أكاديمية كاوست
KAUST ACADEMY

جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

# KAUST ACADEMY 2025 SPECIALIZATION

# TABLE OF CONTENTS

01 STATISTICS

02 ABOUT US

03 OUR SPONSORS

04 TEAM MEMBERS

05 ARTIFCIAL INTELLIGENCE SPECIALIZATION STUDENTS INFO

06 ARTIFCIAL INTELLIGENCE PROGRAMS

07 BIOINFORMATICS SPECIALIZATION STUDENTS INFO

08 BIOINFORMATICS PROGRAM

09 CYBERSECURITY SPECIALIZATION STUDENTS INFO

10 CYBERSECURITY PROGRAM

11 ENERGY TRANSITION SPECIALIZATION STUDENTS INFO

12 ENERGY TRANSITION PROGRAM

# KAUST ACADEMY 2025 SPECIALIZATIONS IN NUMBERS

**297**

Talented university students from **16** nationalities in **16** different training locations.

**45%**

total **female** student percentage

**134**

**different projects** students worked on.

**71**
**Artificial Intelligence**

**25**
**Bioinformatics**

**15**
**Cybersecurity**

**23**
**Energy Transition**

**94** DIFFERENT **PROJECT MENTORS**

**55** DIFFERENT **LOCAL AND INTERNATIONAL UNIVERSITIES** STUDENTS

# ABOUT US

**The KAUST Academy** specializations program represents a strategic response to Saudi Arabia's Vision **2030** objectives, specifically addressing the critical need to develop local talent in emerging technologies that will drive the Kingdom's economic diversification. By offering comprehensive training in artificial intelligence, bioinformatics, cybersecurity, and energy transition, the program directly targets the four key pillars of Vision 2030's research and development priorities: sustainable environment and essential needs, energy and industrial leadership, health and wellness, and economies of the future. This initiative recognizes that Saudi Arabia's transformation from an oil-dependent economy to a knowledge-based one requires a skilled workforce capable of competing in high-tech industries and research sectors.

The program's multi-stage structure creates a natural bridge between undergraduate education in Saudi universities and advanced professional competency in cutting-edge fields. Rather than leaving recent graduates to navigate this transition independently, KAUST Academy provides a systematic pathway that begins with foundational online coursework through Coursera, progresses through intensive in-person training at universities across the Kingdom, and culminates in international summer programs at prestigious institutions like Oxford, Cambridge, Duke, and University of Toronto. This scaffolded approach ensures that students from diverse academic backgrounds can build upon their undergraduate foundation while gaining practical, industry-relevant skills, with the program having successfully trained over 16,000 students across multiple specializations.









**This booklet serves as a comprehensive showcase of the remarkable achievements and outcomes that KAUST Academy's 297 graduating students in 2025 have accomplished through their international summer programs at world-renowned universities. These graduates represent more than mere statistics—they demonstrate the tangible impact of Saudi students engaging with cutting-edge research and advanced methodologies at institutions across the globe. Their success validates the program's effectiveness in not only bridging the gap between traditional university education and specialized knowledge required for Saudi Arabia's emerging technology sectors, but also in positioning Saudi graduates as competitive contributors to international research and innovation networks.**

# OUR SPONSORS

العقيل الخيرية
مؤسسة أبناء عبدالرحمن ناصر العقيل الخيرية
ALAGIL FOUNDATION

مدينة الملك عبد الله للطاقة الذرية والمتجددة
K.A.CARE

ntdp

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Site

women & energy

رزم للاستثمار
RZM INVESTMENT

# TEAM MEMBERS

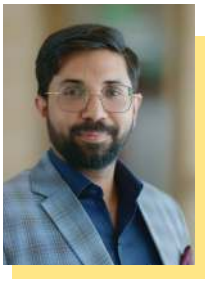


**Sultan Albarakati**

King Abdullah University of Science and Technology

Doctor of Philosophy in Electrical Engineering

**Associate Vice President, Saudi Talent Development**

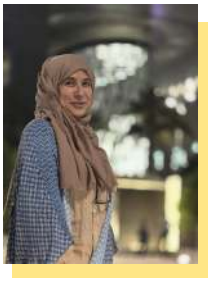


**Naeemullah Khan**

King Abdullah University of Science and Technology

Doctor of Philosophy in Electrical Engineering

**Instruct. Assoc. Professor, Deputy Director KAUST Academy**



**Oroba Al Nasr**

Al Dammam University

Human Research

**Promotions & Outreach Specialist**

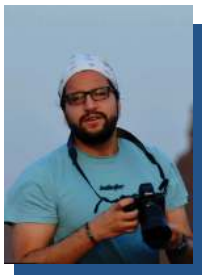


**Abdulrahim Alghamdi**

Curtin University

Human Research

**Master of Commerce, Logistics, Materials, and Supply Chain Management**



**Abdulaziz Altelmissani**

King Abdulaziz University

Medical Laboratory Sciences

**Program Coordinator**



**Ahmed Alhawsawi**

Western Kentucky University

Communication Studies and Business Administration

**Program Coordinator**



**Ali Habibullah**

King Abdulaziz University

Computer Science

**Research Engineer**

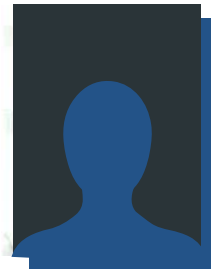


**Asim Abdulfattah**

Florida Institute

Aeronautical Science, Flight

**Program Administrator Pre-University programs**



**Doa'a Aburayya**

King Abdulaziz University

Computer Science

**Research Enginner - AI**



**Emad Surour**

Taibah University

Computer Science information systems

**Academy Programs Administrator**



**Farhanaz Beg**

National University of Singapore

Computer Science and Engineering

**Admissions Lead**



**Fatma Karabulut Ilter**

Istanbul Kültür University

MBA

**Program Administrator**



## Mahmoud Ellouh

King Fahd University of Petroleum and Minerals - KFUPM

Computer Engineering & Cybersecurity

**Research Enginner - Cybersecurity**

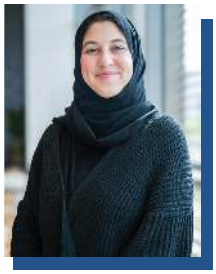


## Majed Alghamdi

Beirut Arab University

English Literature

**Digital Channels Specialist**



## Mariam Yaghmour

UC San Diego/KAUST

Chemistry/Molecular Synthesis

**Program Administrator, Pre-University programs**



## Mohamed Nazar O. AlAli

Saudi Electronic University

Business and Finance MSc.

**Academy Programs Manager**



## Saad Alhusainan

Sultan Qaboos University, Sultanate of Oman

Mass and Communication

**Development Programs Specialist**



## Salman Alomari

University of Indianapolis

MBA

**Program Coordinator**



## Tarek Shehata

Tanta University

Mathematics

**Manager, Pre-University Programs**

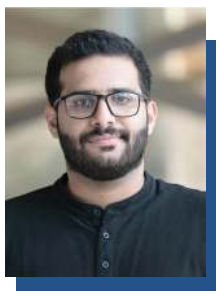


## Venu Kas

North Dakota State University

Doctor of Philosophy in Biochemistry

**Academic Development Specialist**



## Yazan Alshuaibi

King Abdulaziz University

Computer Science

**Research Enginner - AI**



## Yubin Huang

Tianjin University

Material Physics and Chemistry

**Program Administrator**


bersecurity
mmer Camp
SCAN & VISIT
KAUST Academy website

أكاديمية كاوست
KAUST ACADEMY

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

# Cybersecurity Specialization

## 2025





**Omar Ahmed Barasheed**

King Fahd University of Petroleum and Minerals

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdulaziz Mohammed bin Abdullah Al-Ghamdi**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Ammar Abdullah Mohammed Abu Khamis**

Jeddah International College

Cyber Security Summer school - King Abdullah University of Science and Technology



**Zahra Abdullah bin Ahmed Al Salili**

Imam Abdulrahman bin Faisal University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Taif Malfi Bulaid Al - Mutairi**

Imam Mohammad Ibn Saud Islamic University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Manaf Muhammad bin Ali Hussein**

Saudi Electronic University

Duke University - Summer Internship - Cyber Security



**Hatem Hassan Ali AlShudayed**

King Saud University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Ghadah Saeed bin Jaber Alghamdi**

Imam Abdulrahman bin Faisal University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Lama Khaled Abdullah Al-Bishi**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Mohammed Kamil bin Mahdi AlMneian**

King Fahd University of Petroleum and Minerals

Cyber Security Summer school - King Abdullah University of Science and Technology



**Hams Mohammed Bin Atiq Almansori**

Imam Abdulrahman bin Faisal University

Duke University - Summer Internship - Cyber Security



**Khalid Thamir bin Abdulaziz Farsi**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Lama Nasser Fayez Al-Asmari**

Imam Abdulrahman bin Faisal University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Faris Muslim Marzouq Al-Ruhaily**

Islamic University of Madinah

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdulaziz Amer bin Abdulaziz Al-Mubayedh**

Imam Abdulrahman bin Faisal University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdullah Abed J Alharbi**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Jood Hamad bin Abdullah Alolayan**

Qassim University

Duke University - Summer Internship - Cyber Security



**Osama Abdulrahman Alhazmi**

Islamic University of Madinah

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdulaziz Hatim Abdulaziz Almogren**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Obai Ahmed Omar Al-Haidari**

Taibah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Dyaa Fawaz Hamza Malibari**

Jeddah University

Duke University - Summer Internship - Cyber Security



**Khalid Ahmed bin Abdulaziz bin Awad**

King Saud University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Ridha Ali bin Mohammed Alboshafia**

Imam Abdulrahman bin Faisal University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Wasayef Mansour Mohammed Al-Diyabi**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Aram Nawaf Mohammed Al-Harbi**

University of Prince Mugrin

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdulrahman Hussain Ali Alghamdi**

King Fahd University of Petroleum and Minerals

Cyber Security Summer school - King Abdullah University of Science and Technology



**Sultan Ahmed Saleh Bazhaer**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Majed Ghayeb Suayr Almutairi**

Jubail Industrial College

Cyber Security Summer school - King Abdullah University of Science and Technology



**Meshal Mohammed Dhafer Algahtani**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdulrahman Khalid Ali Al-Awam**

King Saud University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Nawaf Abdullah bin Hamoud Al-Otaibi**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Faris Saud bin Dakhil Allah Almutairi**

King Faisal University

Duke University - Summer Internship - Cyber Security



**Sultanh Sami Saleh Al-Diab**

Jeddah University

Duke University - Summer Internship - Cyber Security



**Misk Almomen**

University of California, Berkeley

Cyber Security Summer school - King Abdullah University of Science and Technology



**Ali Zuwayyid Ali Alsulaymi**

King Saud University

Duke University - Summer Internship - Cyber Security



**Essam Khaled Sharaf Al-Otaibi**

Imam Abdulrahman bin Faisal University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Mohammed Abdulrahim Alghamdi**

The Pennsylvania State University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Hadeel Abdullah Abdulrahman bin Jassas**

King Saud University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Al-Jasser Khadir Mohammed Al-Ghamdi**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Mohammed Mansour Mohammed Alsafari**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Aseel Bandar Nasser Almodara**

Princess Nourah Bint Abdul Rahman University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Meshari Abdulrahman bin Ibrahim Alsughayyir**

King Saud University

Duke University - Summer Internship - Cyber Security



**Abdulaziz Fahad Jarallah Al-Harthi**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Mohammed Albahhar**

University of Texas at Austin

Cyber Security Summer school - King Abdullah University of Science and Technology



**Ahmed Sadiq bin Ahmed Al-Ghannam**

Imam Abdulrahman bin Faisal University

Duke University - Summer Internship - Cyber Security



**Sarah Ibrahim Saad Al-Sulami**

Umm Al-Qura University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Ramah Ahmed Saeed Al-Guthmi**

King AbdulAziz University

Duke University - Summer Internship - Cyber Security



**Abdullah Mohammed Ali Al-Asmari**

King Saud University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Dalia Saeed Faiz Al-Asmari**

Imam Mohammad Ibn Saud Islamic University

Duke University - Summer Internship - Cyber Security



**Shaden Almodhy**

University of Illinois at Urbana-Champaign

Cyber Security Summer school - King Abdullah University of Science and Technology



**Abdulrahman Mousa Lafi Al-Ahmadi**

King AbdulAziz University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Mohammed Saad Ali Al-Quraini**

King Fahd University of Petroleum and Minerals

Duke University - Summer Internship - Cyber Security



**Hanin Atiah bin Hamdan Al-Harbi**

Taibah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Hussain Mohammed Hussain Al-Shdaied**

Jeddah University

Cyber Security Summer school - King Abdullah University of Science and Technology



**Fahad Hamoud Mohammed Al-Athel**

King Fahd University of Petroleum and Minerals

Duke University - Summer Internship - Cyber Security



**Shouq Miq'ad Abdullah Al-Otaibi**

King Saud University

Duke University - Summer Internship - Cyber Security



**Razan Faris bin Abdulrahman Almalki**

Umm Al-Qura University

Duke University - Summer Internship - Cyber Security



**Raghad Yousef Lafi Al-Harbi**

Princess Nourah Bint Abdul Rahman University

Duke University - Summer Internship - Cyber Security



**Rahaf Aldalbahi**

University of California, Los Angeles

Cyber Security Summer school - King Abdullah University of Science and Technology

# A GOVERNANCE, RISK, AMD COMPLIANCE (GRC) ASSESSMENT SYSTEM TAILORED FOR SMALL SCALE BYSINESSES IN SAUDI ARABIA

Build an automated cyber risk assessment tool tailored for small businesses. It scans externally exposed assets (domains, IPs), checks common misconfigurations (e.g., SPF/DKIM, open ports), and generates a simple risk report with remediation steps.

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Hatem Hassan Ali AlShudayed,Khalid Ahmed bin Abdulaziz bin Awad, Abdullah Mohammed Ali Al-Asmari, Abdulrahman Khalid Ali Al-Awam

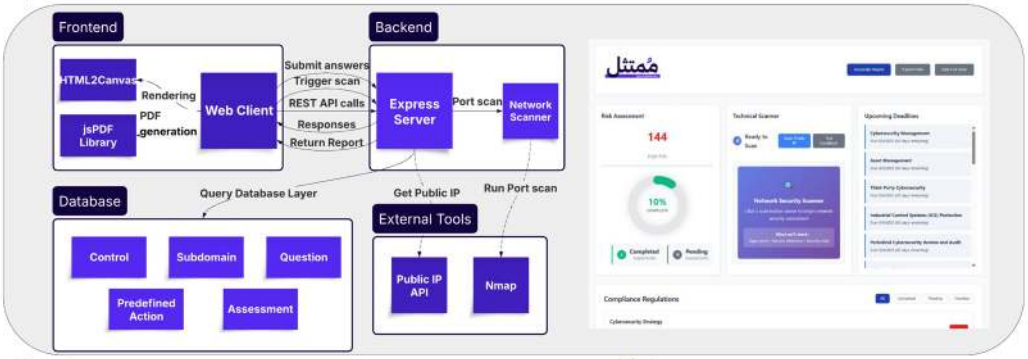
## Mumtathil: GRC Assessment System Tailored for Small Businesses in Saudi Arabia

Hatem AlShudayed, Abdulrahman Alawam, Abdullah Alasmari, Khaled Bin Awad
Supervised by: Prof. Ali Hassan

### Introduction

Small businesses in Saudi Arabia face compliance challenges due to limited resources, lack of localized tools, and rising cyber threats. Mumtathil fills this gap with a tailored GRC system that automates risk classification, compliance tracking, and technical scanning simplifying adherence, reducing manual effort, and supporting NCA frameworks.

### System Architecture & Dashboard




### Problem

Small businesses in Saudi Arabia struggle with NCA compliance due to limited resources and poor tools. Key challenges include manual tracking with spreadsheets, lack of affordable localized GRC solutions, and no real-time visibility into cybersecurity risks.

### Result

- Risk Classification: Categorizes risks as High, Medium, or Low.
- Compliance Report Generation: Produces automated compliance and policy reports.
- Technical Scanner: Identifies vulnerabilities and misconfigurations.
- Dashboard Summary: Provides a centralized view of risk and compliance status.
- Implementation of 3 Frameworks: Ensures standardized assessments and control validation.

### Tools

PostgreSQL, Node.js, JS, HTML, CSS

### Solution

This project delivers a unified GRC platform combining automated risk assessments, technical scanning, and centralized policy management. It improves efficiency, transparency, and reporting while reducing manual effort and strengthening governance against evolving regulatory and security demands.

### Conclusions

Automating GRC processes helps Saudi small businesses comply more effectively with cybersecurity regulations. Mumtathil reduces reliance on manual tools, provides real-time risk visibility, and supports Vision 2030 goals. Future AI integration and broader regulatory coverage will expand its impact.

### Future Work

- Expanded Regulatory Framework Support: Includes SAMA, PDPL, CST, industry-specific modules, and GCC regional coverage.
- Enterprise Scaling and Multi-Business Support: Supports multi-subsidiary management, advanced role controls, and scalable architecture for medium to large enterprises.

### Acknowledgments & References

We thank KAUST Academy, NCA, and SITE for their guidance and support throughout this project.

References

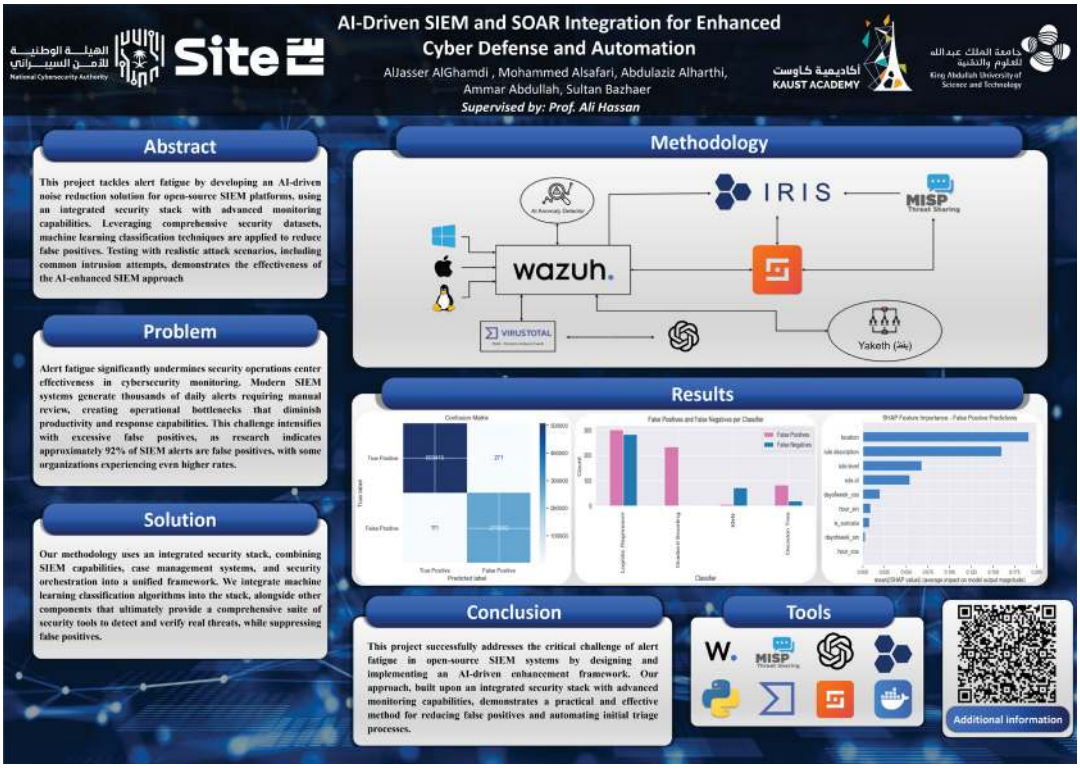
Rate Mumtathil

# AI-DRIVEN SIEM AND SOAR INTEGRATION FOR ENHANCED CYBER DEFENSE AND AUTOMATION

This project focuses on enhancing cybersecurity operations by implementing and integrating Security Information and Event Management (SIEM) systems with Security Orchestration, Automation, and Response (SOAR) platforms, leveraging Artificial Intelligence (AI) for improved threat detection and response.
The project aims to explore how AI-driven analytics can help automate incident detection, investigation, and response processes, reducing manual intervention and speeding up response times.
Key components of the project include:
**1. SIEM Integration: Streamlining real-time monitoring and analysis of security events from various data sources (Applications logs, Firewall logs, WAF, system logs, etc.) to identify potential threats.**
**2. SOAR Implementation: Automating incident response workflows, including alert triage, investigation, and mitigation, through predefined playbooks and AI assistance.**
**3. AI/ML Integration: Applying machine learning techniques to analyze large datasets for anomalous patterns, identify emerging threats, and suggest corrective actions.**
**4. Automation: Developing automated workflows to reduce response time and enhance operational efficiency in handling cybersecurity incidents. This project will allow you to gain hands-on experience with advanced cybersecurity tools and**

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Al-Jasser Khadir Mohammed Al-Ghamdi,Mohammed Mansour Mohammed Alsafari,Sultan Ahmed Saleh Bazhaer Abdulaziz Fahad Jarallah Al-Harthi, Ammar Abdullah Mohammed Abu Khamis



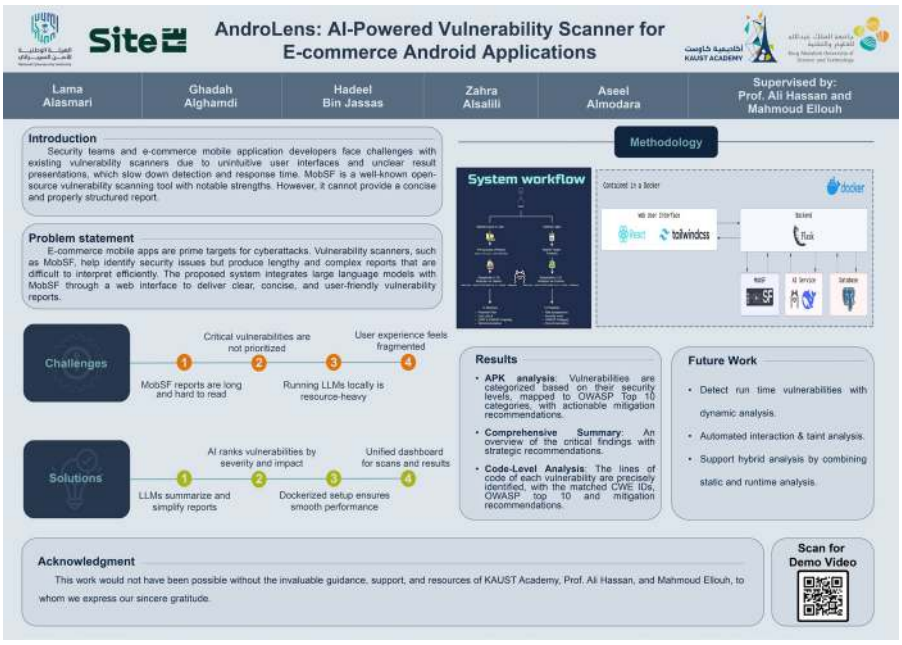
# AI-POWERED VULNERABILITY SCANNER FOR E-COMMERCE ANDROID APPLICATIONS

This project focuses on utilizing Artificial Intelligence (AI) to strengthen the security posture of Jarir e-commerce website and its associated mobile application.
The project will explore AI-driven solutions for threat detection, vulnerability assessment, and continuous monitoring to identify and mitigate risks in real-time. Additionally, AI will be used to review and optimize both the website and mobile app for security, performance, and user experience.
Key objectives include:

**1. AI for Threat Detection: Implementing machine learning algorithms to analyze user behaviors, traffic patterns, and interactions to identify anomalous activities such as fraud, data breaches, and bot attacks.**
**2. Vulnerability Scanning: Using AI-powered tools to scan for security vulnerabilities on the website and mobile app code, identifying common issues and insecure APIs.**
**3. Automated Penetration Testing: Leveraging AI to perform automated penetration testing, simulating real-world cyberattacks on the e-commerce platform to identify weaknesses and suggest corrective actions.**
**4. Real-Time Risk Monitoring: Deploying AI-based solutions for real-time monitoring, alerting on suspicious activity, and quickly responding to potential threats.**
**5. Mobile App Security Optimization: Utilizing AI to analyze and enhance mobile app security, ensuring data protection, secure authentication, and adherence to best practices for mobile security.**
**This project provides an opportunity to work with cutting-edge AI tools, gain hands-on experience in securing e-commerce platforms, and contribute to the development of robust, future-proof security strategies for both websites and mobile applications.**

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Lama Nasser Fayez Al-Asmari,Aseel Bandar Nasser Almodara,Hadeel Abdullah Abdulrahman bin Jassas, Ghadah Saeed bin Jaber Alghamdi, Zahraa Abdullah bin Ahmed Al-Sulaili



# BEHAVIORAL-BASED INSIDER THREAT DETECTION IN A ZERO TRUST CLOUD NETWORK

Build a simulated corporate network that implements zero trust principles, including microsegmentation, strong authentication, and least-privilege access. Test the environment with simulated internal and external threats.

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Lama Khaled Abdullah Al-Bishi,Wasayef Mansour Mohammed Al-Diyabi,Sarah Ibrahim Saad Al-Sulami, Hanin Atiah bin Hamdan Al-Harbi, Aram Nawaf Mohammed Al-Harbi

## Behavioral-Based Insider Threat Detection in Zero Trust Cloud Network

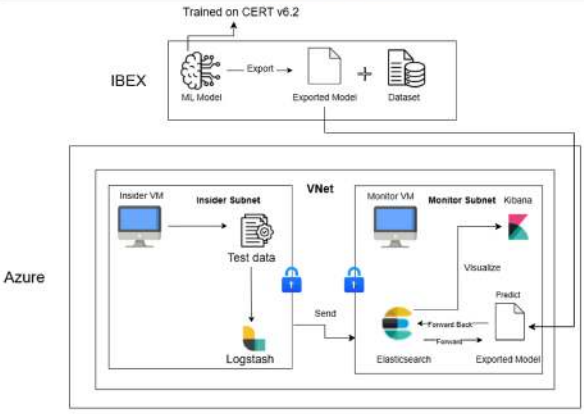
Aram Alharbi [1] Haneen Alharbi [2] Sarah Alsulami [3] Lama Albishi [4] Wasayef Aldiyabi [5]

[1]Prof. Ali Hasssan

### Introduction

Insider threats are among the most difficult challenges for organizations, as trusted individuals can exploit legitimate access to compromise critical assets. Traditional security defenses often fail because insider behaviors are subtle, diverse, and context-dependent. According to CISA (2024), the average cost of an insider incident is $16.2 million, with 86 days required for identification and containment. Furthermore, Workplace Violence Statistics (2018) report that 25% of such incidents go unreported, highlighting serious gaps in detection and response.

### System Architecture




### Future Work

- Extend to real-time streaming of insider logs (streaming pipeline + low-latency inference).
- Evaluate with larger user groups, and multiple datasets.

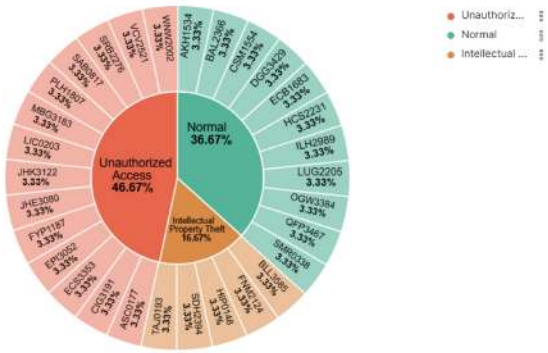
### Tools

### Problem Statement

While machine learning models exist for insider threat detection, most research focuses on theoretical experimentation without exploring real-world deployment. The proposed solution addresses this gap by deploying a pre-trained insider threat detection model in a near real-world environment, integrating it with the ELK Stack for data analysis and visualization.

### Results & Findings

1. Integrated ML predictions into ELK dashboards for inspection.
2. Demonstrated correct categorization of insider-like activities on synthetic sequences.
3. Built a secure pipeline for ingestion, processing, and visualization of stored logs.
4. Showed Azure VNet isolation approximates enterprise deployment constraints.




### Conclusion

This project shows a feasible path from research to deployment for insider-threat ML: preprocessing, feature extraction, offline model inference, and visualization via ELK in a cloud environment.

- Strength: Complete proof-of-concept demonstrating end-to-end flow.
- Limitation: Synthetic data and stored ingestion; production requires streaming, access controls, and monitoring.

### References

[1]Cybersecurity and Infrastructure Security Agency, Insider threat 101 fact sheet, https://www.cisa.gov/sites/default/files/2024-07/insider-threat-101-fact-sheet_07-29-2024_508.pdf. Accessed: 18 July 2025, Jul. 2024.
[2]R. Lindauer, Insider threat test dataset, [Online]. Available: https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247. Accessed: 2025-08-23, 2020.
[3]Elastic NV, Elk stack documentation, [Online]. Available: https://www.elastic.co/guide/index.html. Accessed: 2025-08-19, 2020.

# BEYOND-TRANSISTORS: NEXT GENERATION HARDWARE SECURITY PRIMITVES USING SPINTRONIC DEVICES

The primary objective of this project is to explore the potential of spintronic devices as a foundation for next-generation hardware security primitives. It aims to understand the limitations of traditional CMOS-based hardware in addressing emerging security threats and to investigate how spin-based devices offer inherent advantages like non-volatility, variability, and tamper resistance. The project will also focus on designing and analyzing basic hardware security primitives, such as True Random Number Generators (TRNGs), Hardware Watermarks and Logic Locking.

**PROJECT MENTOR:** Divyanshu & Selma Amara

**PROJECT MEMBERS:** Mohammed Albahhar, Misk Almomen,Shaden Almodhy, Rahaf Aldalbahi, Taif Malfi Bulaid Al-Mutairi

# DECEPTIVE HONEYNET ANALYZER WITH DYNAMIC LURE INJECTION

Design a multi-node honeynet system that simulates various vulnerable services (e.g., SSH, RDP, SMB) and uses a lure injection engine to bait attackers with deceptive data. Analyze attacker behavior in real time and auto-generate attack profiles.

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Abdulrahman Mousa Lafi Al-Ahmadi, Abdulaziz Hatim Abdulaziz Almogren,Abdulaziz Mohammed bin Abdullah Al-Ghamdi, Mohammed Abdulrahim Alghamdi, Khalid Thamer bin Abdulaziz Farsi

## Deceptive Honeynet Analyzer with Automated Attacker Profiling

Abdulrahman M. Alahmadi, Abdulaziz H. Almogren, Abdulaziz M. Alghamdi, Khalid T. Farsi, Mohammed A. Alghamdi.
Cybersecurity Specialization Summer School
KAUST Academy

### Introduction

Cyber attackers are constantly probing networks, searching for weaknesses to exploit. Traditional defenses often only detect attacks after damage has already occurred. Honeynets, however, provide a unique way to observe attackers directly by luring them into controlled, deceptive environments. By studying their actions, security teams can uncover valuable insights into adversary behavior and techniques. Yet, deploying and managing honeynets manually is complex and time-consuming. This project explores how automation and intelligent analysis can make deception a practical defense strategy.

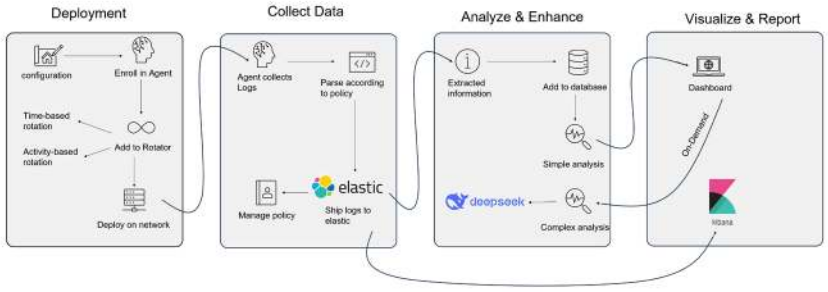
### Problem

Despite their effectiveness, honeynets remain underused because they require significant expertise and effort to deploy, configure, and monitor. Security analysts often struggle with large volumes of unstructured logs that make profiling attackers slow and inconsistent. Without streamlined tools, critical attacker behaviors may go unnoticed, leaving organizations vulnerable. Additionally, existing solutions rarely integrate deception with automated intelligence for deeper insights. This gap limits the value of honeypots in real-world defense. A more efficient, scalable approach is needed to bridge deception and attacker profiling.

### Solution

We developed the Deceptive Honeynet Analyzer with Automated Attacker Profiling to simplify and strengthen this process. Honeypots are deployed automatically in Docker containers, each with a deceptive profile to attract attackers. Logs from interactions are collected with Elastic Agent, centralized in Elasticsearch, and enriched with VirusTotal correlation for malware analysis. The system builds detailed attacker profiles including IPs, ports, commands, and files. Analysts can further enhance investigations with an LLM-powered analyzer for retrospective insights. This integrated approach reduces complexity, saves time, and empowers defenders with actionable intelligence.

### Methodology




### Results

- Automated Honeynet Configuration and Deployment Seamlessly deploy and manage honeynets.
- Intuitive Analyst Interface User-friendly dashboard for security analysts to monitor and control the system.
- Honeypot deceptive profiles that mimic common systems.
- Automated attacker profiling Continuously profile attacker behavior with advanced LLM-driven insights.

### Future Work

- Automated honeypot deployment triggered by commands, e.g., 'Create honeypot for CVE-2025-2938.'
- Leverage dynamic multi-honeypot lures for enhanced attacker analysis.
- Integrate built-in analysis for common attack patterns, such as SQL injection, brute-force login attempts, and cross-site scripting.

### Conclusion

This project demonstrates a fully automated, intelligent honeynet system that simplifies deployment, enhances deception, and provides deep insights into attacker behavior. The system highlights the potential of combining automation and advanced analytics to strengthen cybersecurity defenses efficiently and effectively.

### Tools & Report

deepseek elastic docker kibana

# IOT SECURITY ASSESSMENT PLATFORM

Build a platform that scans and analyzes smart devices on a local or simulated network to identify common IoT security issues. The system will detect exposed services, weak credentials, outdated firmware, and insecure communication protocols. It will then correlate findings with known vulnerabilities from sources like CVE/NVD, Shodan API, or custom threat feeds. A web dashboard will display device details, risk scores, and recommended remediation steps.

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Abdulrahman Hussein Ali Al-Ghamdi, Essam Khaled Sharaf Al-Otaibi,Osama Abdulrahman Alhazmi, Faris Muslim Marzouq Al-Ruhaily, Abdulaziz Amer bin Abdulaziz Al-Mubayedh

# PERSONAL THREAT SURFACE MAPPING TOOL

This project focuses on improving personal and organizational security posture by creating a tool that scans public online data sources—such as GitHub, social media, and leaked credentials—to map an individual's threat surface. It consolidates exposure data into an intuitive dashboard with scoring and visualization, enabling users to identify and remediate vulnerabilities in their digital footprint before adversaries can exploit them.

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

**PROJECT MEMBERS:** Nawaf Abdullah bin Hamoud Al-Otaibi, Abdullah Abed J Alharbi,Majed Ghayeb Suayr Almutairi, Mohammed Kamil bin Mahdi AlMneian, Obai Ahmed Omar Al-Haidari

# THREAT INTELLIGENCE AGGREGATOR & ANALYZER

This project aims to improve cyber defense capabilities by developing a unified platform that aggregates and correlates multiple threat intelligence feeds (STIX/TAXII, abuse.ch, VirusTotal, AlienVault OTX). By integrating diverse data sources into a consolidated dashboard, the project enables real-time identification of emerging threats through IOC trends, geolocation mapping, and attack type analysis. This approach enhances situational awareness and facilitates proactive threat mitigation.

**PROJECT MENTOR:** Ali Hassan & Mahmoud Ellouh

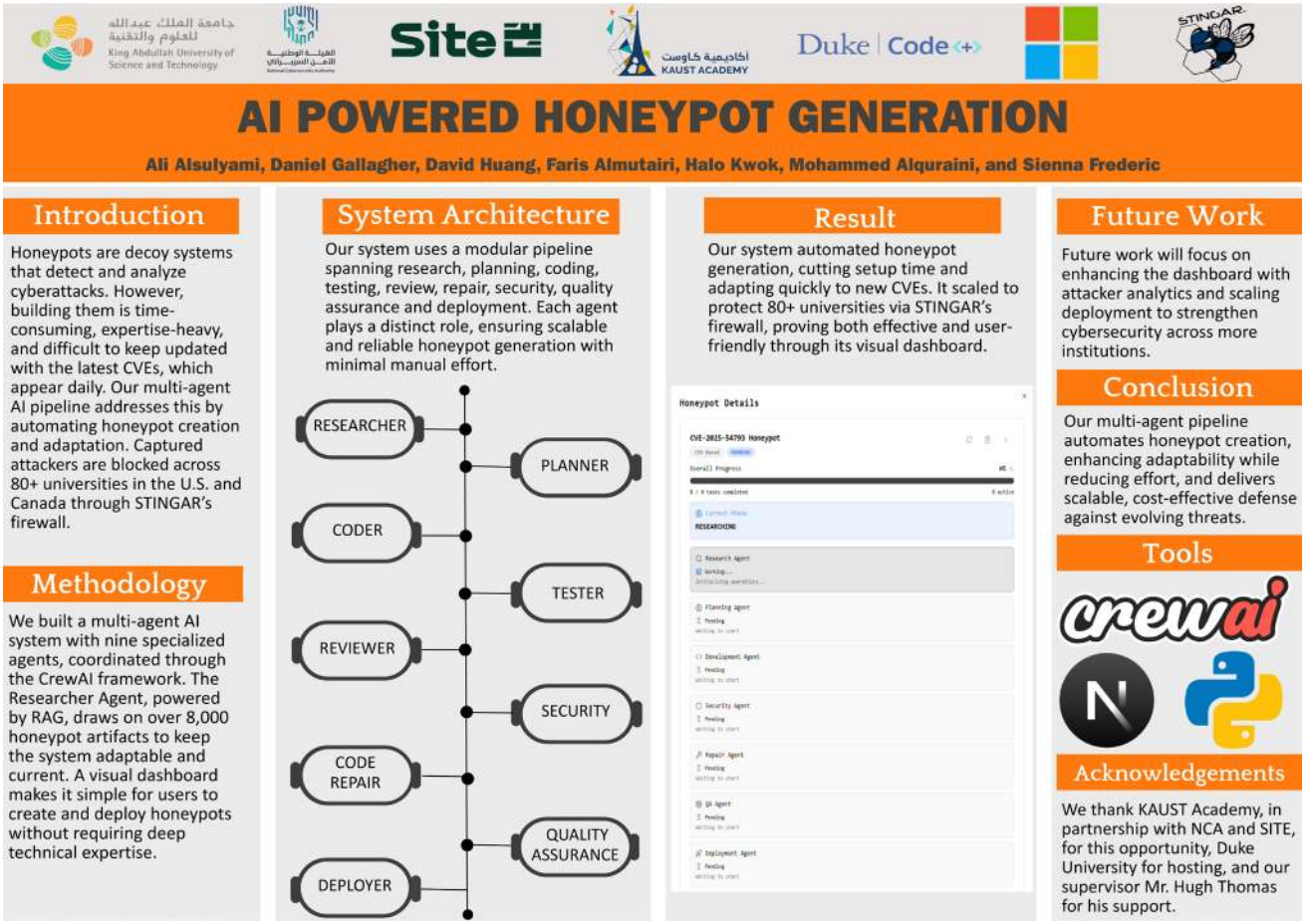
**PROJECT MEMBERS:** Meshal Mohammed Dhafer Algahtani, Hussain Mohammed Hussain Al-Shdaied, Omar Ahmed Barasheed, Ridha Ali bin Mohammed Alboshafia

# ADVANCING HONEYPOTS WITH AI FOR ENHANCED CYBERSECURITY

This project focuses on advancing the STINGAR security platform by designing and deploying new honeypot types using rapid prototyping techniques powered by large language models (LLMs). These updates will improve the detection and mitigation of cyber threats, strengthening the protection of Duke's network and those of over 70 partner universities nationwide. Students will collaborate with Duke's Office of Information Technology (OIT), IT Security Office (ITSO), and cybersecurity experts to research, prototype, and implement innovative honeypot designs. As a stretch goal, the team will develop mechanisms for dynamically adapting honeypots based on evolving attacker behaviors, ensuring that the system remains effective against sophisticated and emerging threats. This project provides hands-on experience with AI-driven security tools and real-world cybersecurity challenges, contributing to a cutting-edge defense network for higher education institutions.

**PROJECT MENTOR:** Hugh Thomas

**PROJECT MEMBERS:** Ali Zuwayyid Ali Alsulaymi,Faris Saud bin Dakhil Allah Almutairi, Mohammed Saad Ali Al-Quraini



# DEVELOPING A USER-FRIENDLY INTERFACE FOR BLOCKLIST AND SAFELIST MANAGEMENT

This project focuses on creating a front-end application for APIARY, a system designed to manage blocklists and safelists for security operations. While the backend API is fully developed, the system needs an intuitive interface to streamline management tasks like adding entries, viewing logs, and performing essential security operations. Students will work with Duke's Office of Information Technology (OIT, IT Security Office (ITSO)), cybersecurity experts and stakeholders to design and build a polished, functional interface. As a stretch goal, the team will prepare the tool for open-source release, making it available to other universities to enhance their security operations. This project offers hands-on experience in front-end development, API integration, and creating collaborative tools for the broader cybersecurity community.

**PROJECT MENTOR:** Anthony Miracle

**PROJECT MEMBERS:** Manaf Muhammad bin Ali Hussein,Dyaa Fawaz Hamza Malibari



# ENHANCING NETWORK SECURITY ANALYSIS WITH MISTRAL

This project focuses on advancing the MISTRAL platform, a National Science Foundation (NSF)-funded initiative designed to capture and analyze network data in research lab environments. Students will collaborate with the MISTRAL team, Duke's IT Security Office (ITSO), and key stakeholders to improve tools for querying, distributing, and visualizing security logs and research data. The team will work on analyzing network security datasets specific to research labs, correlating diverse data sources, and developing intuitive visualizations to make complex insights accessible to researchers and security teams. This project offers hands-on experience in Python programming, user interface and API development, and advanced data analysis techniques, contributing to innovative solutions for research lab security.

**PROJECT MENTOR:** Alexander Merck

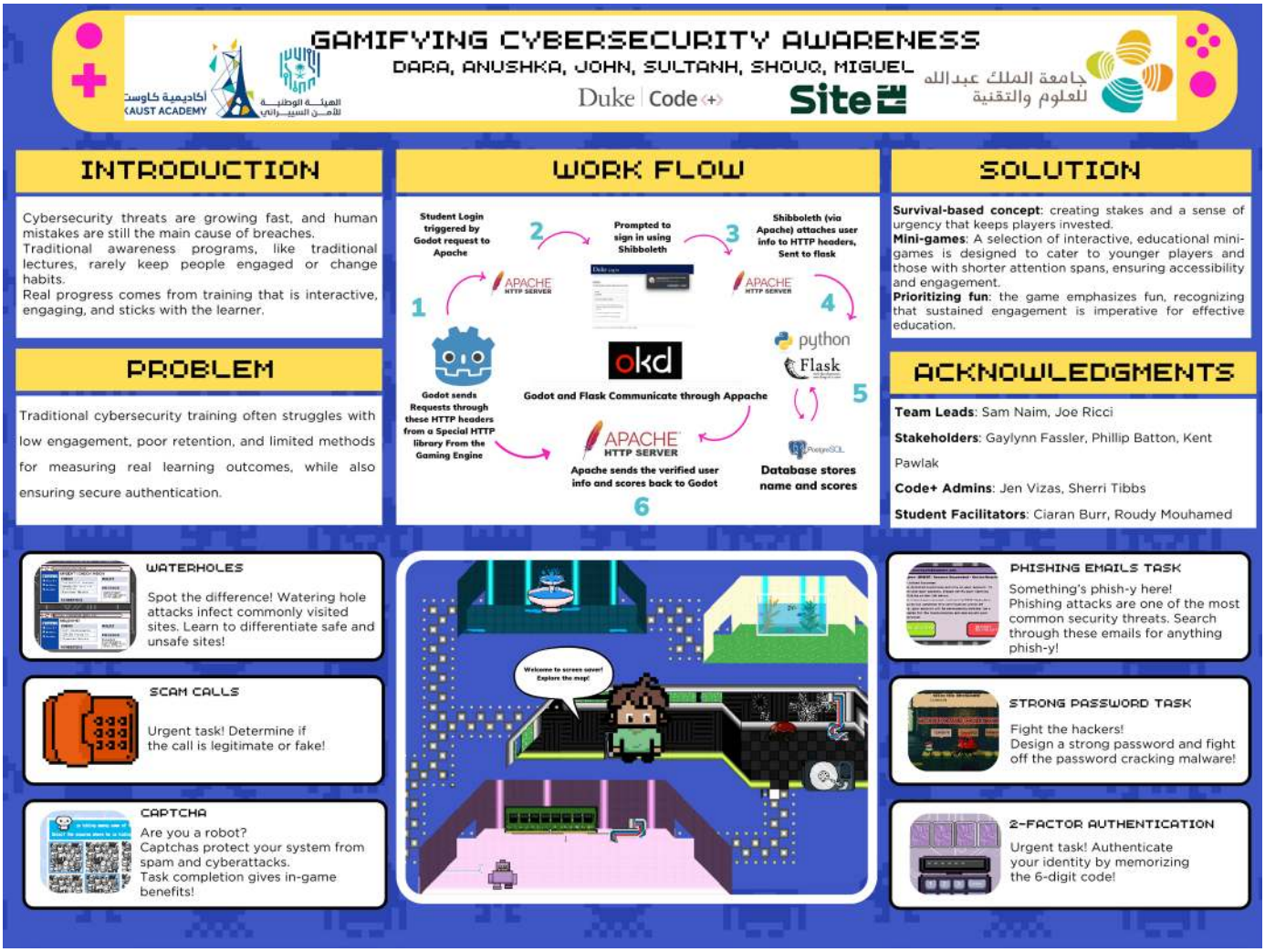
**PROJECT MEMBERS:** Ahmed Sadiq bin Ahmed Al-Ghannam,Fahad Hamoud Mohammed Al-Athel, Meshari Abdulrahman bin Ibrahim Alsughayyir

# GAMIFYING CYBERSECURITY AWARENESS

This project focuses on creating an engaging, interactive experience to raise cybersecurity awareness among students. Using gamification techniques, the team will design and develop a hands-on activity, such as a security-themed escape room, capture-the-flag challenge, or phishing simulation. These activities will immerse participants in solving real-world cybersecurity problems, like decoding encrypted messages, spotting phishing attempts, or configuring secure systems, fostering a deeper understanding of key concepts. Students will collaborate with Duke's Office of Information Technology (OIT), IT Security Office (ITSO), and cybersecurity experts to bring this concept to life. As a stretch goal, the project will be developed as an open-source resource, enabling other universities to adopt these gamified activities and expand cybersecurity awareness in higher education.

**PROJECT MENTOR:** Sam Naim

**PROJECT MEMBERS:** Shouq Miq'ad Abdullah Al-Otaibi,Sultanh Sami Saleh Al-Diab

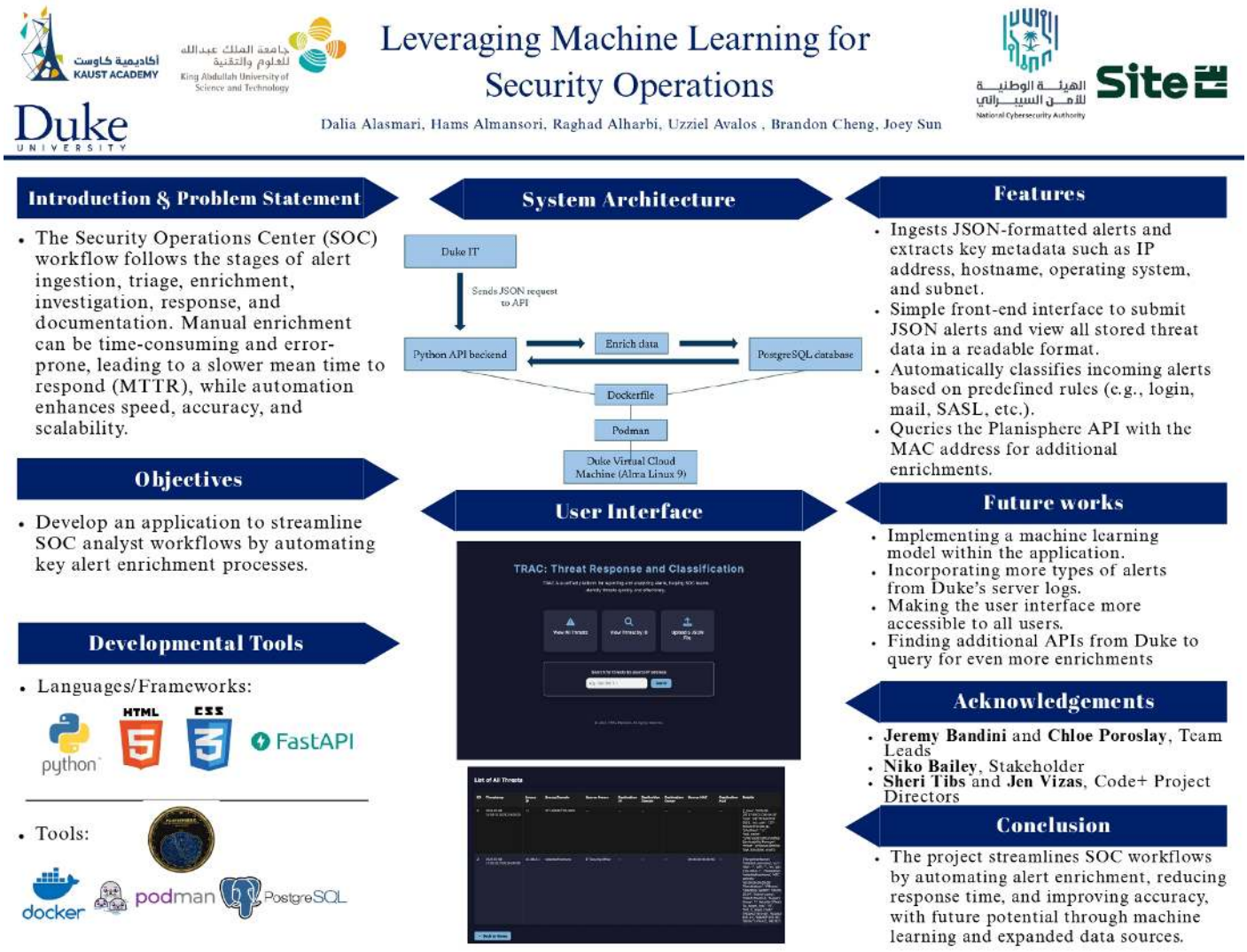


# LEVERAGING MACHINE LEARNING FOR SECURITY OPERATIONS

This project focuses on exploring machine learning (ML) techniques to enhance the efficiency of the Security Operations Center (SOC). By automating lower-level alert triaging, the goal is to save time and reallocate resources to higher-value tasks. Students will design and build tools that leverage ML for data preprocessing, feature optimization, and advanced alert analysis. The project will also include developing pipelines and user interfaces to deliver a production-ready solution. This project aims to provide students with experience in cutting-edge security and ML applications while delivering a practical tool to enhance SOC operations. The resulting solution will improve alert accuracy and streamline investigation workflows, showcasing the transformative potential of ML in cybersecurity.

**PROJECT MENTOR:** Jeremy Bandini

**PROJECT MEMBERS:** Dalia Saeed Faiz Al-Asmari,Hams Mohammed Bin Atiq Almansori, Raghad Yousef Lafi Al-Harbi

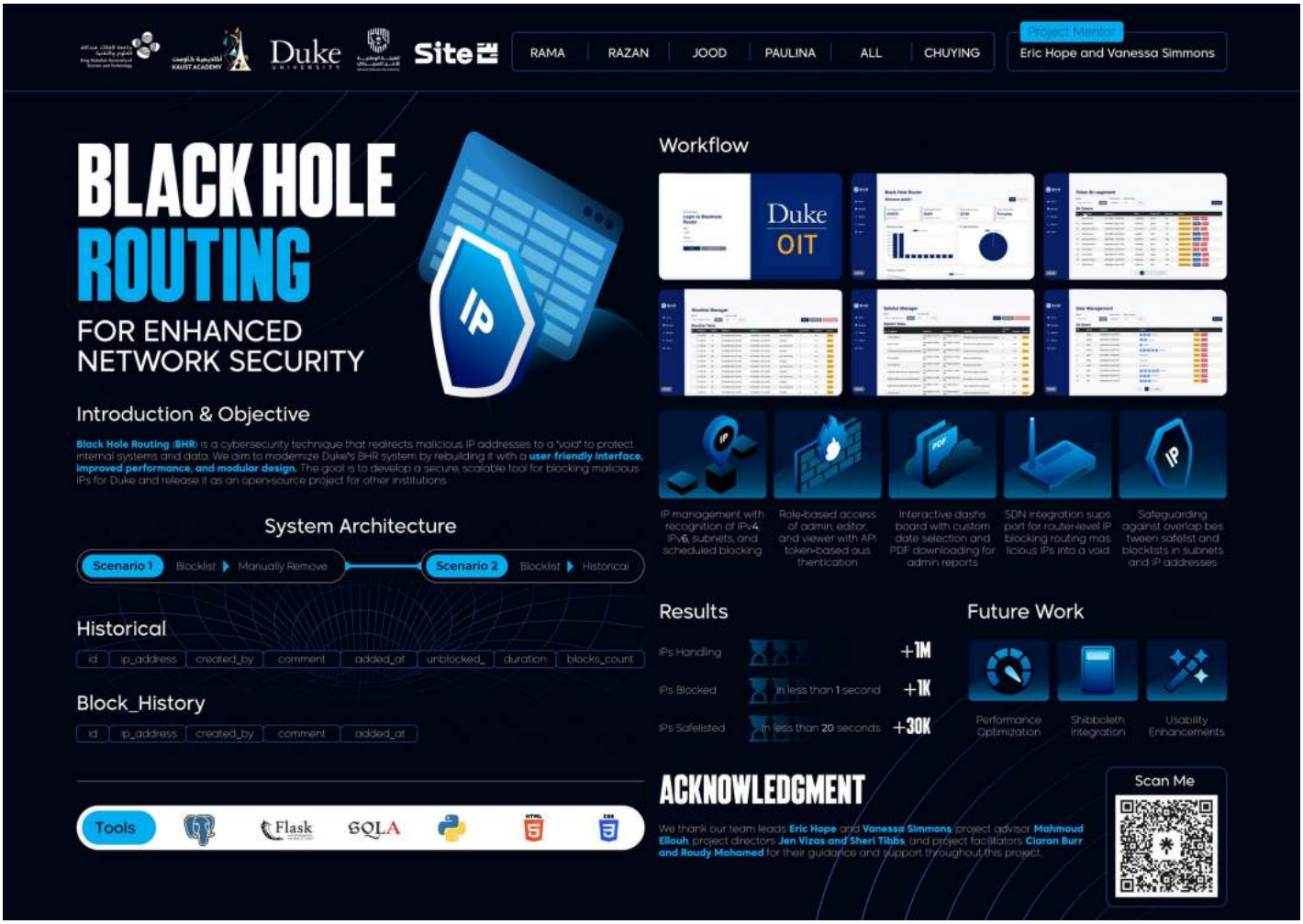


# MODERNIZING BLACK HOLE ROUTING FOR ENHANCED NETWORK SECURITY

This project focuses on upgrading Duke's Black Hole Routing (BHR) system, a key tool for blocking malicious IP addresses and protecting network security. The current system relies on outdated architecture and interfaces, limiting its performance. Students will modernize BHR by developing a portable, containerized solution that integrates with modern infrastructure and can be shared as an open-source tool with other universities. Collaborating with Duke's Office of Information Technology (OIT), IT Security Office (ITSO), and cybersecurity experts, the team will define project requirements and implement a robust, efficient system. This project offers hands-on experience in cybersecurity tool development while contributing to enhanced network security across higher education institutions.

**PROJECT MENTOR:** Eric Hope

**PROJECT MEMBERS:** Razan Faris bin Abdulrahman Almalki,Jood Hamad bin Abdullah Alolayan, Ramah Ahmed Saeed Al-Guthmi



أكاديمية كاوست
KAUST ACADEMY

جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Prepared and presented at King Abdullah University of Science and Technology. We extend our gratitude to all mentors, colleagues, and the KAUST community. For more details and resources, please visit our official website via the QR code