

Diploma in Cloud Cyber Security

EduQual Level 3 Endorsed Diploma



Learner Handbook
AL NAFI INTERNATIONAL COLLEGE
<https://alnafi.com>

Version: 1.0

Issue Date: [Insert Date]

© 2021 Al Nafi E-Learning Private Limited. All rights reserved.

Table of Contents

1. About the Diploma	4
2. Key Features of the Diploma	4
3. About the Diploma Program Endorsed by EduQual	5
4. About Al Nafi International College	5
5. Program Eligibility Criteria and Application Process	5
5.1. Eligibility Criteria	6
5.2. Application Process	6
6. Connect with the Support Operations Center	6
7. Program Outcomes	7
8. Who Should Enroll in this Program?	8
9. Learning Path	9
10. Assessment Information	9
10.1. Assessment Overview	10
Assessment Components	10
10.2. Al Razzaq Lab Assignments (70% weightage in overall Grade)	10
What Are They?	10
How Are They Graded?	10
What If You Need to Resubmit?	11
10.3. Multiple Choice Questions (15% of Your Grade)	11
Assessment Format	11
Attempts and Scoring	11
Diploma Program Access Period	12
10.4. English Language Exam (15% of Your Grade)	12
Mandatory Requirement	12
Submission Requirements	12
Verification and Compliance	12
Why Is This Required?	12
10.5. Al Razzaq Labs Program Access	13
Prerequisites for Lab Access	13
Lab Components	13
Additional Features and Support	13
10.6. Grading Criteria	14
Grade Boundaries	14
Example Calculation	
For a student:	14
Example: Overall Grade Calculation	16
Quick Reference Table	16
10.7. Academic Integrity	17
Violation Response	17
10.8. Support for Students	17
10.9. Accessibility and Reasonable Adjustments	18
10.10. Appeals Process	18

Complete Course Units (24 Units)	18
Unit 1: LinkedIn Course for Job Seekers	18
Unit 2: IELTS Academic and General Training	19
Unit 3: Linux Deep Dive	19
Unit 4: Python Deep Dive	20
Unit 5: Certified Information Systems Security Professional (CISSP)	20
Unit 6: Red Hat Enterprise Linux (RHEL)	21
Unit 7: Cyber Security Essentials Revisit (Post-CISSP)	21
Unit 8: CIS Top 18 Controls Hands-on Implementation	
Unit Objectives:	22
Unit 9: SIEM the HOA Starting the Journey	23
Unit 10: Elastic SOC Engineer	23
Unit 12: Elasticsearch for Data Science and Analytics with Kibana	25
Unit 13: SCADA_ICS Security 101	25
Unit 14: SCADA, ISO 27019:2017 and NIST 800-82 Connection	26
Unit 15: Payment Card Industry Data Security Standard (PCI DSS)	26
Unit 16: Data Science with Python	27
Unit 17: Vulnerability Assessment in Line with Various Frameworks	27
Unit 18: Web application Pen-Testing_Ethical Hacking in line with various frameworks	28
Unit 19: Network Pentesting and Ethical Hacking	29
Unit 20: Web Application Pen-Testing (WSTG)	29
Unit 21: Certified OT/ICS Cybersecurity Fundamentals Professional (AN-CICP)	30
Unit 22: Cybersecurity Risk Assessment Professional (AN-CRAP)	31
Unit 23: Operational Technology Design Specialist (AN-OTDS)	31
Unit 24: Operational Technology Maintenance Specialist (AN-OTMS)	31
COPYRIGHT NOTICE	32
Unauthorized Use Prohibited	32

1. About the Diploma

Our Diploma in Cloud Cyber Security an EduQual Level 3 endorsed programme built for one clear purpose: to give you the job-ready skills that today's cross-industry employers are really looking for.

You'll dive deep into a wide mix of emerging tech – we're talking Linux system admin, Python programming, information security mapped to CISSP, SCADA and industrial control systems security, offensive and defensive network pentesting, web application security, Elasticsearch for SIEM and observability, data science, PCI DSS, ISO management systems, and even the foundational maths that underpins data science.

But it's not just about technical skills. Throughout the diploma, we've woven in professional development units that help you build a sharp LinkedIn profile and prepare for the IELTS UKVI Training exam – because we know that for many learners, global career mobility is the real goal.

Everything is taught using open-source, vendor-neutral content, with a big emphasis on practical, hands-on employability. You'll learn through recorded video lectures, step-by-step practical walkthroughs, and our own cloud-based lab environment. Across all units, there are almost 1,500 hands-on labs – so you're not just reading about real-world tasks, you're actually doing them repeatedly, the same way you'd handle them in a job. And you won't be alone: trainers are right there with you in dedicated communities, forums, and live online classes, offering constant guidance and interaction.

This diploma is designed to build deep practical know-how and advanced problem-solving confidence, opening doors to global careers in areas like Cyber Security, Offensive Security, SCADA/ICS, Data Science, and Cloud Computing. You can finish the whole programme in 6 to 9 months, giving you real flexibility to move forward in your career – whether that's closer to home or on the other side of the world.

2. Key Features of the Diploma

- EduQual endorsement, a globally recognised qualification.
- Nearly 1500 hours of hands-on cloud labs integrated across all units
- Delivered through self-paced online and distance learning.
- Job description-led learning aligned with industry roles.
- 8X higher live interaction through live online classes conducted by industry experts.
- Vibrant student communities for peer support and networking.
- Professional resume building and Internship programme eligibility services through Al Razzaq Program.
- Undergraduate programme progression pathways.
- Gain full expertise in cloud environments with cloud playground's on-demand servers and specialised containers for every lab scenario

3. About the Diploma Program Endorsed by EduQual

The EduQual endorsed 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 endorsement signifies that the program adheres to stringent quality standards of different and equivalent educational frameworks 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 of the Regulated Qualifications Framework (RQF), graduates may qualify for undergraduate program admission upon course completion.

Upon completion of this diploma program, students will:

- Receive one Certificate and one transcript of EduQual diploma after completion of the program.
- Eligible for Al Nafi Alumni membership and admissions in Bachelor's Degree programs.
- Apply for jobs based upon the skills of the student who does not want to take admission in college/university .

4. About Al Nafi International College

Al Nafi International College, 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 diploma programs are designed to help both students, professionals and organizations achieve their career and business objectives.

5. Program Eligibility Criteria and Application Process

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

To enrol in this diploma, individuals just need to have studied up to at least grade 10, or hold a Level 2 qualification – for example Matric, O Level, IGCSE, IB MYP, a Pearson Level 2, or any equivalent qualification.

5.1. Eligibility Criteria

To enrol in this diploma, individuals just need to have studied up to at least grade 10, or hold a Level 2 diploma – for example Matric, O Level, IGCSE, IB MYP, a Pearson Level 2, or any equivalent qualification. In addition, all learners must possess the following:

- A laptop with an average specification 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.

5.2. Application Process

After selecting the preferred payment plan, learners can begin their studies with ease as the application process comprises 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

COMPLETE KYS VERIFICATION

After payment, complete the KYS form and upload your previous qualification documents for verification. Course access will only be provided after the KYS verification process is completed successfully.

STEP 4

ADMISSION

Once your KYS have been completed and verified, immediately begin your studies. Access to the student portal might take 24 to 48 hours to verify. If there are issues in accessing the Al Nafi student portal then learners should connect with support through call, message on the number given on the website. Or either through email at support@alnafi.com

6. 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 course and labs and assessments.
- Guide about job aspects
- Guide about admission by using this diploma.
- clarify any confusion you have about the diploma program.

7. Program Outcomes

- Apply basic differential calculus techniques for optimisation and gradient descent. (Calculus for Emerging Pathways)
- Understand industry standards and best practices in cryptography, network security, risk management, software development security, and access control systems. (Certified Information System Security Professional - CISSP)
- Describe CIS security controls and explain how they protect systems and data against common cyber attacks. (CIS Top 18 Controls)
- Apply cybersecurity principles to basic scenarios involving risk management, security architecture, incident management, and access control. (Cyber Security Essentials Revisit after CISSP)
- Create dashboards and visualise data using machine learning techniques for pattern identification through hands-on exercises and labs. (Elasticsearch for Data Science and Analytics with Kibana)
- Use Elasticsearch tools for security operations and incident response through hands-on training and real-world scenarios. (Elasticsearch SOC Engineer)
- Explain how log, metric, uptime, and APM data are gathered and stored in Elasticsearch for improved system observability. (Elasticsearch Threat Hunting and Observability Engineer)
- Demonstrate basic security skills by identifying cyber threats and following incident response procedures. (Hacking 101 AKA Ethical Hacking and Incident Response Management)
- Prepare for the IELTS exam through reading, writing, listening, and speaking activities. (IELTS Academic and General Training)
- Describe international security standards and explain how security systems are implemented and assessed. (ISO 27001, 27017, 27018, Lead Implementer & Auditor)
- Apply Python programming techniques to data science tasks through hands-on practice and real-world projects. (Learn Data Science Using Python)
- Understand Linear Algebra concepts and apply techniques to solve basic problems. (Linear Algebra for Emerging Pathways)
- Use LinkedIn effectively to pursue job and freelance opportunities in emerging technologies. (LinkedIn Course for Job Seekers)
- Operate a Linux OS to automate tasks and solve routine problems, including configuration, software installation, and file management. (Linux Deep Dive)
- Use tools and techniques to identify network vulnerabilities and contribute to improved security protection. (Network Pentesting and Ethical Hacking in line with various frameworks)
- Describe the PCI DSS requirements and explain how organisations achieve compliance for secure credit card information processing. (PCI DSS Qualified Security Assessor Training)
- Understand the basics of randomness and probability theory from intuitive, mathematical, and procedural perspectives. (Probability for Emerging Pathways)
- Apply Python programming knowledge to data analysis, app development, machine learning, and code optimisation tasks. (Python Deep Dive)

- Describe alternative statistical methods and explain how they contribute to understanding modern statistics. (Real Statistics: A Radical Approach)
- Use Linux to automate tasks, solve routine problems, and support cloud computing application services. (RHEL Intensive-SysOps)
- Demonstrate hands-on techniques for preventing and detecting security incidents in SCADA environments. (SCADA Prevention & Detection a Hands-on Approach)
- Describe SCADA security standards including ISO 27019:2017 and NIST 800-82, and explain their role in protecting industrial control systems. (SCADA, ISO 27019:2017 and NIST 800-82 connection)
- Understand how industrial control systems are secured against attacks and how sensitive information is protected. (SCADA/ICS Security 101)
- Collect, analyse, and correlate security-related data from multiple sources using SIEM tools for effective threat detection and response. (SIEM the HOA starting the journey)
- Apply statistical concepts including measures of location, dispersion, estimation, hypothesis testing, regression, and correlation analysis. (Statistics for Emerging Pathways)
- Use hands-on labs to identify common web application vulnerabilities and contribute to improved security posture. (Vulnerability Assessment in line with various frameworks Code)
- Describe common web application security issues and apply best practices for securing web applications through hands-on training. (Web Application Pentesting - WSTG Labs)
- Apply hands-on web application security techniques to improve security posture and remediate vulnerabilities. (Web Application Pentesting & Ethical Hacking in line with various frameworks)

8. Who Should Enroll in this Program?

This cloud cyber security diploma is designed for:

- School, College and university students looking to gain admission in Bachelor's degree globally and/or expand their knowledge, skills, and career opportunities as well.
- Individuals looking to learn job based skills and secure employment globally.
- 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

9. Learning Path

1. LinkedIn Course for Job Seekers
2. IELTS Academic and General Training
3. Linux Deep Dive
4. Python Deep Dive
5. Certified Information System Security Professional (CISSP)
6. Cyber Security Essentials Revisit after CISSP
7. RHEL Intensive
8. CIS Top 18 Controls Hands-on Implementation
9. SIEM the HOA starting the journey
10. Elasticsearch SOC Engineer
11. Elasticsearch Threat Hunting and Observability Engineer
12. Elasticsearch for Data Science and Analytics with Kibana
13. SCADA_ICS Security 101
14. SCADA, ISO 27019_2017 and NIST 800-82 connection
15. PCI DSS Qualified Security Assessor Training
16. Learn Data Science Using Python
17. Vulnerability Assessment in line with Various Frameworks
18. Web Application Pentesting _ Ethical Hacking in line with various frameworks
19. Network Pentesting and Ethical Hacking in line with various frameworks
20. Web Application Pen Testing - WSTG
21. C1(AI Nafi Certified OT-ICS Cybersecurity Fundamentals Professional (AN-CICP))
22. C2 - AI Nafi Cybersecurity Risk Assessment Professional
23. C3 - AI Nafi Operational Technology Design Specialist– ISA/IEC 62443 (AN-OTDS)
24. C4 - AI Nafi Operational Technology Maintenance Specialist – ISA/IEC 62443 (AN-OTMS)
25. Pass all MCQs and all AI Razzaq part 1 labs given for the diploma
26. Achieve a 6.5 band or more in IELTS for UKVI
27. Attain EduQual Certificate.

10. Assessment Information

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. This section outlines the assessment framework specifically designed for students who enroll in

their EduQual diploma programs from July 2026 onwards.

10.1. Assessment Overview

Student assessments are designed to provide practical, skills-based learning experiences that reflect real-world vocational requirements across emerging technology domains.

Assessment Components

Assessment Component	Weightage	Passing Percentage Requirement
AI Razzaq Lab Assignments(part 1 only)	70%	Minimum 40%
Multiple Choice Questions (MCQs)	15%	Minimum 40%
English Language Exam	15%	Minimum IELTS 6.5 or Duolingo 115–120

Important: You must achieve a minimum of 40% in each of the AI Razzaq Lab Assignments(part 1) and MCQs exam to qualify for diploma completion. Students will have to pay for IELTS for UKVI on their own. The fee is not included in the diploma fee.

10.2. AI Razzaq Lab Assignments (70% weightage in overall Grade)

What Are They?

AI Razzaq Lab Assignments are practical, hands-on tasks divided into three phases:

Phase	Description
Basic Phase	Foundational tasks introducing core concepts and tools
Intermediate Phase	Integrated tasks requiring application of skills in scenario-based contexts
Advanced Phase	Complex, multi-step tasks simulating real-world problem-solving

These assignments are customized based on your chosen emerging technology domain (e.g., AIOps, DevSysOps, DevOps, SysOps, Cloud Advancement).

How Are They Graded?

- Assignments are submitted via the student portal.

- Graded using AI-augmented assessment tools.
- Students receive real-time feedback on their performance
- Final scores are recorded as a percentage

What If You Need to Resubmit?

Scenario	Process
First failure	You may resubmit once within 30 days of receiving your result
Second failure	You must repeat the unit with full attendance and reassessment of all phases
Lab access expires before completion	You must renew access as per the Course Access Policy
Lab assessments incomplete within two years	£100 reassessment fee applies

10.3. Multiple Choice Questions (15% of Your Grade)

Assessment Format

- Each MCQ carries 1 mark
- No negative marking for incorrect answers
- Questions include:
 - Knowledge-based
 - Scenario-based
 - Job-based
 - Critical Thinking
 - Application-based

Attempts and Scoring

Feature	Detail
Attempts	Unlimited attempts within your program access period
Final Score	Average of all attempts that meet or exceed the passing grade

Passing Requirement	Minimum 40%
Requirement	You must pass each individual assessment bank (20 MCQs each)

Diploma Program Access Period

Diploma Level	Access Period
EduQual Level 3 & 4	12 months (in total)
EduQual Level 5	15 months (in total)
EduQual Level 6	18 months (in total)

Note: If you fail to complete all MCQ assessments within your program access period, you must renew access as per the Course Access Policy.

10.4. English Language Exam (15% of Your Grade)

Mandatory Requirement

You must appear for IELTS for UKVI and score a 6.5 band or more to complete the minimum requirements of the exam.

Submission Requirements

You must submit:

- Official score report (verified link or Test Report Form)
- Valid identification matching test records
- Test date (must be within 2 years)
- Registered email used for the test

All submissions must be uploaded via the Al Nafi Student Portal or verified directly through official providers.

Verification and Compliance

Al Nafi International College reserves the right to verify scores with official test providers. Non-compliance or falsification will result in academic disciplinary action and possible program suspension or termination.

Why Is This Required?

Submission of a valid English proficiency score is required for:

- Program completion and diploma issuance
- Participation in Al Razzaq Program (employment pathways)
- Eligibility for international university admissions or work based opportunities

If you do not meet the minimum requirement, you must retake the test until the required benchmark is achieved and participate in mandatory live classes of IELTS happening weekly.

10.5. AI Razzaq Labs Program Access

Prerequisites for Lab Access

Access to AI Razzaq Labs requires completion of:

1. Enrollment in an eligible EduQual diploma program (Levels 3 to 6)
2. Know Your Student (KYS) Form submission, capturing:
 - Academic background
 - Career goals
 - Geographic preferences
 - Industry focus
3. Engagement with the program as per your selected study plan (monthly, quarterly, annual)

Lab Components

Component	Description
Course-Linked Labs	Embedded and mandatory labs directly tied to your diploma coursework
KYS-Based Personalized Labs	Customized labs tailored to your individual career and skill profile

Additional Features and Support

Every learner will benefit from:

Feature	Description
AI-Driven Internship Guidance	Personalized internship recommendations and preparation
Resume Building	ATS scoring and career coaching
Interview Preparation	AI-powered voice interview practice (coming soon)
GitHub Integration	Portfolio building and code repository integration
Skill Certification Badges	Recognition of completed competencies
Global Career Forum	Access to networking and opportunities

University Admission Assistance	Support for university applications worldwide
Visa and Work Permit Support	Assistance for 70+ countries and G20 nations
Post-Employment Services	30, 60, and 90-day post-employment support
Job Placement	Placement assistance with Fortune 500 and global companies

10.6. Grading Criteria

Final grade is determined by applying the weightage of each assessment component to the scores a student achieves. Each component's score is multiplied by its respective weightage, and the results are summed to calculate your overall grade.

Grades are awarded based on absolute grading criteria, meaning the final grade depends solely on the performance against the predefined percentage thresholds, rather than being compared to other students.

Grade Boundaries

Grade	Percentage Range
A*	90% and above
A	80% – 89%
B	70% – 79%
C	60% – 69%
D	50% – 59%
U	Below 50%

Example Calculation

For a student:

Component	Score Achieved	Weightage	Weighted Score
Lab Assignments	75%	× 70%	= 52.5%
MCQs	60%	× 15%	= 9.0%

English Exam	65%	× 15%	= 9.75%
Final Grade			71.25%

A final score of 71.25% would correspond to a Grade B.

IELTS Band Score to Percentage Conversion

The IELTS test does not have a direct, official percentage conversion. However, for the purpose of diploma, the minimum requirement is Band 6.5, and any score above 6.5 is considered as meeting and exceeding the requirement.

What Does a Band 7 Mean?

A Band 7 indicates a student is a “Good User” of English. According to IELTS:

“You have an operational command of the language, though with occasional inaccuracies, inappropriacies and misunderstandings in some situations. You generally handle complex language well and understand detailed reasoning.”

How Is Band 7 Treated for Diploma?

For English Language Exam component (15% of overall grade), the scoring works as follows:

IELTS Band	Status	Percentage Equivalent (for grading purposes)
Below 6.5	Fail	0% – Does not meet the minimum requirement
6.5	Pass (Minimum)	50%
7.0	Pass (Good)	Approximately 75%
7.5	Pass (Very Good)	Approximately 85%
8.0+	Pass (Excellent)	100%

How English Score Affects Final Grade

Since the English Exam contributes 15% to overall grade, here is how a Band 7 (≈75%) contributes:

Component	Student Score	Weightage	Weighted Contribution
English Exam	75%	× 15%	= 11.25% (out of 15%)

Example: Overall Grade Calculation

Component	Your Score	Weightage	Weighted Score
Lab Assignments	70%	× 70%	= 49.00%
MCQs	60%	× 15%	= 9.00%
English Exam	75% (Band 7)	× 15%	= 11.25%
Final Grade	C		69.25%

A final score of 69.25% would correspond to a Grade C.

Quick Reference Table

IELTS Band	Interpretation	Approx. Percentage	Weighted Contribution (15%)
6.5	Minimum Pass	50%	7.5%
7.0	Good User	75%	11.25%
7.5	Very Good User	85%	12.75%
8.0+	Excellent User	100%	15.00%

Note: The percentage equivalents above are used only for the purpose of calculating your overall diploma grade. They do not represent an official IELTS percentage conversion, as IELTS does not provide one. Any score of 6.5 or above satisfies the English proficiency requirement for your diploma.

10.7. Academic Integrity

To maintain academic integrity, the following practices are strictly prohibited:

Prohibited Practice	Description
Use of Automated Tools	Employing bots, scripts, or unauthorized software to answer MCQs or manipulate assessment platforms
Undisclosed AI-Generated Work	Passing off AI-created content as original work without proper acknowledgment or authorization
Unauthorized Assistance	Using prohibited tools, devices, or receiving help during practical exams

Violation Response

If suspected malpractice is detected:

1. Student will be formally informed in writing
2. A panel will review the evidence
3. Student will have the opportunity to respond
4. If confirmed, student may be banned from retaking the assessment and may be disqualified from the diploma program

10.8. Support for Students

The college provides comprehensive support to help students succeed:

Support Type	Description
Academic Integrity Workshops	Sessions on plagiarism prevention and ethical assessment practices
Counseling and Advising	Guidance on academic challenges and career planning
Detailed Feedback	Constructive feedback on assessments to guide improvement
AI Usage Guidance	Resources on responsible AI usage in academic work
Technical Support	Assistance with platform and technical issues via live chat or email

10.9. Accessibility and Reasonable Adjustments

The college is committed to ensuring equal access to assessments. If students have documented disabilities or special needs, they may request reasonable adjustments, including:

- Extra time
- Alternative formats
- Assistive technology
- Modified lab environments

Submit requests to: academics@alnaficoll.com

Timeline: At least 7 working days before the scheduled assessment with supporting documentation.

10.10. Appeals Process

If any student believes an assessment decision is unfair:

Step	Timeline	Action
Informal Review	Within 10 working days of receiving results	Contact academics@alnaficoll.com
Formal Appeal	Within 14 working days of informal response	Submit formal appeal with supporting evidence
Acknowledgment	Within 3 working days	Appeal is acknowledged and assigned for review
Final Decision	Within 15 working days	Impartial panel issues final written decision

Complete Course Units (24 Units)

Unit 1: LinkedIn Course for Job Seekers

Unit Objectives:

- Enable learners to effectively use LinkedIn for job searching and freelancing opportunities
- Develop skills in personal branding and content marketing on LinkedIn
- Build professional networks and identify hidden job markets
- Create an optimized LinkedIn profile that attracts recruiters and clients

Unit Curriculum:

- Understanding LinkedIn's ecosystem for job search and freelancing
 - Branding as a subject matter expert and thought leader
 - Content and keyword targeting strategies
 - About Summary optimization and content relevance
 - Networking and identifying the hidden job market
 - LinkedIn Marketplace for freelancers
 - Tools for targeting global emerging technology opportunities
 - Q&A live sessions with LinkedIn coach
 - Toolkits, worksheets, and best practice guides
-

Unit 2: IELTS Academic and General Training

Unit Objectives:

- Prepare students for the IELTS examination
- Improve reading, writing, listening, and speaking skills
- Develop strategies for attempting each section of the IELTS test
- Build confidence in English language usage for academic and general contexts

Unit Curriculum:

- Reading for gist, scanning details, and in-depth reading
 - Listening for gist, important details, and deeper meanings
 - Writing cohesive essays (argumentative, descriptive, discursive)
 - Letter writing and academic analysis of graphs, charts, and tables
 - Speaking fluently in work-based and academic scenarios
 - Everyday conversation skills in English
 - Test-taking strategies and exam techniques
-

Unit 3: Linux Deep Dive

Unit Objectives:

- Build comprehensive Linux system administration skills
- Master installation, configuration, and management
- Develop security, networking, and monitoring expertise
- Learn automation and high availability concepts

Unit Curriculum:

- Introduction and installation (virtual environment, custom partitions, hardening)
- Basic configuration (system architecture, commands, file systems, permissions)
- Bash shell scripting
- Package management with YUM/DNF
- Advanced Linux configuration (single-user mode, run levels, performance reporting)
- Linux networking (DHCP, static/dynamic IP, DNS, routing)
- Advanced disk management (partitions, LVM, file systems)
- Linux services (SSH, NFS, Samba, NTP, cron)
- Linux security (firewalld, iptables, rkhunter)
- Web, MySQL, and Squid server configuration
- High availability (bonding, teaming, failover, load balancing)

- Linux monitoring (Nagios, NRPE, Docker monitoring)
 - AI-powered automation and optimization
-

Unit 4: Python Deep Dive

Unit Objectives:

- Build deep, professional Python programming skills
- Master OOP, data structures, and advanced features
- Develop web applications, APIs, and data solutions
- Implement testing, debugging, and best practices

Unit Curriculum:

- Introduction to Python environment and setup
 - Basic syntax and operations
 - Data structures (lists, tuples, dictionaries, sets, strings)
 - Modules and packages
 - Object-Oriented Programming (classes, inheritance, polymorphism)
 - Advanced topics (decorators, generators, context managers)
 - Working with data (CSV, JSON, databases, Pandas)
 - Web development (Flask, Django, RESTful APIs)
 - Testing and debugging (unit tests, TDD)
 - Concurrency and parallelism (threading, multiprocessing, asyncio)
 - Network programming (sockets, client-server)
 - Advanced libraries and tools (regex, logging, argparse)
 - Best practices and design patterns (PEP 8)
 - Python 3.13 new features
 - Capstone project
-

Unit 5: Certified Information Systems Security Professional (CISSP)

Unit Objectives:

- Prepare learners for the CISSP certification exam
- Master all domains of the CISSP Common Body of Knowledge
- Develop expertise in security governance, risk management, and operations
- Build comprehensive understanding of security technologies and practices

Unit Curriculum:

- Security governance through principles and policies
- Personnel security and risk management concepts
- Business continuity planning
- Laws, regulations, and compliance
- Protecting security of assets
- Cryptography and symmetric key algorithms
- PKI and cryptographic applications
- Security models, design, and capabilities
- Security vulnerabilities, threats, and countermeasures

- Physical security requirements
 - Secure network architecture and components
 - Secure communications and network attacks
 - Managing identity and authentication
 - Controlling and monitoring access
 - Security assessment and testing
 - Managing security operations
 - Preventing and responding to incidents
 - Disaster recovery planning
 - Investigations and ethics
 - Software development security
 - Malicious code and application attacks
-

Unit 6: Red Hat Enterprise Linux (RHEL)

Unit Objectives:

- Install, configure, and manage Red Hat Enterprise Linux systems
- Implement security, networking, and storage solutions
- Master automation with Shell and Ansible
- Manage containers and virtualization

Unit Curriculum:

- RHEL 9 overview and architecture
 - Installation and initial setup
 - Linux fundamentals and shell
 - Software management with DNF/YUM
 - User and access control
 - Storage and file systems
 - Networking and remote access
 - Security and SELinux
 - Monitoring and performance
 - Automation with Shell and Ansible
 - Containers and Podman
 - Virtualization and high availability
-

Unit 7: Cyber Security Essentials Revisit (Post-CISSP)

Unit Objectives:

- Consolidate core cybersecurity concepts post-CISSP
- Review CyBOK (Cyber Security Body of Knowledge) domains
- Refresh understanding of governance, threats, and system protection
- Explore career opportunities after CISSP

Unit Curriculum:

- Cyber Security Body of Knowledge (CyBOK) overview
- Key questions and concepts post-CISSP

- Career opportunities after CISSP
 - CISSP concepts refresh
 - CyBOK Version 1.0 walkthrough
 - Risk management and governance
 - Law and regulation in cyber security
 - Human factors in security
 - Adversarial behavior
 - Security operations and incident management
 - Digital forensics principles
 - Cryptography basics
 - Operating systems and virtualization security
 - Distributed systems security
 - AAA (Authentication, Authorization, Accounting)
 - Secure Software Development Lifecycle
 - Software security fundamentals
 - Web and mobile security concerns
 - Cyber-physical infrastructure security
 - Network infrastructure security
 - Hardware security measures
 - Telecommunications and physical layer protection
-

Unit 8: CIS Top 18 Controls Hands-on Implementation

Unit Objectives:

- Understand and implement enterprise asset and software inventory management
- Apply data protection strategies and secure configuration baselines
- Manage accounts, access controls, and continuous vulnerability management
- Deploy audit logging, email/browser protections, and malware defenses
- Implement data recovery, network infrastructure management, and monitoring
- Develop security awareness training and service provider management
- Apply application security, incident response, and penetration testing

Unit Curriculum:

- Inventory and Control of Enterprise Assets (Introduction, Implementation, Case Study)
- Inventory and Control of Software Assets (Criticality, Management, Case Study)
- Data Protection (Implementation Pt1/Pt2, Securing Data Pt1/Pt2, Case Study)
- Secure Configuration of Enterprise Assets and Software (Introduction, Implementation, Case Study)
- Account Management (Introduction, Best Practices, Case Study)
- Access Control Management (Introduction, Best Practices, Case Study)
- Continuous Vulnerability Management (Introduction, Implementation, Case Study Pt1/Pt2)
- Audit Log Management (Introduction, Implementation, Case Study)
- Email and Web Browser Protections (Introduction, Implementation, Case Study)
- Malware Defenses (Introduction, Implementation, Case Study)

- Data Recovery (Backup Plans, Offsite Storage, Recovery Testing)
 - Network Infrastructure Management (Secure Configurations, Device Management, Segmentation)
 - Network Monitoring and Defense (Introduction Pt1/Pt2, Implementation Pt1/Pt2, Case Study)
 - Security Awareness and Skills Training (Introduction Pt1/Pt2, Implementation, Case Study)
 - Service Provider Management (Introduction Pt1/Pt2/Pt3, Implementation, Case Study)
 - Application Software Security (Introduction, Code Reviews, Case Study)
 - Incident Response Management (Introduction, Implementation, Case Study)
 - Penetration Testing (Introduction, Implementation, Case Study)
-

Unit 9: SIEM the HOA Starting the Journey

Unit Objectives:

- Understand SIEM fundamentals and architecture
- Implement event collection, correlation, and management
- Deploy intrusion detection and prevention systems
- Configure forensic data collection and reporting

Unit Curriculum:

- Introduction to SIEM (definition, core components, role in cybersecurity)
 - Benefits of SIEM and AI integration
 - Common network threats (malware, phishing, DDoS)
 - AI-enhanced threat intelligence
 - SIEM architecture and deployment
 - Event collection methods and AI-based log aggregation
 - Event correlation with AI for anomaly detection
 - Intrusion detection and prevention fundamentals
 - Machine learning-driven intrusion prevention
 - Correlation rules and alert management
 - Predictive models for early intrusion detection
 - Importance of forensic data
 - Automating forensic readiness with AI
 - Hands-on with AlienVault SIEM
 - Vulnerability scanning and network inventory
 - Introduction to Splunk and reporting
 - AI-enhanced reporting and visualization
-

Unit 10: Elastic SOC Engineer

Unit Objectives:

- Design, deploy, and manage a SOC using Elastic Stack

- Implement data ingestion, analysis, and visualization
- Develop detection rules and security dashboards
- Conduct threat hunting and incident response

Unit Curriculum:

- Introduction to SOC and SIEM
- Elastic Stack components and setup
- Data ingestion pipelines and Elastic Agents
- Fleet architecture and agent policies
- Elastic Common Schema (ECS) and logging
- Security App and AI-powered workflows
- Attack Discovery and AI Assistant
- Custom detection rules (KQL, EQL, Lucene, ES)
- Data discovery and querying in Kibana
- Data visualization and security dashboards
- Threat hunting tools and techniques
- Kill Chain methodology and adversary detection
- Case studies and hands-on scenarios

Unit 11: Elasticsearch Threat Hunting & Observability Engineer

Unit Objectives:

- Master Elastic Stack for proactive threat hunting
- Implement observability and monitoring solutions
- Develop machine learning models for threat detection
- Optimize and scale Elasticsearch deployments

Unit Curriculum:

- Introduction to threat hunting and observability
- Elasticsearch cluster setup and security
- Logstash and Beats integration
- Kibana visualization configuration
- Kibana Query Language (KQL) for threat hunting
- Threat detection with Elastic SIEM
- Custom detection rules and alerting
- Threat intelligence integration
- Security logs analysis and forensic timeline building
- Machine learning in Elasticsearch
- ML job setup and results interpretation
- Incident response and threat mitigation
- Performance tuning and scaling Elasticsearch
- Compliance requirements and best practices

Unit 12: Elasticsearch for Data Science and Analytics with Kibana

Unit Objectives:

- Master Kibana for data visualization and analysis
- Create interactive dashboards and reports
- Implement machine learning and anomaly detection
- Configure security and access controls

Unit Curriculum:

- Introduction to Kibana and ELK Stack
- Kibana interface navigation and spaces
- Working with index patterns
- Discover for querying and exploring data
- KQL and Lucene query syntax
- Data visualizations (area, line, pie, metric, heatmap)
- Dashboard creation and panel management
- Interactive filters and drill-down links
- Kibana Lens for modern data exploration
- Machine learning and anomaly detection
- Alerting and actions (Slack, Email, Webhook)
- Reporting and scheduled snapshots
- Role-Based Access Control (RBAC)
- Security, HTTPS, and TLS configurations
- Log and metrics analysis
- APM and SIEM integration
- Performance tuning and optimization

Unit 13: SCADA_ICS Security 101

Unit Objectives:

- Build foundational understanding of SCADA systems
- Understand SCADA components, architecture, and applications
- Learn SCADA security risks and mitigation strategies
- Explore AI applications in SCADA systems

Unit Curriculum:

- Understanding SCADA systems (definition, role, core components)
- Uses of SCADA (manufacturing, energy, utilities, water treatment, transportation, oil and gas)
- History of SCADA systems
- How SCADA works (OT/IT convergence, data acquisition, control, monitoring)
- Key components of SCADA architecture (RTUs, PLCs, HMI, communication infrastructure)
- Types of SCADA (monolithic, distributed, networked, web-based)

- Benefits and challenges of SCADA
 - SCADA cybersecurity (threats, attacks, mitigation)
 - Selecting the right SCADA solution
 - Integration with IoT, AI, and Big Data
 - Future trends in SCADA technology
 - AI-driven evolution in Industry 4.0
-

Unit 14: SCADA, ISO 27019:2017 and NIST 800-82 Connection

Unit Objectives:

- Understand SCADA systems and their security requirements
- Apply ISO 27019 and NIST SP 800-82 frameworks
- Implement AI-based defense mechanisms for SCADA
- Analyze SCADA logs and detect anomalies using machine learning

Unit Curriculum:

- Foundations of SCADA and cyber physical systems
 - SCADA components (Sensors, PLCs, RTUs, HMIs, Networks)
 - SCADA vs IT systems comparison
 - AI in industrial control systems
 - AI-based anomaly detection in sensor data
 - Predictive maintenance using ML models
 - Traditional security risks in SCADA
 - AI-augmented threat detection
 - Machine learning for intrusion detection
 - NIST SP 800-82r2 overview and key concepts
 - ICS vs IT security controls
 - AI-enhanced risk management
 - ISO/IEC 27019 standard for energy sector ICS
 - NLP-based compliance documentation analysis
 - AI-driven audit preparation
 - Log and traffic analysis in SCADA
 - ML models for anomaly detection in logs
 - AI-driven attack simulation for ICS
-

Unit 15: Payment Card Industry Data Security Standard (PCI DSS)

Unit Objectives:

- Understand PCI DSS requirements and compliance
- Master payment card industry ecosystem and transaction flow
- Implement security controls for cardholder data
- Conduct compliance testing and audits

Unit Curriculum:

- Introduction to the payment card industry
 - Key terminology and entities
 - Types of payment card transactions
 - Transaction data flow and lifecycle
 - EMV chip technology and contactless payments
 - Fraud prevention and data flow security
 - Relationships between organizations (merchants, processors, banks)
 - Payment card brand compliance requirements
 - PCI DSS 12 core requirements
 - Testing and validation procedures
 - Compensating controls
 - PCI hardware and communications infrastructure
 - Secure key management and HSMs
 - Compliance issues and mitigation strategies
 - PCI reporting and audits
-

Unit 16: Data Science with Python

Unit Objectives:

- Build comprehensive data science skills using Python
- Master data manipulation, visualization, and analysis
- Develop machine learning and deep learning models
- Deploy data science solutions and build portfolios

Unit Curriculum:

- Course orientation and tools setup (JupyterLab, VS Code, Git, Docker)
 - Python foundations for data science
 - Working with data (NumPy, Pandas, data cleaning)
 - Data visualization and storytelling (Matplotlib, Seaborn, Plotly, Dash)
 - Statistics and probability for data science
 - Machine learning with scikit-learn
 - Applied NLP with spaCy and NLTK
 - Time series and forecasting (ARIMA, Prophet)
 - Deep learning with TensorFlow and PyTorch
 - Data engineering and big data (Dask, PySpark, Airflow)
 - Data ethics, privacy, and open data
 - Deployment and portfolio building
 - Open-source tools and platforms
-

Unit 17: Vulnerability Assessment in Line with Various Frameworks

Unit Objectives:

- Perform vulnerability assessments across diverse environments
- Master scanning tools and techniques

- Apply risk methodologies and frameworks
- Develop comprehensive assessment reports

Unit Curriculum:

- Foundations of vulnerability assessment
- Common risks to organizations
- Security perception gap analysis
- Enterprise-level VA (IT vs OT)
- Security by design principles
- Risk assessment vs threat modeling
- Asset identification (physical and logical)
- Scanning at scale with Masscan
- Geopolitical cyber landscape
- Network and cloud awareness
- Open source recon tools
- Cyber risk methodologies (Octave, OWASP, CVSS, INFOCON)
- Vulnerability scanner ecosystem (open source vs commercial)
- Web application vs network scanning
- Infrastructure scanning and threat vectors
- Wi-Fi and IoT vulnerabilities
- VOIP and SIP protocol security
- Network mapping and firewall evasion (Nmap, NSE)
- Web vulnerability assessment with OWASP ZAP
- Web vulnerability assessment with Burp Suite
- DNS reconnaissance
- Reporting with Dradis
- Hash cracking with Hashcat

Unit 18: Web application Pen-Testing_Ethical Hacking in line with various frameworks

Unit Objectives:

- Master advanced web application attack techniques
- Identify and exploit complex vulnerabilities
- Understand authentication, injection, and server-side attacks
- Implement AI-assisted security testing

Unit Curriculum:

- Authentication attacks (enumeration, brute force, session management)
- JWT and OAuth vulnerabilities
- Multi-factor authentication bypass
- AI-based behavioral authentication detection
- Advanced SQL Injection techniques
- NoSQL and ORM Injection
- XXE and Server-Side Template Injection
- LDAP Injection attacks
- Injectics tools and labs
- AI-driven injection pattern recognition

- Insecure deserialization
 - Server-Side Request Forgery (SSRF)
 - File inclusion and path traversal
 - Race conditions and prototype pollution
 - XSS (Cross-Site Scripting) advanced techniques
 - CSRF (Cross-Site Request Forgery)
 - DOM-based attacks
 - CORS and SOP exploitation
 - HTTP request smuggling
 - HTTP/2 request smuggling
 - WebSocket smuggling
 - AI-assisted browser behavior analysis
 - HTTP protocol anomaly detection
-

Unit 19: Network Pentesting and Ethical Hacking

Unit Objectives:

- Develop network penetration testing skills
- Master industry-standard hacking tools and frameworks
- Understand exploitation techniques and post-exploitation
- Apply ethical hacking methodologies

Unit Curriculum:

- SNMP pentesting (introduction, exploitation, mitigation)
 - Information gathering with Recon-NG
 - Port scanning and subnet discovery (Masscan, Nmap)
 - OS fingerprinting and Nmap Scripting Engine (NSE)
 - Network enumeration with Netcat
 - Vulnerability scanning with Nessus
 - Exploitation with Metasploit Framework
 - Post-exploitation techniques
 - Advanced attacks with Empire Framework
 - Privilege escalation
 - Lab exercises and case studies
-

Unit 20: Web Application Pen-Testing (WSTG)

Unit Objectives:

- Master web application security testing methodologies
- Apply OWASP Testing Guide (WSTG) framework
- Identify and exploit web application vulnerabilities
- Develop penetration testing reports and remediation strategies

Unit Curriculum:

- OWASP security testing approach and techniques
- Manual inspections and reviews
- Threat modeling and balanced approach

- Security test requirements and data analysis
 - Web security testing framework
 - Security testing in SDLC
 - Information gathering and reconnaissance
 - Configuration and deployment management testing
 - Identity, authentication, and authorization testing
 - Session management testing
 - Input validation testing
 - Error handling and cryptography testing
 - Business logic testing
 - Client-side and API testing
 - Advanced SQL Injection
 - NoSQL and XXE Injection
 - Server-Side Template and LDAP Injection
 - Insecure deserialization and SSRF
 - XSS, CSRF, and DOM-based attacks
 - CORS and SOP vulnerabilities
 - HTTP request smuggling
 - AI-powered vulnerability detection
-

Unit 21: Certified OT/ICS Cybersecurity Fundamentals Professional (AN-CICP)

Unit Objectives:

- Provide comprehensive understanding of ICS and SCADA cybersecurity
- Master ISA/IEC 62443 standards and frameworks
- Develop skills in industrial networking and security controls
- Learn risk assessment and patch management for industrial systems

Unit Curriculum:

- Introduction to control systems security
 - ISA/IEC 62443 standards terminology and core concepts
 - Security levels and cybersecurity lifecycle
 - Developing Cybersecurity Management Systems (CSMS)
 - Global security frameworks and ISA99 committee
 - Industrial networking and ISO/OSI model
 - Network security and firewall applications
 - Industrial communication protocols (Modbus, OPC)
 - PCAP file analysis with Wireshark and Grass Marlin
 - Patch management for ICS environments
 - Security risk assessment for industrial system design
 - Secure product development for IACS
-

Unit 22: Cybersecurity Risk Assessment Professional (AN-CRAP)

Unit Objectives:

- Perform cybersecurity risk assessments for IACS
- Apply ISA/IEC 62443 risk assessment methodologies
- Identify vulnerabilities and evaluate consequences
- Document and report assessment findings effectively

Unit Curriculum:

- Scope determination for risk assessment
 - Asset inventory compilation and cyber criticality evaluation
 - Vulnerability identification and assessment tools
 - Consequence evaluation and operational risk matrices
 - Risk assessment methodologies and process steps
 - Documentation of assessment results
 - Comprehensive report preparation
 - Stakeholder communication
-

Unit 23: Operational Technology Design Specialist (AN-OTDS)

Unit Objectives:

- Design secure IACS following ISA/IEC 62443 lifecycle
- Develop cybersecurity requirements and conceptual designs
- Implement network segmentation and system hardening
- Conduct cybersecurity acceptance testing

Unit Curriculum:

- IACS cybersecurity lifecycle and SDL process
 - Cybersecurity Requirements Specification (CRS) development
 - Conceptual and detailed system design
 - System hardening specifications
 - OSI/ISO reference model application
 - Network segmentation and firewall configuration
 - Intrusion Detection Systems (IDS) implementation
 - Secure remote access solutions
 - Access control mechanisms
 - Cybersecurity Factory Acceptance Tests (CFAT) and Site Acceptance Tests (CSAT)
 - Integration provider responsibilities
-

Unit 24: Operational Technology Maintenance Specialist (AN-OTMS)

Unit Objectives:

- Maintain and operate IACS securely throughout their lifecycle
- Diagnose and troubleshoot network and application issues
- Implement cybersecurity operating procedures

- Develop incident response and recovery plans

Unit Curriculum:

- ICS cybersecurity lifecycle phases
 - Network diagnostics and troubleshooting
 - Application diagnostics and troubleshooting
 - IACS management of change procedures
 - Backup and restoration procedures
 - Configuration management tools
 - Patch management lifecycle and tools
 - Antivirus and whitelisting tools
 - Security incident and event monitoring (SIEM)
 - Incident response plan development
 - Cybersecurity investigations
 - System recovery processes
-

COPYRIGHT NOTICE

This document, including all content, text, images, graphics, logos, and course materials, is the exclusive property of ALNAFI E-LEARNING (PRIVATE) LIMITED.

Unauthorized Use Prohibited

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of the College.

Permitted Use

This document is provided for informational and educational purposes only. You may view, download, and print this document for personal, non-commercial use, provided that:

- All copyright and proprietary notices are retained.
 - The content is not modified or altered in any way.
-

Contact for Permissions

For permission requests or inquiries, please contact:

Where Can I find more information?

UK Office Address:

167-169 Great Portland Street 5th Floor London W1W 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**

