Datachord

# Certification Program:

# Data Science and Cybersecurity Program

by

Dr. Zul Jalil & Dr. Daniel Koh

Version 1: 10th December 2025

Version 2: 23rd December 2025

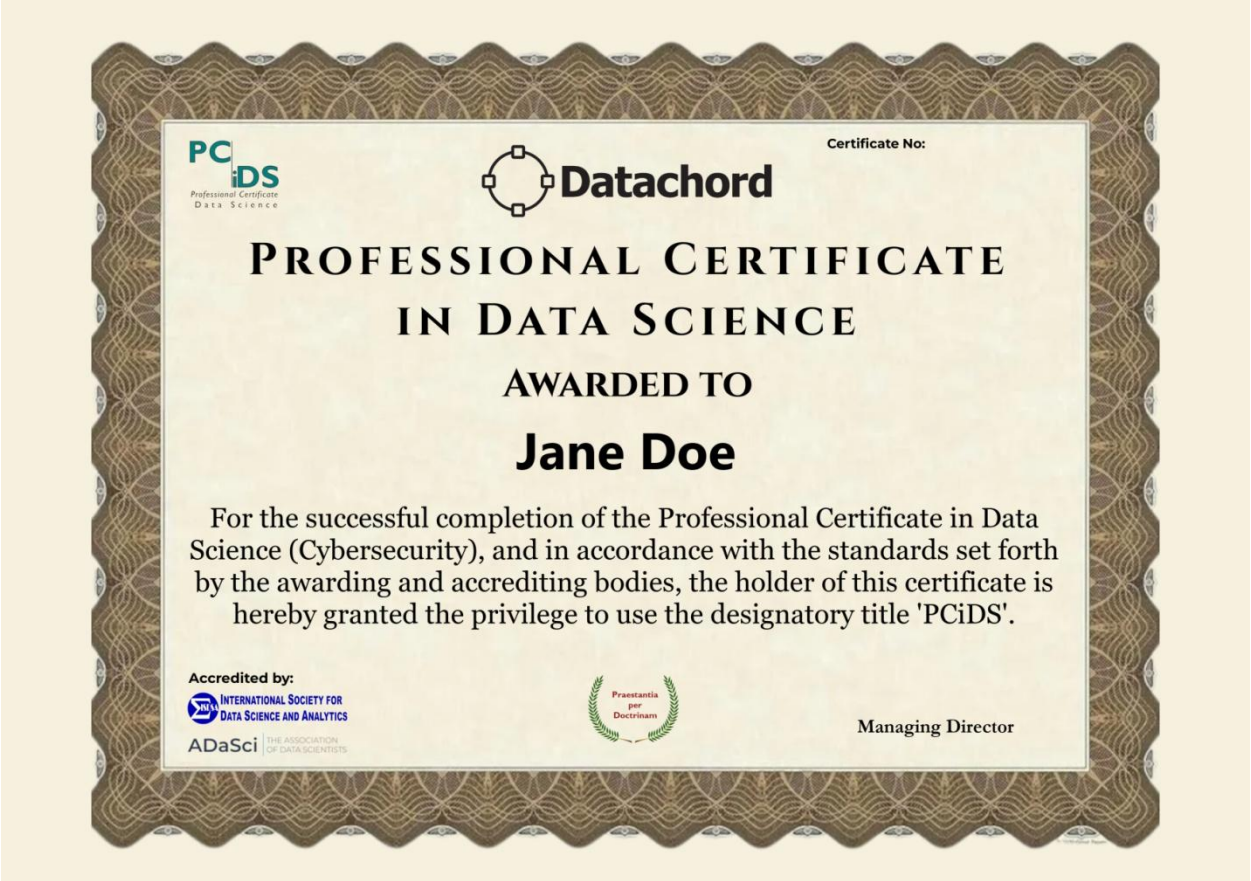
Version 3: 7th January 2026

VERSION 3

# PCiDS™ and Cybersecurity Training and Certification Program

## Contents

## Professional Certificate in Data Science (PCiDS™)




Our comprehensive, fully accredited certification program is designed for professionals seeking to excel at the intersection of data science and real-world applications. Through a structured series of interactive modules, self-directed learning hours, and a capstone project module supported by Canvas LMS, you will gain deep, hands-on knowledge spanning foundational principles in artificial intelligence and data science to advanced domain-specific techniques such as analytics, visualization, modeling, and decision-making—tailored to today's rapidly evolving digital landscape.

Based on early outcomes, 87% of trainees who complete the Professional Certificate in Data Science (PCiDS™) achieve career advancement or secure employment within six months, leveraging the data-driven skills acquired through this upskilling program.

The PCiDS™ certification is globally recognized and supported by international accreditation bodies, an expert assessment panel, and a network of luminary advisors, ensuring its credibility and acceptance across industries and specializations.

**Anchor Level (Foundation) – Data Science**

Course Outcome: This foundational course introduces the core concepts of Artificial Intelligence (AI), Data Science, Personal Data Protection (PDP) & Ethical Analytics, basic data integration (ETL), and fundamental Machine Learning (ML) techniques. It is designed not only to build critical technical skills but also to ensure compliance with industry regulations and quality standards required for ISO certification. The course emphasizes clear learning outcomes, practical exercises, continuous assessment, and quality documentation.

Instructor: Dr. Daniel Koh

Topics:

1. Introduction to Data Science and AI (3 hours) (Online)
    a) Learning Outcome:
        1. Articulate basic definitions and applications of AI and Data Science.
        2. Understand the steps of the Data Science lifecycle.
        3. Apply fundamental statistical concepts to real-world examples.
    b) Description: Basic understanding of the difference between data science and AI.
2. Introduction to PDPD and Ethical Analytics (3 hours) (Online)
    a) Learning Outcome:
        1. Recognize the importance of PDP in protecting individual rights and data integrity.
        2. Evaluate the impact of key data privacy regulations on organizational practices.
        3. Integrate ethical considerations into data analytics workflow.
    b) Description: Basic understanding of Privacy Law and Ethics.
3. Basic ETL Implementation for Data Science Work (6 hours) (Online)
    a) Learning Outcome:
        1. Build and execute basic ETL pipelines.
        2. Develop strategies for data cleaning and transformation to maintain data quality.

3. Implement fundamental anomaly detection techniques to secure and validate data.

b) Description: Basic know-how in extracting, transforming and loading data for cybersecurity-related datasets.

4. Understanding Machine Learning for A.I. Application (8 hours) (Online)

a) Learning Outcome:

1. Understand the complete lifecycle of an ML project and implement a basic ML pipeline.
2. Differentiate between supervised, unsupervised, and reinforcement learning techniques.
3. Apply ML algorithms to fundamental cybersecurity and data quality challenges.

b) Description: Basic understanding of supervised vs. unsupervised learning and how AI can detect vulnerabilities.

Duration: Flexible

Total Hours: 20 hours

**Intermediate Level – Data Science**

Course Outcome: This Intermediate course introduces essential concepts of graph theory—including classification, representation methods, traversal algorithms, and key graph properties—and applies these principles to real-world cybersecurity challenges. The curriculum combines theoretical instruction with hands-on lab exercises (using tools such as Python's NetworkX library) and detailed documentation to ensure quality and traceability for ISO audit compliance.

Instructor: Dr. Daniel Koh

Topics:

1. Introduction to Graph Theory (3 hours) (Online)
    a) Learning Outcome:
        1. Define key graph theory concepts and apply standard terminology.
        2. Classify and represent different types of graphs accurately.
        3. Implement basic traversal algorithms (BFS and DFS) and compute the shortest path using Dijkstra's Algorithm.
        4. Analyze and evaluate graph properties to support various computing problems.
    b) Description: Graph theory has numerous applications in cybersecurity, as it provides a robust framework for analyzing relationships and structures in networks, systems, and data. Students will get to understand the concept of Graph Theory in general.
2. Graph Theory for Cybersecurity (17 hours) (Face-to-Face)
    a) Learning Outcome:
        1. Explain the role of graph theory in analyzing complex cybersecurity scenarios.
        2. Construct both directed and undirected graphs to accurately model computer networks.
        3. Develop attack trees and graphs to represent potential cyberattacks and threat scenarios.

b) Description: Students will have the opportunity to design their own graphs in the domain of cybersecurity.

Duration: 3 Hours (Flexible) + 17 Hours (Face-to-Face)

Total Hours: 20 hours

**Advanced Level – Data Science**

Course Outcome: This course equips learners with the skills to transform complex datasets into insightful visual representations while also developing expertise in merging and analyzing cybersecurity data. The first module introduces key principles and techniques for effective data visualization, and the second module focuses on advanced data analytics tailored to cybersecurity challenges. The curriculum integrates theoretical instruction with practical hands-on exercises (using tools such as Power BI and Python) and detailed documentation to meet ISO audit compliance through traceable, well-documented processes.

Instructor: Dr. Daniel Koh

Mode: Face-to-face

1. Introduction to Data Visualization (3 hours) (Face-to-face)
    a) Learning Outcome:
        1. Define data visualization and explain its role in translating complex data into understandable insights.
        2. Identify various visualization types and select the appropriate method for different analytical scenarios.
        3. Utilize data visualization tools to create clear and interactive visual representations.
        4. Apply best practices to ensure visualizations are effective and communicate the intended messages.
    b) Description: Students have an overview of the different types of data visualization tools that can be used when it comes to joining data from various sources.
2. Data Visualization for Master and Secondary Data (17 hours) (Face-to-face)
    a) Learning Outcome:
        1. Distinguish between master and secondary data in cybersecurity, and understand their significance in a unified analytic framework.
        2. Execute ETL processes and join operations to integrate diverse cybersecurity data sources.

3. Apply statistical methods such as Markov Chains, Bayesian Inference, and Chi-Square tests to analyze cybersecurity events.
4. Develop and present comprehensive reports and dashboards that drive proactive threat management and enhance policy enforcement.

b) Description: Students have the chance to practice joining data sources together from cybersecurity tools and business data, for example.

Duration: 2 - 4 weeks instruction

Total Hours: 40 hours

**Qualifying and Certification Round**

Course Outcome: This is the final assessment for the qualification round of the Professional Certificate in Data Science (Cybersecurity). All final projects are reviewed by an Expert Assessment Panel comprising seasoned professionals with over 20 years of experience in data science.

Instructor: Dr. Daniel Koh

Mode: Online consulting

Assessors: Dr. Daniel Koh, Dr. Kathrin Kind

Topics:

1. Final Project for PCiDS™ (Cybersecurity) certification
    a. Students complete an end-to-end cybersecurity analytics project that integrates machine learning, graph theory, and applied data engineering.
    b. Deliverables include a written report, data pipeline, AI model implementation, and visualization dashboard.
2. Refer to https://datachord.sg/pcids-exam for the full set of certification requirements.

Duration: ~ 3 months (for certification)

Total Hours: 110 hours

*Data Chord Accreditation*

The International Society for Data Science and Analytics (ISDSA) is a global professional association dedicated to advancing data science through research, education, and community collaboration. ISDSA connects scholars, practitioners, and industry leaders across disciplines to promote rigorous scientific standards, foster innovation, and support the responsible use of data in solving real-world problems. Through its conferences, journals, training initiatives, and international partnerships, ISDSA provides a platform for knowledge exchange and drives progress in data-driven decision making worldwide.


The Association of Data Scientists (ADaSci) is a premier global professional body dedicated to advancing the fields of data science, machine learning, and artificial intelligence. ADaSci offers

institutional accreditation that serves as a mark of excellence, validating the quality, relevance, and industry alignment of programs, products, and services in AI, data science, and analytics. This accreditation provides organizations with global recognition, enhances credibility, ensures adherence to industry standards, and offers access to a vast network of professionals and resources. By aligning with ADaSci's rigorous accreditation standards, programs like PCiDS can demonstrate their commitment to excellence and industry relevance.

## Anchor Level (Foundation) – Cybersecurity

**Course Outcome:**
This foundational course equips learners with essential cybersecurity knowledge and practical exposure to ethical hacking concepts. Learners will understand common cyber threats, how basic attacks are conducted, and how organizations detect and respond to security incidents. This level builds the confidence and technical grounding required to progress to intermediate cybersecurity training.

**Instructor:**
Dr. Zulkifli Jalil

Topics

1. **Introduction to Ethical Hacking (Online)**

- Overview of cybersecurity and ethical hacking
- Roles of ethical hackers and security professionals
- Basic attack concepts, threat landscape, and legal boundaries

2. **Footprinting and Reconnaissance (Online)**

- Information gathering concepts and techniques
- Passive and active reconnaissance methods
- Understanding how attackers collect publicly available data

3. **Scanning Networks (Online)**

- Network scanning fundamentals
- Identifying open ports and services
- Introduction to scanning tools such as Nmap

4. **Enumeration (Online)**

- Understanding enumeration and system information exposure
- Identifying users, services, and basic misconfigurations

5. **iLabs: Introduction to AI-Assisted Network Anomaly Detection (Online)**

- Concept of anomaly detection in cybersecurity
- Introduction to AI-assisted threat detection

- Guided labs demonstrating basic network anomaly detection
- No prior AI or programming experience required

6. **Supplementary Practical Modules (Cyb3r Foundation) – Online**

- Cybersecurity fundamentals: threats, vulnerabilities, and defenses
- Ethical hacking hands-on basics (reconnaissance and scanning)
- SOC analyst introduction: basic log analysis and alerts
- Web application security basics (OWASP Top 10 overview)
- Malware and phishing detection fundamentals

**Progression:**
Successful completion prepares learners for the **Intermediate Level – Cybersecurity** and entry-level cybersecurity or SOC-related roles.

1. *All practical activities are conducted in controlled lab environments for educational purposes only*

## Intermediate Level – Cybersecurity

**Course Outcome:**
This intermediate course builds on foundational cybersecurity knowledge and focuses on real-world attack techniques, threat analysis, and incident investigation. Learners will develop the skills to analyze vulnerabilities, understand malware behavior, detect social engineering attacks, and support Security Operations Centre (SOC) activities using practical tools and AI-assisted techniques.

**Instructor:**
Zulkifli Jalil

Topics

1. **Vulnerability Analysis (Online)**

- Understanding common vulnerabilities and weaknesses
- Introduction to vulnerability scanning and assessment concepts
- Interpreting scan results for security improvement

2. **System Hacking (Online)**

- Overview of system-level attacks and exploitation concepts
- Understanding authentication weaknesses and privilege escalation
- Ethical and controlled attack demonstrations

3. **Malware Threats (Online)**

- Types of malware and attack vectors
- Understanding malware behavior and infection methods
- Basic malware detection and analysis concepts

4. **Sniffing (Online)**

- Network traffic monitoring and packet analysis fundamentals
- Understanding how attackers intercept data
- Identifying insecure communication patterns

5. **Social Engineering (Online)**

- Common social engineering techniques and attack scenarios

- Phishing, impersonation, and manipulation tactics
- Awareness and defensive measures against human-based attacks

6. **iLabs: AI-Assisted Malware and Phishing Detection (Online)**
   **Objective:**
   Introduce practical, guided projects using basic AI tools to detect malicious activity.

- Use simple machine learning models for malware and phishing detection
- Understand AI-based anomaly detection in network traffic
- Apply AI tools in controlled lab environments
- No advanced AI background required

7. **Supplementary Practical Modules (Cyb3r Intermediate) – Online**

- SOC log investigation using real-world datasets
- Malware traffic analysis through packet inspection
- Phishing detection workflow (email headers, payloads, indicators of compromise)
- Threat hunting basics: pattern recognition and anomaly identification
- Automation with Python for basic security workflows

**Progression:**
Upon completion, learners are prepared to advance to the **Advanced Level – Cybersecurity** and support roles such as **SOC Analyst (Level 1)**, **Junior Security Analyst**, or **Cybersecurity Operations Support**.

*All practical activities are conducted in controlled lab environments for educational purposes only*

## Advanced Level – Cybersecurity

**Course Outcome:**
This advanced course focuses on hands-on penetration testing, attack simulation, and security evasion techniques used in real-world environments. Learners will gain practical experience in identifying and exploiting system and application weaknesses, automating penetration testing tasks, and producing professional security assessment outputs. This level prepares learners for advanced technical roles and professional cybersecurity certifications.

**Instructor:**
Zulkifli Jalil

### Topics

1. **Denial-of-Service Attacks (Face-to-Face)**

- Understanding DoS and DDoS attack techniques
- Impact of availability attacks on systems and networks
- Detection and mitigation concepts

2. **Session Hijacking (Face-to-Face)**

- Session management vulnerabilities
- Cookie hijacking and session fixation concepts
- Defensive controls against session-based attacks

3. **Evading IDS, Firewalls, and Honeypots (Face-to-Face)**

- Understanding intrusion detection and prevention mechanisms
- Common evasion techniques used by attackers
- Practical demonstrations in controlled environments

4. **Hacking Web Servers (Face-to-Face)**

- Web server vulnerabilities and misconfigurations
- Exploitation techniques targeting server components
- Secure configuration and hardening principles

5. **Hacking Web Applications (Face-to-Face)**

- Advanced web application attack techniques

- Authentication, authorization, and input validation flaws
- Secure coding and defensive awareness

6. **iLabs: AI-Assisted Penetration Testing Automation (Face-to-Face)**
   **Objective:**
   Provide guided, hands-on experience using AI tools to automate penetration testing tasks.

- Use AI-assisted tools for vulnerability discovery and attack simulation
- Automate common penetration testing workflows
- Understand how AI enhances efficiency in security assessments
- Simulated environments only; no live systems

7. **Supplementary Practical Modules (Cyb3r Advanced) – Face-to-Face**

- Web application attack automation using AI-assisted tools
- API security testing and automated input fuzzing
- IDS and firewall evasion techniques using pattern simulation
- Automated vulnerability reporting for SOC and management teams
- Python scripting for penetration testing automation and workflow chaining

**Progression:**
Successful learners may progress to the **Expert Level – Cybersecurity** or pursue roles such as **Junior Penetration Tester**, **Security Engineer**, or **Advanced SOC Analyst**.

*All practical activities are conducted in controlled lab environments for educational purposes only*

## Expert Level – Cybersecurity

**Course Outcome:**
This expert-level course is designed for experienced cybersecurity practitioners seeking advanced specialization in modern attack surfaces and AI-driven security operations. Learners will gain deep technical insight into securing cloud, mobile, wireless, IoT, and cryptographic systems, while applying advanced AI techniques to detect, analyze, and respond to sophisticated cyber threats.

**Instructor:**
Zulkifli Jalil

Topics

1. **SQL Injection (Online)**

- Advanced SQL injection techniques and exploitation scenarios
- Detection, prevention, and secure coding principles

2. **Hacking Wireless Networks (Online)**

- Wireless security standards and vulnerabilities
- Attacks on Wi-Fi authentication and encryption mechanisms

3. **Hacking Mobile Platforms (Online)**

- Mobile operating system security models
- Common mobile attack vectors and defense strategies

4. **IoT and OT Hacking (Online)**

- Security challenges in IoT and operational technology environments
- Identifying and analyzing IoT attack surfaces

5. **Cloud Computing Security (Online)**

- Cloud security architecture and shared responsibility model
- Common cloud misconfigurations and threat scenarios

6. **Cryptography (Online)**

- Cryptographic principles and real-world implementations
- Identifying weak cryptographic practices and flaws

7. **iLabs: Advanced AI-Driven Security Applications (Online)**
   **Objective:**
   Apply advanced AI techniques to secure complex environments and detect sophisticated threats.

- AI-assisted monitoring of cloud and IoT systems
- Machine learning techniques for mobile and platform security
- AI-driven analysis of cryptographic weaknesses
- Guided expert labs in controlled environments

8. **Supplementary Practical Modules (Cyb3r Expert) – Online**

- Cloud security automation and AI-driven misconfiguration detection
- IoT attack surface mapping using graph-based AI models
- Mobile threat analytics through behavioral analysis of applications
- Cryptographic weakness detection using pattern and entropy analysis
- AI-augmented red team simulations across multiple systems

**Progression:**
Completion of the Expert Level prepares learners for **advanced cybersecurity roles**, specialist certifications, and leadership pathways in areas such as **cloud security**, **red teaming**, **threat intelligence**, and **AI-driven security operations**.

*All practical activities are conducted in controlled lab environments for educational purposes only*

## Course Completion

Certifications:

1. Certificate of Completion – Preparation for Cybersecurity Exam. Issued by Cyb3r Singapore.
2. Professional Certificate in Data Science (PCiDS™) - Cybersecurity: Achieved upon completing all Data Science modules and passing the certification exam. Issued by Data Chord Pte. Ltd.; Accredited by The Association of Data Scientists.

Flexible Schedule: (*example – for Face-to-Face*)

• Cybersecurity Training:

o Working Adults: Classes from 7 PM to 10 PM on weekdays.

o Non-Working Adults: Morning or afternoon classes for 3 hours/day.

• Professional Certificate in Data Science (Cybersecurity)

o Working Adults: Classes from 7 PM to 10 PM on weekdays | Classes from 9 AM to 12 PM on weekends.

o Non-Working Adults: Morning or afternoon classes for 3 hours/day across 6 days a week.