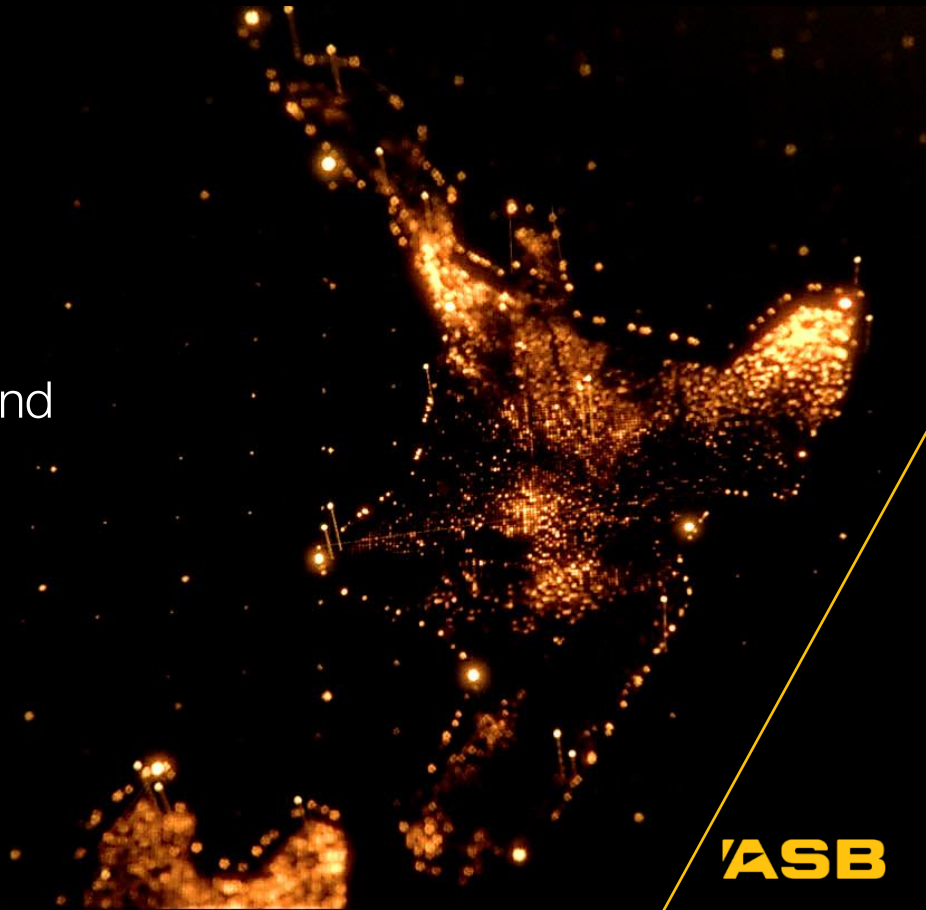
BTECH 451

Implementation of a Threat Detection and Behaviour Profiling Methodology

Raafey Khan

Academic Supervisor: Dr. Aniket Mahanti

Industry Supervisors: Malcolm Allen & Ryan Cotterell



Project Objective

Project Objective

SIEM

Phase 1: Information Security Summary

Phase 2: Behaviour Profiling

Phase 1: Implementation of an Information Security Summary System

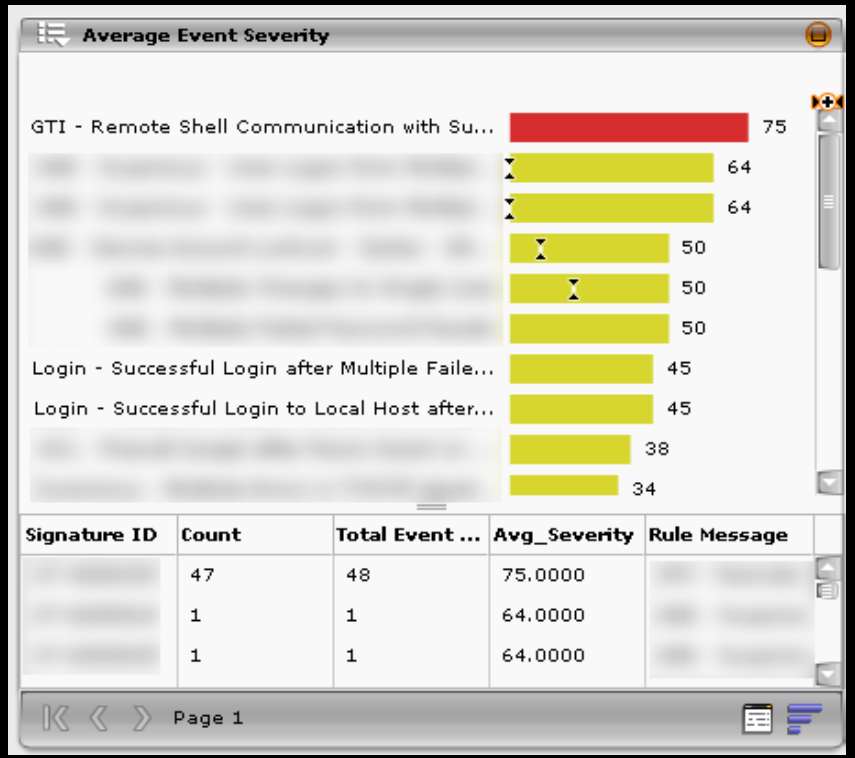
Carbanak Case Study

Internal System Research

Creation of the Information Security Summary System

Information Security Summary– Version 1.0

Information Security Summary – Version 2.0



Phase 2: Recommend and Implement a Behaviour Profiling Methodology

Literature Survey of Academic work

Validation of Methodology

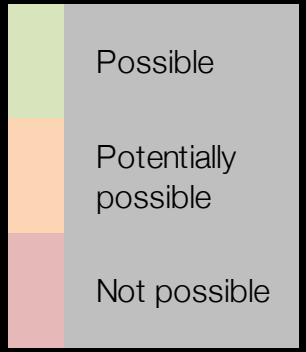
Phase 2: Recommend and Implement a Behaviour Profiling Methodology

Literature Survey of Academic work

Validation of Methodology

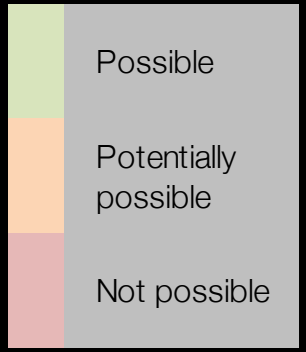
ASB Selection Criteria

Technology	IDS	SIEM	Custom Script
Dataset	User	System	Network
Initial Profile	Rule based	Static	Dynamic
Detection Technique	Hit/Miss	Statistical	Machine Learning



ASB Selection Criteria

Technology		SIEM	
Dataset	User		Network
Initial Profile	Rule based		Dynamic
Detection Technique	Hit/Miss	Statistical	



Phase 2: Recommend and Implement a Behaviour Profiling Methodology

Literature Survey of Academic work

Validation of Methodology

User Group Definition

Executive Leadership & PA	Information Security	SysAdmins

Phase 2: Recommend and Implement a Behaviour Profiling Methodology

Demo

ELT Profiling System

Single User Profiling System

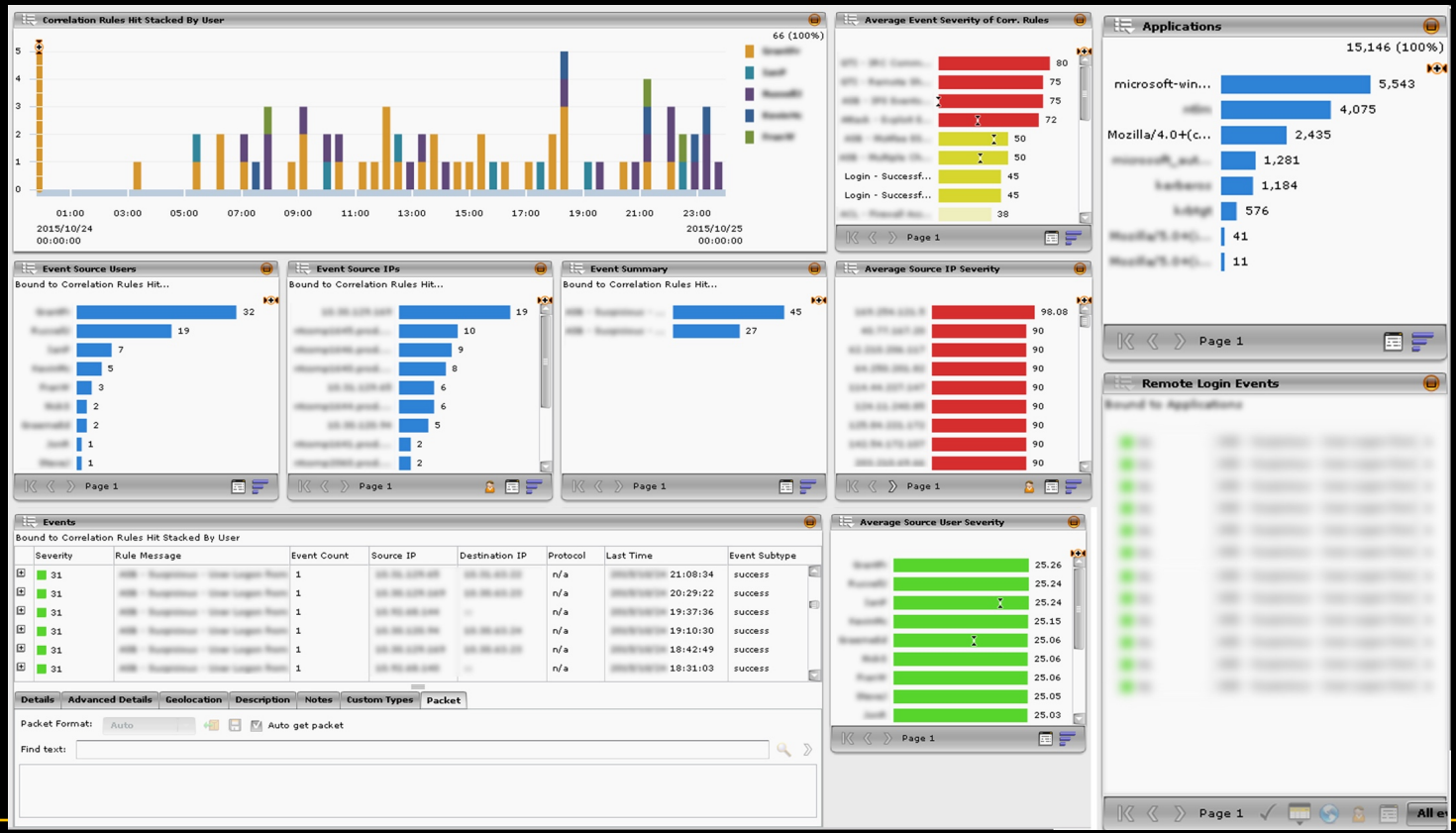
Phase 2: Recommend and Implement a Behaviour Profiling Methodology

Demo

ELT Profiling System

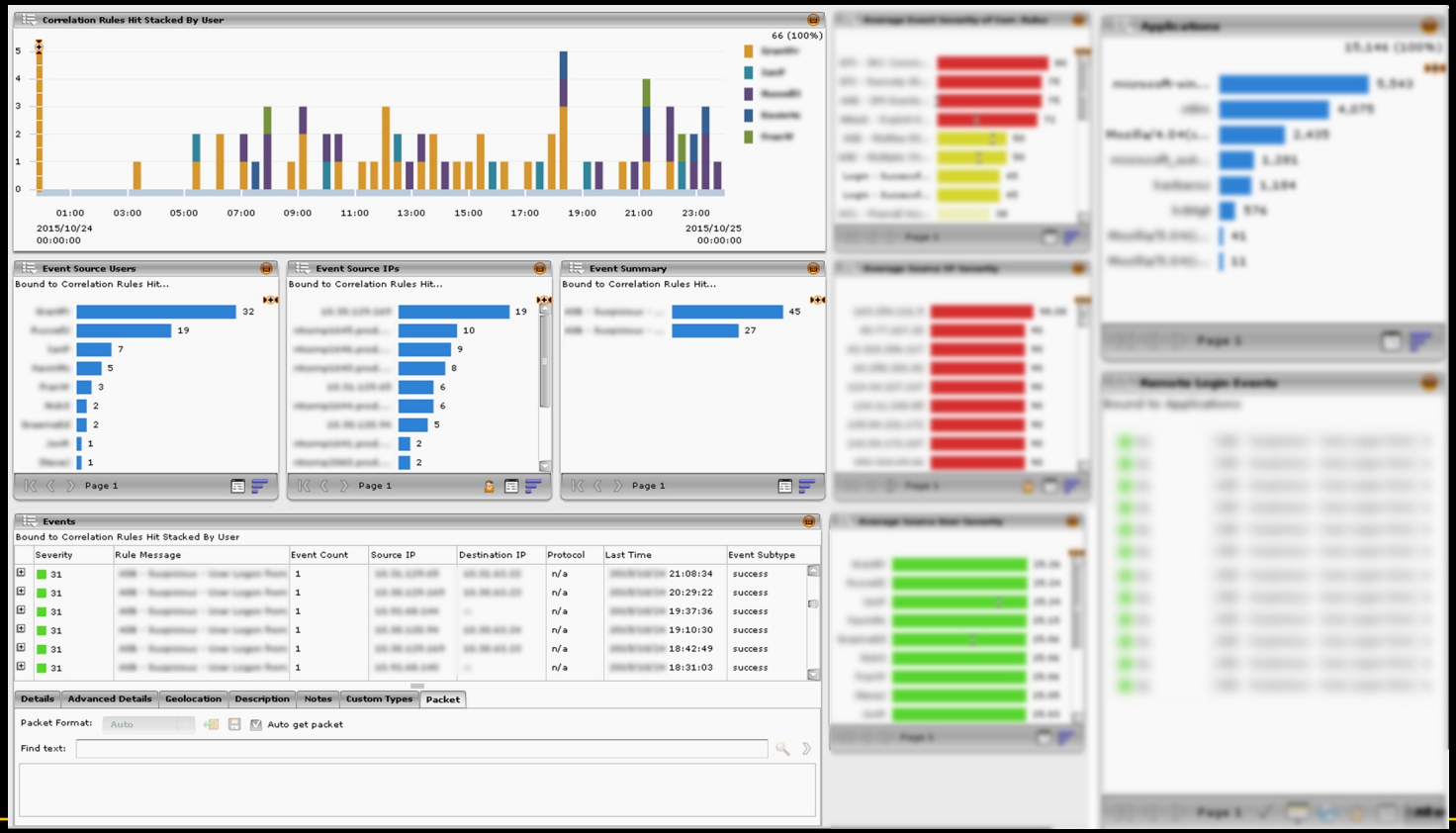
Single User Profiling System

ELT Profiling System



ELT Profiling System

ELT Profiling System



ELT Profiling System

ELT Profiling System

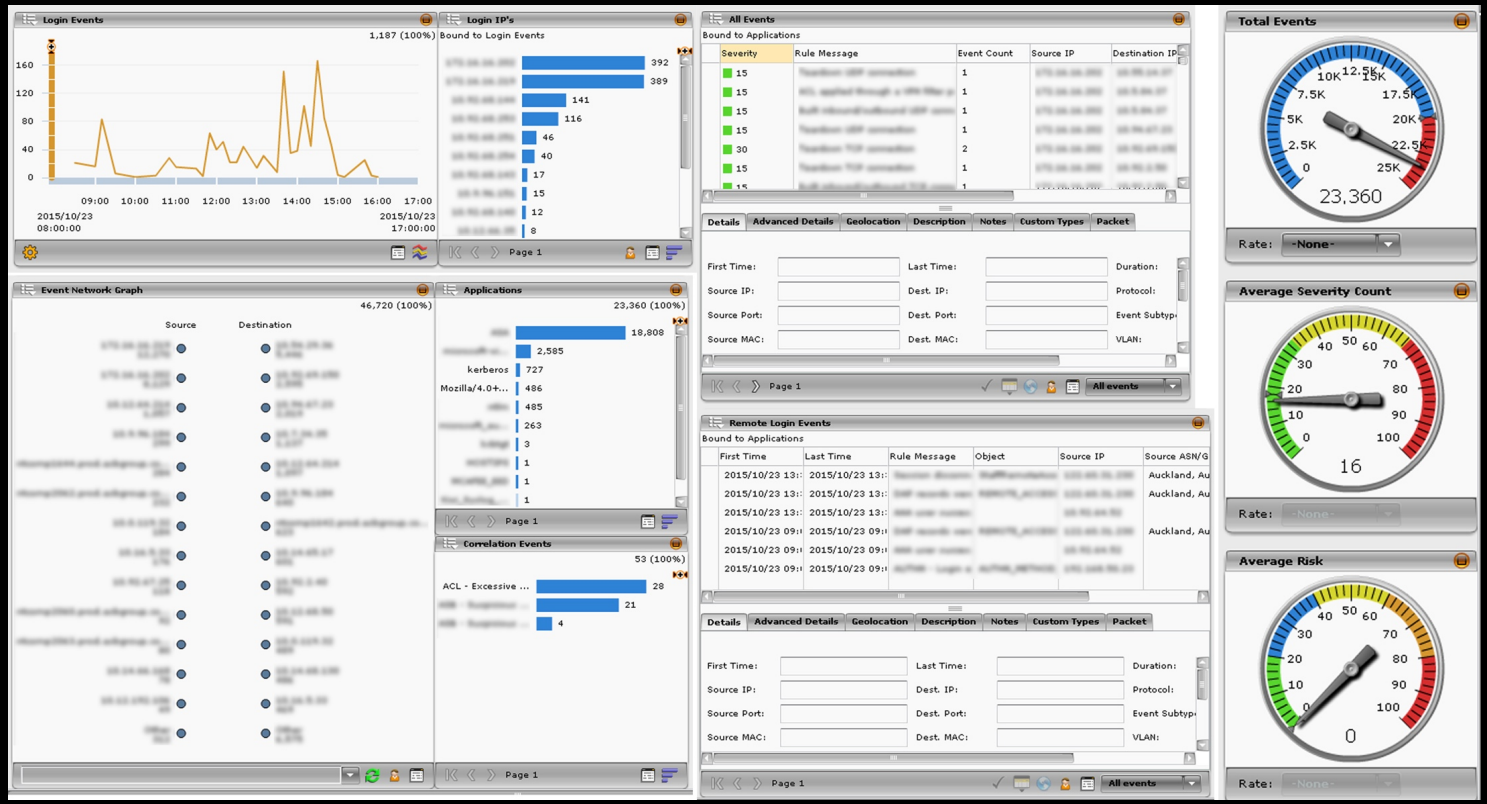
Phase 2: Recommend and Implement a Behaviour Profiling Methodology

Demo

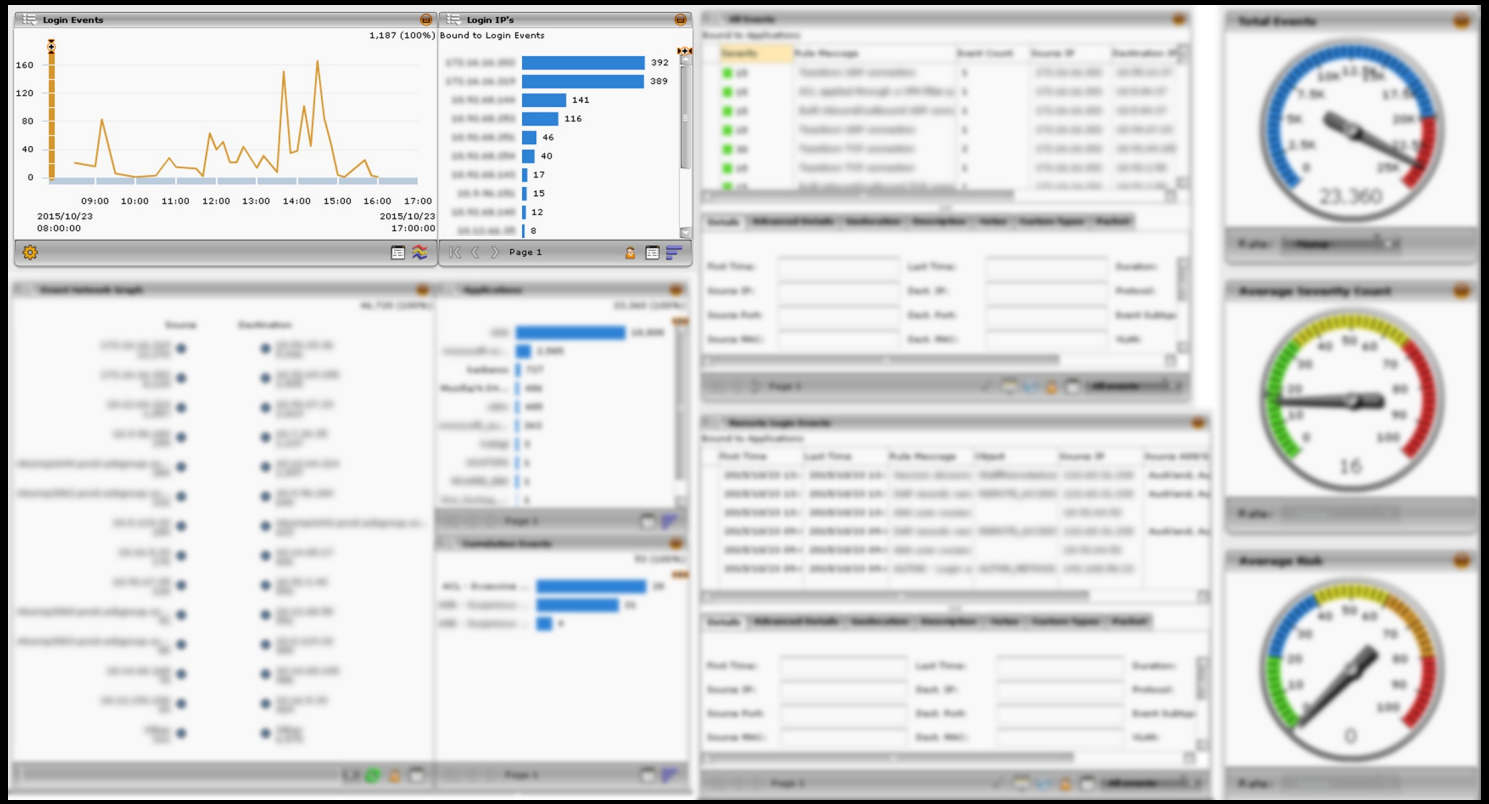
ELT Profiling System

Single User Profiling System

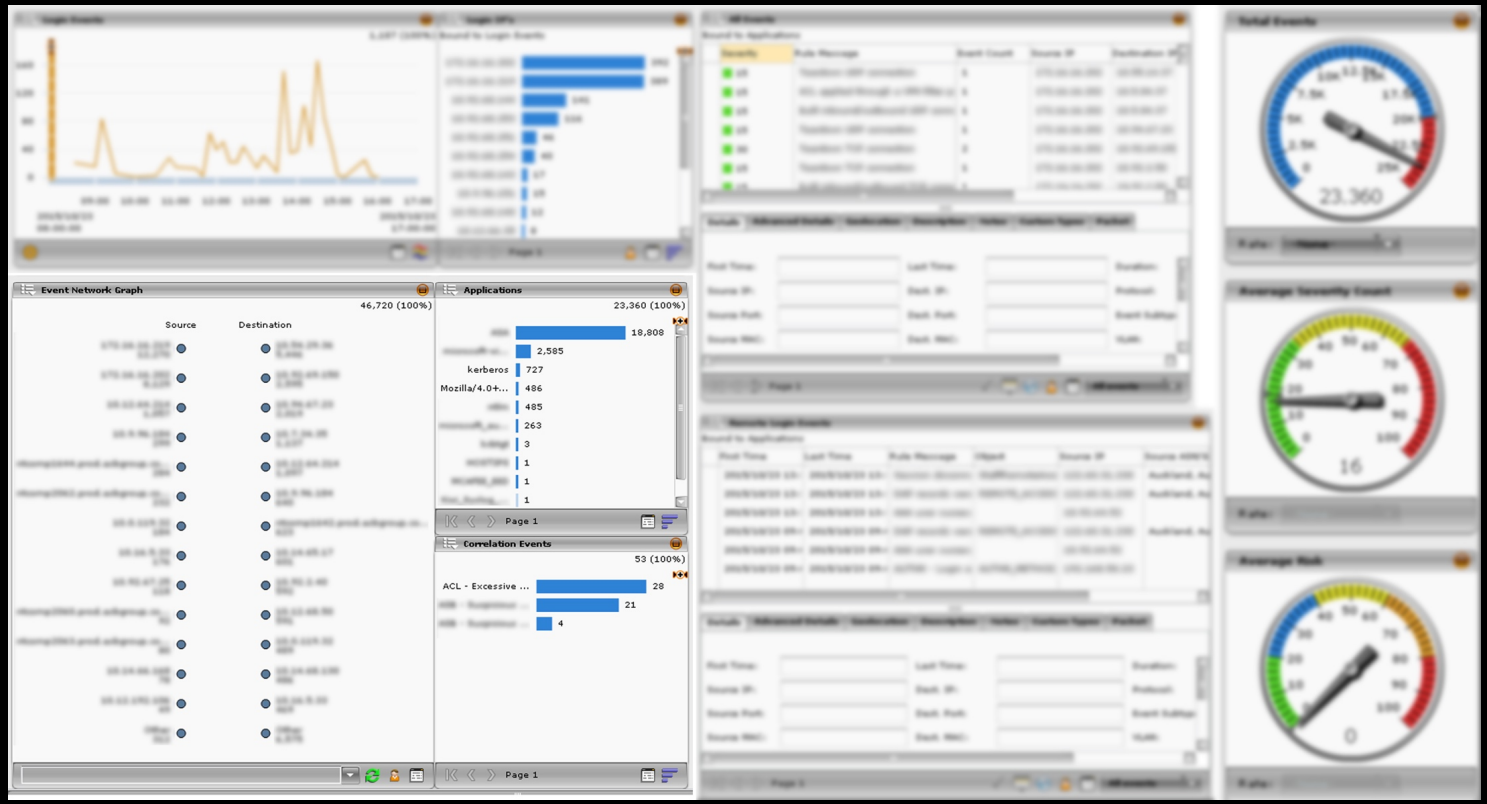
Single User Profiling System



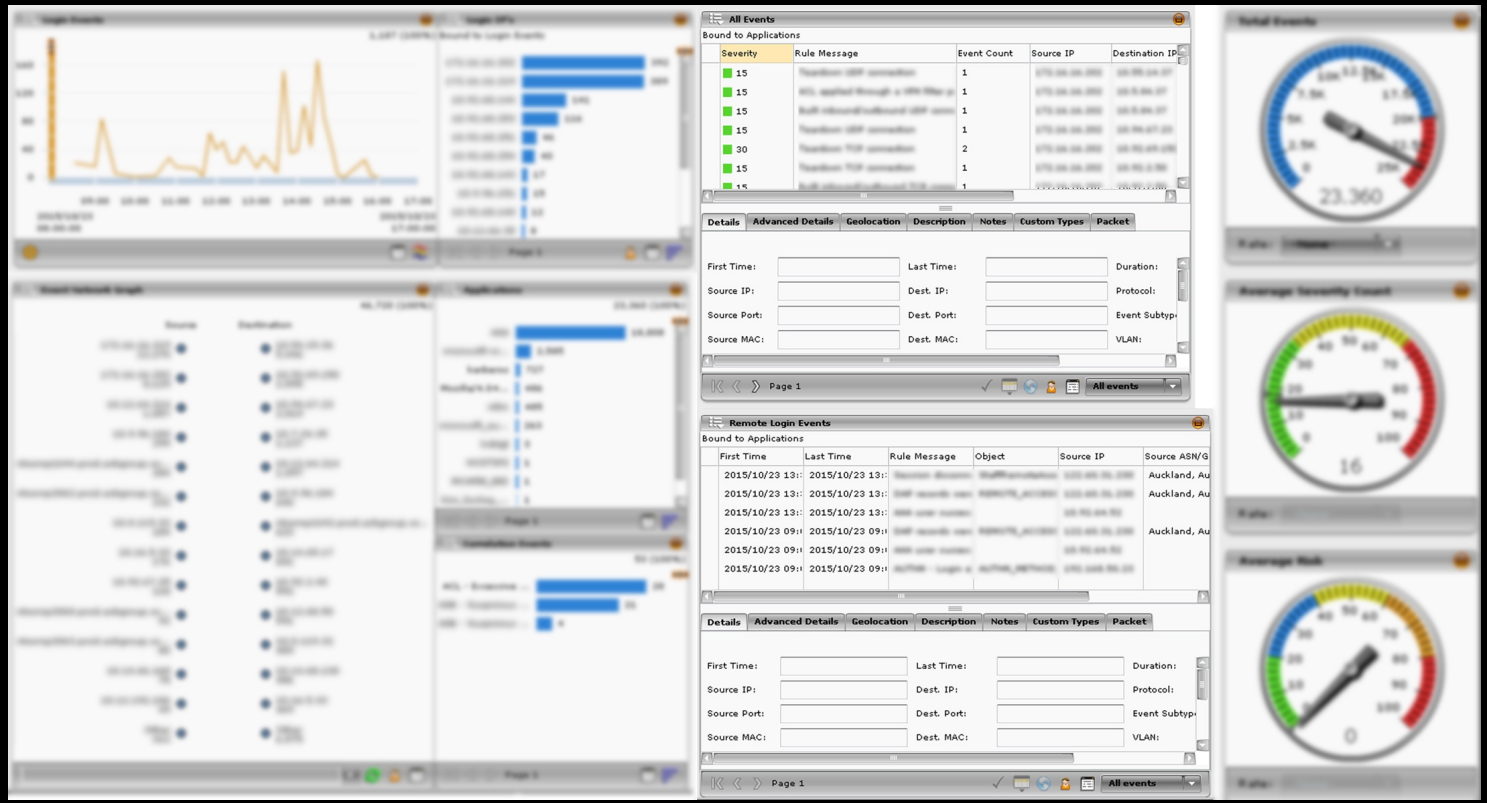
Single User Profiling System



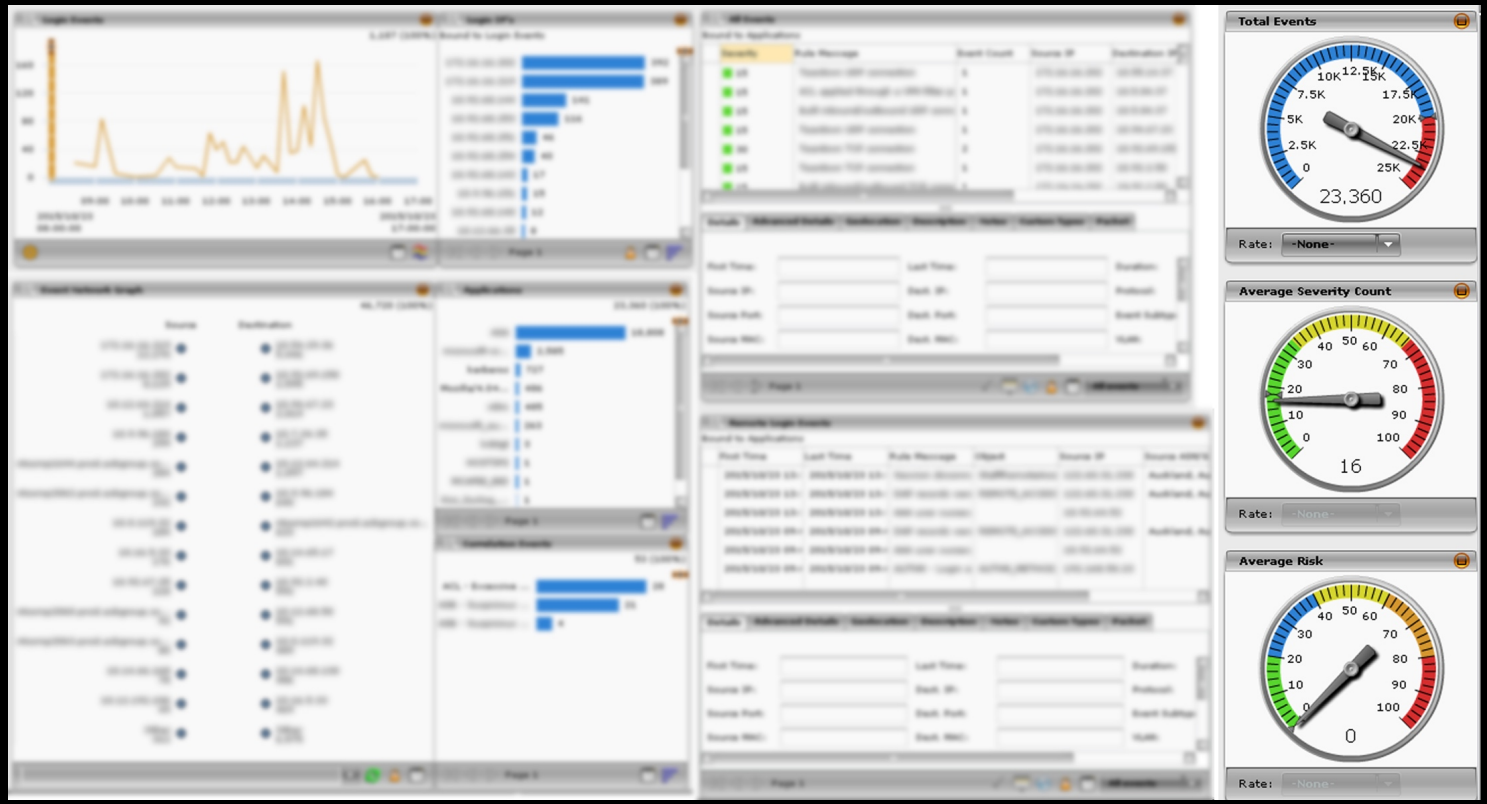
Single User Profiling System



Single User Profiling System

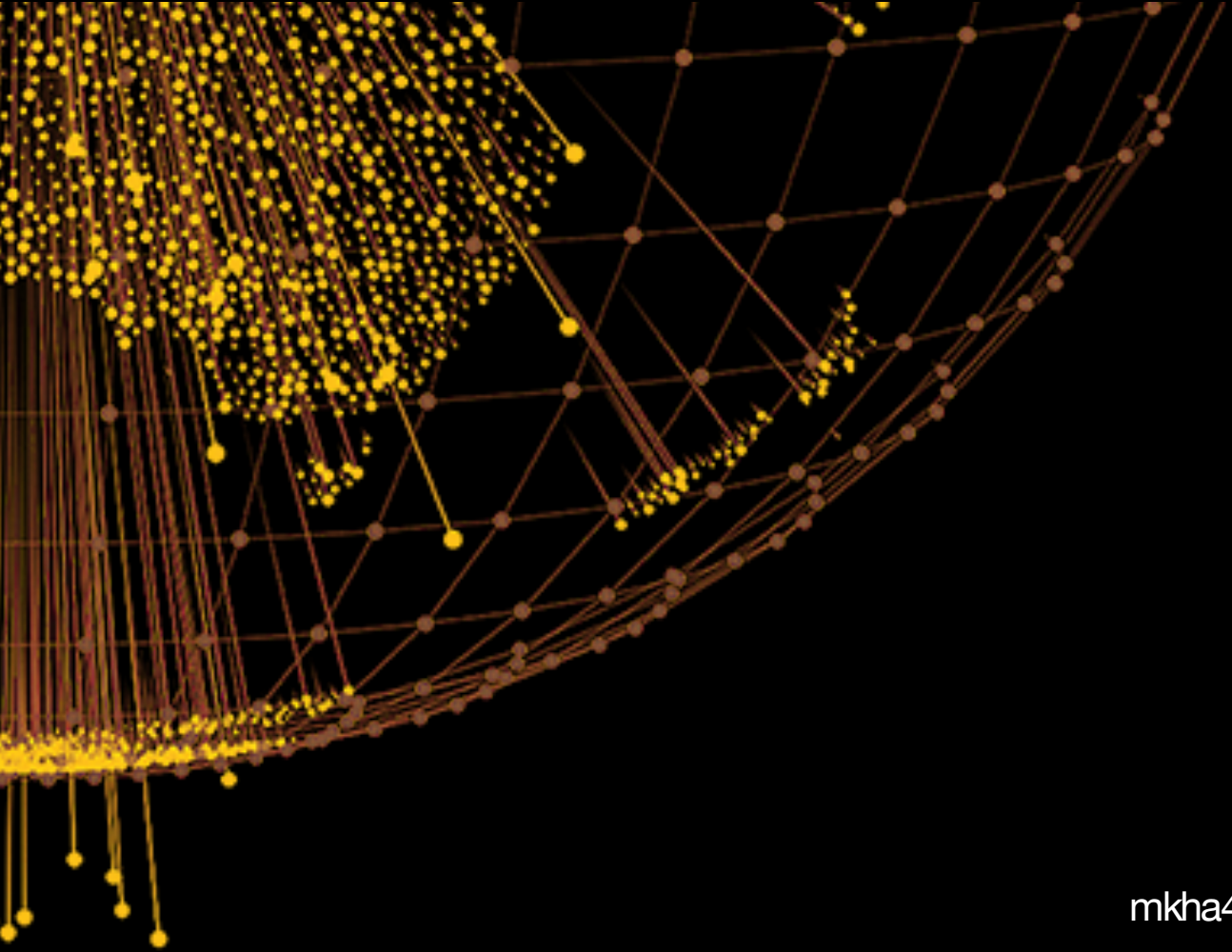


Single User Profiling System



Final Thoughts/Conclusion

- Information Security Summary System is now live and being actively used by the IS team.
- Behaviour Profiling system is in feedback loop and will be adopted shortly.



Raafey Khan
mkha411@aucklanduni.ac.nz

ASB