5 Mẹo để bảo vệ chu kỳ của Vùng chứa

Đến khi bạn bắt đầu nghĩ đến bảo vệ vòng chu kỳ của vùng chứa, đã có nhiều bộ phận luôn luân chuyển để theo dõi thời gian của chúng trước và trong thời gian hoạt động. Đây có thể là một công việc mất công sức. Vậy thì bắt đầu từ đây để tìm được cách tiếp cận vấn đề này tốt nhất? Sau đây là 5 điểm bạn cần lưu ý:

• Độ tin cậy của điểm đăng ký

> Chỉ cho phép triển khai từ điểm đăng kí tin cậy, hoặc tốt hơn, từ trong vùng chứa. Đừng cho phép nhân sự từ bên ngoài lấy hình ảnh không được kiểm tra, công khai mà chưa được quét.

• Cần trọng vùng chứa không được ưu tiên

> Bất cứ khi nào có thể, chỉ cho phép vùng chứa không được ưu tiên chạy mà không được kết nối trực tiếp với máy chủ. Về cơ bản, chỉ cho kết nối khi công việc yêu cầu.

• Bảo mật phân lớp là tốt nhất

> Kết hợp các chiến thuật bảo mật cấu tạo vùng chứa trước khi đến bảo mật vùng chứa thời gian thực để có bảo vệ toàn diện, hữu dụng.

> Kiểm tra hình ảnh để tìm phần mềm độc hại, tài liệu mật và lỗ hổng gói mã nguồn mở đồng thời cung cấp bảo vệ thời gian thực ở cấp độ cụm Kubernetes® và liên tục quét hình ảnh điểm đăng kí để tìm mối đe dọa mới.

• Tích hợp là chìa khóa thành công

> Tiếp nhận và phát triển phương thức bảo vệ tốt nhất cho tổ chức của bạn bằng cách tích hợp bảo vệ vùng chứa với công cụ hiện có.

> Kiểm tra và quét hình ảnh để tìm lỗi khi đang được cấu tạo (Nếu bạn sử dụng phương thức CI/CD). Việc này dễ hơn nhiều so với sửa lỗi trong quá trình cấu tạo trước khi cho chạy.

> Tránh lỗi bảo mật trước khi chạy bằng cách cho triển khai kiểm soát khi hình ảnh chạy sang cụm thời gian hoạt động, cũng như tối ưu hóa các chiến thuật, như là kiểm soát quyền đăng nhập, tại cấp cụm để đảm bảo được bảo vệ.

> Giảm gánh nặng khi triển khai bằng cách ban hành bảo mật vùng chứa với phương thức riêng như Helm.

• Thu hẹp bề mặt tấn công

> Thiết lập nền tảng vững chắc bằng cách xây dựng ứng dụng của bạn sau khi được quét, tăng độ bền hình ảnh vùng chứa. Hoặc nếu có thể, hãy sử dụng distroless container images. mới.
> Sử dụng các chiến thuật này để giảm khả năng bị tấn công của bạn. Nhất là khi bạn cho chạy các khái niệm mới như distroless images, nó có thể làm hẹp hình ảnh để chỉ cho phép tài nguyên phụ thuộc và các gói mà ứng dụng cần để hoạt động.

Trend Micro cam kết cung cấp giải pháp để hỗ trợ các nỗ lực trên. Nếu bạn đang tìm kiếm một giải pháp tích hợp bao gồm cả 5 điều chủ chốt của bảo mật vùng chứa, hãy tham khảo Trend Micro Cloud One™ – Container Security. Nền tảng này kết hợp 3 lĩnh vực chính như liên tục quét hình ảnh vùng chứa ở cả điểm đăng kí và quy trình cấu tạo, kiểm soát đăng nhập vùng chứa đến cụm Kubernetes của bạn, cũng như bảo mật thời gian thực tại cấp cụm. Bắt đầu trải nghiệm bảo mật vùng chứa ngay hôm nay tại dùng **thử Trend Micro Cloud One™ miễn phí**

#TrendTips

Biên dịch bởi Thanh Hiền - Iworld.com.vn

PACISOFT.vn

TREND MICRO™