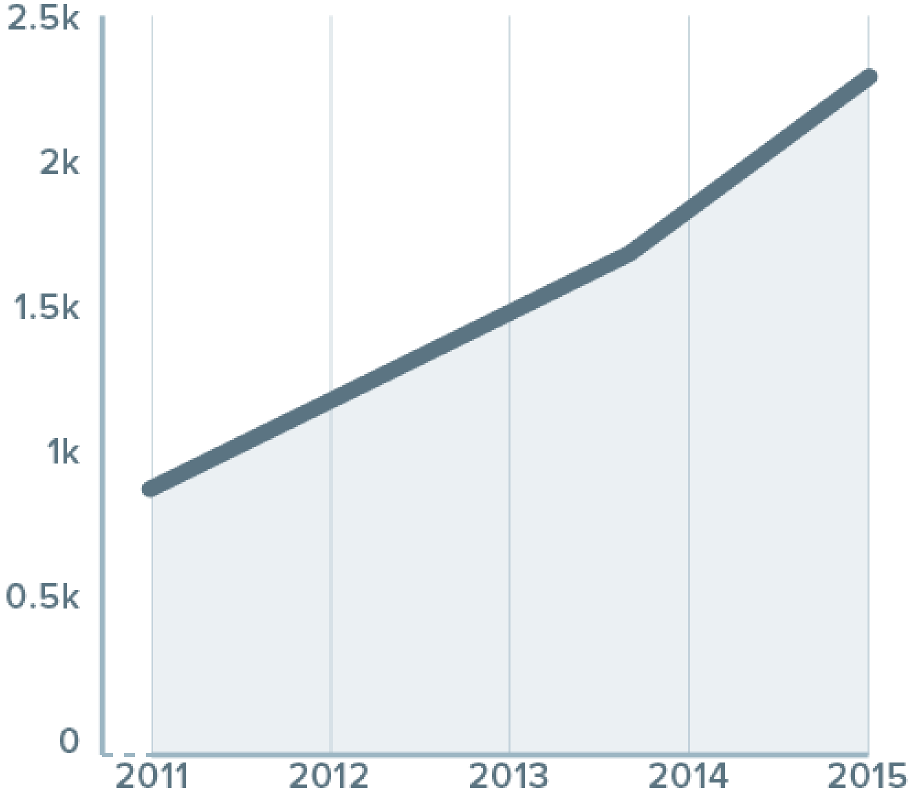
# Problem: The Security Gap

## SECURITY SPEND



PREVENTION & DETECTION (US $B)

## DATA BREACHES



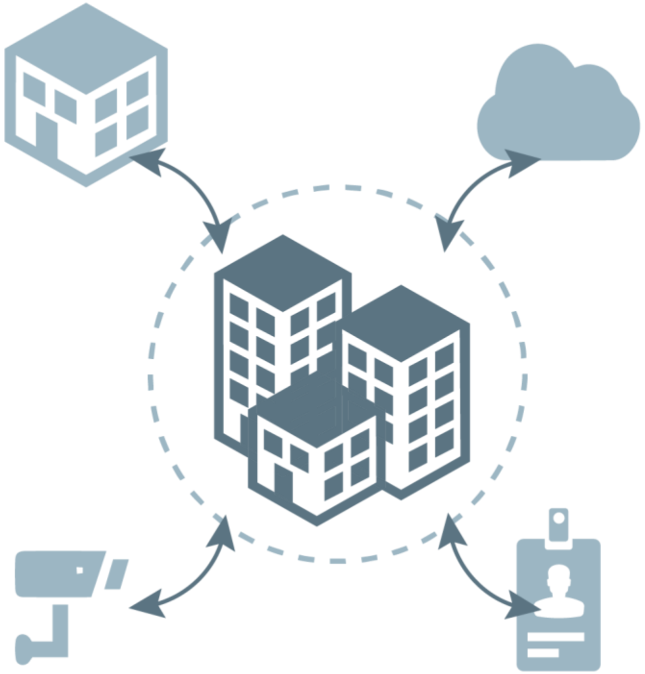
# BREACHES

emea atmosphere '17
THE innovation edge

# Problem: Cause of The Problem

## ATTACKERS

ARE QUICKLY INNOVATING & ADAPTING



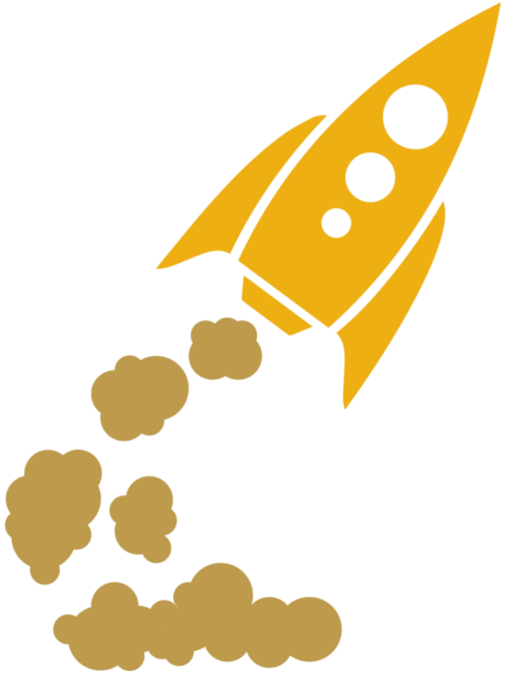
## BATTLEFIELD

WITH IOT AND CLOUD, SECURITY IS BORDERLESS

# Problem: Addressing The Cause

## ATTACKERS

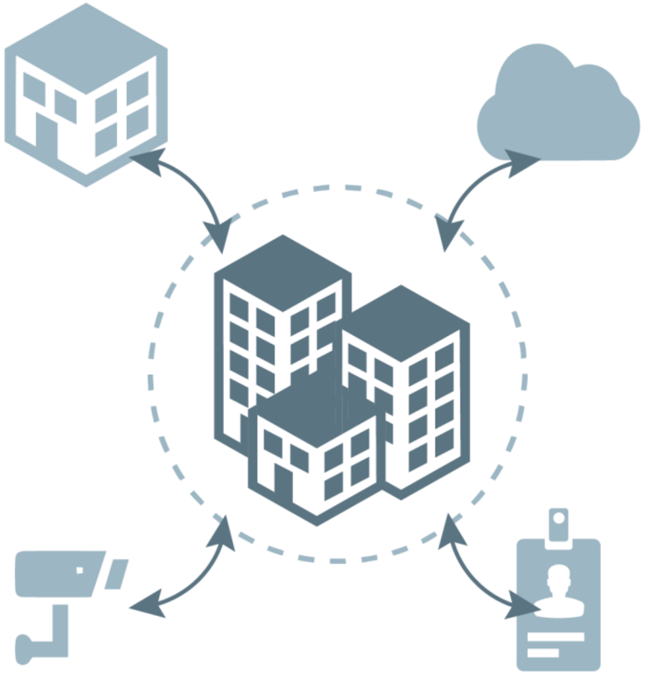
ARE QUICKLY INNOVATING & ADAPTING



## DEEP LEARNING

SOLUTIONS MUST BE RESPONSIVE TO CHANGES

# Problem: Addressing The Cause



## BATTLEFIELD

WITH IOT AND CLOUD, SECURITY IS BORDERLESS

## INSIDER BEHAVIOR

LOOK AT BEHAVIOR CHANGE OF INSIDE USERS AND MACHINES

# Niara: User & Entity Behavior Analytics (UEBA)

**MACHINE LEARNING** DRIVEN
**BEHAVIOR ANALYTICS** IS
A NEW WAY TO **COMBAT ATTACKERS**

1. **Machine driven, not only human driven**
2. **Detect compromised users, not only attackers**
3. **Post-infection detection, not only prevention**

# Real World Attacks Caught by Niara

## SCANNING ATTACK

scan servers in the data center to find out vulnerable targets

DETECTED WITH **AD LOGS**

## DATA DOWNLOAD

download data from internal document repository which is not typical for the host

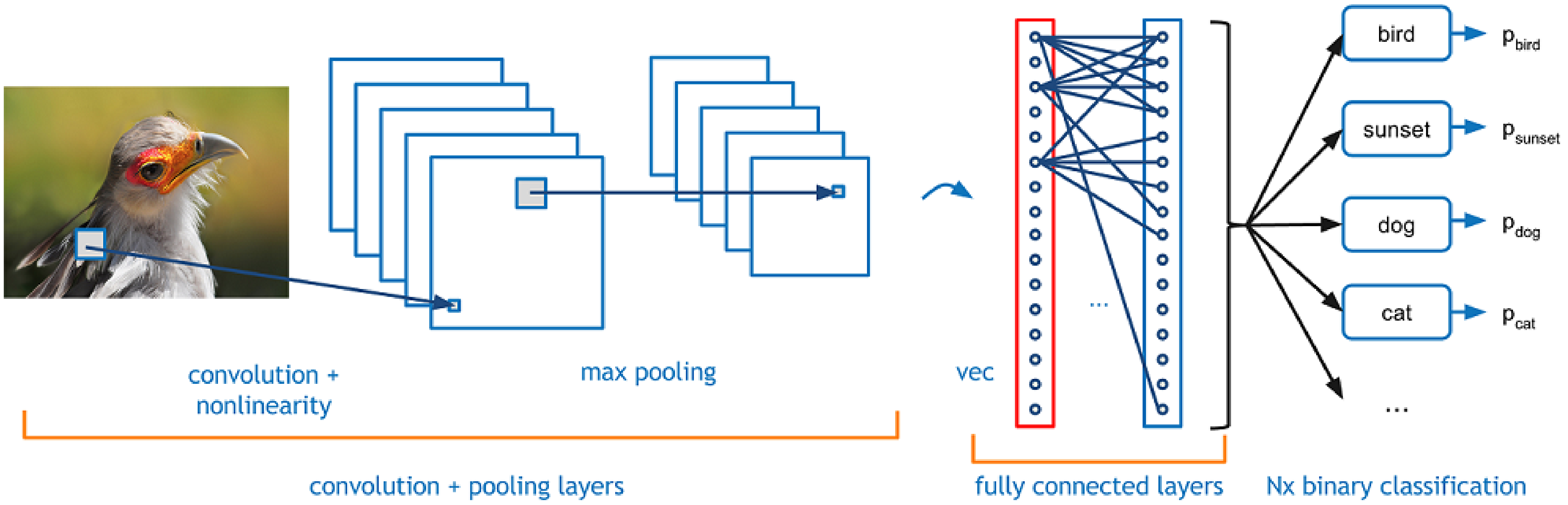
DETECTED WITH **NETWORK TRAFFIC**

## EXFILTRATION OF DATA

upload a large file to cloud server hosted in new country never accessed before

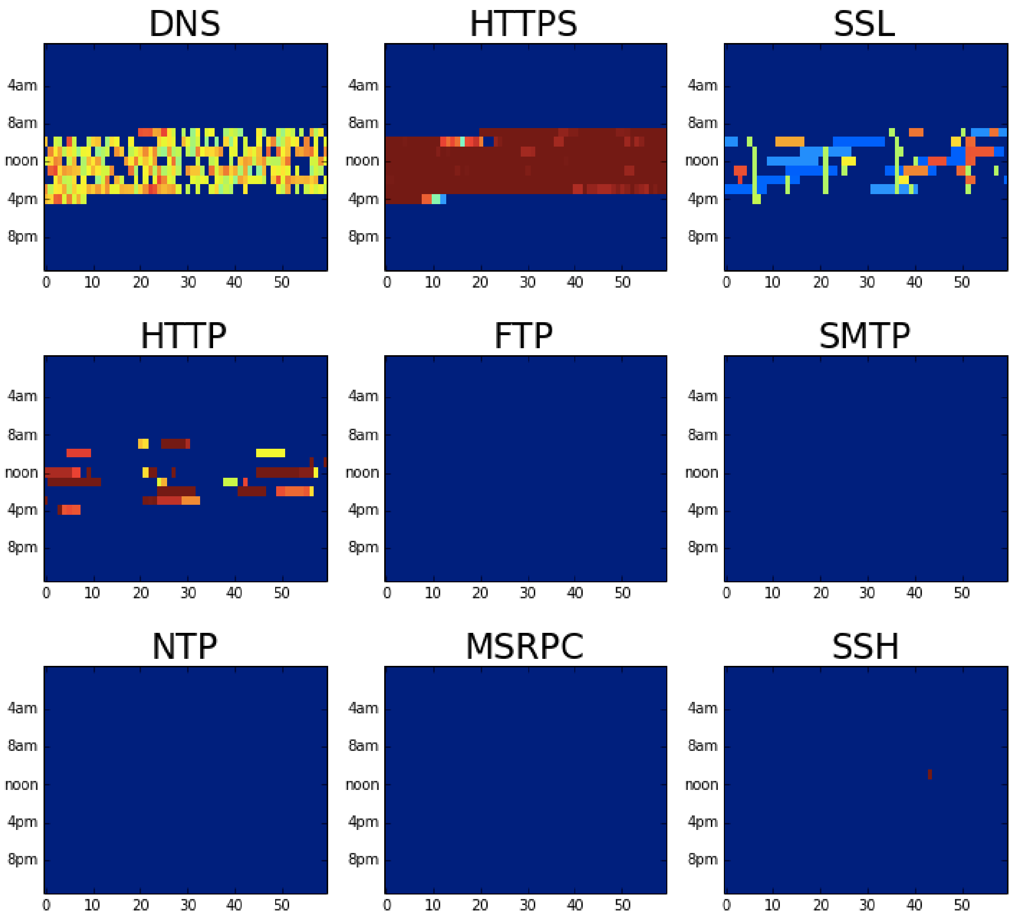
DETECTED WITH **WEB PROXY LOGS**

# Convolutional Neural Network: Object Fingerprinting

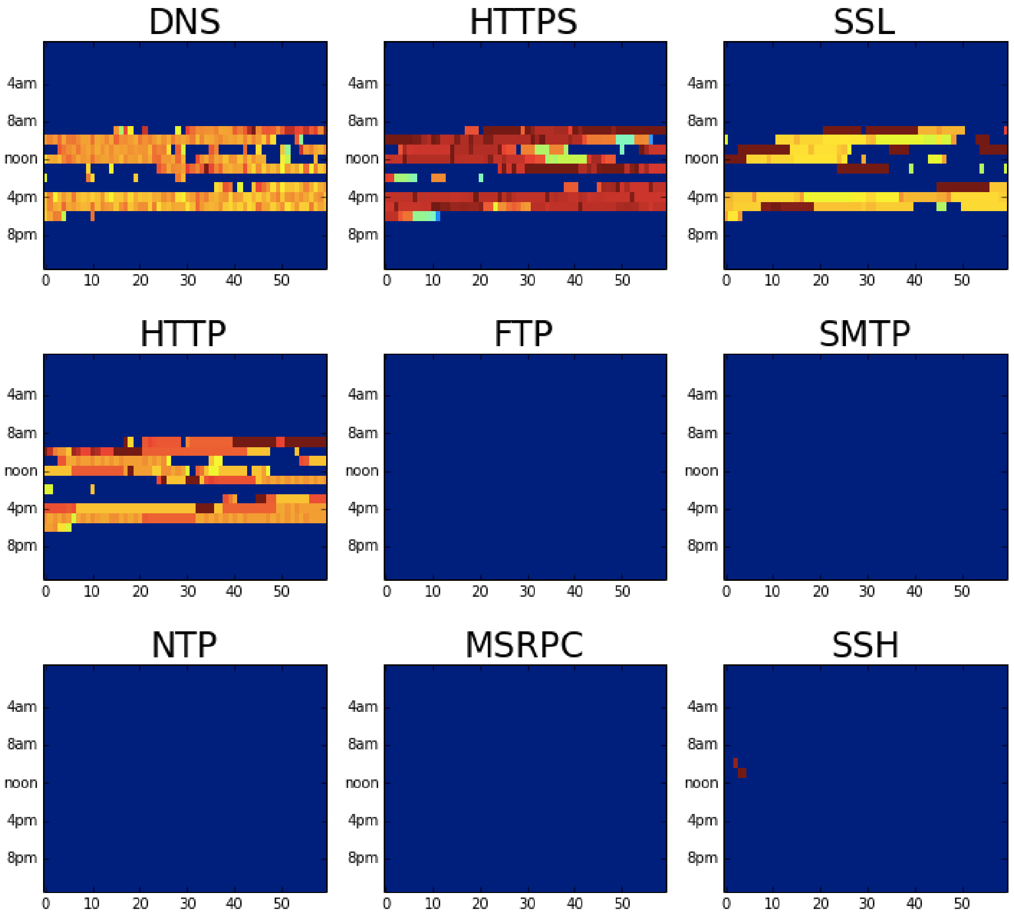


# User Behavior Fingerprinting

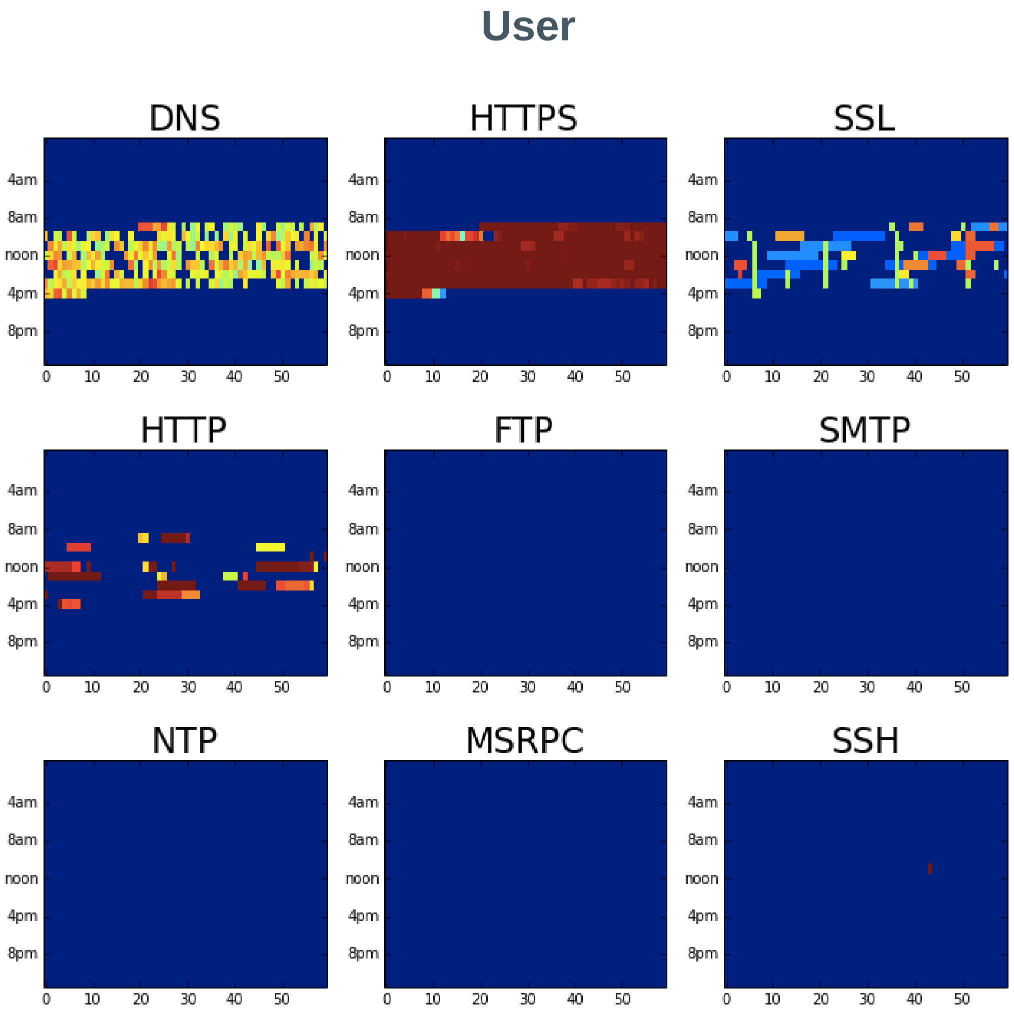
## User 1

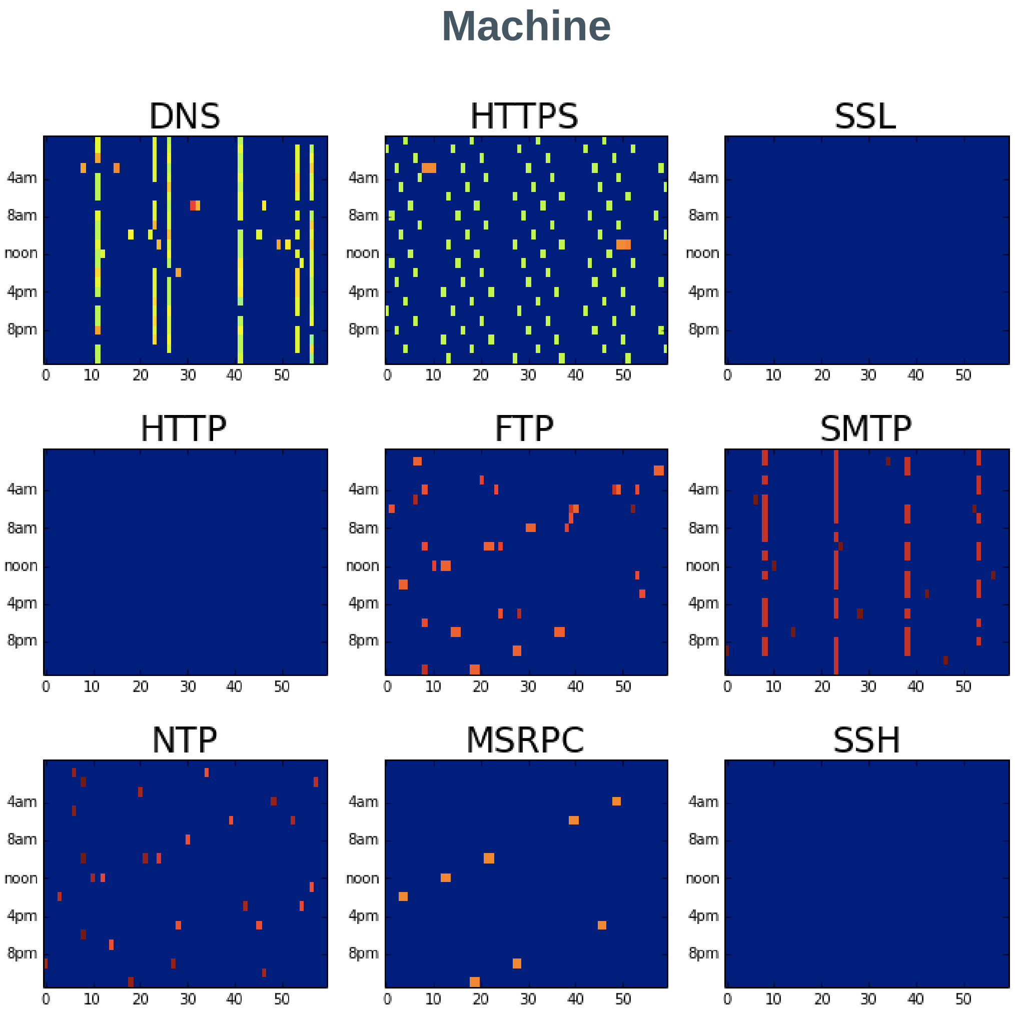


## User 2



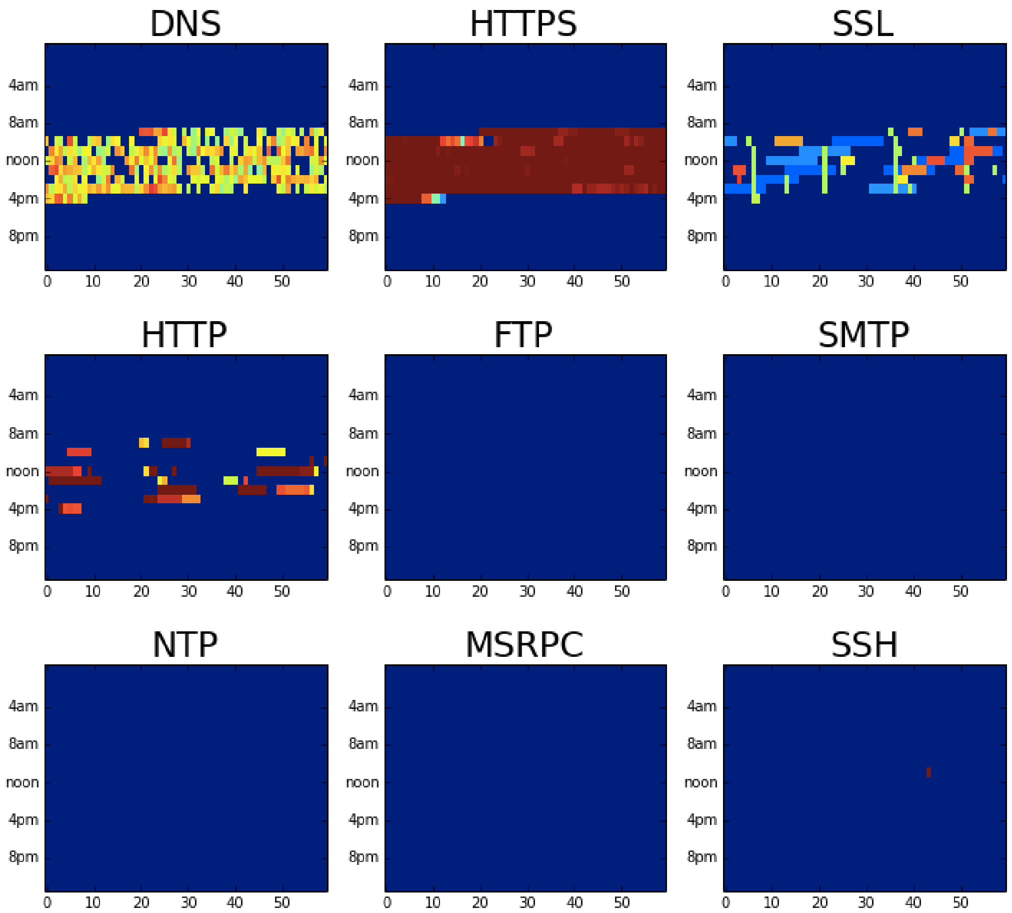
# Machine Behavior Fingerprinting



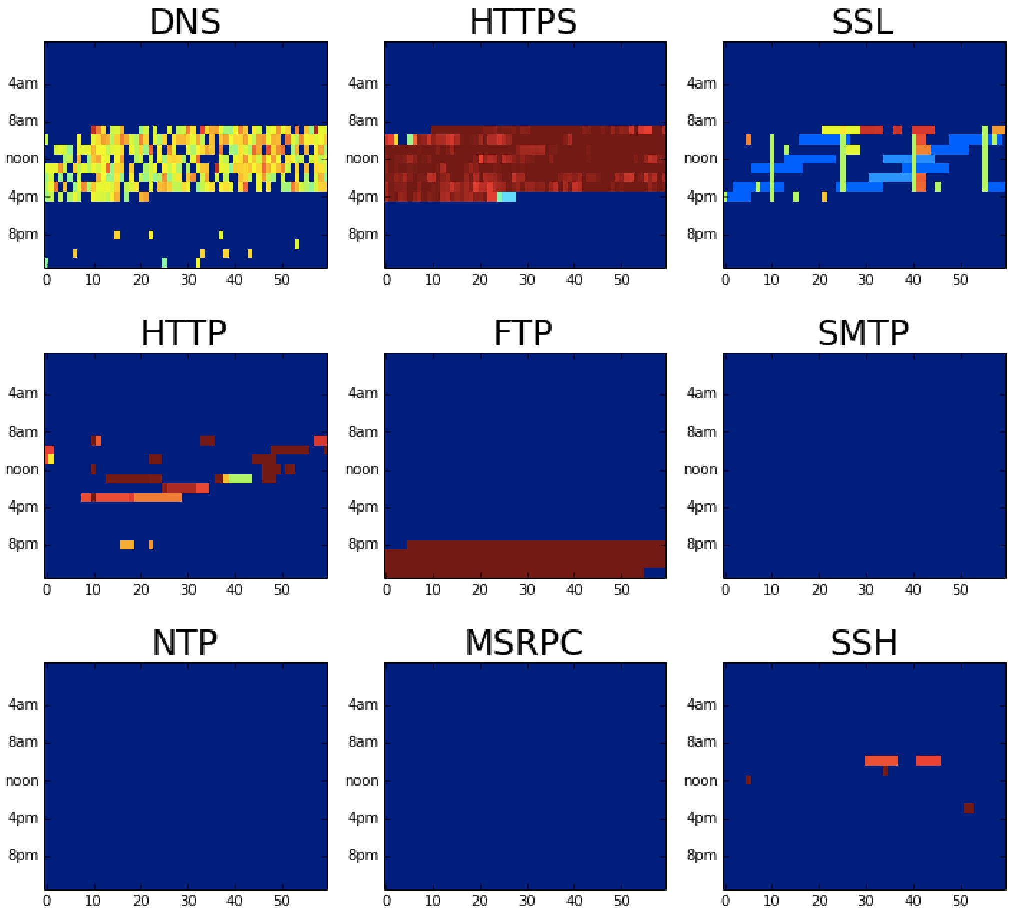


# Behavior Anomaly Detection: Compromised User

## User – Before Compromise

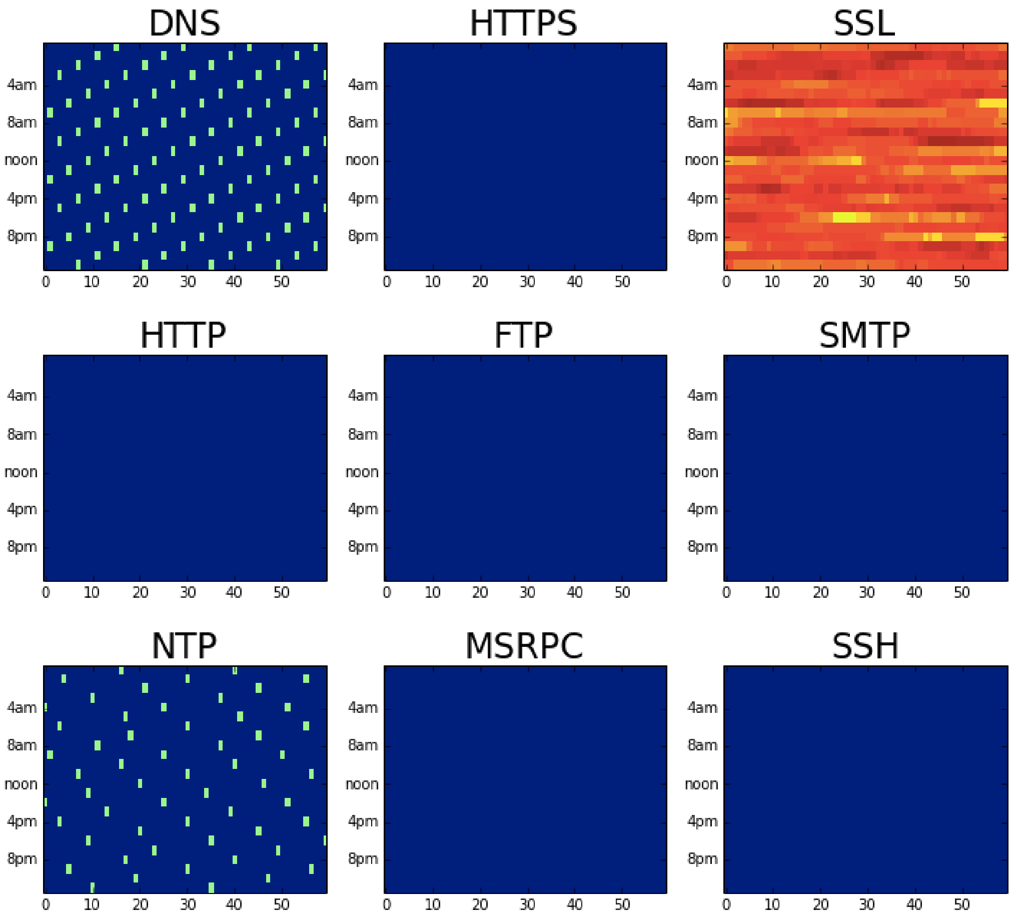


## User – Post Compromise

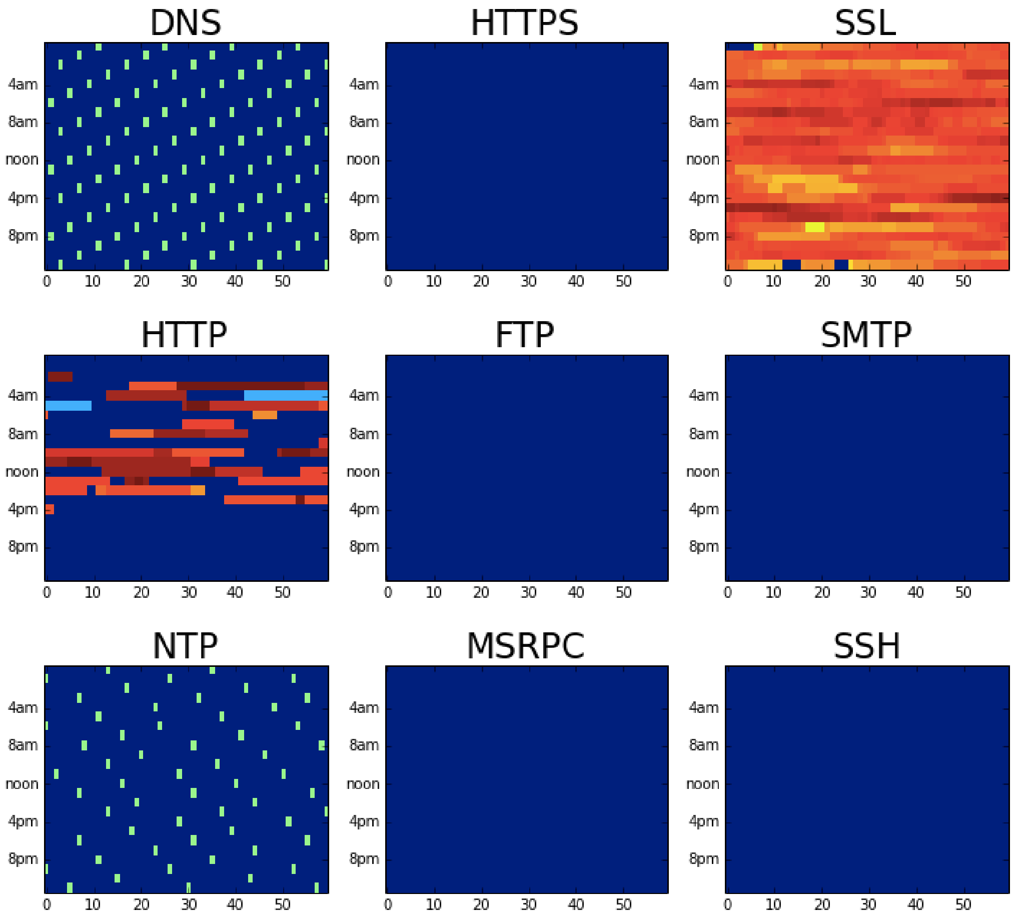


# Behavior Anomaly Detection: Compromised IoT Device

## Dropcam – Before Compromise



## Dropcam – Post Compromise



# Outline

- Terms and Basics
- Machine Learning in Practice
- Applied Machine Learning in Enterprise Networking

# THANK YOU!