Use Cases for Machine Learning for Cyber Security

Dr Cyril Onwubiko
C-MRiC.ORG

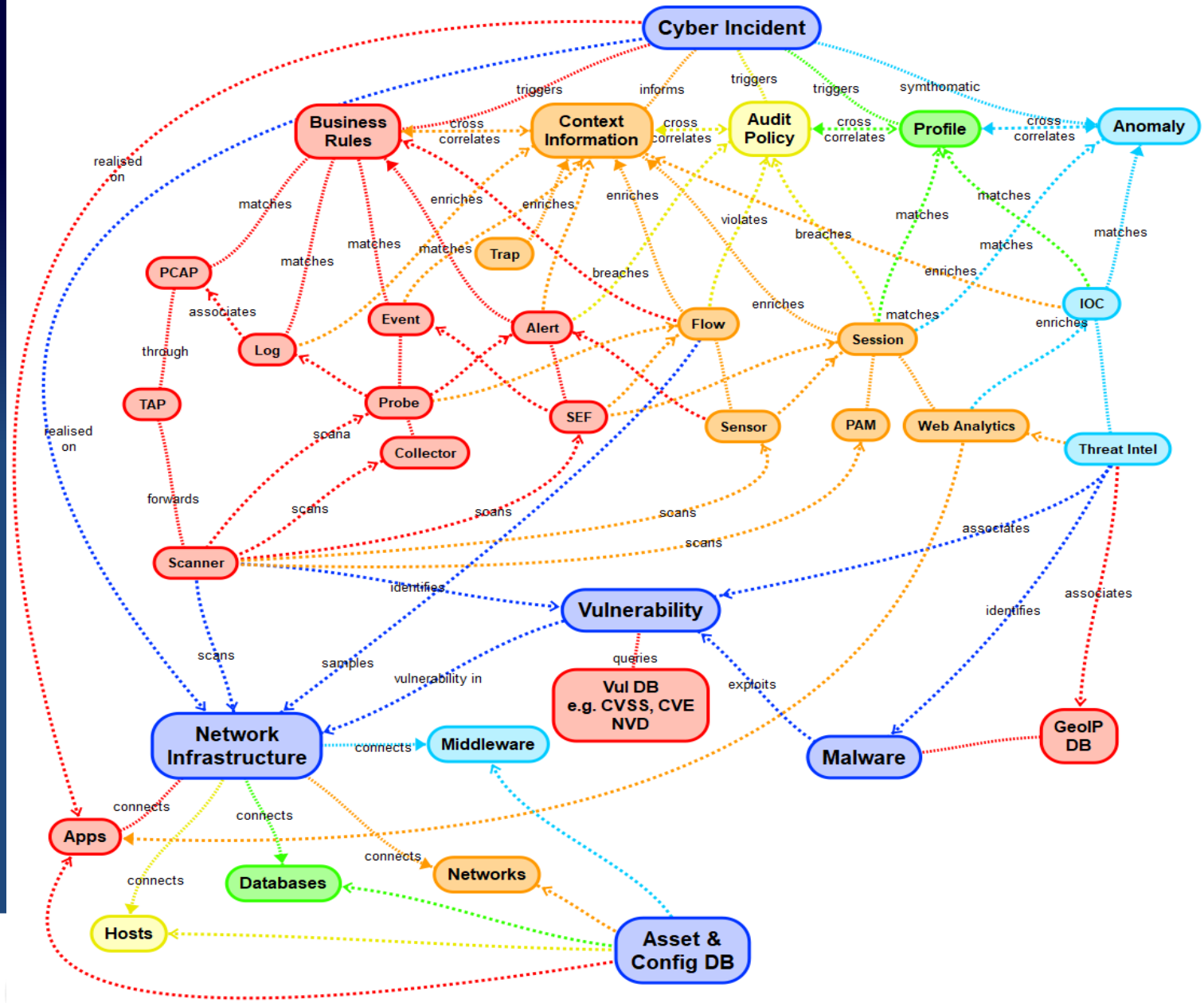
Workshop on Machine Learning for Cyber Security

11th March 2019

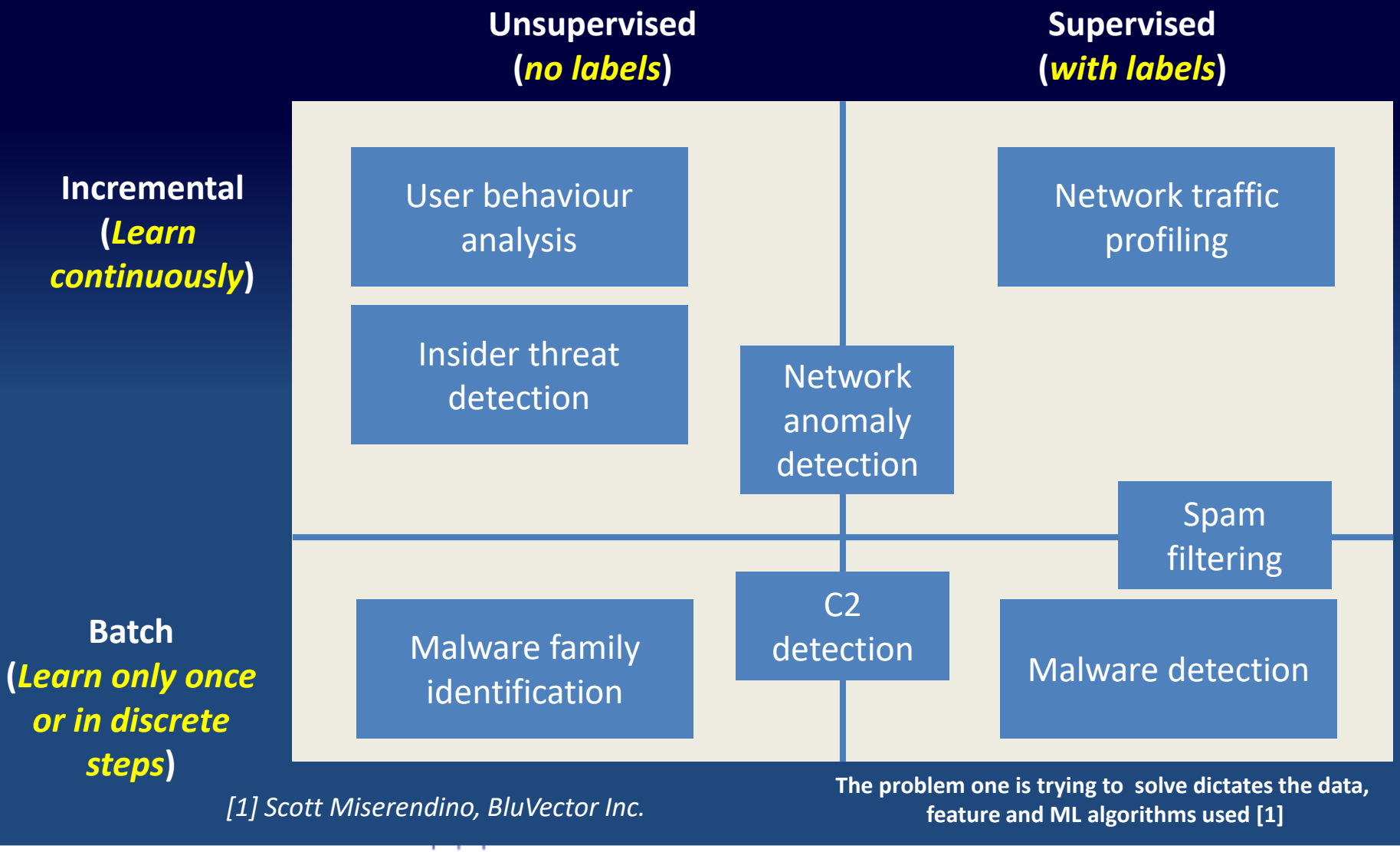
C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

Machine Learning is applied in Cyber Security to detect emerging and sophisticated attacks, especially around ‘point solutions’, e.g. Endpoint detection, Botnets, DNS security, Transaction monitoring and Analytics.

And what are the things Machine Learning for Cyber Security may not be ideal?



[1] Cyril Onwubiko (2018) CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process, IEEE CyberSA 2018 DOI: 10.1109/CyberSA.2018.8551486



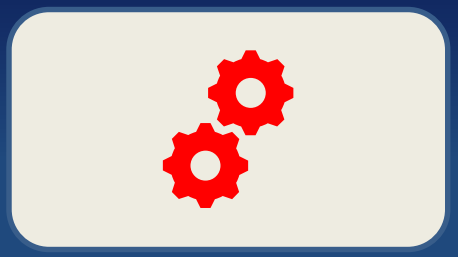
[1] Scott Miserendino, BluVector Inc.

The problem one is trying to solve dictates the data, feature and ML algorithms used [1]

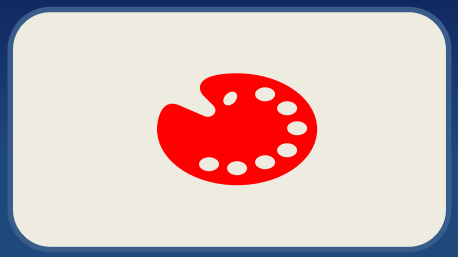
C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

ML Problem Space



ML Algorithms



Feature Engineering

Data Set (Training & Testing)

Examples

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Case Studies

- **Malware Detection**
  - Malware detection, network-based attack detection and code detection and C2 & Bots
- **Profiling & Security Analytics**
  - User & Entity profiling, behavioural analytics, big data, security and web analytics etc
- **Cyber Security Operations Centre**
  - Security Monitoring, Flow Analysis, Log Collection & Collation, Correlation, Analysis, and Cyber Incident Management and 'Human-in-the-loop' etc

C-MRiC.ORG®

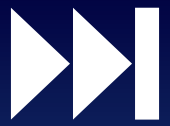
Centre for Multidisciplinary Research, Innovation and Collaboration

Malware Detection

- Intrusion detection systems (IDS) using Rule-based, Heuristic, Machine Learning - Supervised & Unsupervised Learning
- Detect **Bot / C2 (Command & Control)**
- Correlating Intrusion detection alerts on Bot malware infections
- Content inspection – content is inspected against feature set of malignant (malicious) content
- Temporal heuristic & behavioural analysis
- **Featureless Engineering** for Anomaly detection

Feature Engineering

- Cost – Expensive
- Domain Experts / Domain Knowledge
- Data Scientist
- Complex and Convoluted
- Tedious



Parsers / Plugins

UserData Fields Features

Feature engineering, while generally known to boost classification metrics, however, it creates a need for substantial investment of expensive and scarce data science expertise. We find that reliance on domain expertise and feature engineering severely inhibits the feasibility of applying existing correlation and filtering methods in practice [2]

[2] Egon Kidmose – PhD Thesis –Network-based Detection of Malicious Activities – A Corporate Network Perspective, 2018

Features, Reliability & Relevance

Indicators of Compromise (IoC)

- Constantly evolving features
- Feature Reliability & Relevance

Features	Features	Features	Features
IP Address (IPv4 or IPv6)	FilePath	FileHASH-SHA256	Encrypt-AES256
Domain	CIDR	FileHash-IMPHASH	Encrypt-AES128
Hostname	CVE	Mutex	Encrypt-AES224
FQDN	Email	SSDeep /CTPH [3]	Encrypt-DES
URL	FileHash-MD5	GeoIP	Encrypt-Unknown
URI	FileHASH-SHA1	DNS	YARA

[3] SSDeep Project – context triggered piecewise hashes (CTPH) - https://ssdeep-project.github.io/ssdeep/index.html

Feature Engineering Conundrum

- Netflix Prize
  - The **Netflix Prize** was an open competition for the best collaborative filtering algorithm to predict user ratings for films, based on previous ratings without any other information about the users or films, i.e. without the users or the films being identified except by numbers assigned for the contest [3].
  - Cost millions in dollars
  - Took almost 3 years (2 Oct 2006 – 18 Sept. 2009)
  - Won by BellKor's Pragmatic Chaos

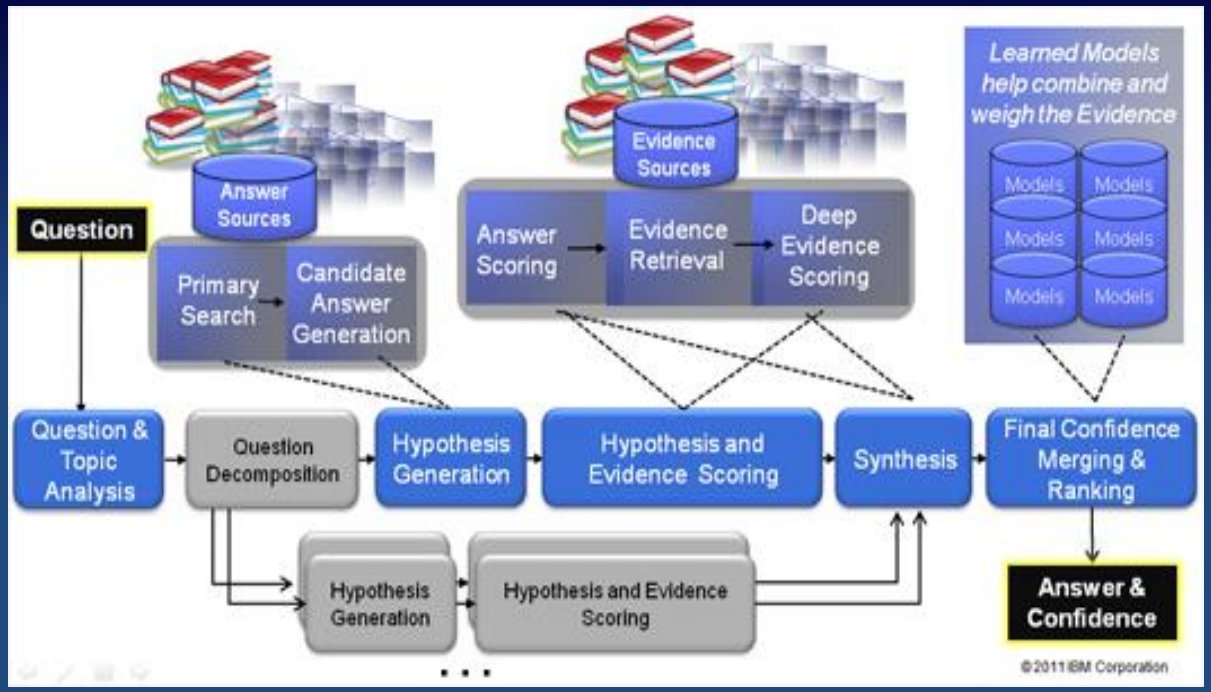
[3] Wikipedia – https://en.Wikipedia.org/wiki/Netflix_Prize

Feature Engineering Conundrum

- IBM DeepQA
  - The **IBM DeepQA Project** was commissioned to build **Watson**.
  - Real language is real hard for computers to grasp. The meaning behind words is implicit, ambiguous and highly contextual.
  - The underlying philosophy of our research approach is that true intelligence will emerge from the development and integration of many different algorithms each looking at the data from different perspectives. No one programmer, no one program design from top to bottom will have all it needs to understand language. Rather a system must evolve from the continuous contribution of many different algorithms. These must all balance and combine to form a holistic and accurate interpretation of the intended meaning. DeepQA is a software architecture for deep content analysis and evidence-based reasoning that embodies that philosophy [4].

[4] IBM – https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=2159

Deep Learning - Conundrum



[4] IBM – https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=2159

- Uses advanced natural language processing, semantic analysis, information retrieval, automated reasoning and machine learning.
- DeepQA deeply analyzes natural language input to better find, synthesize, deliver and organize relevant answers and their justifications from the wealth of knowledge available in a combination of existing natural language text and databases.
- Involves 6 collaborating Universities
- 25 IBM Researchers
- In 4 years

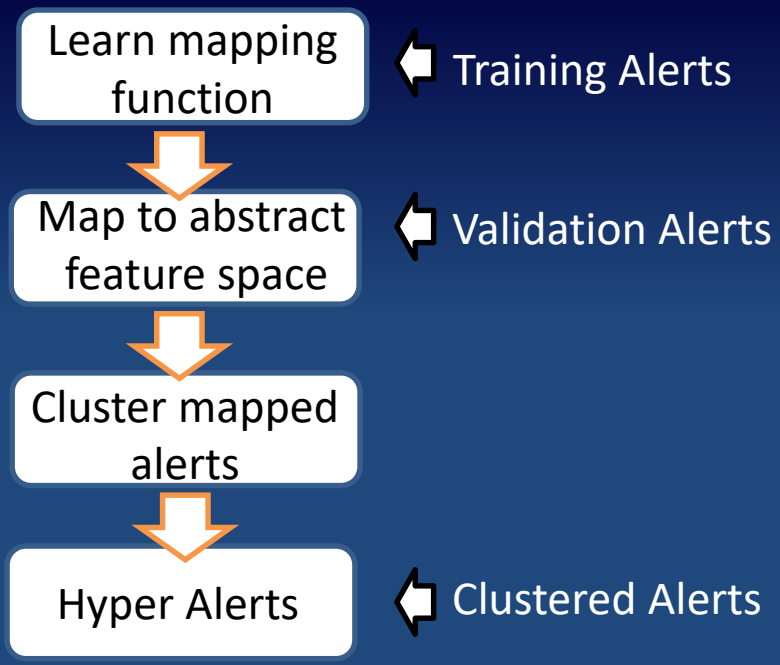
Featureless Engineering & without Domain Expertise

- A case study of Filtering & Correlation of IDS Alerts
  - IDSs produce high volumes of logs/alerts, raise high false positives
  - Reliability / Trust?
  - Alert ≠ Incident
- **Proposal** Neural Networks + Latent Semantic Analysis (LSA) [5] to avoid feature engineering – promising result as reported in [5]

[5] Egon Kidmose – PhD Thesis –Network-based Detection of Malicious Activities – A Corporate Network Perspective, 2018

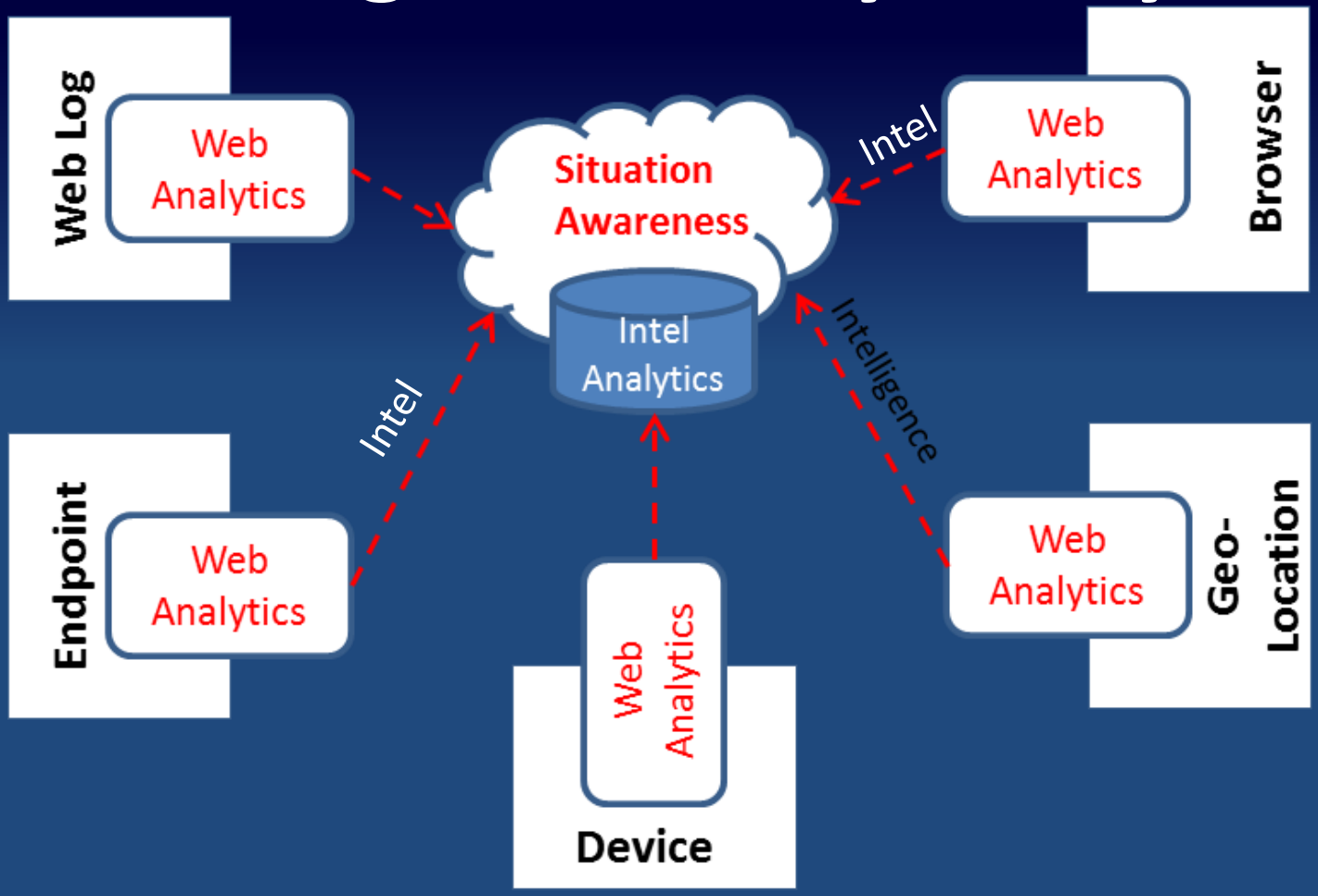
An Approach

- Use Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) and Latent Semantic Analysis (LSA)
  - Alerts → Hyper Alerts (fusion)
  - Alerts are human readable strings of texts
  - Eliminates need for feature engineering and issues of maintenance and adaptability
- **Proposal** LSTM RNN architecture is used to learn from labelled alerts
- LSA is then applied to unlabeled alerts (see implementation on [5 & 6]



[5] Egon Kidmose – PhD Thesis –Network-based Detection of Malicious Activities – A Corporate Network Perspective, 2018
[6] Egon Kidmose - https://github.com/kidmose/lstm-rnn-correlation

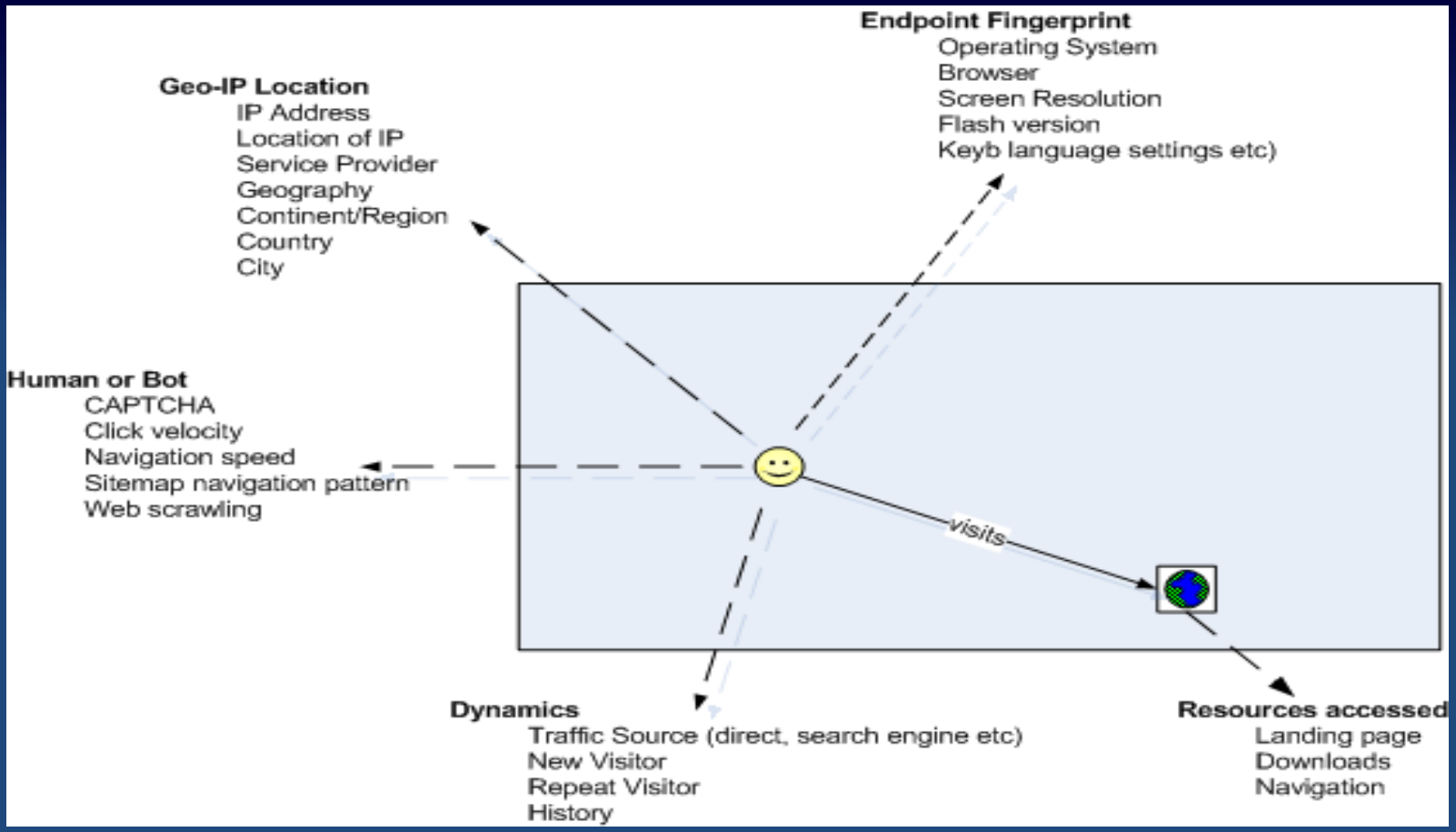
Profiling & Security Analytics



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Entity Profiling



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Endpoint Profiling

- Endpoint fingerprint
  - Operating system fingerprint
  - Browser fingerprint
  - Screen resolution
  - Screen colours
  - Flash version
  - Host IP Address
  - Language setting
  - Robotics (Human or Robot)
  - Device type (Mobile, Tablet, Desktop or Others)
  - Smartphone and Table OS,
- Geo-location fingerprint
  - Service provider fingerprint
  - Country fingerprint
  - City fingerprint

Cyber Security Operations Centre

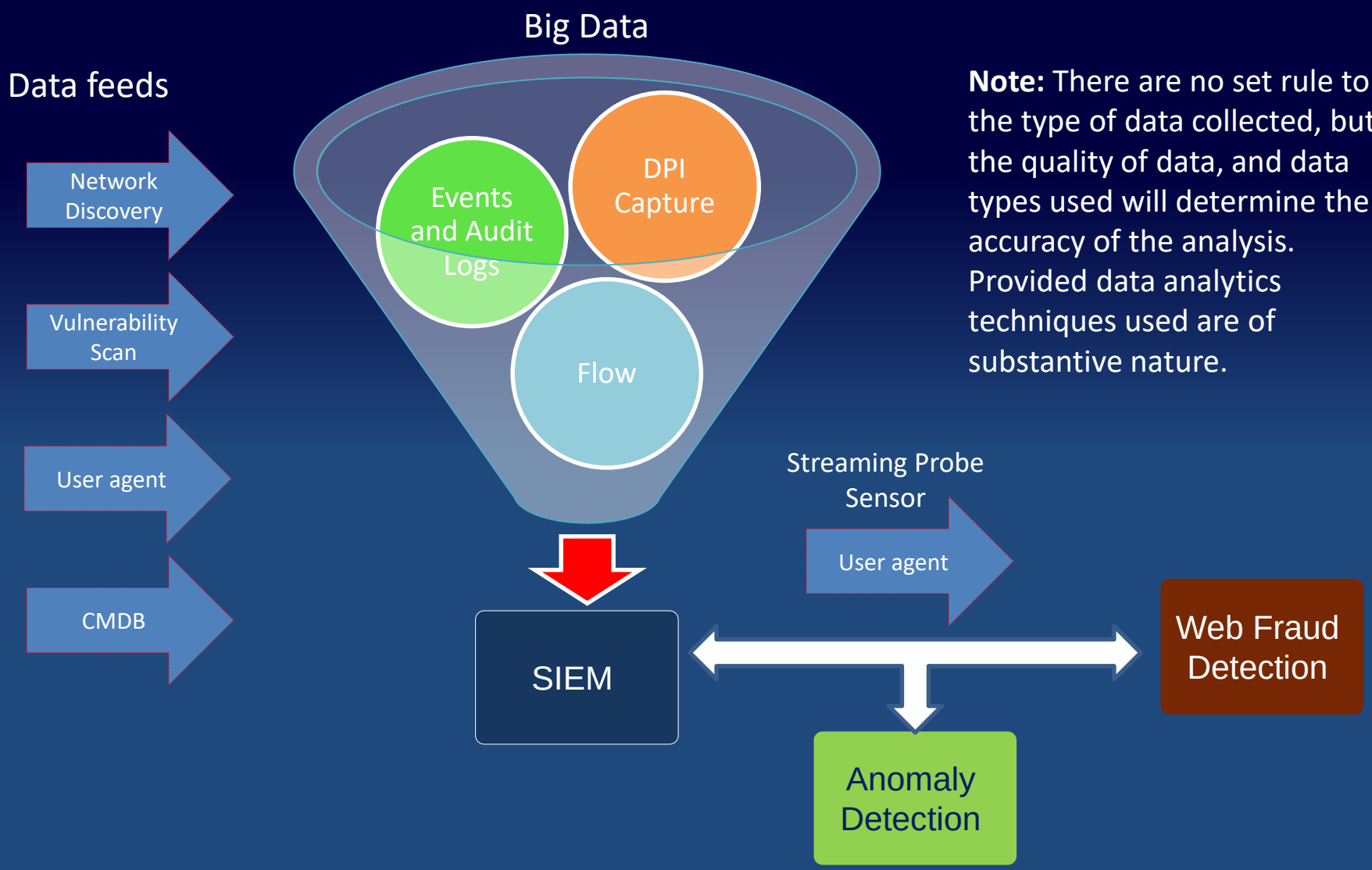
- Technology
  - Tools and technologies used to monitor the network, ranging from ML Anomaly detection, sensors, AV, firewalls, SIEM etc. These tools automatically detect and alert when a potential incident occurs

- Process
  - Processes, policies and procedures leveraged by SOC to monitor, operate and conduct cyber incident investigation, such as incident playbooks, cyber incident management process etc.

- People
  - Analysts, Operators, Administrators & Incident Responders, Threat Hunters etc. who operate, monitor and coordinate cyber incident response, leveraging technology and process

C-MRiC.ORG®

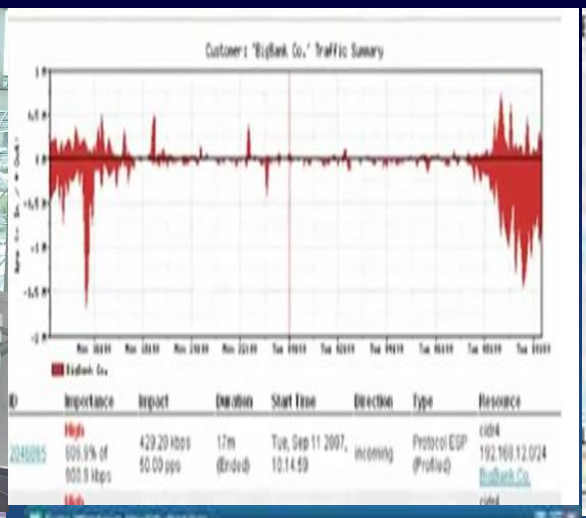
Centre for Multidisciplinary Research, Innovation and Collaboration

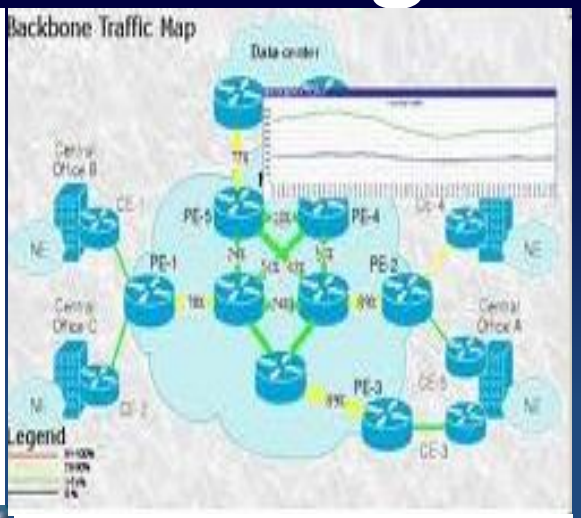


C-MRiC.ORG®

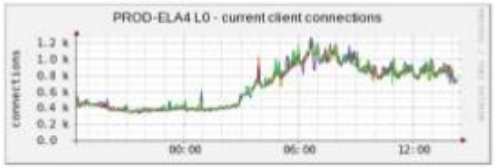
Centre for Multidisciplinary Research, Innovation and Collaboration

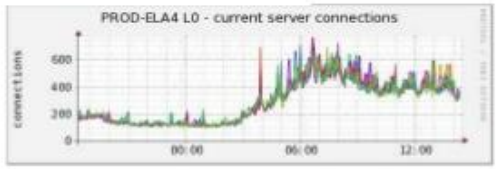
CSOC Operations Monitoring





Monitoring:





C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

CYBER INCIDENT RESPONSE

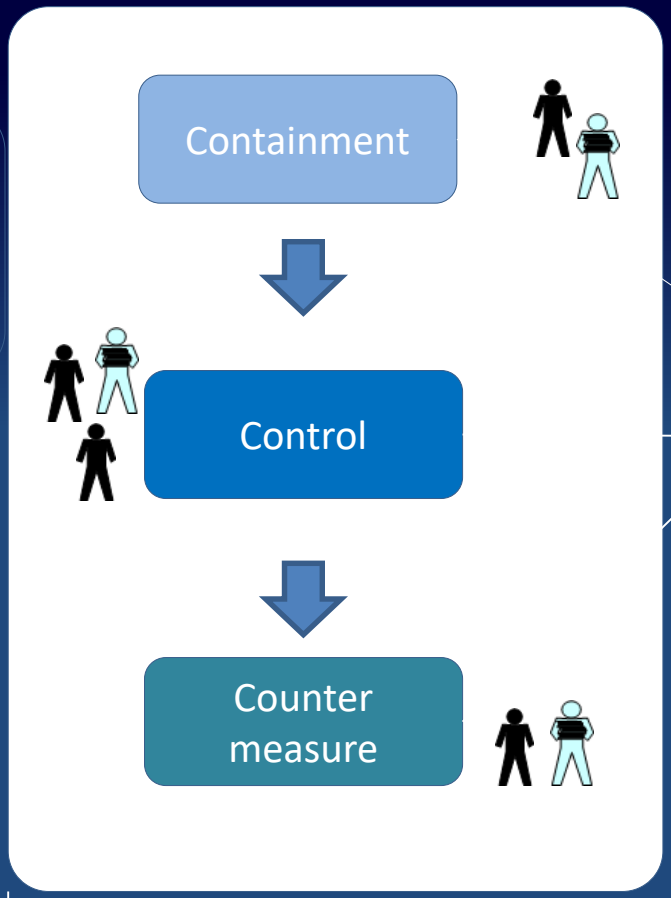
Internal Function

Source of attack (Geo-IP), IP address of Attacker, suspected type of attack, target endpoint(s), location of endpoints, categorisation of incident based on type of attack/target

Initial Triage

Incidents
Major Incidents
Minor Incidents

Time is of essence / critical Major incident escalation / reporting and mitigation in minutes (approx.)



External Function

Callout Specialist Services

- Cyber Incident Responders
- Digital Forensic Investigators
- FIRST* Responders

Reporting

** FIRST – Forum of Incident Response and Security Teams*

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

Conclusion

- AI, ML & DL have been applied to solve Cyber Security real-life problems ranging from malware detection to correlation of alerts and behavioural analytics.
- While ML is extremely useful, feature engineering can be complex and expensive and requires domain expertise and data science, both of which are scare and comes at a premium.
- Human-in-the-loop is and will still be needed in Cyber Security.

Cyber Science 2019 Conference

https://www.c-mric.com/conferences

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Thank – You!

Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC.ORG)

submission@c-mric.org

www.C-MRiC.ORG

@CMRiCORG

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration