BÀI THU HOẠCH WORKSHOP CYBERSECURITY & AI NGÀY 08/09/2021

Câu hỏi thu hoạch:

1. Nêu thuận lợi và thách thức khi sử dụng AI vào Cybersecurity. Hãy tự đưa ra và phân tích một giải pháp AI vào việc an toàn một hệ thống thông tin bất kì như: trường học, ngân hàng, y tế....
2. Hãy cho biết các giải pháp mà Workshop Cybersecurity & AI đã giới thiệu và bạn thu hoạch được gì ở mỗi diễn giả sau buổi Workshop ?

Bài làm:

Câu 1:

Thuận lợi và thách thức khi sử dụng AI vào Cybersecurity.

Thuận lợi:

- ✓ Phát hiện nhanh: Năng lực phân tích và giám sát của Aritifcla Intelligence vượt xa con người. không giống như các phương pháp xử lý thông thường, AI có cái nhìn sâu sắc thông minh: công nghệ có khả năng đối mặt với các mối đe dọa chưa biết và xây dựng chiến lược phản ứng từ đầu.
- ✓ Không có lỗi của con người: Khi các doanh nghiệp không kiểm tra các quyết định của mình bằng thuật toán thông minh, theo hướng dữ liệu, họ có nguy cơ bỏ sót một phần dữ liệu quan trọng hoặc thiếu một mẫu ẩn.
- ✓ Phản hồi nhanh: AI hoạt động trong vài giây, nhanh chóng đi qua hàng terabyte dữ liệu. Với các giải pháp bảo mật AI và ML, ngay cả các tập đoàn lớn cũng có thể phát hiện ra các mối đe dọa trong vài giây
- ✓ Tự động hóa công việc thường ngày: Các giải pháp Trí tuệ nhân tạo tiết kiệm thời gian cho đội bảo mật tập trung vào các mục tiêu chiến lược và tầm nhìn xa.
- ✓ Một cách tiếp cận thông minh cho giáo dục: Trí tuệ nhân tạo có thể được sử dụng để tích lũy và tổng hợp thông tin về các mối đe dọa lan truyền hiện tại, tạo cơ sở dữ liệu thông minh, phân loại rủi ro và ứng phó.

Thách thức:

- o Tội phạm mạng cũng hiểu biết về AI: các giải pháp AI để bảo mật cũng có thể được sử dụng bởi tin tặc.

- Các mối đe dọa trên mạng ngày càng phát triển: Vi rút và phần mềm độc hại luôn được cải thiện và thậm chí các hệ thống AI sẽ cần thiết kế lại, cải tiến và bảo trì liên tục.
- Rào cản chấp nhận cao: Có thể chỉ cần cài đặt một phần mềm sẵn sàng thay vì tốn thời gian và tiền bạc vào việc xây dựng một giải pháp AI tùy chỉnh. Tuy nhiên, tin tốt là AI ngày càng trở nên sẵn có hơn và ngay cả các doanh nghiệp nhỏ cũng có thể đủ khả năng để xây dựng một mạng nơ-ron bảo mật.

Tự đưa ra và phân tích một giải pháp AI vào việc an toàn một hệ thống thông tin bất kì như: trường học, ngân hàng, y tế:

Ví dụ trong hệ thông ngân hàng:

- Các ngân hàng có nhiều khả năng được hưởng lợi nhất từ AI là những ngân hàng có thể suy nghĩ lại về cách tiếp cận con người và quy trình. Cần phải đổi mới ở quy mô và tốc độ, đòi hỏi con người và AI để thúc đẩy hiệu quả hoạt động và quy trình. Các ứng dụng của AI sẽ tạo ra sự tăng trưởng thông qua cả trải nghiệm của khách hàng và nhân viên.
- Nghiên cứu toàn cầu về AI trong Dịch vụ Tài chính cho thấy 85% tất cả những người được hỏi hiện đang sử dụng một số hình thức AI để tăng tốc độ và hiệu quả, với 77% nói rằng đây là một trong những lĩnh vực đầu tư quan trọng nhất của họ trong tương lai.

<u>Câu 2:</u>

Các giải pháp mà Workshop Cybersecurity & AI đã giới thiệu:

1. AI học hỏi nhiều hơn theo thời gian

Như tên gọi, công nghệ AI rất thông minh và nó sử dụng khả năng của mình để cải thiện an ninh mạng theo thời gian.

Các mô hình mà mạng nơ-ron nhân tạo học được theo thời gian có thể giúp cải thiện bảo mật trong tương lai.

2. Trí tuệ nhân tạo xác định các mối đe dọa không xác định

Con người có thể không xác định được tất cả các mối đe dọa mà một công ty phải đối mặt.

Khi những kẻ tấn công thử các chiến thuật mới từ kỹ thuật xã hội tinh vi đến các cuộc tấn công bằng phần mềm độc hại, cần phải sử dụng các giải pháp hiện đại để ngăn chặn chúng.

3. AI có thể xử lý nhiều dữ liệu

Bản thân một công ty quy mô trung bình có lượng truy cập rất lớn. Điều đó có nghĩa là có rất nhiều dữ liệu được chuyển giữa khách hàng và doanh nghiệp hàng ngày. Dữ liệu này cần được bảo vệ khỏi những người và phần mềm độc hại.

AI là giải pháp tốt nhất sẽ giúp bạn phát hiện bất kỳ mối đe dọa nào được che giấu như hoạt động bình thường.

4. Quản lý lỗ hổng bảo mật tốt hơn

Quản lý lỗ hổng bảo mật là chìa khóa để đảm bảo mạng của công ty. Như đã đề cập trước đó, một công ty trung bình đối phó với nhiều mối đe dọa hàng ngày.

AI giúp bạn đánh giá hệ thống nhanh hơn so với nhân viên an ninh mạng, do đó tăng khả năng giải quyết vấn đề.

5. Bảo mật tổng thể tốt hơn

Các mối đe dọa mà các mạng kinh doanh phải đối mặt thay đổi theo thời gian. Tin tặc thay đổi chiến thuật của họ mỗi ngày.

Các mối đe dọa lớn hơn có thể khiến bảo mật trở thành thách thức là do lỗi và sơ suất của con người. Giải pháp ở đây là triển khai AI trên mạng của bạn để phát hiện tất cả các loại tấn công và giúp bạn ưu tiên và ngăn chặn chúng.

6. Giảm các quy trình trùng lặp

Như đã đề cập trước đó, những kẻ tấn công thay đổi chiến thuật của họ thường xuyên. Tuy nhiên, các phương pháp hay nhất về bảo mật cơ bản vẫn giống nhau hàng ngày.

AI, trong khi bắt chước những phẩm chất tốt nhất của con người và loại bỏ những thiếu sót, xử lý các quy trình an ninh mạng trùng lặp có thể gây khó khăn cho nhân viên an ninh mạng.

7. Tăng tốc thời gian phát hiện và phản hồi

Phát hiện mối đe dọa là bước khởi đầu của việc bảo vệ mạng của công ty bạn. Sẽ là tốt nhất nếu bạn nhanh chóng phát hiện ra những thứ như dữ liệu không đáng tin cậy.

AI quét toàn bộ hệ thống của bạn và kiểm tra mọi mối đe dọa có thể xảy ra. Không giống như con người, AI sẽ xác định các mối đe dọa cực kỳ sớm và đơn giản hóa các nhiệm vụ bảo mật.

8. Bảo mật xác thực

Lớp bảo mật bổ sung sẽ đảm bảo rằng khách truy cập của bạn được an toàn khi duyệt qua mạng của bạn.

AI sử dụng các công cụ khác nhau như nhận dạng khuôn mặt, CAPTCHA và máy quét vân tay trong số những công cụ khác để nhận dạng.

Khi kẻ tấn công xâm nhập vào tài khoản người dùng, toàn bộ mạng của bạn có thể gặp rủi ro.

Thu hoạch được ở mỗi diễn giả sau buổi Workshop:

Bảo mật dữ liệu và mạng không phải là điều dễ dàng trong môi trường kinh doanh ngày nay. Có thể thực hiện một bước quyết định để trở nên an toàn hơn bằng cách áp dụng AI để tăng cường cơ sở hạ tầng bảo mật của mình. Có một số lợi ích của việc sử dụng AI cho bảo mật doanh nghiệp và rất sớm thôi trí tuệ nhân tạo sẽ trở thành một phần không thể thiếu của an ninh mạng doanh nghiệp.