Jordan University of Science and Technology

Faculty of Computer and Information Technology

Department of Cyber Security

Subject: EAB meeting minutes

Meeting no.: 1

Date: 20/7/2023

Place: Cyber Security Department

Attendees	Ma'mon, Qussai Kanash(BDM), Dr. Malek Qasaymeh (HoD),Dr.Mazen Alwadi (Dean Assistant) Eng.Areej Bataineh (QA), Mohammad ALNimrat(Cy QA officer) Mohammad Obidat (Students) X,Y (Academic member from the deprtment)
Absent	Rami Yaseen ,Omar Al Omari (BDM)
Recorded By	Mohammad ALNimrat
Agenda	1. **Assess the Syllabus:** Review the cybersecurity syllabus to ensure it covers essential and relevant topics that align with industry demands and technological advancements. 2. **Market Relevance:** Identify training topics that address current market needs, such as SOC operations, incident response, penetration testing, OT security, and cloud security. 3. **Practical Emphasis:** Enhance the curriculum with practical exercises, hands-on labs, and real-world simulations to equip students with tangible skills applicable in professional settings. 4. **Industry Collaboration:** Establish partnerships with companies to provide internship opportunities, giving students valuable industry exposure and networking prospects. 5. **Certifications:** Encourage students to pursue recognized certifications like CISP, boosting their credentials and marketability to potential employers.

	6. **Soft Skills Development:** Integrate soft skill training, including communication, teamwork, and problem-solving, to groom well-rounded professionals capable of thriving in the workplace. 7. **Technical Proficiency:** Ensure students gain strong technical knowledge in networking, operating systems, and relevant programming languages crucial for a successful cybersecurity career. 8. **Critical Thinking:** Foster critical thinking and analytical abilities to enable students to assess complex cybersecurity challenges and devise effective solutions. 9. **Ethical Considerations:** Emphasize ethical practices and principles throughout the syllabus, instilling a sense of responsibility and integrity in future cybersecurity experts. 10. **Adaptability to Change:** Equip students with the ability to adapt to the dynamic cybersecurity landscape, as technologies and threats constantly evolve. 11. **Collaboration Between Teams:** Promote collaboration between Blue and Red teams, allowing students to grasp the importance of teamwork and a comprehensive approach to security. 12. **Exposure to Emerging Trends:** Introduce emerging trends in cybersecurity, such as threat intelligence, AI-driven security, and IoT security, to keep students updated on the latest developments.
The meeting progress	**Evening Session:**
Actions	1. Integrate additional topics related to SOC (Security Operations Center), Incident Response, Penetration Testing, and OT (Operational Technology) Security to enrich the curriculum. 2. Prioritize practical applications and hands-on training, providing students with real-world scenarios and challenges to better understand the concepts. 3. Incorporate in-depth study on the collaboration between the BLUE team (defenders) and RED team (attackers) to foster a comprehensive understanding of cybersecurity strategies.

	4. For students undergoing training in companies, allow them to commence practical training after completing 90 hours of courses, with a specific focus on SOC operations. 5. Highlight the significance of the CISP (Certified Information Security Professional) certification as one of the most valuable certifications for Cyber Security students. 6. Include modules on Cloud Security and Threat Hunting, as these areas play crucial roles in contemporary cybersecurity landscapes. 7. Establish dedicated labs for each topic to provide students with hands-on experiences, allowing them to apply their knowledge in a safe and controlled environment.