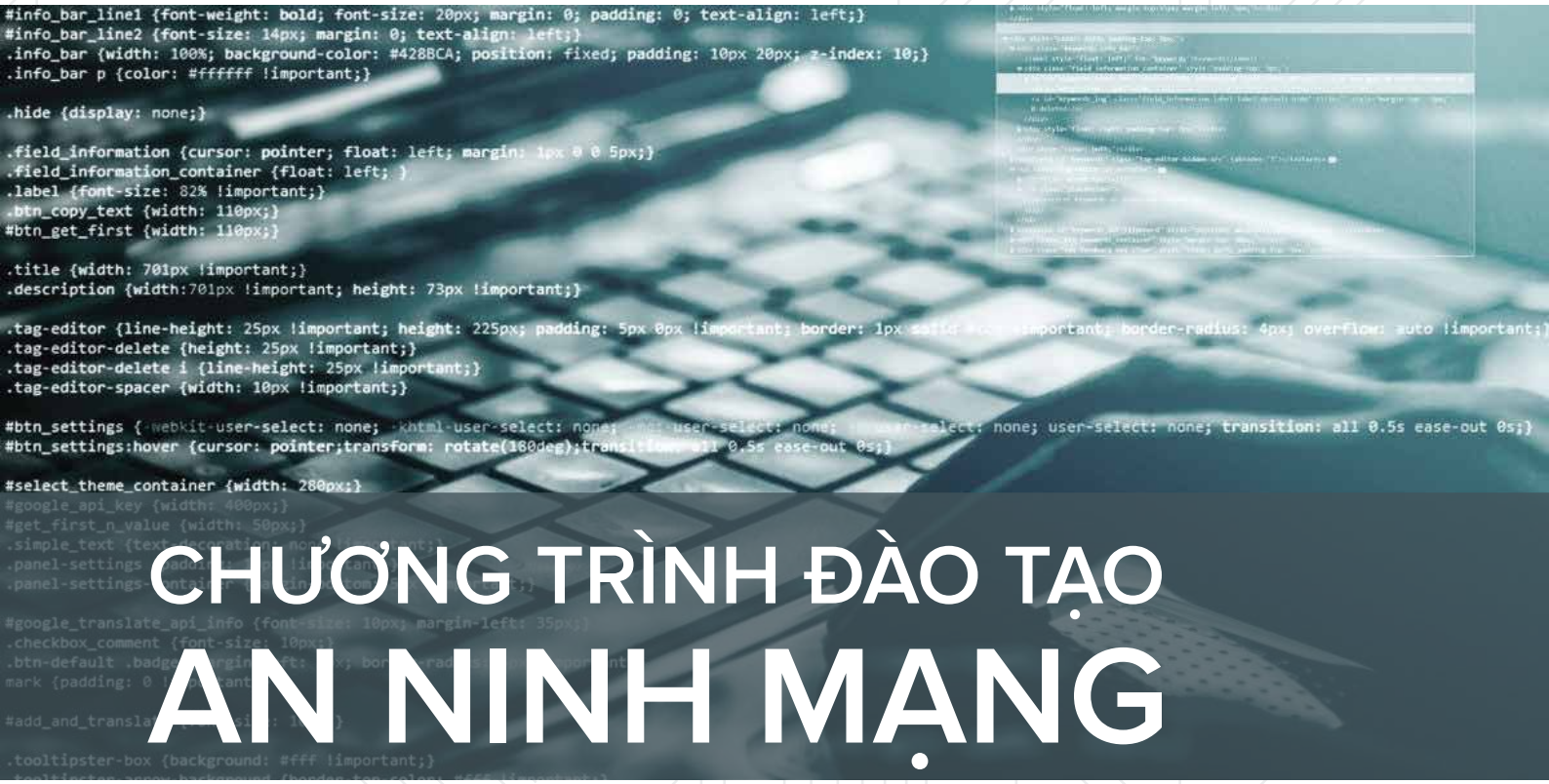
SECURITYBOX™

DỊCH VỤ AN NINH MẠNG TOÀN DIỆN



CHƯƠNG TRÌNH ĐÀO TẠO AN NINH MẠNG

GIỚI THIỆU TỔNG QUAN

Trên cơ sở các kiến thức, kinh nghiệm của **SecurityBox** trong lĩnh vực an ninh mạng, chúng tôi muốn đưa đến người học một chương trình đào tạo sáng tạo, linh hoạt.

Đào tạo nhận thức an ninh mạng đang trở thành một yêu cầu cấp thiết cho các doanh nghiệp, tổ chức khi mà nguy cơ an ninh ngày càng lớn, hình thức và phương pháp tấn công ngày càng đa dạng. Việc tăng cường đào tạo các kiến thức và kĩ năng liên quan đến các vấn đề an ninh là một thành phần quan trọng trong việc quản lí lỗ hổng và giảm thiểu rủi ro.

SecurityBox thiết kế chương trình đào tạo an ninh mạng gồm 03 cấp độ:

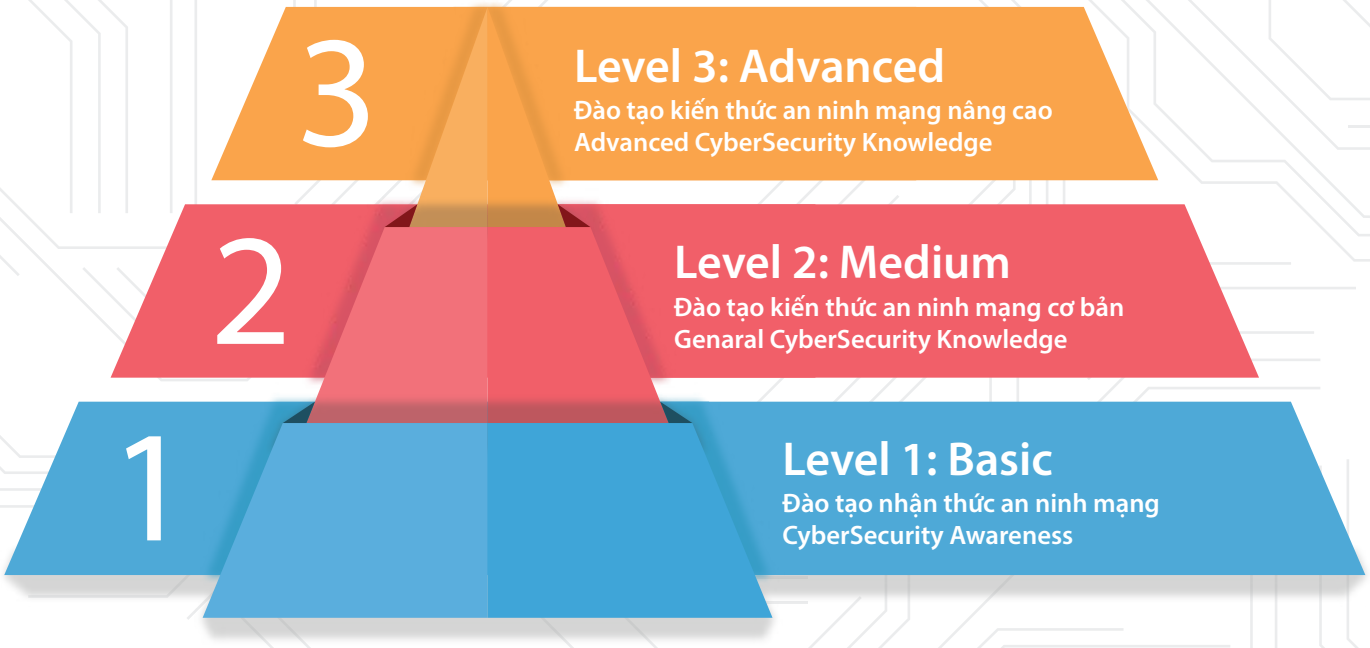
- **Cấp độ 1:** Đào tạo nhận thức an ninh mạng.
- **Cấp độ 2:** Đào tạo kiến thức an ninh mạng cơ bản.
- **Cấp độ 3:** Đào tạo kiến thức an ninh mạng nâng cao.

Bước tiếp theo, chúng ta sẽ phân tích sâu hơn theo từng cấp độ kiến thức người học sẽ học ra sao và thu được những kiến thức gì?

Cấp độ 1: Đào tạo nhận thức an ninh mạng – CyberSecurity Awareness

Cấp độ 1 phù hợp cho những người mới bắt đầu. Ở cấp độ này, người học sẽ được tiếp cận với các kiến thức cơ bản nhất, liên quan trực tiếp tới quá trình làm việc thực tế.
Nội dung đào tạo sẽ hướng tới những mục tiêu sau:

- Cung cấp những kiến thức cơ bản nhất liên quan tới vấn đề an ninh mạng.
- Giải thích nguyên nhân và cách thức ở mức tổng quan về cách thức hacker có thể xâm nhập vào hệ thống.
- Các nguy cơ và hiểm họa từ mã độc cùng với các biện pháp phòng tránh tương ứng.
- Phương pháp bảo vệ máy tính, dữ liệu và các thông tin cá nhân khi tham gia Internet.
- Phương pháp sử dụng và bảo vệ mật khẩu an toàn.
- Cách thức phòng chống lừa đảo trực tuyến trên các mạng xã hội và cách thức bảo vệ bản thân khi tham gia các mạng xã hội.
- Hệ thống quản lí an toàn thông tin – ISO 27001



Chương trình đào tạo An Ninh Mạng

Cấp độ 2: Đào tạo kiến thức an ninh mạng cơ bản – General CyberSecurity Knowledge

Cấp độ 2 hướng tới những cá nhân như: Các quản trị mạng, quản trị website, Quản lí về CNTT. Các bài học trong cấp độ này sẽ cung cấp các kiến thức liên quan tới quá trình vận hành các hệ thống công nghệ thông tin, giới thiệu các công cụ cũng như các phương pháp cơ bản để tham gia điều tra chứng cứ số hoặc phân tích mã độc ở mức tự động.

Nội dung đào tạo sẽ xoay quanh các chủ đề chính như sau:

Tổng quan về an ninh mạng: Người học sẽ nắm bắt được kiến thức cơ bản như sau:

- Sự cần thiết của an ninh mạng trong thực tiễn hoạt động của mỗi cá nhân và doanh nghiệp trên mạng Internet.
- Các phương pháp truy cập và xác thực cơ bản.
- Các phương pháp cấp quyền cho người dùng và một số phương pháp thống kê.
- Tham gia một số trường hợp thực tế về các hình thức tấn công mạng thực tế.

An ninh hạ tầng mạng: Cung cấp các kiến thức liên quan tới hạ tầng mạng:

- An ninh cho kiến trúc mạng và cấu hình luật giữa các thành phần trong mô hình mạng.
- Firewall, IDS/IPS.
- VPN, VLAN, NAT.
- An ninh kết nối, lưu trữ.
- Cân bằng tải.
- Tổng kết phương pháp an ninh cho cở sở hạ tầng mạng.

An ninh ứng dụng: Cung cấp kiến thức cơ bản liên quan tới các dịch vụ và ứng dụng:

- Dịch vụ web, email.
- Giới thiệu về lỗ hổng tràn bộ đệm – Buffer Overflow và phương pháp kiểm tra, đảm bảo an ninh cho ứng dụng và dịch vụ.

Mã độc: Học viên sẽ được tiếp cận tới 04 phần chính:

- Lịch sử và khái niệm về mã độc và virus máy tính.
- Nguyên lý hoạt động, phương pháp lây lan của các loại mã độc.
- Giải pháp tổng thể phòng chống mã độc.
- Một số case study thực tế liên quan tới quá trình xử lí mã độc.

Công cụ phân tích an ninh mạng: Phần này thiên về yếu tố thực hành khi giới thiệu cho học viên các công cụ hữu hiệu sử dụng trong quá trình kiểm tra và phân tích an ninh mạng:

- Kiểm tra kết nối trên máy tính.
- Thực hiện quét cổng, dịch vụ.
- Giám sát và phân tích dữ liệu mạng.
- Rà quét và kiểm tra lỗ hổng máy tính.

Mật mã: Giới thiệu sơ lược kiến thức về mã hóa:

- Kiến thức căn bản về mã hóa.
- Một số giải thuật mã hóa.
- PKI.
- Các tiêu chuẩn và giao thức mã hóa.

Cấp độ 3: Đào tạo kiến thức an ninh mạng nâng cao – Advanced CyberSecurity Knowledge

Cấp độ 3: Đào tạo kiến thức an ninh mạng nâng cao – Advanced CyberSecurity Knowledge
Giai đoạn đào tạo nâng cao phù hợp cho các cá nhân muốn tham gia học tập và chọn Security là một nghề nghiệp cho bản thân.

Để tham gia vào cấp độ này, học viên cần đảm bảo có kiến thức nền tảng tương đối tốt:

- Nhận thức an ninh mạng.
- Kiến thức an ninh mạng cơ bản.
- Kĩ năng lập trình tốt, không bị giới hạn và phụ thuộc vào ngôn ngữ lập trình.

Trong cấp độ 3, chúng tôi tiếp tục chia ra 03 mảng đào tạo riêng biệt. Học viên sẽ được lựa chọn 1 trong 3 lĩnh vực đào tạo:

- Kiến thức và kĩ năng đảm bảo an ninh website.
- Điều tra chứng cứ số.
- Phân tích và dịch ngược mã độc.

KẾ HOẠCH VÀ LỊCH TRÌNH ĐÀO TẠO

SecurityBox xây dựng khung chương trình đạo tạo cho từng cấp độ kiến thức cụ thể như sau:

Cấp độ 1: Đào tạo nhận thức an ninh mạng – CyberSecurity Awareness

STT	Nội dung đào tạo	Thời gian (Ngày)
01	Kiến thức tổng quan về an ninh mạng.	0.5
02	Phương pháp bảo vệ máy tính và dữ liệu khi tham gia Internet, mạng xã hội.	0.5
03	Hệ thống quản lí an toàn thông tin – ISO 27001.	0.5
04	Thi đánh giá cuối khóa và tổng kết.	0.5

Cấp độ 2: Đào tạo kiến thức an ninh mạng cơ bản – General CyberSecurity Knowledge

STT	Nội dung đào tạo	Thời gian (Ngày)
01	Tổng quan về an ninh mạng.	1
02	An ninh hạ tầng mạng.	1.5
03	An ninh ứng dụng.	2
04	Mã độc.	0.5
05	Công cụ phân tích an ninh mạng.	2
06	Mật mã.	0.5
07	Thi đánh giá cuối khóa và tổng kết.	0.5

Cấp độ 3: Đào tạo kiến thức an ninh mạng nâng cao – Advanced CyberSecurity Knowledge

- Kiến thức và kĩ năng đảm bảo an ninh website:

STT	Nội dung đào tạo	Thời gian (Ngày)
01	Tổng quan an ninh và các cơ chế xác thực website.	1
02	Các lỗ hổng phổ biến trong ứng dụng website: XSS, CSRF, SQLinjection, BlindSQL, Remote Command Execution, File Inclusion...	15
03	An ninh trong quá trình vận hành và phòng thủ chủ động.	1
04	An ninh cho ajax và web services.	1
05	Một số kĩ thuật nâng cao.	1
06	Thi đánh giá cuối khóa và tổng kết.	2

- Điều tra chứng cứ số:

STT	Nội dung đào tạo	Thời gian (Ngày)
01	Giới thiệu tổng quan khóa học, các qui tắc khi trở thành một Điều Tra Viên.	1
02	Kiến trúc hệ thống file và phương pháp xây dựng bộ công cụ hỗ trợ.	4
03	Phương pháp thu thập và xử lí các loại dữ liệu không cố định (Volatile Data).	6
04	Phương pháp thu thập và xử lí các loại dữ liệu cố định (Persistent Data).	10
05	Thi đánh giá cuối khóa và tổng kết.	1

Phân tích và dịch ngược mã độc

STT	Nội dung đào tạo	Thời gian (Ngày)
01	Tổng quan về phân tích và dịch ngược mã độc, chuẩn bị môi trường Lab.	1
02	Kiến thức về Asembler và hệ điều hành Windows.	3
03	Định dạng PE file và một số công cụ sử dụng phân tích mã độc.	1
04	Một số trình biên dịch phổ biến: Visual Studio, MFC, Visual Basic, .NET, Delphi, GCC.	1
05	Kĩ thuật phân tích tĩnh từ cơ bản tới nâng cao.	6
06	Kĩ thuật phân tích động từ cơ bản tới nâng cao.	10
07	Tìm hiểu đặc tính của mã độc.	5
08	Các kĩ thuật chống dịch ngược.	10
09	Phân tích nâng cao: Shellcode, Driver, Rookit, Bootkit.	10
10	Thi đánh giá cuối khóa và tổng kết.	2

SECURITYBOX™

DỊCH VỤ AN NINH MẠNG TOÀN DIỆN

CÔNG TY CỔ PHẦN AN TOÀN THÔNG TIN MVS (TÊN GIAO DỊCH: MVS.,JSC)

Trụ sở chính : Tầng 9 , Số 459 Đội Cấn, Ba Đình, Hà Nội.

Chi nhánh : Số A15 Đồng Bông, phường Dịch Vọng Hậu, Cầu Giấy, Hà Nội.

Số điện thoại liên hệ: (+84)248 582 9546

Email : info@securitybox.vn

Website : www.securitybox.vn

Ra đời năm 2015 dựa trên thế mạnh nhiều năm kinh nghiệm làm việc trong lĩnh vực an ninh mạng của các kĩ sư, Công ty Cổ phần An toàn Thông tin MVS cung cấp các giải pháp và dịch vụ an ninh mạng cho các doanh nghiệp, tổ chức.

Công ty Cổ phần An toàn Thông tin MVS là một trong những Công ty an ninh mạng hàng đầu Việt Nam.

SecurityBox là một bộ phận trực thuộc Công ty Cổ phần An toàn Thông tin MVS.