OPSWAT.

CHƯƠNG TRÌNH SAU ĐẠI HỌC VỀ

An ninh mạng trong lĩnh vực cơ sở hạ tầng trọng yếu

Tổng quan về chương trình

Chương trình nghiên cứu và thực hành thực tế này mang đến cho sinh viên năm cuối/sinh viên mới tốt nghiệp cơ hội duy nhất tìm hiểu các lỗ hổng an ninh mạng trong các hệ thống hạ tầng trọng yếu và cách thức giảm thiểu tác hại của chúng trong thế giới thực.

Khi tham gia chương trình này, các bạn sẽ có cơ hội:

- Xác định và tái hiện các lỗ hổng bảo mật đã biết trong môi trường được kiểm soát, thuộc phòng thí nghiệm bảo vệ cơ sở hạ tầng trọng yếu của OPSWAT.
- Phát triển và thử nghiệm các khai thác liên quan đến các lỗ hổng bảo mật, hiểu rõ hơn về các chiến thuật và phương pháp tấn công của tin tặc.
- Thực hiện các báo cáo toàn diện bằng văn bản và nội dung trực quan (như video, hình ảnh) mô tả chi tiết các lỗ hổng bảo mật, lý do đằng sau sự xuất hiện của chúng và các tác động tiềm ẩn của chúng đối với cơ sở hạ tầng trọng yếu.
- Quét phần mềm độc hại và các lỗ hổng bảo mật đã xác định bằng cách sử dụng bộ công cụ của OPSWAT như MultiScanner, Deep CDR, Proactive DLP, Sandbox, Neuralyzer và Vulnerability Scanners, đồng thời ghi lại những phát hiện của bạn.
- Phác thảo chiến lược phòng thủ và các biện pháp bảo vệ chống lại các lỗ hổng bảo mật đã xác định và các mối đe dọa tương tự trong tương lai dựa vào kinh nghiệm thực hành và kết quả thử nghiệm của bản thân.

OPSWAT.

Cấu Trúc Chương Trình

Chương trình gồm 6 học phần như sau:

1 Xác định và tái hiện lỗ hổng bảo mật

- Khởi đầu với lỗ hổng bảo mật đã biết (sẽ được cung cấp khi thực hành)
- Tái hiện lỗ hổng bảo mật trong Phòng thí nghiệm của OPSWAT.

2 Phát triển khai thác

- Phát triển khai thác lỗ hổng bảo mật đã xác định.
- Kiểm tra và tinh chỉnh khai thác.

3 Phân tích và báo cáo

- Điều tra và ghi lại lý do tại sao lỗ hổng bảo mật xảy ra và tác động tiềm ẩn của nó đối với cơ sở hạ tầng trọng yếu.
- Ghi lại quy trình và kết quả báo cáo bằng video, hình ảnh và bằng văn bản.

4 Quét và Nhận dạng

- Sử dụng trình quét MultiScanner, Sandbox, Neuralyzer và Vulnerability của OPSWAT để quét và xác định phần mềm độc hại cũng như các lỗ hổng bảo mật.
- Ghi lại kết quả quét và phân tích của bạn.

5 Chiến lược phòng thủ

- Dựa trên những phát hiện của bạn, xây dựng chiến lược để phòng thủ đối với các lỗ hổng bảo mật được xác định và các mối đe dọa tương tự trong tương lai
- Viết báo cáo chi tiết và tạo nội dụng trực quan (sơ đồ, hình ảnh, video, v.v.) để minh hoạ chiến lược phòng vệ của mình.

6 Bài thuyết trình cuối khóa

- Tổng hợp tất cả các phát hiện, báo cáo và chiến lược của bạn thành một tài liệu và bản trình bày toàn diện.
- Trình bày công việc của bạn trước một nhóm gồm các chuyên gia an ninh mạng từ OPSWAT để nhận phản hồi và học hỏi thêm.
- Tạo video và tài liệu trực tuyến để đăng trên trang web của OPSWAT và trường Đại học của bạn.

Phúc lợi khi tham gia chương trình

- Khi tham gia chương trình, bạn sẽ có cơ hội tìm hiểu và thực hành sâu hơn về phân tích lỗ hổng bảo mật, phát triển và khai thác và các chiến lược bảo vệ an ninh mạng đối với Cơ sở hạ tầng trọng yếu. Kinh nghiệm thực tế này là vô giá, và sẽ giúp bạn xây dựng và phát triển sự nghiệp của bạn trong tương lai trong lĩnh vực An ninh mạng. Ngoài ra bạn cũng có thể đưa kết quả làm việc này vào các đề án nghiên cứu Thạc sĩ/Tiến sĩ trong tương lai.
- Cơ hội làm việc và trải nghiệm thực tế trên phòng lab của OPSWAT.
- Cơ hội tìm hiểu và phát triển nghề nghiệp ở vị trí thực tập sinh/Kỹ sư mới tại OPSWAT.

Các hỗ trợ khác:

- Trợ cấp trước thuế hàng tháng (đối với thời gian làm việc 3 ngày/tuần): 6,000,000 đồng.
- Giải thưởng cho cá nhân/team có thành tích xuất sắc.
- Chỗ gửi xe tại tòa nhà văn phòng.
- Các phúc lợi khi làm việc tại văn phòng như ăn sáng, ăn xế và các hoạt động nhân viên khác.

OPSWAT.

Yêu cầu của chương trình

- Sinh viên năm cuối/Sinh viên mới tốt nghiệp khoa An toàn An ninh mạng/Khoa học máy tính/IT yêu thích lĩnh vực An ninh mạng.
- Tiếng Anh giao tiếp tốt.
- Số lượng: nhóm khoảng 4-6 bạn mỗi đợt.
- Có thể làm việc tại văn phòng ít nhất 3 ngày/tuần (thứ hai – thứ tư – thứ sáu) trong 6 tuần liên tục.

Đợt 1
Từ 2/10/2023 đến 10/11/2023.

Đợt 2
Từ 4/12/2023 đến 19/1/2024.

Đợt 3
Từ 4/3/2024 đến 12/4/2024.

Thời gian đăng ký

- Từ nay cho đến hết ngày 15/9/2023.
- Hồ sơ đăng ký gửi qua email recvietnam@opswat.com
- Công ty sẽ liên hệ các hồ sơ được chọn.

Địa điểm làm việc

Văn phòng OPSWAT Việt Nam, tầng 17, tòa nhà Sài Gòn Giải Phóng, 436-438 Nguyễn Thị Minh Khai, Phường 5, Quận 3, TP. HCM.

OPSWAT.
Protecting the World's Critical Infrastructure

OPSWAT là công ty hàng đầu thế giới về các giải pháp an ninh mạng dành cho các hệ thống công nghệ thông tin (IT), công nghệ vận hành (OT) và điều khiển công nghiệp (ICS) của các cơ sở hạ tầng trọng yếu. Hơn 1,500 tổ chức trên toàn thế giới bao gồm các định chế tài chính, cơ quan quốc phòng, cơ sở sản xuất, nhà máy năng lượng, cơ quan hàng không vũ trụ và hệ thống giao thông đã và đang tin tưởng sử dụng các giải pháp của OPSWAT để bảo vệ tập tin và thiết bị của họ.

OPSWAT có trụ sở chính đặt tại Tampa, Florida, Mỹ và hiện có hơn 18 trụ sở trên toàn cầu. Trong đó, trụ sở tại Việt Nam là trung tâm nghiên cứu & phát triển chiến lược của OPSWAT với đội ngũ hơn 300 kỹ sư phần mềm và lập trình viên tài năng đang làm việc và phát triển sự nghiệp tại đây.

opswat.com/contact