BTECH 451

Threat Detection and Behaviour Profiling

Academic Supervisor: Aniket Mahanti

Industry Supervisors: Ryan Cotterell & Malcolm Allen

ASB

Project Objective

Evolve

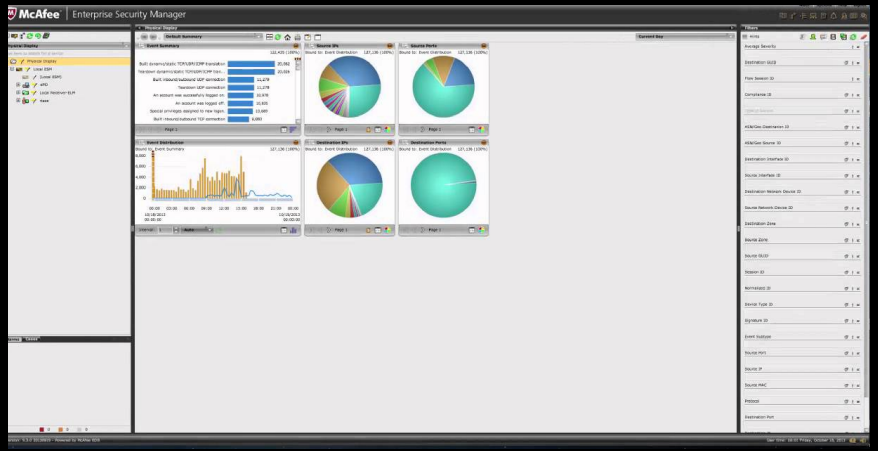
Grow

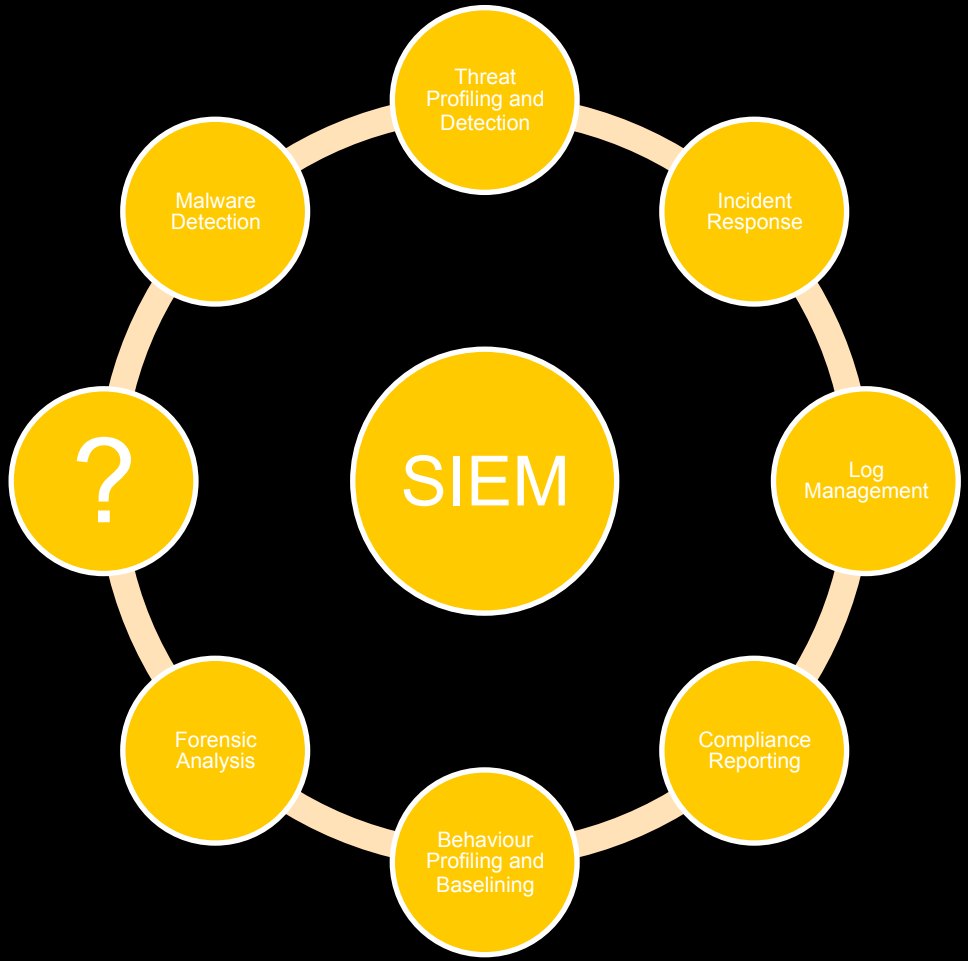
Mature

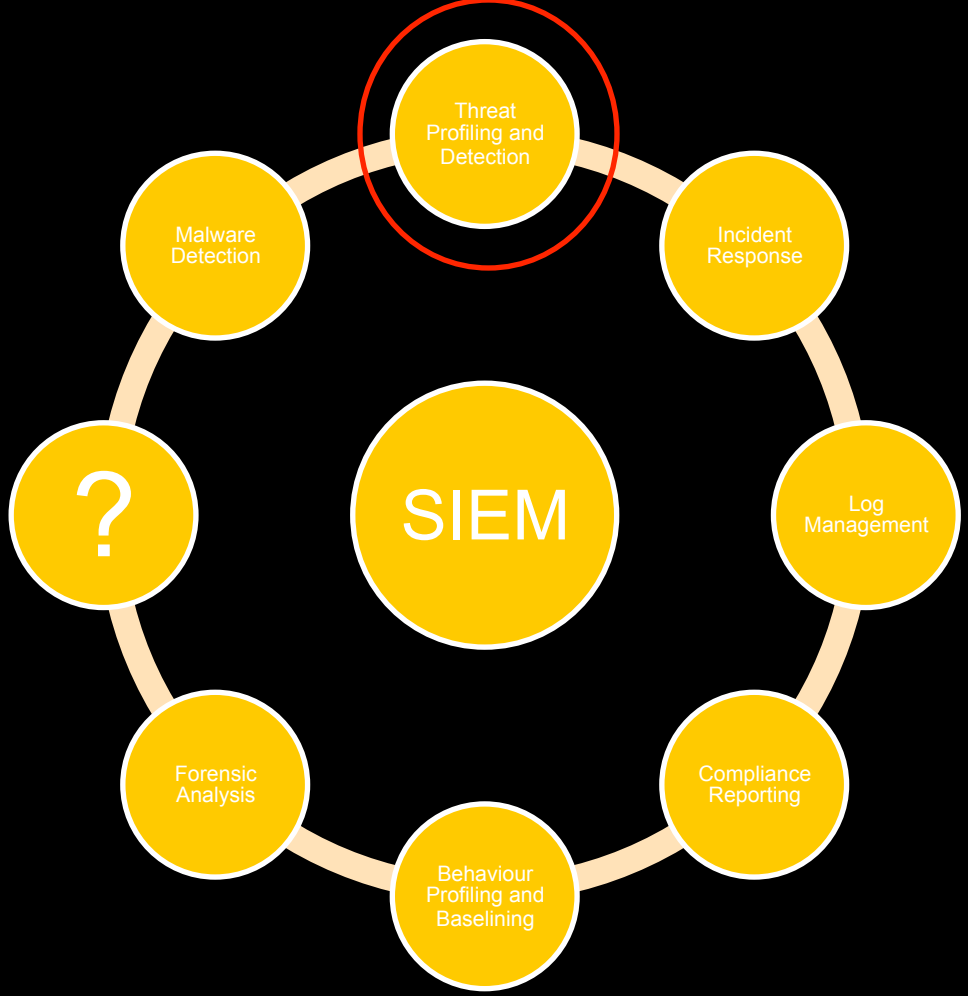
SIEM (Security Information Event Management)

Data In

Intelligence Out

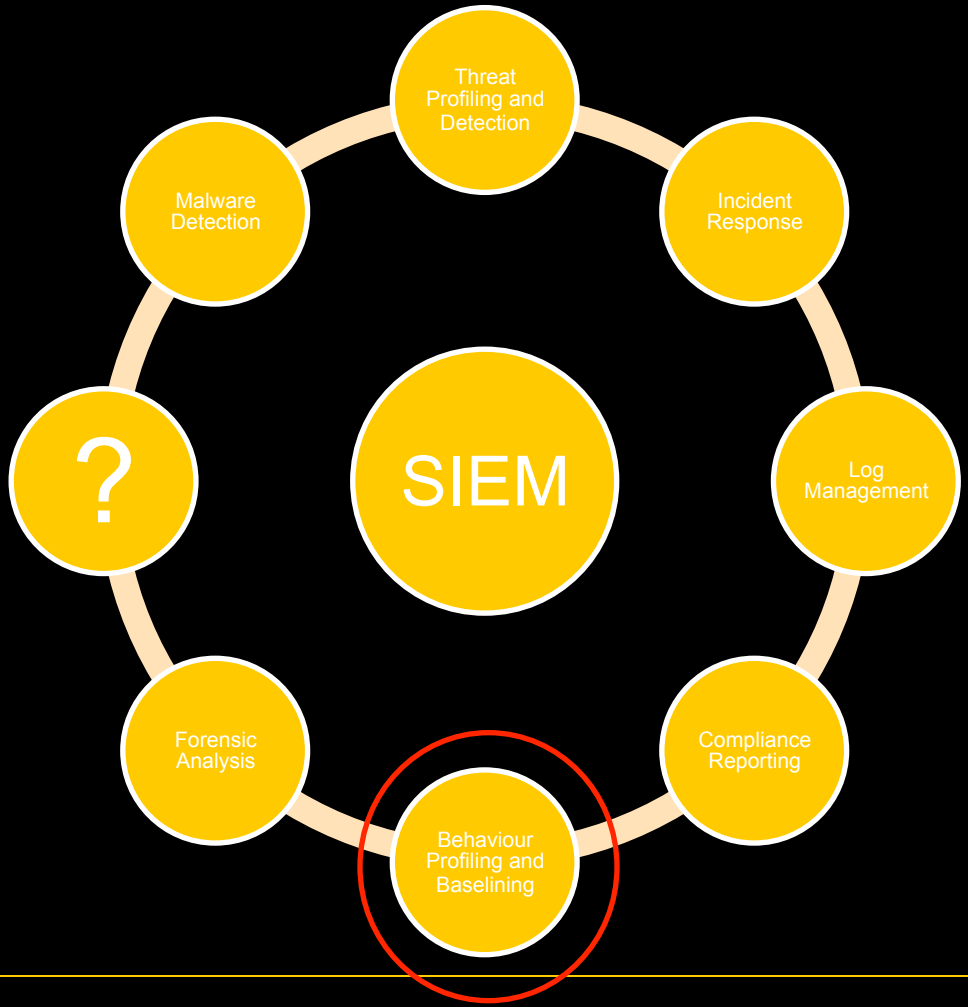



Threat Profiling and Detection
Incident Response
Log Management
Compliance Reporting
Behaviour Profiling and Baselining
Forensic Analysis
?
Malware Detection
SIEM


Threat Profiling and Detection
Incident Response
Log Management
Compliance Reporting
Behaviour Profiling and Baselining
Forensic Analysis
?
Malware Detection
SIEM

Threat Profiling and Detection

Establish a customized dashboard that provides a single point-of-view of potential threat related activity


Threat Profiling and Detection
Incident Response
Log Management
Compliance Reporting
Behaviour Profiling and Baselining
Forensic Analysis
?
Malware Detection
SIEM

Behaviour Profiling and Baselining

Research and recommend a behavioural profiling and base lining methodology that can be easily adopted.

Provide a working implementation based on the system admin community

Behaviour Profiling and Baselining

- Analyse normal behaviour
- Define what a “normal” user profile is
- Raise a flag when an event outside the norm occurs

Key Challenges

- Familiarity with dataset
- Limitations of the Tool
- Permission rules

Timeline – Events prior to mid-year

Complete

Research on ASB's current implementation of the SIEM platform

Familiarity with the dataset

Learning from security professionals

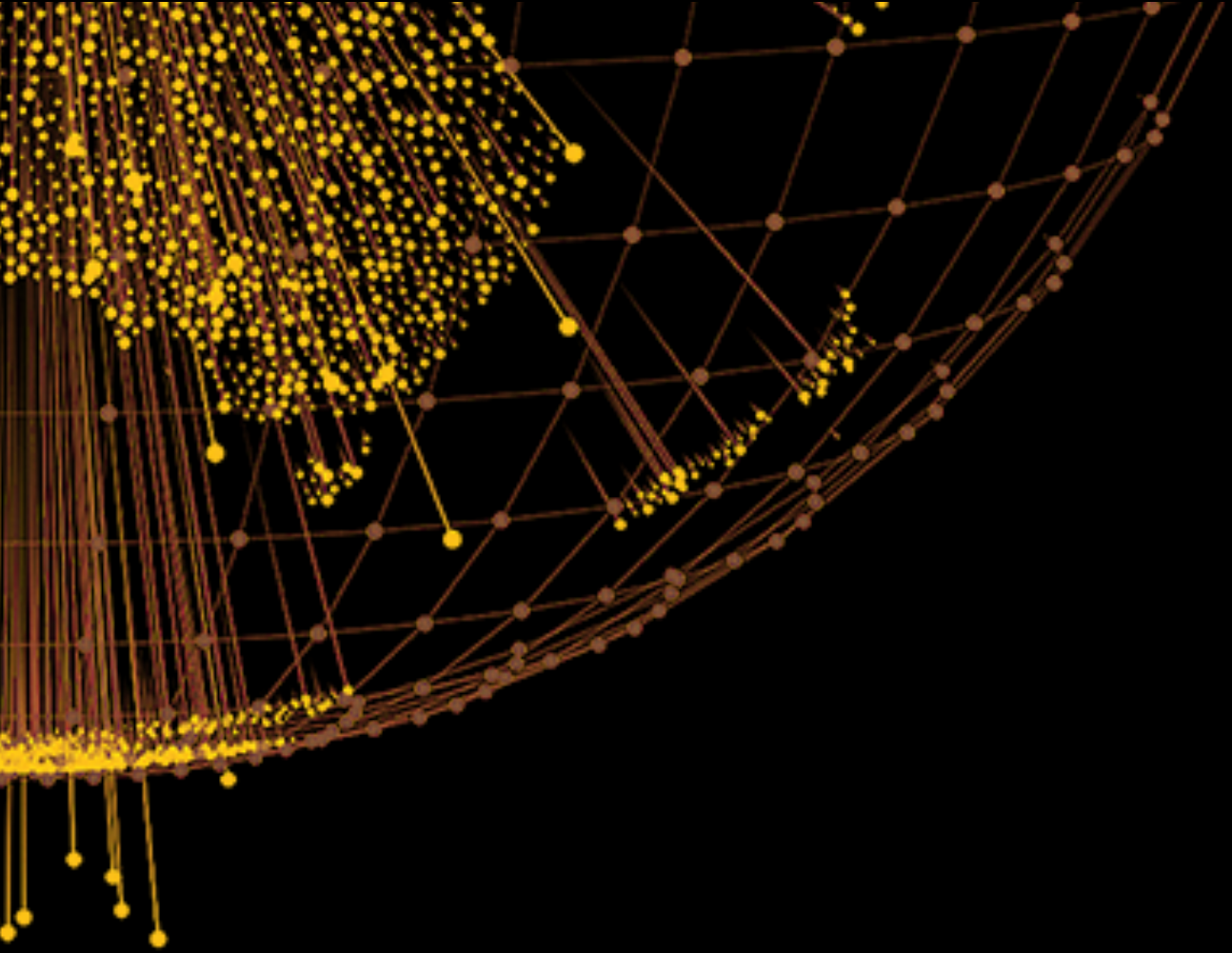
Current

Research on current threats and mitigation techniques

Creation of customized dashboard and completion of first milestone

Immediate

Research on behaviour profile and baselining



Raafey Khan
raafey.khan@asb.co.nz