

**Centre of Cyber Security and Big Data**

Minutes of Research Meeting

Date : 25th September 2024

Time : 10.00am

Venue : Meeting Room, Level 14

**ATTENDEES:**

1. Assoc. Prof. Ts. Dr. Asif Iqbal Manager, AICS
2. Shahswiene Suthas SOC Analyst 1, AICS
3. Nurul Dhabitah Salemi Intern
4. Nurhidayatul Alya Intern

**1. OPENING REMARKS:**

* The Manager welcomed all members to the meeting.

**2. MATTERS DISCUSSED:** During the Security Operation Centre (SOC) Team Meeting held on 3rd January 2024, several matters were discussed, including the assignment of research titles to the interns. Here's a more detailed explanation of the matters discussed:

**3. Discussion of Research Titles:**

1. **Title: Generative AI-Driven Analytics in SOCs: Bridging the Cybersecurity Skills Gap**
   1. **Authors:**
      * Asif Iqbal Hajamydeen (Centre of Cyber Security and Big Data, Management & Science University, Malaysia, asif@msu.edu.my)
      * Shahswiene Suthas (Faculty of Information Sciences and Engineering, Management & Science University, Malaysia, shahswiene\_suthas@msu.edu.my)
      * Muhammad Irsyad Abdullah (Management and Science University, Malaysia, irsyad@msu.edu.my)
2. **Title: Building a Robust SOC: The Benefits of Integrating Wazuh and a Mobile Ticketing System for Security Operations**
   1. **Authors:**
      * Asif Iqbal Hajamydeen (Centre of Cyber Security and Big Data, Management & Science University, Malaysia, asif@msu.edu.my)
      * Nurul Dhabitah Salemi (Faculty of Information Sciences and Engineering, Management & Science University, Malaysia, nuruldhabitahsalemi@gmail.com)
      * Muhammad Irsyad Abdullah (Management and Science University, Malaysia, irsyad@msu.edu.my)
3. **Title: Velociraptor: Empowering Modern SOCs with Enhanced Threat Hunting and Proactive Security Monitoring**
   1. **Authors:**
      * Muhammad Irsyad Abdullah (Management and Science University, Malaysia, irsyad@msu.edu.my)
      * Nurul Dhabitah Salemi (Faculty of Information Sciences and Engineering, Management & Science University, Malaysia, nuruldhabitahsalemi@gmail.com)
      * Asif Iqbal Hajamydeen (Centre of Cyber Security and Big Data, Management & Science University, Malaysia, asif@msu.edu.my)
4. **Title: Authors: Title: AutomatIrsyadcial Engineering Attack Simulations in SOC Environments: Combining SET and Zphisher for Realistic Threat Testing**
   1. **Authors**:
      * Asif Iqbal Hajamydeen (Centre of Cyber Security and Big Data, Management & Science University, Malaysia, asif@msu.edu.my)
      * Nurhidayatul Alya Muhammad Soleh (Faculty of Information Sciences and Engineering, Management & Science University, Malaysia, alyahs823@gmail.com)
      * ⁠Muhammad Irsyad Abdullah (Management and Science University, Malaysia, irsyad@msu.edu.my)
5. **Discussion:**
   1. Correction on paper, adjust formatting according to the requirements.
   2. Updates in References.
   3. Brainstorm ideas on correction review.
   4. Reminding of submission date.
   5. Submission on: End of November

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

The meeting was adjourned at 11.00 am on 25th September 2024.

Prepared by, Endorsed by,

Shahswiene Suthas Assoc. Prof. Dr. Muhammad Irsyad Abdullah