RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MLAI-W10

Machine Learning Toolbox for Cybersecurity Risk Management

Bugra Karabey

Senior Risk Manager
Microsoft

RSAConference2019

Cybersecurity risk manager has no clothes!

Cybersecurity risk manager has no clothes!

- Cybersecurity risk manager is lacking the cutting-edge tools of the trade
- Current state:
  - Subjective risk evaluations based on subject matter expert interviews
  - Limited data driven risk assessment methodologies
  - Qualitative rather than quantitative datapoints
  - 1-to-5 scores for impact and likelihood
  - Focus on known-knowns

Cybersecurity risk management & machine learning

- Machine Learning (ML) usage is already ubiquitous in cybersecurity:
  - Log, telemetry, and traffic pattern analysis
  - Anomaly detection
  - Behavior analytics
- However, for the identification and assessment of dormant/latent risk themes, patterns, and relationships, additional machine learning tools (and mostly Natural Language Processing flavored variants) will be useful:
  - As the insights reside within text heavy datasets
    - Internal audit issues
    - Governance Risk Compliance (GRC) security findings
    - Security policy exceptions
    - Internal & external incidents
  - Natural language driven
  - Artifacts may be at the board room discussion level, rather than technically focused
- In this talk we will be covering some of these scenarios. These are applied in parallel to, and in support of the subject matter expert driven analysis, qualitative/quantitative assessments, and the conventional business analytics. They do not intend to replace these traditional approaches

“Every risk manager needs a machine learning toolbox”

- In this talk, we will be covering 3 scenarios in which a cybersecurity risk manager can benefit from machine learning techniques:
  - Scenario #1: How to identify top risks using Topic Modelling?
  - Scenario #2: How to identify latent/emerging risks using NLP (Natural Language Processing)?
  - Scenario #3: How to identify risk management process issues using PCA (Principal Component Analysis) clustering?

RSAConference2019

Scenario #1: How to identify top risks using Topic Modelling?

Usage scenario: How to identify top risks using Topic Modelling?

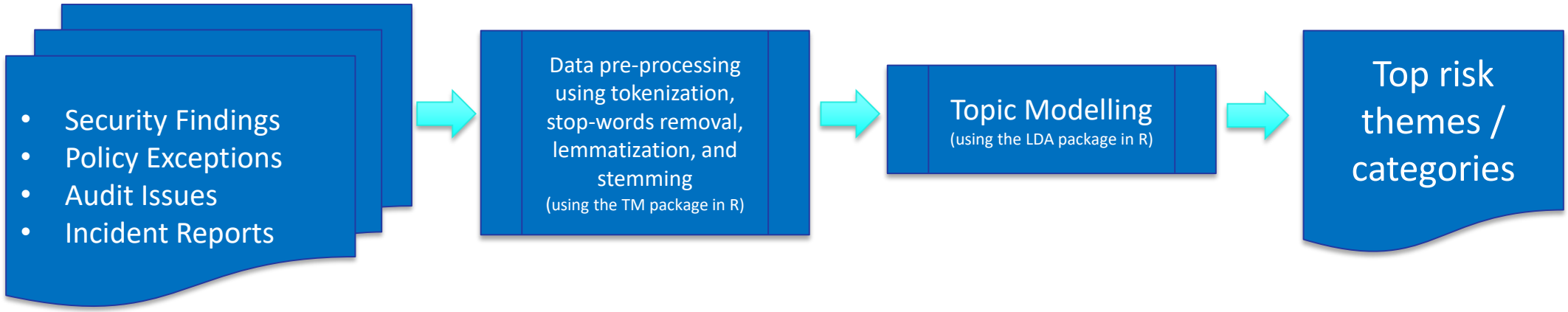
- Topic Modelling: Statistical model for discovering the abstract "topics“, and the discovery of hidden semantic structures in a collection of documents. It is an unsupervised statistical modeling technique used for finding out a group of words, which collectively represent a topic in a large collection of documents
  - Most popular Topic Modelling techniques:
    - Latent Semantic Analysis (LSA)
    - Latent Dirichlet Allocation (LDA)
      - LDA builds topic per document and words per topic models, that are modeled as Dirichlet distributions

How to identify top risks using Topic Modelling?

- Suggested text mining pre-processing steps before Topic Modelling: Tokenization (chopping up sentences, and throwing away punctuation), stop-words removal, lemmatization (converting to base form), and stemming (converting to root form)
- LDA user settings:
  - # of topics -> How many latent topics do we need to explain x% of the variance in the data
  - User entered model settings will be: “Identify x topics, with y words/phrases in each topic”
- **Tools utilized:** LDA and TM (text mining) packages in R

How to identify top risks using Topic Modelling?

- Our workflow:



Sample output

Topic 1	Topic 2	Topic 3	Topic 4	Topic 5
Brute force	Subnet	Crypto	Misconfiguration	Cloud hijacking
App Z	Network environment	Multiple certificate	PKI server	PaaS
MFA	NIC	Asymmetric	Sensitive	Encrypt at rest
Monitor	System Y	Server C	Configuration management	Service P
Confidential	Dual homed	PKI	Dept X	Disclosure
Breach	Isolation	FIPS140	Confidential	Backup

LDA identified words/phrases for each topic

Potential interpretation:

System Y is suffering from an isolation issue, due to the existence of dual-homed interfaces between subnets and/or network environments

RSAConference2019

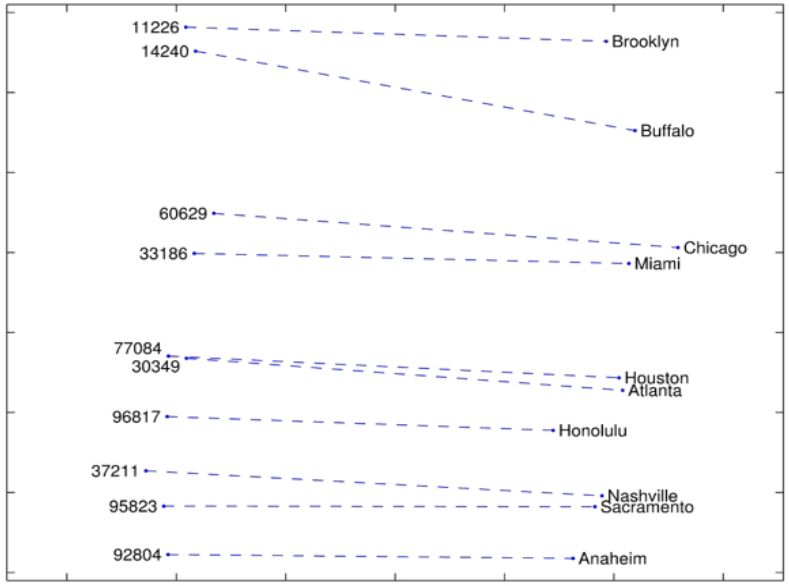
Scenario #2: How to identify latent/emerging risks using Natural Language Processing (NLP)?

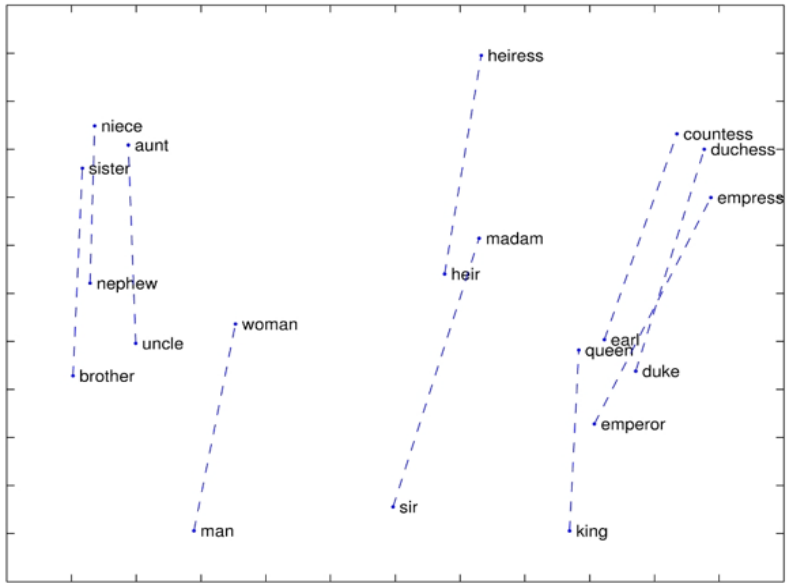
Usage scenario: How to identify latent/emerging risks using Natural Language Processing?

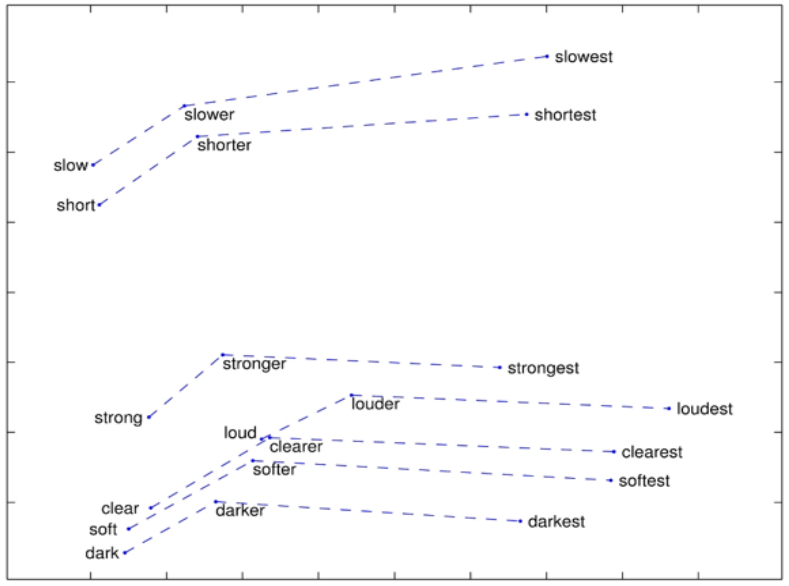
- Experimental NLP based approaches in the identification of latent and emerging risk categories:
  - Word Embeddings
  - LSTM (Long-short term memory) Deep RNNs (Recurrent Neural Nets)

Word Embeddings

- Word Embeddings in a nutshell:
  - Unsupervised learning algorithm for obtaining vector representations for words. Training is performed on aggregated global word-word co-occurrence statistics from a body/corpus, and the resulting representations showcase interesting linear substructures of the word vector space* :







- Our approach:
  - Create a Word Embedding space using corpora of security documents/datasets to build the word vector space
  - Further analysis using 2 & 3D principal component analysis
- **Tools utilized:** Python gensim, nltk, sklearn packages, Jupyter notebooks, and Word2Vec module with the skip-gram algorithm**.

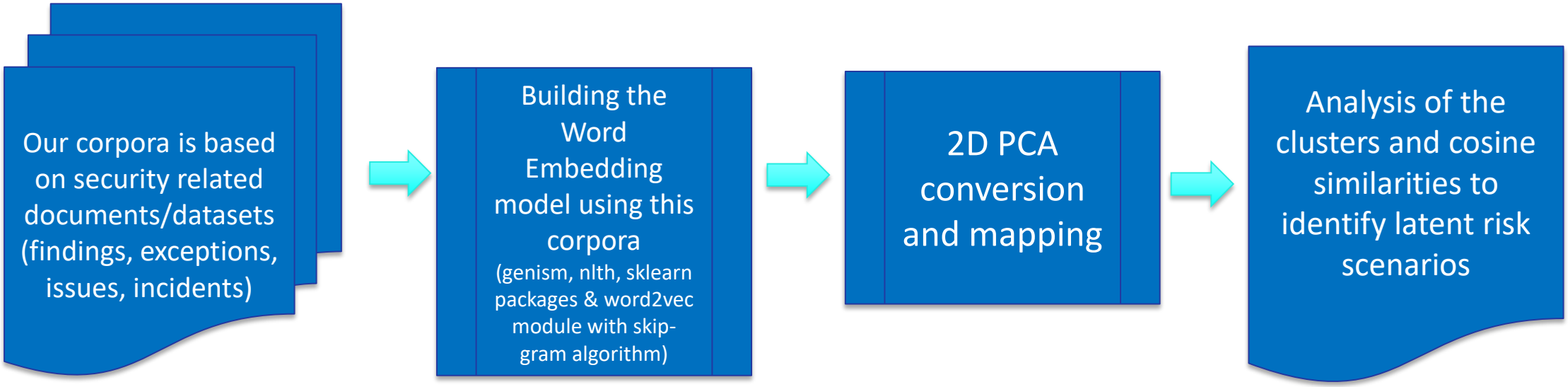
Microsoft

* https://nlp.stanford.edu/projects/glove/

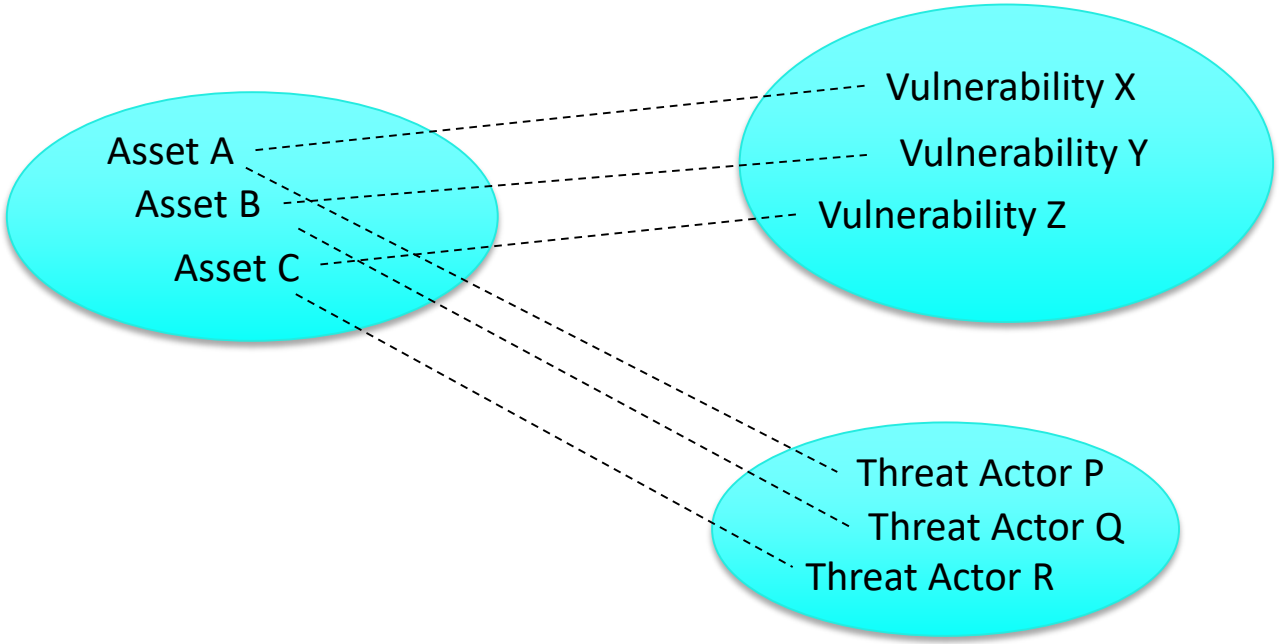
** https://radimrehurek.com/gensim/models/word2vec.html

Word Embeddings

- Our workflow:



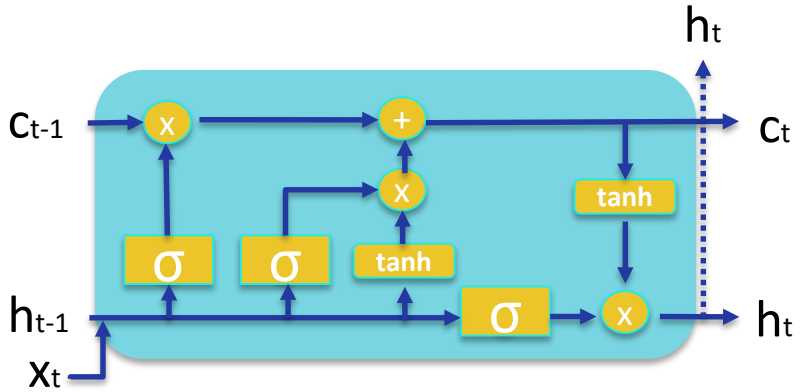
Sample output



- model.most_similar(positive=[‘VulnX', ‘AssetC'], negative=[‘AssetA’] , topn=1)
  - [(‘VulnZ', 0.7543)]
- model.doesnt_match(“supplier secret encryption brute".split())
  - ‘supplier'
- By analyzing the word embedding space (reduced to 2D or 3D), the user can identify the clusters and the latent relationships between entities (like assets, actors, and vulnerabilities)

LSTM (Long-short term memory) Deep RNNs (Recurrent Neural Nets)

- LSTM- RNNs in a nutshell*:

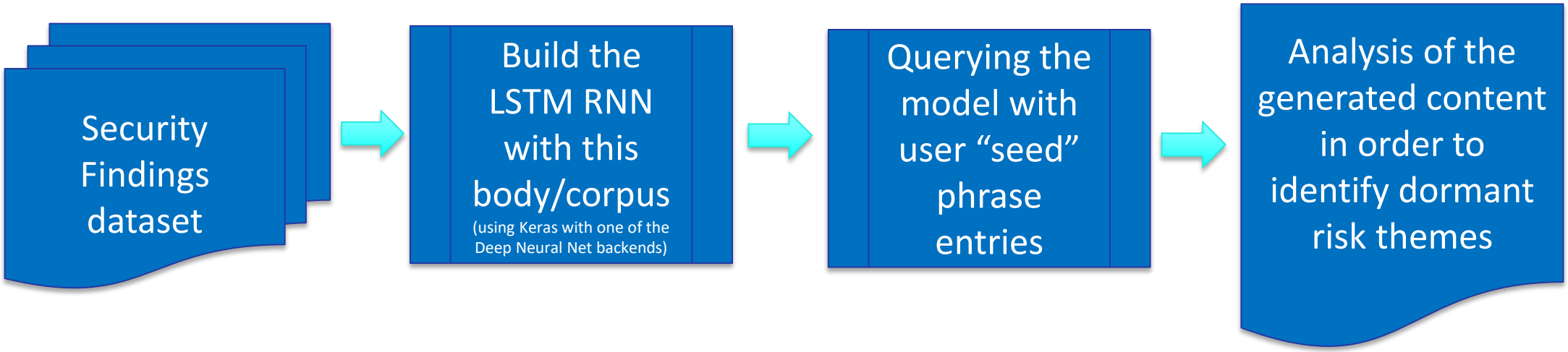


  - Long Short-Term Memory (LSTM), Recurrent Neural Net cell can process data sequentially and keep its hidden state through time
  - Our approach:
    - Text generation using LSTM-RNNs**
    - By utilizing an LSTM-RNN trained on a body/corpus of security findings
  - **Tools utilized:** Keras (with Tensorflow or CNTK as the backend), Jupyter notebooks

* http://people.idsia.ch/~juergen/rnn.html
** http://karpathy.github.io/2015/05/21/rnn-effectiveness/

LSTM (Long-short term memory) Deep RNNs (Recurrent Neural Nets)

- Our workflow:



Sample output

- User enters seed phrases, and the LSTM RNN completes the sentence/argument:
  - *Seed -> isolation*
    - Generated output -> *isolation* issues with the system xyz …
  - *Seed -> encryption*
    - Generated output -> *encryption* algorithm ABC and the expired certificate ….

RSAConference2019

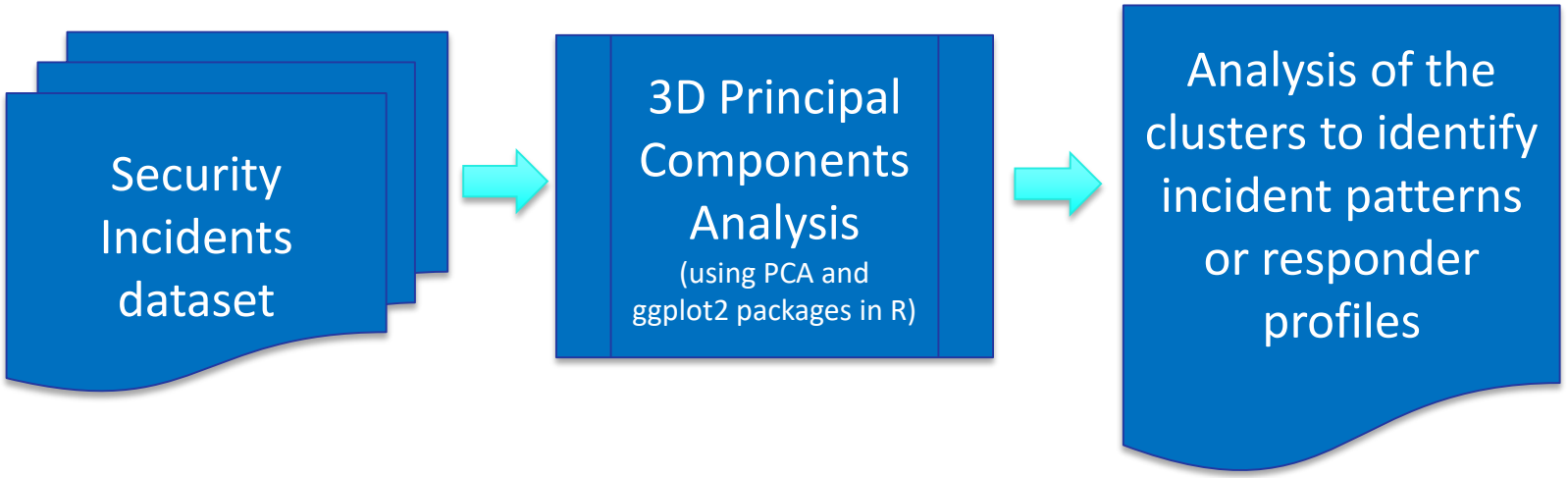
Scenario #3: How to identify risk management process issues using PCA clustering?

Usage scenario: How to identify risk management process issues using PCA clustering?

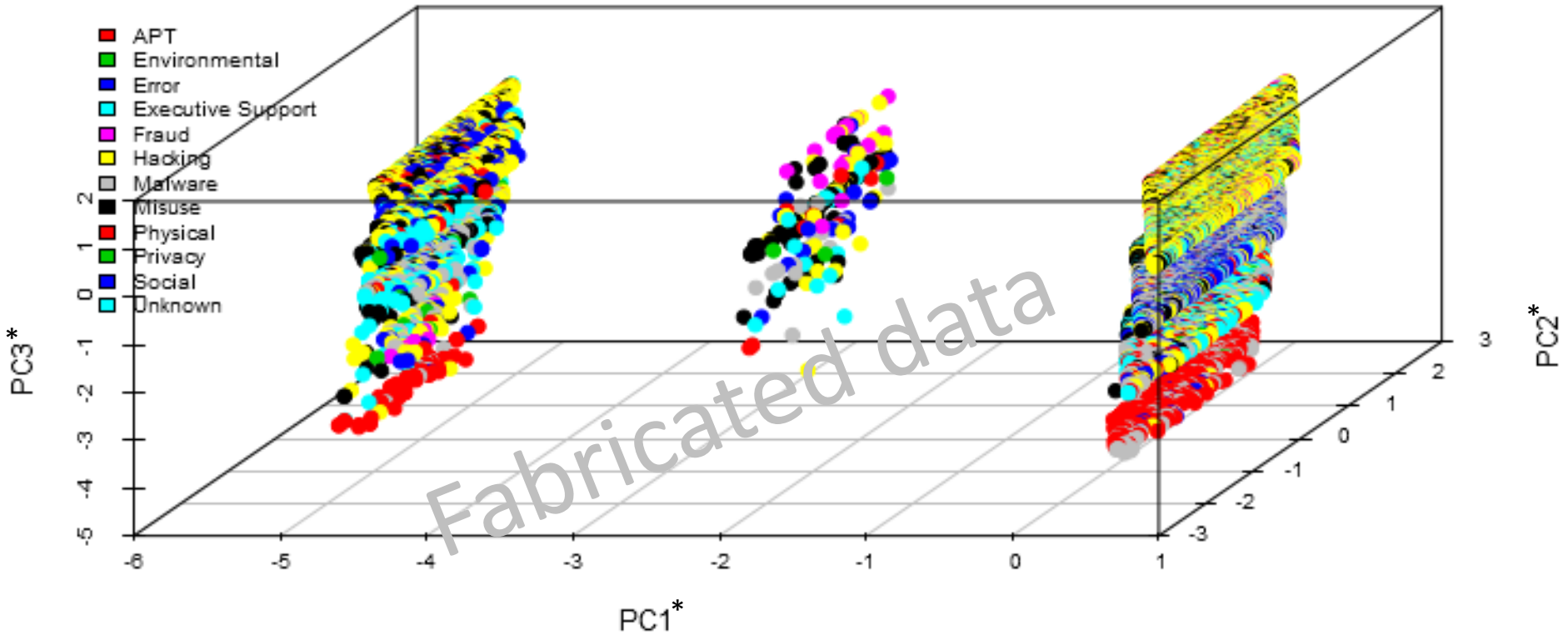
- An example from the incident response domain: There may be security incident response process issues (or even incident patterns) that can be identified using PCA clustering
- PCA: Dimensionality reduction using a statistical procedure
  - Orthogonal transformation to convert a set of observations, into a set of linearly uncorrelated variables (e.g., start with a dataset that has 100 features, and minimize it to 5 principal components that expresses the data in terms of these new variables)
- Our approach:
  - Analysis of the “security incidents” dataset using PCA dimensionality reduction (2d and/or 3d)
  - Identification of incident responder profiles and latent process issues
- **Tools utilized:** PCA and ggplot2 (data visualization) packages in R

PCA clustering

- Our workflow:



Sample output

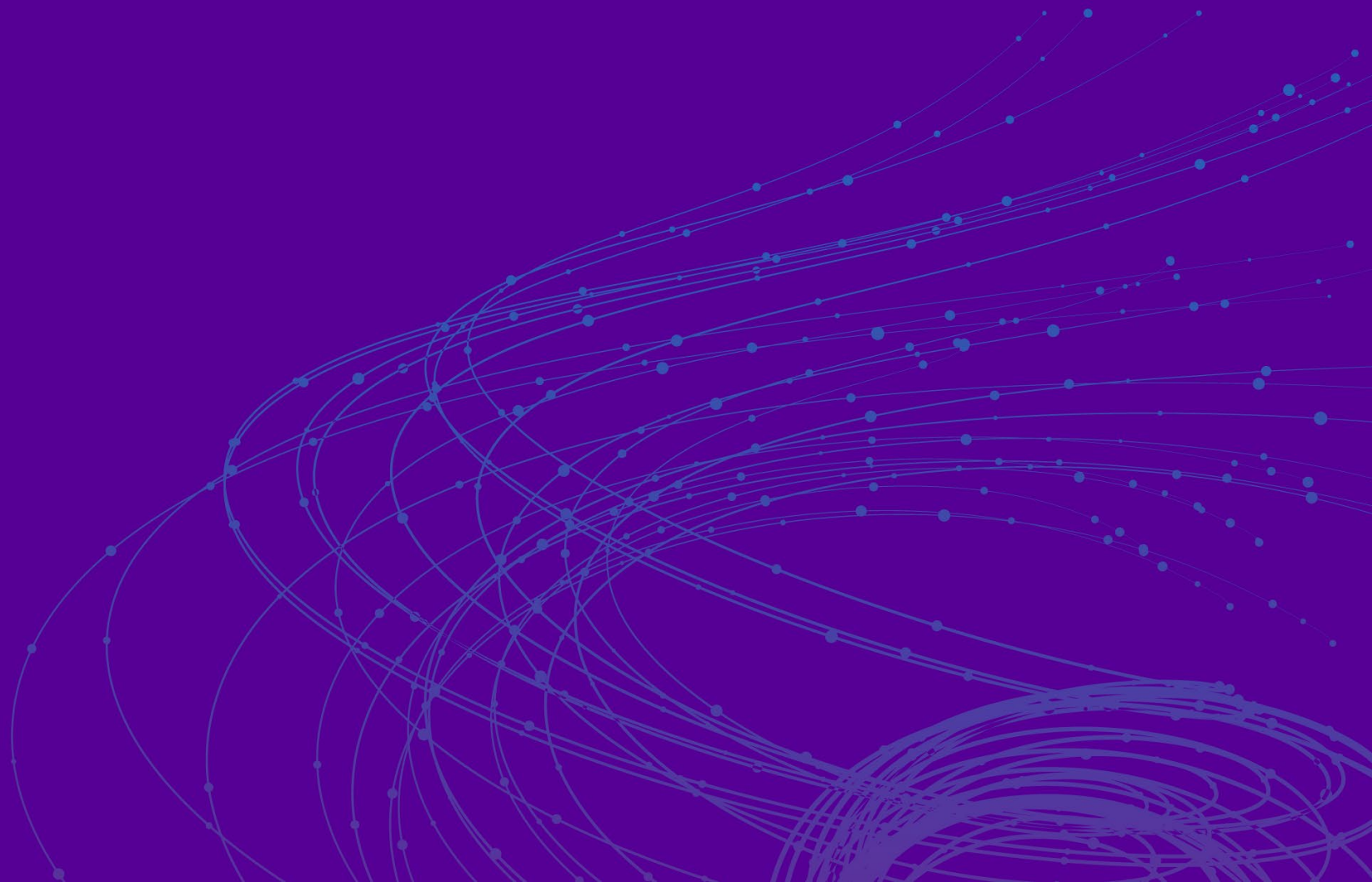


- Interpretation: Incidents are clustered in 3 sets. This may indicate a certain pattern (with an underlying root cause to be investigated) in incident occurrences, or alternately may also indicate different behavioral patterns among the incident responders

* Axes represent the first 3 principal components that define this dataset

RSAConference2019

Conclusion



“Every risk manager needs a machine learning toolbox”

- We covered 3 scenarios in which a Cybersecurity Risk Manager can benefit from Machine Learning techniques:
  - Scenario #1: How to identify top risks using Topic Modelling?
  - Scenario #2: How to identify latent/emerging risks using Natural Language Processing?
  - Scenario #3: How to identify risk management process issues using PCA clustering?

Direct applicability of each scenario

- Topic modelling can be applied to any text heavy risk management dataset (incidents, security/audit findings, exceptions, etc.) to identify the key themes
- Clustering helps identify the patterns and relationships within these risk management datasets, that may not be immediately visible to the analyst
- Experimental utilization of word embeddings, and text generation using LSTM RNNs, may help the analyst identify emerging risk trends, latent/dormant relationships, or themes in these documents

“Every risk manager needs a machine learning toolbox”

- These tools and approaches:
  - Do NOT offer a silver bullet, magic wand, or a crystal ball
  - They help and support the analyst identify dormant/latent themes, patterns, and relationships
  - They require a human (cybersecurity risk manager) in the loop

“Apply” slide

- Suggested immediate actions:
  - Identification of in-house risk relevant datasets
- Suggested action items within 3 months:
  - Application of Topic Modelling, NLP, and PCA analysis on these datasets
  - Suggested tools: Keras, Jupyter notebooks, Word2Vec, R (tm, lda, ls, pca, ggplot2 packages)
  - Utilize these scenarios as part of the enterprise risk review cadence

RSAConference2019

Q&A

Bugra Karabey

bugrak@microsoft.com