IBA Institute of Business Administration Karachi

Leadership and Ideas for Tomorrow

IBA CICT

Centre for Information & Communication Technologies

Certification on

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Centre for Information &
Communication Technologies

IBA CICT

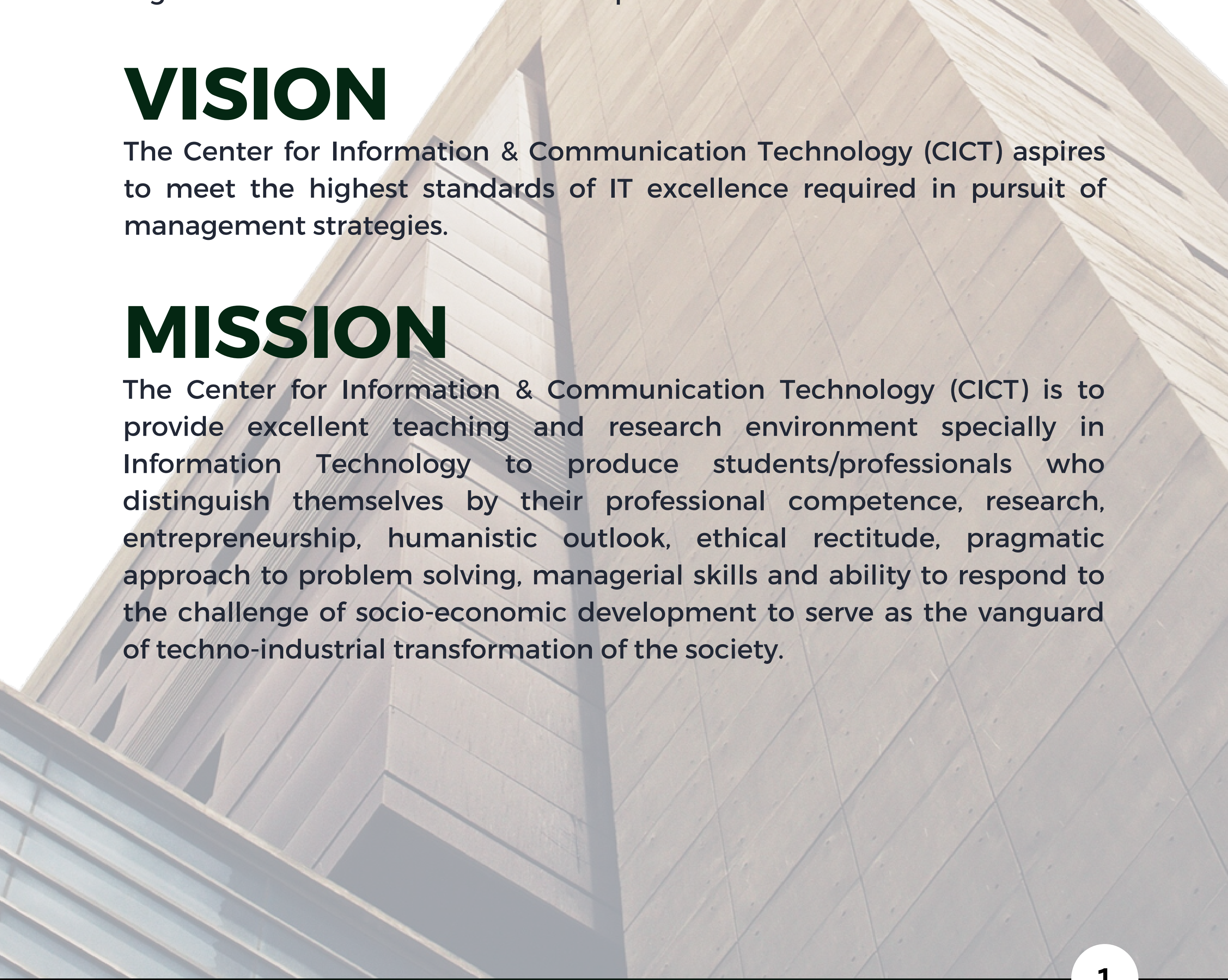
At IBA, education goes beyond the classroom, preparing our students to navigate the corporate world with technology leadership, vision and challenges. The CICT at IBA is a center of excellence in continuing education providing professional diplomas, certifications, and workshops in the field of Information technology, Information Systems, and Computer Science. The CICT was established in 2016 providing high-quality professional education to the private and public sectors in Pakistan. The CICT has been associated with renowned faculty members who conduct certain courses and workshops which contribute to the digitalization in the educational and professional sectors.

VISION

The Center for Information & Communication Technology (CICT) aspires to meet the highest standards of IT excellence required in pursuit of management strategies.

MISSION

The Center for Information & Communication Technology (CICT) is to provide excellent teaching and research environment specially in Information Technology to produce students/professionals who distinguish themselves by their professional competence, research, entrepreneurship, humanistic outlook, ethical rectitude, pragmatic approach to problem solving, managerial skills and ability to respond to the challenge of socio-economic development to serve as the vanguard of techno-industrial transformation of the society.



IBA Institute of Business Administration Karachi
Leadership and Ideas for Tomorrow

IBA CICT
Centre for Information & Communication Technologies

Workshop on

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Are you ready to take your cybersecurity career to the next level and become a master's in security operations Center (SOC) operations and threat management? Our "Advanced SOC Operations and Threat Management Training" program is your gateway to expertise in safeguarding digital landscapes against evolving cyber threats. In today's hyper-connected world, organizations face an ever-expanding array of cyber threats. This intensive and comprehensive course provides a deep dive into the heart of cybersecurity operations, where you'll develop the skills and knowledge neededto excel in the role of a SOC professional.

January 2024

40 Hours

Rs. 85,000

Why Choose Our Training:

- Practical Experience: Benefit from hands-on labs, real-world simulations, and live bug-hunting exercises to hone your skills.
- Expert Instructors: Learn from experienced industry professionals who have defended against and analyzed cyber threats in diverse environments.
- Certification: Obtain a recognized certification, demonstrating your expertise in SOC operations and threat management.
- Career Advancement: Open doors to a wide range of cybersecurity career opportunities, from SOC analyst to security consultant or manager.

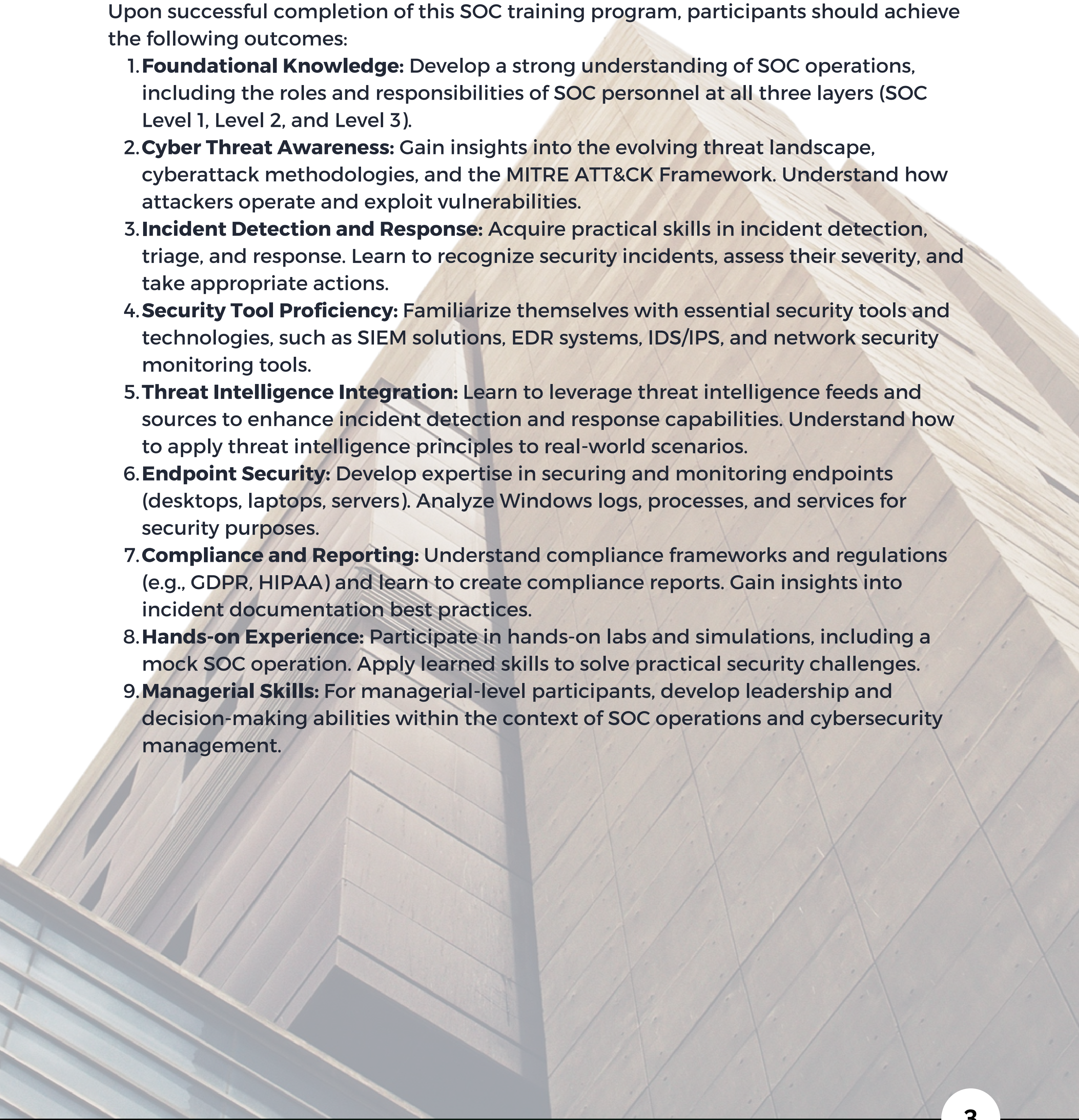
Prerequisites for Training Program

1. **Basic IT Skills:** Participants should have a fundamental understanding of computer systems, networks, and IT terminology.
2. **Networking Knowledge:** Familiarity with networking concepts, including protocols, IP addressing, and routing, is beneficial.
3. **Security Fundamentals**: A basic understanding of cybersecurity principles, such as confidentiality, integrity, and availability (CIA triad), is recommended.
4. **Operating System Proficiency:** Familiarity with common operating systems (e.g., Windows, Linux) and their basic administration is helpful.
5. **Cybersecurity Basics:** Knowledge of key cybersecurity concepts like malware, firewalls, and encryption provides a foundation for SOC training.
6. **IT Experience:** Some prior experience in IT roles, such as system administration or network administration, can be advantageous.

Workshop on

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management



Learning Outcomes

Upon successful completion of this SOC training program, participants should achieve the following outcomes:

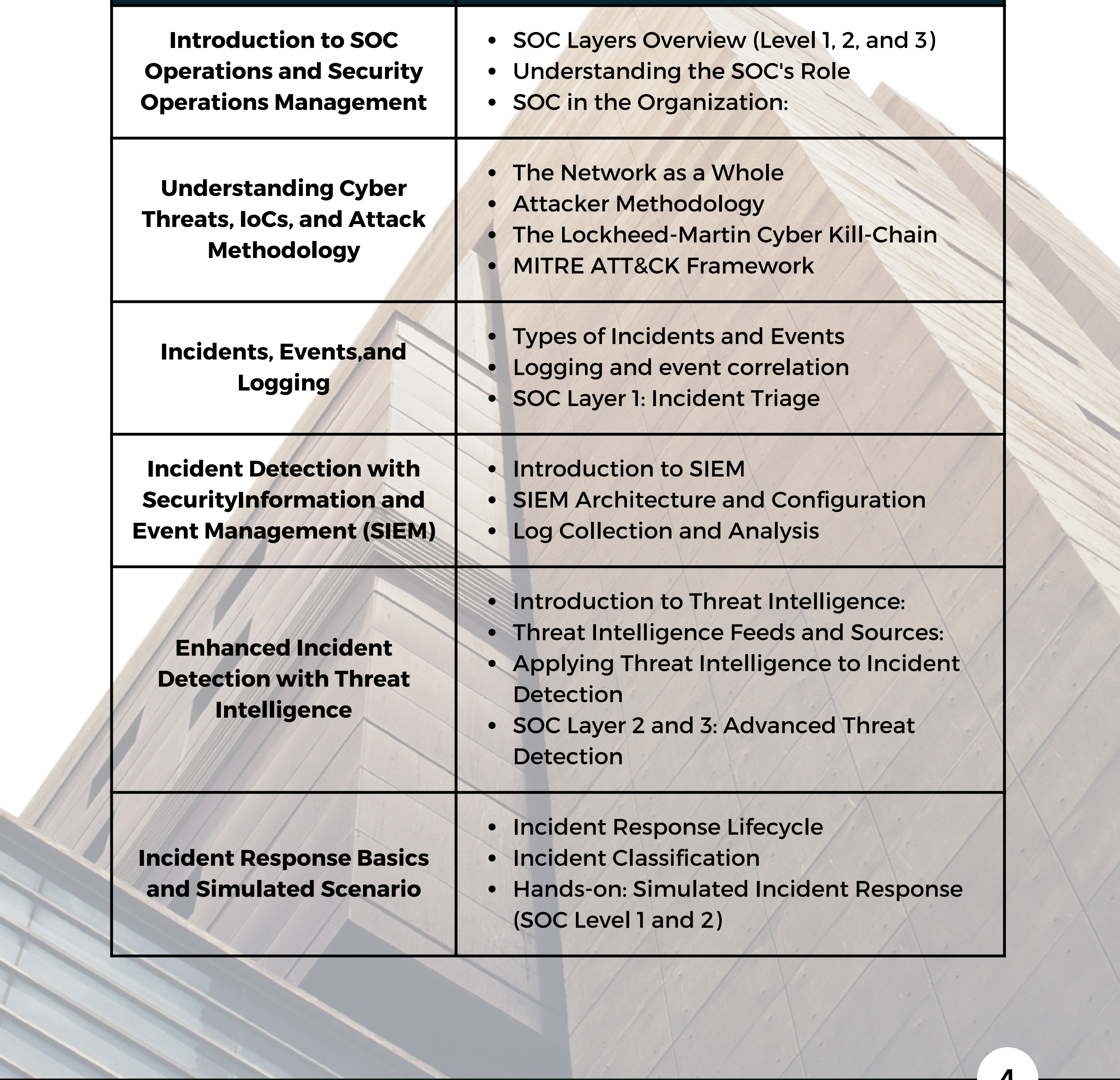
1. **Foundational Knowledge:** Develop a strong understanding of SOC operations, including the roles and responsibilities of SOC personnel at all three layers (SOC Level 1, Level 2, and Level 3).
2. **Cyber Threat Awareness:** Gain insights into the evolving threat landscape, cyberattack methodologies, and the MITRE ATT&CK Framework. Understand how attackers operate and exploit vulnerabilities.
3. **Incident Detection and Response:** Acquire practical skills in incident detection, triage, and response. Learn to recognize security incidents, assess their severity, and take appropriate actions.
4. **Security Tool Proficiency:** Familiarize themselves with essential security tools and technologies, such as SIEM solutions, EDR systems, IDS/IPS, and network security monitoring tools.
5. **Threat Intelligence Integration:** Learn to leverage threat intelligence feeds and sources to enhance incident detection and response capabilities. Understand how to apply threat intelligence principles to real-world scenarios.
6. **Endpoint Security:** Develop expertise in securing and monitoring endpoints (desktops, laptops, servers). Analyze Windows logs, processes, and services for security purposes.
7. **Compliance and Reporting:** Understand compliance frameworks and regulations (e.g., GDPR, HIPAA) and learn to create compliance reports. Gain insights into incident documentation best practices.
8. **Hands-on Experience:** Participate in hands-on labs and simulations, including a mock SOC operation. Apply learned skills to solve practical security challenges.
9. **Managerial Skills:** For managerial-level participants, develop leadership and decision-making abilities within the context of SOC operations and cybersecurity management.

Workshop on

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topics to be covered:



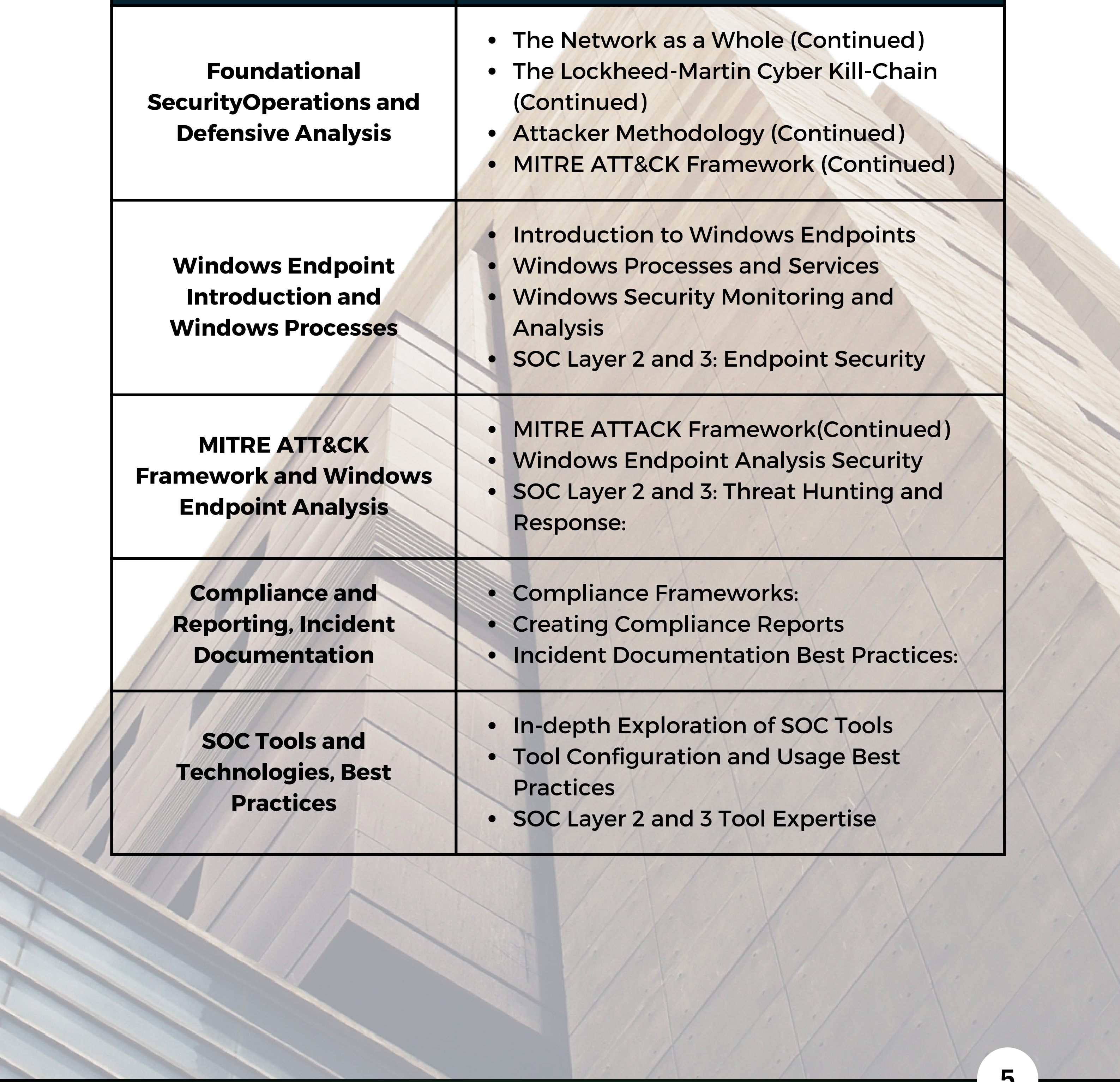
Topic	Sub topics
Introduction to SOC Operations and Security Operations Management	• SOC Layers Overview (Level 1, 2, and 3) • Understanding the SOC's Role • SOC in the Organization:
Understanding Cyber Threats, IoCs, and Attack Methodology	• The Network as a Whole • Attacker Methodology • The Lockheed-Martin Cyber Kill-Chain • MITRE ATT&CK Framework
Incidents, Events,and Logging	• Types of Incidents and Events • Logging and event correlation • SOC Layer 1: Incident Triage
Incident Detection with SecurityInformation and Event Management (SIEM)	• Introduction to SIEM • SIEM Architecture and Configuration • Log Collection and Analysis
Enhanced Incident Detection with Threat Intelligence	• Introduction to Threat Intelligence: • Threat Intelligence Feeds and Sources: • Applying Threat Intelligence to Incident Detection • SOC Layer 2 and 3: Advanced Threat Detection
Incident Response Basics and Simulated Scenario	• Incident Response Lifecycle • Incident Classification • Hands-on: Simulated Incident Response (SOC Level 1 and 2)

Workshop on

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topics to be covered:



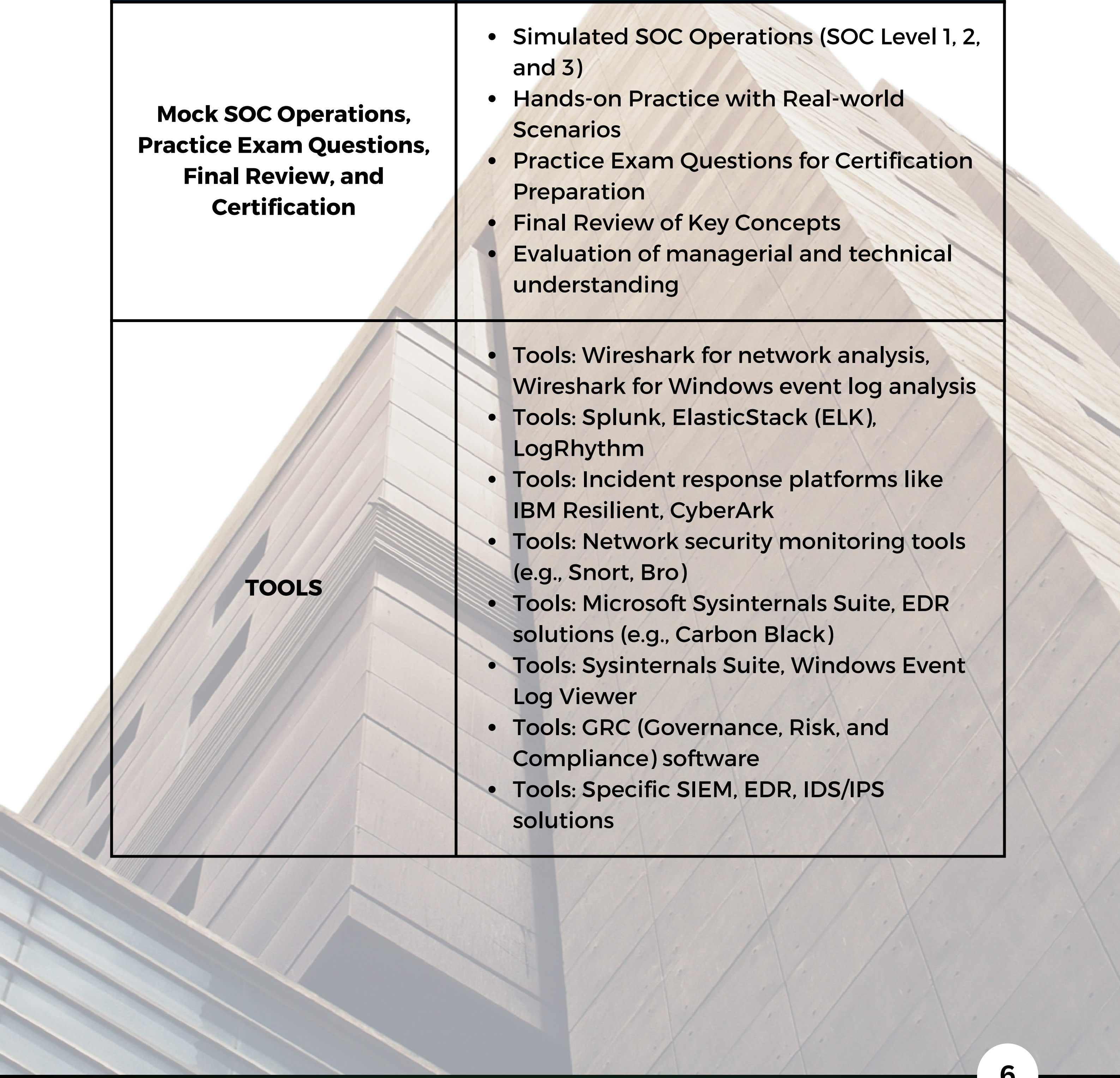
Topic	Sub topics
Foundational SecurityOperations and Defensive Analysis	- The Network as a Whole (Continued) - The Lockheed-Martin Cyber Kill-Chain (Continued) - Attacker Methodology (Continued) - MITRE ATT&CK Framework (Continued)
Windows Endpoint Introduction and Windows Processes	- Introduction to Windows Endpoints - Windows Processes and Services - Windows Security Monitoring and Analysis - SOC Layer 2 and 3: Endpoint Security
MITRE ATT&CK Framework and Windows Endpoint Analysis	- MITRE ATTACK Framework(Continued) - Windows Endpoint Analysis Security - SOC Layer 2 and 3: Threat Hunting and Response:
Compliance and Reporting, Incident Documentation	- Compliance Frameworks: - Creating Compliance Reports - Incident Documentation Best Practices:
SOC Tools and Technologies, Best Practices	- In-depth Exploration of SOC Tools - Tool Configuration and Usage Best Practices - SOC Layer 2 and 3 Tool Expertise

Workshop on

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topics to be covered:



Topic	Sub topics
Mock SOC Operations, Practice Exam Questions, Final Review, and Certification	• Simulated SOC Operations (SOC Level 1, 2, and 3) • Hands-on Practice with Real-world Scenarios • Practice Exam Questions for Certification Preparation • Final Review of Key Concepts • Evaluation of managerial and technical understanding
TOOLS	• Tools: Wireshark for network analysis, Wireshark for Windows event log analysis • Tools: Splunk, ElasticStack (ELK), LogRhythm • Tools: Incident response platforms like IBM Resilient, CyberArk • Tools: Network security monitoring tools (e.g., Snort, Bro) • Tools: Microsoft Sysinternals Suite, EDR solutions (e.g., Carbon Black) • Tools: Sysinternals Suite, Windows Event Log Viewer • Tools: GRC (Governance, Risk, and Compliance) software • Tools: Specific SIEM, EDR, IDS/IPS solutions

Connect with us:

Our Team:

Mahwish Ahmed

Senior Office Coordinator
soc_cict@iba.edu.pk
021-38104701 (Ext. 1160)

Dr. Syed Irfan Nabi

Academic Quality &
Enhancement Specialist
aqes_cict@iba.edu.pk
021-38104701 (Ext. 1151)

Kanwar M. Zarar

Program Associate
kmzarar@iba.edu.pk
021-38104701 (Ext. 1149)

Hafiz M. Obaid

Executive Secretary
hmobaid@iba.edu.pk
021-38104701 (Ext. 1118)

Other Available EXTs

EXT: 1146, 1158, 1148