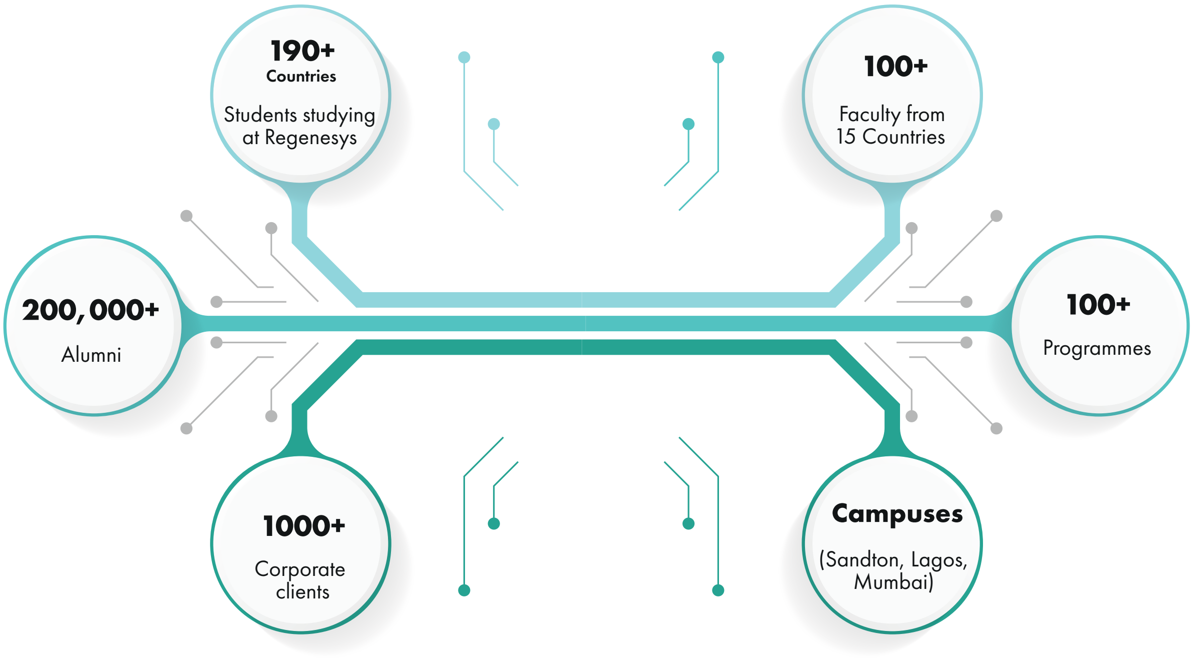
DIGITAL
REGENESYS

CYBERSECURITY

About Regenesys



190+
Countries
Students studying at Regenesys

100+
Faculty from 15 Countries

200,000+
Alumni

100+
Programmes

1000+
Corporate clients

Campuses
(Sandton, Lagos, Mumbai)

Our Clientele

Mercedes-Benz	Microsoft	DANONE	BMW
Standard Bank	SAMSUNG	BARCLAYS	intel
NEDBANK	ANGLO AMERICAN	sasol	Coca-Cola
momentum	LIBERTY	absa	MTN
	Massmart + Walmart	THE PRESIDENCY	

and many more..

Chairperson's Foreword

I am delighted to welcome you to Digital Regenesys at Regenesys Business School. The purpose of Regenesys is to help individuals awaken their potential and achieve their dreams.

New technologies, social media, and innovation have sparked a digital revolution that is rapidly changing the world. The digital revolution demands a new breed of professionals to succeed in the new digital world. To give you a competitive advantage, we have developed cutting-edge digital programmes in the areas of information technology and management. Our programmes are facilitated by leading experts, entrepreneurs, and academics from top local and international institutions.

Regenesys is a global business school with campuses in Johannesburg, Mumbai, and Lagos, delivering cutting-edge online and contact learning management programmes. Over the past 24 years, Regenesys has educated 200,000 students from 195 countries, and delivered corporate education programmes to 1000 reputable local and multinational companies. The majority of them are large multinationals such as Mercedes-Benz, Microsoft, Coca-Cola, Barclays, and Samsung, to name a few.

Regenesys alumni occupy top leadership positions in multinational corporations and government institutions all over the world, and form a very influential alumni network that supports its members with business opportunities across the world.

Get inspired, energised, and transform your career with programmes grounded in the realities of the new digital world.

I wish you success on your journey towards greatness.

Dr Marko Saravanja
Executive Chairperson
Regenesys Group

Cybersecurity

Course Description:

Safety and privacy on the internet is in higher demand than ever before. Corporations have a large amount of data that needs to be protected and kept secure from outside interventions. That is why the requirement for cyber security professionals is at a rise. Upskill yourself with a course in Cyber Security Program, which has high demand to improve business outcomes and unprecedented global demand and career opportunities.

Target Group:

The course is designed for college students, freshers, entrepreneurs and working professionals.

Course Duration:

The course will have a duration of 8 weeks, with sessions conducted each week. Each session is recorded and uploaded on the student portal, so students who missed the sessions can go through them.

Teaching Approach:

At Digital Regenesys we believe in a holistic teaching approach, where each student will learn real world skills and create their own networks of professionals. You'll get to learn this from our expert faculty.

Value For Money:

Each student will have 1 year of unlimited access to the learning portal. Interactive sessions with industry experts will be conducted. And career counselling will be provided to students after the completion of the course.

Cybersecurity

This course will give you an exploration of the various real-life applications of Cyber Security. This Certificate Programme in Cyber Security is designed to give learners a unique opportunity of learning both academic concepts & industry relevant skills in a single program. This program helps you network with Regenesys Global Faculties, industry experts, and fellow professionals, and helps you get on the career track you aspire for.

MODULE 01: WEEK 01

- Introductory fundamentals of cyber security threat actors, attacks, and mitigation
- Cyber security fundamentals
- Security policies and procedures
- Cyber security mitigation methods
- Cia triad

MODULE 02: WEEK 02

- Enterprise Architecture
- Organizational security policy and components
- Internet & networking basics
- Introduction to secured architecture
- Wireless networks
- Network security controls
- Cloud Virtualization
- Byod, and iot security testing

MODULE 03: WEEK 03

- Information system governance and risk assessment
- Introduction to information security
- Governance risk
- Management information security programs
- Network security and spoofing

Cybersecurity

MODULE 04: WEEK 04

- Developing an incident management and response System
- Digital forensics business
- Continuity and disaster recovery
- Wi-Fi network security
- Web security

MODULE 05: WEEK 05

- Cryptography and encryption
- Cryptanalysis
- Malware analysis, Memory forensics
- Cyber forensic
- Application security
- Hands-on security - Network traffic analysis + CTF + VAPT

MODULE 06: WEEK 06

- Introduction to application security
- Web-based applications and associated vulnerabilities
- Cookies and tracking
- Data and database security
- Phishing and other attacks on identity
- Regulation, compliance, and risk management

MODULE 07: WEEK 07

- Introduction to Ethical Hacking –
- Overview of information security, threats, attack vectors, ethical hacking concepts.
- Information security controls
- Penetration testing concepts, and information security laws and standards
- Footprinting and Reconnaissance

Cybersecurity

MODULE 08: WEEK 08

- Session by industry experts
- Session on work readiness skills

Educational Objectives:

The educational objectives of the program are:

- To prepare learners with the technical knowledge and skills needed to protect and defend computer systems and networks.

- To develop learners that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.

- To develop learners that can identify, analyze, and remediate computer security breaches.

List of Cybersecurity Practicals

EXPERIMENT-1

Aim: To study the steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.

Learning Objective:
At the end of the session you will be able to

» Become familiar with how to operate the user account.
» Different types of user accounts and their options.
» How to protect your system with password.

EXPERIMENT-2

To study the steps to protect a Microsoft Word Document of different version with different operating system.

Learning Objective:
At the end of the session you will be able to

» Understand how to protect a Microsoft word document.
» Be familiar with how to password protect Microsoft word document in different type of operating system.

EXPERIMENT-3

Aim: To study the steps to remove Passwords from Microsoft Word.

Learning Objective:
At the end of the session you will be able to be familiar with

» To understand the steps of operation how to remove password from Microsoft Word.

EXPERIMENT-4

Aim: To study various methods of protecting and securing databases.

Learning Objective
After going through this unit, you will be able to:

- » Be familiar with any database environment like MySQL or Oracle etc.
- » Know different techniques of protecting a database.
- » Note the security majors to protect the database.

EXPERIMENT-5

Aim: To study "How to make strong passwords" and "passwords cracking techniques".

Learning Objective
After going through this unit, you will be able to:

- » Generate secure passwords
- » Apply password manager to generate secure password
- » Point out various features of different password managers
- » How to protect your system with password.

EXPERIMENT-6

Aim: To study the steps to hack a strong password.

Learning Objective
At the end of the session you will be able to

- » Know how to hack a simple or a strong password.
- » Know the different types of hacking process and type of applications.

EXPERIMENT-7

AIM: To encrypt and decrypt the given message by using Ceaser Cipher encryption algorithm.

Learning Objective
At the end of the session you will be able to
» Encrypt the given message by using Ceaser Cipher
» Decrypt the given message by using Ceaser Cipher

EXPERIMENT-8

AIM: To implement a program to encrypt a plain text and decrypt a cypher text using play fair Cipher Substitution Techniques

Learning Objective
At the end of the session you will be able to
» Be familiar with any database environment like MySQL or Oracle etc.
» Know different techniques of protecting a database.
» Note the security majors to protect the database.

EXPERIMENT-9

AIM: To implement a program for encryption and decryption using Vigenere Cipher Substitution Techniques

Learning Objective
At the end of the session you will be able to
» Implement Encryption using Vigenere Substitution Techniques
» Implement Decryption using Vigenere Substitution Techniques

EXPERIMENT-10

AIM: To implement a program for encryption and decryption using Rail Fence Cipher Transposition Technique

Learning Objective
At the end of the session you will be able to

- Encrypt a plain text into equivalent cypher text using Rail Fence Cipher Transposition Technique
- Decrypt a plain cypher text into equivalent plain text using Rail Fence Cipher Transposition Technique

EXPERIMENT-11

AIM: To implement RSA (Rivest–Shamir–Adleman) algorithm by using HTML and Javascript.

Learning Objective
At the end of the session you will be able to

- Learn Public Key and Private Key
- Distinguish between Public Key and Private Key.

EXPERIMENT-12

AIM: To implement the Diffie-Hellman Key Exchange algorithm for a given problem.

Learning Objective
At the end of the session you will be able to

- Establish a shared secret that can be used for secret communications while exchanging data over a public network.

EXPERIMENT-13

AIM:To build a Trojan and know the harmness of the trojan malwares in a computer system.

Learning Objective
At the end of the session you will be able to

- Create a simple trojan by using Windows Batch File
- Understand Ransomware attacks.

Cybersecurity

Job Profiles

- » Security Analyst/Manager
- » Security Architect
- » Security Auditor
- » Cryptographer
- » Forensic Expert
- » Security Specialist
- » Incident Responder
- » Penetration Tester
- » Security Engineer
- » Source Code Auditor

Program Learning Outcomes

Upon completion of the program, learners will be able to:

- Analyze and evaluate the Cybersecurity needs of an individual and organization.
- Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure.
- Conduct a Cybersecurity risk assessment.
- Measure the performance and troubleshoot Cybersecurity systems.
- Implement Cybersecurity solutions.
- Identify the key Cybersecurity vendors in the marketplace.
- Identify security architecture for an organization.
- Design operational and strategic Cybersecurity strategies and policies
- Identify, test and evaluate secure software.
- Develop policies and procedures to manage enterprise security risks.
- Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training.
- Interpret and forensically investigate security incidents.
- Impact Cybersecurity risk in an Ethical, Social, and Professional Manner.

Tools Covered

Not only restricted to

Cain and Abel	NICE FRAMEWORK	TrueCrypt	Paros	WIRESHARK
NetStumbler	Nikto	OWASP	SIEM	AIRCRACK-NG
nexpose	NMAP	KeePass	Tor	splunk>

and many more..

Key Features

Course designed by doctorate faculty	1 year of unlimited access to the learning portal	Capstone projects
Interaction with industry experts	Course completion certificate	Career counselling (Profile Building, Assessment Tests, Mock Interviews)

CYBER
CRIME

Contact Us

Head Office
South Africa Campus

165 West Street, Sandton
Johannesburg, South Africa.

☎ +27 (11) 669 5000

🌐 www.regenesys.net

Nigeria Campus

8th Floor, Churchgate Tower 2
PC 31, Victoria Island,
Lagos, Nigeria.

☎ +234 (1) 453 0959

🌐 www.nigeria.regenesys.net

India Campus

Proxima Building, Unit 1101,
11th Floor, Plot 19, Sector 30A, Vashi,
Navi Mumbai, India. 400705

☎ 1800 212 9950

🌐 www.india.regenesys.net