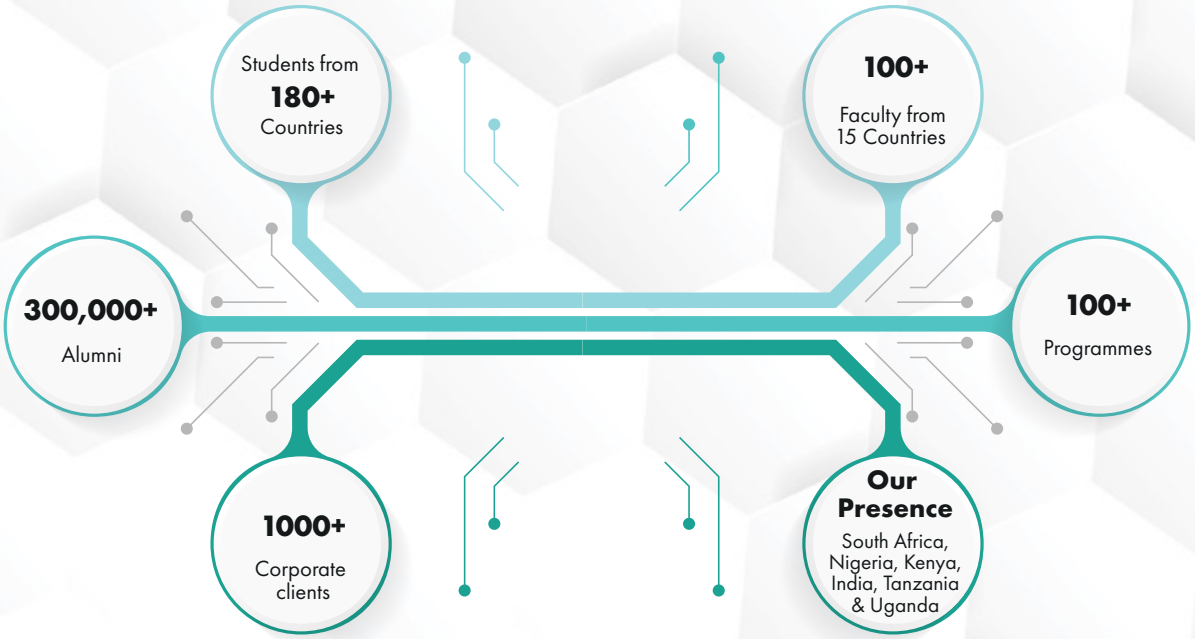
DIGITAL REGENESYS
Awakening Potential

COMPLETE CYBERSECURITY SOLUTION

- **Cybersecurity Fundamentals:**
  Building a Secure Online Presence
- **Cyber Defence Toolbox:**
  Essential Tools and Techniques

ABOUT REGENESYS



OUR CLIENTELE

Mercedes-Benz · Microsoft · DANONE · BMW

Standard Bank · SAMSUNG · BARCLAYS · intel

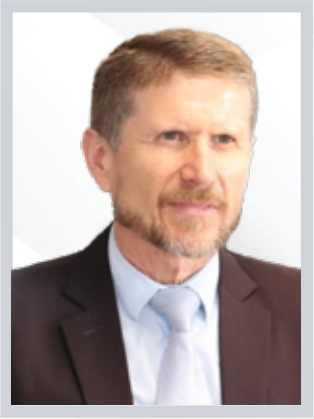
NEDBANK · ANGLO AMERICAN · sasol · Coca-Cola

momentum · LIBERTY · absa · MTN

Massmart + Walmart · THE PRESIDENCY

And 1000+ Organisations...

Chairman's Message



I am delighted to welcome you to Digital Regenesys, part of the Regenesys Group. 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 education institute with presence in South Africa, India, Nigeria, Kenya, Tanzania, Croatia & Uganda, delivering cutting-edge online and contact learning programmes. Over the past 25 years, Regenesys has educated more than 300,000 students from 180+ 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 Fundamentals

Building a Secure Online Presence

DURATION
2.5 MONTHS

Course Description:

Internet safety and privacy are more critical than ever. With corporations holding vast amounts of sensitive data, protecting it from external threats is paramount. This has led to a growing demand for cybersecurity professionals. Elevate your skills with a Cybersecurity program, designed to meet this high demand, improve business outcomes, and offer exceptional global career opportunities.

Target Group:

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

Course Duration:

The course will last for 8 weeks, with sessions conducted every 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 a network of professionals. Students will get to study from our expert faculty.

Value For Money:

Each student will have 3 years of unlimited access to the learning portal. Interactive sessions with industry experts will be conducted, and career counselling will be provided to students after completing the course.

Course Content

This course provides an in-depth exploration of real-life applications of cybersecurity. Our certificate program in Cybersecurity offers a unique blend of academic concepts and industry-relevant skills within a single curriculum. Additionally, the program facilitates networking with Regenesys global faculty, industry experts, and fellow professionals, helping you chart the career path you aspire to.

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
- Organisational security policy and components
- Internet & networking basics
- Introduction to secured architecture
- Wireless networks
- Network security controls
- Cloud virtualisation
- BYOD and IOT security testing

MODULE 03: WEEK 03

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

MODULE 04: WEEK 04

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

MODULE 05: WEEK 05

- Cryptography and Encryption
- Cryptanalysis
- Malware analysis, memory forensics
- Cyber forensic
- Application security

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, and ethical hacking concepts
- Information security controls
- Penetration testing concepts and information security laws and standards
- Footprinting and Reconnaissance

MODULE 08: WEEK 08

- Session by industry experts
- Session on work readiness skills

EDUCATIONAL OBJECTIVES:

The educational objectives of the programme 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, analyse, and remediate computer security breaches

List of Cybersecurity Practicals

EXPERIMENT 1

Aim: To study the steps to protect your computer system by creating user accounts with passwords and types of user accounts for safety and security.

Learning Objectives:

By the end of the session, you will be able to

- Become familiar with how to operate the user account
- Know different types of user accounts and their options
- Learn how to protect your system with a password

EXPERIMENT 2

Aim: To study the steps to protect a Microsoft Word Document of different versions with different operating systems.

Learning Objectives:

By 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 PowerPoint in different types of operating systems

EXPERIMENT 3

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

Learning Objective:

By the end of the session, you will be able to

- Understand how to remove passwords from Microsoft Word

EXPERIMENT 4

Aim: To study the steps to protect Microsoft PowerPoint files in a different type of operating system.

Learning Objectives:

By the end of the session, you will be able to

- Understand how to protect Microsoft PowerPoint files
- Be familiar with how to password protect Microsoft PowerPoint in a different operating system

EXPERIMENT 5

Aim: To study the steps to remove passwords from Microsoft PowerPoint.

Learning Objective:

By the end of the session, you will be able to

- Understand the steps to remove passwords from Microsoft PowerPoint

EXPERIMENT 6

Aim: To study the steps to protect Microsoft Excel files in a different type of operating system.

Learning Objectives:

By the end of the session, you will be able to

- Understand how to protect Microsoft Excel files
- Be familiar with how to password protect Microsoft Excel in different operating systems

EXPERIMENT 7

Aim: To study the steps to remove passwords from Microsoft Excel.

Learning Objective:

By the end of the session, you will be able to

- Understand the steps to remove passwords from Microsoft Excel

EXPERIMENT 8

Aim: To study the concepts of Python programming with the help of a few basic programmes.

Learning Objectives:

By the end of the session, you will be familiar with basic concepts and programmes in Python like

- Understand basic concepts and programmes in python
- Using arithmetic operators in Python
- Understanding control structures like if-else statements and loops in Python
- Using functions in Python

Participants will gain a basic understanding of Python programming and will be able to write simple programmes using the concepts covered in the session. In addition, this will serve as a foundation for further learning and development in Python programming.

EXPERIMENT 9

Aim: To study the concepts of HTML with the help of a few basic programmes.

Learning Objectives:

By the end of the session, you will be able to

- Understanding the structure and syntax of HTML
- Creating basic HTML elements like headings, paragraphs, and links
- Understanding the concept of HTML tags and attributes
- Creating tables and forms in HTML
- Understanding the basics of Cascading Style Sheets (CSS) for styling HTML pages
- Implementing multimedia elements like images and videos in HTML

Participants will gain a basic understanding of HTML and will be able to create simple web pages using the concepts covered in the session. This will serve as a foundation for further learning and development in the field of web development.

EXPERIMENT 10

Aim: To study the concepts of JavaScript with the help of a few basic programmes.

Learning Objectives:

By the end of the session, you will be familiar with basic concepts and programmes in JavaScript like:

- Understanding the fundamentals of JavaScript
- Understanding variables and data types in JavaScript
- Using arithmetic, comparison and logical operators in JavaScript
- Understanding control structures like if-else statements and loops in JavaScript
- Using functions and objects in JavaScript

Participants will gain a basic understanding of JavaScript and will be able to write simple programmes using the concepts covered in the session. This will serve as a foundation for further learning and development in the field of web development.

EXPERIMENT 11

Aim: To encrypt and decrypt the given message by using the Caesar Cipher encryption algorithm.

Learning Objectives:

By the end of the session, you will

- Encrypt the given message by using Caesar Cipher
- Decrypt the given message by using Caesar Cipher

EXPERIMENT 12

Aim: To implement a programme to encrypt plain text and decrypt cypher text using play fair Cipher Substitution Techniques.

Learning Objectives:

By the end of the session, you will be able to

- Encrypt a plain text into equivalent cypher text using play fair Cipher Substitution Techniques
- Decrypt a plain cypher text into equivalent plain text using play fair Cipher Substitution Techniques

EXPERIMENT 13

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

Learning Objectives:

By the end of the session, you will be able to

- Be familiar with any database environment like MySQL, etc
- Know different techniques for protecting a database
- Note the security majors to protect the database

EXPERIMENT 14

Aim: To study how to make strong passwords and password cracking techniques.

Learning Objectives:

By the end of the session, you will be able to

- Generate secure passwords
- Apply password manager to generate secure passwords
- Point out various features of different password managers

EXPERIMENT 15

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

Learning Objectives:

By 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 processes and types of applications

EXPERIMENT 16

Aim: To implement RSA (Rivest–Shamir–Adleman) algorithm using HTML and JavaScript.

Learning Objectives:

By the end of the session, you will be able to

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

EXPERIMENT 17

Aim: To build a Trojan and know the harm of the Trojan malware in a computer system.

Learning Objectives:

By the end of the session, you will be able to

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

EXPERIMENT 18

Aim: Study of Linux basic commands

Learning Objectives:

By the end of the session, you will be able to

- Know how to access the folders and files in command line
- Familiar with the command lines

EXPERIMENT 19

Aim: To study hashing techniques and checking the integrity

Learning Objectives:

By the end of the session, you will be able to

- Learn how to take hash value using different hashing techniques
- Find the integrity of the files and folders

JOB PROFILES

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

Programme Learning Outcomes

Upon completion of the programme, you will be able to:

- Analyse and evaluate the cyber security needs of an individual and organisation
- Analyse and resolve security issues in networks and computer systems to secure IT infrastructure
- Conduct a cyber-security risk assessment
- Measure the performance and troubleshoot cyber security systems
- Implement cyber security solutions
- Identify the key cyber security vendors in the marketplace
- Identify security architecture for an organisation
- Design operational and strategic cyber security 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, emphasising ethics, social engineering vulnerabilities and training
- Interpret and forensically investigate security incidents
- Impact Cyber Security risk in an ethical, social, and professional manner

Defence Toolbox

DURATION 2 MONTHS

Essential Tools and Techniques

Email Forensics:

Email forensics involves the process of collecting, analysing, and interpreting electronic mail messages and metadata as evidence in legal or investigative matters.

The key steps in email forensics include:

- The key steps in email forensics include identification, collection, analysis, interpretation, and reporting.
- It is an essential tool for investigating criminal or fraudulent activities, data breaches, harassment, or other workplace violations involving email messages.

By following a systematic and rigorous process, email forensic experts can uncover evidence that can be used in court or to improve the security posture of an organisation.

John The Ripper:

John the Ripper is a popular open-source password cracking tool that is commonly used by security professionals and hackers alike. It was originally developed for Unix-based systems but has since been ported to a variety of platforms, including Windows and MacOS. The tool uses a various attack methods to crack passwords, including dictionary attacks, brute-force attacks, and hybrid attacks.

- John the Ripper can leverage various types of password cracking techniques, such as rainbow tables, which can greatly increase its speed and efficiency.
- One of the key features of John the Ripper is its ability to detect weak passwords and provide recommendations for stronger ones.
- It can also be used to audit password policies and identify vulnerabilities in systems and applications.

KeePass:

KeePass is a popular open-source password manager that allows users to store and manage their passwords in a secure and organised manner. It is available for Windows, MacOS, Linux, and mobile platforms. The tool uses strong encryption algorithms to protect users' passwords, ensuring that they are secure even in the event of a data breach. KeePass also offers several additional security features, such as two-factor authentication, a master password, ability to lock the database after a set period of inactivity.

KeePass allows users to store various types of information, including usernames, passwords, and website URLs. In addition, users can create custom fields to store additional information, such as security questions and answers.

- One of the key advantages of KeePass is its flexibility and customisation options.
- Users can create and manage multiple password databases, each with its own unique settings and password requirements.
- The tool also offers a range of plugins and integrations that allow users to customise their experience even further.

Overall, KeePass is a powerful and secure password manager that provides users with an easy way to manage their passwords and keep them safe from cyber threats.

VeraCrypt:

VeraCrypt is a popular open-source disk encryption tool that allows users to encrypt and protect their data stored on a computer or external drive. It is available for Windows, MacOS, and Linux. The tool uses strong encryption algorithms such as AES, Serpent, and Twofish to ensure that users' data is secure from unauthorised access, theft, and hacking attempts.

VeraCrypt also offers several advanced security features, such as

- Hidden volumes,
- Deniable encryption, and
- Keyfile support, which provides users with added protection against brute-force attacks and other types of threats.

VeraCrypt can be used to encrypt an entire hard drive, a partition, or a removable storage device such as a USB drive. Overall, VeraCrypt is a powerful and reliable encryption tool that provides users with robust protection for their data.

Burpsuite:

Burp Suite is a popular web application security testing tool used by security professionals, ethical hackers, and penetration testers. It is designed to identify vulnerabilities and security issues in web applications, including Cross-Site Scripting (XSS), SQL injection, and session hijacking. Burp Suite offers a range of features and tools to help users identify and exploit vulnerabilities in web applications.

- Its proxy server intercepts all web traffic, allowing users to inspect and modify HTTP requests and responses.
- Its scanner identifies common web application vulnerabilities and provides detailed reports and recommendations for remediation.
- In addition to its scanning and proxy features, Burp Suite also offers a range of tools for advanced penetration testing and vulnerability research, including a repeater, intruder, and sequencer.
- It offers a wide range of plugins and extensions, allowing users to tailor the tool to their specific needs and preferences.
- It also provides integration with other tools and platforms, including popular vulnerability scanners and security frameworks.

Overall, Burp Suite is a powerful and comprehensive web application security testing tool that provides users with a range of features and tools to identify and remediate vulnerabilities in web applications.

Nikto:

Nikto is an open-source web server scanner that helps security professionals identify and remediate vulnerabilities in web servers and applications. It is designed to test web servers for common vulnerabilities, such as outdated software versions, misconfigured server settings, and known vulnerabilities. In addition, Nikto offers a range of features and tools to help users identify and exploit vulnerabilities in web servers.

- It can scan multiple web servers simultaneously, allowing users to identify vulnerabilities across their entire infrastructure.
- It also provides detailed reports on the vulnerabilities it finds, including recommendations for remediation.
- It offers a simple and intuitive interface allowing users to configure and run scans quickly and easily.
- It also provides detailed documentation and tutorials to help users get started and make the most of its features.
- In addition to its scanning features, Nikto offers a range of customisation options and plugins, allowing users to tailor the tool to their specific needs and preferences.

- It also integrates with other security tools and platforms, making it a valuable addition to any security toolkit.

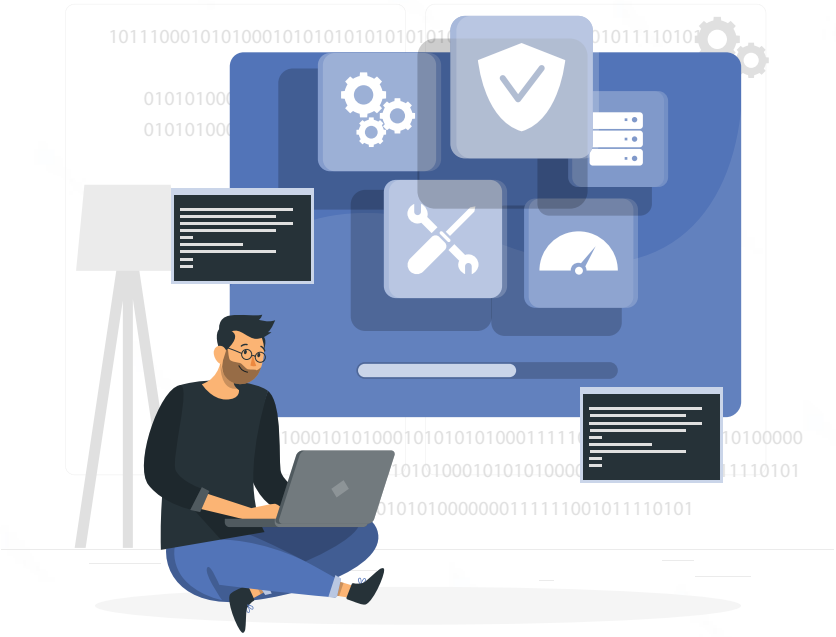
Overall, Nikto is a powerful and comprehensive web server scanner that provides users with a range of features and tools to identify and remediate vulnerabilities in web servers and applications.

OWASP:

OWASP (Open Web Application Security Project) is a non-profit organisation dedicated to improving the security of software and web applications. It is a community-driven organisation providing tools, resources, and guidelines to help developers and security professionals build secure applications and protect against common web application vulnerabilities. OWASP offers a range of resources and tools to help organisations improve their application security posture.

- Its flagship project, the OWASP Top 10, identifies the top 10 most critical web application security risks, including injection attacks, cross-site scripting, broken authentication and session management.
- The organisation also offers a range of guides, tools, and best practices to help developers and security professionals mitigate these risks and protect their applications.
- In addition to its educational and awareness-raising efforts, OWASP also supports a number of software security projects, including web application security scanners, vulnerability scanners, and security testing frameworks
- These projects are open source and community-driven, providing users with free and reliable security tools that can help them improve their security posture.

Overall, OWASP is a valuable resource for developers and security professionals looking to improve the security of their software and web applications.



Wireshark:

Wireshark is a popular open-source network protocol analyser that allows users to capture and analyse network traffic in real-time. It is used by security professionals, network administrators, and developers to troubleshoot network issues, identify security threats, and optimise network performance.

- Wireshark offers a range of features and tools to help users analyse network traffic
- Ethernet, Wi-Fi, and Bluetooth are just a few of the network interfaces whose traffic its packet capture engine may record.
- It can decode and analyse a wide range of network protocols, including TCP/IP, HTTP, DNS, and SSL/TLS. It also offers a powerful filtering engine, allowing users to focus on specific packets or protocols of interest.
- Additionally, it offers integration with other tools and platforms, such as network vulnerability scanners and intrusion detection systems.
- Wireshark includes a variety of statistics and visualisation tools alongside its packet analysis features to aid users in understanding network traffic patterns and optimising network efficiency.
- Its powerful scripting engine allows users to automate and customise their analysis, making it more efficient and effective.

One of the key advantages of Wireshark is its versatility and customisation options. Overall, Wireshark is a powerful and comprehensive network protocol analyser that provides users with a range of features and tools to analyse network traffic, identify security threats, and optimise network performance.

Nmap:

Nmap (Network Mapper) is a popular open-source network scanning tool that allows users to discover hosts and services on a network, identify security vulnerabilities, and map network architecture. It is used by security professionals, network administrators, and developers to secure their networks and optimise network performance.

Its powerful scanning engine can detect hosts and services on a wide range of network protocols, including TCP, UDP, and ICMP. It can also perform a range of scanning techniques, including ping scans, port scans, and OS detection. One of the key advantages of Nmap is its versatility and customisation options.

- It offers a wide range of scanning options and configuration parameters, allowing users to tailor the tool to their specific needs and preferences.
- It also provides integration with other tools and platforms, including network vulnerability scanners and intrusion detection systems.
- In addition to its scanning features, Nmap also offers a range of scripting and automation options, allowing users to automate their scanning and analysis tasks and integrate with other tools and platforms.
- Its powerful reporting engine allows users to generate detailed reports on their network scans and analysis, making identifying and remediating security vulnerabilities easier.

Overall, Nmap is a powerful and comprehensive network scanning tool that provides users with a range of features and tools to discover hosts and services on a network, identify security vulnerabilities, and map network architecture.

inSSIDer

inSSIDer is a popular Windows-based wireless network scanner that allows users to discover and analyse wireless networks in their vicinity. It is used by security professionals, network administrators, and wireless network enthusiasts to troubleshoot wireless network issues, optimise wireless network performance, and identify security vulnerabilities. inSSIDer offers a range of features and tools to help users analyse wireless networks.

- Its wireless network scanner can detect and display information on wireless networks, including inSSIDer, signal strength, encryption type, and channel.
- It can also perform a range of scanning techniques, including active scanning, passive scanning, and war driving.
- One of the key advantages of inSSIDer is its ease of use and user-friendly interface.
- It provides clear and concise information on wireless networks, making it easy for users to understand and analyse their wireless network environment.
- Additionally, a variety of customisation options are provided, enabling users to tailor the tool to meet their specific needs and preferences.
- inSSIDer includes a variety of statistics and visualisation tools as well to its scanning features that help users in comprehend wireless network traffic patterns and enhance network efficiency.

Overall, inSSIDer is a powerful and comprehensive wireless network scanner that provides users with a range of features and tools to analyse wireless networks, troubleshoot network issues, and optimise network performance.

Tor:

Tor (The Onion Router) is a free and open-source network protocol that allows users to browse the internet anonymously. It is used by individuals and organisations to protect their privacy, avoid censorship and surveillance, and access content that may be restricted in their location. Tor works by routing internet traffic through a network of volunteer-operated servers known as nodes or relays. Each relay in the network only knows the IP address of the previous and next relays in the chain, creating multiple layers of encryption and making it difficult for anyone to trace the source of the traffic.

- One of the key advantages of Tor is its ability to protect user privacy & anonymity.
- By encrypting internet traffic and routing it through multiple relays, Tor makes it difficult for anyone to monitor or track user activity.
- It also allows users to access content that may be blocked or censored in their location, such as social media, news sites, and messaging apps.
- In addition to its anonymity features, Tor also offers a range of security and privacy tools, including a built-in web browser, support for end-to-end encryption, and protection against common internet threats, such as malware and phishing attacks.

Overall, Tor is a powerful and versatile tool that provides users with a range of features and tools to protect their privacy and security online.

Splunk:

Splunk is a powerful and versatile data analysis platform used by organisations to collect, analyse, and visualise large amounts of machine-generated data in real-time. It is used by security professionals, IT administrators, and business analysts to gain insights into their systems, applications, and processes and to detect and remediate security threats and performance issues. One of the key advantages of Splunk is its ability to collect and analyse data from a wide range of sources, including servers, applications, network devices, and security systems.

- It provides a centralised platform for organisations to monitor and analyse data in real-time, making it easier to detect and remediate issues as they arise.
- Splunk also offers a range of advanced analytics and visualisation tools, allowing users to gain insights into their data and identify trends and patterns.
- Its machine learning and artificial intelligence capabilities enable it to identify anomalies and threats automatically, making it easier for organisations to detect and respond to security threats quickly.
- In addition to its data analysis and visualisation features, Splunk also offers a range of integration options, allowing users to integrate with other tools and platforms, such as security information and event management (SIEM) systems, cloud platforms, and IT service management (ITSM) tools. This makes it easier for organisations to streamline their operations and improve their overall security posture.

Overall, Splunk is a powerful and comprehensive data analysis platform that provides organisations with a range of features and tools to monitor and analyse their systems, applications, and processes.

Wazuh – SIEM:

Wazuh is an open-source security information and event management (SIEM) platform that provides organisations with a comprehensive set of tools to monitor and analyse security events across their network. It is used by security professionals and IT administrators to detect and respond to security threats in real-time and to improve the overall security posture of their organisation. One of the key advantages of Wazuh is its ability to collect, monitor, and analyse security events from a wide range of sources, including servers, network devices, and cloud platforms.

- Wazuh offers a range of compliance and regulatory compliance features, allowing organisations to monitor and enforce security policies and regulatory requirements, such as PCI DSS, HIPAA, and GDPR.
- Its powerful reporting and visualisation tools allow organisations to generate detailed reports on security events and compliance status, making it easier to demonstrate compliance to auditors and stakeholders.
- In addition to its SIEM features, Wazuh also offers a range of intrusion detection and prevention (IDS/IPS) capabilities, allowing organisations to detect and respond to known and unknown threats in real-time.
- Its integration options with other security tools and platforms, such as endpoint detection and response (EDR) tools and vulnerability scanners, make it easier for organisations to streamline their security operations and improve their overall security posture.

Overall, Wazuh is a comprehensive and powerful open-source SIEM platform that provides organisations with a range of features and tools to monitor and analyse security events across their network.

Tools Covered

many more...

KEY FEATURES

Course designed by doctorate faculty

3 years of unlimited access to the learning portal

Capstone projects

Interaction with industry experts

Course completion certificate

Career counselling (Profile Building, Assessment Tests, Mock Interviews)

Contact Us

SOUTH AFRICA

165 West Street, Sandton
Johannesburg, South Africa.

NIGERIA

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

KENYA

1203, 12th Floor, GTC Office Tower
Intersection of Waiyaki Way,
Chiromo Ln, Nairobi, Kenya

INDIA

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

TANZANIA

G11 Ground Floor,
Kwik Spaces, 1040 Haile Selassie Road,
Masaki Dar es Salaam, 16572

UGANDA

Arie Tower, 6th floor,
16 Mackinnon Rd, Kampala,
Uganda

www.digitalregenesys.com

@digital_regenesys @digitalregenesys @digital-regenesys