BTECH 451

Threat Detection and Behaviour Profiling

Academic Supervisor: Aniket Mahanti

Industry Supervisors: Ryan Cotterell & Malcolm Allen

ASB

Project Objective

Evolve

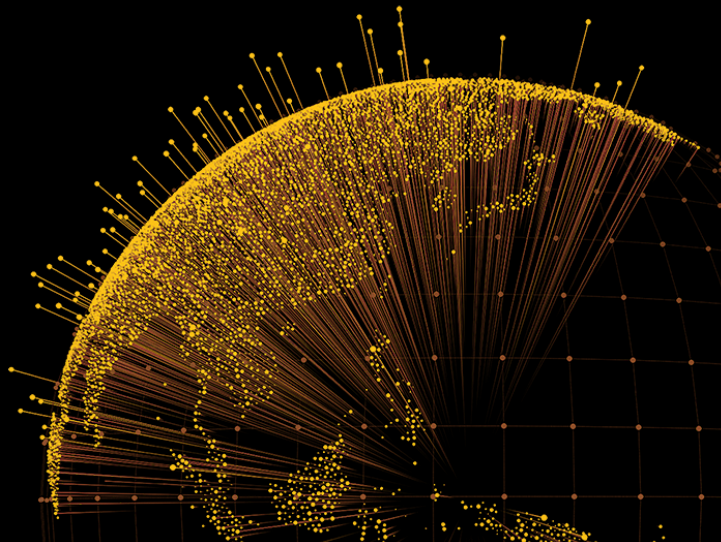
Grow

Mature

Project Phases

- Threat Profiling and Detection

- Behaviour Profiling and Base lining



Case Studies

- TJ Max and Marshalls Breach – 2007
- Carbanak – 2012 - ?
- Shell Shock – 2014
- Heartbleed – 2014
- Sony Entertainment Breach – 2014
- JP Morgan and Chase Breach – 2014
- Apple Icloud Breach - 2014

Case Studies

- TJ Max and Marshalls Breach – 2007
- Carbanak – 2012 - ?
- Shell Shock – 2014
- Heartbleed – 2014
- Sony Entertainment Breach – 2014
- JP Morgan and Chase Breach – 2014
- Apple Icloud Breach - 2014

Carbanak

- Losses from Carbanak per bank range from $2.5 million to approximately $10 million
- Up to 100 financial institutions have been hit. Total financial losses could be as a high as $1bn.
- Each bank robbery took 2-4 months, from infecting the first computer to cashing the money out

Lockheed Martin, 2014

How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Cash transfer systems

3. Mimicking the staff

How the money was stolen

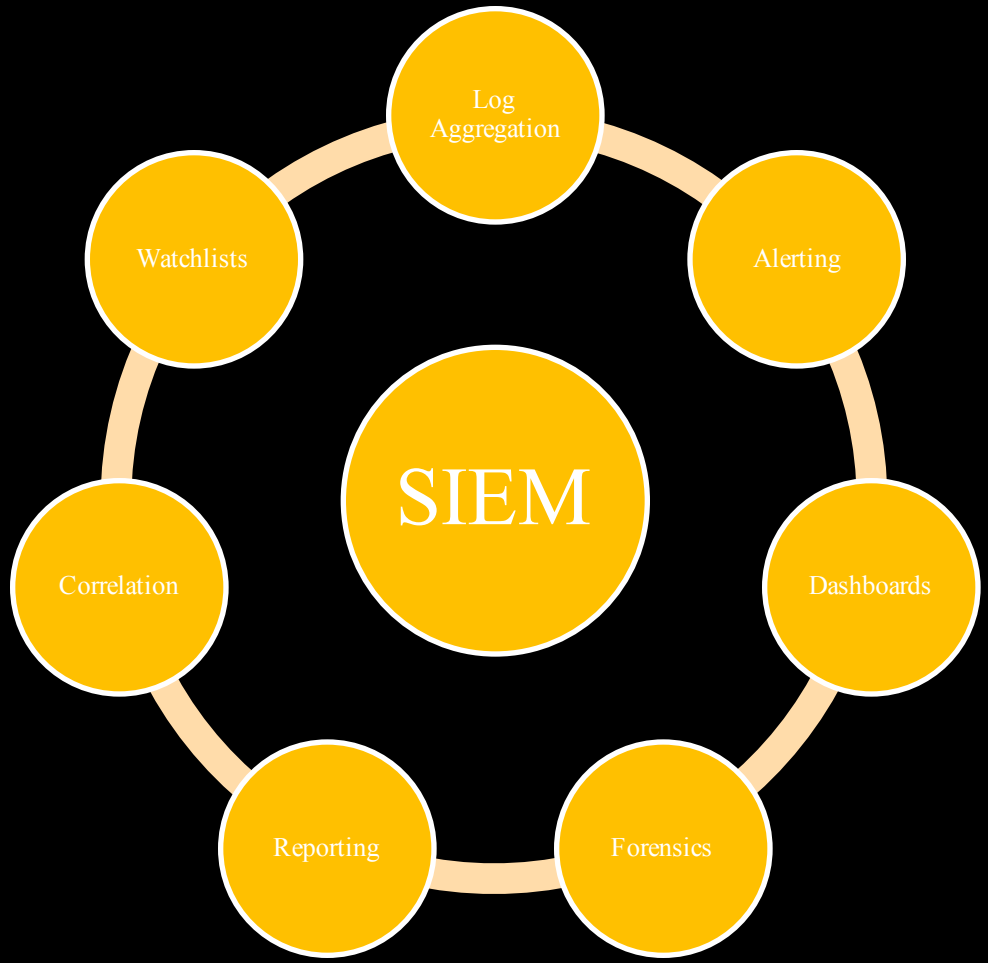
Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

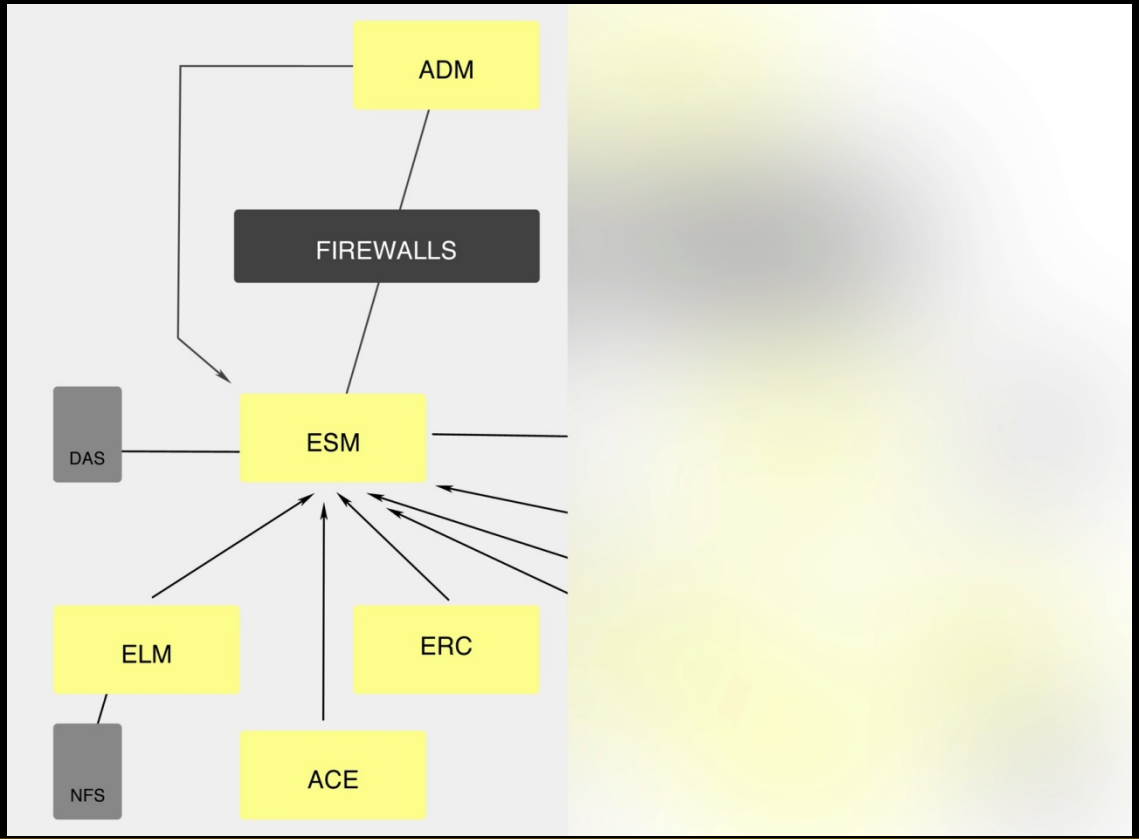
Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

GREAT KASPERSKY


Log Aggregation
Alerting
Dashboards
Forensics
Reporting
Correlation
Watchlists
SIEM

SIEM Architecture

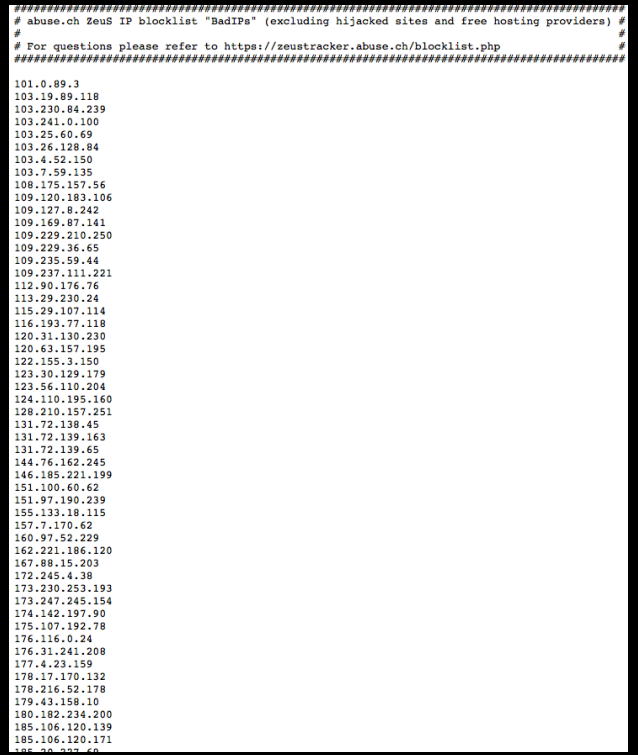


SIEM – Use of Global Threat Intelligence (GTI)

- Cloud based threat intelligence tool
- Gathers data from millions of sensors worldwide
- Allows real time decision making based on preset rules
  - File Reputation
  - Web Reputation
  - Message Reputation
  - Network Connection Reputation

SIEM – Use of IP Blacklists

- Third party blacklists of known malicious activity
- Open source databases
  - Malc0de
  - EmergingThreats
- Can target particular types of malware
  - Zeus tracker
  - Dyre



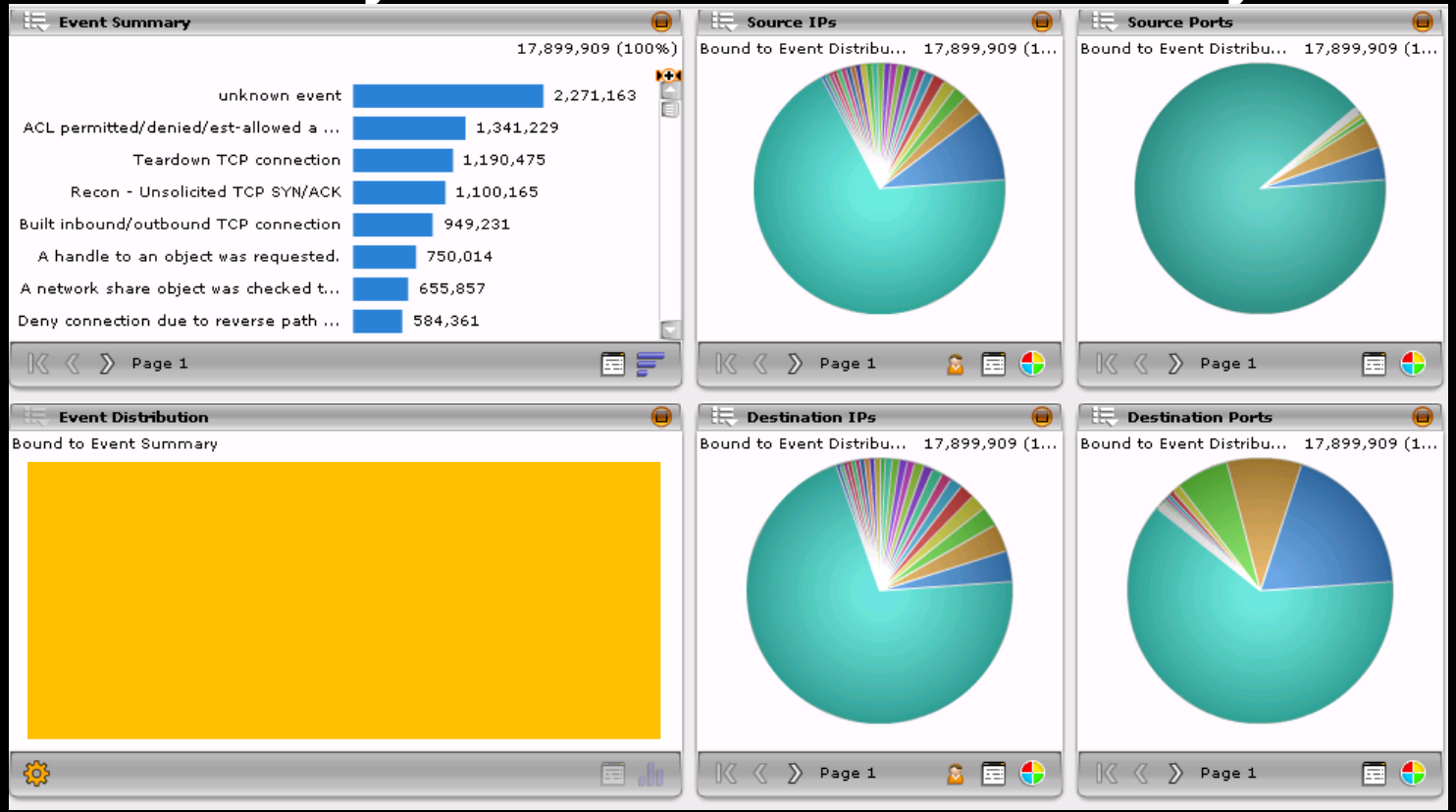
```
###########################################################################
# abuse.ch ZeuS IP blocklist "BadIPs" (excluding hijacked sites and free hosting providers) #
#                                                                         #
# For questions please refer to https://zeustracker.abuse.ch/blocklist.php                #
###########################################################################

101.0.89.3
103.19.89.118
103.230.84.239
103.241.0.100
103.25.60.69
103.26.128.84
103.4.52.150
103.7.59.135
108.175.157.56
109.120.183.106
109.127.8.242
109.169.87.141
109.229.210.250
109.229.36.65
109.235.59.44
109.237.111.221
112.90.176.76
113.29.230.24
115.29.107.114
116.193.77.118
120.31.130.230
120.63.157.195
122.155.3.150
123.30.129.179
123.56.110.204
124.110.195.160
128.210.157.251
131.72.138.45
131.72.139.163
131.72.139.65
144.76.162.245
146.185.221.199
151.100.60.62
151.97.190.239
155.133.18.115
157.7.170.62
160.97.52.229
162.221.186.120
167.88.15.203
172.245.4.38
173.230.253.193
173.247.245.154
174.142.197.90
175.107.192.78
176.116.0.24
176.31.241.208
177.4.23.159
178.17.170.132
178.216.52.178
179.43.158.10
180.182.234.200
185.106.120.139
185.106.120.171
```

Abuse.ch – Swiss Security Blog, 2015

Current System

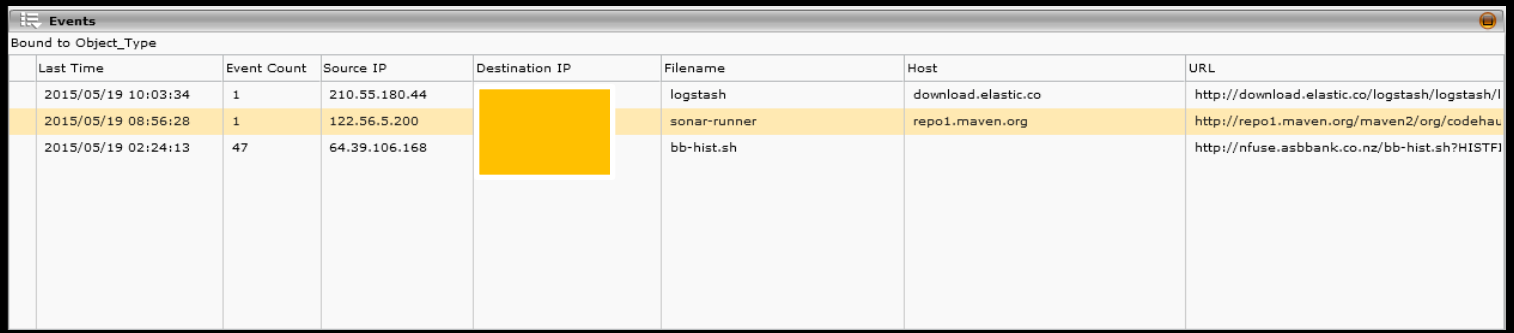
- Default Summary
- GTI Inbound and Outbound
- Inbound Exe
- Inbound Office

Current System – Default Summary



Current System – Inbound Exe.

- Detects and record all inbound executable files.
  - SEM looks into header of file to determine type.
  - Done by looking at the unique “signature ID”

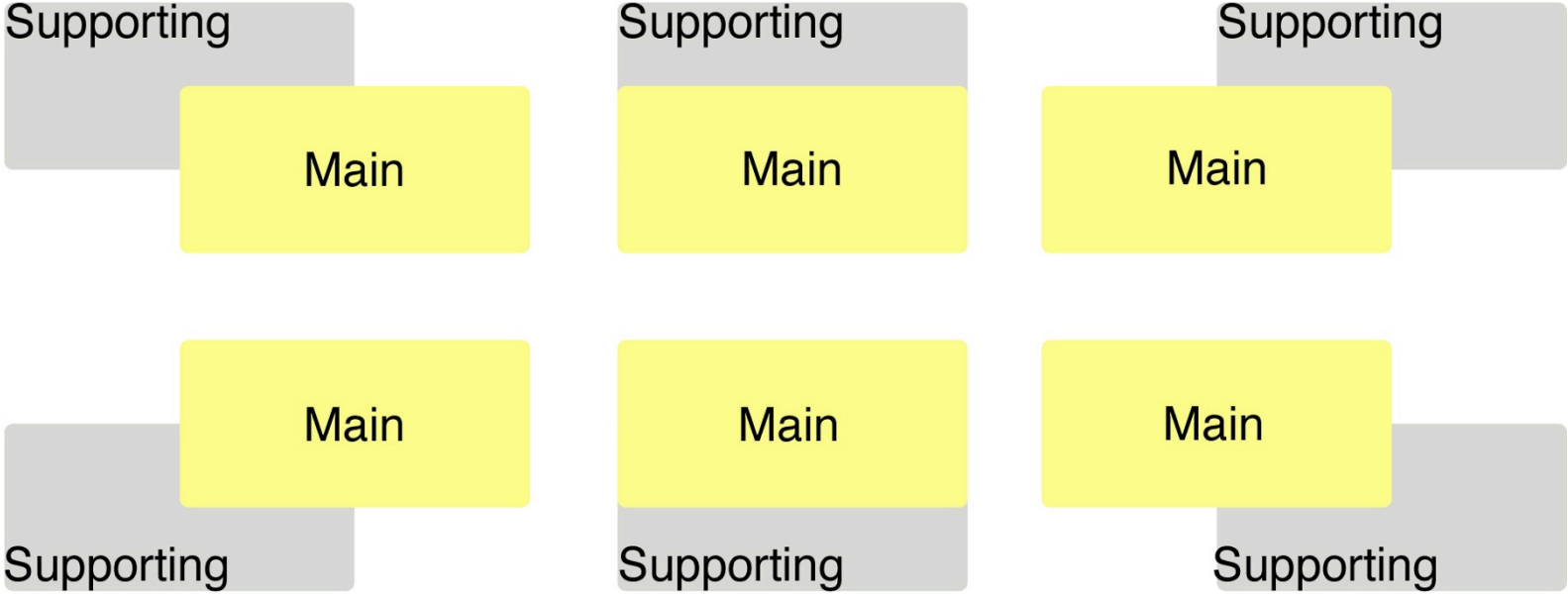


Events

Bound to Object_Type

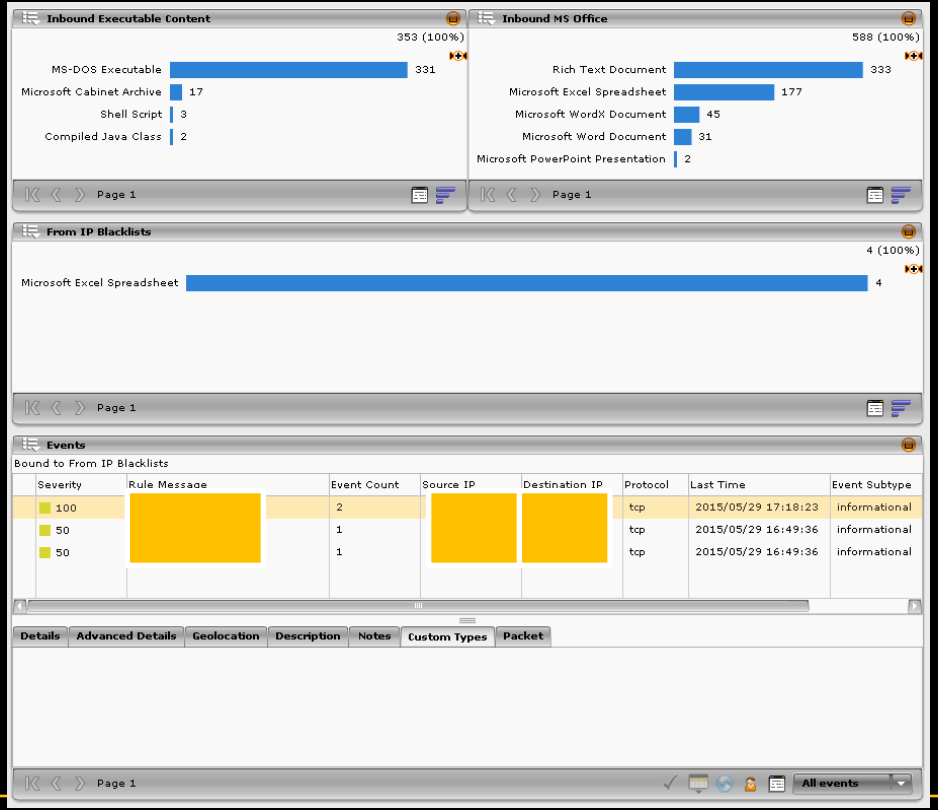
Last Time	Event Count	Source IP	Destination IP	Filename	Host	URL
2015/05/19 10:03:34	1	210.55.180.44		logstash	download.elastic.co	http://download.elastic.co/logstash/logstash/l
2015/05/19 08:56:28	1	122.56.5.200		sonar-runner	repo1.maven.org	http://repo1.maven.org/maven2/org/codehau
2015/05/19 02:24:13	47	64.39.106.168		bb-hist.sh		http://nfuse.asbbank.co.nz/bb-hist.sh?HISTFI

Subsystem Creation



Subsystem Creation – Version 1.0

Subsystem Creation – Malicious File Subsystem



Key Challenges

- Familiarity with and size of Dataset
- Missing Dataset
- Access Privelages

Timeline – Events prior to mid-year

Complete

Research on ASB's current implementation of the SIEM platform

Case studies on related security breaches

Research on current threats and mitigation techniques

Creation of customized subsystem and completion of first milestone

Current

Research on behaviour profiling and base lining methodoligies

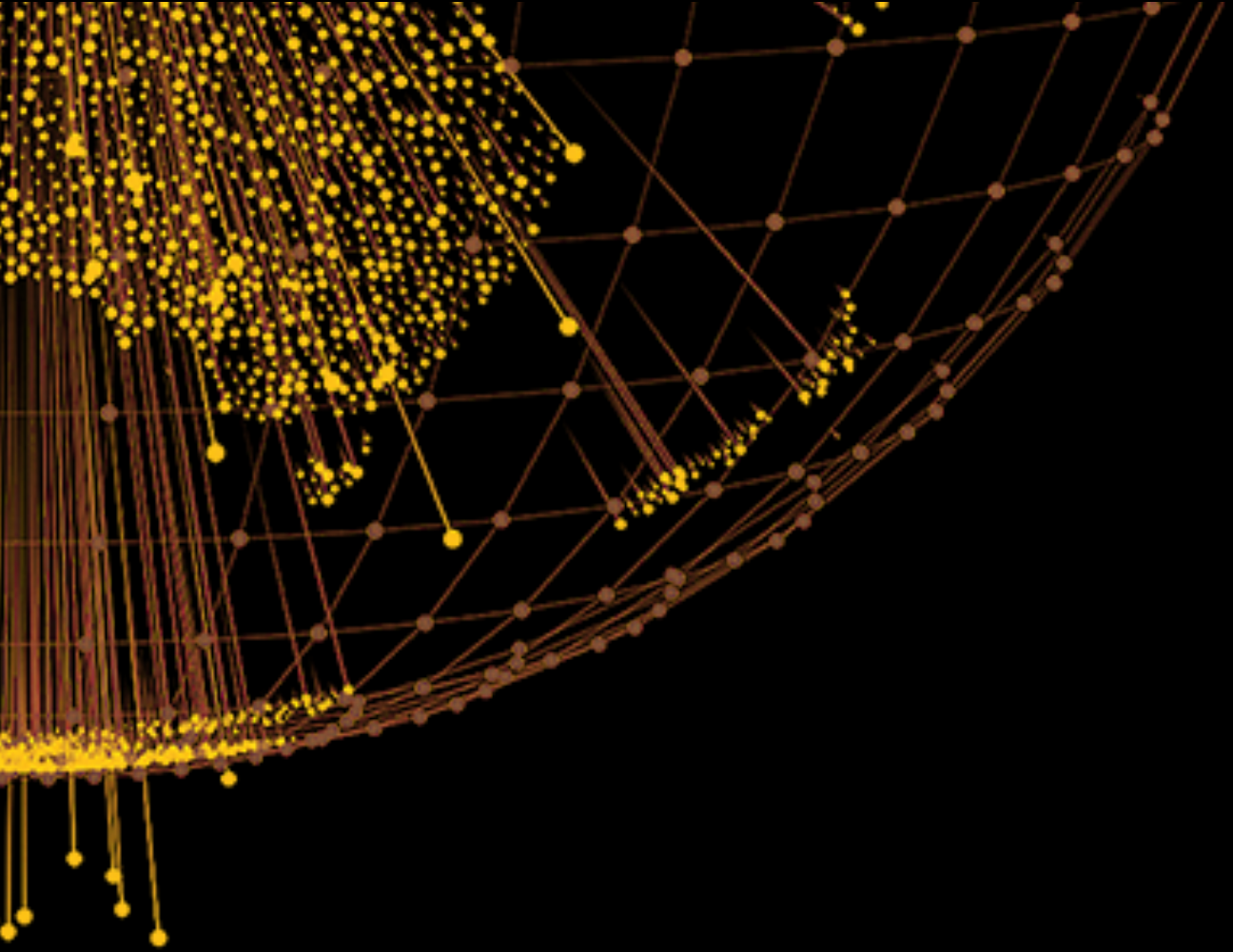
Literature survey of problem statement. Analysis of peer reviewed publications

Future

Selection of behaviour profiling scheme

Implementation of scheme in ASB Enterprise

Testing and evaluation of implemented scheme



Raafey Khan
raafey.khan@asb.co.nz