Deep Learning In Security

An Empirical Example in User & Entity Behavior Analytics (UEBA)

Jisheng Wang

June 7, 2017

aruba
a Hewlett Packard Enterprise company

ME, NIARA, HPE

aruba
a Hewlett Packard Enterprise company

- **Jisheng Wang, Senior Director of Data Science, CTO Office, Aruba / HPE**
  - Over 12-year experiences: Machine Learning + Big Data => Security
  - Chief Scientist, Niara, lead overall data analytics innovation and development
  - Ph.D from Penn State, Technical Lead in Cisco

- **Niara – a Hewlett Packard Enterprise company**
  - Recognized leader by Gartner in User and Entity Behavior Analytics (UEBA)
  - Re-invent enterprise security using big data and data science
  - Acquired by Aruba, a Hewlett Packard Enterprise company in Feb, 2017

USER & ENTITY BEHAVIOR ANALYTICS

aruba
a Hewlett Packard Enterprise company

UEBA SECURITY

why this matters

UEBA SOLUTION

how to detect attacks before damage is done

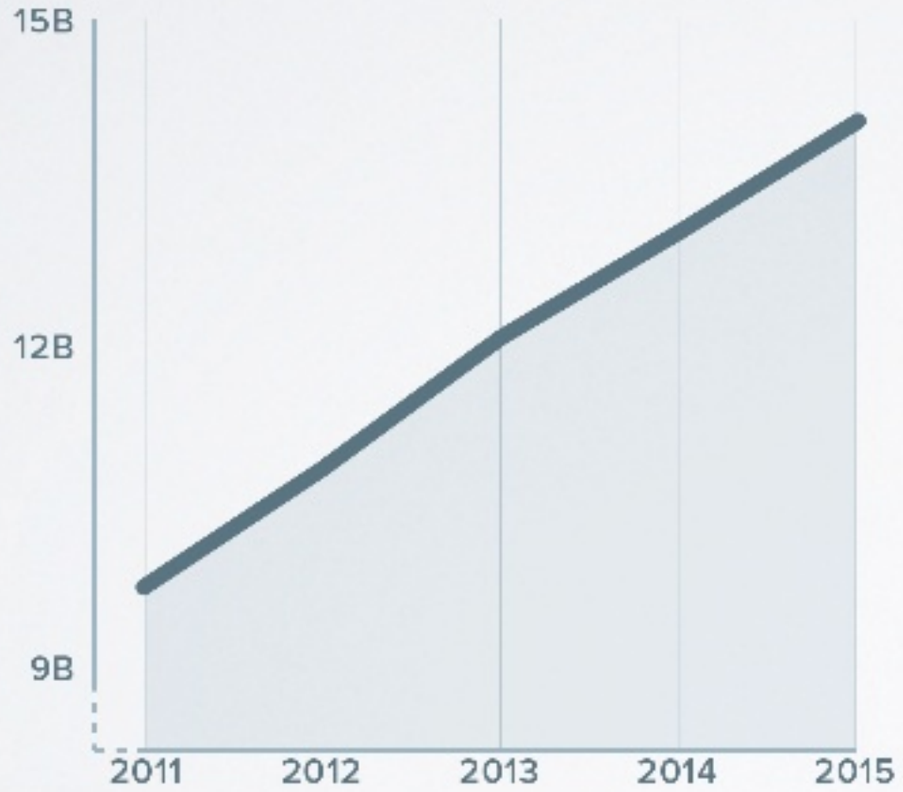
BEYOND DEEP LEARNING

how to build a comprehensive solution

PROBLEM THE SECURITY GAP

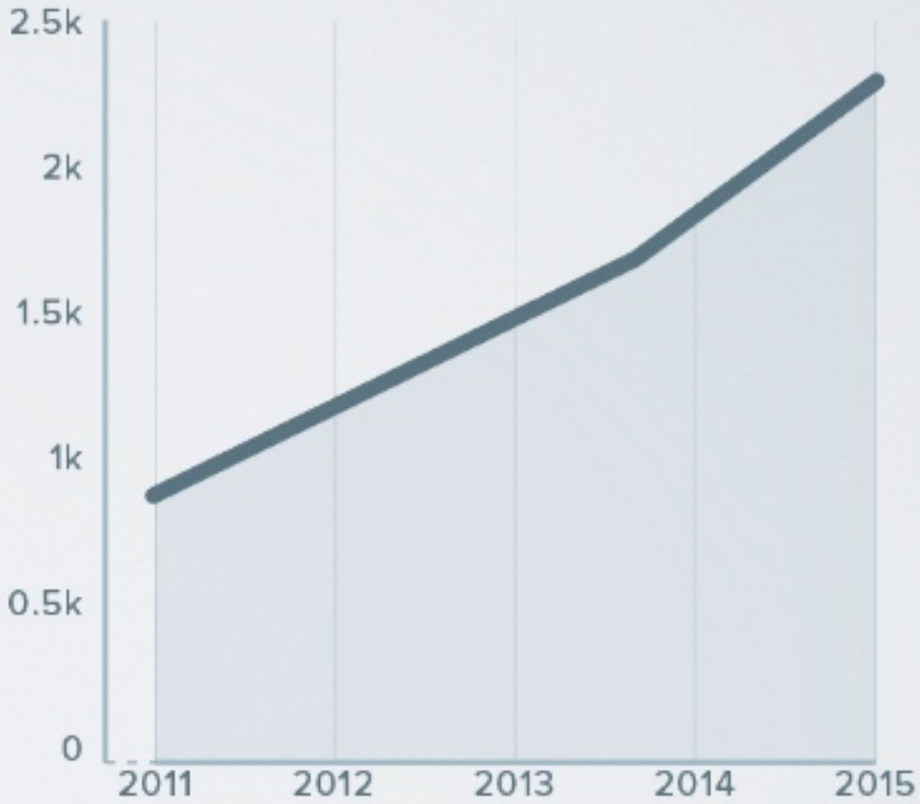
aruba
a Hewlett Packard Enterprise company

SECURITY SPEND



PREVENTION & DETECTION (US $B)

DATA BREACHES



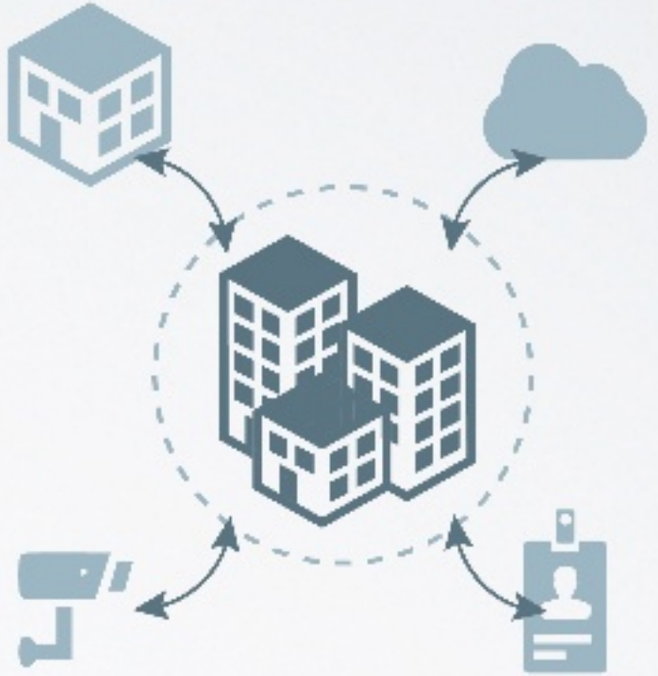
BREACHES

PROBLEM CAUSE OF THE GAP

aruba
a Hewlett Packard Enterprise company

ATTACKERS

ARE QUICKLY INNOVATING & ADAPTING



BATTLEFIELD

WITH IOT AND CLOUD, SECURITY IS BORDERLESS

PROBLEM ADDRESSING THE CAUSE

aruba
a Hewlett Packard Enterprise company

ATTACKERS

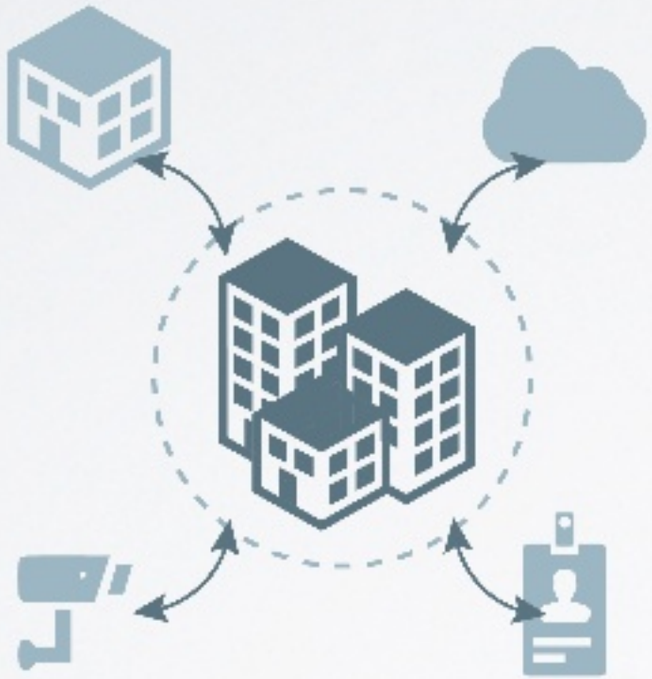
ARE QUICKLY INNOVATING & ADAPTING

DEEP LEARNING

SOLUTIONS MUST BE RESPONSIVE TO CHANGES

PROBLEM ADDRESSING THE CAUSE

aruba
a Hewlett Packard Enterprise company



BATTLEFIELD

WITH IOT AND CLOUD, SECURITY
IS BORDERLESS

INSIDER BEHAVIOR

LOOK AT BEHAVIOR CHANGE OF
INSIDE USERS AND MACHINES

USER & ENTITY BEHAVIOR ANALYTICS (UEBA)

aruba
a Hewlett Packard Enterprise company

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 NEWS WORTHY EXAMPLES

aruba
a Hewlett Packard Enterprise company

COMPROMISED

40 million credit cards were stolen from Target's severs

STOLEN CREDENTIALS

MALICIOUS

Edward Snowden stole more than 1.7 million classified documents

INTENTED TO LEAK INFORMATION

NEGLIGENT

DDoS attack from 10M+ hacked home devices took down major websites

ALL USED THE SAME PASSWORD

USER & ENTITY BEHAVIOR ANALYTICS

aruba
a Hewlett Packard Enterprise company

UEBA SECURITY

why this matters

UEBA SOLUTION

how to detect attacks before damage is done

BEYOND DEEP LEARNING

how to build a comprehensive solution

REAL WORLD ATTACKS CAUGHT BY NIARA

aruba
a Hewlett Packard Enterprise company

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

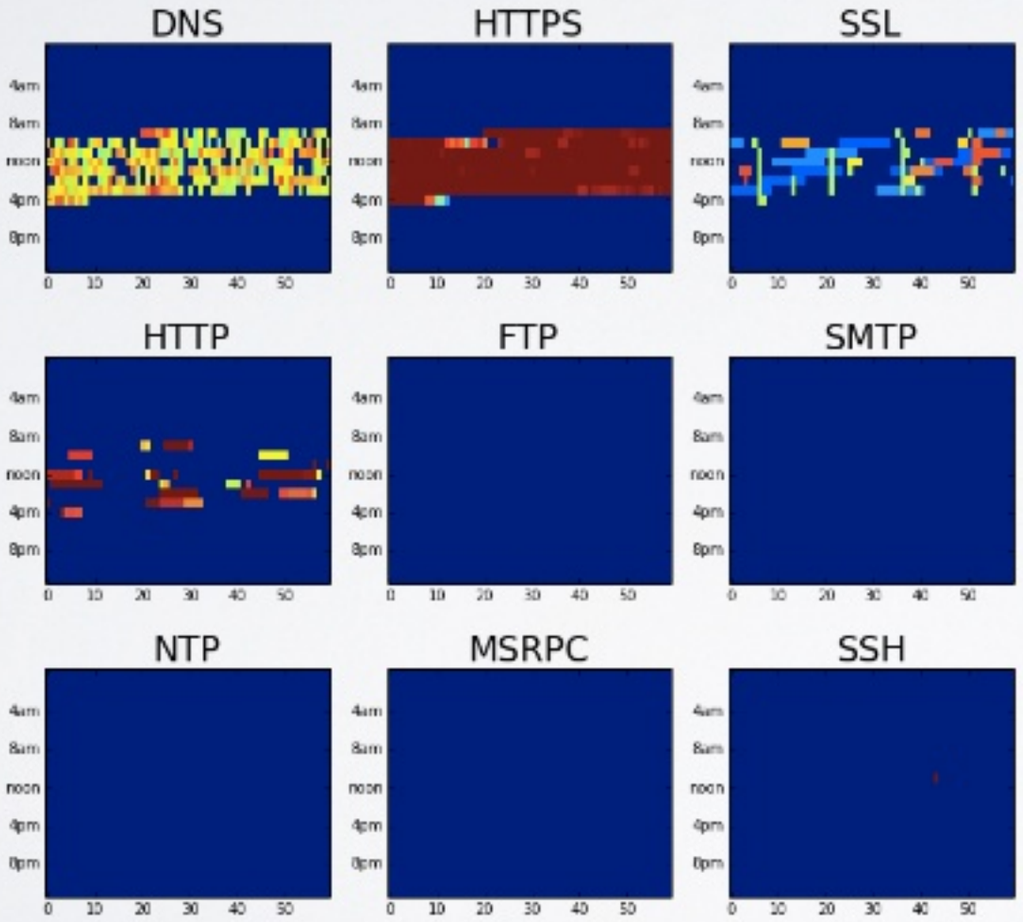
upload a large file to cloud server hosted in new country never accessed before

DETECTED WITH **WEB PROXY LOGS**

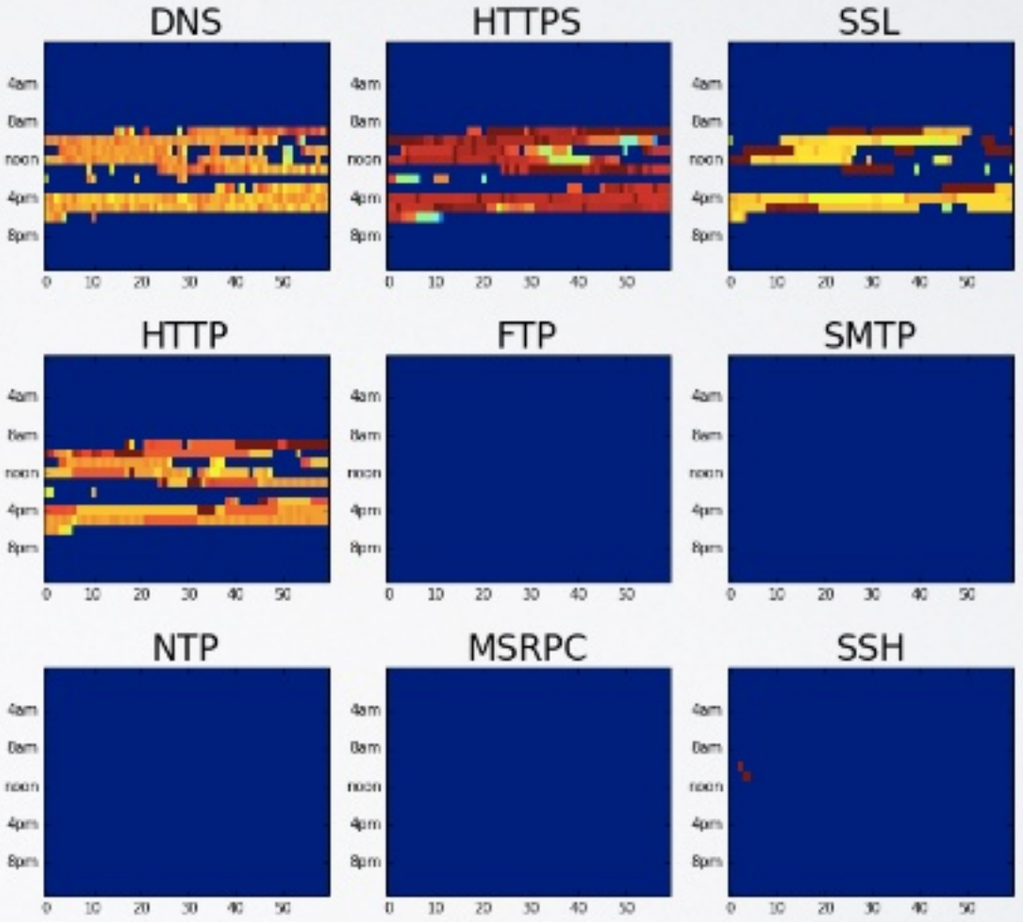
BEHAVIOR ENCODING USERS

aruba
a Hewlett Packard Enterprise company

User 1

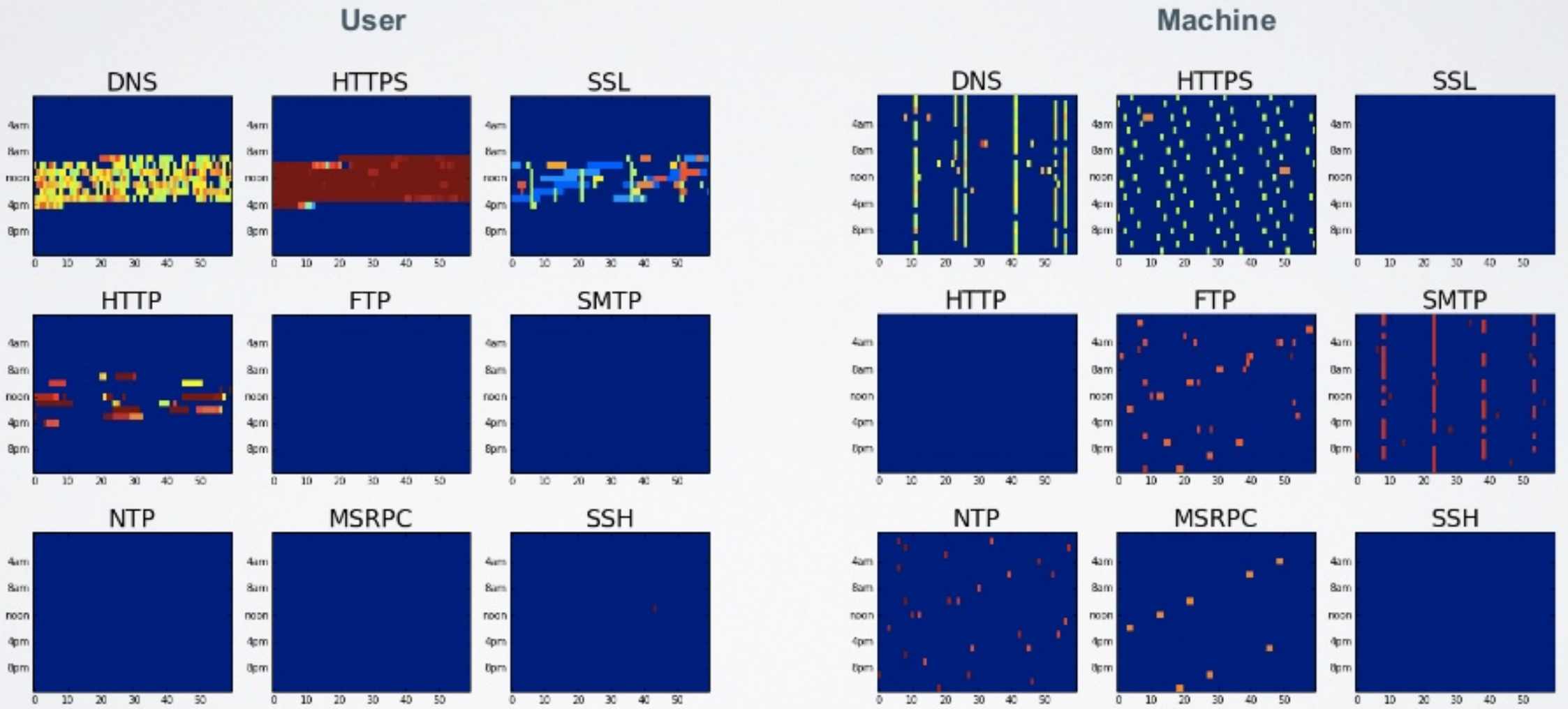


User 2

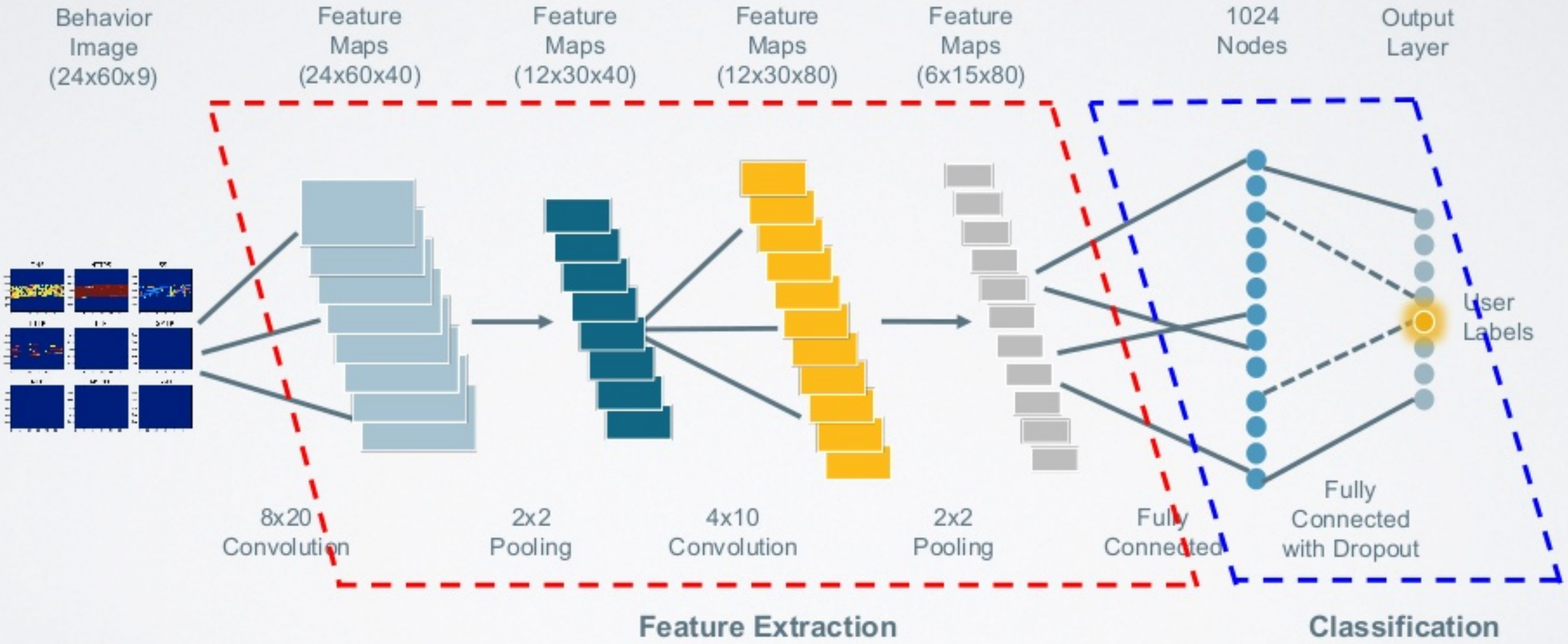


BEHAVIOR ENCODING USER VS MACHINE

aruba
a Hewlett Packard Enterprise company

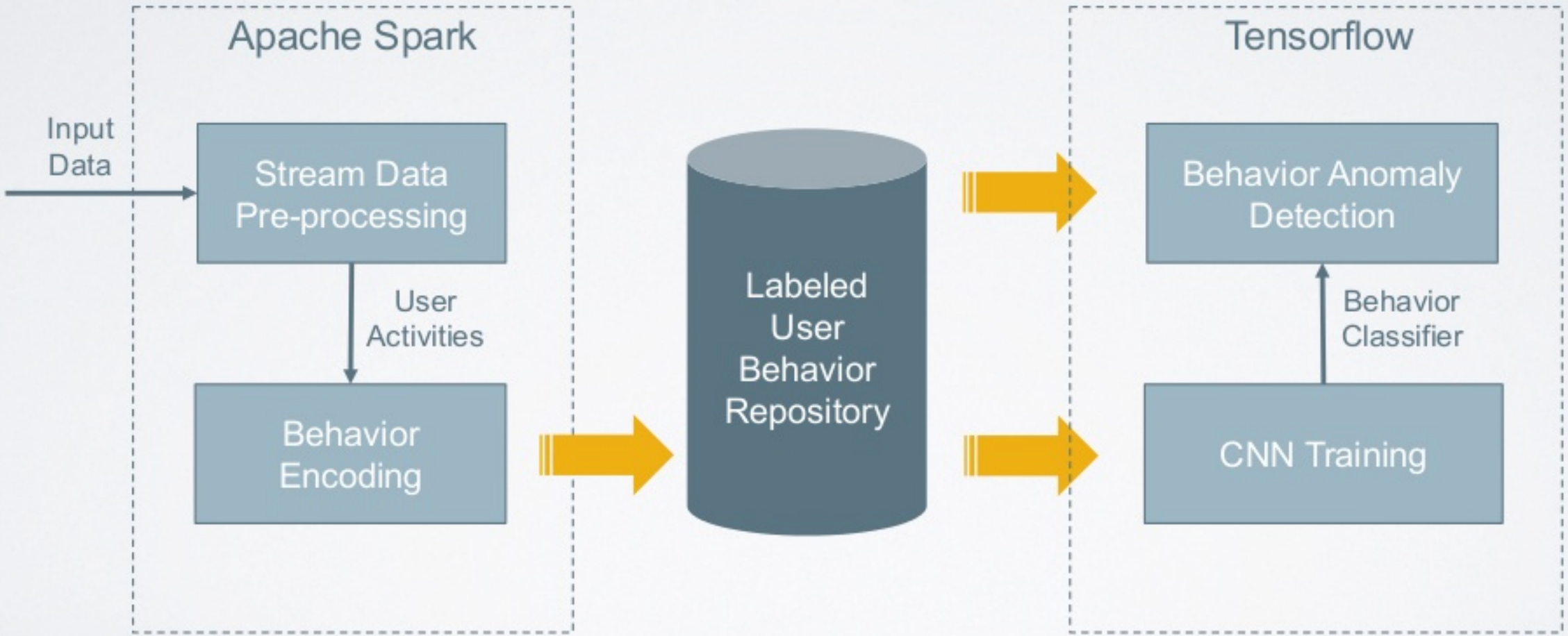


ANOMALY DETECTION CONVOLUTIONAL NEURAL NETWORK (CNN)



ANOMALY DETECTION ARCHITECTURE

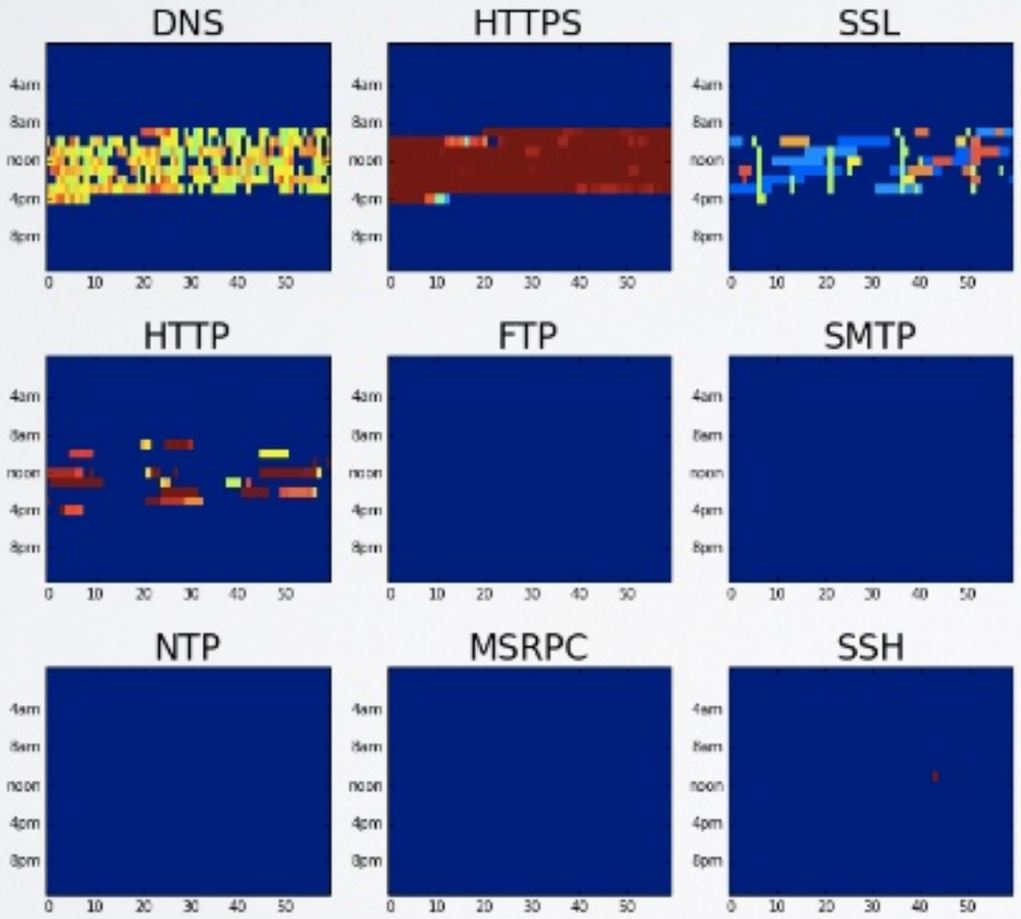
aruba
a Hewlett Packard Enterprise company



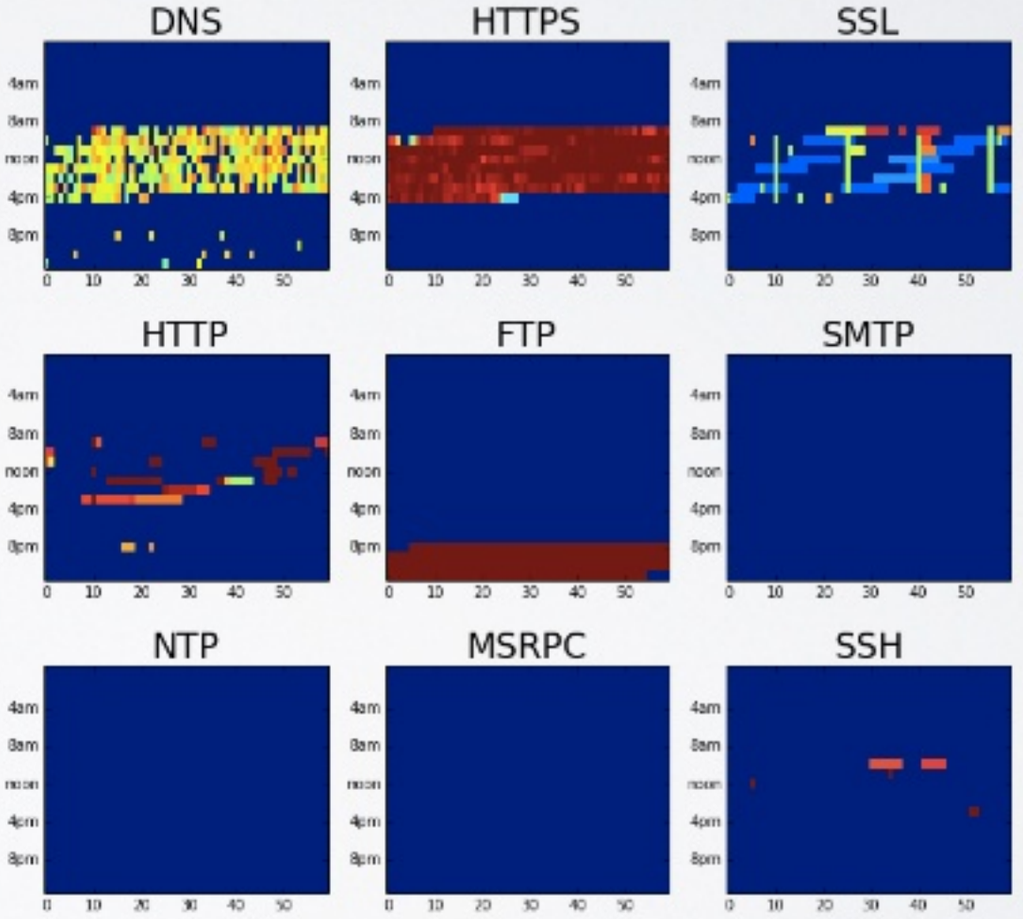
BEHAVIOR ANOMALY USER | EXFILTRATION

aruba
a Hewlett Packard Enterprise company

User – Before Compromise



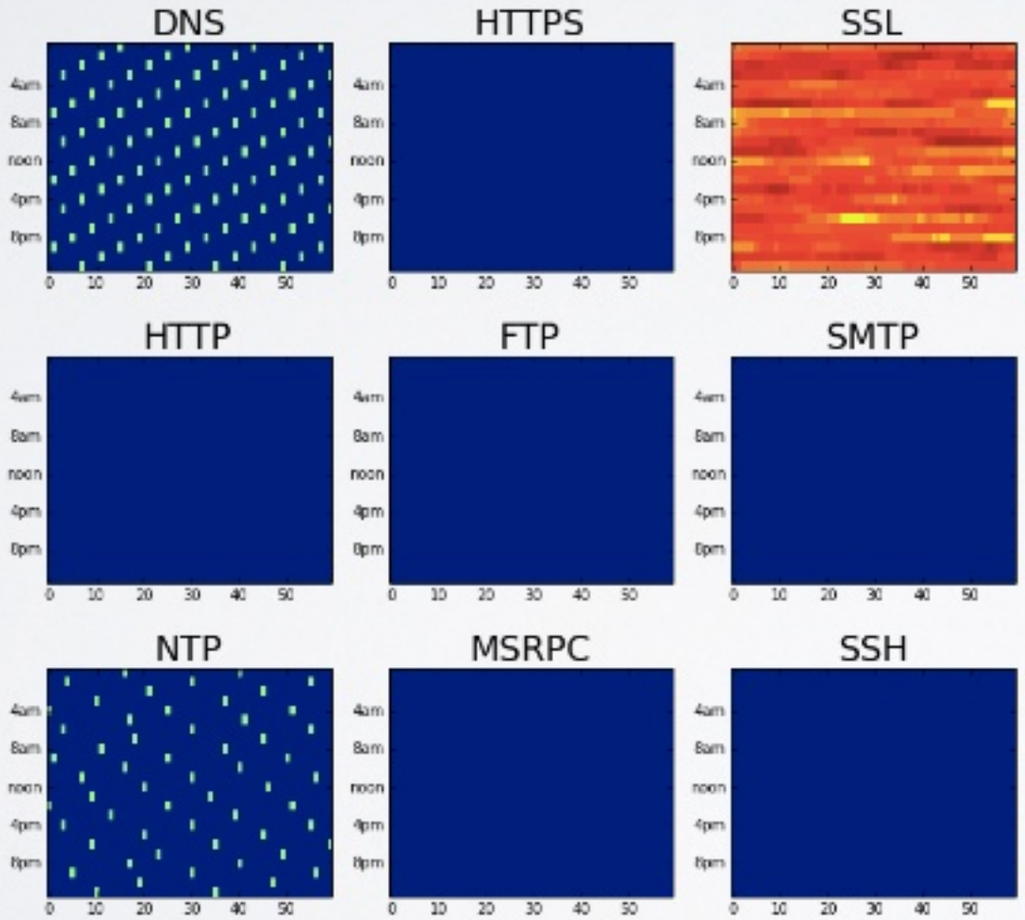
User – Post Compromise



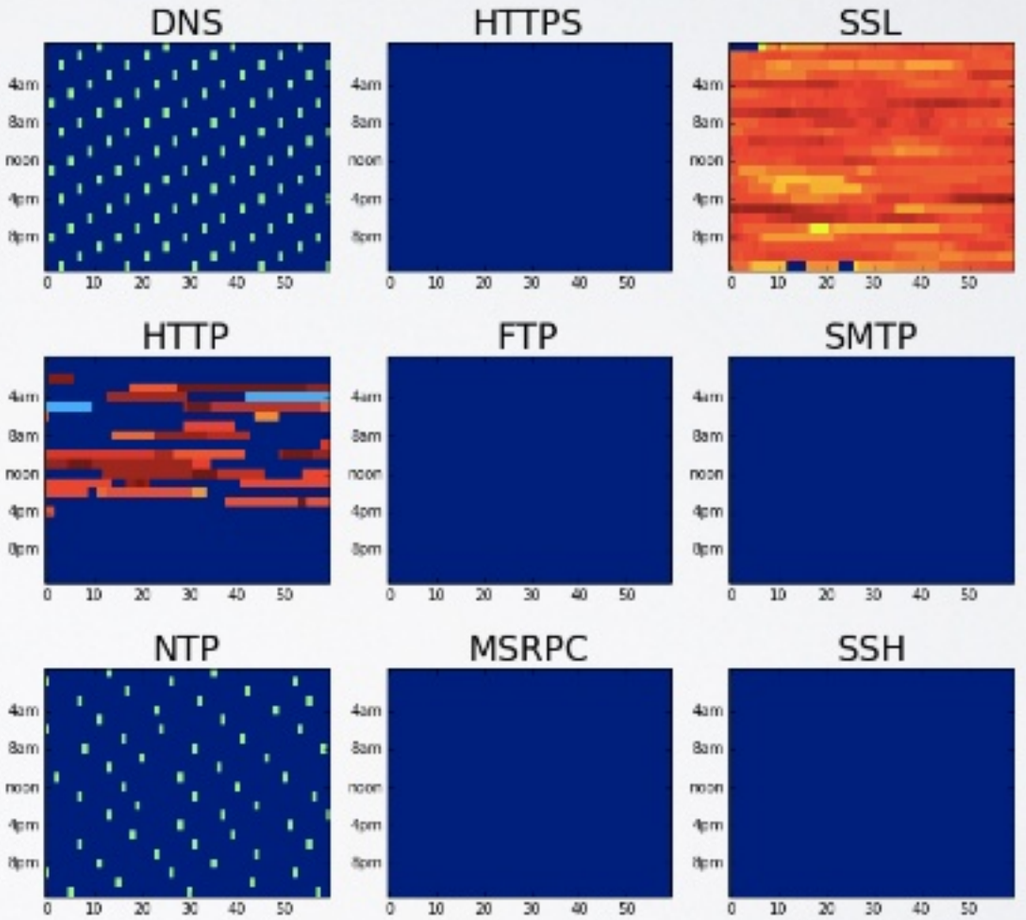
BEHAVIOR ANOMALY IOT DEVICE | DATA DOWNLOAD

aruba
a Hewlett Packard Enterprise company

Dropcam – Before Compromise

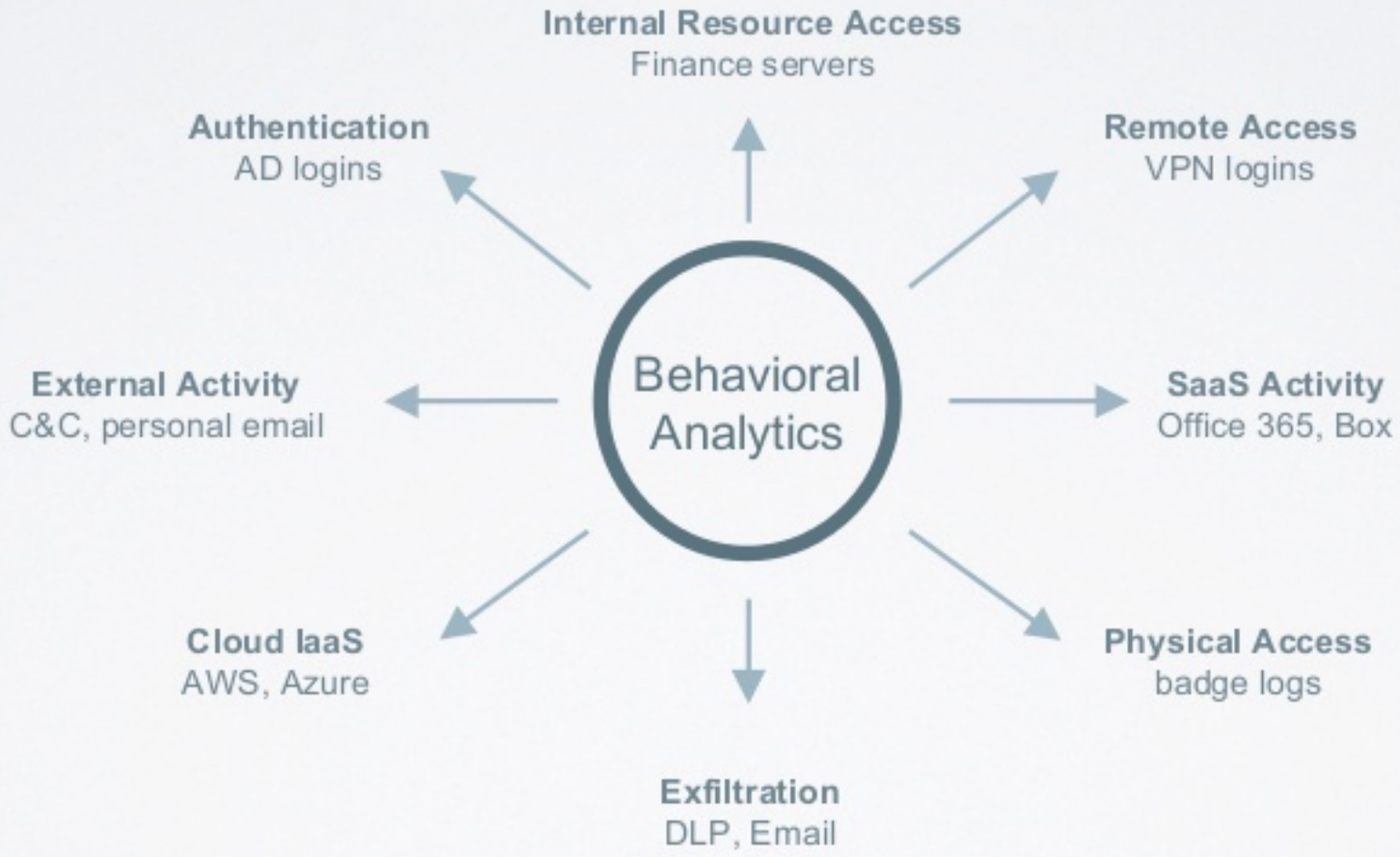


Dropcam – Post Compromise

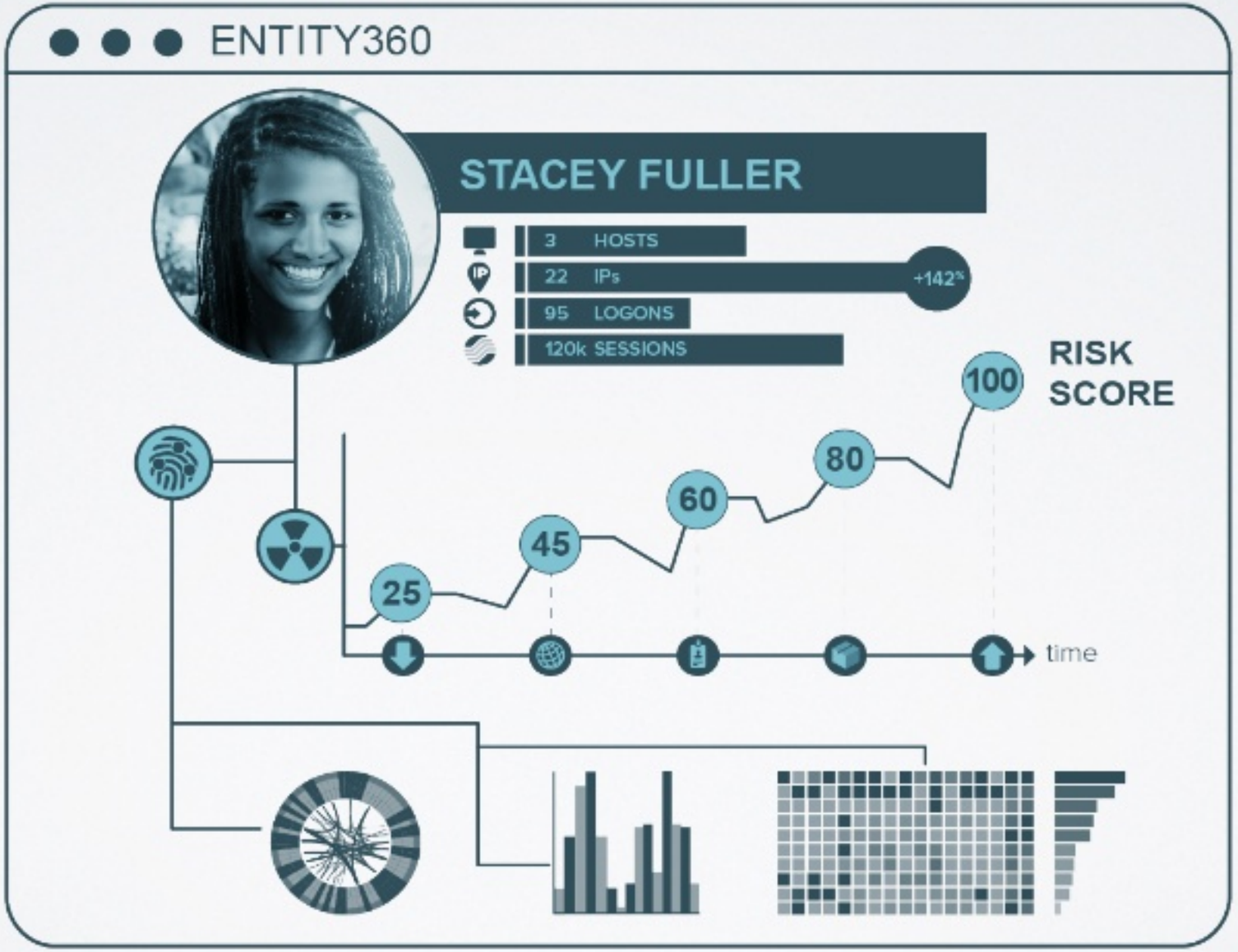


BEHAVIOR ANALYTICS MULTI-DIMENSIONAL

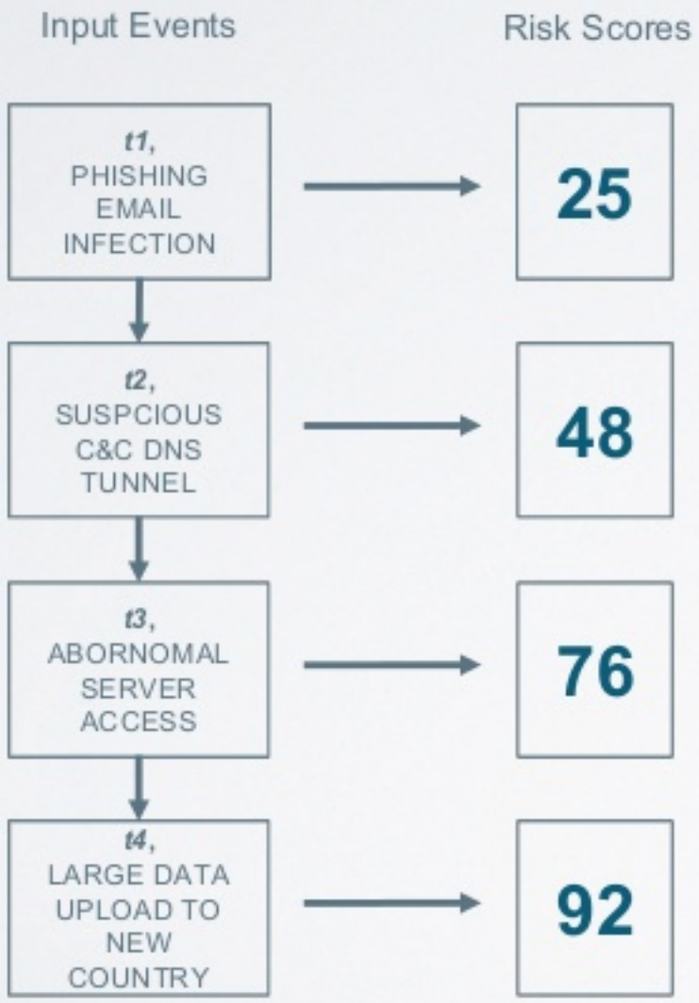
aruba
a Hewlett Packard Enterprise company



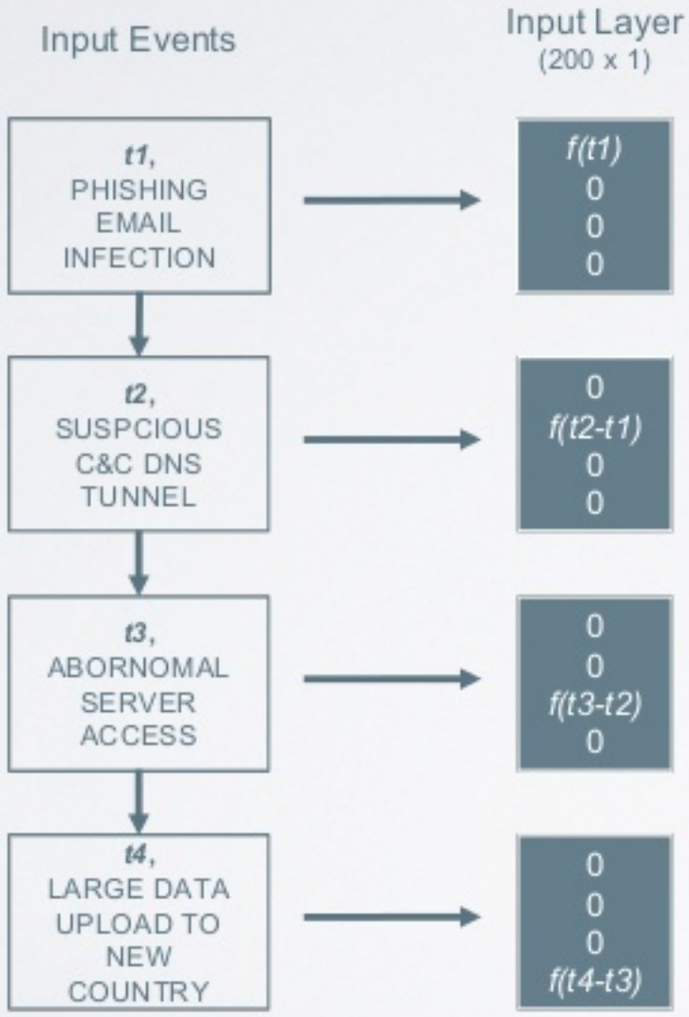
ENTITY SCORING TEMPORAL SEQUENCE TRACKING



ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)

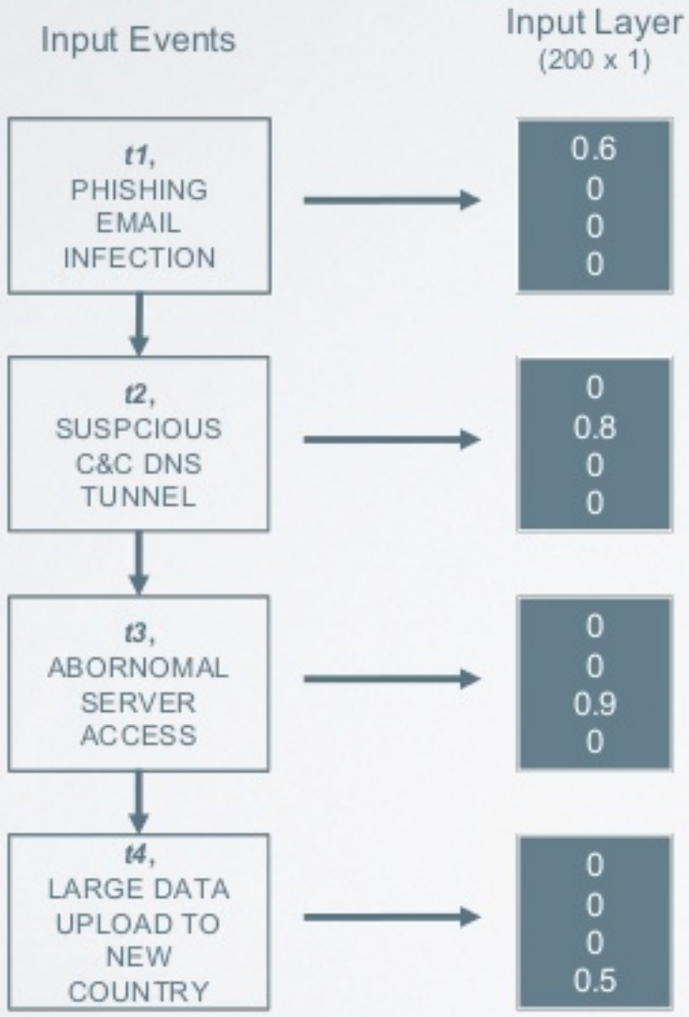


ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



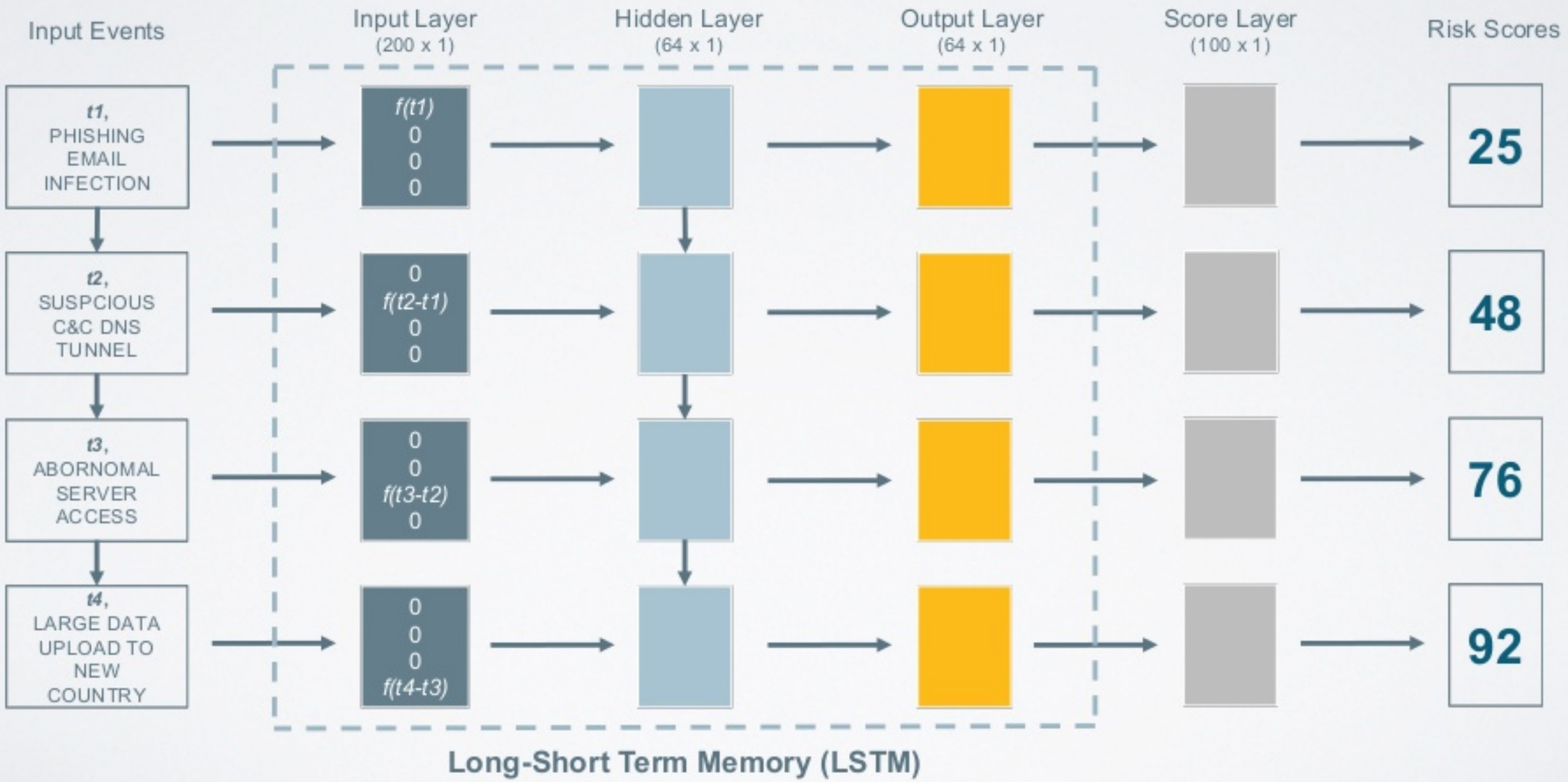
one hot
time-decayed
encoding

ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)



one hot
time-decayed
encoding

ENTITY SCORING RECURRENT NEURAL NETWORK (RNN)

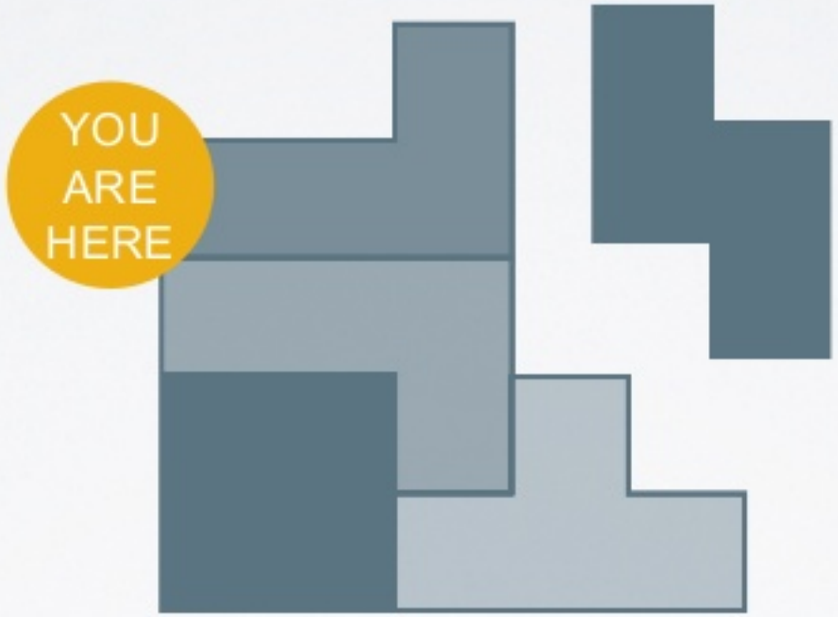


USER & ENTITY BEHAVIOR ANALYTICS

aruba
a Hewlett Packard Enterprise company

UEBA SECURITY

what is UEBA



UEBA SOLUTION

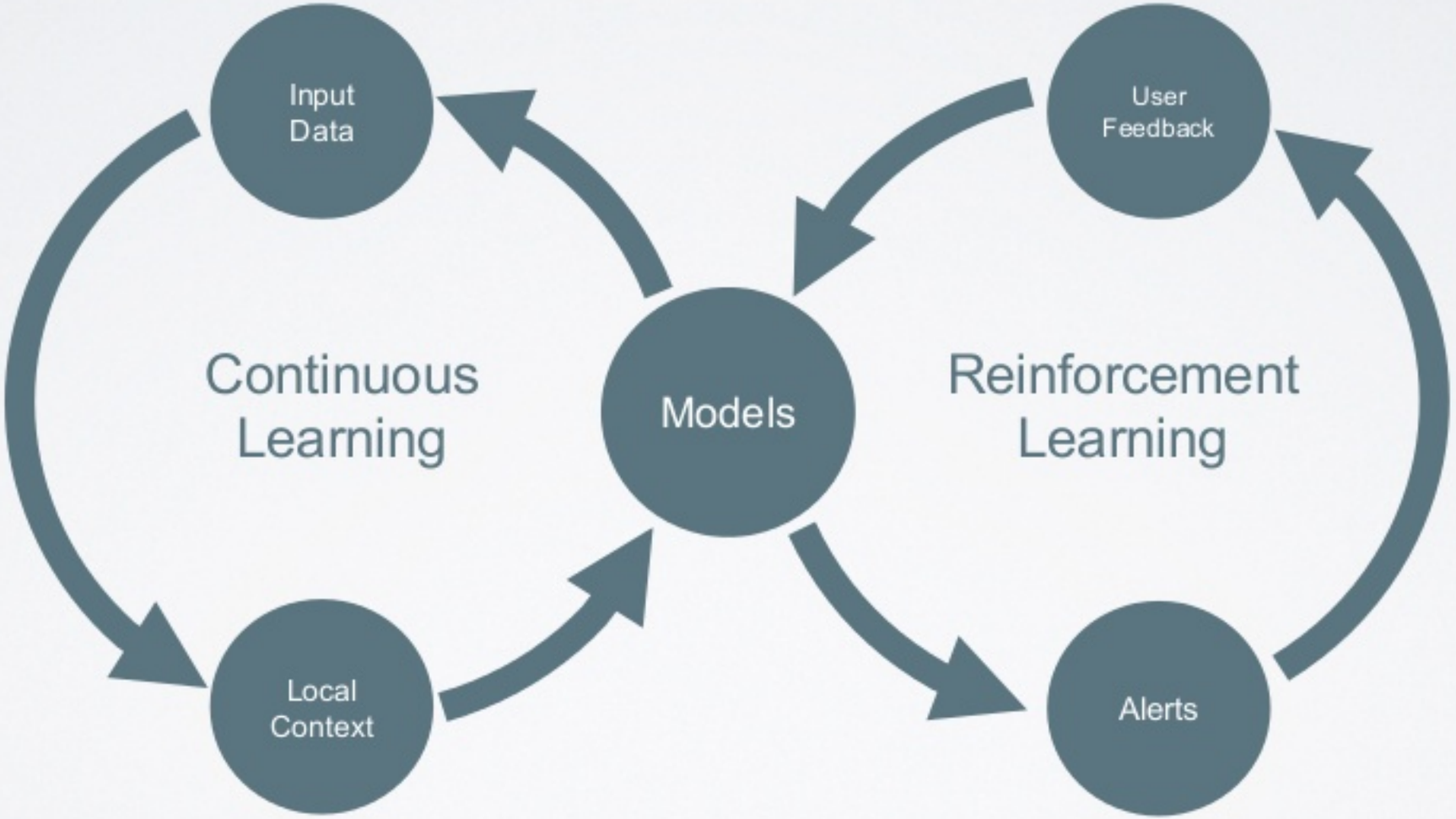
infrastructure needed to deep learning

BEYOND DEEP LEARNING

how to build a comprehensive solution

LOCAL CONTEXT MACHINE + HUMAN INTELLIGENCE

aruba
a Hewlett Packard Enterprise company



TRAINING DATA GLOBAL + LOCAL INTELLIGENCE

aruba
a Hewlett Packard Enterprise company

USER & ENTITY BEHAVIOR ANALYTICS

aruba
a Hewlett Packard Enterprise company

UEBA SECURITY

what is UEBA

UEBA SOLUTION

infrastructure needed to deep learning

BEYOND DEEP LEARNING

how to build a comprehensive solution

Thank You

aruba
a Hewlett Packard
Enterprise company