Ahmed Abdulrahman Alghamdi

Linkedin:
www.linkedin.com/in/alghamdi-ahmed
Phone:
+966506761402
Email:
alhabish@bu.edu.sa

Education

PhD: **Computer Science –** 2021 – **University of Manchester**, United Kingdom

My PhD work involved the implementation of unsupervised machine learning techniques in processing security logged data to extract patterns of cyber attack behaviours and correlation of sequential events for multi-stage attacks and APT.

MSc: **Cyber Security–** 2016 – **Queen's University of Belfast**, United Kingdom

Bachelor: **Computer Information Systems –** 2012 - **Albaha University**, KSA

Skill Highlights

- Project management
- Strong decision maker
- Complex problem solver
- Creative design
- Innovative
- Communication

Experience

Supervisor of Cybersecurity Unit – Albaha University (KSA) - Since Nov 2023 until present,

Vice Dean of E-learning and Digital Transformation at the E-learning deanship – Albaha University (KSA) - Since Nov 2023 until present,

Assistant Professor of Cybersecurity at the Faculty of Computer Science – Albaha University (KSA) - Since Feb 2023 until present,

Lecturer at the Faculty of Computer Science – Albaha University (KSA) - Since 2013 until Feb 2023,

Teaching Assistant - University of Manchester (UK) **–** From Jan 2017 to Feb 2020

My work at the Computer Science school includes the development of undergraduate and postgraduate course materials. Also, organising summer schools and short training courses for coding and other computer science aspects. Moreover I work as a teaching assistant for teaching and marking the modules: Operating Systems, Cryptography, and Foundation Year Projects.

SOC Security Analyst - Allstate Northern Ireland (UK) – From June 2016 to Aug 2016

I worked at Allstate NI as a SOC Security Analyst during my internship. My work involved the creation of a novel framework for Anomalies Detection and IP hosts profiling for RSA Security Analytics' Sessions. The framework automates the enrichment of details about the detected threats via using OSINT. Therefore, SOC specialists can then build accurate decisions based on clear understanding of the threats' classifications and natures.

Technical Skills & interests

Programming Languages: C, C++, Python, Java, HTML, CSS, MySQL, MongoDB, Firebase, VB.NET
INTERESTS: Penetration testing, networks security, physical-cyber security, data analysis and system planning, Malware analysis, big data analysis, software assurance, advanced threats, digital forensics, security awareness, digital transformation, business processes automation.

Projects

Human Resources Management System

A graduation project for BSc degree. The project is coded in VB.NET and SQL database. The aim of the project is to connect all organizations' employees and managers in one program in order to control the productivity and efficiency and to insure the processes flow. The project got A+ as a final score.

RSA Packets Analyser

As a part of my master in Cyber Security at Queen's University Belfast, I worked on an individual research. The project aims to produce a tool that imports malicious network packets and performs further studies on them based on different resources (including open source communities and tools). By using big data analysis and presenting methods, the tools can present meaningful and significant information for users and network administrators for improving the network security and avoiding potential threats. Furthermore, the tool was built to adapt more
features such as performing more analysis processes, adding extra resources, or linking the tool with other security software, which gives users the ability to take active decisions based on the presented data in the tool. The tool is 16 thousand lines of code, and programmed by (Python, PYQT, SQLITE).

The UAHL Security Analysis Framework

UAHL is an unsupervised (Machine Learning) patterns extracting framework, which I developed during my PhD research for the purpose of analysing security-related heterogeneous log-files without the need of training data and per-configurations. The framework consists of two main phases of data analysis to extract inner-behaviours of log-files and then the patterns of those behaviours over analysed files. The framework components and used algorithms are explained in my GitHub repo. https://github.com/aag1990/UAHL

Certifications

Prosci® Certified Change Practitioner
Prosci® - October 2023

Diploma in Scholarly Teaching and Learning in Computing and Engineering
Uppsala University – Sweden.

Fellow of the Higher Education Academy
Higher Education Academy – United Kingdom

Academic Quality Practitioner
Education & Training Evaluation Commission - May 2023 – KSA.

Languages

Arabic (Native speaker) & **English** (Professional working proficiency)

Publications

Pattern Extraction for Behaviours of Multi-Stage Threats via Unsupervised Learning
IEEE International Conference on Cyber Situational Awareness June 19, 2020

Detection of Advanced Persistent Threats Using Heterogeneous Log-Files Monitoring and Machine Learning. - Computer Science Postgraduate Research Symposium, The University of Manchester, UK. 2019

Honors & Awards

Scientific Excellence Award - Royal Embassy of Saudi Arabia Cultural Bureau - UK
Outstanding Research Poster - Postgraduate Research Symposium at the University of Manchester