IBA 70 YEARS & BEYOND
Leadership ▪ Excellence ▪ Impact

IBA CICT
Center for Information & Communication Technology

Certificate Program

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

+92-21-38104701 (1148) | cict.iba.edu.pk | cict@iba.edu.pk

Follow us 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.

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.

Program Details

Dates To Be Announced Soon

Weekend Program

Investment: Rs. 85,000/- (+3% SST)

2-Months Certification

Duration: 06:00 PM - 09:00 PM

+92-21-38104701 (1148) | cict.iba.edu.pk | cict@iba.edu.pk Follow us on:

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.

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.

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topic	Sub Topic
Introduction to SOC Operations and Security Operations Management	SOC Layers Overview (Level 1, 2, and 3): • SOC Level 1: Monitoring and Alert Triage • SOC Level 2: Analysis and Investigation • SOC Level 3: Threat Hunting and Response
	Understanding the SOC's Role: • Protecting digital assets • Detecting and responding to threats • Incident management
	SOC in the Organization: • Integration with IT and business goals
Understanding Cyber Threats, IoCs, and Attack Methodology	The Network as a Whole: • Demilitarized Zone (DMZ) • Core vs. Edge Network Devices • Virtual Private Networks (VPNs)
	Attacker Methodology: • Reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives
	The Lockheed-Martin Cyber Kill-Chain: • Application to Malware and Ransomware
	MITRE ATT&CK Framework: • Classifications and Case Studies
	Tools: Wireshark for network analysis, Wireshark for Windows event log analysis

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topic	Sub Topic
Incidents, Events,and Logging	Types of Incidents and Events: • Security incidents vs. operational incidents • Security Information and Event Management (SIEM) events
	Logging and EventCorrelation: • Log sources (e.g., firewalls, IDS/IPS) • Event correlation and normalization
	SOC Layer 1: Incident Triage: • Initial assessment of alerts
Incident Detection with SecurityInformation and Event Management (SIEM)	Introduction to SIEM: • Purpose and benefits • Centralized log management
	SIEM Architecture and Configuration: • Log collectors, correlation engines, dashboards • Log collection and aggregation
	Log Collection and Analysis: • Log sources, log formats, log analysis
	Tools: Splunk, ElasticStack (ELK), LogRhythm

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topic	Sub Topic
Enhanced Incident Detection with Threat Intelligence	Introduction to Threat Intelligence: • External and internal threat intelligence • Threat intelligence feeds and sources
	Threat Intelligence Feeds and Sources: • Open source vs. commercial feeds • Threat indicators (IoCs)
	Applying Threat Intelligence to Incident Detection: • Threat feeds in SIEM • Identifying IoCs in logs
	SOC Layer 2 and 3: Advanced Threat Detection: • Threat intelligence-driven detection
Incident Response Basics and Simulated Scenario	Incident Response Lifecycle: • Preparation, identification, containment, eradication, recovery, lessons learned.
	Incident Classification: • Severity levels, incident types
	Hands-on: Simulated Incident Response (SOC Level 1 and 2): • Responding to a simulated incident
	Tools: Incident response platforms like IBM Resilient, CyberArk

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topic	Sub Topic
Foundational SecurityOperations and Defensive Analysis	The Network as a Whole (Continued): • Remote sites and their security considerations
	Attacker Methodology (Continued): • Application to real-world case studies
	The Lockheed-Martin Cyber Kill-Chain (Continued): • Application to real-world case studies
	MITRE ATT&CK Framework (Continued): • Application to real-world case studies
	Tools: Network security monitoring tools (e.g., Snort, Bro)
Windows Endpoint Introduction and Windows Processes	Introduction to Windows Endpoints: • Desktops, laptops, servers
	Windows Processes and Services: • Understanding what runs on Windows • Relationship between processes and services
	Windows Security Monitoring and Analysis: • Endpoint securitylogs and event IDs
	SOC Layer 2 and 3: Endpoint Security: • Monitoring and protecting endpoints
	Tools: Microsoft Sysinternals Suite, EDR solutions (e.g., Carbon Black)

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topic	Sub Topic
MITRE ATT&CK Framework and Windows Endpoint Analysis	MITRE ATT&CK Framework(Continued): • Application to real-world case studies
	Windows Endpoint Analysis and Security: • Analyzing Windows logs and event data
	SOC Layer 2 and 3: Threat Huntingand Response: • Using endpoint data for threat hunting
	Tools: Sysinternals Suite,Windows Event Log Viewer
Compliance and Reporting, Incident Documentation	Compliance Frameworks: • GDPR, HIPAA, PCI DSS, etc.
	Creating Compliance Reports: • Reporting tools and templates
	Incident Documentation Best Practices: • Documenting incident details
	Tools: GRC (Governance, Risk, and Compliance) software

SECURITY OPERATIONS CENTER

Advance SOC Operations and Threat Management

Topic	Sub Topic
SOC Tools and Technologies, Best Practices	In-depth Exploration of SOC Tools: • SIEM, EDR, IDS/IPS, firewall management
	Tool Configuration and Usage Best Practices: • Setting up alerts and rules • Incident investigation using tools.
	SOC Layer 2 and 3 Tool Expertise: • Advanced usage of SOC tools
	Tools: Specific SIEM, EDR, IDS/IPSsolutions
Mock SOC Operations, Practice Exam Questions, Final Review, and Certification	Simulated SOC Operations (SOC Level 1, 2, and 3): • Handling real-world scenarios
	Hands-on Practice with Real-world Scenarios: • Applying skills to mock incidents
	Practice Exam Questions for Certification Preparation: • Reviewing key concepts
	Final Review of Key Concepts: • Summarizing the entire course
	Certification Assessment (Managerial Level): • Evaluation of managerial and technical understanding

IBA 70 YEARS & BEYOND
Leadership ▪ Excellence ▪ Impact

IBA CICT
Center for Information & Communication Technology

Click Here To Register Now

Contact Us:

0320-3861073

021-38104701
(Ext. 1148)

cict@iba.edu.pk

Connect With Us