Chương trình đào tạo cấp chứng nhận:

Data Science and Cybersecurity Program

Giảng dạy bởi

TS. Zul Jalil & TS. Daniel Koh

Phiên bản 1: ngày 10 tháng 12 năm 2025

Phiên bản 2: ngày 23 tháng 12 năm 2025

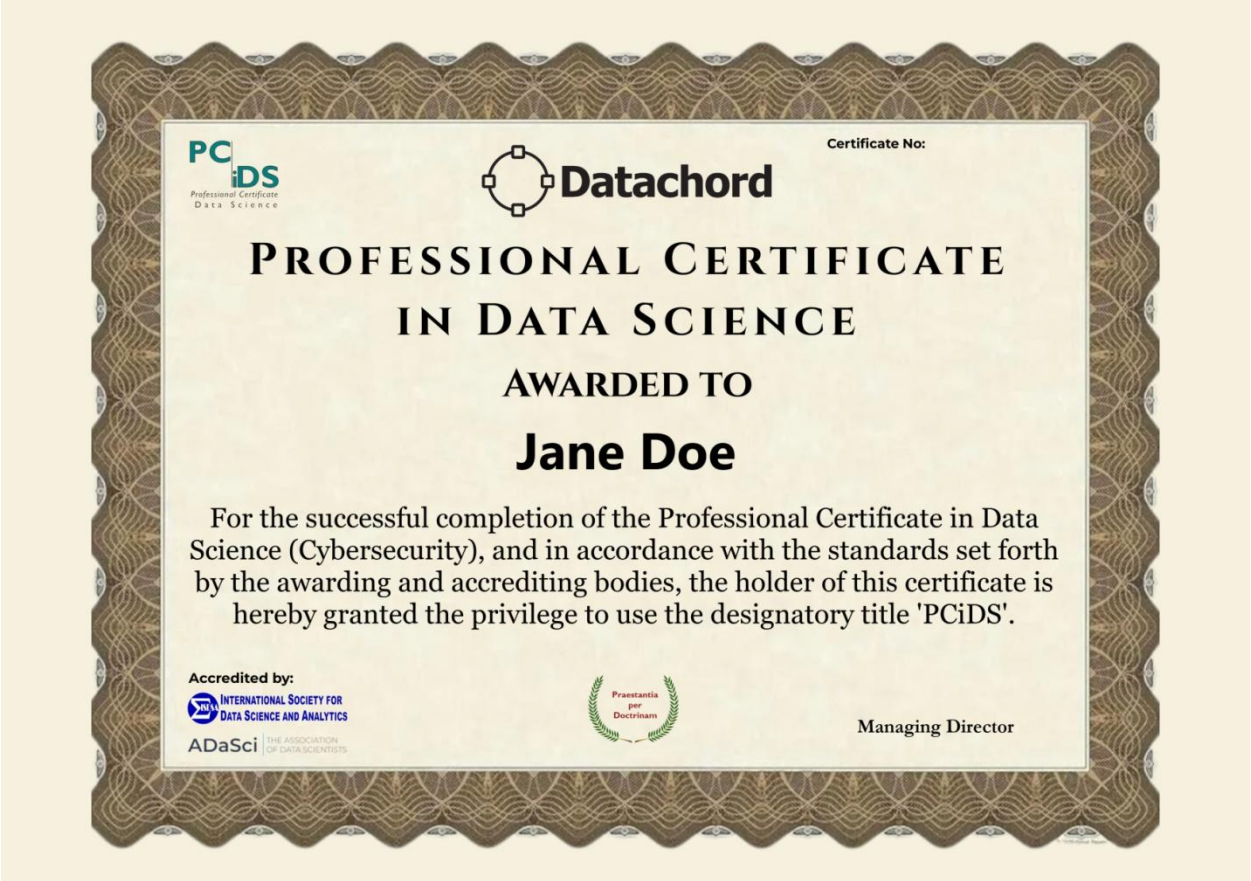
Phiên bản 3: ngày 07 tháng 01 năm 2026

PHIÊN BẢN 3

Chương trình đào tạo và chứng nhận về PCiDS™ và An ninh mạng

Nội dung chương trình

Chứng chỉ chuyên nghiệp về Khoa học Dữ liệu (PCiDS™)



Chương trình chứng nhận toàn diện, được kiểm định đầy đủ này được thiết kế dành cho các chuyên gia mong muốn phát triển năng lực chuyên sâu tại giao điểm giữa khoa học dữ liệu và các ứng dụng thực tiễn. Thông qua hệ thống mô-đun học tập có cấu trúc, các hoạt động học tập tương tác, thời lượng tự học có hướng dẫn và mô-đun đồ án tổng hợp (capstone project) được hỗ trợ bởi nền tảng Canvas LMS, học viên sẽ được trang bị kiến thức thực hành chuyên sâu, bao quát từ các nguyên lý nền tảng của trí tuệ nhân tạo và khoa học dữ liệu đến các kỹ thuật chuyên ngành nâng cao như phân tích dữ liệu, trực quan hóa, mô hình hóa và hỗ trợ ra quyết định, phù hợp với bối cảnh chuyển đổi số đang phát triển nhanh chóng hiện nay.

Theo các kết quả đánh giá ban đầu, 87% học viên hoàn thành Chứng chỉ Chuyên nghiệp về Khoa học Dữ liệu (PCiDS™) đã đạt được sự thăng tiến trong sự nghiệp hoặc tìm được việc làm trong vòng sáu tháng, nhờ vận dụng hiệu quả các năng lực dựa trên dữ liệu được hình thành thông qua chương trình nâng cao kỹ năng này.

Chứng chỉ PCiDS™ được công nhận trên phạm vi toàn cầu, với sự bảo trợ của các tổ chức kiểm định quốc tế, hội đồng đánh giá chuyên gia và mạng lưới các cố vấn uy tín, qua đó bảo đảm tính tin cậy, giá trị học thuật và mức độ chấp nhận rộng rãi trong nhiều lĩnh vực và chuyên ngành khác nhau.

Cấp độ Nền tảng (Anchor Level) – Khoa học Dữ liệu

Chuẩn đầu ra khóa học (Course Outcome):

Khóa học nền tảng này giới thiệu các khái niệm cốt lõi về Trí tuệ nhân tạo (AI), Khoa học Dữ liệu, Bảo vệ Dữ liệu Cá nhân (PDP) và Phân tích dữ liệu có đạo đức, các kỹ thuật tích hợp dữ liệu cơ bản (ETL), cùng những nguyên lý nền tảng của Học máy (Machine Learning – ML). Khóa học được thiết kế không chỉ nhằm hình thành các năng lực kỹ thuật thiết yếu mà còn bảo đảm sự tuân thủ các quy định của ngành và các tiêu chuẩn chất lượng phục vụ cho chứng nhận ISO. Nội dung khóa học chú trọng xác định rõ chuẩn đầu ra học tập, tăng cường thực hành ứng dụng, đánh giá liên tục và xây dựng hệ thống tài liệu chất lượng.

Giảng viên: TS. Daniel Koh

Nội dung khóa học

1. Giới thiệu về Khoa học Dữ liệu và Trí tuệ Nhân tạo (3 giờ) – Học trực tuyến
    a) Chuẩn đầu ra học tập:
        1. Trình bày được các khái niệm cơ bản và ứng dụng của AI và Khoa học Dữ liệu.
        2. Hiểu và mô tả được các bước trong vòng đời của Khoa học Dữ liệu.
        3. Vận dụng các khái niệm thống kê cơ bản vào các ví dụ thực tiễn.
    b) Mô tả: Cung cấp kiến thức nền tảng nhằm phân biệt sự khác nhau giữa Khoa học Dữ liệu và Trí tuệ Nhân tạo.
2. Giới thiệu về PDPD và Phân tích Dữ liệu có Đạo đức (3 giờ) – Học trực tuyến
    a) Chuẩn đầu ra học tập:
        1. Nhận thức được tầm quan trọng của bảo vệ dữ liệu cá nhân trong việc bảo đảm quyền cá nhân và tính toàn vẹn của dữ liệu.
        2. Đánh giá được tác động của các quy định pháp lý trọng yếu về quyền riêng tư dữ liệu đối với hoạt động của tổ chức.
        3. Tích hợp các yếu tố đạo đức vào quy trình phân tích dữ liệu.
    b) Mô tả: Trang bị hiểu biết cơ bản về pháp luật liên quan đến quyền riêng tư và các nguyên tắc đạo đức trong phân tích dữ liệu.

3. Triển khai ETL Cơ bản cho Công việc Khoa học Dữ liệu (6 giờ) – Học trực tuyến
    a) Chuẩn đầu ra học tập:
        1. Xây dựng và thực thi các quy trình ETL cơ bản.
        2. Phát triển các chiến lược làm sạch và chuyển đổi dữ liệu nhằm bảo đảm chất lượng dữ liệu.
        3. Áp dụng các kỹ thuật phát hiện bất thường ở mức cơ bản để bảo mật và xác thực dữ liệu.
    b) Mô tả: Cung cấp kiến thức và kỹ năng cơ bản về trích xuất, chuyển đổi và nạp dữ liệu, đặc biệt đối với các bộ dữ liệu liên quan đến an ninh mạng.
4. 4. Tổng quan về Học máy trong Ứng dụng Trí tuệ Nhân tạo (8 giờ) – Học trực tuyến
    a) Chuẩn đầu ra học tập:
        1. Hiểu được vòng đời đầy đủ của một dự án học máy và triển khai được một quy trình ML cơ bản.
        2. Phân biệt được các phương pháp học có giám sát, không giám sát và học tăng cường.
        3. Vận dụng các thuật toán học máy để giải quyết các bài toán cơ bản về an ninh mạng và chất lượng dữ liệu.
    b) Mô tả: Trang bị kiến thức nền tảng về học có giám sát và không giám sát, cũng như cách AI được ứng dụng trong việc phát hiện lỗ hổng.

Thời lượng: Linh hoạt

Tổng thời gian học: 20 giờ

Cấp độ Trung cấp (Intermediate Level) – Khoa học Dữ liệu

Chuẩn đầu ra khóa học (Course Outcome):

Khóa học ở cấp độ trung cấp này giới thiệu các khái niệm thiết yếu của lý thuyết đồ thị, bao gồm phân loại đồ thị, phương pháp biểu diễn, các thuật toán duyệt đồ thị và những thuộc tính quan trọng của đồ thị; đồng thời vận dụng các nguyên lý này vào việc giải quyết các bài toán an ninh mạng trong thực tiễn. Chương trình đào tạo kết hợp giữa giảng dạy lý thuyết và các bài thực hành trong phòng lab (sử dụng các công cụ như thư viện NetworkX của Python), cùng với hệ thống tài liệu chi tiết nhằm bảo đảm chất lượng, khả năng truy xuất và đáp ứng yêu cầu kiểm toán theo tiêu chuẩn ISO.

Giảng viên: TS. Daniel Koh

Nội dung khóa học

1. Giới thiệu về Lý thuyết Đồ thị (3 giờ) – Học trực tuyến
    a) Chuẩn đầu ra học tập:
        1. Định nghĩa và sử dụng đúng các khái niệm, thuật ngữ cốt lõi của lý thuyết đồ thị.
        2. Phân loại và biểu diễn chính xác các dạng đồ thị khác nhau.
        3. Triển khai các thuật toán duyệt đồ thị cơ bản (BFS, DFS) và tính toán đường đi ngắn nhất bằng thuật toán Dijkstra.
        4. Phân tích và đánh giá các thuộc tính của đồ thị nhằm hỗ trợ giải quyết các bài toán trong lĩnh vực máy tính.
    b) Mô tả: Lý thuyết đồ thị có nhiều ứng dụng trong lĩnh vực an ninh mạng, cung cấp khung phân tích hiệu quả cho các mối quan hệ và cấu trúc trong mạng, hệ thống và dữ liệu. Học viên sẽ được trang bị kiến thức tổng quan và nền tảng về lý thuyết đồ thị.
2. Ứng dụng Lý thuyết Đồ thị trong An ninh mạng (17 giờ) – Học trực tiếp
    a) Chuẩn đầu ra học tập:
        1. Giải thích được vai trò của lý thuyết đồ thị trong việc phân tích các kịch bản an ninh mạng phức tạp.

2. Xây dựng các đồ thị có hướng và vô hướng để mô hình hóa chính xác mạng máy tính.
3. Phát triển các cây tấn công (attack trees) và đồ thị tấn công nhằm biểu diễn các kịch bản và mối đe dọa an ninh mạng tiềm ẩn.

b) Mô tả: Học viên có cơ hội thiết kế và xây dựng các mô hình đồ thị của riêng mình trong bối cảnh an ninh mạng, qua đó tăng cường năng lực phân tích và ứng dụng thực tiễn.

Thời lượng: 3 giờ (linh hoạt) + 17 giờ (học trực tiếp)

Tổng thời gian học: 20 giờ

Cấp độ Nâng cao (Advanced Level) – Khoa học Dữ liệu

Chuẩn đầu ra khóa học (Course Outcome):

Khóa học này trang bị cho học viên năng lực chuyển đổi các tập dữ liệu phức tạp thành các biểu diễn trực quan có giá trị phân tích cao, đồng thời phát triển chuyên môn trong việc tích hợp và phân tích dữ liệu an ninh mạng. Mô-đun thứ nhất tập trung giới thiệu các nguyên lý và kỹ thuật cốt lõi của trực quan hóa dữ liệu hiệu quả; mô-đun thứ hai đi sâu vào các phương pháp phân tích dữ liệu nâng cao, được thiết kế chuyên biệt để giải quyết các thách thức trong lĩnh vực an ninh mạng. Chương trình đào tạo kết hợp chặt chẽ giữa lý thuyết và thực hành ứng dụng (sử dụng các công cụ như Power BI và Python), cùng với hệ thống tài liệu chi tiết nhằm đáp ứng yêu cầu kiểm toán ISO thông qua các quy trình có khả năng truy xuất và được chuẩn hóa.

Giảng viên: TS. Daniel Koh

Hình thức đào tạo: Học trực tiếp (Face-to-face)

Nội dung khóa học

1. Giới thiệu về Trực quan hóa Dữ liệu (3 giờ) – Học trực tiếp
    a) Chuẩn đầu ra học tập:
        1. Định nghĩa được khái niệm trực quan hóa dữ liệu và giải thích vai trò của nó trong việc chuyển tải dữ liệu phức tạp thành các thông tin dễ hiểu.
        2. Nhận diện các loại hình trực quan hóa khác nhau và lựa chọn phương pháp phù hợp cho từng bối cảnh phân tích.
        3. Sử dụng các công cụ trực quan hóa dữ liệu để xây dựng các biểu đồ, báo cáo trực quan rõ ràng và có tính tương tác.
        4. Vận dụng các nguyên tắc và thông lệ tốt nhất nhằm bảo đảm các sản phẩm trực quan hóa truyền tải đúng và hiệu quả thông điệp phân tích.
    b) Mô tả: Cung cấp cho học viên cái nhìn tổng quan về các công cụ trực quan hóa dữ liệu, đặc biệt trong bối cảnh tích hợp dữ liệu từ nhiều nguồn khác nhau.
2. Trực quan hóa Dữ liệu cho Dữ liệu Gốc và Dữ liệu Thứ cấp (17 giờ) – Học trực tiếp
    a) Chuẩn đầu ra học tập:

1. Phân biệt được dữ liệu gốc (master data) và dữ liệu thứ cấp (secondary data) trong an ninh mạng, cũng như vai trò của chúng trong một khung phân tích thống nhất.
2. Thực hiện các quy trình ETL và các phép nối dữ liệu nhằm tích hợp đa dạng nguồn dữ liệu an ninh mạng.
3. Áp dụng các phương pháp thống kê như Chuỗi Markov, Suy luận Bayes và kiểm định Chi-bình phương để phân tích các sự kiện an ninh mạng.
4. Xây dựng và trình bày các báo cáo, bảng điều khiển (dashboard) tổng hợp nhằm hỗ trợ quản lý mối đe dọa chủ động và tăng cường hiệu quả thực thi chính sách.

b) Mô tả: Học viên có cơ hội thực hành tích hợp và kết nối các nguồn dữ liệu đến từ các công cụ an ninh mạng và dữ liệu nghiệp vụ, qua đó nâng cao năng lực phân tích và trực quan hóa dữ liệu trong bối cảnh thực tiễn.

Thời gian đào tạo: 2 – 4 tuần

Tổng thời lượng: 40 giờ

Vòng Đánh giá và Cấp Chứng nhận (Qualifying and Certification Round)

Chuẩn đầu ra khóa học (Course Outcome):

Đây là giai đoạn đánh giá cuối cùng trong quy trình xét cấp Chứng chỉ Chuyên nghiệp về Khoa học Dữ liệu (An ninh mạng) – PCiDS™. Toàn bộ các đồ án tốt nghiệp được thẩm định bởi Hội đồng Đánh giá Chuyên gia, gồm các chuyên gia giàu kinh nghiệm với trên 20 năm hoạt động trong lĩnh vực khoa học dữ liệu, nhằm bảo đảm tính học thuật, tính ứng dụng và chuẩn mực nghề nghiệp của chương trình.

Giảng viên hướng dẫn: TS. Daniel Koh

Hình thức: Tư vấn trực tuyến (Online consulting)

Giám khảo: TS. Daniel Koh, TS. Kathrin Kind

Nội dung đánh giá

1. Đồ án tốt nghiệp để cấp chứng nhận PCiDS™ (An ninh mạng)
    a) Học viên thực hiện một dự án phân tích an ninh mạng tổng thể (end-to-end), tích hợp các nội dung: học máy, lý thuyết đồ thị và kỹ thuật dữ liệu ứng dụng.
    b) Sản phẩm đánh giá bao gồm: báo cáo viết, quy trình xử lý dữ liệu (data pipeline), triển khai mô hình AI và bảng điều khiển trực quan hóa dữ liệu (dashboard).
2. Tham khảo đầy đủ các yêu cầu cấp chứng nhận tại: https://datachord.sg/pcids-exam

Thời gian thực hiện: Khoảng 3 tháng (để cấp chứng nhận)

Tổng thời lượng: 110 giờ

Kiểm định chất lượng Data Chord

Hiệp hội Quốc tế về Khoa học Dữ liệu và Phân tích (ISDSA) là một tổ chức nghề nghiệp toàn cầu, hoạt động với sứ mệnh thúc đẩy sự phát triển của khoa học dữ liệu thông qua nghiên cứu, giáo dục và hợp tác cộng đồng. ISDSA kết nối các học giả, chuyên gia thực hành và các nhà lãnh đạo ngành đến từ nhiều lĩnh vực khác nhau nhằm thúc đẩy các chuẩn mực khoa học nghiêm ngặt, khuyến khích đổi mới sáng tạo và hỗ trợ việc sử dụng dữ liệu một cách có trách nhiệm trong giải quyết các vấn đề thực tiễn. Thông qua các hội nghị, tạp chí khoa học, chương trình đào tạo và mạng lưới hợp tác quốc tế, ISDSA cung cấp một diễn đàn trao đổi tri thức, đồng thời góp phần thúc đẩy tiến bộ trong quá trình ra quyết định dựa trên dữ liệu trên phạm vi toàn cầu.

Hiệp hội Các Nhà Khoa học Dữ liệu (Association of Data Scientists – ADaSci) là một tổ chức nghề nghiệp hàng đầu trên phạm vi toàn cầu, hoạt động với mục tiêu thúc đẩy sự phát triển của các lĩnh vực khoa học dữ liệu, học máy và trí tuệ nhân tạo. ADaSci cung cấp hoạt động kiểm định chất lượng cho tổ chức, được xem là dấu chứng nhận uy tín, nhằm xác nhận chất lượng, tính cập

nhật và mức độ gắn kết với nhu cầu ngành của các chương trình, sản phẩm và dịch vụ trong lĩnh vực AI, khoa học dữ liệu và phân tích. Việc được kiểm định bởi ADaSci mang lại cho các tổ chức sự công nhận quốc tế, nâng cao uy tín học thuật và nghề nghiệp, bảo đảm tuân thủ các chuẩn mực của ngành, đồng thời mở rộng khả năng tiếp cận mạng lưới chuyên gia và nguồn lực toàn cầu. Thông qua việc đáp ứng các tiêu chuẩn kiểm định nghiêm ngặt của ADaSci, các chương trình như PCiDS™ có thể khẳng định cam kết về chất lượng, tính xuất sắc và mức độ phù hợp với yêu cầu thực tiễn của ngành.

Cấp độ Nền tảng (Anchor Level) – An ninh mạng

Chuẩn đầu ra khóa học (Course Outcome):

Khóa học nền tảng này trang bị cho người học những kiến thức cốt lõi về an ninh mạng và trải nghiệm thực hành ban đầu đối với các khái niệm liên quan đến tấn công có đạo đức (ethical hacking). Người học sẽ hiểu được các mối đe dọa an ninh mạng phổ biến, cách thức các cuộc tấn công cơ bản được thực hiện, cũng như phương pháp mà tổ chức phát hiện và ứng phó với các sự cố an toàn thông tin. Cấp độ này nhằm xây dựng nền tảng kỹ thuật và sự tự tin cần thiết để người học tiếp tục tham gia các khóa đào tạo an ninh mạng ở trình độ trung cấp.

Giảng viên:

TS. Zulkifli Jalil

Nội dung khóa học

1. **Giới thiệu về Tấn công có Đạo đức (Ethical Hacking) – Học trực tuyến**

- Tổng quan về an ninh mạng và tấn công có đạo đức.
- Vai trò của chuyên gia tấn công có đạo đức và các chuyên gia an ninh thông tin.
- Các khái niệm tấn công cơ bản, bức tranh tổng thể về mối đe dọa và các giới hạn pháp lý.

2. **Thu thập Dấu vết và Trinh sát (Footprinting & Reconnaissance) – Học trực tuyến**

- Các khái niệm và kỹ thuật thu thập thông tin.
- Phương pháp trinh sát thụ động và chủ động.
- Hiểu cách kẻ tấn công khai thác các thông tin công khai sẵn có.

3. **Quét Mạng (Scanning Networks) – Học trực tuyến**

- Nguyên lý cơ bản của hoạt động quét mạng.
- Xác định các cổng mở và dịch vụ đang hoạt động.
- Giới thiệu các công cụ quét mạng như Nmap.

4. **Liệt kê Thông tin (Enumeration) – Học trực tuyến**

- Khái niệm về liệt kê thông tin và mức độ lộ lọt thông tin hệ thống.

- Xác định người dùng, dịch vụ và các cấu hình sai cơ bản.

5. iLabs: Giới thiệu Phát hiện Bất thường Mạng có Hỗ trợ AI – Học trực tuyến

- Khái niệm phát hiện bất thường trong an ninh mạng.
- Giới thiệu phương pháp phát hiện mối đe dọa có sự hỗ trợ của trí tuệ nhân tạo.
- Thực hành có hướng dẫn về phát hiện bất thường mạng ở mức cơ bản.
- Không yêu cầu kiến thức nền về AI hoặc lập trình.

6. Các Mô-đun Thực hành Bổ trợ (Cyb3r Foundation) – Học trực tuyến

- Nền tảng an ninh mạng: mối đe dọa, lỗ hổng và biện pháp phòng vệ.
- Thực hành cơ bản về tấn công có đạo đức (trinh sát và quét hệ thống).
- Giới thiệu vai trò chuyên viên SOC: phân tích log và cảnh báo ở mức cơ bản.
- Kiến thức nền về an ninh ứng dụng web (tổng quan OWASP Top 10).
- Cơ sở phát hiện mã độc và tấn công lừa đảo (phishing).

Lộ trình phát triển (Progression):

Hoàn thành khóa học sẽ giúp người học đủ điều kiện tiếp tục tham gia **Cấp độ Trung cấp – An ninh mạng,** đồng thời sẵn sàng cho các vị trí an ninh mạng hoặc SOC ở cấp độ đầu vào.

Lưu ý: Tất cả các hoạt động thực hành được triển khai trong môi trường phòng lab được kiểm soát chặt chẽ và chỉ phục vụ mục đích đào tạo.

Cấp độ Trung cấp (Intermediate Level) – An ninh mạng

Chuẩn đầu ra khóa học (Course Outcome):

Khóa học an ninh mạng ở cấp độ trung cấp này được xây dựng trên nền tảng kiến thức cơ bản, tập trung vào các kỹ thuật tấn công trong môi trường thực tế, phân tích mối đe dọa và điều tra sự cố an toàn thông tin. Người học sẽ phát triển năng lực phân tích lỗ hổng, hiểu hành vi của mã độc, phát hiện các hình thức tấn công kỹ nghệ xã hội, đồng thời hỗ trợ các hoạt động của Trung tâm Điều hành An ninh (Security Operations Centre – SOC) thông qua việc sử dụng các công cụ thực hành và kỹ thuật có hỗ trợ của trí tuệ nhân tạo.

Giảng viên:
Zulkifli Jalil

Nội dung khóa học

1. **Phân tích Lỗ hổng (Vulnerability Analysis) – Học trực tuyến**

- Nhận diện các lỗ hổng và điểm yếu an ninh phổ biến trong hệ thống.
- Giới thiệu các khái niệm về quét và đánh giá lỗ hổng.
- Phân tích và diễn giải kết quả quét nhằm đề xuất các biện pháp cải thiện an ninh.

2. **Tấn công Hệ thống (System Hacking) – Học trực tuyến**

- Tổng quan về các hình thức tấn công ở cấp độ hệ thống và khái niệm khai thác lỗ hổng.
- Hiểu các điểm yếu trong cơ chế xác thực và leo thang đặc quyền.
- Trình diễn các kịch bản tấn công có đạo đức trong môi trường kiểm soát.

3. **Mối đe dọa Mã độc (Malware Threats) – Học trực tuyến**

- Phân loại mã độc và các con đường tấn công phổ biến.
- Phân tích hành vi mã độc và phương thức lây nhiễm.
- Các khái niệm cơ bản về phát hiện và phân tích mã độc.

4. **Nghe lén và Phân tích Lưu lượng (Sniffing) – Học trực tuyến**

- Nguyên lý giám sát lưu lượng mạng và phân tích gói tin.

- Hiểu cách thức kẻ tấn công thu thập và chặn dữ liệu truyền trên mạng.
- Nhận diện các mô hình giao tiếp không an toàn.

5. Kỹ nghệ Xã hội (Social Engineering) – Học trực tuyến

- Các kỹ thuật và kịch bản tấn công kỹ nghệ xã hội thường gặp.
- Phishing, giả mạo danh tính và các thủ thuật thao túng người dùng.
- Nâng cao nhận thức và các biện pháp phòng vệ trước các hình thức tấn công dựa trên yếu tố con người.

6. iLabs: Phát hiện Mã độc và Phishing có Hỗ trợ AI – Học trực tuyến

Mục tiêu:

Giới thiệu các dự án thực hành có hướng dẫn, sử dụng các công cụ AI cơ bản để phát hiện hoạt động độc hại.

- Ứng dụng các mô hình học máy đơn giản trong phát hiện mã độc và phishing.
- Hiểu nguyên lý phát hiện bất thường dựa trên AI trong lưu lượng mạng.
- Thực hành sử dụng công cụ AI trong môi trường phòng lab được kiểm soát.
- Không yêu cầu kiến thức chuyên sâu về AI.

7. Các Mô-đun Thực hành Bổ trợ (Cyb3r Intermediate) – Học trực tuyến

- Điều tra log SOC trên các bộ dữ liệu thực tế.
- Phân tích lưu lượng mã độc thông qua kiểm tra gói tin.
- Quy trình phát hiện phishing (phân tích header email, payload và chỉ số xâm nhập – IoC).
- Cơ sở săn tìm mối đe dọa (threat hunting): nhận dạng mẫu và phát hiện bất thường.
- Tự động hóa các quy trình an ninh cơ bản bằng Python.

Lộ trình phát triển (Progression):

Sau khi hoàn thành khóa học, người học đủ điều kiện tiếp tục tham gia **Cấp độ Nâng cao – An ninh mạng**, đồng thời sẵn sàng đảm nhiệm các vị trí như **SOC Analyst (Cấp độ 1)**, **Chuyên viên An ninh Thông tin Junior** hoặc **Nhân sự hỗ trợ vận hành an ninh mạng.**

Lưu ý: Tất cả các hoạt động thực hành được triển khai trong môi trường phòng lab được kiểm soát và chỉ phục vụ cho mục đích đào tạo.

Cấp độ Nâng cao – An ninh mạng (Advanced Level – Cybersecurity)

Chuẩn đầu ra của khóa học (Course Outcome):

Khóa học nâng cao này tập trung vào thực hành kiểm thử xâm nhập (penetration testing), mô phỏng tấn công và các kỹ thuật né tránh hệ thống bảo mật trong môi trường thực tế. Người học sẽ được trang bị kinh nghiệm thực tiễn trong việc phát hiện và khai thác các điểm yếu của hệ thống và ứng dụng, tự động hóa các tác vụ kiểm thử xâm nhập, đồng thời xây dựng báo cáo đánh giá an ninh chuyên nghiệp. Trình độ này chuẩn bị cho người học đảm nhiệm các vị trí kỹ thuật nâng cao và theo đuổi các chứng chỉ an ninh mạng chuyên nghiệp.

Giảng viên:
Zulkifli Jalil

Nội dung khóa học

1. **Tấn công từ chối dịch vụ – DoS/DDoS (Học trực tiếp)**

- Tổng quan về kỹ thuật tấn công DoS và DDoS
- Tác động của các cuộc tấn công làm gián đoạn tính sẵn sàng đối với hệ thống và mạng
- Các khái niệm về phát hiện và giảm thiểu tấn công

2. **Chiếm quyền phiên làm việc – Session Hijacking (Học trực tiếp)**

- Lỗ hổng trong quản lý phiên làm việc
- Các khái niệm về đánh cắp cookie và cố định phiên (session fixation)
- Biện pháp phòng vệ trước các tấn công dựa trên phiên

3. **Né tránh IDS, Tường lửa và Honeypot (Học trực tiếp)**

- Cơ chế phát hiện và ngăn chặn xâm nhập
- Các kỹ thuật né tránh phổ biến được kẻ tấn công sử dụng
- Minh họa thực hành trong môi trường kiểm soát

4. **Tấn công máy chủ Web (Học trực tiếp)**

- Lỗ hổng và cấu hình sai trên máy chủ web
- Kỹ thuật khai thác nhắm vào các thành phần của máy chủ
- Nguyên tắc cấu hình an toàn và gia cố hệ thống

5. **Tấn công ứng dụng Web (Học trực tiếp)**

- Các kỹ thuật tấn công nâng cao đối với ứng dụng web
- Lỗi trong xác thực, phân quyền và kiểm tra dữ liệu đầu vào
- Nhận thức về lập trình an toàn và biện pháp phòng thủ

6. **iLabs: Tự động hóa kiểm thử xâm nhập với sự hỗ trợ của AI (Học trực tiếp)**

Mục tiêu:

Cung cấp trải nghiệm thực hành có hướng dẫn trong việc sử dụng công cụ AI để tự động hóa các tác vụ kiểm thử xâm nhập.

- Sử dụng công cụ hỗ trợ AI để phát hiện lỗ hổng và mô phỏng tấn công
- Tự động hóa các quy trình kiểm thử xâm nhập phổ biến
- Hiểu cách AI nâng cao hiệu quả trong đánh giá an ninh
- Chỉ thực hiện trong môi trường mô phỏng; không áp dụng trên hệ thống đang vận hành thực tế

7. **Các mô-đun thực hành bổ trợ (Cyb3r Advanced) – Học trực tiếp**

- Tự động hóa tấn công ứng dụng web bằng công cụ hỗ trợ AI
- Kiểm thử an ninh API và tự động fuzzing dữ liệu đầu vào
- Kỹ thuật né tránh IDS và tường lửa thông qua mô phỏng mẫu
- Tự động hóa báo cáo lỗ hổng phục vụ SOC và đội ngũ quản lý
- Lập trình Python để tự động hóa kiểm thử xâm nhập và liên kết quy trình làm việc

Lộ trình phát triển (Progression):

Người học hoàn thành tốt có thể tiếp tục học lên **Trình độ Chuyên gia – An ninh mạng (Expert Level – Cybersecurity)** hoặc đảm nhiệm các vị trí như **Penetration Tester sơ cấp**, **Kỹ sư An ninh**, hoặc **Chuyên viên SOC nâng cao**.

Lưu ý: Toàn bộ các hoạt động thực hành được triển khai trong môi trường phòng thí nghiệm kiểm soát, chỉ phục vụ mục đích đào tạo.

Cấp độ Chuyên gia (Expert Level) – An ninh mạng

Chuẩn đầu ra khóa học (Course Outcome):

Khóa học an ninh mạng ở cấp độ Chuyên gia được thiết kế dành cho các chuyên gia an ninh mạng đã có kinh nghiệm, có nhu cầu phát triển chuyên môn sâu trong việc bảo vệ các bề mặt tấn công hiện đại và vận hành an ninh dựa trên trí tuệ nhân tạo. Người học sẽ được trang bị kiến thức kỹ thuật chuyên sâu về bảo mật hệ thống điện toán đám mây, nền tảng di động, mạng không dây, IoT/OT và mật mã học; đồng thời áp dụng các kỹ thuật AI tiên tiến để phát hiện, phân tích và ứng phó với các mối đe dọa an ninh mạng ở mức độ phức tạp cao.

Giảng viên:

Zulkifli Jalil

Nội dung khóa học

1. **1. Tấn công SQL Injection – Học trực tuyến**

- Các kỹ thuật SQL Injection nâng cao và các kịch bản khai thác trong thực tế.
- Phương pháp phát hiện, phòng ngừa và các nguyên tắc lập trình an toàn.

2. **2. Tấn công Mạng Không dây – Học trực tuyến**

- Các chuẩn bảo mật không dây và các lỗ hổng liên quan.
- Phân tích các hình thức tấn công vào cơ chế xác thực và mã hóa Wi-Fi.

3. **3. Tấn công Nền tảng Di động – Học trực tuyến**

- Mô hình bảo mật của các hệ điều hành di động.
- Các vector tấn công phổ biến trên thiết bị di động và chiến lược phòng vệ.

4. **4. Tấn công IoT và OT – Học trực tuyến**

- Các thách thức về an ninh trong môi trường IoT và công nghệ vận hành (OT).
- Nhận diện và phân tích các bề mặt tấn công trong hệ sinh thái IoT.

5. **5. An ninh Điện toán Đám mây – Học trực tuyến**

- Kiến trúc an ninh đám mây và mô hình trách nhiệm chia sẻ.
- Các cấu hình sai phổ biến và kịch bản mối đe dọa trong môi trường đám mây.

6. **Mật mã học (Cryptography) – Học trực tuyến**

- Các nguyên lý mật mã và việc triển khai trong thực tiễn.
- Phát hiện các điểm yếu và sai sót trong việc áp dụng các cơ chế mật mã.

7. **iLabs: Ứng dụng An ninh Nâng cao dựa trên AI – Học trực tuyến**

Mục tiêu:

Vận dụng các kỹ thuật AI tiên tiến nhằm bảo vệ các môi trường phức tạp và phát hiện các mối đe dọa tinh vi.

- Giám sát hệ thống đám mây và IoT với sự hỗ trợ của AI.
- Ứng dụng các kỹ thuật học máy trong bảo mật nền tảng và thiết bị di động.
- Phân tích điểm yếu mật mã dựa trên AI.
- Thực hành chuyên sâu có hướng dẫn trong môi trường phòng lab được kiểm soát.

8. **Các Mô-đun Thực hành Bổ trợ (Cyb3r Expert) – Học trực tuyến**

- Tự động hóa an ninh đám mây và phát hiện cấu hình sai bằng AI.
- Lập bản đồ bề mặt tấn công IoT bằng các mô hình AI dựa trên đồ thị.
- Phân tích mối đe dọa di động thông qua phân tích hành vi ứng dụng.
- Phát hiện điểm yếu mật mã bằng phân tích mẫu và độ hỗn loạn (entropy).
- Mô phỏng hoạt động red team có tăng cường AI trên nhiều hệ thống.

Lộ trình phát triển (Progression):

Hoàn thành Cấp độ Chuyên gia – An ninh mạng giúp người học sẵn sàng **đảm nhiệm các vị trí an ninh mạng cao cấp**, theo đuổi các chứng chỉ chuyên sâu và lộ trình phát triển lãnh đạo trong các lĩnh vực như **an ninh đám mây, red teaming, tình báo mối đe dọa và vận hành an ninh dựa trên AI**.

Lưu ý: Tất cả các hoạt động thực hành được triển khai trong môi trường phòng lab được kiểm soát và chỉ phục vụ cho mục đích đào tạo.

Hoàn thành khóa học

Chứng nhận sau khi hoàn thành khóa học (Certifications):

1. Giấy chứng nhận hoàn thành khóa học – Chuẩn bị cho Kỳ thi An ninh mạng, do Cyb3r Singapore cấp.
2. Chứng chỉ Chuyên nghiệp về Khoa học Dữ liệu (PCiDS™) – An ninh mạng: Được cấp sau khi học viên hoàn thành đầy đủ các mô-đun Khoa học Dữ liệu và đạt yêu cầu trong kỳ thi chứng nhận. Chứng chỉ do Data Chord Pte. Ltd. cấp và được Hiệp hội Các Nhà Khoa học Dữ liệu (Association of Data Scientists) kiểm định chất lượng.

Thời khóa biểu linh hoạt (*ví dụ – đối với hình thức học trực tiếp*):

- Đào tạo An ninh mạng:
    - Người đi làm: Học buổi tối từ 19:00 đến 22:00 vào các ngày trong tuần.
    - Người không đi làm: Học buổi sáng hoặc buổi chiều, mỗi buổi 3 giờ/ngày.
- Chương trình Chứng chỉ Chuyên nghiệp về Khoa học Dữ liệu (An ninh mạng):
- Người đi làm: Học buổi tối từ 19:00 đến 22:00 vào các ngày trong tuần; Hoặc học cuối tuần từ 09:00 đến 12:00.
- Người không đi làm: Học buổi sáng hoặc buổi chiều, mỗi buổi 3 giờ/ngày, học liên tục 6 ngày/tuần.