Deep Learning In Security:

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

Jisheng Wang, Min-Yi Shen

niara®

ME, US

- Jisheng Wang, Chief Scientist in Niara
  - Over 12-year experiences of applying machine learning and big data technology to security
  - Ph.D from Penn State – ML in security with 100GB data
  - Technical Leader in Cisco – Security Intelligence Operations (SIO) with 10B/day
  - 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

USER & ENTITY BEHAVIOR ANALYTICS

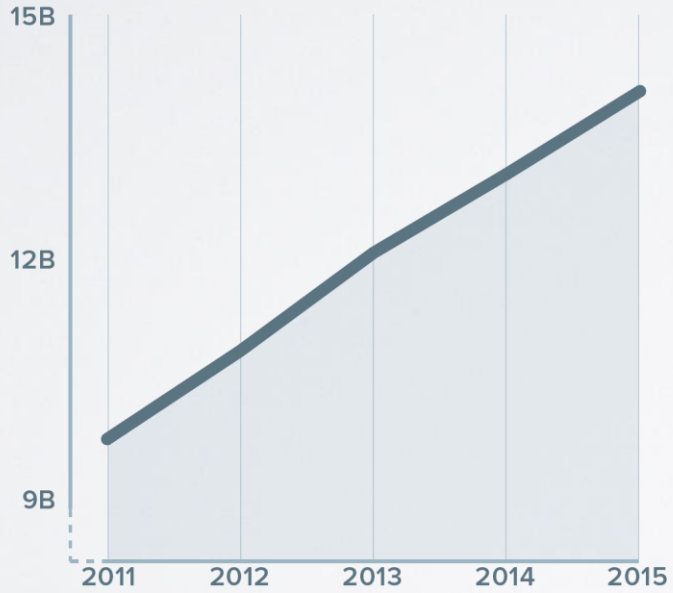
UEBA SECURITY
why this matters

UEBA SOLUTION
how to detect attacks before damage is done

BEYOND DEEP LEARNING
how to build a comprehensive solution

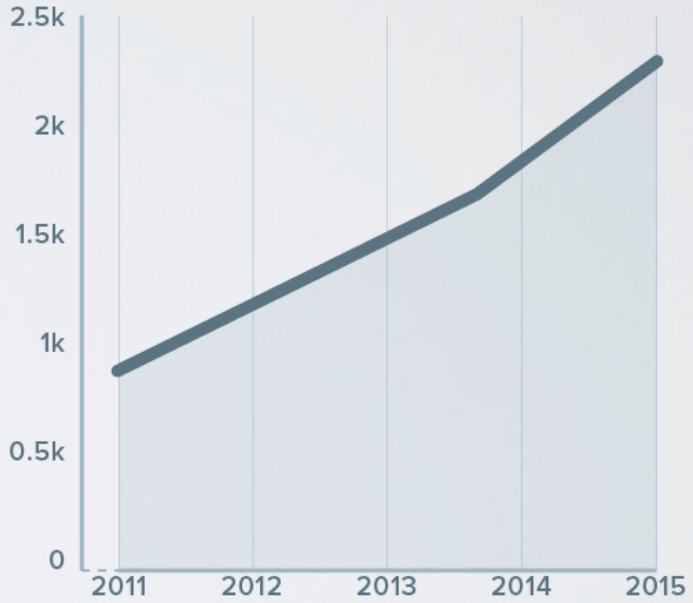
PROBLEM THE SECURITY GAP

SECURITY SPEND



PREVENTION & DETECTION (US $B)

DATA BREACHES



BREACHES

PROBLEM CAUSE OF THE GAP

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

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 NEWS WORTHY EXAMPLES

COMPROMISED

40 million credit cards were stolen from Target's severs

STOLEN CREDENTIALS

MALICIOUS

Edward Snowden stole more than 1.7 million classified documents

INTENTIONAL TO LEAK INFORMATION

NEGLIGENT

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

ALL USED THE SAME PASSWORD

USER & ENTITY BEHAVIOR ANALYTICS

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

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

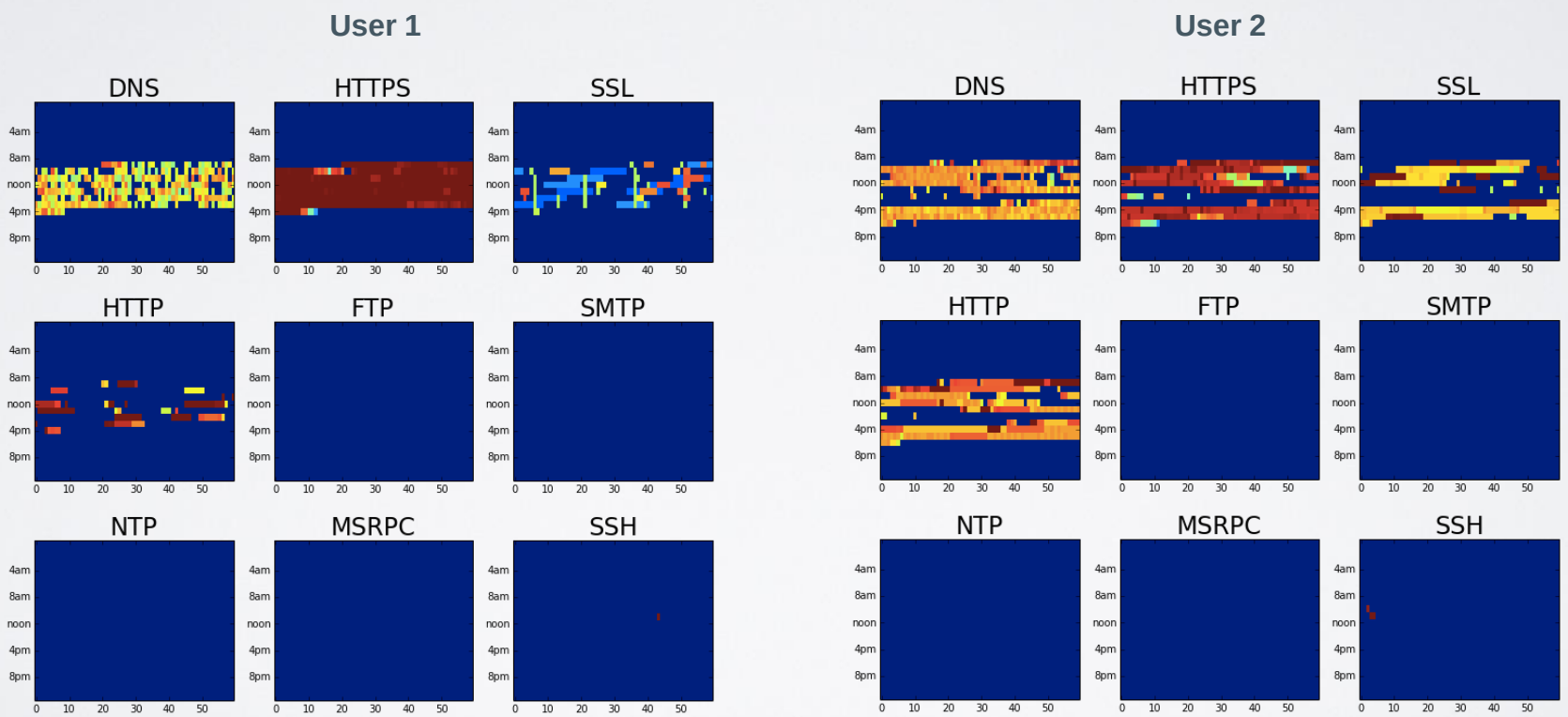
DETECTED WITH **NETWORK TRAFFIC**

EXFILTRATION OF DATA

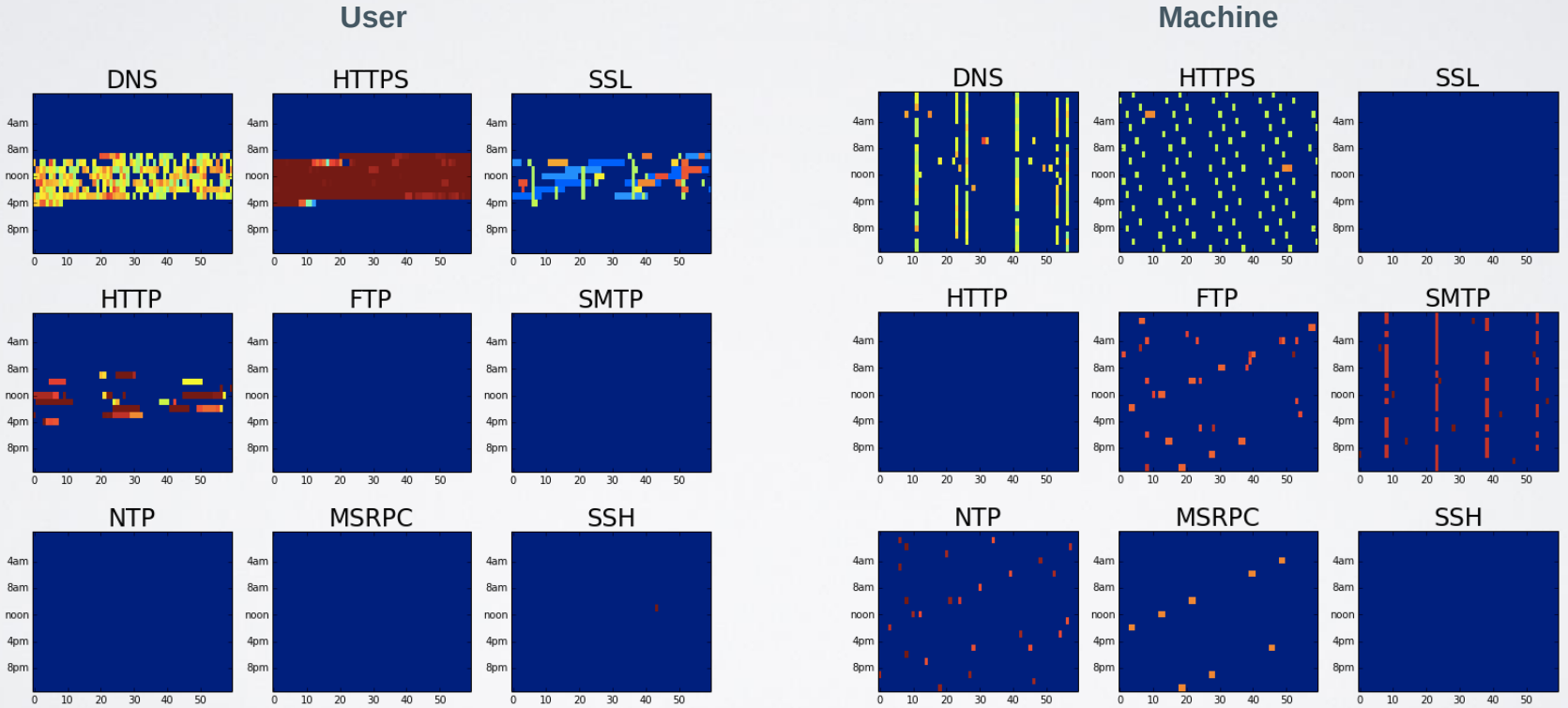
upload a large file to cloud server hosted in new country never accessed before

DETECTED WITH **WEB PROXY LOGS**

BEHAVIOR ENCODING – USER

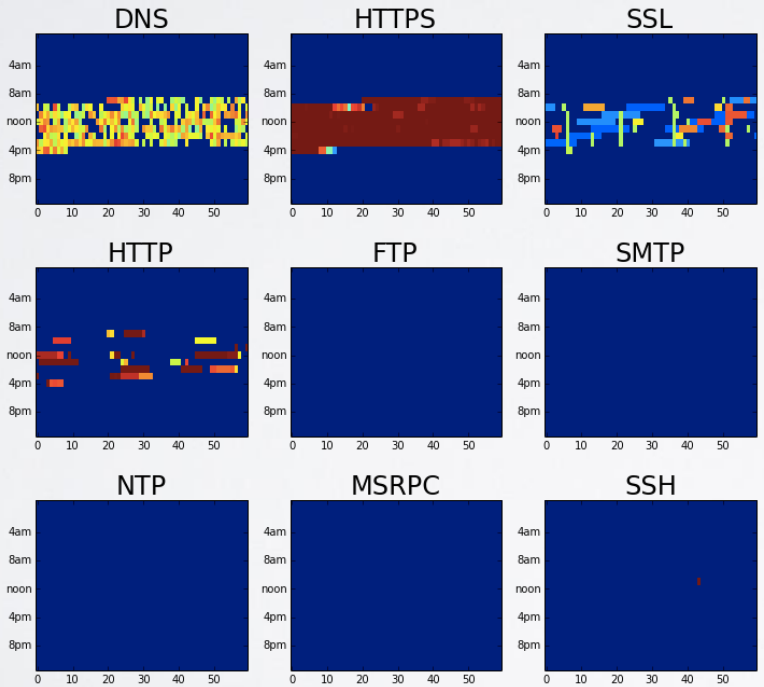


BEHAVIOR ENCODING – USER VS MACHINE

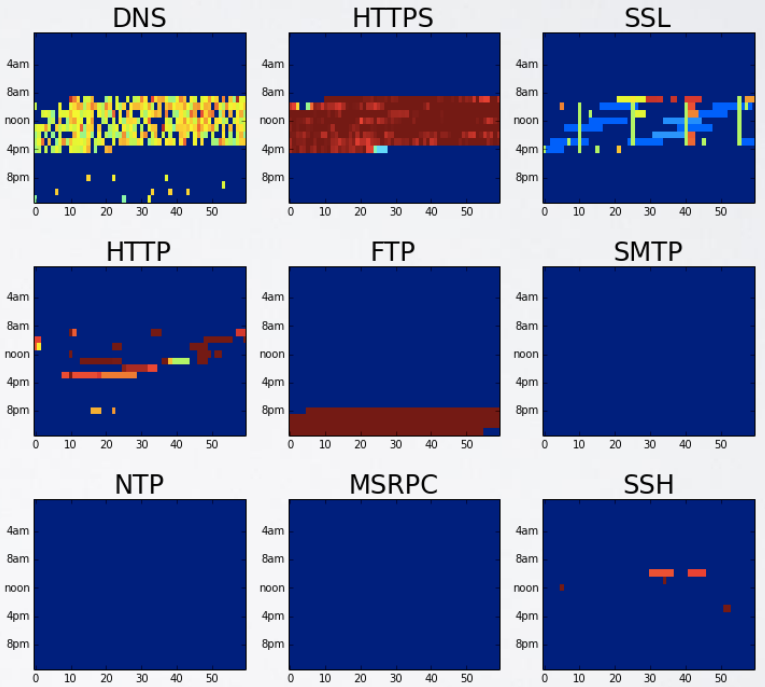


BEHAVIOR ANOMALY USER | EXFILTRATION

User – Before Compromise



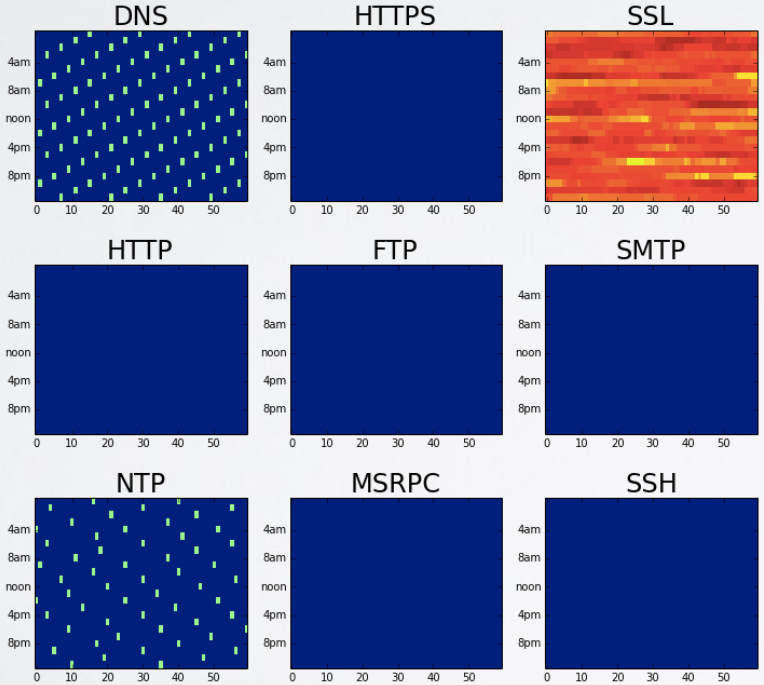
User – Post Compromise



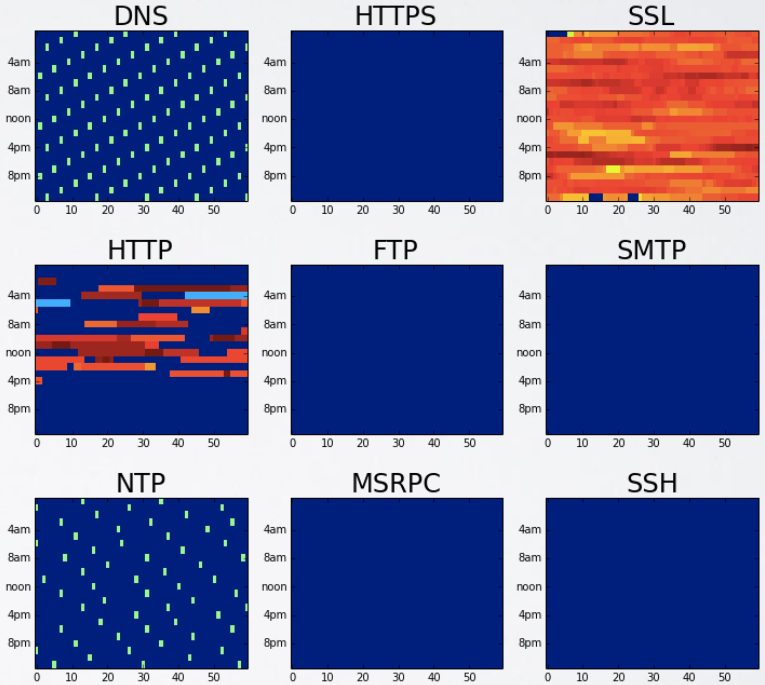
BEHAVIOR ANOMALY MACHINE | DATA DOWNLOAD

niara

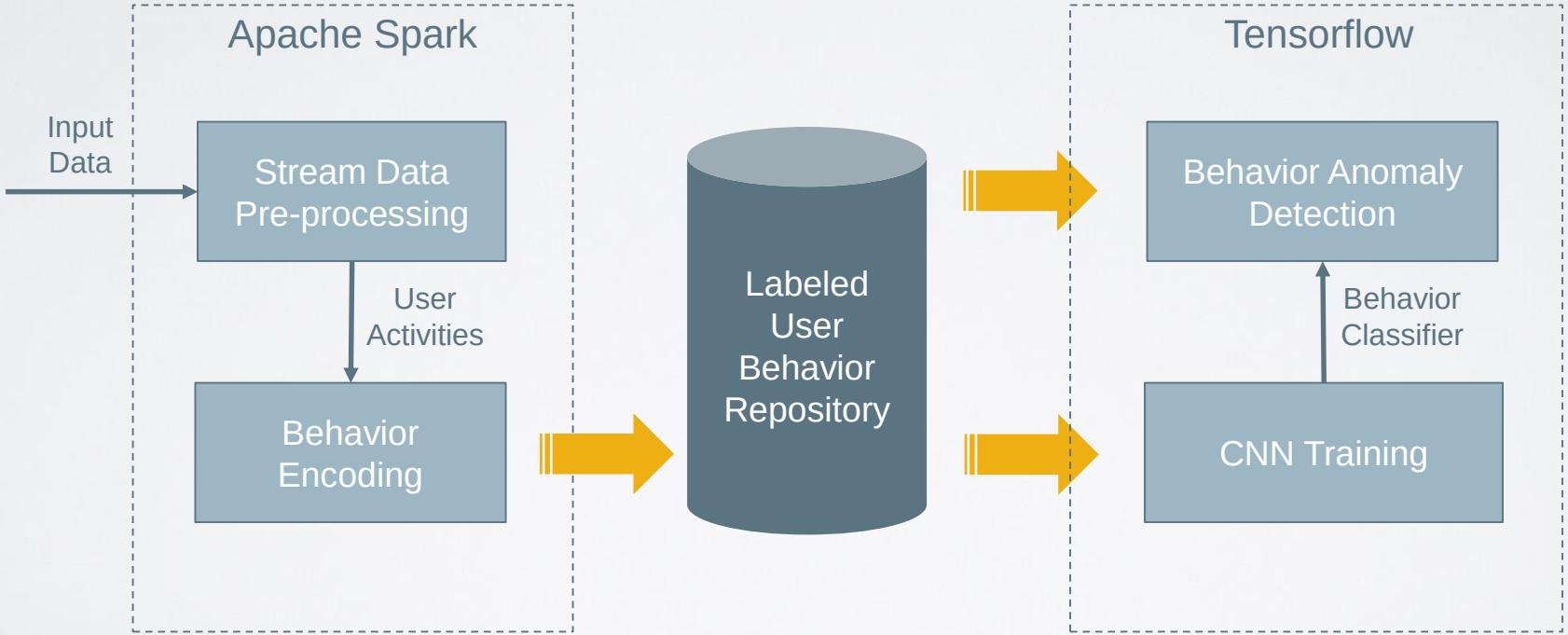
Dropcam – Before Compromise



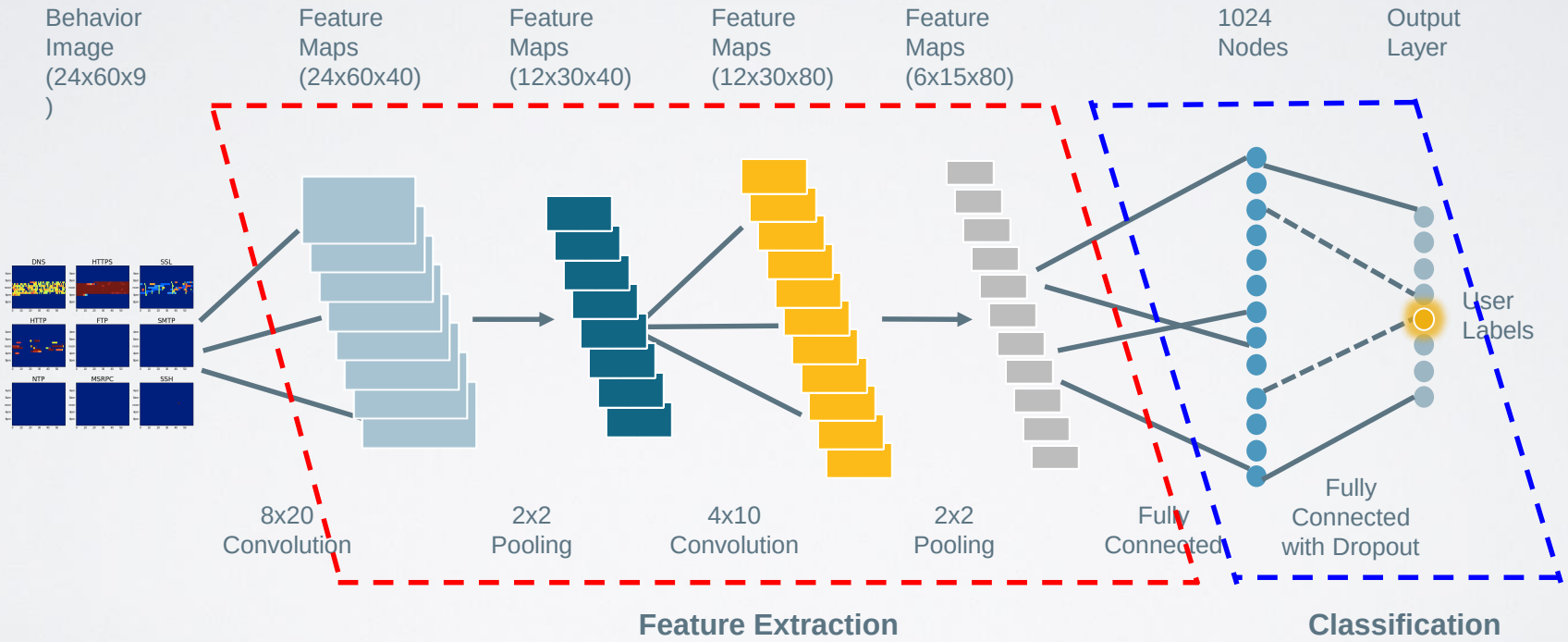
Dropcam – Post Compromise



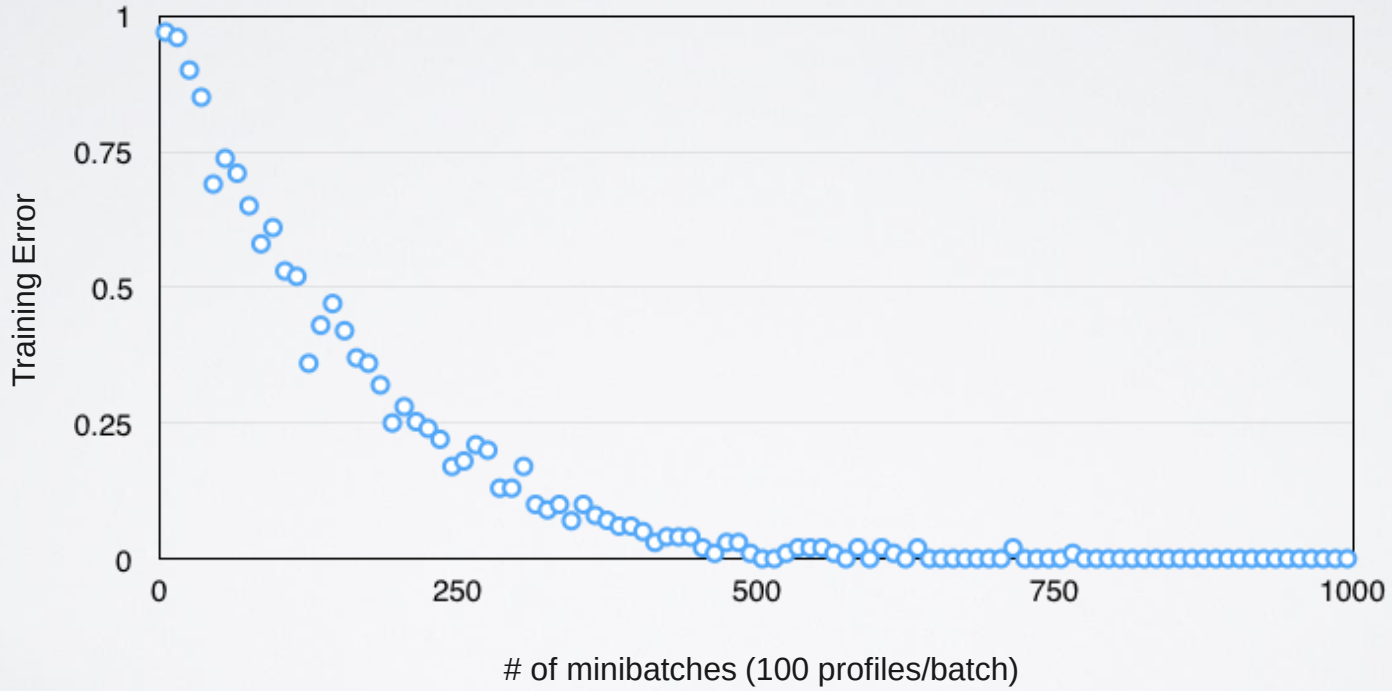
BEHAVIOR DETECTION ARCHITECTURE



CNN – COMPUTATION GRAPH



CNN – PROGRESSION OF TRAINING ERROR



USER & ENTITY BEHAVIOR ANALYTICS

niara

UEBA SECURITY

what is UEBA

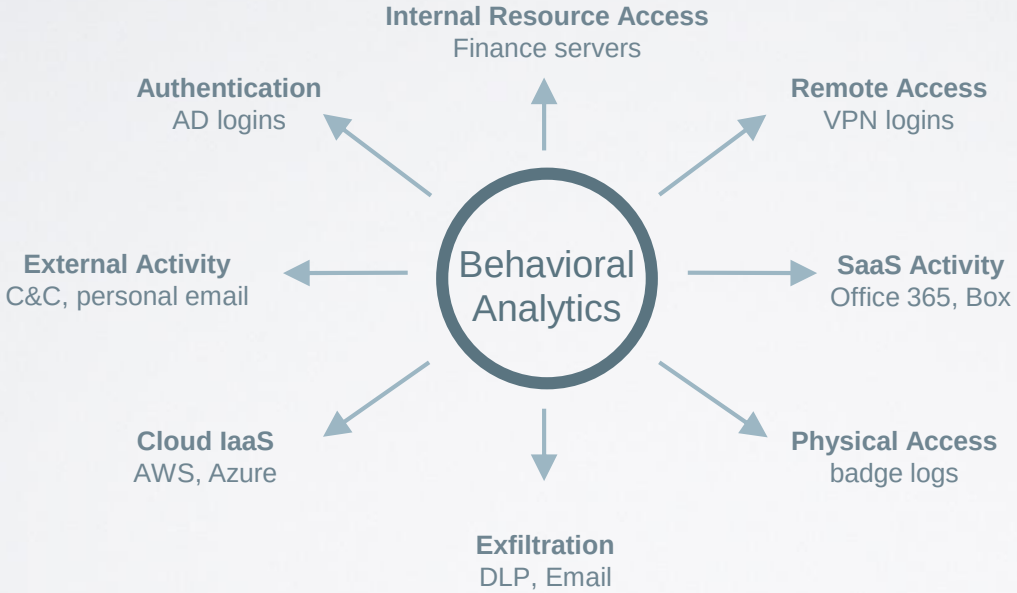
UEBA SOLUTION

infrastructure needed to deep learning

BEYOND DEEP LEARNING

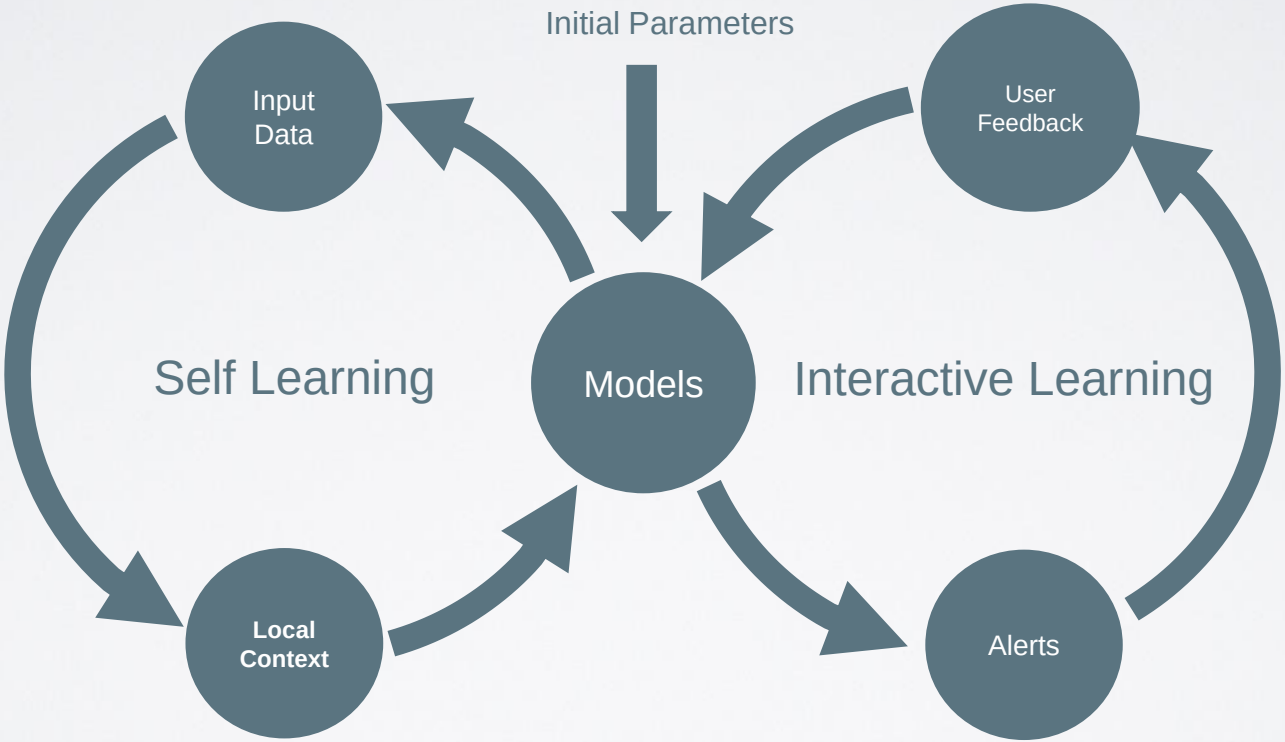
how to build a comprehensive solution

BEYOND DEEP LEARNING ENSEMBLE LEARNING



Ensemble approach using a mix of ***different*** models over ***various*** types of behaviors from the same entity

BEYOND DEEP LEARNING REINFORCEMENT LEARNING



USER & ENTITY BEHAVIOR ANALYTICS

UEBA SECURITY

what is UEBA

UEBA SOLUTION

infrastructure needed to deep learning

BEYOND DEEP LEARNING

how to build a comprehensive solution

Thank You

niara®