CYBERSECURITY CENTER OF EXCELLENCE (CCoE)

CCOE COURSE CATALOGUE

Scan here for further information

BlackBerry Cybersecurity Center of Excellence
GF, MCMC Centre of Excellence (CoE), Persiaran Multimedia, Jalan Impact, Cyber 6,
63000 Cyberjaya, Selangor, Malaysia

TABLE OF CONTENTS

CYBERSECURITY SKILLS TRAINING

ENTRY LEVEL

Course Name	Description	Duration	Target Audience
Cybersecurity Awareness	BlackBerry's security awareness training will help you become cyber-safe through implementing key behaviours to reduce risk. Learn why security awareness is a life skill, how to reduce your online risk, protect yourself and others, and what to do if you suspect you have been a victim of a security attack. There is no exam for this course, but students will be tested on their knowledge through class quizzes. Ready to be a Cyber Defender? Sign up to this fun and informative short course today.	3 Hours	Students, new graduates, career-change, employees (for annual compliance)
Introduction to Cybersecurity	Introduction to Cybersecurity: a comprehensive instructor-led entry level course designed to provide you with essential knowledge in the field of IT and Cybersecurity. Understand computer components and their functions, explore network architecture and security protocols & develop virtualization models. Dig into cloud computing and the complexities of wireless technology. Gain insights into crucial concepts including operating systems and security, cybersecurity essentials, malware, phishing, social engineering, as well as proactive versus reactive security.	2 Days	Students, new graduates, career-change, entry-level IT employees
Information Technology - Computer Essentials	Information Technology is the use of computer systems to store, process, manipulate and retrieve information. Information technology or IT is an integral component of most business functions. Gain essential technologies competencies and durable skills,like setting up your own computer,configuring the computer settings, working with the hard drive & many more.	1 Day	Students, new graduates, career-change, IT professionals (Help Desk Technician, Technical Support, IT Technician)
Information Technology - Networking Essentials	Gain a wide range of technical and hands-on skills required of today's early-career in network. Understand routing and important factors of physical installations; configure switching technologies and wireless devices.	1 Day	Tech-adjacent workers, IT professionals (Network Support Technician, Help Desk Support)
Information Technology - Security Essentials	Gain insights into safeguarding digital information and ensuring privacy and data protection. Course will equip individuals with the essential understanding of cybersecurity which includes the CIA Triad, authentication, encryption and much more.	1 Day	Students, new graduates, career-change, IT professionals (Technical Support, Help Desk Support).
Introduction to Cloud Computing	This course introduces cloud computing and its benefits and underlying technologies. Concepts such as private cloud, public cloud, service deployment model such as IaaS,PaaS & SaaS are explained. The course also provides a quick demonstration of a public cloud in action so participant can better relate the theory with the actual solution helping them appreciate how the cloud technology will impact & transform the entire industry. This course is suited to newcomers to IT and Cybersecurity as well as those already in the profession looking to gain additional insights.	2 Hours	Students, new graduates, career-change, IT professionals
Introduction to Mobile Security Technology	The course aims to provide participants with a foundational understanding of mobile security technologies, focusing on concepts such as Mobile Device Management (MDM), Mobile Application Management (MAM), and Runtime Application Self-Protection (RASP). By the end of the course, participants will be equipped to understand various threats on mobile, then evaluate and choose the appropriate mobile security technology.	2 Hours	Students, new graduates, career-change, IT professionals
Introduction to Identity & Access Management (IAM)	This course provides a foundational understanding of Identity and Access Management (IAM) principles, and technologies. Participants will gain insights into IAM basic and theoretical concepts in securing organizational resources and managing user access effectively. Learners will explore key IAM components, authentication methods and authorization mechanisms.	2 Hours	Students, new graduates, career-change, IT professionals

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY SKILLS TRAINING

INTERMEDIATE LEVEL

Course Name	Description	Duration	Target Audience
Cybersecurity Tools	Throughout the Cybersecurity Tools course, participants will explore an array of essential cybersecurity tools, including tools for network security, endpoint security, data loss prevention, application security, data security, cloud security, and monitoring and incident response. Discover how these tools form an important line of defence for organizations who need to protect themselves in an ever-evolving threat landscape.	6 Hours	Students, new graduates, career-change, IT professionals
Cybersecurity & AI	Delve into the world of cybersecurity and AI through this comprehensive instructor-led course. Gain an in-depth understanding of artificial intelligence and its applications in cybersecurity. Analyze the benefits and potential risks associated with the integration of AI in cybersecurity. Learn about effective AI mitigation strategies to address cybersecurity challenges. Explore advanced AI techniques tailored for cybersecurity applications. Examine the ethical and legal considerations surrounding the use of AI in cybersecurity. Understand how AI is transforming the cybersecurity landscape.	6 Hours	Students, new graduates, career-change, IT professionals
Scripting for Cybersecurity	This course is designed to equip aspiring cybersecurity professionals with the essential skills to automate security tasks through scripting. This course covers the fundamentals of scripting languages commonly used in cybersecurity, such as Python, Bash, and PowerShell, with a focus on practical applications in real-world security scenarios.	6 Hours	Students, new graduates, career-change, IT professionals
Reverse Malware Engineering	How do you determine a file is malicious? This course will cover Windows EXE and DLL malware analysis, OSINT triage, static file analysis, behavioral analysis & threat intelligence basics to help you determine with high confidence which files are a security concern. Students must have a technical background including being familiar with common terminology associated with malware.	2 Days	New to threat research and forensic investigation, IT professionals
Cyber Risk Management	This course prepares members of the senior management to understand, assess, and take a proactive posture in cybersecurity. With this training, you gain the fundamental knowledge and skills to assess cyber risk aligned to your enterprise risk management framework. We discuss some common security findings, reports and initiatives management can expect from their technology teams. This course is ideally suited to those in senior management including C-Suite Executives.	3 Hours	Professionals in Management, Senior Management including C-Suite Executives
Cloud Architecture & Security in AWS	This course provides essential skills for understanding cloud architectures using Amazon Web Services (AWS). Emphasis is placed on implementing security best practices, such as encryption, identity management, and network protection, while ensuring compliance with regulatory standards. **Prerequisites**: Basic knowledge of cloud computing.	5 days	Students, new graduates, career-change, IT professionals
Mobile Security Intermediate	This hands-on intermediate-level course provides a practical understanding of mobile security with a focus on real-world threats and defenses. Participants will explore mobile OS architecture, emulators, Android Debug Bridge (ADB), and scripting techniques. Through guided labs, they'll learn how to use tools like Frida for app instrumentation and simulate Man-in-the-Middle (MITM) attacks to assess mobile app vulnerabilities. The course also covers critical defense mechanisms such as Runtime Application Self-Protection (RASP) and Unified Endpoint Management (UEM), equipping learners with the skills to secure mobile environments in enterprise settings. **Prerequisites**: Attended Intro to Mobile Security OR has basic mobile security knowledge	2 days	Learners who have attended Intro to Mobile Security, Mobile developer, IT professionals, Solution Architect, System Engineer
Identity & Access Management (IAM) Intermediate	This 2-day hands-on course is designed for IT and cybersecurity professionals seeking to deepen their practical knowledge of Identity and Access Management (IAM) using free and open-source tools. Participants will explore core IAM concepts including authentication, authorization, directory integration, single sign-on (SSO), identity governance, and privileged access management (PAM). Through guided labs with tools like Keycloak, OpenLDAP, OneSpan, learners will build and secure an end-to-end IAM environment, gaining practical skills to implement IAM solutions in real-world scenarios. **Prerequisites:** Attended Intro to IAM or has basic IAM knowledge	5 days	Learners who have attended Intro to IAM, Mobile developer, IT professionals, Solution Architect, System Engineer

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CAREERS COURSES

CAREER PATH

2 Hours

- Calling all University graduates and those with 1-3 years work experience in tech or cyber!
- Discuss potential career paths for a cybersecurity professional and the different roles one can play within the cybersecurity team and journey.
- Discuss some relevant skills, knowledge, and certifications relevant to these roles.
- Suitable for students, new graduates, career-change, IT professionals.

ENTRY

2 Hours

- Delves into various aspects, current trends in the cybersecurity job market.
- Explore the common entry-level roles in cybersecurity, analyse the skills necessary to thrive in these roles, an overview of the associated responsibilities, a discussion of potential certifications, and guidance on choosing a career path within the cybersecurity domain.
- Suitable for those who are new to cybersecurity, recent graduates, career-change, IT professionals

EXPERT

2 hours

- Explore the cybersecurity landscape of your country and expert roles in cybersecurity. Focus on essential knowledge and skills required in the field to understand tasks and responsibilities involved in expert cybersecurity roles. Get guidance on career development in the cybersecurity field along with insight into relevant certifications.
- Suitable for Cybersecurity professionals, IT professionals, career change in tech.

SPECIALIST

2 Hours

- Explore the cybersecurity landscape of your country and specialized roles in cybersecurity. Focus on essential knowledge and skills required in the field to understand tasks and responsibilities involved in specialized cybersecurity roles. Get guidance on career development in the cybersecurity field along with insight into relevant certifications.
- Suitable for cybersecurity professionals looking to specialize.

MANAGEMENT

2 Hours

- Delve into the intricacies of cybersecurity in your country, explore the NICE Framework and specialized roles in the industry, and gain valuable insights into the knowledge, skills, tasks, and responsibilities necessary for a successful management career in cybersecurity. Discover the importance of certifications and explore avenues for career development in this dynamic field.
- Suitable for Cybersecurity professionals, IT professionals looking to move into Management positions.

Course fees: contact ccoemalaysia@blackberry.com for quotation

ROLE-BASED EDUCATION PROGRAMS

ADVANCED LEVEL

Course Name	Description	Duration	Target Audience
SOC Analyst and Security Manager	The SOC Analyst and Security Manager course is designed to equip students with the essential skills to protect digital assets within a Security Operation Center (SOC). This comprehensive course not only offers theoretical knowledge but also provides practical hands-on training, covering crucial topics such as network intrusion detection, hybrid infrastructure security, blue team fundamentals, threat intelligence, Windows security, and SIEM and monitoring. By enrolling, you will learn robust security architecture, monitor network traffic, identify and mitigate threats, and automate security processes using industry standards tool such as SOAR platforms and PowerShell. This course is ideal for aspiring cybersecurity professionals, IT practitioners, and organizations looking to upskill their teams, providing a solid foundation for a successful career in cybersecurity.	5 Days	Cybersecurity / IT professionals, SOC analyst, security manager
Incident Response, Threat Intelligence & Digital Forensic Investigators	This course provides hands-on training in managing cybersecurity incidents, conducting proactive threat hunting, and performing digital forensics. Students will learn to respond effectively to security incidents, from preparation to recovery, while applying threat intelligence and analyzing advanced threats. The course also covers the skills needed to investigate breaches through forensic techniques, including evidence handling, memory analysis, and malware investigation. By the end, students will be equipped to identify, analyze, and respond to cyber threats and incidents effectively. **Prerequisites:** Basic understanding of cybersecurity concepts.	5 Days	Cybersecurity / IT professionals, security analyst, new to incident response, threat intelligence and forensic investigation
Vulnerability Managers & Pen Testers	This course explores every stage of a penetration test, from pre-engagement and reconnaissance through enumeration, exploitation, and reporting. Emphasis is placed on interpreting network and host vulnerabilities, understanding common attack vectors, and mapping technical findings to business risk. This course uses structured tabletop simulations, guided walkthroughs, and scenario-based learning to reinforce concepts. By the end, learners will gain the skills to perform reconnaissance, analyze systems, discover vulnerabilities, and communicate risk professionally in preparation for CREST CPSA certification or junior security roles. **Prerequisites:** Basic understanding of cybersecurity concepts.	5 Days	Cybersecurity / IT professionals with one to three years of experience in networking, systems, or cybersecurity operations

Course fees: contact ccoemalaysia@blackberry.com for quotation

TRAINING COURSES FOR BLACKBERRY PRODUCTS

Course Name	Description	Duration	Target Audience
CylanceENDPOINT	As an organization scales, its fleet of end-user devices grows with it. With a greater number of endpoints comes a higher risk of threat actors. In today's digital era of AI and Machine learning, learn how an AI-driven Cylance endpoint solution can secure your organization from existing as well as emerging threats. In this course, you will explore how AI and machine learning play an important role together to form an industry-leading endpoint security tool.	1 Day	Product User (prospective product user), industry experts, IT professionals
BlackBerry SecuSUITE	In today's digital era, where privacy is at stake, learn how your organization can maintain confidentiality, integrity, and availability with BlackBerry SecuSUITE, a leading multi-platform solution for encrypted communication. This course will demystify encryption by deep-diving into types of encryption and encryption algorithms. Learn how these technologies interact to form a robust cybersecurity product and get hands-on experience with the BlackBerry SecuSUITE app.	1 Day	Product User (prospective product user), industry experts, IT professionals
BlackBerry UEM	With hybrid work, organizations need to find a balance that enables worker productivity, while keeping them secure, and maintaining their privacy. All while meeting regulatory requirements. With the BlackBerry UEM, learn how organizations can accomplish all of this while maintaining control and the visibility needed to secure all endpoints.	1 Day	Product User (prospective product user), industry experts, IT professionals
BlackBerry AtHoc	In the event of a crisis, communication with all key stakeholders, including employees, management, and board members is essential. Learn how BlackBerry AtHoc critical event management solution combines a secure emergency notification system with incident response tools and capabilities—enable your response team to better prepare for, respond to, and recover from critical events.	3 Hours	Product User (prospective product user), industry experts, IT professionals

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

CompTIA

Course Name	Description	Duration	Target Audience
CompTIA Tech+	In this CompTIA certification course, students will identify PC components, work with files and folders, and conduct basic software installations. As one of the top IT certifications for beginners globally, this course will provide students with the fundamental skills and concepts required to maintain, support, and work efficiently with personal computers. In addition, it covers the essential skills and information needed to set up, configure, maintain, troubleshoot, and perform preventative maintenance of the hardware and software components of a basic personal computer workstation and basic wireless devices. Students will also implement basic security measures and implement basic computer and user support practices.	3 Days	Students, new graduates, career-change
CompTIA A+	CompTIA A+ is the industry standard for establishing a career in IT and proves IT pros can perform critical IT support tasks in the moment. The CompTIA A+ certification validates fundamental IT knowledge including networking, operating systems and security, as well as developing problem-solving skills needed for entry-level technical support careers. This official CompTIA certification training covers mobile devices, networking technology, hardware, virtualization and cloud computing and network troubleshooting as well as installing and configuring operating systems, expanded security, software troubleshooting and operational procedures.	5 Days	Students, new graduates, career-change, IT professionals
CompTIA Server+	CompTIA Server+ is a global certification that validates the hands-on skills needed to securely deploy, manage, and troubleshoot servers in data centre and hybrid environments. The CompTIA Server+ certification demonstrates essential knowledge in server administration, including hardware, storage, networks, and security, while strengthening students' problem-solving abilities in technical support and operations. This official CompTIA certification training covers server hardware installation and maintenance, storage technologies, virtualization, disaster recovery, security best practices, and performance monitoring, as well as diagnosing and resolving common server issues across diverse environments.	5 Days	Students, new graduates, career-change, career-change, IT support technicians, junior system administrators
CompTIA Linux+	CompTIA Linux+ is the industry certification that validates the foundational skills required to configure, manage, and troubleshoot Linux systems used in enterprise and cloud environments. The CompTIA Linux+ certification confirms core Linux competencies including command-line operations, system configuration, and security, while building students' confidence in solving day-to-day technical issues. This official CompTIA certification training covers Linux installation, command-line tools, scripting basics, system services, networking, permissions, security controls, and troubleshooting procedures, as well as maintaining and optimizing Linux systems in real-world IT environments.	5 Days	Students, new graduates, career-change, IT support technicians, system administrators, cloud/DevOps beginners

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

CompTIA

Course Name	Description	Duration	Target Audience
CompTIA Network+	The Official CompTIA Network+ course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. It also addresses the content described in the exam objectives for the CompTIA Network+ certification. If you are pursuing a CompTIA technical certification path, obtaining the CompTIA A+ certification is an excellent first step to take before preparing for the CompTIA Network+ examination.	5 Days	Students, new graduates, career-change, IT professionals
CompTIA Security+	The official CompTIA Security+ course is the primary curriculum you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination. As one of the top IT certifications for beginners globally, this course will provide guidance and expertise to build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.	5 Days	Students, new graduates, career-change, IT professionals
CompTIA PenTest+	CompTIA PenTest+ is a penetration testing certification for cybersecurity professionals tasked with penetration testing and vulnerability assessment and management and is an intermediate-skills level cybersecurity certification that focuses on offensive skills through pen testing and vulnerability assessment. Cybersecurity professionals with CompTIA PenTest+ know how to plan, scope, and manage weaknesses, not just exploit them. This CompTIA Penetration testing course focuses on offense through penetration testing and vulnerability assessment. It involves launching attacks on systems, discovering the vulnerabilities and managing them. In this CompTIA PenTest+ course, you will be introduced to some general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.	5 Days	Students, new graduates, career-change, IT professionals
CompTIA Cybersecurity Analyst (CySA+)	This CompTIA Cybersecurity Analyst certification course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.	5 Days	Students, new graduates, career-change, IT professionals

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

ISC2™

Course Name	Description	Duration	Target Audience
ISC2 Certified in Cybersecurity Certification (CC)	ISC2 CC training course and certification enable trainees to have the foundational knowledge, skills and abilities necessary for an entry- or junior-level cybersecurity role. This training course is to prepare the trainees for taking the exam of ISC2 CC.	3 Days	Students, new graduates, career-change, IT professionals
ISC2 Certified Information Systems Security Professional Certification (CISSP)	ISC2 CISSP training course and certification enable trainees with the knowledge, skills, and abilities to lead an organization's information security program. The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles. This training course is to prepare the trainees for taking the exam of ISC2 CISSP.	5 Days	IT professionals with at least 5 years of cumulative, paid work experience in 2 or more of the 8 domains of the ISC2 CISSP Common Body of Knowledge (CBK)*
ISC2 Certified Cloud Security Professional (CCSP)	ISC2 CCSP training course and certification enable trainees to prepare for the CCSP exam. Earning the globally recognized CCSP cloud security certification is a proven way to build your career and better secure critical assets in the cloud. The CCSP shows you have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by our certified members and cybersecurity experts around the globe.	5 Days	IT professionals with at least 5 years of cumulative work experience in information technology, of which 3 years must be in information security, and 1 year in 1 or more of the six domains of the ISC2 CCSP Common Body of Knowledge (CBK)*
ISC2 Certified Secure Software Lifecycle Professional (CSSLP)	This 5-day ISC2 Certified Secure Software Lifecycle Professional (CSSLP) training course equips participants with the knowledge and skills to integrate security best practices throughout the software development lifecycle (SDLC). Covering key domains such as secure software concepts, requirements, design, implementation, testing, deployment, and maintenance, this course prepares attendees for the CSSLP certification exam. Ideal for software developers, engineers, security professionals, and project managers, the training blends theoretical concepts with practical insights to promote secure coding and reduce software vulnerabilities from the start.	5 Days	IT Professionals with at least 4 years working experience.Software Architect, Software Engineer, Software Developer, Quality Assurance Tester, Penetration Tester
ISC2 Governance, Risk and Compliance Certification (CGRC)	The ISC2 Certified in Governance, Risk and Compliance (CGRC) training course provides a comprehensive understanding of how to assess and manage risk, ensure compliance, and implement governance frameworks within an organization. Covering key areas such as authorization processes, security and privacy controls, continuous monitoring, and the RMF (Risk Management Framework), this course is ideal for professionals working with systems subject to regulatory and compliance requirements. Whether you're a security practitioner, risk manager, or compliance officer, this course prepares you to earn the CGRC certification and contribute to secure, compliant, and well-governed systems across various sectors.	5 Days	IT Professionals with at least 2 years working experience. Cybersecurity Auditor, Cybersecurity Compliance Officer, GRC Architect, GRC Manager, Cybersecurity Risk & Compliance Project Manager, Cybersecurity Risk & Controls Analyst, Cybersecurity Third Party Risk Manager, Enterprise Risk Manager, GRC Analyst, GRC Director, Information Assurance Manager

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

EC-Council
Building A Culture Of Security

Course Name	Description	Duration	Target Audience
Ethical Hacking Essentials	Covers the fundamentals of ethical hacking, including cyberattack vectors, penetration testing phases, and basic countermeasures. Learners explore how hackers think and how to defend against common threats. **Prerequisites:** Basic understanding of computers and networking.	Self-paced learning	Beginners in cybersecurity, IT students, technical support staff, and anyone exploring a cybersecurity career.
Network Defense Essentials	Introduces network security fundamentals, focusing on firewalls, VPNs, intrusion detection systems (IDS), and endpoint protection. Learners gain insight into secure network architecture and defensive technologies. **Prerequisites:** Familiarity with networking concepts.	Self-paced learning	Aspiring network administrators, IT support personnel, and students interested in infrastructure protection.
Digital Forensics Essentials	Explores the basics of digital forensics, including evidence collection, file systems, incident response, and investigation techniques for cybercrime. **Prerequisites:** Basic IT or cybersecurity knowledge recommended.	Self-paced learning	Individuals interested in forensic analysis, law enforcement IT units, and students considering a cybersecurity investigation role.
Cloud Security Essentials	Provides foundational knowledge in cloud computing and cloud security principles. Topics include cloud service models, shared responsibility, data protection, and risk management in cloud environments. **Prerequisites:** General understanding of IT concepts.	Self-paced learning	IT professionals, system administrators, and students transitioning into cloud technologies.
DevSecOps Essentials	Introduces the integration of security into DevOps practices, covering secure coding, CI/CD pipeline risks, and automation tools for security enforcement. **Prerequisites:** Familiarity with software development and basic IT security.	Self-paced learning	Developers, DevOps engineers, and IT professionals aiming to incorporate security into development workflows.
IoT Security Essentials	Explains Internet of Things (IoT) architecture, security challenges, and countermeasures. Covers risk management and best practices in securing IoT devices and networks. **Prerequisites:** Basic knowledge of networks and connected devices.	Self-paced learning	IT staff, engineers, and security learners involved with IoT ecosystems.
SOC Essentials	Covers the functions of a Security Operations Center (SOC), including threat monitoring, SIEM tools, and incident handling. Learners understand the daily tasks of SOC analysts. **Prerequisites:** Basic cybersecurity understanding is recommended.	Self-paced learning	Aspiring SOC analysts, NOC staff transitioning to security, and students exploring blue team roles.
Threat Intelligence Essentials	Focuses on the collection, analysis, and use of threat intelligence to anticipate and respond to cyber threats. Includes threat actor profiling and threat data sources. **Prerequisites:** Some cybersecurity knowledge preferred.	Self-paced learning	Security analysts, incident responders, and individuals interested in cyber threat hunting.

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

EC-Council
Building A Culture Of Security

Course Name	Description	Duration	Target Audience
Certified Ethical Hacker (CEH)	Equips professionals with the skills to think and act like hackers. Covers footprinting, scanning, enumeration, system hacking, malware, sniffing, social engineering, web/server hacking, and more. **Prerequisites:** Basic knowledge of networking and security; CEH (Practical) requires hands-on skills.	Self-paced learning	Penetration testers, security officers, auditors, site administrators, and anyone responsible for securing IT infrastructure
Certified Hacking Forensic Investigator (CHFI)	Focuses on identifying, tracking, and prosecuting cybercriminals. Topics include investigation tools, evidence collection, analysis, and reporting for legal procedures. **Prerequisites:** Understanding of cybersecurity concepts; CEH or similar background recommended.	Self-paced learning	Digital forensic investigators, law enforcement personnel, system administrators, and security professionals handling incident response.
Certified Network Defender (CND)	Teaches network security technologies and operations. Emphasizes network defense, risk management, firewall configuration, secure routing, and incident detection. **Prerequisites:** Basic knowledge of networking and TCP/IP protocols.	Self-paced learning	Network administrators, security analysts, and IT professionals seeking hands-on defensive capabilities
EC-Council Certified Incident Handler (ECIH)	Prepares professionals to respond to and manage cybersecurity incidents. Includes threat detection, handling malware, email security, insider threats, and digital forensics. **Prerequisites:** Basic understanding of cybersecurity and incident management.	Self-paced learning	Incident response team members, SOC analysts, cybersecurity engineers, and risk management professionals.
EC-Council Certified Encryption Specialist (ECES)	Covers cryptography concepts including symmetric/asymmetric encryption, hashing, and encryption algorithms like AES and RSA. **Prerequisites:** Basic knowledge of information security or networking.	Self-paced learning	Security practitioners, penetration testers, and IT professionals who need a practical understanding of encryption technologies.
Certified Threat Intelligence Analyst (CTIA)	Provides skills to collect, analyze, and interpret threat data. Focus on building effective threat intelligence for proactive defense. **Prerequisites:** Understanding of cybersecurity concepts; experience in security operations is helpful.	Self-paced learning	Threat hunters, SOC analysts, cybersecurity strategists, and those involved in cyber threat intelligence programs

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

EC-Council
Building A Culture Of Security

Course Name	Description	Duration	Target Audience
Certified SOC Analyst (CSA)	Entry-level course designed for SOC analysts. Covers SIEM, log analysis, network and host security monitoring, incident detection, and reporting. **Prerequisites:** Basic networking and cybersecurity knowledge.	Self-paced learning	Aspiring SOC professionals, NOC analysts transitioning to security, and junior IT security team members.
Certified Cloud Security Engineer (C|CSE)	Covers cloud platform security, governance, risk, compliance, and cloud-specific attack vectors. Provides knowledge for securing AWS, Azure, and GCP environments. **Prerequisites:** Familiarity with cloud platforms and cybersecurity.	Self-paced learning	Cloud administrators, architects, security engineers, and professionals managing cloud environments
EC-Council Certified DevSecOps Engineer (ECDE)	Focuses on embedding security into the DevOps pipeline using tools and practices for secure code, automation, CI/CD pipeline protection, and vulnerability management. **Prerequisites:** Knowledge of DevOps practices and basic security concepts.	Self-paced learning	DevOps engineers, software developers, system architects, and cybersecurity professionals supporting development teams
Certified Cybersecurity Technician (CCT)	An entry-level course covering network defense, ethical hacking, digital forensics, and security operations. Designed to build a solid foundation in cybersecurity. **Prerequisites:** None officially required; basic IT knowledge is helpful.	Self-paced learning	Students, fresh graduates, and individuals entering the cybersecurity field.
Certified Chief Information Security Officer (CCISO)	Designed for senior professionals, this course focuses on governance, risk management, strategic program development, leadership, and compliance to align cybersecurity with business goals. **Prerequisites:** Minimum 5 years experience in any 2 of the 5 domains in CCISO.	Self-paced learning	Current and aspiring CISOs, senior security managers, and security professionals preparing for executive leadership roles

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

PECB

Course Name	Description	Duration	Target Audience
ISO/IEC 27001 Information Security Management Systems	SO/IEC 27001 provides the requirements for organizations aiming to establish, implement, maintain, and continually enhance an information security management system. The ISO/IEC 27001 certification represents a global benchmark in Information Security Management Systems (ISMS). This certification guides organizations in implementing a structured method for safeguarding sensitive information. It involves a comprehensive framework for pinpointing, evaluating, and addressing information security risks, crucial for maintaining the confidentiality, integrity, and availability of vital organizational data.		IT and security professionals, managers, auditors, and person involved in implementing or maintaining an ISO/IEC 27001 Information Security Management System
ISO/IEC 27001 Foundation	Gain knowledge on the fundamental components necessary to implement and manage an ISMS based on ISO/IEC 27001	2 Days	IT and security professionals, managers, auditors, and person involved in implementing or maintaining the system
ISO/IEC 27001 Lead Implementer	Develop the skills to support an organization in implementing and maintaining an ISMS based on ISO/IEC 27001	5 Days	IT and security professionals, managers, auditors, and person involved in implementing or maintaining the system
ISO/IEC 27001 Lead Auditor	Acquire the knowledge and skills to perform an ISMS audit by applying widely recognized audit principles, procedures, and techniques	5 Days	IT and security professionals, managers, auditors, and person involved in implementing or maintaining the system
Certified Chief Information Security Officer (CISO)	PECB CISO (Chief Information Security Officer) is a specialized accreditation for professionals aiming to assume senior-level executive positions in information security management. Embarking on the journey to obtain a CISO certification involves an in depth exploration of the strategic and operational aspects of information security leadership. This certification process covers a comprehensive curriculum including cybersecurity policies, risk management, incident response, compliance, and stakeholder communication. Gain necessary knowledge, skills, and strategies to lead information security programs effectively.	5 Days	Senior IT professionals, security managers, aspiring CISOs, risk and compliance leaders, experienced cybersecurity practitioners

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

PECB

Course Name	Description	Duration	Target Audience
ISO 22301 Business Continuity Management System	ISO 22301 is a globally recognized standard for business continuity management, ensuring organizations are prepared to continue operations during and after a disruptive incident. Embarking on the ISO 22301 certification journey entails mastering the art of business continuity and resilience. This certification process involves understanding and implementing the best practices for developing, maintaining, and improving a Business Continuity Management System (BCMS). It covers critical areas such as risk assessment, incident response planning, business impact analysis, and recovery strategies		Professionals & managers in business continuity, IT, risk management, auditing, operations, person implementing or maintaining a Business Continuity Management System
ISO 22301 Foundation	Understand the essential principles, concepts, and techniques of a BCMS and the requirements of ISO 22301	2 Days	Professionals & managers in business continuity, IT, risk management, auditing, operations, person implementing or maintaining the system
ISO 22301 Lead Implementer	Gain a comprehensive understanding of the BCMS implementation techniques and learn how to lead a team in implementing a BCSM based on ISO 22301	5 Days	Professionals & managers in business continuity, IT, risk management, auditing, operations, person implementing or maintaining the system
ISO 22301 Lead Auditor	Obtain knowledge and become competent to audit an organization's BCMS against the requirements of ISO 22301	5 Days	Professionals & managers in business continuity, IT, risk management, auditing, operations, person implementing or maintaining the system

Course fees: contact ccoemalaysia@blackberry.com for quotation

CYBERSECURITY CERTIFICATIONS

SANS

Course Name	Description	Duration	Target Audience
FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics	An in-depth training program designed for incident responders and threat hunters. This course provides advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks. It covers tactics and procedures that have evolved to address sophisticated adversaries such as APT nation-state actors, organized crime syndicates, and ransomware operators.	5 Days	Cybersecurity professionals
FOR509: Enterprise Cloud Forensics and Incident Response	An intermediate to advanced level course that focuses on the unique challenges of conducting forensics and incident response in cloud environments. This course teaches students how to effectively locate, identify, and collect data across various cloud platforms, including Microsoft Azure, AWS, and Google Cloud Platform.	5 Days	Cybersecurity professionals
SEC575: IOS and Android Application Security Analysis	This course focuses on the security of mobile devices and applications. It is designed to provide students with the skills necessary to understand the security strengths and weaknesses of Apple iOS and Android devices, including the latest versions.	5 Days	Cybersecurity professionals
FOR518: Mac and iOS Forensic Analysis and Incident Response Training	This course provides in-depth training on forensic analysis and incident response for Apple's Mac and iOS devices. This course is the first of its kind that is not vendor-based and focuses on raw data and detailed analysis to maximize the outcomes of Mac and iOS cases	5 Days	Cybersecurity professionals
FOR585: Smartphone Forensic Analysis in Depth	This course is designed for examiners and investigators who wish to acquire advanced skills in mobile device forensics. The course is continuously updated to keep pace with the latest developments in smartphone operating systems, third-party applications, and forensic techniques. It aims to provide participants with the knowledge to correctly interpret evidence from mobile devices, which is crucial in criminal cases, security threats, and other investigative scenarios	5 Days	Cybersecurity professionals

Course fees: contact ccoemalaysia@blackberry.com for quotation

CLIC PROGRAM

ROGERS cybersecure catalyst SANS

Course Name	Description	Duration	Target Audience
Certifications in Cybersecurity Leadership (CLIC)	CLIC (Certifications for Leadership in Cybersecurity) is an intensive cybersecurity training and certification program designed to give you the skills you need to launch a career in cybersecurity or elevate your career with cybersecurity skills. This rigorous cybersecurity training program, CLIC offers you the opportunity to earn two globally-recognized SANS GIAC certifications, hone your skills in the Catalyst Cyber Range and gain career mentorship from leading cyber experts. SANS GIAC certifications: GFACT and GSEC	6 Months	Students, new graduates, career-change, IT professionals

Course fees: contact ccoemalaysia@blackberry.com for quotation

OUR CONTACT:

☎ +603 83222396

@ ccoemalaysia@blackberry.com

Ground Floor,
MCMC Centre of Excellence (CoE)
Persiaran Multimedia, Jalan Impact, Cyber 6,
63000 Cyberjaya, Selangor, Malaysia.