al-nafi
EDUCATION BENEFITS ALL

Diploma in Cloud Cyber Security

Al Razzaq Program
Included in Al Razzaq Program
Included in Al Razzaq Program

Pearson

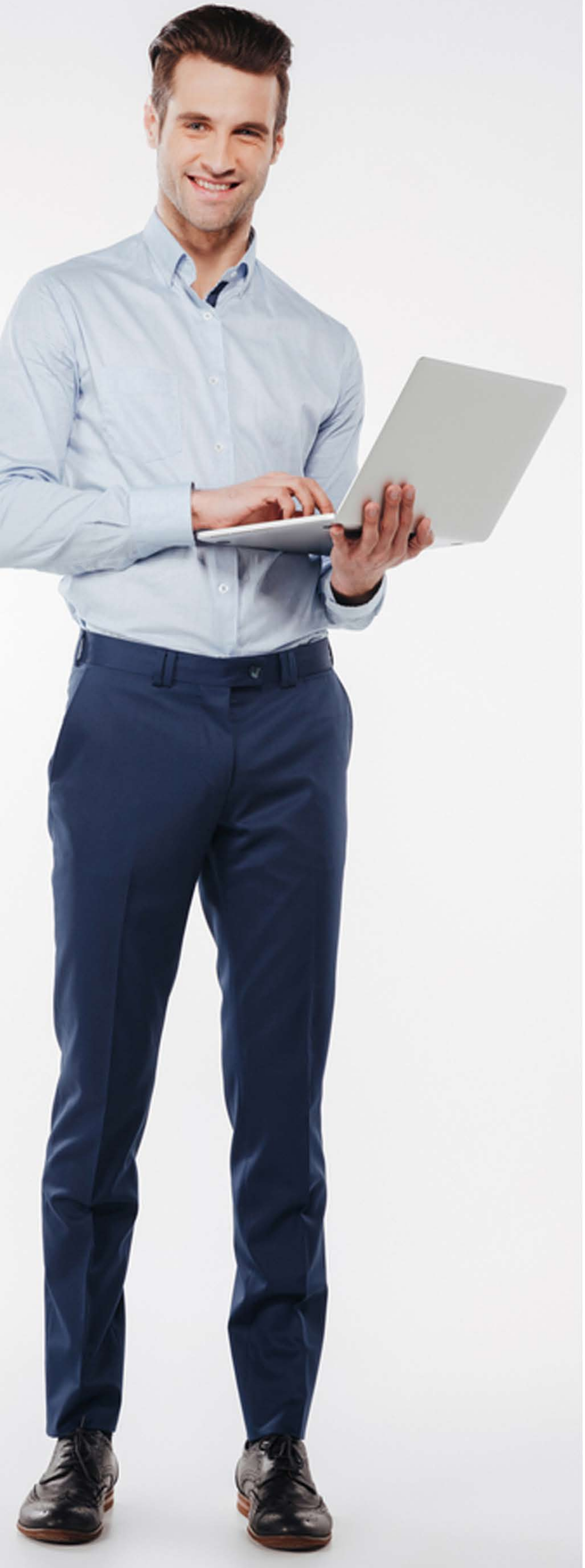
Endorsed by EduQual UK

ISACA Accredited Partner

EADL European Association for Distance Learning

Table of Contents

Table of Contents



About the Diploma

Our Cloud Cyber Security Diploma, a Level 3 course accredited by EduQual, focuses on teaching learners the job description of emerging sciences skills for various multidisciplinary industries. It offers hands-on training in areas such as cyber defense, SCADA, offensive pentesting, digital forensics, data science, security information management, statistics, and Emaths, along with LinkedIn networking and IELTS and SELT test preparation.

Using open-source, vendor-neutral content, the course emphasizes employability and provides learners with recorded videos, hands-on practice, proprietary cloud labs, and assignments. Hands-on Practice involves step-by-step instructions and trainer interaction through communities, forums, and live classes.

The diploma develops practical skills and problem-solving abilities, preparing learners for global jobs in Cyber Security, Offensive Security, SCADA/ICS, Data Science, and Cloud Computing within 6-9 months, allowing for national or global career mobility.

Unlock Al Razzaq Program Opportunities

Learners who pass the EduQual exam and complete their internship can enrol in the Al Razzaq Program, an augmentation program offering additional professional growth prospects. Moreover, our company actively endorses these learners when applying for Fortune 500 and global job positions, highlighting the invaluable achievements and skills acquired during the internship Program.

To qualify for Al Razzaq Program, you must meet any 1 of the 4 criteria mentioned below:

Yearly Bundle:

Students enrolled in the Yearly bundle are automatically eligible for the Al Razzaq Program without any additional conditions.

Monthly Bundle:

Students enrolled in the Monthly bundle become eligible for the Al Razzaq Program after they have paid the monthly fees for a total of 12 consecutive months.

Half-Yearly Bundle

Students enrolled in the Half-Yearly Bundle qualify for the Al Razzaq Program once they have successfully paid the fees for two consecutive half-year terms.

Quarterly Bundle:

Students enrolled in the Quarterly Bundle are eligible for the Al Razzaq Program after they have paid the fees for four consecutive quarters.

Key Features of the Diploma

EduQual Globally Recognized Certificate

300+ hands-on cloud labs

Self-paced learning
5000+ hands-on projects

Job description learning

8X higher live interaction with live online classes by Industry experts

Student Communities

Resume building

Interview Preparation

Internship Program

Global Undergraduate program eligibility

Gain full expertise in Cloud Environments with Cloud Playground's on-demand servers and specialized containers for labs

Al Razzaq Program

About the Diploma Program Accredited by EduQual

The EduQual-accredited Cloud Cyber Security Diploma is a valuable credential for those pursuing careers in cloud computing and cybersecurity. EduQual, an internationally renowned awarding organization, offers high-quality qualifications acknowledged by employers and educational institutions globally. The Cloud Cyber Security Diploma's accreditation signifies that the program adheres to stringent quality standards and equips students to safeguard cloud systems against cyber threats. This diploma is an outstanding choice for individuals aiming to enhance their cybersecurity skills and boost their career prospects in a rapidly evolving field. Additionally, as the diploma aligns with Level 3 , graduates may qualify for undergraduate program admission upon course completion.

Upon completion of this diploma program, you will:

- Receive a Certificate from EduQual after completion of the diploma program.
- Eligible for Al Nafi Alumni membership

About Al Nafi

Al Nafi, the leading global e-Learning platform, offers rigorous and specialized training in emerging technologies and processes shaping the digital landscape. With a cost-effective, self-paced learning and time-efficient approach, we have served more than 300,000 learners, with numerous alumni excelling in Fortune 500 companies worldwide.
Our customized programs are designed to help both individuals and organizations achieve their career and business objectives.

Program Eligibility Criteria and Application Process

To apply for the Cloud Cyber Security Diploma at Eduqual Level 3, individuals who are interested will need to register for the diploma through the website. The provided link www.alnafi.com/cloud cyber security can be used by learners to complete their application.

Eligibility Criteria

To enrol in the Cloud Cyber Security Diploma at Eduqual Level 3, there are no specific courses or academic prerequisites required. However, candidates must possess the following:

- A laptop or desktop computer that is in good working order
- A dependable internet connection
- Proficiency in using the internet and the ability to troubleshoot internet-related issues.

Application Process

After selecting the preferred payment plan, learners can begin their studies with ease as the application process comprises of only three straightforward steps.

STEP 1
CHOOSE THE PAYMENT PLAN AND TYPE

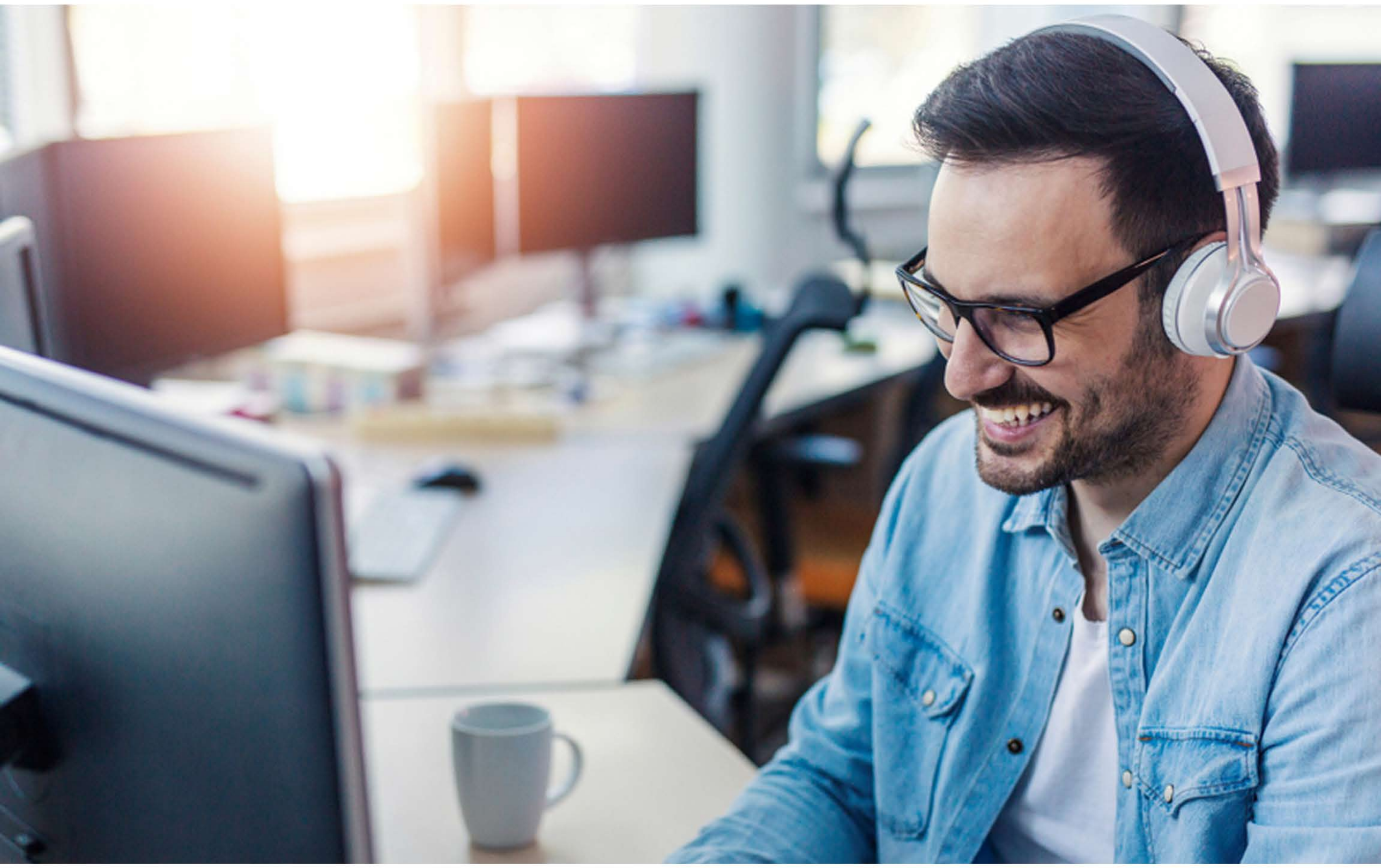
Fill out the application form and choose your preferred payment plan, which includes options for monthly, quarterly, half-yearly, and annual payments.

STEP 2
SUBMIT THE APPLICATION PROCESS

With just one click, submit your application once you have chosen the payment method and plan.

STEP 3
ADMISSION

Once your payment method and plan have been verified, immediately begin your studies.



Connect with the Support Operations Center

Our dedicated support team is here to assist you with any questions or concerns you may have regarding the application process and related matters, 24/7. They can help you with inquiries regarding

- The application
- Provide information on the interest-free student loan (if applicable)
- Clarify any confusion you have about the diploma program.

Program Outcomes

Learn basic differential calculus or optimization and gradient descent algorithms. (Calculus for Emerging Pathways)

Learn industry standards & best practices by studying cryptography, network security, risk mgmt, software dev security & access control systems (Certified Information System Security Professional CISSP)

Gain knowledge on CIS security controls for protecting systems & data against cyber attacks. Learn to defend against pressing cyber threats (CIS Top 20 Controls)

Develop cybersecurity skills through evaluation & interpretation using the latest principles & methodologies. Focus on risk mgmt, security arch, incident mgmt, & access control. (Cyber Security Essentials Revisit after CISSP)

Learn to create dashboards, visualize data, custom viz & use ML for pattern identification in hands-on exercises & labs (Elasticsearch for Data Science and Analytics with Kibana)

Learn to use ElasticSearch for security ops and incident response through hands-on training and real-world scenarios (Elasticsearch SOC Engineer)

Discover how to gather and store log, metric, uptime & APM data in Elasticsearch for improved system observability, stability, and high availability (Elasticsearch Threat Hunting and Observability Engineer)

Enhance security skills, identify and respond to cyber threats, and incident response training (Hacking 101 AKA ethical hacking and incident response management)

Prepare for the IELTS exam through reading, writing, listening & speaking activities (IELTS Academic and General Training)

Learn international security standards, implement & assess security systems, and focus on assessments & audits (ISO 27001, 27017, 27018, Lead Implementer & Auditor)

Gain a comprehensive knowledge of Python in data science through hands-on practice & real-world projects(Learn Data Science Using Python)

Learn Linear Algebra through concepts, techniques, intuition, math, & procedure (Linear Algebra for Emerging Pathways)

Empower Emerging Tech learners to secure job/freelance opportunities via effective LinkedIn use (LinkedIn Course for Job Seekers)

Learn Linux OS for task automation & problem-solving. Study config, software install, file/dir management (Linux Deep Dive)

Learn to identify, evaluate and assess network vulnerabilities for improved security and threat protection. Real-world lab experience included (Network Pentesting, and Ethical Hacking in line with various frameworks)

Learn to assess orgs' PCI DSS compliance for secure credit card info processing (PCI DSS Qualified Security Assessor Training)

Learn alt. stats methods challenging dominant paradigms. Develop the ability to explain modern stats based on logic & human reasoning (Real Statistics: A Radical Approach)

Learn to automate tasks, solve complex problems & use cloud computing for application services (RHEL Intensive-SysOps)

SCADA security training w/ hands-on techniques for preventing & detecting incidents (SCADA Prevention & Detection a Hands-on Approach)

"Gain expertise in SCADA security w/ ISO 27019:2017 & NIST 800-82. Learn info security controls & industrial control systems standards."(SCADA, ISO 27019:2017 and NIST 800-82 connection)

Learn to secure industrial control systems against attacks & protect sensitive info through practical & theoretical knowledge (SCADA/ICS Security 101)

Learn to collect, analyze, and correlate security data for effective threat detection and response with hands-on SIEM practice (SIEM the HOA starting the journey)

Learn statistical concepts: location/dispersion, estimation, hypothesis testing, regression, correlation analysis (Statistics for Emerging Pathways)

Learn to identify & assess web app vulnerabilities. Enhance security posture & become job ready IT professional with hands-on labs (Vulnerability assessment in line with various frameworks Code)

Hands-on web app security training, educating & raising awareness on common issues, providing guidance & best practices, (WEB APPLICATION PENTESTING WSTG-LABS)

Web app security hands-on training to improve security posture, and remediate vulnerabilities (Web Application Pentesting & Ethical Hacking in line with various frameworks)

Who Should Enroll in this Program?

This cloud cyber security diploma is designed for:

- School and university students looking to expand their knowledge, skills, and career opportunities
- Professionals in the industry who want to enhance their skills and advance their careers

This diploma program is suitable for individuals between the ages of 16 and 45 who are self-motivated and capable of studying independently. The diverse student body, composed of individuals from various industries and backgrounds, enriches class discussions and interactions.

The diploma prepares individuals for careers such as:

- Information Security Analyst
- Security Engineer
- Network Security Engineer
- Cybersecurity Consultant
- Information Security Manager
- Security Operations Center (SOC) Analyst
- Penetration Tester
- Compliance Manager
- Incident Response Analyst
- Cloud Security Engineer

Important Features:

No academic prerequisites required
Only a reliable internet connection and a laptop/PC needed

Learning Path

1. LinkedIn Course for Job Seekers
2. IELTS Academic and General Training
3. Linux Deep Dive
4. Linear Algebra for Emerging Pathways
5. RHEL Intensive-SysOps
6. SCADA/ICS Security 101
7. Python Deep Dive
8. Certified Information System Security Professional (CISSP)
9. Cyber Security Essentials Revisit after CISSP
10. Elasticsearch SOC Engineer
11. Probability for Emerging Pathways
12. Vulnerability assessment in line with various frameworks Code
13. ISO 27001, 27017, 27018, Lead Implementer & Auditor
14. PCI DSS Qualified Security Assessor Training

Learning Path

15 **Hacking 101 AKA ethical hacking and incident response management**

16 **SIEM the HOA starting the journey**

17 **Statistics for Emerging Pathways**

18 **Web Application Pentesting & Ethical Hacking in line with various frameworks**

19 **Elasticsearch threat Hunting and Observability Engineer**

20 **CIS Top 18 Controls**

21 **SCADA Prevention & Detection a Hands-on Approach**

22 **SCADA, ISO 27019:2017 and NIST 800-82 connection**

23 **Calculus for Emerging Pathways**

24 **Real statistics: A Radical Approach**

25 **Elasticsearch for Data Science and Analytics with Kibana**

26 **Network Pentesting, and Ethical Hacking in line with various frameworks**

27 **Web Application Pentesting WSTG-Labs**

28 **Prepare and give the exam**

29 **EduQual Certificate**

LinkedIn Course for Job Seekers

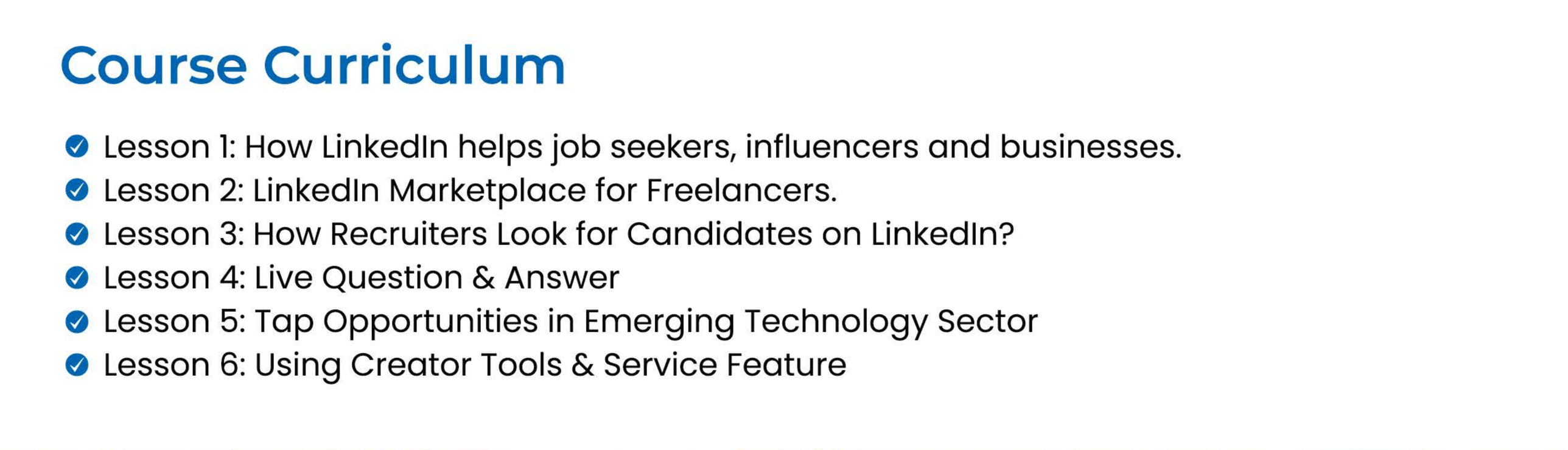
The objective of this course is to empower Emerging Technology learners to utilize LinkedIn effectively in order to secure employment or freelance opportunities. This implies that the course aims to equip learners with the necessary skills and knowledge to utilise LinkedIn to find and apply for job openings or market themselves as freelancers in their field. The focus is on helping learners effectively utilize LinkedIn in their job search, as well as building their professional network and making connections in their industry.

Key Learning Objectives

- Empower Emerging Technology learners
- Utilize LinkedIn effectively
- Secure employment or freelance opportunities
- Equip learners with skills and knowledge to use LinkedIn for job search
- Build professional network and make industry connections

Course Curriculum

- Lesson 1: How LinkedIn helps job seekers, influencers and businesses.
- Lesson 2: LinkedIn Marketplace for Freelancers.
- Lesson 3: How Recruiters Look for Candidates on LinkedIn?
- Lesson 4: Live Question & Answer
- Lesson 5: Tap Opportunities in Emerging Technology Sector
- Lesson 6: Using Creator Tools & Service Feature



IELTS Academic and General Training

The objective of this unit is to equip students with the necessary skills and knowledge to succeed in their IELTS exam. Through active participation in various activities, learners will develop their reading, writing, listening, and speaking abilities in English, thereby enhancing their overall proficiency and preparing them for the IELTS examination.

Key Learning Objectives

- Learn to read to understand the gist, scan important details and read in-depth and between the lines.
- Learn to listen to understand the gist, scan important details and read in-depth and between the lines.
- Learn to write cohesive and coherent argumentative essays, descriptive essays, discursive essays, letters and academic analyses of graphs, charts and tables.
- Learn to speak fluently and accurately in a number of work-based and academic scenarios along with being able to carry out regular and casual conversations in the target language.

Course Curriculum

- Lesson 1: Introduction to IELTS
- Lesson 2: IELTS Writing Tasks - Marking Criteria
- Lesson 3: Writing - Looking at the paper
- Lesson 4: General Training Tasks
- Lesson 5: Argumentative Writing
- Lesson 6: Discursive Writing
- Lesson 7: Letter Writing
- Lesson 8: Model Essay
- Lesson 9: Model Letter (General Training)
- Lesson 10: Final Practice - Essay Writing, Letter Writing (General Training)
- Lesson 11: IELTS Reading and Listening
- Lesson 12: IELTS Reading: Techniques
- Lesson 13: IELTS Reading (Types of Questions)
- Lesson 14: IELTS Resource Material
- Lesson 15: IELTS Speaking Tips and Strategies
- Lesson 16: Speaking - Sample Scenarios
- Lesson 17: IELTS Speaking - Role-play Cards

Linux Deep Dive

This course teaches students about the Linux Operating System and its applications in completing tasks and solving complex problems. Students will gain factual, procedural, and theoretical knowledge and learn to configure and install software, manage files and directories, and interpret and evaluate relevant information. The course provides hands-on practice to develop practical skills and different perspectives within the field of work.

Key Learning Objectives

- Understand the differences between Unix and Linux
- Learn how to install Linux and understand the different distros available
- Use pre-made images to install Ubuntu, CentOS, or Parrot OS
- Learn basic Linux commands for working with files, directories, and users
- Understand ownership, groups, and permissions for files and directories
- Work with text files and learn basic networking in Linux
- Understand processes, daemons, and how to install software and get help
- Learn Bash Scripting and understand echo and read commands, loops, and conditional statements
- Understand advanced Bash Scripting commands and tools such as grep, cut, AWK, SED, and find
- Gain practical experience through real-time hands-on projects and tasks

Course Curriculum

- Lesson 1: Introduction to Unix and Linux
- Lesson 2: Linux Installation and Distributions
- Lesson 3: Using Pre-Made Images to Install Linux
- Lesson 4: Basic Linux Commands, Files, and Directories
- Lesson 5: Working with Users, Groups, Ownership, and Permissions
- Lesson 6: Editing Text Files and Networking in Linux
- Lesson 7: Linux Processes, Daemons, and Software Installation
- Lesson 8: Introduction to Bash Scripting and Bash Commands
- Lesson 9: Advanced Bash Scripting, Loops, and Conditional Statements
- Lesson 10: Practical Hands-on Experience in Bash Scripting

Linear Algebra for Emerging Pathways

The course teaches basic concepts and techniques of Linear Algebra, including systems of linear equations, matrices, matrix algebra, determinants and inverses, linear combinations and linear independence, and linear transformations eigenvalues and eigenvectors. After completing the course, students will be able to comprehend the theory of the system of linear equations and solve problems using matrices, finite-dimensional vector spaces, and linear transformations. The course emphasizes intuition, mathematics, and geometry, and provides mathematical and solved examples supplemented with geometrical interpretation to build the visualization.

Key Learning Objectives

- Understand linear combination, linear equation, and system of linear equations and express them as matrices
- Solve the system of linear equations
- Understand the geometric interpretation of linear transformation and express the linear transformation as a matrix
- Understand the composition of transformations
- Understand the concept of eigenvalues and eigenvectors.

Course Curriculum

- Lesson 1: Linear vs. Nonlinear Equations and Systems
- Lesson 2: Matrices and Systems of Linear Equations
- Lesson 3: Solving Matrix Equations using Matrix Inverse, Cramer's Rule, RREF, etc.
- Lesson 4: Linear Transformations and Their Geometry
- Lesson 5: Relationship between Linear Transformations and Matrix Multiplication
- Lesson 6: Multiple Transformations as Multiplication of Matrices
- Lesson 7: Eigenvalues and Eigenvectors
- Lesson 8: Computing Eigenvalues and Eigenvectors

RHEL Intensive-SysOps

Upon completing the course, students will gain factual, procedural, and theoretical knowledge about Linux Fundamentals and its applications in addressing complex problems and automating tasks. They will be able to interpret and evaluate relevant information and perform tasks such as Network-User-Administration and AWS services. Additionally, students will develop hands-on skills and have a complete understanding of Linux distribution, enabling them to approach work from different perspectives. Ultimately, they will be equipped with the necessary tools to deliver application services.

Key Learning Objectives

- Understanding the Linux file system hierarchy and file permissions
- Partitioning disks and managing logical volumes using LVM
- Configuring network interfaces and services like DNS and FTP
- Installing and managing software packages using RPM and YUM
- Monitoring system performance using tools like top, find, and Zabbix
- Managing user accounts and permissions, including SUID, SGID, and sudoers
- Configuring and securing Apache web server and reverse proxy using Nginx
- Understanding the AWS cloud computing infrastructure and launching EC2 instances
- Managing EBS volumes, Elastic IPs, and S3 storage on AWS
- Implementing high availability and failover using Keepalived and HAProxy
- Managing MySQL databases and SAN storage
- Developing and fine-tuning Linux kernel drivers and patches

Course Curriculum

- Lesson 1: CentOS 6 ISO download and installation
- Lesson 2: File system hierarchy overview
- Lesson 3: File system hierarchy editors and AWS account configuration
- Lesson 4: Softlinks and hardlinks, copying and moving files
- Lesson 5: Installation of RHEL 7/8 and ownership and permissions overview
- Lesson 6: Editors, ownership, and permissions
- Lesson 7: Advanced permissions and runlevels
- Lesson 8: Disk partitioning and runlevels continuation
- Lesson 9: Targets, partition logic concepts, and FSTab
- Lesson 10: Partition task solving and compression tools

- Lesson 11: Archive and compression tools
- Lesson 12: RSync, Lun scanning, disk scanning, and logical extended partition
- Lesson 13: Fdisk, partitioning cases, standards, and mounting
- Lesson 14: Filesystem check and repair using FSCK, e2fsck, lsblk, pipe, less, and more
- Lesson 15: Searching using grep, find, locate, fstab, process daemons, and performance monitoring
- Lesson 16: Network configuration part 1 - How to configure IP gateway
- Lesson 17: Network configuration part 2 - DNS and resolv.conf
- Lesson 18: Network configuration part 3 - IP class and IP aliasing
- Lesson 19: Protocols, ports, and OSI layer
- Lesson 20: Ports, sniffer, and RPM
- Lesson 21: RPM install, upgrade, erase, and package in Linux
- Lesson 22: RPM SWAP
- Lesson 23: Interview preparation and performance monitoring tools
- Lesson 24: Performance monitoring using TOP, FIND, and FSH
- Lesson 25: Tape backups and YUM
- Lesson 26: SWAP extension and resume development overview
- Lesson 27: YUM and network configuration in CentOS 7/8
- Lesson 28: JOB details and resume development
- Lesson 29: Yum deep dive, local repo server, and LVM2
- Lesson 30: LVM3 - Add, extend, and remove logical volume
- Lesson 31: LVM4 - Add, extend, and remove logical volume mappings
- Lesson 32: LVM5 - Structure backup, snapshot, RHCSA PE extent question
- Lesson 33: Yum, OS software, kernel patching, undo, and rollback
- Lesson 34: Source code installation
- Lesson 35: Cron scheduler and user management
- Lesson 36: Advance permission - SUID, SGID, sticky bit, and sudoers
- Lesson 37: Sudoers, UMASK, and kernel driver management
- Lesson 38: Kernel management, patching, and tuning
- Lesson 39: AWS cloud computing overview and global infrastructure
- Lesson 40: Launching EC2 instance on AWS
- Lesson 41: AWS services overview, billing, support center, and waiver off
- Lesson 42: AWS cloud watch and instance types, families, and EBS volumes
- Lesson 43: AWS elastic IP and S3 calculator
- Lesson 44: NFS, server-client model, and NFS server 2 and FTP

SCADA/ICS Security 101

The course focuses on teaching students how to protect industrial control systems from malicious attacks and unauthorized access to sensitive information. Students will learn to implement technical and operational security measures, conduct risk assessments, and develop incident response and recovery plans. The course also provides hands-on practice through proprietary labs to prepare students for a career as SCADA professionals.

Key Learning Objectives

- Understanding the basics of SCADA and CADA security.
- Understanding the basics of vulnerability assessment and penetration testing using Cybati VM.
- Understanding the regulatory requirements related to SCADA security, particularly the NERC coverage.
- Familiarization with certification exams related to SCADA security.
- Understanding the vulnerable protocols within SCADA systems.
- Understanding the role of tools such as Shodan, ICS CERT, and other security resources for SCADA systems.
- Understanding the risk factors associated with SCADA systems and how to manage them, including vendor risk management and the ISO 27036 standard.
- Understanding the architecture of PERA and CPWe for SCADA systems.
- Understanding the importance of physical and network security for SCADA systems and how to implement them.
- Understanding the role of SIEM, SOC, and NOC in SCADA security.
- Understanding the security context of computer and application security in SCADA systems.
- Developing a SCADA security program

Course Curriculum

- Lesson 1: SCADA Security 101 intro
- Lesson 2: CADA Security 101 intro Cybati VM for labs
- Lesson 3: SCADA Security 101 intro NERC Coverage
- Lesson 4: SCADA Security What Certification exams we will cover
- Lesson 5: SCADA Security 101 the first phase
- Lesson 6: Vulnerable Protocols within SCADA
- Lesson 7: The role of Shodan, ICS CERT and beyond
- Lesson 8: SCADA Security 101 the second phase
- Lesson 9: CSET Tool walkthrough
- Lesson 10: Risk Factors, vendor risk mgmt and ISO 27036 standard
- Lesson 11: PERA and CPWe Architecture review
- Lesson 12: Physical and Network Security within SCADA
- Lesson 13: The role of SIEM, SOC and the NOC
- Lesson 14: Computer Security and SCADA Context
- Lesson 15: Application Security and SCADA Context
- Lesson 16: SCADA Security Program Development

Python Deep Dive

The course focuses on developing advanced skills in Python for complex and non-routine tasks, including data analysis and visualization, building applications using Python frameworks, deploying machine learning models, and optimizing code. It includes practical experience and labs to help students become professional Python programmers.

Key Learning Objectives

- Gain practical knowledge of programming concepts through hands-on practice.
- Apply programming concepts practically through hands-on practice.
- Utilize Python programming language to implement advanced concepts through hands-on practice.
- Develop skills for automating tasks through hands-on practice using Python.

Course Curriculum

- Lesson 1: Python Primer
- Lesson 2: Python Alpha
- Lesson 3: Python Beta
- Lesson 4: Python Automation

Certified Information System Security Professional (CISSP)

The CISSP course teaches students how to protect and secure information systems by covering topics such as cryptography, network security, risk management, and access control systems. Students also learn about industry standards and best practices for information security. After completing the course, students can work in information security roles in private and public sector organisations.

Key Learning Objectives

- Understand Security & Risk Management principles and concepts (Domain 1)
- Learn about Asset Security, including data classification and management (Domain 2)
- Learn about Security Architecture and Engineering, including secure design principles (Domain 3)
- Understand Communication and Network Security, including secure network components and protocols (Domain 4)
- Gain knowledge on Identity and Access Management (IAM), including user identification and management (Domain 5)
- Understand Security Assessment and Testing, including vulnerability assessments and security audits (Domain 6)
- Learn about Security Operations, including incident management and disaster recovery (Domain 7)
- Understand Software Development Security, including secure coding practices and software testing (Domain 8)

Course Curriculum

- Lesson 1: CISSP Intro
- Lesson 2: Domain 1 Security & Risk Management
- Lesson 3: Domain 2 Asset Security
- Lesson 4: Domain 3 Security Architecture and Engineering
- Lesson 5: Domain 4 Communication and Network Security
- Lesson 6: Domain 5 Identity and Access Management (IAM)
- Lesson 7: Domain 6 Security Assessment and Testing
- Lesson 8: Domain 7 Security Operations
- Lesson 9: Domain 8 Software Development Security

Cyber Security Essentials Revisit after CISSP

The course on cybersecurity teaches fundamental concepts related to CISSP, which allows students to interpret and evaluate relevant information using the latest cybersecurity principles and methodologies. Students will learn about core security concepts like risk management, security architecture, incident management, and access control through hands-on practice and skills training in homegrown labs. Upon completion, students will be job-ready and prepared to become cybersecurity professionals.

Key Learning Objectives

- Importance of Cyber Security Body of Knowledge
- Refreshing of knowledge and concepts from the CISSP course
- Formulation of the process for aligning technological aspects with organizational goals and stakeholder protection
- Comprehensive understanding of security principles for system protection and implementing countermeasures against cyber attacks
- Understanding of methodologies for protecting computer systems and data storage and processing
- Understanding of methodologies for ensuring the security and reliability of various software platforms by identifying vulnerabilities
- Understanding of implementation and methodologies associated with the organization's technology infrastructure reliability and security

Course Curriculum

- Lesson 1: Cyber Security Essentials Revisit Starting up
- Lesson 2: Cyber Security Revisit the next steps Introduction
- Lesson 3: Domain 1 Human, Organisational, and Regulatory Aspects
- Lesson 4: Domain 2 Attacks & Defences
- Lesson 5: Domain 3 Systems Security
- Lesson 6: Domain 4 Software Platform Security
- Lesson 7: Domain 5 Infrastructure Security

Elasticsearch SOC Engineer

The objective of this course is to teach students the skills and knowledge necessary to become a successful Elastic Search SOC Engineer. Upon completion of the course, students will be able to use ElasticSearch to detect and respond to security threats, as well as design and implement ElasticSearch-based security solutions, troubleshoot and optimize ElasticSearch performance, and proactively protect their organizations from cyber attacks. The course involves hands-on training and real-world scenarios to equip students with practical experience in using ElasticSearch for security operations and incident response.

Key Learning Objectives

- Index data using Kibana and Elasticsearch API
- Understand text and keywords and create custom mappings
- Write advanced search requests using Elasticsearch Query DSL and search templates
- Re-index or delete documents and define ingested node pipeline
- Write Painless scripts and define runtime fields
- Create metrics and bucket aggregations, and manipulate advanced aggregation
- Configure shards, replicas, and analyse shard allocation for optimizing index performance
- Work with index aliases, templates, and index life-cycle policy
- Set up a remote cluster for cross-cluster search and configure cross-cluster replication
- Monitor clusters and identify issues using CAT APIs

Course Curriculum

- Lesson 1: Introduction to Elasticsearch, Logstash, and Kibana (ELK) Stack, Data in, Information Out
- Lesson 2: Strings in Elasticsearch, Index Mapping in Elasticsearch, Text Analysis, Types and Parameters
- Lesson 3: Searching with DSL Queries, More DSL Queries, Developing Search Applications
- Lesson 4: Changing Data, Enriching Data, Runtime Fields
- Lesson 5: Metrics and Buckets Aggregations, Combining Aggregations, More Aggregations
- Lesson 6: Understanding Shards, Scaling Elasticsearch, Distributed Operations
- Lesson 7: Data Management Concepts, Index Life-cycle Management Policy, Snapshots in Elasticsearch Stack
- Lesson 8: Elasticsearch Cluster Management, Elasticsearch Troubleshooting & Monitoring

Probability for Emerging Pathways

To gain an understanding of the fundamental principles of randomness in nature and probability techniques through intuitive, mathematical, and procedural approaches.

Key Learning Objectives

- To gain a fundamental understanding of probability and its basic concepts.
- To learn the methods of computing probability, including counting techniques.
- To gain a deeper understanding of advanced concepts in probability theory.
- To understand the concept of continuous random variables and distributions.
- To learn how to apply continuous distributions to real-world problems.
- To develop the ability to analyze continuous data and make statistical inferences.

Course Curriculum

- Lesson 1: Introduction Module
- Lesson 2: Introduction to Probability
- Lesson 3: Advanced Concepts of Probability
- Lesson 4: Discrete Random Variable
- Lesson 5: Continuous Random Variable

Vulnerability assessment in line with various frameworks Code

Upon completing this course, learners will be able to identify, evaluate, and assess the web-based application and system vulnerabilities in accordance with industry standards. They will gain practical experience through homegrown labs and develop skills to provide remediation recommendations and promote best practices in web application security. Learners will also gain an understanding of different perspectives and approaches within the field, preparing them for a career in IT.

Key Learning Objectives

- Understand various frameworks, standards, and methodologies in cybersecurity
- Identify the difference between vulnerabilities and patching, and conceptualize vulnerabilities for exploitation
- Recognize the importance of network data and open-source tools in cybersecurity

- Understand how to scan and assess cloud providers and their associated risks
- Identify the appropriate scanners to use for vulnerability assessment
- Understand different types of vulnerability scanners and their associated tools
- Use vulnerability assessment tools for attacking purposes and identify web application types
- Understand SSL and non-SSL websites and how to scan the infrastructure
- Understand vulnerabilities in wifi and Internet of Things connections
- Differentiate between voice over internet protocol and session internet protocol
- Perform hands-on network mapping and vulnerability assessment using Zed Attack Proxy and Burp Suite
- Perform reconnaissance on DNS and use Dradis for penetration testing
- Crack a hash using a specific tool

Course Curriculum

- Lesson 1: The Beginning of the Journey in the World of Vulnerability Assessment
- Lesson 2: Masscan Lab how to scan the whole internet
- Lesson 3: Difference between VA and patching
- Lesson 4: Everything is Vulnerable just like Humans
- Lesson 5: Network data and why it matters in the context of VA
- Lesson 6: Open Source Tools to rest Recon play with them.
- Lesson 7: Scanning the Cloud what you need to know as a VA Analyst
- Lesson 8: Global Cloud Providers
- Lesson 9: Inspector Gadget and assessing the cloud providers automatically
- Lesson 10:The connection between army doctrine vs vulnerability assessment
- Lesson 11:Which vulnerability scanners to use
- Lesson 12:Understanding Cyber Security Risk and Risk Methodologies
- Lesson 13:Open Source Scanners vs Commercial Scanners
- Lesson 14:Scanners that you should know and will learn on our Labs
- Lesson 15:Difference between web and network scanning
- Lesson 16:Web Application types and tools to attack them
- Lesson 17:SSL vs non-SSL what to use
- Lesson 18:VOIP and SIP their importance
- Lesson 19:Scanning the Infrastructure where it hurts
- Lesson 20:Wifi and IoT Connection
- Lesson 21:Network Mapper
- Lesson 22:Vulnerability Assessment (VA) Using ZAP
- Lesson 23:Play Around With Burpsuite
- Lesson 24:DNS
- Lesson 25:Pentesting Project Management
- Lesson 26:Hash Cracking
- Lesson 27:Sherlock
- Lesson 28:Scanning with FLAN

ISO 27001, 27017, 27018, Lead Implementer & Auditor

Upon completion of this course, learners will have acquired factual, procedural, and theoretical knowledge of international security management standards. They will be able to implement and evaluate information security management systems, specifically focusing on assessments and audits. Learners will have practical, hands-on experience using proprietary labs, gaining proficiency in different global perspectives and approaches, thereby developing job readiness.

Key Learning Objectives

- Conceptualize the scope of the ISO 27001 audit
- Understand and implement the ISO 27000 family of standards
- Assess risks and understand their treatment, including policies and documentation procedures
- Review and conceptualize ISO 27001, ISO 27017, and ISO 27018 standards
- Implement ISO 27001 Annex A Policy and Procedures through in-depth lessons and relevant documents
- Gain training and awareness of information security management system
- Understand the procedure for internal audit
- Implement management Review Minutes & Corrective Actions Procedures through hands-on practice

Course Curriculum

- Lesson 1: ISO 27001 Audit Course 101
- Lesson 2: ISO family of Standards (Video Only, no notes)
- Lesson 3: ISO 27001 Audit Course 200a ISO family of Standards (Video Only, no notes)
- Lesson 4: ISO 27001 Audit Course 200b ISO family of Standards (Video Only, no notes)
- Lesson 5: ISO 27001 Audit Course 200c ISO family of Standards (Video Only, no notes)
- Lesson 6: ISO 27001 Audit Course 200d Walk-through of ISO 27001 part 1
- Lesson 7: Walkthrough of ISO 27001 part 2
- Lesson 8: Walk-through of ISO 27002
- Lesson 9: Walkthrough of ISO 27002
- Lesson 10: Walk-through of ISO 27017 Cloud Security Standard
- Lesson 11: Walkthrough of ISO 27018 PII Security Standard
- Lesson 12: Walkthrough of Project Plan
- Lesson 13: ISO 27001 Documentation List to focus on
- Lesson 14: Procedure_for_Document_and_Record_Control
- Lesson 15: ISO 27001 Documentation List to focus on. Annex A 06 part 1 BYOD
- Lesson 16: Annex A 06 part 2 Mobile device and Teleworking
- Lesson 17: Annex A 07 Human_resource_security
- Lesson 18: Annex A 8 Asset_management
- Lesson 19: Annex A 10_Cryptography
- Lesson 20: Annex A 11_Physical_and_environmental_security
- Lesson 21: Annex A 12_Operations_security
- Lesson 22: Annex A 13_Communications_security
- Lesson 23: Annex A 14_System_acquisition_development_and_maintenance Policy
- Lesson 24: Annex A 15_Supplier_relationships
- Lesson 25: Annex A 16_Information_security_incident_management
- Lesson 26: Annex A 17_Business_Continuity
- Lesson 27: Training_and_Awareness_Plan
- Lesson 28: Procedure_for_Internal_Audit
- Lesson 29: Management_Review_Minutes and Corrective Action Procedures and Forms

PCI DSS Qualified Security Assessor Training

The learning objective of this course is to equip students with the knowledge and skills required to assess an organization's compliance with the Payment Card Industry Data Security Standards (PCI DSS). By the end of the course, students will have factual, procedural, and theoretical knowledge of the PCI DSS and will have hands-on practice and skills using Security Information and Event Management (SIEM) tools. They will also be able to understand different approaches to this area of work.

Key Learning Objectives

- Gain practical experience working with system logs and understanding the role of SIEM in an organization
- Understand the benefits and importance of PCI DSS (Payment Card Industry Data Security Standard)
- Explore global jobs in the PCI DSS domain
- Analyze the importance of people, procedures, and technology in relation to PCI DSS through a report
- Review the PCI DSS standards document library
- Understand key terms, abbreviations, and acronyms related to PCI DSS through the PCI DSS Glossary of Terms

Course Curriculum

- Lesson 1: Introduction to PCI DSS
- Lesson 2: Global Jobs in the PCI DSS Domain
- Lesson 3: People, Procedures and Technology
- Lesson 4: Analysis of PCI DSS through a Report
- Lesson 5: PCI DSS Standards Document Library Review
- Lesson 6: PCI DSS Glossary of Terms, Abbreviations, and Acronyms
- Lesson 7: PCI DSS Architecture deep dive

Hacking 101 AKA ethical hacking and incident response management

Learners will be equipped with the skills and knowledge needed to improve the overall security of an organization and identify, prevent, and respond to cyber security threats. Students will learn about attack techniques, incident response, and recovery, and gain practical, hands-on experience through proprietary labs to become job-ready IT professionals.

Key Learning Objectives

- Define ethical hacking and understand the necessary documentation
- Understand incident response management and its role in organizations
- Use source tools for ethical hacking, digital forensics, and penetration testing
- Learn international standards for information security incident management
- Familiarize learners with practical aspects of ethical hacking and incident response through hands-on labs
- Use tools to protect data and websites, including cyber security search engine,
- Google hacking database, and open-source tools for cyber risks
- Assess a cybersecurity incident and apply the incident response process to help an organization
- Identify the process of hacking a network and use web-based and wireless network reconnaissance tools
- Use open-source exploration tools, security auditing, and mapping
- Understand the role of senior management in incident response and identify the process of notifying affected parties
- Evaluate and recall lessons learned in incident response management.

Course Curriculum

- Lesson 1: Hacking 101 Intro
- Lesson 2: ISO 27035 a quick review to understand Incident Response Management
- Lesson 3: Parrot OS our distro for pentesting and forensics
- Lesson 4: ISO 27035 Revisit
- Lesson 5: NIST Incident Handling Document Revisit Deep Dive.
- Lesson 6: Deep Dive Hacking Mindset with labs
- Lesson 7:Challenge Lab for SysInternal
- Lesson 8: IR Table Top Exercise
- Lesson 9:Lab: Going down the Linux Rabbit hole
- Lesson 10:Lab RITA next steps in threat hunting.
- Lesson 11:OSINT Lab deep dive
- Lesson 12:Major Challenge Lab Creating a Shodan like tool
- Lesson 13: have I been pwned?
- Lesson 14:#Spyse Tool
- Lesson 15:Google Exploit Database
- Lesson 16:Maltego and Dark Trace the future
- Lesson 17:Tools on parrot OS and installing creepy and running it as a test run
- Lesson 18:MITRE ATT&CK, Chain of Custody and Security ops
- Lesson 19:The role of CSIRT, ENISA, and First in the overall IM process globally
- Lesson 21:The Role of Senior Mgmt, CPR and wordWebBugs
- Lesson 22:Affected parties, write blockers, short & long-term IM goals
- Lesson 24:Lessons learned in Incident Response Management
- Lesson 25:Review how to install MS SCCM in your lab
- Lesson 26:Kansa Challenge Lab and Applied Incident Response Management
- Lesson 27:Hacking mindset deep dive into networks
- Lesson 28:Maltego Challenge Lab
- Lesson 29:Hacking 101 mindset the next phase
- Lesson 30: Hacking 101 mindset the wireless hacking area
- Lesson 31: AL Nafi Linux and Nmap

SIEM the HOA starting the journey

By the end of this course, students will have the necessary knowledge and skills to collect, analyze, and correlate security-related data from multiple sources within an organization's network. They will be able to interpret and evaluate data to detect, respond and prevent security threats in real-time using SIEM. Students will have a practical and hands-on understanding of different approaches and perspectives within this field of work.

Key Learning Objectives

- Understand the role of SIEM in organizations
- Gain practical experience in working with system logs
- Learn the benefits and importance of SIEM
- Understand the role of compliance in having a SIEM
- Learn about threat intelligence (CREST)
- Understand intelligence-led security and cyber security monitoring and logging
- Learn about Security Big Data Analytics
- Understand the benefits of logs consolidation in a SIEM environment
- Understand the compliance climate

Course Curriculum

- Lesson 1: Introduction to SIEM
- Lesson 2: Complete Guide to SIEM
- Lesson 3:Role of Compliance in Having a SIEM
- Lesson 4:Threat Intelligence
- Lesson 5:Cyber Security Monitoring and Logging Guide
- Lesson 6:Security Big Data Analytics
- Lesson 7:Compliance Climate

Statistics for Emerging Pathways

Gain an understanding of statistical concepts such as measurements of location and dispersion, estimation, hypothesis testing, regression, and correlation analysis. Key Learning Objectives

Key Learning Objectives

- Understand measures of location and dispersion
- Understand hypothesis testing and confidence intervals
- Understand linear regression modelling
- Analyze the direction and strength of the relationship between two variables

Course Curriculum

- Lesson 1: Measures of central tendency
- Lesson 2: Measures of variability
- Lesson 3: Statistical significance testing
- Lesson 4: Confidence intervals
- Lesson 5: Simple linear regression
- Lesson 6: Correlation coefficient computation

Web Application Pentesting & Ethical Hacking in line with various frameworks

Students will develop the ability to assess and evaluate vulnerabilities in web applications and systems through practical exercises. They will learn industry-standard practices and be able to provide recommendations for remediation and promote best practices in web application security. By completing hands-on lab exercises, students will gain the necessary skills to become IT professionals and implement secure practices in organizations to protect against potential security threats.

Key Learning Objectives

- Understanding of Web Application Security (WAP) and its importance in securing web applications.
- Differentiating between web apps and native apps and understanding why it is difficult to secure web applications.
- Understanding the importance of threat modelling in WAP and how it can be used to identify and mitigate potential security risks.
- Understanding the importance of source code review and how it can be used to identify vulnerabilities in code.
- Knowledge of various tools and techniques used in WAP, such as SAST, DAST, IAST, and OAST.
- Understanding of various penetration testing methodologies used to identify and exploit vulnerabilities in web applications.
- Practical experience with labs focused on WAP, such as SQL injections, CSRF attacks, role hijacking, remote code execution, and vulnerability searching using tools like Shodan and the Harvester.
- Ethical hacking skills and understanding of ethical hacking principles and frameworks.
- Knowledge of how to prevent and mitigate potential security threats in web applications.
- Understanding of the importance of ethical behaviour and professional conduct when working with WAP and ethical hacking

Course Curriculum

- Lesson 1: Introduction to WAP & Ethical Hacking in line with various frameworks
- Lesson 2: Understanding Web Application and its security challenges
- Lesson 3: Threat Modelling and Its importance
- Lesson 4: Importance of Code Review
- Lesson 5: Tools of the trade SAST vs DAST vs IAST vs OAST
- Lesson 6: Penetration Testing Methodologies
- Lesson 7: Labs for WAP, including SQL Injections, CSRF, Role Hijacking, Metasploit, Remote Code Execution, Reverse Shells, Exploiting MS-SQL, Shodan Vulnerabilities and Targeting.

Elasticsearch threat Hunting and Observability Engineer

This course will train learners on how to implement unified observability on a single platform using Elastic. They will learn how to collect various data such as logs, metrics, uptime, and APM, and send it to Elasticsearch. The goal is to create an observable system that is designed and built for usability, high availability, stability, and observability as a system attribute. The learner will also be taught how to use machine learning, alerting, and data correlation to make the unified observability data more actionable. Finally, the content will help learners experiment with using Kibana's user-friendly interface to visualize observability data and become an Elastic Certified Observability Engineer.

Key Learning Objectives

- Combine React web client and Java RESTful server through hands-on practice
- Utilize Heartbeat to track the availability of services such as Elasticsearch, Pet Clinic client/server, and MySQL database through hands-on practice
- Use Elastic Agent to gather NGINX metrics and logs, read MySQL log files and index them into Elasticsearch, and gather system/container metrics through hands-on practice
- Investigate Petclinic application's architecture and configure agents for Petclinic application core, backend server, and React frontend
- Investigate Logs and Metrics apps in Kibana, and use APM software to investigate performance indicators and check for faults in the Petclinic application
- Use ingest pipeline editor to define pipelines and extract events from NGINX and MySQL logs using dissect processor
- Adjust ingest pipelines to change data kinds and timestamp formats
- Learn about predefined machine learning jobs in Kibana and how to create them, and develop alerting rules using Observability apps
- Use integrations' dashboards to display observability data and solve complex system problems.

Course Curriculum

- Lesson 1: Introduction to the Course
- Lesson 2: Lab Setup-ES-Fundamentals
- Lesson 3: Up Time
- Lesson 4: Elastic Agent
- Lesson 5: Logs - Mysql
- Lesson 6: Metrics - System
- Lesson 7:Elastic APM Configuration
- Lesson 8: Java Agent Configuration
- Lesson 9:Node.js Agent Configuration
- Lesson 10:RUM Agent Configuration
- Lesson 11:Logs App Visibility
- Lesson 12:Metrics App Visibility
- Lesson 13: APM App Visibility
- Lesson 14:UX App Visibility
- Lesson 15:Pipelines Configuration
- Lesson 16:Extracting Events
- Lesson 17:Transforming Events
- Lesson 18:Machine Learning Custom Jobsading Events-2
- Lesson 19:Alerts and Rules Configuration
- Lesson 21:Dashboards

CIS Top 18 Controls

Upon completion of this course, students will be able to demonstrate factual, procedural, and theoretical knowledge of the Center for Internet Security's (CIS) comprehensive set of security controls to protect systems and data against common cyber attacks. They will also gain hands-on practice and skills through homegrown labs, enabling them to understand different perspectives and approaches within the cybersecurity field and become job-ready Cyber Security professionals.

Key Learning Objectives

- Understanding the core controls and CIS Top 18 Controls that are essential for securing an organization's IT infrastructure.
- Familiarity with the CIS resources and the 18 CIS controls to identify and mitigate common cybersecurity risks.
- Understanding the purpose and importance of each of the CIS Top 18 Controls, how they work, and how they can be implemented in an organization.
- Ability to complete CIS Controls 1-17 from start to finish, which involves understanding the control requirements, identifying gaps in the current environment, and developing and implementing plans to address those gaps.
- Knowledge of the changes between CIS Control v7 and v8 and how they impact an organization's security posture.
- Deep dive into the CIS Controls, which involves understanding the security requirements and implementation guidelines for each of the controls.
- Practical experience in implementing the CIS Controls in a real-world environment

Course Curriculum

- Lesson 1: Introduction to Core Controls and CIS Top 18 Controls
- Lesson 2: CIS Top 18 Controls Control 1
- Lesson 3: CIS Top 18 Controls Control 2
- Lesson 4: CIS Top 18 Controls Control 3
- Lesson 5: CIS Top 18 Controls Control 4
- Lesson 6: CIS Top 18 Controls Control 5
- Lesson 7: CIS Top 18 Controls Control 6
- Lesson 8: CIS Top 18 Controls Control 7
- Lesson 9: CIS Top 18 Controls Control 8, 9, 10
- Lesson 10: CIS Top 18 Controls Control 11
- Lesson 11: CIS Top 18 Controls Control 12
- Lesson 12: CIS Top 18 Controls Control 13
- Lesson 13: CIS Top 18 Controls Control 14
- Lesson 14: CIS Top 18 Controls Control 15
- Lesson 15: CIS Top 18 Controls Control 16
- Lesson 16: CIS Top 18 Controls Control 17
- Lesson 17: CIS Control v7 vs v8
- Lesson 18: CIS Top 18 Controls Control 18
- Lesson 19: CIS Top 18 Controls CSA Deep Dive Introduction

Real Statistics: A Radical Approach

Upon completion of this course, students will possess factual, procedural, and theoretical knowledge regarding alternative statistical methods and approaches that challenge conventional paradigms in statistics. They will be able to articulate how contemporary statistics is constructed based on logic and objective human reasoning. Students will have the capacity to apply this knowledge in real-world scenarios to analyze and interpret complex data sets.

Key Learning Objectives

- Understand the different chapters and sections in the book "Journey Towards the Light"
- Recognize the limitations of traditional statistical approaches and the need for a new approach to statistics
- Explore the moral foundations of knowledge and the differences between Islamic and Western conceptions of knowledge
- Understand the concept of comparing numbers, the arbitrary nature of rankings, and the values embodied in the choice of factors and weights for rankings
- Analyze life expectancies, including how to compute them from mortality tables and how to interpret data sets using histograms
- Learn about reducing data to one number, including the concepts of inflation and the quantity theory of money
- Examine the history and evolution of statistics, including the role of eugenics and the creation of statistics
- Understand stochastic relationships, quartiles as natural data summaries, and how to compare progress between countries on a given metric
- Learn about probabilities, binomials, and p-values, including their applications in time-branching probability models and random sampling
- Understand the flawed foundations of econometrics and the differences between real models and econometric models
- Explore the relationship between two series and the potential for spurious correlations
- Learn about the applications of statistics in real-world scenarios, including assessing the effectiveness of vaccines and identifying causes of global financial crises
- Understand causal analysis and path diagrams, including common causes and the concept of causation as a deep structure
- Recognize the potential for Simpson's Paradox in data analysis and the importance of randomization as a solution to confounding

Course Curriculum

- Lesson 1: Journey Towards the Light
- Lesson 2: A New Approach to Statistics
- Lesson 3: The Moral Foundations of Knowledge
- Lesson 4: Comparing Numbers
- Lesson 5: Life Expectancies
- Lesson 6: Reducing Data to One Number
- Lesson 7: Eugenics and the Creation of Statistics
- Lesson 8: Five Quartile Summaries of Stochastic Relationships
- Lesson 9: Probabilities, Binomials, and p-values
- Lesson 10: Causality and Regression Models:
- Lesson 11: Assessing Association Between Two Series
- Lesson 12: Some Applications:
- Lesson 13:Causal Analysis & Path Diagrams:
- Lesson 14:Simpson's Paradox

SCADA Prevention & Detection a Hands-on Approach

Students will acquire factual, procedural, and theoretical knowledge about Supervisory Control and Data Acquisition (SCADA) systems, with a focus on preventing and detecting security incidents through hands-on techniques. Upon completion of the course, students should be able to understand the security challenges in SCADA systems, develop effective strategies to defend against cyber-attacks, and gain hands-on skills and practice through indigenous labs. The goal is to prepare students to become job-ready SCADA professionals with a broad perspective on the area of study or work.

Key Learning Objectives

- Understanding the basics of SCADA (Supervisory Control and Data Acquisition)
- systems and their importance in industrial control systems.
- Learning about the Stuxnet malware attack and how it impacted SCADA systems.
- Understanding the vulnerabilities in WinCC, a popular SCADA software, and the ways to prevent and detect attacks on it.
- Gaining practical knowledge of the MODBUS protocol and its implementation in industrial systems.
- Learning about the different methods of hacking SCADA systems and the ways to prevent them.
- Understanding the concept of Hands-On-Attack (HOA) and its importance in learning about SCADA systems and their security

Course Curriculum

- Lesson 1: SCADA Prevention and Detection - The Beginning
- Lesson 2: Stuxnet - How it Really Moves Around
- Lesson 3: WinCC - Connecting the Dots
- Lesson 4: SIMATIC WinCC - Further Review
- Lesson 5: MODBUS Hands-On Protocol Hacking

SCADA, ISO 27019:2017 and NIST 800-82 connection

Completing this course will provide students with factual, procedural, and theoretical knowledge on ensuring SCADA systems adhere to security standards like ISO 27019:2017 and NIST 800-82. Students will become familiar with these standards and gain hands-on skills through proprietary labs to prepare them to become job-ready SCADA professionals with a comprehensive understanding of the topic.

Key Learning Objectives

- Understanding of SCADA (Supervisory Control and Data Acquisition) and its role in industrial control systems.
- Familiarity with cyber-physical security education and training related to SCADA systems.
- Understanding of NIST (National Institute of Standards and Technology) Review SP.800-82r2, which covers topics like industrial control systems, risk management, and ICS security controls.
- Ability to compare and contrast security measures used in IT systems versus those used in ICS systems.
- Knowledge of ISO 27019, which provides guidelines for information security management in the context of industrial control systems.
- Understanding of the key concepts related to ISO/IEC 27019 and its practical application in the SCADA environment

Course Curriculum

- Lesson 1: SCADA explained
- Lesson 2:Cyber-physical security education training
- Lesson 3: SCADA NIST Review SP.800-82r2
- Lesson 4:Overview of industrial control systems
- Lesson 5:Comparing ICS and IT systems security
- Lesson 6:Introduction to risk management
- Lesson 7:Select ICS security controls
- Lesson 8:Introduction to SCADA ISO 27019
- Lesson 9:Review of SCADA ISO 27019
- Lesson 10:Final Lecture on ISO/IEC 2701

Calculus for Emerging Pathways

After completing this course learners will understand the basic concepts and techniques of differential calculus in order to apply them to optimization and the gradient descent algorithm.

Key Learning Objectives

- Understand the slope of the function, tangent and secant line
- Compute derivatives of multivariable functions
- Understand minima, maxima and saddle points
- Comprehend first and second derivative tests for single variable function optimization
- Extend first and second derivative tests to multivariable function
- Understand and apply the gradient descent algorithm

Course Curriculum

- Lesson 1: Learn slope geometry, relevance to derivative, and extend derivative concept to multivariable functions.
- Lesson 2: Understand derivative creation procedure and corresponding rules, compute partial derivatives, and create gradient vector and Hessian matrix.
- Lesson 3: Understand optimum points' geometric and mathematical interpretation, and apply first and second derivative tests to find them.
- Lesson 4: Understand gradient and Hessian matrix calculation interpretation and procedure, and apply it to multivariable function optimum point calculation.
- Lesson 5: Understand gradient descent algorithm geometric interpretation, meaning of parameters, and apply procedure to optimize multivariable functions

Elasticsearch for Data Science and Analytics with Kibana

Upon completion of this course, learners will have the ability to effectively use Elasticsearch and Kibana to implement data science and analytics by setting up dashboards, visualizing data, creating custom visualizations, using machine learning algorithms to identify patterns and anomalies, and correlating data to make unified observability more actionable. They will gain the skills necessary to gain insights and make informed decisions based on the data.

Key Learning Objectives

- Understand Elastic Stack components: Elasticsearch, Kibana, Logstash, and Beats
- Build and customize interactive dashboards
- Effectively manage and organize Kibana objects
- Explore and analyze data using Kibana's Discover feature
- Create filters, change time filters, and save visualizations to dashboards
- Use Lens to create advanced visualizations and fine-tune settings
- Work with maps, including custom markers and polygons
- Upload images and add links to text
- Interact with dashboards and use visualizations to create filters
- Share and manage dashboards while protecting sensitive information
- Use Canvas to create professional-looking infographics
- Implement anomaly detection techniques and respond to anomalies
- Use runtime fields to define a "schema on read" approach
- Create custom visualizations and ask questions about data

Course Curriculum

- Lesson 1: Introduction to Kibana
- Lesson 2: Hello, Dashboard!
- Lesson 3: Spaces!
- Lesson 4: Discover and Data Visualizer
- Lesson 5: KQL and filters
- Lesson 6: Field focus
- Lesson 7: Create visualizations
- Lesson 8: Adjust visualizations
- Lesson 9: Create maps
- Lesson 10: Text on dashboards
- Lesson 11: Tables
- Lesson 12: Interactive dashboards
- Lesson 13: Sharing a Dashboard
- Lesson 14: Sharing with Users
- Lesson 15: Canvas
- Lesson 16: Time series anomaly detection
- Lesson 17: Adding Anomalies in Dashboard
- Lesson 18: Entity-centric analysis
- Lesson 19: Formulas
- Lesson 20: Runtime fields
- Lesson 21: Vega
- Lesson 22: Asking questions

Network Pentesting, and Ethical Hacking in line with various frameworks

The learning objective of this course is to provide students with practical skills to identify, evaluate and assess vulnerabilities in network systems and infrastructure. By the end of the course, learners will be able to implement these practices in organisations to improve the security posture and protect against potential security threats. Students will gain hands-on experience through industry-standard labs and be able to provide recommendations for remediation and promote best practices in web application security. The course aims to prepare students to become IT professionals who are job-ready and aware of different perspectives or approaches within the field.

Key Learning Objectives

- Understand SNMP Pentesting and how to perform it effectively.
- Learn how to use Recon-ng for reconnaissance purposes, including deep dive into Recon-ng, marketplace and modules, keys, and report generation.
- Learn how to scan subnets with Masscan, perform OS fingerprinting with Nmap, and use Nmap scripting engine for port scanning.
- Learn how to use Netcat for banner grabbing, moving files from one system to another, and establishing a reverse shell.
- Understand how to use Nessus to scan systems for vulnerabilities and generate reports.
- Introduction to Metasploit and learn how to use it to scan targets and find exploits, exploit Windows servers and perform post-exploitation.
- Introduction to Empire Framework and learn how to use it to exploit targets, perform privesc, mimicatz, collection, situational awareness, and persistence.
- Learn how to break multiple service passwords with Hydra, dump and crack hashes with JTR and Hashcat.
- Installation of BloodHound, SCP-SSH SharpHound, and learn how to use AD (Active Directory) collection to analyze gathered data with BloodHound per-built queries

Course Curriculum

- Lesson 1: SNMP Pentesting Introduction
- Lesson 2: Recon-NG Introduction and Deep Dive
- Lesson 3: Recon-ng Marketplace and Modules
- Lesson 4: Recon-ng Modules and Keys
- Lesson 5: Generate Report in Recon-NG
- Lesson 6: Scan Subnet with Masscan
- Lesson 7: OS Fingerprinting with Nmap
- Lesson 8: Nmap Scripting Engine
- Lesson 9: Port Scanning Using Netcat
- Lesson 10: Use Netcat to Move Files From One System to Another System
- Lesson 11: Banner Grabbing Using Netcat
- Lesson 12: Netcat Reverse Shell
- Lesson 13: Nessus Scan for Vulnerabilities
- Lesson 14: Generate a Report after Nessus Scan
- Lesson 15: Introduction to Metasploit
- Lesson 16: Scan Target and Find Exploit Using Metasploit
- Lesson 17: Exploit Windows Server 2003 with Metasploit
- Lesson 18: Exploit RCE on Windows XP with Metasploit
- Lesson 19: Exploit RCE on Windows Server 2008 with Metasploit
- Lesson 20: Metasploit Post Exploitation
- Lesson 21: Introduction to Empire Framework
- Lesson 22: Target Exploitation with Empire Framework
- Lesson 23: Privesc, Mimikatz, Collection, Situational Awareness, Persistence
- Lesson 24: Break Multiple Service Passwords with Hydra
- Lesson 25: Dump Hashes and Crack with JTR
- Lesson 26: Crack Hashes with Hashcat
- Lesson 27: Installation of BloodHound, SCP-SSH SharpHound
- Lesson 28: AD Collection with BloodHound
- Lesson 29: Analyzing Gathered Data with BloodHound Pre-Built Queries

Web Application Pentesting WSTG-Labs

This course will provide hands-on training to students interested in web application security, educating them on common security issues and best practices for securing web applications. By completing industrial-standard labs and providing recommendations for remediation, students will gain practical skills and become job-ready IT professionals with a comprehensive understanding of different perspectives within the field.

Key Learning Objectives

- Understanding the role and responsibilities of a Bug Bounty Hunter
- Conducting search engine discovery reconnaissance for information leakage
- Fingerprinting web servers and web application frameworks
- Identifying application entry points and testing file extensions handling for sensitive information
- Enumerating infrastructure and application admin interfaces
- Testing HTTP methods and subdomain takeover
- Integrating Burp Suite with an external browser
- Testing for sensitive information sent via unencrypted channels, default credentials, weak lockout mechanisms, and bypassing authentication schema
- Testing for vulnerable remember password and browser cache weaknesses
- Testing for weak password policy and weaker authentication in alternative channels
- Testing for directory traversal file inclusion, privilege escalation, and insecure direct object reference
- Testing for session management schema and cookies attributes, session fixation, and session hijacking
- Testing for reflected and stored cross-site scripting, HTTP parameter pollution, SQL injection, NoSQL injection, ORM injection, client-side vulnerabilities, and XPath injection
- Testing for IMAP SMTP injection, code injection, local and remote file inclusion, command injection, and format string injection
- Testing for incubated vulnerability, server-side template injection, server-side request forgery, host header injection, HTTP splitting smuggling, and improper error handling
- Understanding business logic and testing data validation, ability to forge requests, integrity checks, and process timing
- Testing for the circumvention of workflows, upload of unexpected and malicious files,
- and defenses against application misuse
- Testing for DOM-based cross-site scripting, JavaScript execution, HTML injection, client-side URL redirect, CSS injection, client-side resource manipulation, cross-site script inclusion, clickjacking, web storage testing, and websockets
- API testing

Course Curriculum

- Lesson 1: Introduction to WSTG and Bug Bounty Hunting, Search Engine Discovery Reconnaissance, and Fingerprinting Web Servers
- Lesson 2: Web Application Enumeration and Fingerprinting
- Lesson 3: Infrastructure and Admin Interfaces Enumeration, HTTP Method Testing, Subdomain Takeover Testing, and Burp Suite Introduction and Integration.
- Lesson 4: Infrastructure and Admin Interface Enumeration, Role Definition, and User Registration and Authentication Testing
- Lesson 5: Testing Authentication and Password Security
- Lesson 6: Authentication and Authorization Vulnerability Testing
- Lesson 7: Session Management and Security Testing
- Lesson 8: Testing for Session and XSS Vulnerabilities
- Lesson 9: Injection Attacks - SQL, NoSQL, ORM, Client-side, and XML-XPATH
- Lesson 10: Testing for Injection Vulnerabilities (XPath, IMAP SMTP, Code, Local and Remote File Inclusion)
- Lesson 11: Advanced Injection Testing Techniques
- Lesson 12:Testing for Network Vulnerabilities
- Lesson 13: Business Logic Testing and Validation
- Lesson 14: Testing Function Usage Limits, File Uploads, and Defenses Against Application Misuse
- Lesson 15:Testing for Client-side Vulnerabilities including DOM-Based Cross Site Scripting, JavaScript Execution, HTML Injection, Client-side URL Redirect, and CSS Injection.
- Lesson 16: Client-side Vulnerability Testing including Resource Manipulation, Cross Site Script Inclusion, Clickjacking, Web Storage Testing, and WebSockets.
- Lesson 17: API Testing

Comprehensive Assessment Approach

Assessments are an essential component of any diploma course, and at our online and distance learning platform, we ensure that our students are evaluated thoroughly. Multiple choice questions (MCQs) will be the standard form of assessment across all diploma courses. However, for certain individual courses, students may be required to deliver an oral presentation or participate in an interview. Additionally, after completing the entire diploma course, students will be required to present an oral presentation, which will be mandatory. This approach allows us to evaluate our students comprehensively and helps them develop essential skills for their future careers.

This track allows you to work in multiple industries

Features	
Accredited with EduQual	Yes
Access to Complete Course Content	Yes
Access to complete Hands On Labs	Yes
Resume Development	Yes
Interview Preparation	Yes
Internship Letter	Yes
Practice Exams	Yes
Weekly Live Sessions with Trainer	Yes
Available Languages	Yes

This track allows you to work in multiple industries

01

Information Security Analyst

Average Salary:
$98,350 per year

02

Security Engineer

Average Salary:
$115,000 per year

03

Network Security Engineer

Average Salary:
$115,000 per year

04

Cyber Security Consultant

Average Salary:
$115,000 per year

05

Information Security Manager

Average Salary:
$140,000 per year

06

Security Operations Center (SOC) Analyst

Average Salary:
$85,000 per year

07

Penetration Tester

Average Salary:
$115,000 per year

08

Compliance Manager

Average Salary:
$115,000 per year

09

Incident Response Analyst

Average Salary:
$115,000 per year

10

Cloud Security Engineer

Average Salary:
$120,000 per year

Our students are working all over the globe in fortune 500 companies

*Any third-party logos displayed in this booklet are the property of their respective companies.

Where Can I find more information?

UK Office Address.
167-169 Great Portland Street
5th Floor
London
WIW 5PF

Regional Office:
Pakistan: D-182, Block-7, Gulshan-e-Iqbal, Karachi, Sindh, Pakistan.

Contact Us:
+92-304-1110 400,
+1 (647) 680-0258 (WhatsApp)

Send Us Message
Support@alnafi.com

Visit:
www.alnafi.com