| QF01/0408-4.0E | Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department |
|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Study plan No.** | **2024/2025** | | **University Specialization** | **Cybersecurity** | |
| **Course No.** | **0133409** | | **Course name** | Security Operations Center (SOC) | |
| **Credit Hours** | **3** | | **Prerequisite Co-requisite** | Infrastructure Security Using Linux (0125233)<br>Secure Communication Protocols (0125347) | |
| **Course type** | ☐ MANDATORY UNIVERSITY REQUIREMENT | ☐ UNIVERSITY ELECTIVE REQUIREMENTS | ☐ FACULTY MANDATORY REQUIREMENT | ☐ Support course family requirements | ☐ ✓ **Mandatory requirements** ☐ Elective requirements |
| **Teaching style** | ☐ **Full online learning** | | ☐ Blended learning | | ☐ ✓ Traditional learning |
| **Teaching model** | ☐ 2Synchronous: 1asynchronous | | ☐ 2 face to face : 1synchronous | | ☐ ✓ **3 Traditional** |

## Faculty member and study divisions information (to be filled in each semester by the subject instructor)

| **Name** | **Academic rank** | **Office No.** | **Phone No.** | **E-mail** | |
|---|---|---|---|---|---|
| **Dr Omran Salem** | **Assistant Professor** | **316** | | **o.salem@zuj.edu.jo** | |
| | | | | | |
| **Division number** | **Time** | **Place** | **Number of students** | **Teaching style** | **Approved model** |
| | | | | | |
| | | | | | |
| | | | | | |

## Brief description

The Security Operations Center (SOC) Course equips students with the skills to detect, analyze, and respond to cyber threats using industry-standard tools like SIEM, IDS/IPS, and SOAR. Through hands-on labs and real-world simulations, students learn threat hunting, incident response, and the role of automation in cybersecurity. The course emphasizes teamwork, communication, and ethical practices, preparing students for careers in SOC operations. By the end, students will be proficient in managing cyber threats and operating effectively in a SOC environment.

## Learning resources

| | |
|---|---|
| Course book information (Title, author, date of issue, publisher ... etc.) | SOC Essentials (SCE), V1<br>Publisher: EC-Council Academia<br>Year: 2022<br>https://www.eccouncil.org/train-certify/soc-essentials-course-sce/ |
| Supportive learning resources (Books, databases, periodicals, software, applications, others) | 1. Title: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide<br>Author(s): Omar Santos<br>Publisher: Cisco Press<br>Year: 2021<br>2. Title: Cisco Certified CyberOps Associate 200-201 Certification Guide<br>Author(s): Glen D. Singh<br>Publisher: Packt Publishing<br>Year: 2021<br>3. Title: Effective Threat Investigation for SOC Analysts<br>Author(s): Mostafa Yahia |

| | | | | |
|---|---|---|---|---|
| | Publisher: Packt Publishing<br>Year: 2023<br>ISBN: 1837634785; 9781837634781<br>4. Title: Jump-start Your SOC Analyst Career: A Roadmap to Cybersecurity Success<br>Author(s): Tyler Wall; Jarrett Rodrick<br>Publisher: Apress<br>Year: 2021<br>ISBN: 9781484269046; 1484269047 | | | |
| Supporting websites | https://app.letsdefend.io/path/soc-analyst-learning-path<br>https://socradar.io/top-10-training-platforms-for-soc-analysts/ | | | |
| The physical environment for teaching | ☐ **Class room** | ☐ ✓labs | ☐ **Virtual educational platform** | ☐ Others |
| Necessary equipment and software | | | | |
| Supporting people with special needs | | | | |
| For technical support | **E-learning and Open Educational Center. Computer Center** | | | |

## Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

| No. | Course learning outcomes | The associated program learning output code |
|---|---|---|
| | **Knowledge** | |
| **K1** | Demonstrate knowledge of foundational cybersecurity concepts, principles, and theories relevant to SOC. | PLO1 |
| **K2** | Understand the processes, tools, and techniques used in SOC for threat detection and response. | PLO2 |
| **K3** | Explain the relationship between data networks, protocols, and cybersecurity in a SOC environment. | PLO3 |
| **K4** | Identify and describe current and emerging trends, tools, and technologies in SOC operations. | PLO5 |
| | **Skills** | |
| **S1** | Analyze and evaluate complex cybersecurity threats and incidents using SOC methodologies. | PLO6 |
| **S2** | Apply cybersecurity tools and techniques to detect, analyze, and respond to threats in a SOC. | PLO7 |
| **S3** | Use computational and quantitative methods to process and interpret cybersecurity data. | PLO9 |
| **S4** | Demonstrate creativity and innovation in solving cybersecurity problems within a SOC. | PLO8 |
| | **Competences** | |
| **C1** | Independently manage SOC tasks, including threat monitoring, analysis, and reporting. | PLO11 |
| **C2** | Make ethical and professional decisions in high-pressure SOC scenarios. | PLO12 |
| **C3** | Collaborate effectively in a team-based SOC environment to achieve cybersecurity objectives. | PLO11 |

| | | |
|---|---|---|
| **C4** | Contribute to the development of SOC processes and community service in cybersecurity. | PLO13 |

## Mechanisms for direct evaluation of learning outcomes

| Type of assessment / learning style | Fully electronic learning | Blended learning | Traditional Learning (Theory Learning) | Traditional Learning (Practical Learning) |
|---|---|---|---|---|
| First exam | 0 | **0** | 0 | 0 |
| Second / midterm exam | %30 | **%30** | %30 | %30 |
| Participation / practical applications | 0 | **0** | 0 | 0 |
| Asynchronous interactive activities | %30 | **%30** | %30 | %30 |
| final exam | %40 | **%40** | %40 | %40 |

**Note:** Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc., which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

## Schedule of simultaneous / face-to-face encounters and their topics

| Week | Subject | learning style* | Reference ** |
|---|---|---|---|
| **1-2** | **Module 1: Introduction to SOC and Cybersecurity Fundamentals**<br>- Networking & Cyber Threats<br>- Overview of SOC and its role in cybersecurity<br>- Fundamental concepts of cybersecurity<br>- Threat landscape and attack vectors<br>- Legal and ethical considerations | Face to Face | SOC Essentials (SCE), V1 |
| **3** | **Module 2: SOC Tools and Technologies**<br>- Overview of SOC tools (SIEM, IDS/IPS, firewalls, EDR)<br>- Log collection, correlation, and analysis<br>- Threat intelligence platforms | Face to Face | SOC Essentials (SCE), V1 |
| **4** | **Module 3: Threat Detection and Analysis**<br>- Threat detection methodologies<br>- Indicators of Compromise (IoCs)<br>- Malware analysis basics | Face to Face | SOC Essentials (SCE), V1 |
| **5** | **Module 4: Incident Response and Handling**<br>- Incident response lifecycle<br>- Role of SOC in incident response<br>- Forensic basics for SOC analysts | Face to Face | SOC Essentials (SCE), V1 |
| **6 - 7** | **Module 5: Advanced SOC Operations** | Face to Face | SOC Essentials (SCE), V1 |

| | | | |
|---|---|---|---|
| | - Advanced threat hunting techniques<br>- Automation and orchestration in SOC<br>- Machine learning and AI in cybersecurity | | |
| **8** | **Midterm Exam** | | |
| **9-10** | **Module 6: SOC Team Collaboration and Communication**<br>- Role of teamwork in SOC operations<br>- Effective communication strategies<br>- Reporting and escalation procedures | Face to Face | SOC Essentials (SCE), V1 |
| **11-12** | **Module 7: Ethical and Professional Conduct in SOC**<br>- Ethical hacking and responsible disclosure<br>- Legal frameworks (e.g., GDPR, HIPAA)<br>- Professional standards and certifications | Face to Face | SOC Essentials (SCE), V1 |
| **13-14** | **Module 8: Capstone Project**<br>- Simulate a real-world SOC environment<br>- Tasks: Threat detection, analysis, response, and reporting | Face to Face | SOC Essentials (SCE), V1 |
| **15** | Project Discussion | Face to Face | |
| **16** | Final Exam | | |

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

## Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

**This activities was designed using the** Project-Based Learning (PBL)

### Project 1: SOC Analyst Toolkit Development (Modules 2 & 3)

| Task / Activity | Reference | Expected Results |
|---|---|---|
| Build a mini-SIEM using ELK Stack (Elasticsearch, Logstash, Kibana) to collect & correlate firewall & system logs. Implement a custom IDS rule (e.g., Snort/YARA) to detect a specific IoC. | Splunk/SIEM Admin Guides, MITRE ATT&CK, Snort Rule Documentation | A working log dashboard with correlated alerts and a functional detection rule generating alerts for the specified IoC. |

### Project 2: Incident Response Simulation Lab (Modules 3 & 4)

| QF01/0408-4.0E | Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department |
|---|---|

| Task / Activity | Reference | Expected Results |
|---|---|---|
| Simulate a malware incident. Analyze provided artifacts (logs, hashes) to identify IoCs, contain the threat, and draft an incident report following the NIST IR lifecycle. | NIST SP 800-61, SANS IR Steps, Malware Analysis Reports | A completed IR report containin identified IoCs, containment ste taken, and forensic timeline of t attack. |

| Week | Task / activity | Reference | Expected results |
|---|---|---|---|
| 1-2 | Lab: Setting up a virtual SOC environment<br>Exercise: Identifying and categorizing common threats | Online guides for setting up SOC environments (e.g., VMware, VirtualBox)<br>Threat databases (e.g., MITRE ATT&CK) | Students successfully set up a virtual SOC and create a categorized list of common threats. |
| 3 | Lab: Configuring and using a SIEM tool (e.g., Splunk, ELK Stack)<br>Exercise: Analyzing logs to detect anomalies | Splunk/ELK documentation, tutorials, and YouTube walkthroughs | Students configure the SIEM tool, ingest logs, and identify anomalies using built-in search and analysis tools. |
| 4 | Lab: Using threat intelligence feeds to identify IoCs<br>Exercise: Analyzing malware samples in a sandbox | Threat intelligence platforms (e.g., AlienVault, VirusTotal)<br>Malware analysis tools (e.g., Any.Run, Cuckoo Sandbox) | Students identify IoCs from threat feeds and analyze a malware sample, documenting key findings. |
| 5 | Lab: Simulating an incident response scenario<br>Exercise: Writing incident reports | Incident response frameworks (e.g., NIST 800-61)<br>Templates for incident reports | Students handle a simulated incident and produce a detailed, well-structured incident report. |
| 6-7 | Lab: Writing scripts to automate SOC tasks (e.g., Python for log analysis)<br>Exercise: Using SOAR tools (e.g., Phantom, Demisto) | Python scripting tutorials<br>SOAR platform documentation and online walkthroughs | Students write automation scripts and integrate workflows using SOAR tools to respond to predefined scenarios. |
| 8 | Midterm Exam | | |
| 9 - 10 | Lab: Simulating a SOC team exercise (e.g., responding to a multi-stage attack)<br>Exercise: Writing and presenting a detailed incident report | Case studies on multi-stage attacks<br>Incident report presentation guides | Students work collaboratively, respond to a simulated attack, and present findings in a professional manner. |
| 11-12 | Lab: Conducting a vulnerability assessment and reporting findings ethically<br>Exercise: Case study on ethical dilemmas in cybersecurity | Nessus/Qualys documentation for vulnerability assessments<br>Articles on ethical cybersecurity practices | Students complete a vulnerability assessment and critically discuss ethical dilemmas in cybersecurity. |
| 13-14 | Lab: Full-scale SOC simulation using a cyber range (e.g., RangeForce, CyberBit)<br>Exercise: Presenting findings to a mock executive board | Cyber range platforms and documentation<br>Cybersecurity presentation techniques | Students perform full-scale SOC operations and deliver executive-level reports to a mock board. |