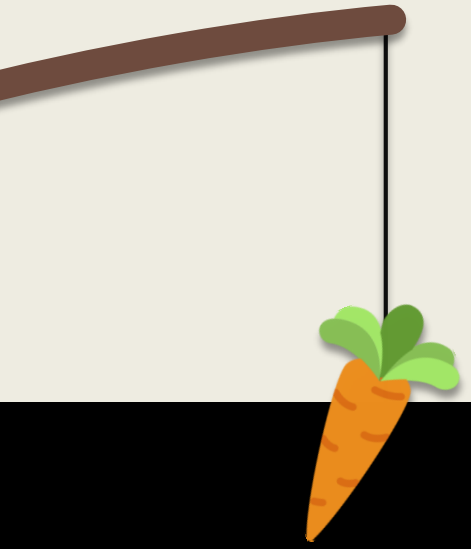
NavTalk- April 5, 2017

Cyberthreat Discovery in Open Source Intelligence (OSINT) Using Deep Learning Techniques

Eunice Branco
Pedro Ferreira
Alysson Bessani



MOTIVATION

Motivation

Security Information and Event Management systems help monitor infrastructures and correlate the obtained events in order to discover possible threats to the organization

Open Source Intelligence Data Fusion and Analysis

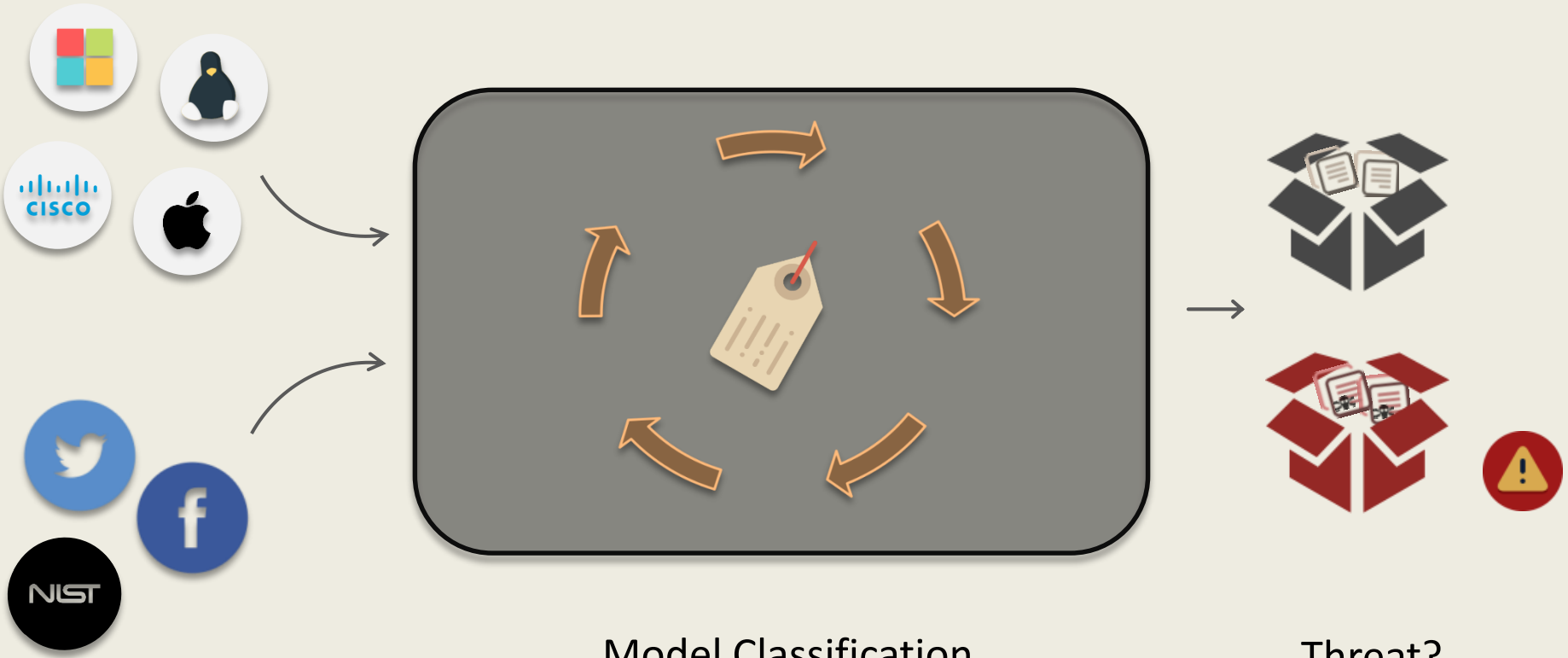
Motivation

An increasing need to process **large amounts of data** regarding new emerging **security threats**

State of the Art

State of the Art – Problem Statement

Monitored IT Infrastructure

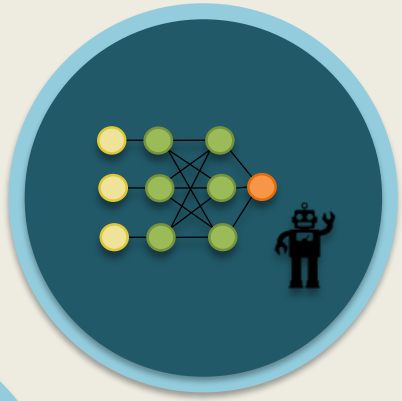


OSINT Data Sources

Model Classification

Threat?

State of the Art – Approaches



Shallow Neural Networks,
Support Vector Machines

Text based filters

Statistical
approaches

State of the Art – Limitations

Shallow learning methods rely on **searching** and **specifying the input features** to define a model

ENVISIONED SOLUTION

Envisioned Solution

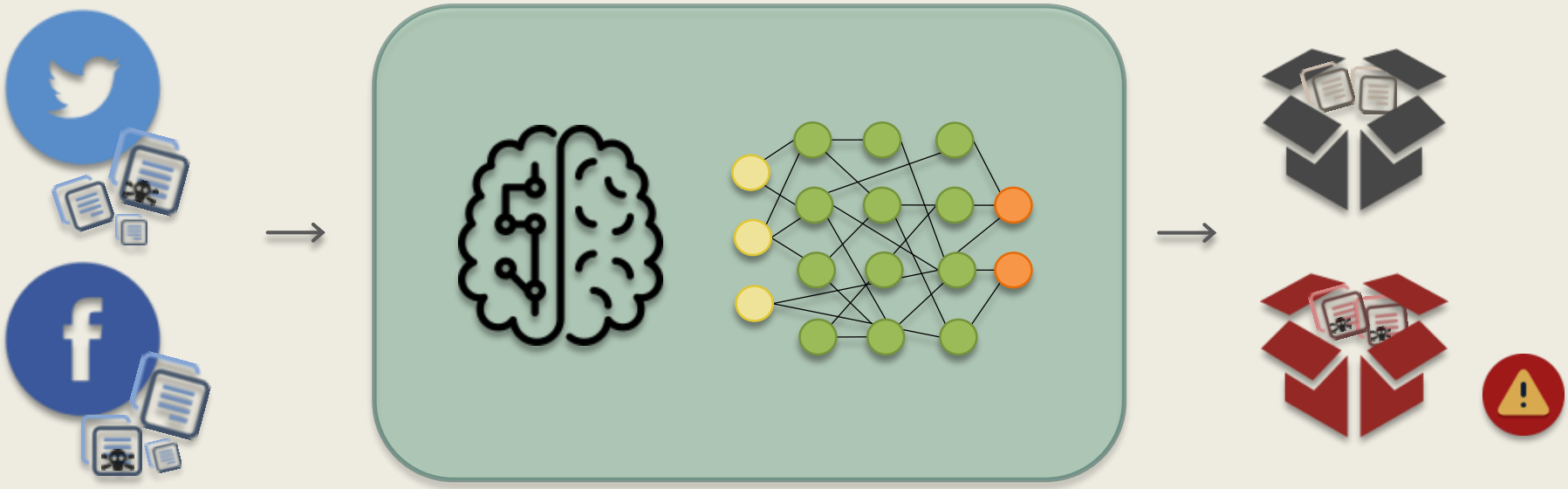
Deep learning models learn concepts and features directly from raw data and work on huge data sets

- Works with non-trained parameters
- It is not problem specific oriented
- More layers equal more functions

OBJECTIVE

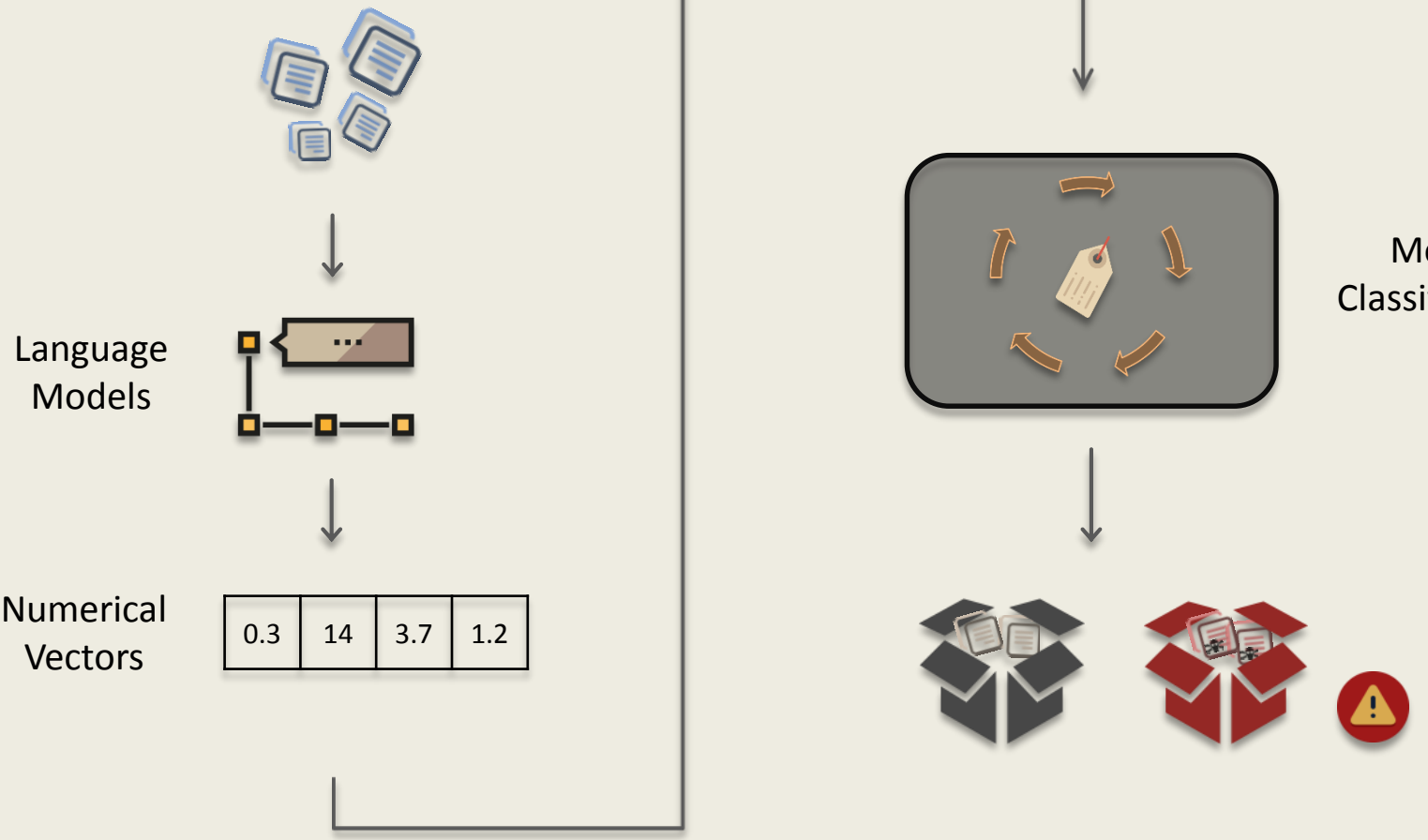
OBJECTIVE

Process large amounts of **OSINT data** using **deep learning techniques** with a high degree of accuracy regarding **cyberthreat discovery**

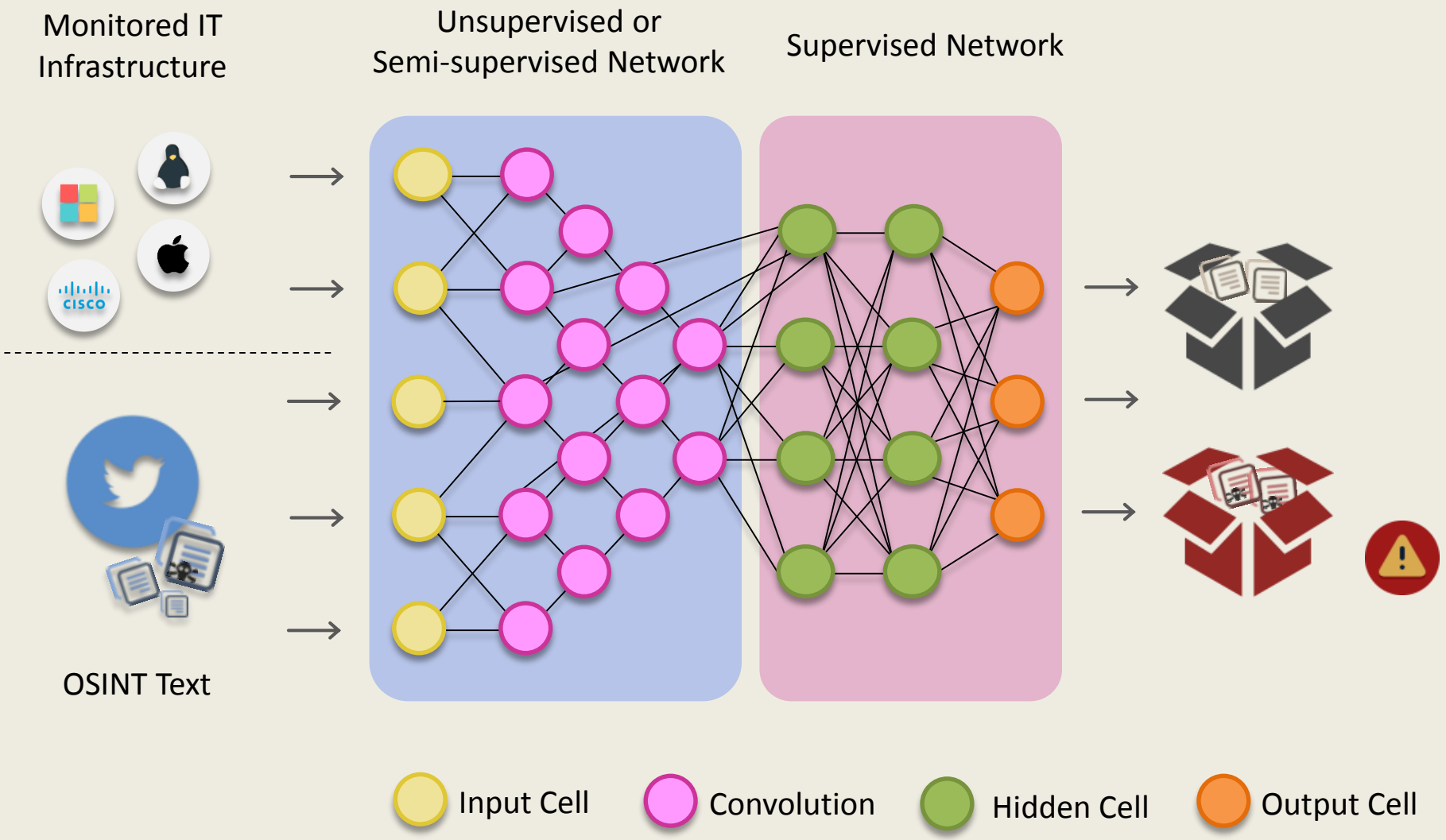


Ongoing Work

Ongoing Work



Ongoing Work



Cyberthreat Discovery in Open Source Intelligence (OSINT) Using Deep Learning Techniques

Eunice Branco,
Pedro Ferreira,
Alysson Bessani

1. Motivation

The increasing need to process **large amounts of data** regarding new emerging **security threats**

2. State of the Art

Text based filters

Statistical approaches

Shallow Neural Networks, SVMs

3. Limitations

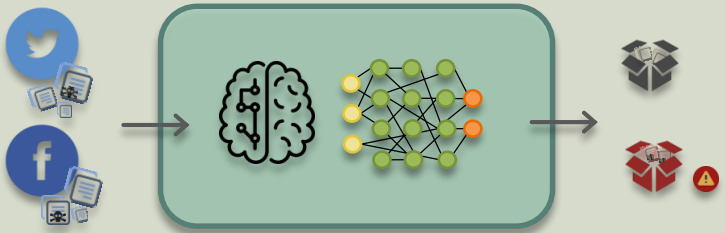
Shallow learning methods rely on **searching** and **specifying the input features** to define a model

Envisioned Solution:

Deep learning models learn concepts and features directly from raw data and work on huge data sets

4. Objective

Process large amounts of **OSINT data** using **deep learning techniques** with a high degree of accuracy regarding **cyberthreat discovery**



5. Ongoing Work

We will consider complementary approaches while making use of **Deep Neural Networks**