CyStack

DATA SHEET

Security Monitoring

Giám sát liên tục và bảo vệ tài sản số doanh nghiệp

Bối cảnh

Security Monitoring, hay giám sát bảo mật, là một yếu tố quan trọng trong các khâu vận hành kinh doanh hiện đại. Security Monitoring giúp các tổ chức bảo vệ tài sản số và đảm bảo an ninh mạng cũng như bảo mật hệ thống.

Ngày nay, các doanh nghiệp phụ thuộc rất lớn vào dữ liệu số để vận hành. Dữ liệu này có tính nhạy cảm cao, chứa thông tin mật của doanh nghiệp, các báo cáo tài chính và dữ liệu cá nhân của khách hàng cũng như nhân viên của doanh nghiệp. Các tổ chức bởi vậy phải đối diện với các mối đe dọa tiềm tàng từ những kẻ tấn công sẵn sàng dùng mọi chiến thuật, kỹ thuật, quy trình để phá hoại hệ thống và đánh cắp dữ liệu. Với Security Monitoring, các tổ chức sẽ phát hiện, phản ứng kịp thời trước các cuộc tấn công, hạn chế ảnh hưởng và giúp ngăn chặn lộ lọt dữ liệu.

Việc tuân thủ các điều luật và tiêu chuẩn liên ngành cũng là một lý do lớn khiến Security Monitoring trở nên rất quan trọng trong các doanh nghiệp. Rất nhiều ngành nghề và quốc gia có những quy định yêu cầu các doanh nghiệp phải triển khai và duy trì các biện pháp bảo mật mạnh, bao gồm Security Monitoring. Những quy định này bao gồm các bộ luật bảo vệ dữ liệu như Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu (GDPR), hoặc các tiêu chuẩn trong ngành công nghiệp thẻ thanh toán như PCI DSS. Các tổ chức không đảm bảo tuân thủ những quy định này có khả năng chịu những án phạt tài chính đáng kể và hủy hoại uy tín doanh nghiệp.

Thêm vào đó, Security Monitoring giúp các tổ chức có góc nhìn toàn vẹn để đánh giá tình trạng bảo mật hiện tại, xác định các vấn đề cần cải thiện và triển khai các biện pháp bảo mật tốt nhất để giảm thiểu rủi ro xảy ra tấn công mạng.

Lợi ích của khách hàng

- Tình trạng an ninh mạng được cải thiện thông qua việc giám sát và phân tích liên tục
- Tuân thủ chặt chẽ các quy định bảo mật
- Liên tục cải thiện với các công nghệ mới nhất
- Yên tâm khi các hệ thống và dữ liệu luôn được bảo vệ trước các sự cố an ninh mạng
- Được làm việc với đội ngũ các chuyên gia bảo mật dày dặn kinh nghiệm trong việc đảm bảo an toàn an ninh mạng và các hệ thống

Giải pháp của CyStack

Đội ngũ chuyên gia CyStack là những kỹ sư bảo mật tài năng và dày dặn kinh nghiệm trong giám sát an ninh mạng, hiểu rõ các mối đe dọa bảo mật và công nghệ mới nhất giúp các doanh nghiệp triển khai Security Monitoring.

CyStack cung cấp một giải pháp tổng hợp bao gồm ứng cứu sự cố và các dịch vụ giám sát liên tục bằng các công cụ và phương pháp luận hiện đại để giúp doanh nghiệp luôn duy trì trạng thái bảo mật tối ưu nhất. Với cách thức tiếp cận của được thiết kế linh hoạt và dễ mở rộng, giải pháp này đảm bảo đáp ứng nhu cầu của doanh nghiệp ở các quy mô và yêu cầu bảo mật khác nhau.

Phương pháp luận

Phương pháp triển khai Security Monitoring của CyStack luôn toàn vẹn và thông qua nhiều bước tiếp cận, giúp các doanh nghiệp bảo vệ tài sản số và đảm bảo bảo mật mạng và hệ thống. Phương pháp của CyStack bao gồm các bước sau:

1. **Đánh giá**: Trong quá trình đánh giá, đội ngũ CyStack xem xét thực trạng an ninh mạng hiện tại của doanh nghiệp, bao gồm hạ tầng an ninh sẵn có, cấu hình mạng, các chính sách và quy trình bảo mật thông tin. Bước này cung cấp góc nhìn toàn vẹn về tình trạng an ninh mạng của doanh nghiệp và giúp xác định các thiếu sót bảo mật cần khắc phục.
2. **Thiết kế**: Dựa vào bước đánh giá trên, các chuyên gia sẽ thiết kế gói Security Monitoring đáp ứng nhu cầu cụ thể của doanh nghiệp. Quá trình này bao gồm việc chọn ra các công nghệ bảo mật thích hợp, như tường lửa, hệ thống phát hiện xâm nhập và các giải pháp quản lý log. Kế hoạch giám sát và các yêu cầu về báo cáo cũng được thống nhất trong bước này.
3. **Triển khai**: Đội ngũ CyStack triển khai các công nghệ bảo mật và tiến hành gói giám sát. Bước này bao gồm việc cài đặt các cảm biến bảo mật, cấu hình các giải pháp quản lý log và cài đặt giám sát thời gian thực. Đội ngũ chuyên gia ngoài ra sẽ thiết lập các kênh liên lạc để phản ứng hiệu quả và tối ưu trước sự cố bảo mật.
4. **Giám sát**: Hoạt động giám sát mạng và hệ thống của doanh nghiệp liên tục, sử dụng đa dạng các công cụ và kỹ thuật để phát hiện và phản ứng trước các sự cố bảo mật kịp thời nhất. Việc này bao gồm giám sát thời gian thực, phân tích log và threat intelligence. Đội ngũ chuyên gia cũng xem xét các báo cáo bảo mật và cập nhật gói giám sát bảo mật nếu cần thiết để giải quyết các mối đe dọa mới và gần đây nhất.
5. **Ứng cứu sự cố**: Trong tình huống xảy ra sự cố bảo mật, đội ngũ CyStack sẽ nhanh chóng xác định gốc rễ vấn đề để xảy ra sự cố, ngăn chặn sự cố trở nên nghiêm trọng hơn và giải quyết các vấn đề liên quan. Đội ngũ chuyên gia sẽ liên hệ với doanh nghiệp thường xuyên để cung cấp các cập nhật liên tục về tình trạng của sự cố và các thao tác phù hợp đã được tiến hành để ngăn chặn sự cố tương tự xảy ra trong tương lai..
6. **Báo cáo**: Các chuyên gia CyStack cung cấp các báo cáo bảo mật định kỳ cho doanh nghiệp. Trong báo cáo sẽ mô tả chi tiết các sự cố bảo mật đã được phát hiện, các công việc đã được tiến hành để khắc phục các sự cố này, và đánh giá tổng thể tình trạng bảo mật của doanh nghiệp. Các báo cáo này sẽ giúp khách hàng hiểu rõ thực trạng an ninh mạng trong hệ thống của họ và cung cấp góc nhìn khách quan về tính hiệu quả của hạ tầng an ninh của họ.
7. **Liên tục cải thiện**: Đội ngũ CyStack liên tục cải thiện, thường xuyên cập nhật gói Security Monitoring và tích hợp các công nghệ bảo mật mới nhất để đảm bảo cung cấp các dịch vụ quản lý giám sát an ninh mạng hiệu quả nhất. Đội ngũ cũng hỗ trợ đào tạo và luôn chủ động thông báo cho doanh nghiệp về các mối đe dọa bảo mật và biện pháp bảo mật gần đây nhất.

Tính năng chính

- Đánh giá toàn diện
- Gói giám sát thiết kế riêng cho từng khách hàng và sát nhu cầu thực tế
- Triển khai với các công nghệ bảo mật vượt bậc nhất
- Giám sát và phân tích log thời gian thực
- Threat Intelligence, thu thập từ nhiều nguồn và phát hiện sớm các mối đe dọa
- Ứng cứu sự cố

Các loại hình Security Monitoring

CyStack cung cấp các loại hình Security Monitoring sau:

- **Network Security Monitoring**, hay giám sát bảo mật mạng: bao gồm việc giám sát hạ tầng mạng, bao gồm các server, router, switch và tường lửa, được thiết kế để phát hiện và ngăn chặn các sự cố bảo mật, ví dụ như các cuộc tấn công xâm nhập, truy cập trái phép và lộ lọt dữ liệu. Để đạt được hiệu quả trên, gói giám sát bảo mật mạng sử dụng rất nhiều các công nghệ, bao gồm các hệ thống phát hiện xâm nhập (NIDS), hệ thống phòng chống xâm nhập (NIPS), tường lửa và các ứng dụng khác.
- **Endpoint Security Monitoring**, hay giám sát bảo mật thiết bị đầu cuối: bao gồm việc giám sát thiết bị đầu cuối cá nhân, ví dụ như máy tính xách tay, máy tính để bàn và các thiết bị di động, được thiết kế để phát hiện và ngăn chặn các sự cố bảo mật, như lây nhiễm các phần mềm độc hại, truy cập trái phép và lộ lọt dữ liệu. Để đạt được hiệu quả trên, gói giám sát bảo mật thiết bị đầu cuối sử dụng rất nhiều các công nghệ, như phần mềm chống virus, tường lửa và các ứng dụng khác.
- **Application Security Monitoring**, hay giám sát bảo mật ứng dụng: Hình thức này bao gồm việc giám sát các ứng dụng và các hệ thống phần mềm, được thiết kế để phát hiện và ngăn chặn các sự cố bảo mật, như các lỗ hổng phần mềm, truy cập trái phép và lộ lọt dữ liệu. Để đạt được hiệu quả trên, gói giám sát bảo mật ứng dụng dùng rất nhiều các công nghệ, như tường lửa ứng dụng web (WAF), phần mềm rà quét lỗ hổng bảo mật và các ứng dụng khác.
- **Cloud Security Monitoring**, hay giám sát bảo mật điện toán đám mây: Hình thức này bao gồm việc giám sát hạ tầng và các ứng dụng triển khai trên nền tảng điện toán đám mây, được thiết kế để phát hiện và ngăn chặn các sự cố bảo mật, như truy cập trái phép, lộ lọt dữ liệu và cấu hình thiếu an toàn. Để đạt được các hiệu quả trên, gói giám sát bảo mật điện toán đám mây sử dụng rất nhiều các công nghệ, bao gồm công cụ quản lý tình trạng an ninh nền tảng điện toán đám mây (CSPM), hệ thống quản lý thông tin và sự kiện bảo mật (SIEM) và các ứng dụng khác.
- **Database Security Monitoring**, hay giám sát bảo mật cơ sở dữ liệu: Hình thức này bao gồm việc giám sát các cơ sở dữ liệu và các kho lưu trữ dữ liệu, được thiết kế để phát hiện và ngăn chặn các sự cố bảo mật, như truy cập trái phép, lộ lọt và đánh cắp dữ liệu. Để đạt được hiệu quả trên, gói giám sát bảo mật cơ sở dữ liệu sử dụng rất nhiều các công nghệ, bao gồm hệ thống giám sát hoạt động cơ sở dữ liệu (DAM), hệ thống quản lý thông tin và sự kiện bảo mật (SIEM) và các ứng dụng khác.
- **Compliance Monitoring**, hay giám sát tuân thủ quy định: Hình thức này bao gồm việc đảm bảo tổ chức đang tuân thủ chặt chẽ các điều luật và tiêu chuẩn bảo mật liên quan như PCI DSS, HIPAA hoặc các quy định khác. Để đạt được hiệu quả trên, gói giám sát tuân thủ quy định sử dụng rất nhiều công nghệ, bao gồm hệ thống quản lý thông tin và sự kiện bảo mật, các phần mềm rà quét lỗ hổng và các ứng dụng khác.
- **Insider Threat Monitoring**, hay giám sát mối đe dọa nội bộ: Hình thức này bao gồm việc phát hiện và ngăn chặn các sự cố bảo mật gây ra bởi tác nhân bên trong doanh nghiệp, như nhân viên, nhà thầu hay đối tác. Để đạt được hiệu quả trên, gói giám sát mối đe dọa nội bộ sử dụng rất nhiều các công nghệ, bao gồm hệ thống quản lý thông tin và sự kiện bảo mật (SIEM), phần mềm phân tích hành vi người dùng (UBA) và các ứng dụng khác.

Về CyStack

CyStack là một công ty đổi mới sáng tạo trong lĩnh vực an ninh mạng tại Việt Nam, chúng tôi tiên phong xây dựng các sản phẩm bảo mật thế hệ mới cho cả doanh nghiệp và cá nhân. Các giải pháp của CyStack tập trung vào bảo vệ dữ liệu, phòng chống tấn công mạng và quản lý lỗ hổng bảo mật.

Để biết thêm chi tiết, liên lạc tới hotline **(+84) 247 109 9656** hoặc gửi mail tới **contact@cystack.net** để trao đổi cùng các chuyên gia bảo mật tại CyStack.
cystack.net