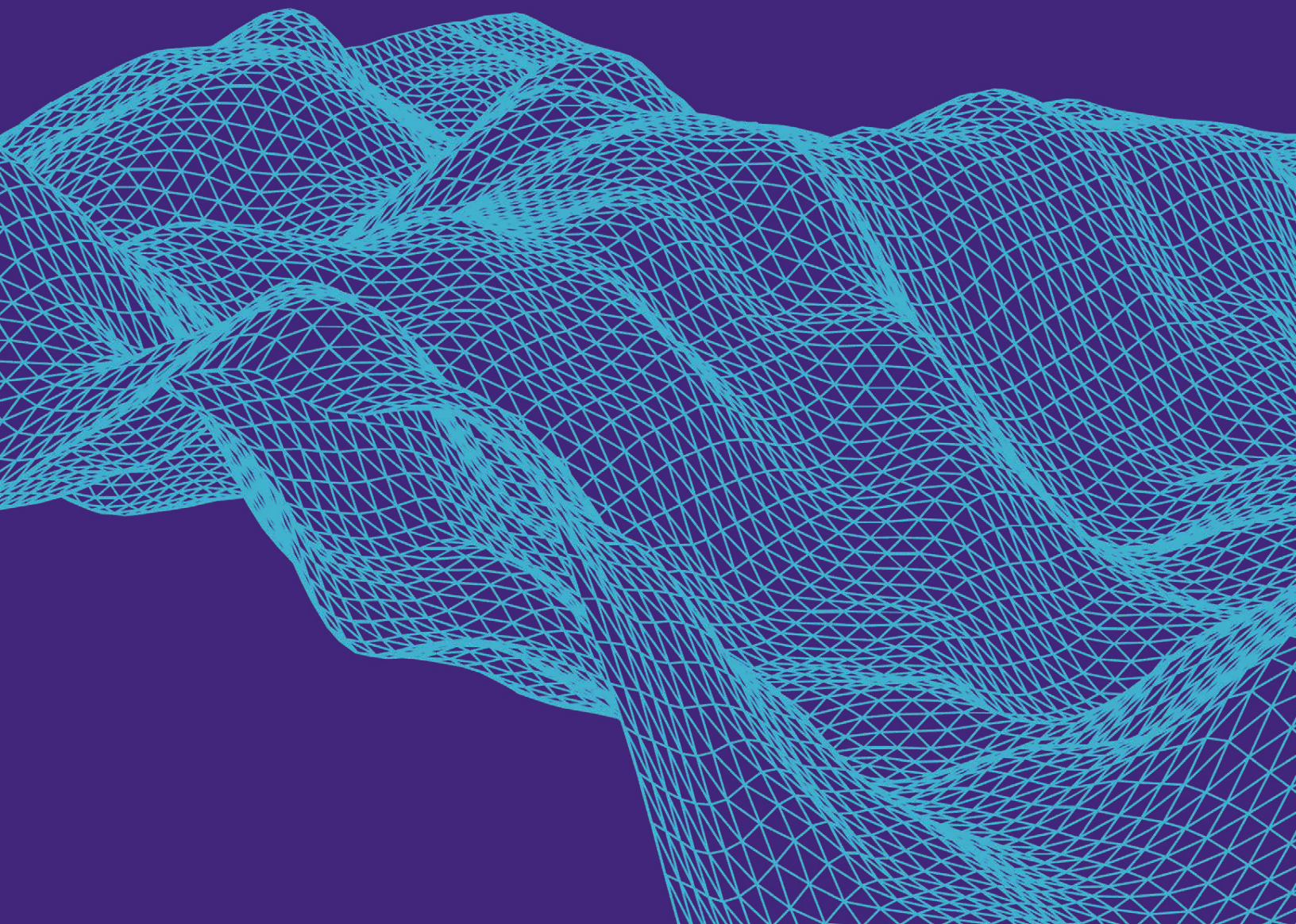
ADVANCE VISION TECHNOLOGY

eSENTIRE

eBOOK

XDR: Bí quyết để có Nền tảng Quản lý, Nhận diện và Xử lý (MDR) Hiệu quả cao



Mục lục

I. Lời mở đầu: Phản ứng Tức thời trước Cảnh báo Đe dọa Mạng hiện đại

Công việc của một chuyên gia an ninh mạng luôn đầy thách thức, và những biến cố trong hai năm qua đã đặt sự kiên nhẫn của các nhà bảo vệ lên thử thách theo cách chưa từng có. Với việc tiếp cận dễ dàng hơn tới các công cụ ngày càng tinh vi, các kẻ tấn công đã sử dụng các chiến thuật đe dọa đã quá quen thuộc để phát động một làn sóng tấn công leo thang.

An ninh Mạng qua số liệu

$4.24M

chi phí trung bình cho mỗi vụ rò rỉ thông tin

$847K

mức tiền chuộc trung bình bị yêu cầu trong năm 2020

51%

Kỹ sư Bảo mật cho biết hiệu suất của nhóm đã bị ảnh hưởng tiêu cực bởi việc làm việc từ xa

3.1M

vị trí Chuyên gia An ninh Mạng chưa tuyển dụng trên thế giới năm 2020

Các cuộc tấn công qua email, những vụ lợi dụng các thông tin cá nhân bị rò rỉ và các cuộc Tấn công phi kỹ thuật đang tiếp tục dẫn đến các vụ rò rỉ dữ liệu quy mô lớn,[1] với chi phí trung bình cho mỗi vụ rò rỉ hiện là 4,24 triệu Đô la Mỹ — đây là mức tăng chi phí lớn nhất trong gần một thập kỷ qua.[2] Bên cạnh đó, số lượng các cuộc tấn công bằng mã độc tống tiền đã đạt mức cao nhất từ trước tới nay, và mức yêu cầu tiền chuộc trung bình cũng đã tăng vọt lên tới mức kỷ lục là 847.344 Đô la Mỹ vào năm 2020.[3]

Với chi phí và rủi ro ngày càng tăng, các đội ngũ bảo mật đang phải căng mình hơn bao giờ hết. Việc chuyển sang mô hình làm việc từ xa đã không hề dễ dàng cho nhiều đội ngũ an ninh Mạng, khi 51% các Kỹ sư Bảo mật trong một cuộc khảo sát do FireEye thực hiện gần đây cho biết hiệu suất của nhóm của họ đã bị ảnh hưởng tiêu cực bởi việc làm việc từ xa.[4] Trong cùng cuộc khảo sát đó, hơn 80% các Nhà phân tích Bảo mật Thông tin đã miêu tả công việc của họ là "đau khổ" hoặc "rất đau khổ" do tăng tải công việc, khiến họ đứng trước nguy cơ kiệt sức.[5]

Dù đối mặt với nhiều thách thức, việc duy trì khả năng phản ứng nhanh chóng vẫn hết sức quan trọng. Những vụ vi phạm dữ liệu mất hơn 200 ngày để phát hiện và xử lý có chi phí trung bình cao hơn 1,26 triệu Đô la so với những vụ được phát hiện và giải quyết hoàn toàn trong vòng dưới 200 ngày.[6] Để giảm thiểu rủi ro tài chính đáng kể này, các tổ chức cần phải có khả năng kiểm soát các hoạt động độc hại trong môi trường của mình một cách nhanh chóng và liên tục.

Để đạt được mục tiêu này, điều quan trọng là phải duy trì khả năng phát hiện, điều tra và phản ứng trước các mối đe dọa một cách hiệu quả, và đảm bảo hoạt động này diễn ra liên tục 24/7.

Ngày càng có nhiều tổ chức đang tìm đến các nhà cung cấp Nền tảng Quản lý, Nhận diện và Xử lý (MDR) để cung cấp dịch vụ an ninh mạng, giúp họ đáp ứng nhu cầu bảo mật hiện tại. Hiện tại, chỉ 54% các tổ chức có quyền truy cập vào Trung tâm Điều hành An ninh (SOC) của riêng họ – và chỉ có 44% là tổ chức có dưới 10,000 nhân viên có cơ sở này.[7] Điều này vẫn đang xảy ra bất chấp thực tế rằng khả năng của SOC là chìa khóa để xây dựng một chương trình an ninh mạng toàn diện. Do đó, nhiều công ty đã tìm đến giải pháp thuê ngoài các hoạt động này để có thể tiếp cận với chuyên môn và giảm thiểu rủi ro mà không làm ảnh hưởng đến trọng tâm kinh doanh chính của họ.

[1]https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf, [2]https://www.ibm.com/downloads/cas/OJDVQGRY, [3]https://start.paloaltonetworks.com/unit-42-ransomware-threat-report, [4]https://www.fireeye.com/content/dam/collateral/en/rpt-ponemon-institute-second-annual-study-economics-of-the-soc-2021.pdf, [5]https://www.fireeye.com/content/dam/collateral/en/rpt-ponemon-institute-second-annual-study-economics-of-the-soc-2021.pdf, [6]https://www.ibm.com/downloads/cas/OJDVQGRY, [7]451 Research. Voice of the Enterprise: Information, Security, Organizational Dynamics 2020. [8]

Tổ chức có Trung tâm Điều hành An ninh (SOC) Nội bộ

54%
số tổ chức có
trung tâm SOC nội bộ

44%
số tổ chức có dưới 10,000 nhân viên
có trung tâm SOC nội bộ

Vì thế, thị trường Dịch vụ Quản lý An ninh Mạng (MSS) đang phát triển mạnh mẽ và ngày càng cạnh tranh. Báo cáo của Gartner cho thấy đã có mức tăng trưởng 44% về số lượng yêu cầu từ khách hàng tiềm năng trong năm qua.[8] Tuy nhiên, với hơn một nghìn công ty trên khắp thế giới hiện đang cung cấp các dịch vụ MSS, việc xác định yếu tố nào làm nên một dịch vụ "hiệu quả cao" trở nên khó khăn hơn bao giờ hết. Trong ngành này, không tồn tại một phương pháp báo cáo kết quả thống nhất, cũng như thiếu vắng các biện pháp đo lường rõ ràng và có thể áp dụng một cách phổ biến để đánh giá hiệu suất.

Trên thực tế, mỗi nhà cung cấp Nền tảng Quản lý, Nhận diện và Xử lý (MDR) cũng gặp phải các thách thức tương tự như các Trung tâm an ninh mạng nội bộ (SecOps). Ngành An ninh Mạng vẫn đang thiếu hụt nhân lực có kỹ năng, với khoảng 3.1 triệu vị trí chưa được lấp đầy trên toàn cầu vào năm 2020.[9] Chất lượng dịch vụ của các nhà cung cấp MDR lại phụ thuộc vào hiệu quả của đội ngũ nhân sự, bao gồm các nhân viên phân tích Bảo mật Thông tin, nhân viên Săn tìm các mối đe dọa, nhân viên Phản ứng sự cố, và Kỹ sư nội dung và tự động hóa - những nhân tố này đảm nhiệm các nhiệm vụ điều tra, phát hiện và vận hành để kiểm soát các mối đe dọa.

Công việc của họ rất khó khăn, đặc biệt là khi phải quản lý đồng thời cho nhiều khách hàng khác nhau. Điều này làm nổi bật tầm quan trọng của việc hỗ trợ và trao quyền cho các đội ngũ SecOps trong công việc của họ. Để cung cấp dịch vụ MDR hiệu quả cao, nhà cung cấp cần phải đầu tư vào một nền tảng công nghệ phù hợp, nền tảng này làm tăng cường hiệu quả hoạt động và giúp việc phát hiện và xử lý các mối đe dọa được thực hiện một cách nhanh chóng và dễ dàng hơn.

XDR chính là nền tảng công nghệ đó. Trong phần tiếp theo của báo cáo, chúng ta sẽ tìm hiểu XDR là gì, cũng như cơ chế hoạt động của nó, và lý do vì sao nền tảng này sẽ giúp các chuyên gia an ninh hoàn thành công việc một cách xuất sắc nhất.

[8]451 Research. Voice of the Enterprise: Information, Security, Organizational Dynamics 2020. [9]https://www.gartner.com/doc/reprints?id=1-27JN2ORS&ct=210928&st=sb," https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

II. Khám phá Nền tảng Nhận diện và Xử lý Mở rộng (XDR)

Ngay cả trước các sự kiện của năm 2020, nhiều tổ chức đã vật lộn để duy trì các chương trình hoạt động bảo mật hiệu quả. Với việc ngày càng nhiều tác vụ chuyển thông tin lên hệ thống đám mây, cấu trúc hệ thống CNTT đã trở nên phức tạp và phân tán hơn bao giờ hết. Cùng lúc đó, việc áp dụng phổ biến các phương pháp DevOps đã làm cho chu kỳ phát hành phần mềm ngày càng ngắn lại. Kết hợp với tính chất biến đổi nhanh chóng của hệ thống đám mây, điều này khiến cho môi trường tính toán của các tổ chức liên tục thay đổi và ngày càng trở nên động hơn.

Không chỉ bề mặt tấn công bị mở rộng, các hoạt động quan trọng của doanh nghiệp cũng ngày càng dựa vào công nghệ số hơn, điều này sẽ khiến hậu quả của bất kỳ sự cố hoặc rò rỉ nào càng trở nên nghiêm trọng hơn. Cùng với sự mở rộng của bề mặt tấn công, lượng nhật ký và nguồn dữ liệu thông tin từ xa từ môi trường mà các đội SecOps phải giám sát cũng tăng lên tương ứng.

Ngày nay, các quy trình kinh doanh số đã trở nên quan trọng đối với kết quả kinh doanh hơn bao giờ hết, trong khi việc áp dụng rộng rãi các chính sách làm việc từ xa và mô hình làm việc hybrid tiếp tục làm mở rộng bề mặt tấn công. Đối mặt với những thách thức này, các hệ thống bảo mật truyền thống dựa trên nhiều giải pháp điểm hoạt động theo cách tách biệt, đã không còn đủ khả năng để đáp ứng nhu cầu hiện tại.

Các nền tảng Quản lý sự kiện và thông tin bảo mật (SIEM) thường kém hiệu quả và cồng kềnh, không được thiết kế để cung cấp thông tin nền và bối cảnh đầy đủ mà các nhà phân tích cần để đưa ra các quyết định chính xác ngay lập tức.

Hạn chế của SIEM trong Bối cảnh đe dọa hiện đại

Công nghệ SIEM ban đầu được phát triển chủ yếu để đáp ứng các yêu cầu tuân thủ, buộc các tổ chức phải lưu trữ và giữ dữ liệu nhật ký tại một địa điểm trung tâm duy nhất. Dù SIEM đã sớm được nhận định là có ích cho việc săn lùng mối đe dọa và điều tra sau sự cố, nó chưa bao giờ được thiết kế để hoạt động như một công cụ tương quan dữ liệu theo thời gian thực. Việc trả lời các câu hỏi phức tạp qua dữ liệu tương quan không phải là điểm mạnh của SIEM, các nền tảng cần phải được tinh chỉnh kỹ lưỡng, viết quy tắc hoặc lập trình trước khi có thể giúp các nhà phân tích hiểu những gì đang diễn ra trong môi trường.

XDR được phát triển để giải quyết những vấn đề này.

Dù có nhiều cách định nghĩa khác nhau, chúng tôi ưu tiên sử dụng định nghĩa do 451 Research đưa ra. Theo đó, Nền tảng Nhận diện và Xử lý Mở rộng (XDR) là một phương pháp công nghệ tích hợp sẵn nhiều nguồn dữ liệu bảo mật với các công cụ phân tích và phản ứng, nhằm tạo ra một giải pháp bảo mật toàn diện và hiệu quả.[10]

Trong nhiều chương trình bảo mật, các giải pháp SIEM đã được sử dụng để lưu trữ nhật ký sự kiện nội bộ từ một loạt các công cụ bảo mật, hệ điều hành, ứng dụng và thiết bị mạng. . SIEM cho phép các nhà phân tích tương quan và tìm kiếm trong dữ liệu nhật ký này, nhưng thường không cung cấp đầy đủ khả năng hiển thị thời gian thực về các hoạt động trên các điểm cuối, nơi mà phần lớn các tác nhân đe dọa bắt đầu xâm nhập. Do đó, các chương trình SecOps đã bắt đầu áp dụng các công cụ Phát hiện và Phản ứng tại Điểm cuối (EDR) được thiết kế đặc biệt. EDR cho phép thu thập dữ liệu trực tiếp từ các thiết bị điểm cuối để hỗ trợ phát hiện và điều tra mối các đe dọa, cũng như thực hiện các biện pháp phản ứng cụ thể. Tuy nhiên, hạn chế của EDR là khả năng phát hiện và phản ứng của nó chỉ tập trung vào điểm cuối.

[10]451 Research. Technology & Business Insight: The Rise of Extended Detection and Response

XDR đem lại khả năng phát hiện và phản ứng tiên tiến thế hệ mới, mở rộng khả năng hiển thị nâng cao và chức năng kiểm soát mối đe dọa mà NDR và EDR cung cấp trên toàn bộ hệ sinh thái CNTT. XDR cung cấp ngữ cảnh cho thông tin tình báo mối đe dọa bên ngoài và môi trường kinh doanh nội bộ bằng cách tổng hợp dữ liệu từ nhiều nguồn bảo mật như mạng, điểm cuối, đám mây, email, danh tính, Internet of Things (IoT) và nhiều hơn nữa.

Ra đời với mục tiêu cung cấp cái nhìn toàn diện về bề mặt tấn công trong các hệ sinh thái điện toán phân tán và đa dạng ngày nay, XDR phân tích dữ liệu để phát hiện mẫu mối đe dọa, giảm thiểu các báo động sai và tự động hóa các biện pháp phản ứng và xử lý mối đe dọa. Điều này biến XDR trở thành một công cụ hiệu quả và có giá trị đối với các nhóm an ninh. Với các phương pháp XDR tiên tiến, có đủ thông tin ngữ cảnh và hiểu biết để tự tin xử lý các mối đe dọa, thậm chí có thể tự động hóa quy trình mà không làm gián đoạn các hoạt động kinh doanh quan trọng.

Lãnh đạo Doanh nghiệp hướng tới hiệu suất bảo mật cao

94%

khối lượng công việc được dự đoán sẽ chạy trên hệ thống đám mây vào cuối năm 2021.[11]

80%

tổ chức được dự đoán sẽ tiếp tục cho phép nhân viên làm việc tại nhà sau khi đại dịch kết thúc.[12]

84%

các nhóm DevOps đang phát hành các tính năng mới nhanh hơn bao giờ hết.[13]

87%

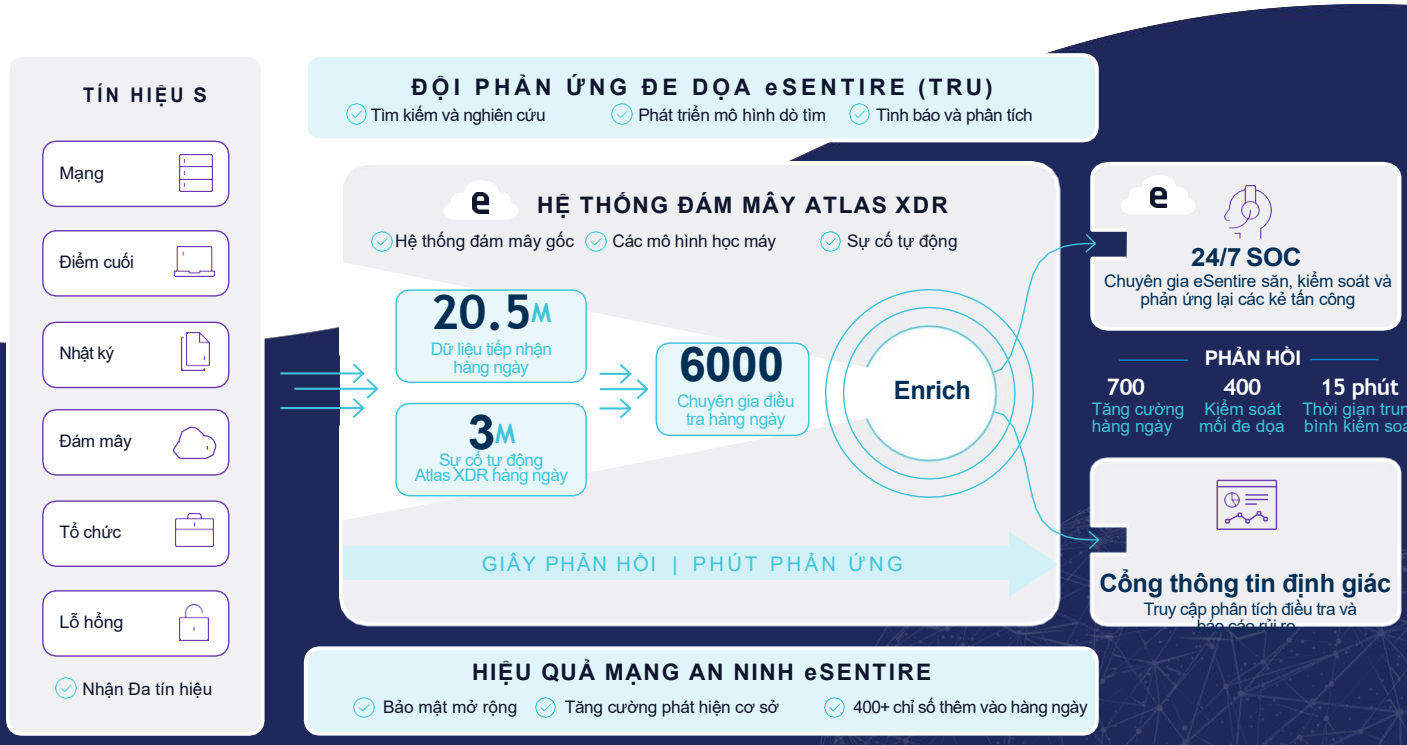
tổ chức báo cáo rằng họ không có đủ tài nguyên an ninh mạng.[14]

[11] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html,
[12]https://www.gartner.com/en/newsroom/press-releases/2020-10-13-gartner-identifies-three-dimensions-that-define-the-new-employer-employee-relationship, [13]https://learn.gitlab.com/c/2021-devsecops-report?x=u5RjB_, [14]451 Research. Technology & Business Insight: The Rise of Extended Detection and Response.

III. Tìm hiểu sâu về cách thức hoạt động của XDR

Mặc dù chúng tôi đã miêu tả XDR như là nền tảng công nghệ giúp các nhà cung cấp dịch vụ MDR hiệu quả cao phát hiện và giải quyết mối đe dọa một cách nhanh chóng, nhưng XDR không chỉ đơn thuần là một loại công nghệ. Đó là một phương pháp tích hợp các công cụ bảo mật, điểm kiểm soát, các dữ liệu thông tin từ xa và các phân tích vào hệ thống toàn diện của doanh nghiệp để loại bỏ nhiễu, đồng thời tập trung phân tích các diễn biến an ninh quan trọng nhất.

XDR tổng hợp tín hiệu từ nền tảng hệ thống đám mây gốc và lai ngày nay. Nó chuẩn hóa, bổ sung và ngữ cảnh hóa cho các dữ liệu này, kích hoạt các phản ứng tự động chỉ trong vài giây để phát hiện bảo mật với độ chính xác cao. Các mô hình học máy (ML) mạnh mẽ được tích hợp vào các nền tảng XDR để cung cấp thông tin chính xác và kịp thời cho các chuyên gia. Các chuyên gia SOC và những chuyên gia săn mối đe dọa được trang bị để tìm kiếm, kiểm soát và phản ứng lại các cuộc tấn công nhanh hơn nhiều mà không gây ra mệt mỏi và thất vọng, trong những trường hợp phản ứng tự động không khả thi. XDR cũng cung cấp thông tin đáng tin cậy để tăng tốc quá trình phân tích điều tra và làm cho việc báo cáo về rủi ro trở nên hiệu quả hơn.



Dưới đây là một số thông tin quan trọng về những khả năng cốt lõi của XDR:

- **XDR nhận đa nguồn tín hiệu.** Sức mạnh của XDR nằm ở khả năng thu thập và chuẩn hóa dữ liệu từ mọi phần của môi trường. Điều này làm cho việc dò tìm mối nguy trở nên chính xác hơn, vì nó mang lại cho đội ngũ bảo mật cái nhìn toàn diện từ thiết bị cuối đến đám mây và nhiều hơn nữa. Điều lý tưởng nhất là không nên có bất kỳ hạn chế nào về thông tin mà đội ngũ an ninh có thể truy cập hoặc số lượng dữ liệu có thể tích hợp vào phân tích. Điều này đồng nghĩa với việc các công nghệ được sử dụng không nên bị giới hạn trong danh mục sản phẩm hoặc bộ giải pháp của một nhà cung cấp duy nhất.

- **Hệ thống phân tích thông minh loại nhiễu và giảm tỉ lệ các báo động sai.** Trong hệ thống bảo mật truyền thống tập trung vào SIEM, tỷ lệ báo động sai cao là một vấn đề lâu dài, cũng như là nguyên nhân chính gây mệt mỏi cho các chuyên gia bảo mật. Sự nhiễu loạn quá mức cũng dễ dàng dẫn đến quá tải cảnh báo, và điều này có thể dẫn đến việc không phát hiện mối đe dọa được nếu các chuyên gia quyết định bỏ qua cảnh báo chỉ vì không đủ thời gian để điều tra tất cả các phát sinh. Trong XDR, các mô hình học máy (ML) và thuật toán trí tuệ nhân tạo (AI) hỗ trợ các nhà phân tích trong việc nhận biết các mẫu. ông nghệ này tự động đưa dữ liệu thực tế và thực hiện các bước điều tra mà trước đây chỉ con người mới có thể thực hiện được. Kết quả cuối cùng là tiết kiệm thời gian và ít báo động sai hơn rất nhiều.

- **Dữ liệu phong phú và thông tin thực tế hỗ trợ truy lùng mối nguy.** Vì nền tảng XDR tiếp nhận nhiều loại tín hiệu khác nhau, việc quan sát các mối quan hệ trong dữ liệu phong phú này trở nên khả thi khi nó là đối tượng điều tra của con người trong việc săn lùng mối đe dọa. Nếu có bằng chứng về kỹ thuật tấn công đã được sử dụng trong quá khứ, về mối quan hệ giữa các phần khác nhau của một chuỗi tấn công, hoặc về các mẫu hoạt động rõ rang là độc hại, thì điều này sẽ trở nên rõ ràng đối với các nhà nghiên cứu bảo mật. Khi các mô hình có độ tin cậy cao, các hành động phản ứng tự động có thể được kích hoạt.

- **Khả năng phản ứng tự động đẩy nhanh quá trình kiểm soát mối đe dọa.** Khi một nền tảng XDR tích hợp khả năng phản ứng tự động, các hoạt động kiểm soát có thể được khởi động chỉ trong vài giây nếu có mức độ tin cậy cao rằng hoạt động được quan sát là nguy hiểm hoặc độc hại. Một nền tảng XDR hàng đầu sử dụng công nghệ tự đưa ra quyết định riêng để tăng cường các sự cố tự động, giúp thực hiện các giao thức kiểm soát hiệu quả, an toàn và phù hợp mỗi khi có bằng chứng rõ ràng cho thấy chúng là cần thiết, giảm thiểu thời gian tồn tại của các đối tượng đe dọa.

- **Các nền tảng XDR có khả năng học từ thông tin điều tra về mối đe dọa mới nhất, các báo cáo quan sát, và các biện pháp phản ứng đã thực hiện trên toàn bộ hệ thống.** Các nền tảng XDR hàng đầu có khả năng sử dụng lượng dữ liệu lớn về các mối đe dọa hiện tại và mới nổi để cải thiện độ chính xác của việc phát hiện. Đặc biệt, một nền tảng XDR có thể theo dõi các phát hiện, cuộc điều tra và các hành động phản ứng trên nhiều môi trường khách hàng, từ đó học hỏi và tổng hợp kiến thức để hỗ trợ tất cả các khách hàng. Bằng cách này, các bước điều tra đã học được từ một môi trường có thể được tự động hóa và áp dụng cho các môi trường khác, và các hoạt động phản ứng và kiểm soát đã được chứng minh là thành công có thể được mở rộng ra toàn bộ cơ sở khách hàng của nhà cung cấp, tạo nên một chu trình phản hồi liên tục giúp cải thiện và củng cố bảo mật cho tất cả các khách hàng.

- **XDR cung cấp giải pháp bảo mật tiên tiến có khả năng mở rộng.** Trong các hệ thống bảo mật truyền thống dựa trên SIEM, mỗi nguồn tín hiệu mới mà nhóm bảo mật thêm vào có thể làm tăng tỷ lệ báo động sai và gây quá tải cho các chuyên gia bảo mật. Tuy nhiên, với XDR, việc tiếp nhận ngày càng nhiều tín hiệu thực tế càng làm tăng tính chính xác của việc phát hiện mối nguy hại. Ngoài ra, khi tiếp nhận nhiều dữ liệu hơn, các cuộc điều tra và phản ứng cũng được cải thiện chất lượng, đặc biệt là khi có nhiều khách hàng hơn sử dụng nền tảng. Hiệu ứng hệ thống này giải thích tại sao việc mở rộng quy mô của một nhà cung cấp MDR toàn cầu sẽ nâng cao khả năng của họ.

IV. Đột phá Công nghệ: Khai thác Học máy để tối ưu hóa MDR

Làm thế nào một nền tảng XDR có thể giúp các nhóm bảo mật giải quyết những thách thức đau đầu nhất và lau dài nhất đã gây ám ảnh cho các nhóm SecOps kể từ thuở sơ khai của thời đại công nghệ máy tính hiện đại? Để trả lời câu hỏi này, chúng ta cần xem xét kỹ lưỡng các thuật toán tiên tiến tạo nên cốt lõi của nó.

Thời gian và nguồn nhân lực hạn chế là một vấn đề lớn khi các chuyên gia bảo mật phải giám sát và xử lý các sự kiện một cách thủ công. Việc phải phân bổ sự chú ý đúng mức cho mỗi cảnh báo không hề dễ dàng, đặc biệt là khi họ phải đối mặt với hàng trăm cảnh báo mỗi ngày và phải phân tích một lượng lớn dữ liệu không cấu trúc. Trên thực tế, có đến 79% cảnh báo không được xem xét trong một số chương trình bảo mật do sự thiếu hụt thời gian. [15]

Học máy (ML) làm rất tốt trong việc nhận dạng mẫu. Tìm ra các mẫu tinh tế trong lượng lớn dữ liệu không phải là nhiệm vụ phù hợp với con người, nhưng lại là điểm mạnh của ML. Các mô hình học máy được sử dụng để điều tra các sự kiện trong một nền tảng XDR hàng đầu trong ngành có khả năng phát hiện các mối quan hệ trong các loại dữ liệu và tín hiệu khác nhau đi qua nền tảng.

[15]https://www.enterprisemanagement.com/research/asset.php/3441/InfoBrief:-A-Day-in-the-Life-of-a-Cyber-Security-Pro

Trong nhiều trường hợp, các mô hình ML "suy nghĩ" theo một cách tiếp cận hoàn toàn khác với cách con người tư duy. Khi gặp phải quá nhiều thông tin và sự phân tán, con người gặp nhiều khó khăn hơn để nhìn và nhớ những điều quan trọng nhất. Tuy nhiên, đó là điều ngược lại đối với ML - càng nhận nhiều dữ liệu trong huấn luyện, càng học được nhiều ví dụ. Và càng học nhiều ví dụ thì mô hình càng có khả năng dự đoán giải pháp cho các trường hợp mới tốt hơn. Điều này lý giải vì sao dữ liệu đóng vai trò quan trọng như vàng đối với các hệ thống dựa trên trí tuệ nhân tạo. Thậm chí, dữ liệu được chú thích sẵn là để sử dụng như một bài học được coi là vô cùng quý giá. Đây cũng là lý do tại sao các hệ thống dựa trên trí tuệ nhân tạo rất hiệu quả trong việc tự động hóa các hành động mà thường khiến con người cảm thấy mệt mỏi và bị áp đặt.

XDR hoạt động như một lực kênh cho các chuyên gia bảo mật trong môi trường SOC bằng cách tập trung sự chú ý của họ vào những vấn đề quan trọng nhất. Công nghệ này học từ các cuộc điều tra trước đó, từ đó có thể đề xuất những hành động tốt nhất trong mỗi tình huống điều tra mới.

"Bộ não" của SOC: Cách XDR Hỗ trợ Phát hiện, Điều tra và Phản ứng Tự động

Một nền tảng XDR hàng đầu trong ngành sẽ tự động hóa các phản ứng đối với các mối đe dọa có độ tin cậy cao. Khi không thể xử lý tự động, nền tảng sẽ cung cấp cho các chuyên gia bảo mật khối lượng phong phú dữ liệu chi tiết để điều tra. Lượng dữ liệu này sẽ được cập nhập các thông tin về tính huống, đồng thời loại bỏ các chi tiết đặc thù của nhà cung cấp để dễ hiểu hơn.

Nền tảng này sẽ giúp các chuyên gia dễ dàng xác định:

- Các thông tin liên quan
- Những sự kiện liên quan
- Các hoạt động rõ ràng là độc hại
- Thời điểm phù hợp để bắt đầu một quy trình phản ứng tự động
- Những điều cần được các chuyên gia chú ý hơn

Sau khi những điều này được xác định rõ ràng, quá trình điều tra và phản ứng có thể khởi động hoàn toàn tự động mà không cần đến sự can thiệp của con người.

Trong trường hợp gặp những tình huống không rõ ràng, nền tảng cung cấp cho các chuyên gia bảo mật các thông tin chi tiết giúp họ thực hiện công việc một cách thuận lợi hơn. Điều này cũng khuyến khích họ trở nên sáng tạo hơn, tự tin hơn vào năng lực của mình và ngăn chặn được nhiều mối đe dọa hơn. Sự tích hợp của các công nghệ bảo mật không chỉ giúp tăng 10.5% hiệu quả của chương trình bảo mật mà còn liên quan mạnh mẽ đến việc cải thiện tuyển dụng và giữ chân nhân tài.[16]

Trường hợp sử dụng XDR: Truy quét các mối đe dọa từ hoạt động của PowerShell

PowerShell đã là đồng hành cùng Windows suốt hơn một thập kỷ. Nó được ưa chuộng vì cung cấp khả năng truy cập chi tiết vào bên trong hệ điều hành. Tuy nhiên, nó cũng là mục tiêu thường xuyên bị các kẻ tấn công ngắm vào.

Các nhân viên truy tìm mối đe dọa thường tập trung vào tìm kiếm các lỗ hổng của PowerShell vì chúng quá mức phổ biến.

Tuy nhiên, việc kiểm tra từng mã kịch bản PowerShell chạy trong môi trường IT doanh nghiệp thủ công sẽ đòi hỏi một lượng lớn thời gian và năng lượng.

Sử dụng một mô hình ML sẽ giúp theo dõi tất cả các thực thi PowerShell một cách dễ dàng. Mỗi thực thi có thể tự động được đánh giá dựa trên khả năng liên quan đến hoạt động độc hại. Các thực thi kích hoạt cảnh báo thường có độ tin cậy cao. Điều này đạt được nhờ nền tảng có quyền truy cập vào một lượng lớn các ví dụ về các thực thi PowerShell trước đó – tất cả đã được phân loại là "vô hại" hoặc "độc hại" khi được điều tra.

Điều này biến việc truy tìm mối đe dọa từ việc "mò kim đáy bể" thành một hoạt động dựa trên giả thuyết, với khả năng cao tìm thấy các mối đe dọa thực tế và hiện hữu.

[16]https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-main-report.pdf

V. Tăng cường Bảo mật - Sự kết hợp hoàn hảo của MDR và XDR

Trong bối cảnh đầy thách thức về bảo mật mạng hiện nay, không ngạc nhiên khi có ngày càng nhiều lãnh đạo doanh nghiệp chọn Nền tảng Quản lý, Nhận diện và Xử lý (MDR) thay vì các Dịch vụ Quản lý An ninh Mạng (MSS) truyền thống. Ưu điểm nổi bật của MDR là việc ưu tiên phản ứng nhanh chóng, kiểm soát mối đe dọa cùng các biện pháp khắc phục, kèm theo đó khả năng cảnh báo và giám sát như là một phần của các dịch vụ MSS tiêu chuẩn.

Khi một nhà cung cấp đã đầu tư đầy đủ từ việc quản lý các sự cố cho đến việc giải quyết chúng, họ có động lực mạnh mẽ để cung cấp một hệ thống bảo mật tổng thể vượt trội. Họ sẽ không thể chỉ đóng vai trò như một cái máy cảnh báo, đưa ra một lượng lớn các cảnh báo sai lầm mà không có phản ứng có cụ thể.

Mặc dù các chữ viết tắt có thể gây nhầm lẫn cho người mới, nhưng MDR và XDR không phải là cùng một thứ.

MDR là một dịch vụ toàn diện được xây dựng trên nền tảng công nghệ này, nhưng nó còn cung cấp quyền cho những người có chuyên môn thực hiện các hành động thủ công và trực quan để phản ứng và khắc phục các mối đe dọa, cũng như tối ưu hóa hoạt động bảo mật khi không thể tự động hóa.

XDR là một công nghệ cho phép phát hiện mối nguy với độ chính xác cao, tổ chức điều tra nhanh chóng và chính xác hơn, và cuối cùng phản ứng tự động.

Không chỉ là một công nghệ, XDR là một kiệt tác

Khi các nhà cung cấp bảo mật mạng bán các giải pháp XDR, họ chỉ đang cung cấp các công cụ. Mặc dù những công cụ này có thể mạnh mẽ và đầy đủ tính năng, nhưng chúng vẫn chỉ là những công cụ tĩnh. Trái lại, một nhà cung cấp MDR sẽ cung cấp toàn bộ việc lập trình và kỹ thuật cần thiết để biến các công cụ này thành một giải pháp mạnh mẽ cho hoạt động bảo mật hiệu quả và kiểm soát mối đe dọa nhanh chóng. Việc vận hành hiệu quả một nền tảng XDR đòi hỏi chuyên môn cao — từ việc tạo ra các tài liệu hướng dẫn, quản lý nội dung, tận dụng thông tin tình báo về mối đe dọa, đến học hỏi từ các cuộc điều tra trước đó — điều mà ít chương trình bảo mật nội bộ nào có thể dễ dàng tiếp cận.

Lấy ví dụ về kỹ thuật phát hiện. Đây là một chức năng hỗ trợ quan trọng cho các nhóm vận hành bảo mật và các nền tảng XDR nhưng thường ít được thảo luận. Kỹ thuật phát hiện là yếu tố quan trọng giúp nền tảng XDR thực hiện phát hiện chính xác và toàn diện. Cùng với kỹ thuật tự động hóa, kỹ thuật phát hiện cung cấp nội dung để vận hành nền tảng. Tuy nhiên, để có thể luôn đón đầu các hành vi tấn công liên tiếp, nó đòi hỏi sự quan tâm liên tục từ nhóm chuyên gia.

Các hiệu ứng mạng an ninh cũng đóng vai trò quan trọng trong sự thành công của XDR: mô hình ML được học về càng nhiều dữ liệu độc hại và các hoạt động điều tra và phản ứng thì càng phát hiện, điều tra và phản ứng đúng mức độ độc hại hơn. Vì vậy, một nền tảng XDR có khả năng tích hợp một lượng lớn dữ liệu điều tra từ nhiều môi trường khách hàng MDR vào tập dữ liệu đào tạo ML của nó sẽ thành công và hiệu quả hơn so với một nền tảng có ít thông tin điều tra hơn. Lịch sử điều tra tổng hợp của một nhà cung cấp MDR mang lại cho nền tảng một nguồn kiến thức lớn hơn tổng cộng lại của bất kỳ lịch sử đe dọa và sự cố an ninh mạng của bất kỳ doanh nghiệp cá nhân nào.

Một nhà cung cấp dịch vụ MDR hàng đầu sẽ cung cấp không chỉ là quyền truy cập vào các công nghệ XDR mà còn có:

- ✔ Phủ sóng giám sát bảo mật đầy đủ và tích hợp
- ✔ Chuyên gia SOC hỗ trợ 24/7
- ✔ Công nghệ phát hiện tiên tiến thúc đẩy việc ngăn chặn tự động mối đe dọa
- ✔ Săn tìm mối đe dọa theo các giả thuyết cấp cao
- ✔ Cảnh báo liên quan, khả năng phân loại, điều tra mối đe dọa và kiểm soát tình huống tác chiến
- ✔ Các đề xuất khắc phục, hành động và xác nhận đã được học và được xác thực trên nhiều môi trường khách hàng

VI. Nhà cung cấp MDR - Những tiêu chí không thể bỏ qua

Trong bối cảnh các mối đe dọa ngày càng phức tạp và biến đổi không ngừng, tốc độ trở thành yếu tố quan trọng nhất. Đa số kẻ tấn công (54%) có thể xâm nhập vào một môi trường mục tiêu trong vòng dưới 15 giờ,[17] và hầu hết các dạng mã độc ransomware có thể lan rộng trên hệ thống mạng của nạn nhân trong vòng ba đến bốn giờ, mã hóa các tập tin trên mỗi thiết bị chỉ trong vài giây. Các loại mã độc nguy hiểm nhất có thể thực hiện điều này trong ít hơn 45 phút.[18]

Khi đánh giá các nhà cung cấp dịch vụ MDR, bạn cần lưu ý tới một số yếu tố quan trọng sau:

Đánh giá thời gian kiểm soát trung bình

Chiến lược tốt nhất để giảm thiểu rủi ro và bảo vệ tổ chức cảu bạn khỏi những tổn thất tiềm ẩn của các cuộc tấn công là phát triển khả năng phản ứng nhanh chóng. Do đó, điều đầu tiên và quan trọng nhất là tìm kiếm một nhà cung cấp dịch vụ MDR cam kết được Thời gian kiểm soát các mối nguy hại trung bình. Ngoài ra, bạn cũng cần nắm rõ thời gian cần thiết để kiểm soát mối đe dọa đến máy chủ trong môi trường của bạn và đảm bảo rằng nhà cung cấp có thể thực hiện cam kết này.

Quy mô cơ sở khách hàng rất quan trọng

Đối với một nhà cung cấp MDR, khách hàng chính là nguồn dữ liệu để huấn luyện các mô hình ML của nền tảng XDR. Vì vậy, việc lựa chọn một nhà cung cấp có uy tín là rất quan trọng. Với càng nhiều khách hàng, dữ liệu sẽ càng phong phú và đa dạng, từ đó củng cố khả năng phát hiện mối nguy chính xác, tăng tốc độ điều tra và kiểm soát mối đe dọa.

Chọn một nhà cung cấp MDR mà các khách hàng tin tưởng

Một trong những ưu điểm chính của việc sử dụng dịch vụ MDR là nhà cung cấp có thể thực hiện các biện pháp kiểm soát và khắc phục thay bạn. Tuy nhiên, bạn sẽ cần phải cho phép họ làm điều này, đồng nghĩa với việc từ bỏ quyền kiểm soát các hệ thống và quy trình quan trọng của doanh nghiệp. Một nhà cung cấp có kinh nghiệm trong việc thay mặt khắc phục sự cố với các khách hàng cùng ngành sẽ có hiểu biết và kinh nghiệm để giành được lòng tin của bạn.

Ngoài ra, một nhà cung cấp MDR thực hiện nhiều biện pháp kiểm soát và khắc phục từ đầu đến cuối sẽ có khả năng tích hợp thông tin về những hoạt động đó vào dữ liệu huấn luyện ML của XDR. Điều này có nghĩa là mô hình của họ sẽ hoạt động dựa trên thông tin phong phú hơn — bao gồm toàn bộ chu kỳ của sự cố — so với các công ty chỉ giám sát.

Đừng đánh giá thấp giá trị của việc tích hợp các ứng dụng và hệ thống

Dù có vẻ đơn giản nhưng vẫn cần nhấn mạnh lại, bạn sẽ tiết kiệm được nhiều chi phí nếu không cần phải thay thế toàn bộ công nghệ bảo mật hiện tại trong hệ thống. Quan trọng hơn, sử dụng nhiều công cụ và giải pháp của các nhà cung cấp khác nhau có thể giúp bạn nhìn rõ hơn bề mặt tấn công và cải thiện độ chính xác của việc phát hiện. Điều này cũng tăng tính đa dạng của tập dữ liệu huấn luyện mọi mô hình, giúp chúng bám sát với tình hình thực tế hơn. Tuy nhiên, tập trung tích hợp sâu với một số công cụ chính quan trọng hơn là tích hợp rộng rãi với mọi công cụ. Điều quan trọng nhất là tích hợp đầy đủ dữ liệu thông tin từ xa và phản ứng EDR hơn là tích hợp với tất cả các bộ công cụ bảo mật có sẵn.

> “Để đạt được kết quả tốt hơn từ các hệ thống AI, điều cốt yếu là có quyền truy cập vào tập dữ liệu phù hợp để huấn luyện các mô hình. Giá trị thực sự đến từ những dự đoán chính xác, nhưng để có được điều này, cần phải có một tổ hợp lớn các ví dụ chất lượng cao để học hỏi. Là một nhà cung cấp MDR, mỗi ngày chúng tôi đều tổng hợp lượng lớn các ví dụ điều tra và phản ứng chất lượng cao trong SOC của mình. Điều này mang lại cho chúng tôi lợi thế lớn trong việc tìm kiếm các mô hình học tập phù hợp để nâng cao hiệu quả của nền tảng XDR.
>
> - Dustin Hillard, Giám đốc Công nghệ tại eSentire

[17]https://www.nuix.com/sites/default/files/downloads/marketo/report_nuix_black_report_2018_web_us.pdf, [18]https://www.zdnet.com/article/microsoft-some-ransomware-attacks-take-less-than-45-minutes/

VII. Điều khiển dịch vụ MDR của eSentire khác biệt

Nền tảng Quản lý, Nhận diện và Xử lý đa tín hiệu và toàn diện của eSentire mang lại bảo vệ liên tục 24/7, chống lại những cuộc tấn công phức tạp nhất, kể cả những cuộc tấn công có khả năng phá vỡ các biện pháp bảo mật thông thường.

Xây dựng trên Nền tảng Đám mây Atlas XDR của eSentire, dịch vụ MDR của chúng tôi tận dụng hiệu quả mà nó tạo ra cho việc phát hiện mối đe dọa, điều tra và phản ứng đầy đủ cho các sự cố. Atlas XDR sử dụng các mô hình học máy để loại bỏ nhiễu, giúp hệ thống phát hiện mối đe dọa và tự động ngăn chặn tức thì. Atlas tiếp nhận hơn 20 triệu tín hiệu bảo mật và tự động chặn 3 triệu mối đe dọa mỗi ngày mà không cần sự can thiệp từ đội ngũ SOC của chúng tôi hoặc đội ngũ bảo mật của bạn. Trong trường hợp chuỗi phản ứng không khả thi, Atlas XDR sẽ trang bị cho các chuyên gia an ninh mạng của chúng tôi các thông tin và công cụ cần thiết để thực hiện các điều tra sâu hơn và triển khai biện pháp kiểm soát thủ công, với thời gian trung bình để kiểm soát là 15 phút.

MDR của eSentire không chỉ giới hạn trong việc đưa ra các cảnh báo. Chúng tôi chú trọng vào việc mang lại kết quả bảo mật xuất sắc. Thông qua Nền tảng Đám mây Atlas XDR của eSentire, chúng tôi tiên phong chống lại các mối đe dọa mới bằng cách biến mỗi phát hiện mới trong môi trường của một khách hàng thành sự bảo vệ toàn cầu cho cơ sở khách hàng của chúng tôi. Sử dụng các thuật toán được ML bảo hộ, chúng tôi liên tục cải thiện hiệu suất của hệ thống để tăng cường khả năng phát hiện, điều tra, săn mối đe dọa và khắc phục hậu quả.

CHÚNG TÔI CÓ:				
Hệ thống đám mây gốc	**Mô hình học máy được bảo hộ**	**Phủ sóng đa tín hiệu**	**Hiệu ứng An ninh Mạng**	**Khả năng Phản Ứng Mở Rộng**
Một nền tảng phân tán trên đám mây, có khả năng mở rộng và phân phối, cung cấp tính bảo mật và tính dự phòng	Các mô hình ML và AI thích ứng hỗ trợ loại bỏ nhiễu	Thu thập, chuẩn hóa và tương quan dữ liệu trên mạng, điểm cuối, email, danh tính, nhật ký, đám mây và các nguồn khác	Một trong những bộ dữ liệu quản lý sự cố toàn diện lớn nhất trong ngành	Hệ thống phòng thủ tự động ngăn chặn các mối đe dọa đã biết trong khi các chuyên gia điều tra, hỗ trợ việc kiểm soát nhanh chóng các chiến thuật tấn công mới
BẠN NHẬN ĐƯỢC:				
Sự tin cậy trên quy mô lớn và theo nhu cầu, cũng như các dịch vụ có thể phát triển cùng với doanh nghiệp của bạn	Phát hiện mối đe dọa chính xác và ngăn chặn nhanh chóng, ngay cả đối với các mối đe dọa hoàn toàn mới, trong thời gian thực	Sự giám sát và bảo vệ toàn diện toàn bộ bề mặt tấn công	Quyền truy cập vào các mô hình học máy cực kỳ chính xác và luôn được cải thiện	Thời gian trung bình để kiểm soát các mối nguy hại là 15 phút hoặc ít hơn

> Mỗi khi liên hệ với đội ngũ SOC của eSentire, chúng tôi luôn được một chuyên gia an ninh tiếp đón và hướng dẫn về các sự cố một cách rõ ràng và hiệu quả. Chưa có nhà cung cấp nào cung cấp dịch vụ cá nhân hóa và chuyên môn như họ. Bằng cách sử dụng nền tảng Atlas của eSentire, kết hợp với việc tiếp cận đội ngũ tình báo mối đe dọa tinh vi của họ, chúng tôi đã có thể giảm thời gian giải quyết sự cố của mình đi một nửa.
>
> - Michael Smith, Phó Chủ tịch, Giám đốc Công nghệ Thông tin tại HKS

Không phải MDR nào cũng giống nhau

	eSentire	Nhà cung cấp khác
Hệ thống giám sát 24/7	✓	Giới hạn
Chuyên gia An ninh SOC hỗ trợ trực tuyến 24/7	✓	Giới hạn
Truy quét mối đe dọa 24/7	✓	✗
Hỗ trợ kiềm chế và tiêu diệt mối đe dọa 24/7	✓	✗
Thời gian kiểm soát trung bình 15 phút	✓	✗
Nền tảng Đám mây XDR sử dụng Học máy mạnh mẽ	✓	✗
Trực quan và Phủ sóng đa tín hiệu (Điểm cuối, Mạng, Nhật ký, Đám mây, Email, Danh tính, Lỗ hổng, Tổ chức)	✓	✗
Phát hiện tự động với Chữ ký, IOC và Địa chỉ IP	✓	Giới hạn
Phát hiện được dẫn tới Khung làm việc MITRE ATT&CK	✓	Giới hạn
Phát hiện các cuộc tấn công không xác định bằng cách sử dụng mẫu và phân tích hành vi	✓	Giới hạn
Cảnh báo về các hoạt động đáng ngờ	✓	Giới hạn
Phân loại và xác nhận các cảnh báo	✓	Giới hạn
Chuyên viên vào cuộc điều tra nhanh chóng	✓	Giới hạn
Cô lập và kiểm soát mối đe dọa	✓	Giới hạn
Hỗ trợ và xác minh việc phục hồi	✓	Giới hạn
Biểu đồ trực tiếp trên Cổng thông tin	✓	Giới hạn
Cảnh báo mối đe dọa, nghiên cứu và lãnh đạo tư duy	✓	Giới hạn
Cố vấn rủi ro An ninh Mạng	✓	✗
Dịch vụ Bảo mật bổ sung bao gồm Quản lý lừa đảo và Đào tạo nhận thức bảo mật, Lập kế hoạch phản ứng khi bị xâm nhập bảo mật, Phản ứng trường hợp khẩn cấp và nhiều hơn nữa	✓	Giới hạn

> Chúng tôi đã sử dụng hệ thống Atlas trong một thời gian dài và rất hài lòng khi thấy việc bảo vệ điểm cuối được thêm vào danh sách dịch vụ chúng tôi nhận thật dễ dàng. Điều này không đòi hỏi quá nhiều công việc từ đội ngũ IT của chúng tôi và củng cố sự an tâm trong bối cảnh đầy rẫy nguy hiểm như hiện nay.
>
> - Neil Waugh, Giám đốc Thông tin tại M&C Saatchi

VIII. Lời kết

Những xu hướng hiện tại không có dấu hiệu đảo ngược trong thời gian sắp tới. Việc áp dụng điện toán đám mây và làm việc từ xa sẽ tiếp tục tăng lên, môi trường máy tính doanh nghiệp sẽ tiếp tục phức tạp hóa và các kẻ tấn công sẽ tiếp tục tìm kiếm điểm yếu nhất trong hệ thống phòng thủ của bạn. Các biện pháp kiểm soát bảo mật truyền thống và Dịch vụ Quản lý An ninh Mạng đã từng hiệu quả, nhưng chúng không thể sánh kịp với những mối đe dọa hiện đại.

Đồng hành cùng eSentire, bạn được bảo vệ bởi nhà tiên phong hàng đầu trong ngành, được hỗ trợ bởi một nền tảng XDR tích hợp trên hệ thống đám mây. Điều này có nghĩa là chúng tôi có khả năng thấy và chặn những gì các nhà cung cấp MDR khác sẽ bỏ qua.

eSentire được công nhận toàn cầu là "Chuyên gia hàng đầu" trong Nền tảng Quản lý, Nhận diện và Xử lý vì chúng tôi hỗ trợ chương trình an ninh mạng của bạn bằng cách kết hợp công nghệ tiên tiến XDR sử dụng máy học, chuyên môn săn mối đe dọa 24/7, và lãnh đạo vận hành an ninh để giảm thiểu rủi ro kinh doanh và thúc đẩy phát triển chương trình an ninh mạng của bạn.

Bạn sẵn sàng chưa?

Kết nối với một Chuyên gia an ninh của eSentire để biết thêm về cách mà dịch vụ Đa tín hiệu MDR, được hỗ trợ bởi Hệ thống Đám mây Atlas XDR của chúng tôi, có thể cung cấp giải pháp bảo mật cho doanh nghiệp của bạn.

Liên Hệ Chúng Tôi

Đang gặp phải sự cố bảo mật hoặc bị tấn công? Liên hệ ngay 1-866-579-2200

eSENTIRE ADVANCE VISION TECHNOLOGY