CÔNG TY TNHH THƯƠNG MẠI VÀ DỊCH VỤ KTD
Địa chỉ: Thửa đất số 136A+136B, Tổ dân phố số 2, Phường Hải An, Thành phố Hải Phòng, Việt Nam.
- Mã số thuế: 0200659600
- Điện thoại: 0225 7308688 Fax: 0225 3630889

TÀI LIỆU XDR

DÀNH CHO NGƯỜI MỚI BẮT ĐẦU

HẢI PHÒNG, NĂM 2025

MỤC LỤC

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

THÔNG TIN VỀ PALO ALTO VÀ CORTEX

Về Palo Alto Networks

Palo Alto Networks, công ty hàng đầu toàn cầu về an ninh mạng, đang định hình tương lai lấy đám mây làm trung tâm bằng công nghệ giúp thay đổi cách thức vận hành của con người và tổ chức.

Sứ mệnh của chúng tôi là trở thành đối tác an ninh mạng được lựa chọn, bảo vệ lối sống số của chúng ta. Chúng tôi giúp giải quyết những thách thức bảo mật lớn nhất thế giới bằng sự đổi mới liên tục, tận dụng những đột phá mới nhất trong trí tuệ nhân tạo, phân tích, tự động hóa và điều phối. Bằng cách cung cấp một nền tảng tích hợp và trao quyền cho một hệ sinh thái đối tác ngày càng phát triển, chúng tôi đang đi đầu trong việc bảo vệ hàng chục nghìn tổ chức trên khắp các môi trường đám mây, mạng và thiết bị di động. Tầm nhìn của chúng tôi là một thế giới nơi mỗi ngày đều an toàn và bảo mật hơn ngày hôm trước.

Để biết thêm thông tin, vui lòng truy cập www.paloaltonetworks.com.

Về Cortex của Palo Alto Networks

Cortex® của Palo Alto Networks đã định nghĩa lại các giải pháp cho hoạt động an ninh nhằm giúp các tổ chức mang lại trải nghiệm trung tâm điều hành an ninh (SOC) hiện đại. Cortex cung cấp khả năng phát hiện mối đe dọa, phòng chống, quản lý bề mặt tấn công và tự động hóa an ninh tốt nhất trong một nền tảng tích hợp được hỗ trợ bởi học máy và thông tin tình báo về mối đe dọa từ Unit 42.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

GIỚI THIỆU

Năm này qua năm khác, thách thức trong việc bảo vệ dữ liệu quan trọng ngày càng gia tăng khi việc áp dụng nhanh chóng các xu hướng như AI, điện toán đám mây và chuyển đổi số làm tăng rủi ro đối với dữ liệu nhạy cảm của các công ty. Đồng thời, các tác nhân đe dọa cũng lợi dụng chính những xu hướng công nghệ này để mở rộng sức mạnh và quy mô của các cuộc tấn công ngày càng tinh vi.

Các đội ngũ bảo mật đã triển khai các công cụ, thực hiện các quy trình và tuyển dụng nhân sự để đối phó với các mối đe dọa mới khi chúng xuất hiện, nhưng họ đang ở thế yếu cả về số lượng và trang bị. Việc liên tục bổ sung các tính năng mới vào các hệ thống hiện có nhanh chóng tạo ra các công cụ tích hợp kém, đòi hỏi nhiều thời gian, công sức và kỹ năng vốn đã khan hiếm.

Các quy trình tĩnh không thích ứng với các xu hướng và môi trường thay đổi nhanh chóng như đám mây và làm việc từ xa sẽ nhanh chóng trở nên lỗi thời và kém hiệu quả. Các nhà phân tích bảo mật được giao nhiệm vụ gần như bất khả thi là phân loại một cơn lũ cảnh báo an ninh không bao giờ dứt, nhưng thường là họ được đào tạo hạn chế và các công cụ cũng hạn chế không kém. Quá nhiều cảnh báo và quá ít bối cảnh khiến các đội ngũ bảo mật mất đi tầm nhìn và khả năng kiểm soát. Cuối cùng, công ty càng trở nên rủi ro hơn.

Phát hiện và Phản hồi Mở rộng (Extended Detection and Response - XDR) đã nổi lên như một giải pháp cho sự phức tạp này. XDR là một loại giải pháp phát hiện, điều tra và phản hồi mối đe dọa hoạt động phối hợp trên tất cả các vector tấn công trong cơ sở hạ tầng của công ty — bao gồm mạng, điểm cuối, đám mây và định danh — thay vì chỉ một khía cạnh của cơ sở hạ tầng. Bằng cách tích hợp trực tiếp vào kiến trúc, các công cụ XDR được thiết kế để cung cấp thông tin chi tiết và khuyến nghị về mối đe dọa nhằm tối ưu hóa cách thức hoạt động của các đội ngũ bảo mật.

Về Cuốn sách này

XDR Dành Cho Người Mới Bắt Đầu giúp bạn cập nhật kiến thức về loại giải pháp bảo mật XDR và ý nghĩa của nó đối với công ty của bạn. Cuốn sách này bao gồm năm chương, khám phá các nội dung sau:

- Thực trạng hiện tại của việc phát hiện và hành động, bao gồm các mối đe dọa, hạn chế và thách thức (Chương 1)
- XDR là gì và không phải là gì (Chương 2)
- Cách XDR phá vỡ vòng đời tấn công để ngăn chặn các cuộc tấn công (Chương 3)
- Các trường hợp sử dụng XDR khác nhau (Chương 4)
- Các năng lực và tính năng bắt buộc phải có của XDR (Chương 5)

Mỗi chương được viết để có thể đọc độc lập, vì vậy nếu bạn thấy một chủ đề nào đó thu hút sự quan tâm của mình, hãy thoải mái chuyển đến chương đó. Bạn có thể đọc cuốn sách này theo bất kỳ thứ tự nào phù hợp với bạn (mặc dù tôi không khuyến khích đọc ngược từ dưới lên hoặc từ sau ra trước).

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

Các giả định

Người ta nói rằng hầu hết các giả định đều đã lỗi thời, nhưng tôi vẫn giả định một vài điều!

Chủ yếu, tôi giả định rằng bạn làm việc cho một tổ chức đang tìm kiếm một cách tốt hơn để cải thiện hiệu quả của chiến lược bảo mật, cụ thể là khả năng phát hiện và phản hồi. Có thể bạn là một nhà điều hành CNTT như giám đốc an ninh thông tin (CISO), giám đốc thông tin (CIO), giám đốc công nghệ (CTO), hoặc phó chủ tịch hay giám đốc bảo mật. Hoặc có thể bạn là một kiến trúc sư hoặc kỹ sư mạng hay bảo mật. Do đó, cuốn sách này được viết cho độc giả có kiến thức kỹ thuật với sự hiểu biết chung về các khái niệm và công nghệ vận hành an ninh hiện đại.

Nếu bất kỳ giả định nào trong số này mô tả đúng về bạn, đây chính là cuốn sách dành cho bạn! Nếu không có giả định nào mô tả đúng về bạn, hãy cứ tiếp tục đọc — XDR là một công nghệ phải biết, và đội ngũ của bạn sẽ cảm ơn bạn vì đã trở thành một chuyên gia về XDR!

Ngoài cuốn sách

Tôi chỉ có thể đề cập đến một lượng thông tin nhất định trong cuốn sách ngắn này, vì vậy nếu bạn đọc đến cuối và nghĩ rằng, “Chà, đây là một cuốn sách tuyệt vời! Tôi có thể tìm hiểu thêm ở đâu?”, hãy truy cập

www.paloaltonetworks.com/cortex/cortex-xdr.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

CHƯƠNG 1: NHÌN LẠI THỰC TRẠNG PHÁT HIỆN VÀ PHẢN HỒI MỐI ĐE DỌA

Trong chương này, tôi sẽ giải thích các mối đe dọa hiện đại đã phát triển như thế nào để có khả năng phá hoại lớn hơn; tại sao các phương pháp phòng chống, phát hiện và phản hồi truyền thống không còn đủ hiệu quả; và làm thế nào tình trạng quá tải cảnh báo và thiếu hụt kỹ năng an ninh mạng làm tăng rủi ro cho tổ chức của bạn.

1. Khảo sát Bối cảnh Mối đe dọa Hiện đại

Các vụ vi phạm dữ liệu và tấn công ransomware đã trở nên thường xuyên đến mức chúng gần như xứng đáng có một chuyên mục tin tức riêng bên cạnh thời tiết, thể thao và giao thông. Tuy nhiên, việc các sự kiện an ninh này trở nên phổ biến không làm chúng bớt nguy hiểm. Mỗi phút một tác nhân đe dọa hoạt động trong môi trường của bạn, thiệt hại to lớn sẽ xảy ra.

Theo Viện Ponemon, vào năm 2023, chi phí trung bình của một vụ vi phạm dữ liệu đã lên tới 4.45 triệu USD. Đây là chi phí cao nhất từng được ghi nhận trong một năm.

Tất nhiên, bạn đã biết và đang sống trong thực tế này, và bạn làm việc chăm chỉ để phát hiện các mối đe dọa và phản hồi nhanh chóng và hiệu quả nhất có thể trước khi mất mát dữ liệu có thể xảy ra. Tuy nhiên, đây là một cuộc chiến đầy cam go trước các chiến thuật, kỹ thuật và quy trình (Tactics, Techniques, procedures - TTPs) ngày càng tiên tiến được các tác nhân đe dọa sử dụng.

Những kẻ tấn công giờ đây có thể xâm nhập vào một môi trường gần như theo ý muốn, mà không cần sử dụng các phương pháp truyền thống như phần mềm độc hại dựa trên tệp. Thay vào đó, chúng sẽ sử dụng các phương pháp xâm phạm các tệp hệ thống được ủy quyền, chèn các cuộc tấn công vào registry của thiết bị, hoặc sử dụng các tiện ích như PowerShell một cách độc hại. Sự gia tăng của các phương pháp tấn công mới và lẩn tránh hơn đã thúc đẩy nhu cầu về các chiến lược và chiến thuật mới để phát hiện và phản hồi, bên cạnh việc phòng chống mối đe dọa.

Khả năng của một tổ chức để theo kịp bối cảnh mối đe dọa hiện đại đòi hỏi các công cụ hiệu quả và một đội ngũ các nhà phân tích bảo mật có năng lực. Thật không may, việc có được sự cân bằng hợp lý giữa công nghệ và các chuyên gia lành nghề lại là ngoại lệ đối với hầu hết các tổ chức, thay vì là quy luật.

2. Nhận diện hạn chế của các công nghệ và phương pháp truyền thống

Trong khi các đội ngũ bảo mật của bạn cố gắng ngăn chặn các cuộc tấn công thành công vào tổ chức, bạn phải chuẩn bị cho một thực tế không thể tránh khỏi rằng không có môi trường nào là an toàn tuyệt đối. Cuối cùng, một mối đe dọa sẽ xâm nhập vào môi trường của bạn.

Một loạt các công cụ ghi nhật ký, phát hiện và phản hồi đã ra đời để giúp các đội ngũ bảo mật tìm ra các mối đe dọa. Mỗi công cụ này đều có điểm mạnh và điểm yếu và có thể hữu ích chống lại các cuộc tấn công như các sự cố phần mềm

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

độc hại dựa trên tệp đã biết hoặc các cuộc tấn công được thiết kế để đánh bại chỉ một phần của cơ sở hạ tầng. Tuy nhiên, hầu hết các công cụ này được tinh chỉnh cho một mục đích duy nhất, và không có công cụ nào đặc biệt phù hợp để xử lý các mối đe dọa tinh vi một mình.

Nghiên cứu của ESG cho thấy **66%** các tổ chức cảm thấy hiệu quả phát hiện và phản hồi mối đe dọa của họ bị hạn chế vì nó dựa trên nhiều công cụ độc lập. Trong các phần sau, tôi sẽ xem xét kỹ hơn một số công cụ ghi nhật ký, phát hiện và phản hồi phổ biến hơn được các đội ngũ bảo mật sử dụng, và thông tin cho bạn về những thách thức và hạn chế của chúng.

3. Phát hiện và phản hồi điểm cuối

Phát hiện và Phản hồi Điểm cuối (Endpoint Detection and Response - EDR) là một loại công cụ được sử dụng để phát hiện và điều tra các mối đe dọa trên các thiết bị điểm cuối. Các công cụ EDR thường cung cấp các khả năng phòng chống, phát hiện, phân tích, điều tra và phản hồi.

EDR lần đầu tiên xuất hiện vào năm 2013 để hỗ trợ các cuộc điều tra pháp y đòi hỏi dữ liệu đo lường từ xa (telemetry) rất chi tiết từ điểm cuối để phân tích ngược phần mềm độc hại và hiểu chính xác những gì một tác nhân đe dọa đã làm trên một thiết bị bị xâm nhập.

Các công cụ EDR giám sát các sự kiện được tạo ra bởi các tác nhân (agent) điểm cuối để tìm kiếm hoạt động đáng ngờ. Các cảnh báo mà công cụ EDR tạo ra giúp các nhà phân tích hoạt động bảo mật xác định, điều tra và khắc phục sự cố. Các công cụ EDR cũng thu thập dữ liệu đo lường từ xa về hoạt động đáng ngờ và có thể làm phong phú dữ liệu đó bằng thông tin ngữ cảnh khác từ các sự kiện có liên quan. EDR đóng vai trò quan trọng trong việc rút ngắn thời gian phản hồi cho các đội ứng phó sự cố thông qua các chức năng này.

Tuy nhiên, chỉ riêng EDR không thể cung cấp khả năng phát hiện mối đe dọa trên toàn doanh nghiệp do chỉ tập trung vào điểm cuối. Nó không cung cấp tầm nhìn vào lưu lượng mạng và các thiết bị mạng như router, switch, máy chủ, thiết bị Internet of Things (IoT), thiết bị cá nhân (BYOD), và hệ thống điều khiển công nghiệp (ICS) - cũng như các tài nguyên đám mây như workload, mạng đám mây, và các dịch vụ nền tảng (PaaS).

4. Nền tảng bảo vệ điểm cuối

Nền tảng Bảo vệ Điểm cuối (Endpoint Protection Platform - EPP) là một tác nhân phần mềm được cài đặt trên các thiết bị điểm cuối để ngăn chặn các cuộc tấn công phần mềm độc hại dựa trên tệp và phát hiện hoạt động độc hại. EPP là sự phát triển của các giải pháp chống virus và chống phần mềm độc hại truyền thống trên máy chủ và thường được coi là tuyến phòng thủ đầu tiên trên một điểm cuối.

Khả năng phát hiện giữa các giải pháp EPP khác nhau, nhưng hầu hết đều sử dụng một sự kết hợp của các kỹ thuật phát hiện và phòng chống, bao gồm:

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

- Các chỉ số xâm phạm tĩnh (IOCs; tức là, phát hiện dựa trên chữ ký)
- Danh sách trắng (cho phép) hoặc danh sách đen (chặn) các ứng dụng, URL, cổng và địa chỉ
- Phân tích hành vi và học máy
- Sandboxing để "kích nổ" (hoặc kiểm tra) các mối đe dọa bị nghi ngờ, chẳng hạn như các tệp thực thi

Một giải pháp EPP nên được quản lý trên đám mây để cho phép giám sát và thu thập dữ liệu hoạt động liên tục, cùng với khả năng thực hiện các hành động khắc phục từ xa cho dù điểm cuối đang được sử dụng trên mạng công ty hay từ xa. Ngoài ra, các giải pháp EPP được hỗ trợ bởi dữ liệu đám mây. Nói cách khác, tác nhân điểm cuối không cần phải duy trì một cơ sở dữ liệu cục bộ về tất cả các IOC đã biết; thay vào đó, tác nhân điểm cuối có thể kiểm tra một tài nguyên đám mây để tìm các phán quyết mới nhất về các đối tượng mà nó không thể phân loại và tận dụng thông tin tình báo về mối đe dọa theo thời gian thực.

EPP được thiết kế hoàn toàn để phòng chống hoặc kiểm soát, và do đó, không tập trung vào việc phát hiện hoặc thu thập thông tin để phòng thủ chống lại các cuộc tấn công hiện đại. Hầu hết các nền tảng EPP cũng thiếu các khả năng phản hồi cần thiết để điều tra sự cố. Do đó, chỉ riêng EPP không cung cấp các tính năng thiết yếu để ngăn chặn các cuộc tấn công hiện đại. Vì lý do đó, nhiều nhà cung cấp bảo mật cung cấp chức năng EDR cùng với EPP.

5. Quản lý sự kiện và thông tin bảo mật

Các công cụ phần mềm Quản lý Sự kiện và Thông tin Bảo mật (Security Information and Event Management - SIEM) cung cấp khả năng thu thập, tương quan và phân tích gần như thời gian thực các sự kiện bảo mật, cũng như thông báo về các cảnh báo bảo mật được tạo ra bởi các thiết bị và ứng dụng mạng khác nhau.

Nhiều tổ chức phân bổ một phần lớn ngân sách bảo mật của họ cho các công cụ SIEM để thu thập nhật ký từ các thiết bị bảo mật và môi trường máy chủ khác nhau. SIEM ban đầu được thiết kế chủ yếu như một công cụ thu thập nhật ký cho mục đích báo cáo tuân thủ. Theo thời gian, việc sử dụng chúng đã mở rộng sang phát hiện mối đe dọa, và SIEM hiện là kho lưu trữ cảnh báo trung tâm cho nhiều trung tâm điều hành an ninh (SOC).

Một SIEM tập trung hóa các cảnh báo và tổng hợp dữ liệu nhật ký bằng cách phân tích và chuẩn hóa nó. Các đội ngũ bảo mật có thể xem tất cả dữ liệu nhật ký ở một nơi. Tuy nhiên, nó thường không được ghép nối một cách có ý nghĩa, và các nhà phân tích tuyến đầu được giao nhiệm vụ hiểu rõ nó thường không thể sử dụng các công cụ chứa dữ liệu nguồn phong phú hơn để xác thực các cảnh báo. Nhìn chung, SIEM thiếu chiều sâu phân tích cho các nguồn dữ liệu chính, chẳng hạn như dữ liệu điểm cuối và dữ liệu mạng, và chúng có thể khó triển khai, cấu hình và bảo trì, một phần vì chúng thiếu kiến thức sẵn có này.

6. Phát hiện và phản hồi mạng và phân tích hành vi người dùng và thực thể

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

Các công cụ Phát hiện và Phản hồi Mạng (Network Detection and Response - NDR) và Phân tích Hành vi Người dùng và Thực thể (User and Entity Behavior Analytics - UEBA) đại diện cho một lớp công cụ phân tích bảo mật mới hơn đã xuất hiện để giải quyết những thách thức mà SIEM gặp phải trong việc phát hiện các cuộc tấn công không xác định. Các công cụ này sử dụng học máy để phát triển một đường cơ sở hoạt động từ dữ liệu đo lường từ xa đã thu thập và sau đó tìm kiếm các hành động bất thường có thể chỉ ra hành vi độc hại. Những công nghệ này cho phép các tổ chức xác định các cuộc tấn công chưa từng được biết đến trước đây bằng cách nhận ra các mẫu lưu lượng bất thường.

UEBA ngày càng được gọi là Phát hiện và Phản hồi Mối đe dọa Định danh (Identity Threat Detection and Response - ITDR), và trong những trường hợp như vậy, nó biểu thị một sự tiến bộ trong phân tích phát hiện mối đe dọa và các hành động phản hồi đối với các mối đe dọa dựa trên định danh.

Tuy nhiên, các công cụ này cũng có những hạn chế. Các sản phẩm dựa trên mạng bị giới hạn trong phạm vi mạng và không thể giám sát hoặc theo dõi các sự kiện cục bộ, chẳng hạn như thông tin quy trình được thu thập trên các điểm cuối. NDR cũng có chiều sâu rất hạn chế; nếu EDR sâu và hẹp, thì NDR rộng và nông.

Sự phức tạp của các cuộc tấn công hiện đại đòi hỏi phải phân tích nhiều nguồn dữ liệu để xác định và xác nhận hoạt động độc hại. Việc xếp chồng các công cụ một chiều làm tăng đáng kể chi phí cho các đội ngũ bảo mật, tạo ra các điểm mù tiềm ẩn, và đòi hỏi nhiều nỗ lực thủ công từ phía các nhà phân tích bảo mật để chuyển đổi giữa các bảng điều khiển và hiểu rõ một cuộc tấn công.

7. Quá nhiều Cảnh báo, Quá ít Thời gian và Nhân sự

Các công cụ phát hiện và phòng chống tạo ra hàng ngàn cảnh báo mỗi ngày — vượt xa khối lượng mà các đội ngũ bảo mật có đủ nhân lực để xử lý hiệu quả. Những cảnh báo này đến từ nhiều nguồn không kết nối, khiến các nhà phân tích bảo mật phải tự mình ghép nối các mảnh ghép.

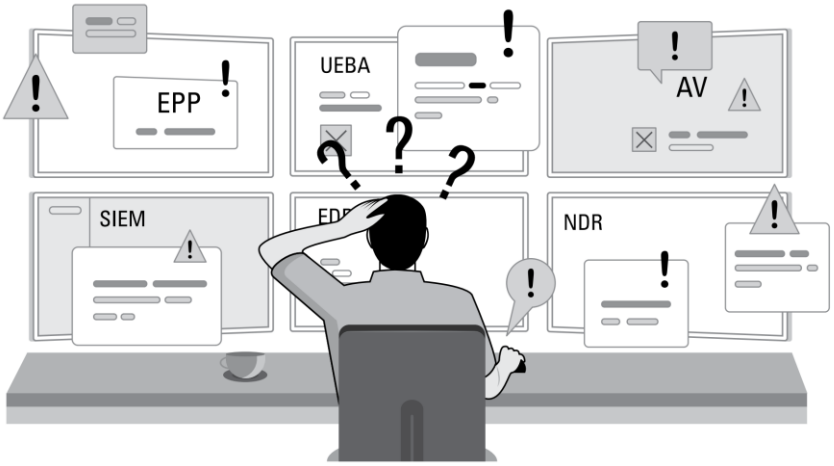

Figure 1: Các công cụ riêng lẻ làm chậm quá trình điều tra và phản hồi.

Sơ đồ mô tả các công cụ bảo mật riêng lẻ như UEBA, EPP, SIEM, EDR, NDR, và AV (Antivirus) hoạt động độc lập, tạo ra các cảnh báo phân mảnh và làm chậm

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

quá trình ứng phó.

Phân tích một mối đe dọa tiềm tàng thường đòi hỏi một số bước:

- Xem xét dữ liệu nhật ký có sẵn để bắt đầu ghép nối những gì có thể đã xảy ra.
- So sánh thủ công dữ liệu với các nguồn thông tin tình báo về mối đe dọa để xác định xem các chỉ số có được biết là độc hại hay không.
- Tìm kiếm các sự kiện liên quan bằng cách sử dụng IOC để xác định xem cảnh báo có phải là một phần của một cuộc tấn công lớn hơn hay không.
- Thu thập bối cảnh xung quanh sự cố, bao gồm các hệ thống, máy chủ, tài sản, tài nguyên, địa chỉ IP và các tệp liên quan đến mỗi cảnh báo.
- Xây dựng một dòng thời gian và xác định nguyên nhân gốc rễ của một cảnh báo.
- Kiểm tra xem các thành viên khác trong nhóm có đang xử lý các liên kết thông tin mới đến các cảnh báo để phối hợp nỗ lực hay không.
- Đánh giá xem cảnh báo có cần được leo thang, loại bỏ, hoặc khắc phục nhanh chóng và đóng lại hay không.

Tất cả các bước này tốn rất nhiều thời gian và cần nhiều công cụ để hoàn thành trong một SOC truyền thống — và đó mới chỉ là việc phân loại. Kết quả cuối cùng là các nhà phân tích chỉ có thời gian để giải quyết các cảnh báo "ưu tiên cao nhất" mà họ gặp phải mỗi ngày; trong khi đó, một số lượng đáng lo ngại các cảnh báo "ưu tiên thấp hơn" hoàn toàn không được giải quyết. Và nếu không có bối cảnh phù hợp để phân loại một cảnh báo là "cao" hay "thấp", SOC có thể đang bỏ lỡ những gì quan trọng và/hoặc theo đuổi các vấn đề không nghiêm trọng.

Hơn nữa, các nhà phân tích bảo mật chịu trách nhiệm phân loại cảnh báo thường không có đủ bối cảnh để xác định rủi ro thực sự mà một cuộc tấn công gây ra cho tổ chức. Do đó, cảnh báo được leo thang lên một nhóm cấp cao hơn để xác thực thêm, đòi hỏi nhiều thời gian, công sức và tài nguyên hơn — tạo ra sự kém hiệu quả ở mọi cấp độ.

Hầu hết các doanh nghiệp nhận được hàng ngàn cảnh báo từ vô số các giải pháp giám sát, nhưng nhiều tiếng ồn hơn lại phản tác dụng. Phát hiện nâng cao không phải là về việc có nhiều cảnh báo hơn mà là về các cảnh báo tốt hơn, có thể hành động được. Để đạt được loại phát hiện nâng cao này đòi hỏi sự tích hợp của tất cả các công nghệ phát hiện đang được sử dụng, cũng như các phân tích tinh vi phân tích dữ liệu điểm cuối, mạng, đám mây và định danh để tìm và xác thực hoạt động của đối thủ trong môi trường của bạn.

8. ĐỘI NGŨ SOC LÀM GÌ?

Các đội ngũ vận hành an ninh, dù lớn hay nhỏ, đều chia sẻ một số chức năng chính. Một mô hình truyền thống cho nhiều đội SecOps và SOC chia các chức năng này thành một cấu trúc phân tích theo cấp, dựa trên mức độ kinh nghiệm. Dưới đây là các trách nhiệm chính của các cấp đó:

- **Cấp 1 - Phân loại:** Đây là nơi phần lớn thời gian của các nhà phân tích bảo

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

mật thường được dành ra. Các nhà phân tích Cấp 1 thường là những người ít kinh nghiệm nhất, và chức năng chính của họ là giám sát nhật ký sự kiện để tìm hoạt động đáng ngờ. Khi họ cảm thấy có điều gì đó cần điều tra thêm, họ thu thập càng nhiều bối cảnh từ càng nhiều nguồn càng tốt vào một báo cáo dưới dạng một sự cố bao gồm người dùng, máy chủ, địa chỉ IP, và bất kỳ IOC liên quan nào, và leo thang sự cố lên Cấp 2.

- **Cấp 2 - Điều tra:** Các nhà phân tích Cấp 2 đào sâu hơn vào hoạt động đáng ngờ để xác định bản chất của mối đe dọa và mức độ nó đã xâm nhập vào môi trường, bao gồm việc xây dựng một dòng thời gian để hiểu trình tự và tương quan các sự kiện để xác định nguyên nhân gốc rễ. Họ phải thực hiện điều tra thêm để hiểu cuộc tấn công đã đi xa đến đâu. Các nhà phân tích này sau đó phối hợp một phản ứng để khắc phục vấn đề. Đây là một hoạt động có tác động cao hơn thường đòi hỏi nhiều kinh nghiệm phân tích hơn.
- **Cấp 3+ - Săn lùng mối đe dọa:** Đây là những nhà phân tích có kinh nghiệm nhất, những người hỗ trợ ứng phó sự cố phức tạp và dành bất kỳ thời gian còn lại để tìm kiếm trong dữ liệu pháp y và đo lường từ xa các mối đe dọa có thể chưa được phần mềm phát hiện xác định là đáng ngờ.

Công ty trung bình dành ít thời gian nhất cho các hoạt động săn lùng mối đe dọa, bởi vì các hoạt động của Cấp 1 và Cấp 2 tiêu tốn rất nhiều tài nguyên phân tích. Mặc dù mô hình này có thể là phổ biến nhất, nhưng nó không nhất thiết là lý tưởng. Hầu hết mọi người không phù hợp để giám sát nhật ký cả ngày. Tình trạng quá tải cảnh báo là có thật, và các mối đe dọa lọt qua giữa tất cả tiếng ồn được tạo ra bởi vô số cảm biến trong một SOC. Có thể khó giữ chân các nhà phân tích để thực hiện nhiệm vụ này — họ thà đóng góp một cách có ý nghĩa vào các cuộc điều tra (và có thể có những cách tiếp cận mới và sáng tạo không bao giờ được tiết lộ vì họ không có các kỹ năng kỹ thuật cần thiết cho các quy trình điều tra cũ). Quá ít thời gian được dành cho việc săn lùng mối đe dọa và cải tiến quy trình vì phần lớn thời gian tài nguyên được dành để phát hiện và giảm thiểu các mối đe dọa.

Ngay cả với các công cụ tốt hơn và toàn diện hơn để phát hiện mối đe dọa, việc xử lý các cảnh báo — và các sự cố có thể xảy ra — đòi hỏi phải có sự xác thực và phân loại thêm từ các chuyên gia ứng phó có tay nghề. Thật không may, không có đủ các chuyên gia bảo mật này, và khoảng trống kỹ năng đáng kể này ảnh hưởng đến khả năng của các tổ chức để theo kịp những kẻ tấn công.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

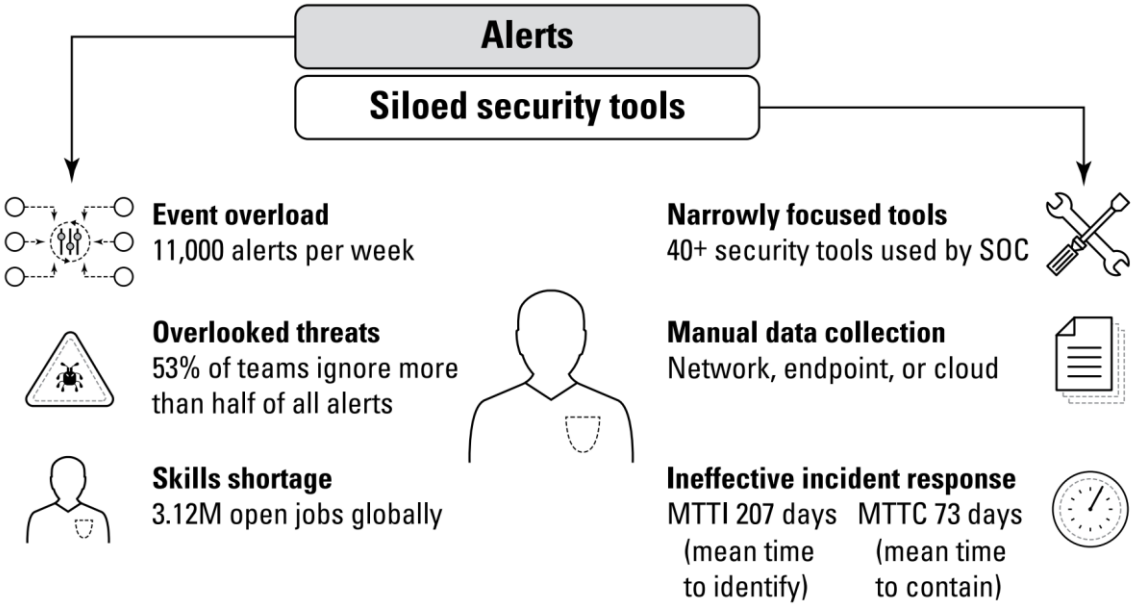

Figure 2: Nhiều thách thức của một nhà phân tích bảo mật.

Sơ đồ mô tả các thách thức bao gồm: Quá tải sự kiện (11,000 cảnh báo mỗi tuần), các công cụ bảo mật riêng lẻ (hơn 40 công cụ), bỏ qua các mối đe dọa (53% đội ngũ bỏ qua hơn một nửa số cảnh báo), thiếu hụt kỹ năng (3.12 triệu việc làm còn trống trên toàn cầu), và ứng phó sự cố không hiệu quả (thời gian trung bình để xác định là 207 ngày, thời gian trung bình để ngăn chặn là 73 ngày).

Các tác nhân đe dọa sử dụng các công cụ và kỹ thuật tự động hóa cao để tìm ra các lỗ hổng và giành quyền truy cập ban đầu vào môi trường của bạn. Điều này càng làm trầm trọng thêm khoảng trống kỹ năng vì những kẻ tấn công có thể mở rộng quy mô bộ công cụ tự động của chúng nhanh hơn và với chi phí thấp hơn so với việc các tổ chức có thể bổ sung nhân sự bảo mật có tay nghề. Vì vậy, bạn cần tìm kiếm các công cụ có thể:

- Làm cho nhân viên ít kinh nghiệm của bạn hiệu quả và năng suất hơn
- Tự động hóa việc phát hiện các mối đe dọa phức tạp
- Đơn giản hóa các cuộc điều tra
- Giúp các nhà phân tích cải thiện kỹ năng của họ

Trong Nghiên cứu Lực lượng Lao động An ninh mạng năm 2023, Hiệp hội Chứng nhận Bảo mật Hệ thống Thông tin Quốc tế, hay (ISC)², báo cáo tình trạng thiếu hụt 4 triệu chuyên gia an ninh mạng có tay nghề trên toàn cầu. Theo Cyberseek, có hơn 470,000 vị trí tuyển dụng an ninh mạng tại Hoa Kỳ hiện nay — một con số dự kiến sẽ tăng đáng kể trong những năm tới.

Nhiều công ty thuê ngoài các chức năng phát hiện và phản hồi của họ, toàn bộ hoặc một phần, cho các nhà cung cấp dịch vụ bảo mật được quản lý (MSSPs) hoặc các nhà cung cấp phát hiện và phản hồi được quản lý (MDR). Việc thuê ngoài chức năng này là phổ biến (và được coi là thực tiễn tốt nhất trong nhiều trường hợp), đặc biệt đối với các đội có ngân sách bảo mật nhỏ hơn hoặc các tổ chức không có mong muốn hoặc nguồn lực để tự quản lý bảo mật của mình. Tuy nhiên,

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

các tổ chức muốn có tầm nhìn và kiểm soát toàn diện không nên bị mắc kẹt trong việc thuê ngoài bảo mật chỉ vì các công cụ của họ không đủ. Cũng cần lưu ý rằng bộ công nghệ cũng quan trọng không kém đối với một đội ngũ bảo mật thuê ngoài; các nhà cung cấp sử dụng các công cụ cũ sẽ phải vật lộn với những sự kém hiệu quả tương tự như các đội ngũ bảo mật nội bộ.

Điều cần thiết là một bộ công nghệ để giảm tổng số lượng cảnh báo đồng thời cho phép các nhà phân tích ít kinh nghiệm hơn đánh giá các mối đe dọa một cách hiệu quả và tự tin, đảm bảo rằng chỉ có các cảnh báo có độ tin cậy cao mới được leo thang lên các nhà phân tích cấp cao hơn.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

CHƯƠNG 2: ĐỊNH NGHĨA XDR

Phát hiện và Phản hồi Mở rộng (Extended Detection and Response - XDR) là một phương pháp tiếp cận toàn diện để phát hiện và phản hồi mối đe dọa. Thuật ngữ XDR được đặt ra vào năm 2018 bởi Nir Zuk, giám đốc công nghệ (CTO) và đồng sáng lập của Palo Alto Networks. Lý do cơ bản để tạo ra XDR là để ngăn chặn các cuộc tấn công hiệu quả hơn, phát hiện các kỹ thuật và chiến thuật của kẻ tấn công không thể ngăn chặn được, và giúp các đội ngũ trung tâm điều hành an ninh (SOC) phản hồi tốt hơn với các mối đe dọa cần điều tra.

Theo Forrester Research, XDR "tối ưu hóa việc phát hiện, điều tra, phản hồi và săn lùng mối đe dọa trong thời gian thực. XDR hợp nhất các phát hiện liên quan đến bảo mật từ điểm cuối với dữ liệu đo lường từ xa từ các công cụ bảo mật và kinh doanh như phân tích và hiển thị mạng (NAV), bảo mật email, quản lý định danh và truy cập, bảo mật đám mây, và nhiều hơn nữa."

Chữ **X** trong XDR là viết tắt của *extended* (mở rộng), nhưng nó đại diện cho **bất kỳ** nguồn dữ liệu nào, bởi vì việc xem xét các thành phần riêng lẻ của một môi trường một cách cô lập là không hiệu quả. XDR mang lại một phương pháp tiếp cận chủ động để phát hiện và phản hồi mối đe dọa, cung cấp tầm nhìn trên khắp các mạng, đám mây và điểm cuối trong khi áp dụng phân tích và tự động hóa để giải quyết các mối đe dọa ngày càng tinh vi hiện nay.

Trong chương này, bạn sẽ tìm hiểu XDR là gì và các yêu cầu chính của một giải pháp XDR.

1. Đảm bảo Phòng chống Mối đe dọa Mạnh mẽ

Nền tảng của XDR là khả năng phòng chống mối đe dọa vững chắc. Một giải pháp XDR nên chặn chính xác hơn 99% các mối đe dọa có thể được chặn tự động trong thời gian thực hoặc gần thời gian thực — mà không cần xác minh thủ công. Với khả năng phòng chống mối đe dọa hàng đầu, đội ngũ của bạn có thể tập trung vào việc xác định và ngăn chặn các cuộc tấn công tinh vi và lén lút hơn thay vì lãng phí thời gian điều tra mọi mối đe dọa tiềm tàng lọt qua hàng rào phòng thủ của bạn.

Để đánh bại các mối đe dọa điểm cuối, bạn cần một giải pháp mạnh mẽ với phần mềm chống virus thế hệ mới (NGAV) tích hợp có thể phát hiện và chặn mọi giai đoạn của một cuộc tấn công — từ khai thác ban đầu và cài đặt phần mềm độc hại đến các hành động bất hợp pháp được thực hiện bởi một tác nhân đe dọa đang chạy phần mềm độc hại. Mỗi lớp phòng thủ phải đủ thông minh để đánh bại các kỹ thuật lẩn tránh của tác nhân đe dọa và liên tục thích ứng để ngăn chặn các mối đe dọa mới nhất.

Hãy tìm kiếm các khả năng NGAV sau trong một giải pháp XDR:

- Phân tích cục bộ và phòng chống mối đe dọa dựa trên học máy
- Phòng chống mối đe dọa dựa trên hành vi để phân tích động các quy trình đang chạy

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

- Phòng chống khai thác theo kỹ thuật khai thác

- Phòng chống mối đe dọa đã biết dựa trên thông tin tình báo về mối đe dọa, chẳng hạn như hash của tệp

- Tích hợp tự động với dịch vụ phòng chống phần mềm độc hại dựa trên đám mây, với báo cáo phân tích và hỗ trợ kích thước tệp tối thiểu 100MB

- Chữ ký không có độ trễ để nhanh chóng cung cấp bảo vệ và chia sẻ thông tin tình báo về mối đe dọa

- Khả năng bảo vệ chống lại reverse shell

- Cập nhật công cụ phát hiện mối đe dọa một cách minh bạch

- Hồ sơ bảo mật và các ngoại lệ

- Quét điểm cuối theo yêu cầu và theo lịch trình

- Bảo vệ chống lại phần mềm độc hại, ransomware và các cuộc tấn công không dùng tệp (fileless attacks)

- Tác nhân nhẹ duy nhất để bảo vệ, phát hiện và phản hồi điểm cuối

- Hỗ trợ một loạt các hệ điều hành và máy chủ, bao gồm tất cả các máy người dùng cuối và môi trường đám mây chính

Giải pháp XDR của bạn cũng nên giảm bề mặt tấn công và bảo vệ dữ liệu nhạy cảm với các tính năng bảo vệ điểm cuối, bao gồm:

- Tường lửa máy chủ
- Mã hóa đĩa
- Kiểm soát thiết bị USB
- Các quy tắc phòng chống có thể tùy chỉnh

Cuối cùng, giải pháp XDR của bạn phải tương thích với một máy khách bảo mật mạng cho các điểm cuối để cung cấp truy cập từ xa an toàn, phòng chống mối đe dọa và lọc URL.

2. Cung cấp Tầm nhìn và Khả năng Phát hiện Toàn diện

Tầm nhìn và khả năng phát hiện là rất quan trọng để giảm thiểu mối đe dọa. Nếu bạn không thể nhìn thấy một mối đe dọa, bạn không thể xác định hoặc điều tra nó, và chắc chắn bạn không thể ngăn chặn nó. Các tác nhân đe dọa tận dụng đám mây và học máy để tiến hành các cuộc tấn công lớn, đa diện cho phép chúng thiết lập sự tồn tại lâu dài và trích xuất dữ liệu và tài sản trí tuệ có giá trị.

Điều này có nghĩa là XDR phải có khả năng hiển thị và phát hiện mạnh mẽ, bao gồm:

- **Tầm nhìn rộng và hiểu biết theo ngữ cảnh:** Các sản phẩm độc lập dẫn đến dữ liệu bị cô lập — và điều đó không hiệu quả. Bạn không thể hy vọng phòng thủ chống lại các cuộc tấn công một cách hiệu quả nếu bạn không linh hoạt trong môi trường của mình như các tác nhân đe dọa. XDR phải có khả năng hiển thị và phát hiện trên toàn bộ môi trường của bạn, tích hợp dữ liệu đo lường từ xa từ các

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

điểm cuối, mạng và môi trường đám mây của bạn. Hơn nữa, nó phải có khả năng tương quan các nguồn dữ liệu này để hiểu các sự kiện khác nhau được liên kết như thế nào và khi nào một hành vi nhất định là (hoặc không phải là) đáng ngờ dựa trên ngữ cảnh.

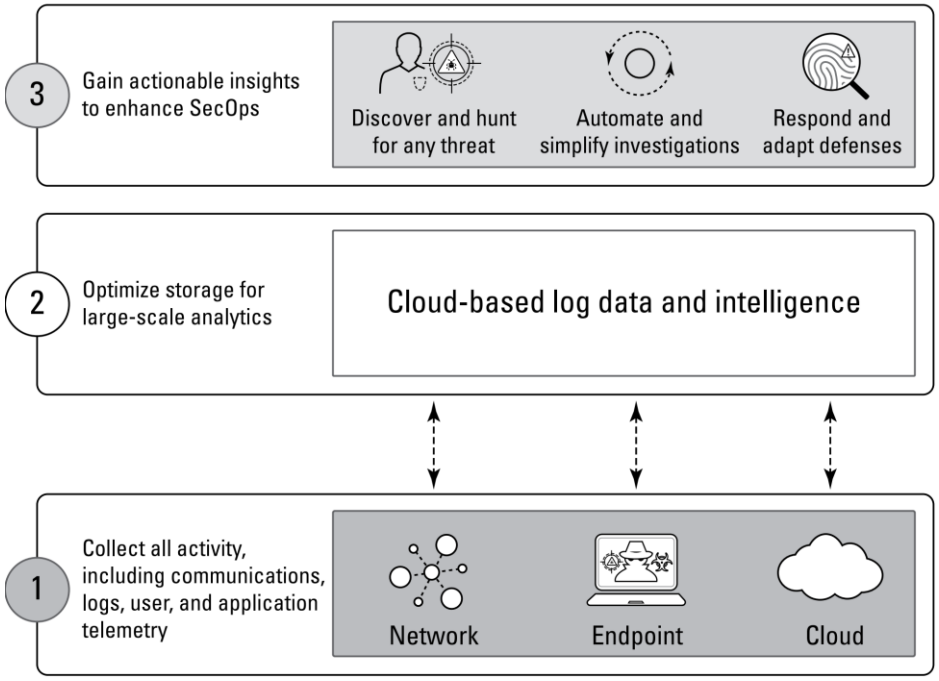

Figure 3: XDR phá vỡ các silo truyền thống của việc phát hiện và phản hồi.

Sơ đồ mô tả một quy trình 3 bước: (1) Thu thập tất cả hoạt động từ Mạng, Điểm cuối, Đám mây. (2) Tối ưu hóa lưu trữ và phân tích trên đám mây. (3) Đạt được thông tin chi tiết có thể hành động để tăng cường hoạt động bảo mật, khám phá và săn lùng mối đe dọa, tự động hóa điều tra và thích ứng phòng thủ.

- **Lưu giữ dữ liệu:** Những kẻ tấn công rất kiên nhẫn và bền bỉ. Chúng biết rằng chúng khó bị phát hiện hơn nếu di chuyển chậm, chờ đợi qua các khoảng thời gian lưu giữ nhật ký của các công nghệ phát hiện mà chúng đang đối mặt. XDR không nên làm điều này dễ dàng cho chúng. Hệ thống phát hiện của bạn cần thu thập, tương quan và phân tích dữ liệu từ mạng, điểm cuối và đám mây trong một kho lưu trữ duy nhất, cung cấp 30 ngày hoặc hơn về lưu giữ lịch sử.

- **Phân tích cả lưu lượng nội bộ và bên ngoài:** Các kỹ thuật phát hiện truyền thống chủ yếu tập trung vào những kẻ tấn công bên ngoài, cung cấp một cái nhìn không đầy đủ về các tác nhân đe dọa tiềm tàng. Việc phát hiện không thể chỉ tìm kiếm các cuộc tấn công đến từ bên ngoài vành đai. Nó cũng phải lập hồ sơ và phân tích các mối đe dọa nội bộ để tìm kiếm hành vi bất thường và có khả năng độc hại và xác định việc lạm dụng thông tin xác thực.

- **Thông tin tình báo về mối đe dọa tích hợp:** Bạn phải được trang bị để đối phó với các cuộc tấn công không xác định. Một phương pháp để cân bằng cán cân là tận dụng các cuộc tấn công đã biết mà các tổ chức khác nhìn thấy trước. Việc phát hiện cần dựa vào thông tin tình báo về mối đe dọa được thu thập trên một mạng lưới toàn cầu của các doanh nghiệp. Khi một tổ chức trong mạng lưới mở

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

rộng xác định một cuộc tấn công, bạn có thể sử dụng kiến thức thu được từ cuộc tấn công ban đầu đó để xác định các cuộc tấn công tiếp theo trong môi trường của riêng bạn.

- **Phát hiện có thể tùy chỉnh:** Việc bảo vệ tổ chức của bạn đặt ra những thách thức riêng liên quan đến các hệ thống cụ thể, các nhóm người dùng khác nhau và các tác nhân đe dọa khác nhau. Các hệ thống phát hiện cũng phải có khả năng tùy chỉnh cao dựa trên nhu cầu cụ thể của môi trường của bạn. Những thách thức này đòi hỏi một giải pháp XDR hỗ trợ cả các phát hiện tùy chỉnh và được xác định trước.

- **Phát hiện dựa trên học máy:** Với các cuộc tấn công không giống như phần mềm độc hại truyền thống, chẳng hạn như những cuộc tấn công xâm phạm các tệp hệ thống được ủy quyền, sử dụng môi trường kịch bản và tấn công registry, công nghệ phát hiện cần sử dụng các kỹ thuật phân tích tiên tiến để phân tích tất cả dữ liệu đo lường từ xa đã thu thập. Các phương pháp này bao gồm học máy có giám sát và bán giám sát.

- Hãy tìm một giải pháp XDR giải quyết các yêu cầu chính về tầm nhìn và phát hiện sau:

- Phân tích hành vi để lập hồ sơ hành vi và phát hiện các bất thường cho thấy một cuộc tấn công bằng cách phân tích lưu lượng mạng, sự kiện điểm cuối và sự kiện người dùng theo thời gian

- Khả năng học máy có giám sát và không giám sát

- Các quy tắc phát hiện dựa trên hành vi được xác định trước và có thể tùy chỉnh

- Các quy tắc tùy chỉnh có thể phát hiện các cuộc tấn công một cách hồi tố

- Loại trừ cảnh báo chi tiết để điều chỉnh tùy chọn các cảnh báo từ điểm cuối, mạng, đám mây hoặc bên thứ ba

- Chia sẻ thông tin tình báo về mối đe dọa để phân phối thông tin tình báo về mối đe dọa từ cộng đồng từ một dịch vụ phân tích phần mềm độc hại dựa trên đám mây đến tường lửa, tác nhân điểm cuối và các dịch vụ phát hiện và phản hồi

- Khả năng tiêu thụ các nguồn cấp dữ liệu thông tin tình báo về mối đe dọa từ các nguồn bên thứ ba ở định dạng JSON và CSV

- Kết hợp dữ liệu quản lý định danh và truy cập, với các phân tích phát hiện các tài khoản bị xâm nhập, leo thang đặc quyền, và nhiều hơn nữa

- Phát hiện các kỹ thuật tấn công trong suốt vòng đời tấn công, bao gồm khám phá, di chuyển ngang, chỉ huy và kiểm soát, và trích xuất dữ liệu

- Khả năng đã được chứng minh trong việc phát hiện các chiến thuật và kỹ thuật của kẻ tấn công thông qua các đánh giá MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

- Gắn thẻ các chiến thuật và kỹ thuật MITRE ATT&CK trong các cảnh báo và quy tắc phát hiện

- Quản lý tài sản với khả năng phát hiện thiết bị trái phép

- Đánh giá lỗ hổng

- Kiểm kê máy chủ với thông tin chi tiết về người dùng, hệ thống và ứng dụng

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

3. Tự động hóa Điều tra và Phản hồi

Khi bạn được cảnh báo về các mối đe dọa tiềm tàng trong môi trường của mình, bạn phải có khả năng phân loại và điều tra nhanh chóng các mối đe dọa đó. Việc thực hiện điều này một cách hiệu quả — đặc biệt là trong một cuộc tấn công ảnh hưởng đến nhiều phần của môi trường của bạn — là nơi các hệ thống phát hiện và phản hồi truyền thống thất bại.

Các giải pháp XDR có thể cải thiện đáng kể quy trình này với các khả năng điều tra và phản hồi bao gồm:

- **Tương quan và nhóm các cảnh báo và dữ liệu đo lường từ xa liên quan:** Khi nói đến các cuộc tấn công chống lại tổ chức của bạn, thời gian là yếu tố cốt lõi. Vào thời điểm bạn nhận được một cảnh báo mối đe dọa, kẻ tấn công đã làm việc cật lực để thực hiện nhiệm vụ và đạt được mục tiêu của chúng trong môi trường của bạn. Bạn cần nhanh chóng hiểu được cuộc tấn công và toàn bộ chuỗi nhân quả của nó. Điều này có nghĩa là công cụ XDR của bạn trước tiên phải giảm tiếng ồn bằng cách tự động nhóm các cảnh báo liên quan và ưu tiên hiệu quả các sự cố đòi hỏi sự chú ý khẩn cấp nhất của bạn. Sau đó, công cụ XDR của bạn phải có khả năng xây dựng một dòng thời gian của cuộc tấn công, xâu chuỗi các nhật ký hoạt động từ các môi trường mạng, điểm cuối và đám mây của bạn. Bằng cách trực quan hóa hoạt động và sắp xếp các sự kiện, nguyên nhân gốc rễ của mối đe dọa có thể được xác định, và thiệt hại và phạm vi tiềm tàng có thể được đánh giá.

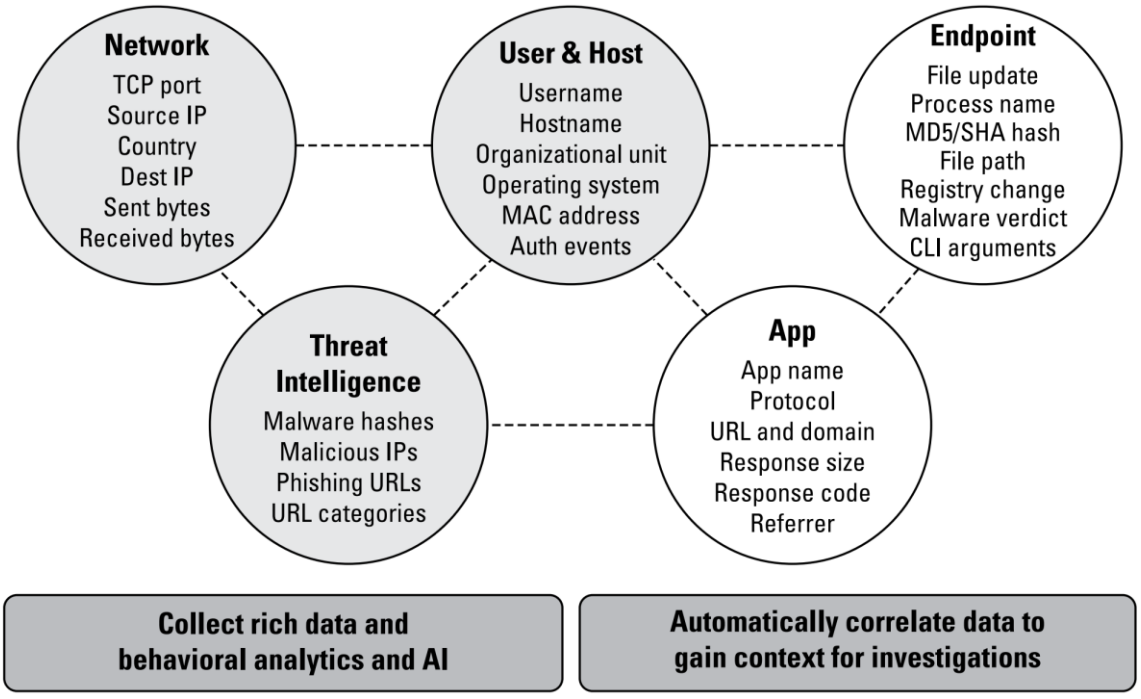

Figure 4: XDR tương quan và xâu chuỗi dữ liệu phong phú

- Sơ đồ mô tả cách XDR thu thập dữ liệu phong phú từ Mạng, Thông tin tình báo về mối đe dọa, Người dùng & Máy chủ, Ứng dụng, và Điểm cuối. Sau đó, nó sử dụng phân tích hành vi và AI để tự động tương quan dữ liệu, cung cấp bối cảnh

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

cho các cuộc điều tra.

- **Điều tra nhanh chóng các sự cố với quyền truy cập tức thì vào tất cả các tạo tác pháp y, sự kiện và thông tin tình báo về mối đe dọa ở một địa điểm:** Nhanh chóng xác định hoạt động của kẻ tấn công bằng cách xem xét các tạo tác chính như nhật ký sự kiện, khóa registry, lịch sử trình duyệt, và nhiều hơn nữa. Các công cụ mã nguồn mở ngày nay buộc các đội ngũ phải thu thập bằng chứng từ một loạt các tác nhân và kịch bản khác nhau. Các tác nhân một mục đích cho pháp y, bảo vệ điểm cuối, và phát hiện và phản hồi có thể làm chậm hiệu suất và tăng thêm sự phức tạp. Để giải quyết một sự cố, bạn cần tìm ra điểm xâm nhập và theo dõi các dấu vết còn lại — ngay cả khi đối thủ đã cố gắng che giấu dấu vết của chúng.
- **Giao diện người dùng hợp nhất với khả năng chuyển đổi nhanh chóng:** Khi họ bắt đầu đào sâu vào các cảnh báo, các nhà phân tích bảo mật của bạn cần một môi trường làm việc được sắp xếp hợp lý cho phép họ chuyển đổi trong dữ liệu từ bất kỳ nguồn nào chỉ bằng một cú nhấp chuột. Các nhà phân tích không nên lãng phí thời gian chuyển đổi giữa nhiều công cụ khác nhau.
- **Săn lùng mối đe dọa thủ công và tự động:** Ngày càng có nhiều tổ chức chủ động săn lùng các đối thủ đang hoạt động, cho phép các nhà phân tích của họ phát triển các giả thuyết tấn công và tìm kiếm hoạt động liên quan trong môi trường. Việc hỗ trợ săn lùng mối đe dọa đòi hỏi khả năng tìm kiếm mạnh mẽ để tìm kiếm bằng chứng chứng minh các giả thuyết, cũng như thông tin tình báo về mối đe dọa tích hợp để tìm kiếm hoạt động đã được nhìn thấy trong mạng lưới mở rộng. Thông tin tình báo về mối đe dọa này nên được tích hợp và tự động hóa để làm rõ liệu một mối đe dọa đã được nhìn thấy trước đây hay chưa mà không cần hàng tấn công việc phân tích thủ công (ví dụ, mở 30 tab trình duyệt khác nhau để tìm kiếm nhiều nguồn cấp dữ liệu thông tin tình báo về mối đe dọa cho một địa chỉ IP độc hại đã biết).
- **Điều phối phản hồi:** Sau khi hoạt động mối đe dọa đã được phát hiện và điều tra, bước tiếp theo là khắc phục và thực thi chính sách hiệu quả và hiệu quả. Hệ thống của bạn phải điều phối một phản ứng phối hợp đối với các mối đe dọa đang hoạt động và ngăn chặn các cuộc tấn công trong tương lai trên các môi trường mạng, điểm cuối và đám mây của bạn. Điều này bao gồm giao tiếp giữa các công nghệ phòng chống (tức là, một cuộc tấn công bị chặn trên mạng tự động cập nhật các chính sách trên các điểm cuối), hoặc là tự nhiên hoặc được xây dựng thông qua các giao diện lập trình ứng dụng (API). Nó cũng bao gồm khả năng cho một nhà phân tích thực hiện các hành động phản hồi trực tiếp thông qua giao diện XDR.

Hãy tìm kiếm các khả năng điều tra và phản hồi sau trong một giải pháp XDR:

- Phân tích nguyên nhân gốc rễ tự động của bất kỳ cảnh báo nào, bao gồm cả cảnh báo mạng, nếu có dữ liệu điểm cuối
- Trực quan hóa các chuỗi thực thi dẫn đến một cảnh báo
- Chế độ xem phân tích dòng thời gian để xem tất cả các hành động và cảnh báo trên một dòng thời gian

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

- Truy vấn các chỉ số xâm phạm (IOC) và hành vi điểm cuối, máy chủ trực tuyến và ngoại tuyến, nhật ký lưu lượng mạng từ tường lửa, và nhật ký xác thực từ các nhà cung cấp quản lý định danh
- Ngôn ngữ truy vấn nâng cao với hỗ trợ cho các ký tự đại diện, biểu thức chính quy, JSON, tổng hợp dữ liệu, thao tác trường và giá trị, hợp nhất dữ liệu từ các nguồn khác nhau, và trực quan hóa dữ liệu
- Khả năng cho một nhà phân tích dễ dàng chuyển đổi giữa các chế độ xem với bộ lọc và sắp xếp chi tiết các kết quả truy vấn
- Tổng hợp tự động thông tin IP hoặc hash liên quan, bao gồm thông tin tình báo về mối đe dọa, sự kiện và các sự cố liên quan trong một chế độ xem duy nhất để đơn giản hóa các cuộc điều tra và chặn truy cập vào các địa chỉ IP hoặc tên miền độc hại
- Xác định xem một sự kiện có bị chặn bởi một tác nhân điểm cuối, tường lửa, hoặc một công nghệ phòng chống khác hay không và khả năng xem, tạm dừng hoặc chấm dứt các quy trình đang chạy hoặc tải xuống các tệp nhị phân từ xa
- Tự động xâu chuỗi các cảnh báo bảo mật, chẳng hạn như cảnh báo tường lửa, với dữ liệu điểm cuối
- Loại bỏ nhiễu và loại bỏ các tệp nhị phân và thư viện liên kết động (DLL) không quan trọng khỏi chuỗi
- Bối cảnh của nhà phân tích SOC về các chiến thuật, kỹ thuật và quy trình (TTP) để sử dụng kiến thức thu được để giúp trong các cuộc điều tra trong tương lai
- Tích hợp với các giải pháp điều phối, tự động hóa và phản hồi an ninh (SOAR) và quản lý sự kiện và thông tin bảo mật (SIEM)
- Chấm điểm sự cố để xếp hạng và ưu tiên các sự cố có rủi ro cao để các nhà phân tích có thể nhanh chóng tập trung vào các mối đe dọa nghiêm trọng nhất; tạo điểm số sự cố dựa trên các thuộc tính cảnh báo, bao gồm người dùng hoặc máy chủ trong một cảnh báo
- Cách ly các tệp độc hại và loại bỏ chúng khỏi các thư mục làm việc của chúng
- Nhanh chóng tìm và xóa các tệp trên toàn tổ chức của bạn với Search and Destroy, lập chỉ mục các tệp điểm cuối
- Truy cập trực tiếp vào các điểm cuối với Live Terminal để chạy các lệnh hoặc kịch bản Python, PowerShell, hoặc hệ thống; xem xét và quản lý các quy trình đang hoạt động; và xem, xóa, di chuyển hoặc tải xuống các tệp

Nâng cao hiệu quả An ninh

XDR nên tăng tốc đáng kể lợi tức đầu tư (ROI) của bạn vào bảo mật. Điều này có nghĩa là tăng hiệu quả và hiệu suất của đội ngũ bảo mật của bạn để giúp ngăn chặn hoặc khắc phục tình trạng thiếu nhân sự, cải thiện sự tích hợp giữa các công cụ hiện có của bạn, và tăng cường hiệu quả phòng chống của bạn theo thời gian với cơ sở hạ tầng có thể mở rộng và trí tuệ nhân tạo (AI).

Để đáp ứng các tiêu chí này, XDR phải có các khả năng sau:

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

- **Điều phối an ninh có thể mở rộng:** Các thuộc tính tương tự làm cho việc điều phối trở nên quan trọng để đơn giản hóa các cuộc điều tra cũng cho phép nó tối đa hóa ROI của bộ công cụ bảo mật của bạn. Mọi tổ chức đều có một cơ sở các giải pháp bảo mật đã được cài đặt có thể được sử dụng để phản ứng với các mối đe dọa đang hoạt động. Một khía cạnh quan trọng của bất kỳ hệ thống phát hiện và phản hồi nào là tận dụng các khoản đầu tư vào các giải pháp hiện có này, đảm bảo bất kỳ phản ứng nào cũng có thể được thực hiện một cách nhất quán trên toàn doanh nghiệp. Các nền tảng XDR nên có thể mở rộng để bao gồm các công cụ SOAR, thêm các khả năng này trực tiếp vào quy trình làm việc của XDR.

- **Thu thập dữ liệu của bên thứ ba:** Mọi tổ chức ngày nay đều có một mớ hỗn độn các công cụ bảo mật riêng lẻ, bị cô lập. Một giải pháp XDR càng có khả năng hiển thị dữ liệu từ mỗi công cụ khác nhau đó, thì bảo mật mà nó có thể cung cấp sẽ càng toàn diện. Các giải pháp XDR tốt nhất sẽ có sự linh hoạt để thu thập dữ liệu từ các công cụ khác trong môi trường của bạn để tối đa hóa cả giá trị và hiệu quả.

- **Lưu trữ và tính toán có thể mở rộng:** Với sự bền bỉ của các tác nhân đe dọa ngày nay, bạn không muốn loại bỏ dữ liệu đo lường từ xa có thể cung cấp bằng chứng pháp y quan trọng về hoạt động của kẻ tấn công trong các cuộc tấn công "chậm và âm thầm" có thể kéo dài hàng tháng hoặc thậm chí hàng năm. Bạn cũng cần sức mạnh phân tích để sử dụng tất cả dữ liệu đo lường từ xa này một cách hiệu quả. Các nền tảng XDR dựa trên đám mây cung cấp khả năng truy cập và quy mô gần như không giới hạn.

- **Cải thiện theo thời gian:** Việc phát hiện các cuộc tấn công ngày càng tinh vi đòi hỏi AI và học máy nhúng, cũng như tự động hóa và điều phối để giảm nỗ lực thủ công và cho phép các nhà phân tích bảo mật hiệu quả và năng suất hơn. Các giải pháp XDR nên học hỏi từ kinh nghiệm, giảm rủi ro trong tương lai và liên tục tăng cường phòng chống bằng cách áp dụng kiến thức thu được thông qua phát hiện, điều tra và phản hồi.

- **Báo cáo và bảng điều khiển:** Các đội ngũ bảo mật cần hiểu và truyền đạt tình hình bảo mật và các chỉ số hoạt động của tổ chức. Các giải pháp XDR nên có khả năng cung cấp các kết quả bảo mật tốt hơn và tóm tắt tình trạng bảo mật thông qua các báo cáo và bảng điều khiển trực quan và có thể tùy chỉnh.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

CHƯƠNG 3: PHÁ VỠ VÒNG ĐỜI TẤN CÔNG VỚI XDR

Các tác nhân đe dọa đã phát triển từ các cuộc tấn công trực tiếp vào một máy chủ hoặc tài sản có giá trị cao (gây sốc và kinh hoàng) sang một quy trình nhiều bước, kiên nhẫn, kết hợp các khai thác, phần mềm độc hại, tàng hình và lẩn tránh trong một cuộc tấn công mạng phối hợp (chậm và âm thầm).

Trong chương này, bạn sẽ tìm hiểu về vòng đời tấn công và cách Phát hiện và Phản hồi Mở rộng (XDR) giúp bạn phá vỡ vòng đời để ngăn chặn các cuộc tấn công vào môi trường của bạn. Chương này phác thảo một đại diện chung về các giai đoạn phổ biến của một cuộc tấn công.

Nhiều đội ngũ bảo mật đã áp dụng khuôn khổ MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) để giúp họ theo dõi các mối đe dọa ở các giai đoạn khác nhau của một cuộc tấn công. Một giải pháp XDR thực sự phải có khả năng phát hiện mọi bước đi của đối thủ và ánh xạ mỗi bước tới các chiến thuật và kỹ thuật của MITRE ATT&CK để đơn giản hóa các cuộc điều tra.

1. Tìm hiểu vòng đời tấn công

Vòng đời tấn công minh họa chuỗi các sự kiện (hoặc các bước) mà một kẻ tấn công trải qua để xâm nhập vào một mạng và trích xuất (hoặc đánh cắp) dữ liệu có giá trị. Các bước này bao gồm khai thác lỗ hổng ban đầu, cài đặt phần mềm độc hại, chỉ huy và kiểm soát, di chuyển ngang và trích xuất dữ liệu.

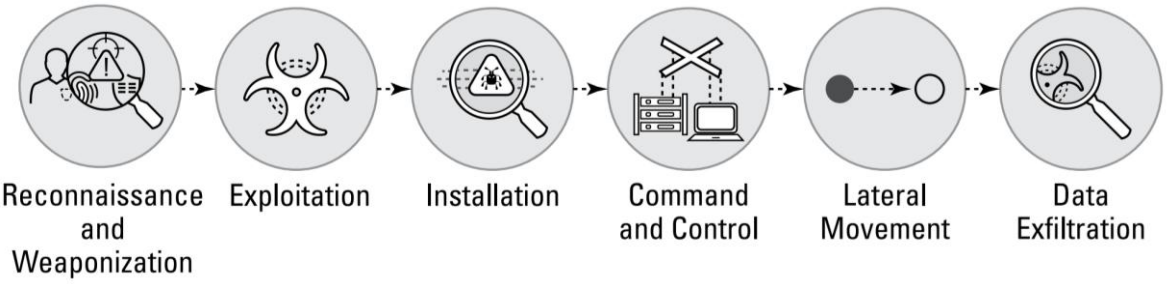

Figure 5: Các cuộc tấn công thành công đòi hỏi nhiều bước.

Sơ đồ mô tả các giai đoạn của Vòng đời Tấn công: *Trinh sát và Vũ khí hóa -> Khai thác -> Cài đặt -> Chỉ huy và Kiểm soát -> Di chuyển ngang -> Trích xuất dữ liệu.*

Nếu bạn có thể phát hiện các bước sớm hơn trong vòng đời, bạn có thể ngăn chặn những kẻ tấn công thực hiện các giai đoạn sau của một cuộc tấn công. Các phần sau đây sẽ xem xét kỹ hơn về vòng đời tấn công và cách XDR giúp bạn phá vỡ vòng đời đó.

Trinh sát

Các tác nhân đe dọa lên kế hoạch tấn công một cách tỉ mỉ. Chúng nghiên cứu, xác định và lựa chọn mục tiêu, thường trích xuất thông tin công khai từ hồ sơ mạng xã hội của nhân viên mục tiêu hoặc trang web của công ty, những thông tin này có thể hữu ích cho các kế hoạch kỹ thuật xã hội và lừa đảo. Kẻ tấn công cũng sử dụng nhiều công cụ khác nhau để quét các lỗ hổng mạng, dịch vụ và ứng dụng

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

mà chúng có thể khai thác, chẳng hạn như các công cụ phân tích mạng, quét lỗ hổng mạng, bẻ khóa mật khẩu, quét cổng và quét lỗ hổng ứng dụng web.

XDR phá vỡ vòng đời trong giai đoạn trinh sát thông qua việc giám sát và kiểm tra liên tục các luồng lưu lượng mạng để phát hiện và ngăn chặn các lần quét cổng và lỗ hổng trái phép, quét máy chủ và các hoạt động đáng ngờ khác.

Vũ khí hóa

Tiếp theo, những kẻ tấn công xác định phương pháp nào sẽ sử dụng để xâm nhập vào một điểm cuối mục tiêu. Chúng có thể nhúng mã xâm nhập vào các tệp có vẻ vô hại như tài liệu Microsoft Word hoặc email. Hoặc, đối với các cuộc tấn công có mục tiêu cao, kẻ tấn công có thể tùy chỉnh các sản phẩm để phù hợp với sở thích cụ thể của một cá nhân trong tổ chức mục tiêu.

Kẻ tấn công tiếp theo cố gắng gửi tải trọng đã được vũ khí hóa của chúng đến một điểm cuối mục tiêu, ví dụ, qua email, tin nhắn tức thời (IM), tải xuống ngẫu nhiên (drive-by download, trong đó trình duyệt web của người dùng cuối được chuyển hướng đến một trang web tự động tải phần mềm độc hại xuống điểm cuối trong nền), hoặc chia sẻ tệp bị nhiễm.

Việc phá vỡ vòng đời ở giai đoạn này của một cuộc tấn công là một thách thức vì việc vũ khí hóa thường xảy ra trong mạng của kẻ tấn công. Tuy nhiên, việc phân tích các tạo tác (cả phần mềm độc hại và công cụ vũ khí hóa) có thể cung cấp thông tin tình báo về mối đe dọa quan trọng để cho phép bảo vệ zero-day hiệu quả khi việc gửi được thực hiện. XDR cung cấp tầm nhìn vào tất cả lưu lượng mạng để chặn hiệu quả các trang web, ứng dụng và địa chỉ IP độc hại hoặc rủi ro, và ngăn chặn phần mềm độc hại và khai thác đã biết và chưa biết.

Khai thác

Sau khi một tải trọng đã được vũ khí hóa được gửi đến một điểm cuối mục tiêu, nó phải được kích hoạt. Một người dùng cuối có thể vô tình kích hoạt một khai thác, ví dụ, bằng cách nhấp vào một liên kết độc hại hoặc mở một tệp đính kèm bị nhiễm trong email, hoặc một kẻ tấn công có thể kích hoạt từ xa một khai thác chống lại một lỗ hổng máy chủ đã biết trên mạng mục tiêu.

Việc phá vỡ vòng đời ở giai đoạn này của một cuộc tấn công đòi hỏi các khả năng XDR bao gồm:

- Quản lý lỗ hổng và bản vá
- Phát hiện và phòng chống phần mềm độc hại
- Thông tin tình báo về mối đe dọa (bao gồm các mối đe dọa đã biết và chưa biết)
- Chặn các ứng dụng và dịch vụ rủi ro, trái phép hoặc không cần thiết
- Ghi nhật ký và giám sát tất cả hoạt động mạng, điểm cuối, đám mây, định danh và ứng dụng

Một tác nhân XDR hiệu quả ngăn chặn các lỗ hổng đã biết, zero-day và chưa

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

được vá bằng cách chặn các kỹ thuật khai thác của kẻ tấn công để thao túng các ứng dụng. Mặc dù có hàng ngàn khai thác, chúng thường dựa vào một bộ nhỏ các kỹ thuật khai thác ít khi thay đổi. Bằng cách chặn các kỹ thuật này, XDR ngăn chặn các nỗ lực khai thác trước khi các điểm cuối có thể bị xâm nhập.

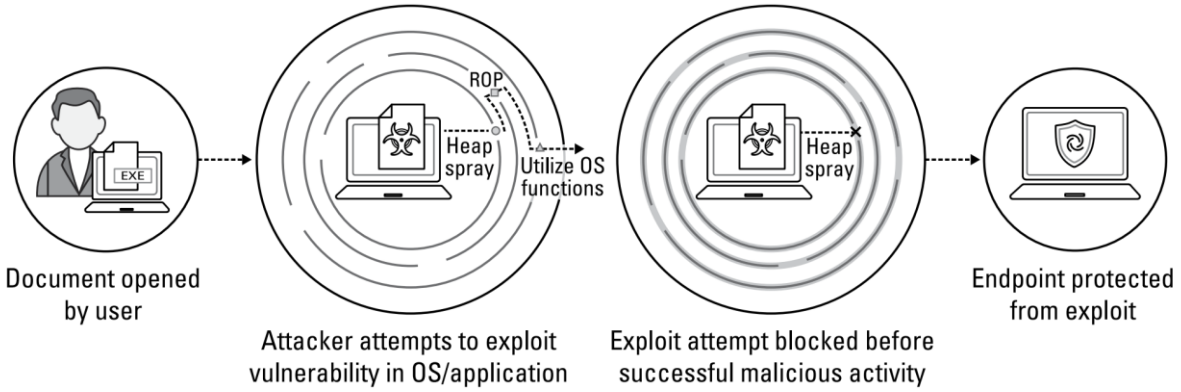

Figure 6: Một giải pháp XDR tiên tiến tập trung vào các kỹ thuật và hành vi khai thác thay vì chính các khai thác

Sơ đồ mô tả một cuộc tấn công khai thác: *(1) Người dùng mở tài liệu. (2) Kẻ tấn công cố gắng khai thác lỗ hổng trong HĐH/ứng dụng bằng các kỹ thuật như ROP, Heap spray. (3) Điểm cuối được bảo vệ khỏi khai thác. (4) Nỗ lực khai thác bị chặn trước khi hoạt động độc hại thành công.*

Cài đặt

Tiếp theo, một kẻ tấn công sẽ leo thang đặc quyền trên điểm cuối bị xâm nhập (ví dụ, bằng cách thiết lập quyền truy cập shell từ xa và cài đặt rootkit hoặc phần mềm độc hại khác). Với quyền truy cập shell từ xa, kẻ tấn công có quyền kiểm soát điểm cuối và có thể thực thi các lệnh ở chế độ đặc quyền từ giao diện dòng lệnh (CLI), như thể đang ngồi trước điểm cuối. Kẻ tấn công sau đó sẽ di chuyển ngang qua mạng của mục tiêu, thực thi mã tấn công, xác định các mục tiêu cơ hội khác, và xâm nhập thêm các điểm cuối để thiết lập sự tồn tại lâu dài.

Chìa khóa để phá vỡ vòng đời ở giai đoạn này của một cuộc tấn công là ngăn chặn việc cài đặt trên điểm cuối và hạn chế hoặc giới hạn sự di chuyển ngang của kẻ tấn công trong mạng. XDR tận dụng các công nghệ phát hiện và phản hồi điểm cuối (EDR) và nền tảng bảo vệ điểm cuối (EPP) để ngăn chặn việc cài đặt. XDR cũng giám sát và kiểm tra tất cả lưu lượng giữa các vùng hoặc phân đoạn trong mô hình Zero Trust và cung cấp quyền kiểm soát chi tiết các ứng dụng được phép trong môi trường.

Chỉ huy và kiểm soát

Các tác nhân đe dọa thiết lập các kênh liên lạc được mã hóa trở lại các máy chủ chỉ huy và kiểm soát qua Internet. Phương pháp này cho phép chúng sửa đổi mục tiêu và phương pháp tấn công khi các mục tiêu cơ hội bổ sung được xác định trong mạng nạn nhân, cũng như lẩn tránh bất kỳ biện pháp đối phó bảo mật mới nào mà tổ chức có thể cố gắng triển khai nếu các tạo tác tấn công được phát hiện. Giao

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

tiếp là điều cần thiết cho một cuộc tấn công vì nó cho phép kẻ tấn công chỉ đạo cuộc tấn công và thực hiện các mục tiêu tấn công từ xa. Lưu lượng chỉ huy và kiểm soát phải có khả năng phục hồi và tàng hình để một cuộc tấn công thành công.

Việc phá vỡ vòng đời ở giai đoạn này của một cuộc tấn công đòi hỏi:

- Kiểm tra tất cả lưu lượng mạng (bao gồm cả các giao tiếp được mã hóa)
- Chặn các giao tiếp chỉ huy và kiểm soát đi ra ngoài bằng các chữ ký chống chỉ huy và kiểm soát (cùng với việc tải lên các mẫu tệp và dữ liệu)
- Chặn tất cả các giao tiếp đi ra ngoài đến các URL và địa chỉ IP độc hại đã biết
- Chặn các kỹ thuật tấn công mới sử dụng các phương pháp lẩn tránh cổng
- Ngăn chặn việc sử dụng các công cụ ẩn danh và proxy trên mạng
- Giám sát Hệ thống Tên miền (DNS) để tìm các tên miền độc hại và chống lại bằng DNS sinkholing hoặc DNS poisoning
- Chuyển hướng các giao tiếp đi ra ngoài độc hại đến các honeypot để xác định hoặc chặn các điểm cuối bị xâm nhập và phân tích lưu lượng tấn công

Di chuyển ngang và trích xuất dữ liệu

Kẻ tấn công thường có nhiều mục tiêu tấn công, bao gồm đánh cắp dữ liệu; phá hủy hoặc sửa đổi các hệ thống, mạng và dữ liệu quan trọng; và từ chối dịch vụ (DoS). Một kẻ tấn công cũng có thể sử dụng giai đoạn cuối cùng này của vòng đời để thúc đẩy các giai đoạn đầu của cuộc tấn công chống lại một mục tiêu khác. Ví dụ, một kẻ tấn công có thể xâm nhập vào extranet của một công ty để đột nhập vào một đối tác kinh doanh là mục tiêu chính.

Việc phá vỡ vòng đời ở giai đoạn này đòi hỏi các công cụ XDR tự động phát hiện và ngăn chặn việc trích xuất dữ liệu và các hành động độc hại hoặc trái phép khác.

2. Nhìn vào một Ví dụ Tấn công

Hãy xem xét kỹ hơn một cuộc tấn công giả định để giúp hình dung tất cả các bước của vòng đời tấn công và vai trò của chúng trong một cuộc tấn công.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

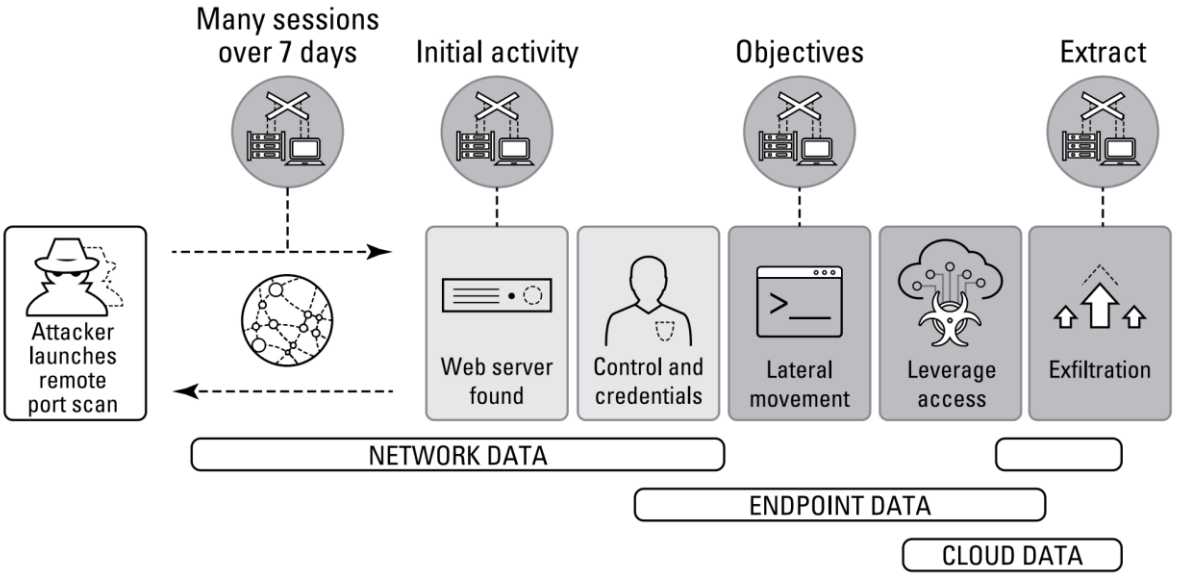

Figure 7: XDR có thể ngăn chặn duy nhất các cuộc tấn công đa bước, tiên tiến này vì nó thu thập dữ liệu từ mọi nguồn và có thể phát hiện và ngăn chặn các chiến thuật tấn công mà các công cụ khác bỏ lỡ.

Sơ đồ phức tạp mô tả một cuộc tấn công đa giai đoạn. Kẻ tấn công quét cổng, tìm thấy máy chủ web, khai thác nó để lấy thông tin xác thực, di chuyển ngang, và cuối cùng trích xuất dữ liệu. Dữ liệu từ MẠNG, ĐIỂM CUỐI, và ĐÁM MÂY được XDR thu thập để phát hiện và ngăn chặn cuộc tấn công ở mỗi giai đoạn.

Trong Hình trên , một tác nhân đe dọa thực hiện các bước sau để tấn công một mục tiêu:

- **Khai thác.** Kẻ tấn công khai thác một lỗ hổng trên máy chủ web để chiếm quyền kiểm soát máy chủ.
- **Cài đặt.** Kẻ tấn công sử dụng quyền kiểm soát máy chủ để cài đặt mimikatz và có quyền truy cập vào thông tin xác thực của quản trị viên.
- **Chỉ huy và kiểm soát.** Kẻ tấn công cài đặt thêm phần mềm độc hại và các công cụ truy cập từ xa để thiết lập sự tồn tại lâu dài và các giao tiếp chỉ huy và kiểm soát.
- **Di chuyển ngang.** Đối thủ di chuyển ngang qua mạng, xâm nhập nhiều điểm cuối, và truy cập các ứng dụng đám mây riêng tư và công cộng.
- **Truy cập và trích xuất.** Kẻ tấn công xem xét các tệp cấu hình trên máy chủ, tìm vị trí cơ sở dữ liệu backend, truy vấn cơ sở dữ liệu, và lưu kết quả vào một tệp cục bộ. Dữ liệu thu thập được tải lên một vị trí lưu trữ đám mây "được ủy quyền" hoặc "được phê duyệt". Kẻ tấn công sau đó xóa tệp chứa dữ liệu từ cơ sở dữ liệu, xóa các nhật ký cục bộ, và đóng phiên làm việc.

Một nền tảng XDR thu thập và phân tích nhiều loại dữ liệu để phát hiện và ngăn chặn các chiến thuật của đối thủ trong suốt vòng đời tấn công.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

CHƯƠNG 4: KHÁM PHÁ CÁC TRƯỜNG HỢP SỬ DỤNG XDR

Trong chương này, tôi sẽ giới thiệu các trường hợp sử dụng phổ biến nhất để giúp tổ chức của bạn cải thiện khả năng phát hiện và phản hồi, bao gồm phát hiện, phân loại và xác thực cảnh báo, tự động hóa điều tra và phản hồi, và săn lùng mối đe dọa.

1. Phát hiện

Để ngăn chặn các cuộc tấn công mạng thành công, bạn nên tập trung vào việc phát hiện các cuộc tấn công ở mỗi giai đoạn của vòng đời tấn công. Phát hiện và Phản hồi Mở rộng (XDR) sử dụng học máy để khám phá các đặc điểm độc đáo của tổ chức bạn, cho phép nó phân biệt giữa hoạt động đe dọa và hoạt động bình thường, vượt xa những gì có thể thực hiện bằng phân tích thủ công hoặc các quy tắc tương quan tĩnh. Học máy này thúc đẩy các phân tích nâng cao, lập hồ sơ và phát hiện mối đe dọa hành vi. Thông qua việc phát hiện toàn diện này, một giải pháp XDR cải thiện khả năng phát hiện hoạt động bất chính, bao gồm các cuộc tấn công có chủ đích, người dùng nội bộ độc hại, và nhiều hơn nữa.

2. Tấn công có chủ đích

Những kẻ tấn công cố gắng hòa trộn các hoạt động của chúng với việc sử dụng hợp pháp ở mọi giai đoạn trong vòng đời tấn công. Với khả năng của XDR trong việc thu thập dữ liệu từ bất kỳ nguồn nào để phát hiện và tự động xâu chuỗi dữ liệu bảo mật quan trọng cho các phân tích chéo dữ liệu nâng cao, bạn có thể phát hiện các cuộc tấn công lén lút nhất. Với các phân tích, bạn có thể lập hồ sơ hành vi người dùng và xác định hành vi bất thường, chẳng hạn như nỗ lực của kẻ tấn công để xâm nhập thiết bị và di chuyển ngang trên mạng, tìm kiếm và trích xuất dữ liệu nhạy cảm.

3. Người dùng nội bộ độc hại

Người dùng nội bộ độc hại sử dụng thông tin xác thực và quyền truy cập đáng tin cậy của họ để đánh cắp dữ liệu công ty mà không bị phát hiện. XDR giải quyết mối đe dọa này bằng cách tìm kiếm các bất thường trong hành vi và hoạt động của người dùng. Các giải pháp XDR có thể hợp lý hóa việc phân tích bằng cách trình bày một cái nhìn 360 độ về mỗi người dùng với một điểm số rủi ro rõ ràng.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

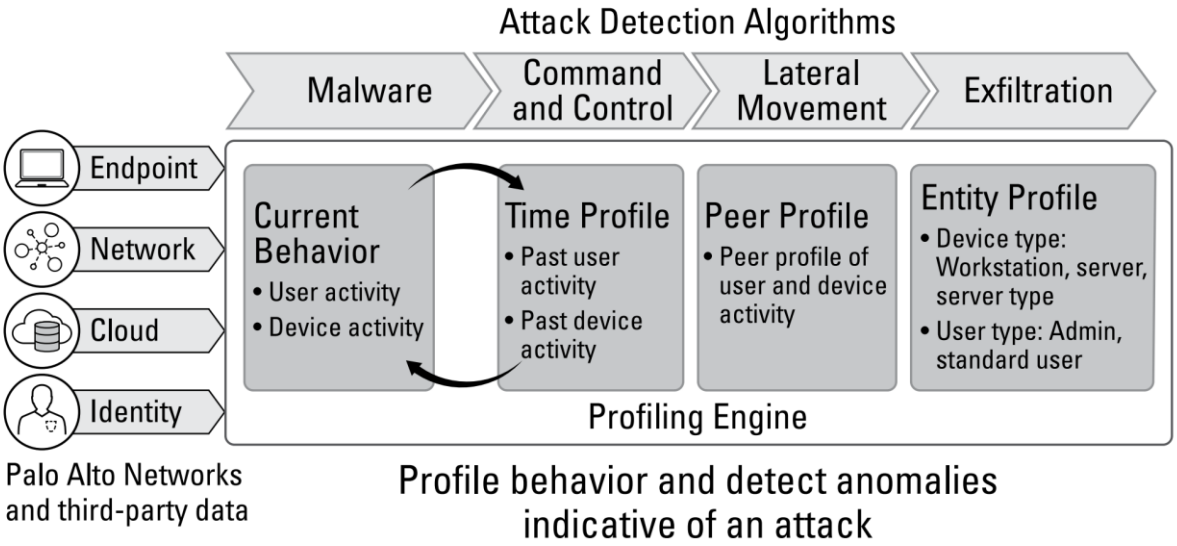

Figure 8: Phân tích hành vi phát hiện các bất thường của người dùng, ứng dụng và thiết bị.

Sơ đồ mô tả cách các thuật toán phát hiện tấn công (Phần mềm độc hại, Chỉ huy và Kiểm soát, Di chuyển ngang, Trích xuất) được cung cấp bởi một Công cụ Lập hồ sơ. Công cụ này phân tích dữ liệu từ Điểm cuối, Mạng, Đám mây, và Định danh, so sánh hành vi hiện tại với Hồ sơ Thời gian (hoạt động trong quá khứ) và Hồ sơ Ngang hàng (hoạt động của các thực thể tương tự) để phát hiện các bất thường.

4. Tấn công định danh

Kẻ tấn công thường sẽ cố gắng giành quyền truy cập vào thông tin xác thực người dùng hợp pháp hoặc các mã thông báo quản lý định danh và truy cập (IAM) trong một dịch vụ đám mây, để chúng có thể di chuyển khắp các hệ thống và trông giống như một người dùng thực. Luôn có điều gì đó về hành vi của chúng sẽ có vẻ bất thường — không giống như một người dùng thực — chẳng hạn như tạo tài khoản mới với các đặc quyền nâng cao hoặc di chuyển một lượng lớn dữ liệu. XDR có thể giám sát các hành vi này khi chúng đi chệch khỏi chuẩn mực và bắt các cuộc tấn công dựa trên định danh trước khi chúng gây ra thiệt hại thêm.

5. Các điểm cuối bị xâm nhập

Kẻ tấn công thường sử dụng phần mềm độc hại để xâm nhập vào các mạng mục tiêu bằng cách xâm nhập một điểm cuối và di chuyển ngang qua mạng. XDR mang dữ liệu bảo mật trên khắp các mạng và điểm cuối để tìm kiếm lưu lượng bất thường được tạo ra bởi phần mềm độc hại và các hoạt động bất chính khác. Dữ liệu bảo mật này cũng cung cấp phương tiện để điều tra trên toàn môi trường để xác định mức độ của cuộc tấn công.

Ví dụ, nếu một tác nhân đe dọa thêm một giá trị mới vào khóa registry Autorun, một giải pháp XDR có thể phát hiện giá trị Autorun mới và tạo ra một cảnh báo với mô tả rõ ràng về hoạt động đáng ngờ này, bao gồm bối cảnh điều tra phong phú với chiến thuật và kỹ thuật của MITRE ATT&CK. Giải pháp XDR thậm chí

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

có thể xác định quy trình nào đã thêm giá trị Autorun và chuỗi các sự kiện dẫn đến việc cập nhật để cung cấp một câu chuyện hoàn chỉnh về cuộc tấn công.

XDR phát hiện các cuộc tấn công đang hoạt động với độ chính xác vô song và tăng cường khả năng của các đội ngũ bảo mật để:

- Phát hiện hoạt động độc hại từ các tài nguyên nội bộ và bên ngoài bằng cách tìm ra các mẫu trong hoạt động trên mạng, tại các điểm cuối, từ các nhà cung cấp định danh, và trong đám mây.
- Sử dụng các kỹ thuật phân tích tiên tiến trên một lượng lớn dữ liệu bảo mật để xác định hoạt động bất thường mà không làm tăng mức độ dương tính giả.
- Tận dụng phản ứng nội bộ và thông tin tình báo về mối đe dọa bên ngoài để học hỏi từ các cuộc tấn công trong quá khứ và làm cho kinh nghiệm đó có thể tiếp cận được với các nhà phân tích ít kinh nghiệm hơn, cải thiện hiệu suất của toàn bộ đội ngũ bảo mật.

6. Phân loại và Điều tra Cảnh báo

Các giải pháp XDR đơn giản hóa việc phân loại và phân tích cảnh báo bằng cách tiết lộ nguyên nhân gốc rễ của các cảnh báo, giúp chúng nhanh hơn nhiều để điều tra. Nếu chỉ có dữ liệu điểm cuối, thì nguyên nhân gốc rễ của điểm cuối được trình bày. Nếu có dữ liệu mạng và điểm cuối, nền tảng XDR có thể tự động liên kết hoạt động mạng với các sự kiện điểm cuối. Ví dụ, XDR không chỉ xác định tệp thực thi điểm cuối nào chịu trách nhiệm cho một cảnh báo mạng, mà nó còn có thể tìm ra ứng dụng nào đã khởi chạy tệp thực thi đó.

Với những thách thức do khoảng trống kỹ năng bảo mật được thảo luận trong Chương 1, XDR cải thiện khả năng của một nhà phân tích ít kinh nghiệm hơn để phát hiện và xác thực một cuộc tấn công tiềm tàng bằng cách nhóm các cảnh báo thành các sự cố và, trong các sự cố đó, tóm tắt các hoạt động hoặc hành động thành các thẻ để thêm bối cảnh. Sự linh hoạt này đảm bảo rằng kiến thức được nắm bắt và tận dụng cho toàn bộ đội ngũ.

XDR tạo ra một dòng thời gian của các sự kiện dẫn đến cảnh báo và cung cấp thông tin tình báo về mối đe dọa tích hợp. Tất cả những điều này cho phép các nhà phân tích hiểu được nguyên nhân gốc rễ của một cảnh báo, bản chất chính xác của mối đe dọa, và hành động cần thực hiện.

Dưới đây là cách XDR giúp đơn giản hóa việc phân tích và điều tra sự cố:

- **Đánh giá.** Quá trình bắt đầu với việc giải pháp XDR đánh giá các cảnh báo bên ngoài (chẳng hạn như từ các công cụ bảo mật của bên thứ ba) và các cảnh báo được tạo ra nội bộ (dựa trên các quy tắc và các chỉ số khác) để xác định hành vi có khả năng đáng ngờ.
- **Ưu tiên.** Công cụ XDR sau đó tự động nhóm các cảnh báo đó thành các sự cố, gán một mức độ ưu tiên cho mỗi sự cố để hướng các nhà phân tích đến các sự cố gây ra mối đe dọa lớn nhất. Các nhà phân tích có thể nhấp vào mỗi sự cố và xem danh sách đầy đủ các cảnh báo, thiết bị, thông tin tình báo về mối đe dọa liên quan, và bối cảnh khác để giúp hiểu toàn bộ mức độ của cảnh báo.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

- **Phân tích.** XDR cung cấp một chuỗi tấn công trực quan (xem Hình 4-2), tận dụng các nguồn dữ liệu đo lường từ xa khác nhau để thu thập bất cứ thứ gì và mọi thứ liên quan đến sự cố và cung cấp thêm bối cảnh, tính nhân quả, và để đảm bảo phân tích nhanh hơn và tốt hơn. Chuỗi tấn công cho thấy các bước của kẻ tấn công bằng cách tiết lộ chuỗi các quy trình dẫn đến bước tấn công cuối cùng.

- **Làm giàu dữ liệu.** Chuỗi tấn công sau đó được làm giàu với thông tin ngữ cảnh bổ sung, bao gồm một cái nhìn chi tiết về cách cảnh báo được tạo ra; nguyên nhân gốc rễ của nó; các điểm cuối, mạng, và thiết bị đám mây khác có liên quan; và danh tiếng của tất cả các tạo tác pháp y.

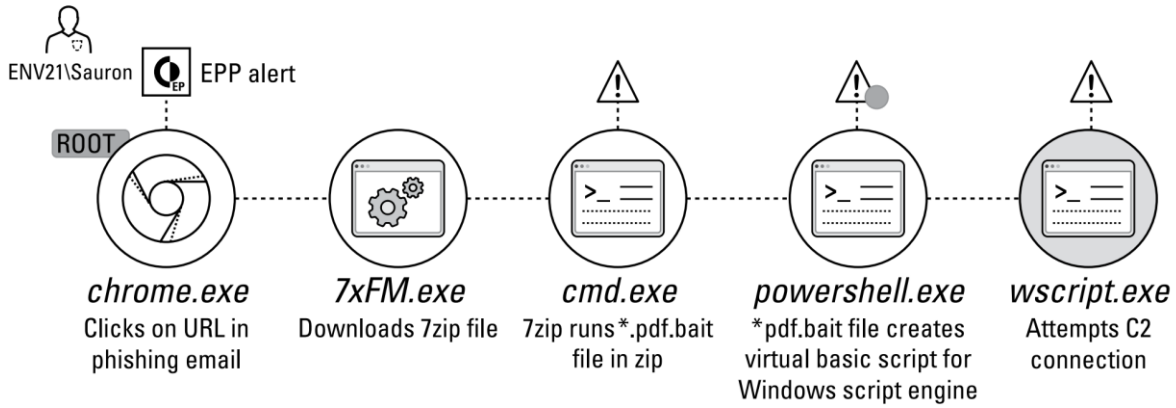

Figure 9: Một ví dụ về chuỗi tấn công được trực quan hóa bằng XDR.

Sơ đồ chuỗi tấn công cho thấy: *(1) chrome.exe nhấp vào URL trong email lừa đảo. (2) 7xFM.exe tải xuống tệp 7zip. (3) 7zip chạy tệp *.pdf.bait. (4) Tệp .pdf.bait tạo kịch bản cho wscript.exe. (5) wscript.exe cố gắng kết nối C2 (Chỉ huy và Kiểm soát).*

Với hàng ngàn cảnh báo đến mỗi ngày, việc tự động hóa quy trình phân loại và cung cấp cho các nhà phân tích thông tin ngữ cảnh được làm giàu là cách duy nhất để quản lý khối lượng. Với XDR, các đội ngũ bảo mật có thể tập trung thời gian và năng lượng của họ vào nơi nó sẽ có tác động lớn nhất đến việc khắc phục các cảnh báo có khả năng gây ra thiệt hại nhiều nhất.

Với XDR, các nhà phân tích có khả năng tăng cường để:

- Giảm bớt lượng cảnh báo tồn đọng với quản lý sự cố, nhóm cảnh báo thông minh, và bối cảnh điều tra.
- Giảm đáng kể khả năng bỏ lỡ một cuộc tấn công.
- Phân tích các cảnh báo để cải thiện việc phát hiện và đảm bảo rằng năng suất và khả năng phòng thủ ở các giai đoạn sau không bị ảnh hưởng tiêu cực.
- Áp dụng các trình kích hoạt hành vi mới để cải thiện thời gian phân loại, và tùy chọn chuyển đổi các quy tắc phát hiện thành các quy tắc phòng chống để phòng chống vòng lặp khép kín.

7. Điều tra và Phản hồi Tự động và Đơn giản hóa

Một cuộc điều tra sâu hơn là cần thiết sau khi một cảnh báo đã được phân loại và ưu tiên. Sự tự động hóa của XDR tăng tốc quá trình điều tra của bất kỳ cảnh

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

báo hoặc chiến dịch săn lùng nào, loại bỏ các nhiệm vụ thủ công tốn thời gian bằng cách cung cấp một bức tranh rõ ràng về mối đe dọa, thực hiện phân tích nguyên nhân gốc rễ, xác minh danh tiếng, và giải quyết việc quy kết tấn công.

Các công cụ XDR bắt đầu bằng cách tổng hợp tất cả dữ liệu đo lường từ xa trong một kho lưu trữ dữ liệu bảo mật, chẳng hạn như một hồ dữ liệu đám mây.

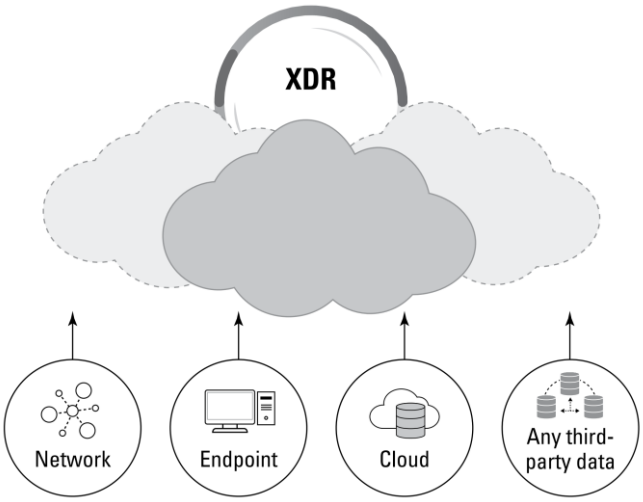

Figure 10: Các công cụ XDR xâu chuỗi dữ liệu từ các cảm biến khác nhau trong một kho lưu trữ dữ liệu dựa trên đám mây.

Sơ đồ đơn giản cho thấy dữ liệu từ Mạng, Điểm cuối, Đám mây, và bất kỳ dữ liệu bên thứ ba nào đều được đưa vào một nền tảng XDR trung tâm.

Để giảm thời gian điều tra, giải pháp XDR có thể tương quan và nhóm các cảnh báo từ khắp các công cụ phát hiện thành một số lượng nhỏ các sự cố chính xác, có thể hành động, bao gồm thông tin về người dùng, ứng dụng và thiết bị. XDR cũng có thể hỗ trợ các cuộc điều tra pháp y bằng cách truy vấn các điểm cuối để xác định quy trình hoặc tệp thực thi nào đã khởi xướng một cuộc tấn công.

Các công cụ XDR cũng có thể thích ứng các biện pháp phòng thủ, áp dụng kiến thức từ các sự cố và chiến dịch săn lùng trước đó để tự động ngăn chặn sự tái diễn thành công của bất kỳ mối đe dọa nào đã được tìm thấy trước đó. "Học tập có hỗ trợ" này cho phép phát hiện sớm các cuộc tấn công dựa trên những gì đã được nhìn thấy trong môi trường.

Sau khi mối đe dọa đã được xác thực, các chuyên gia ứng phó sự cố sau đó có thể chọn từ hàng chục kỹ thuật phản hồi và khắc phục từ xa để ngăn chặn cuộc tấn công, ngăn chặn các cuộc tấn công tiếp theo, khôi phục các tệp bị hỏng hoặc bị xóa, và nhiều hơn nữa. Các tùy chọn phản hồi bao gồm cách ly các điểm cuối, chặn, xóa hoặc cách ly các tệp, hoàn nguyên các tệp và registry về trạng thái sạch, truy cập trực tiếp vào các điểm cuối, và thực thi các kịch bản. Đội ngũ bảo mật sẽ trở nên hiệu quả cao, đòi hỏi ít đào tạo hơn, giảm gánh nặng cho các chuyên gia ứng phó sự cố có kinh nghiệm hơn, và giảm thiểu thời gian giải quyết sự cố.

8. Săn lùng Mối đe dọa

Các giải pháp XDR cải thiện khả năng săn lùng mối đe dọa của bạn thông qua

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

cả việc xác định hoạt động độc hại tự động và theo yêu cầu trên toàn môi trường của bạn. Các thợ săn mối đe dọa có thể thực hiện các truy vấn nâng cao và nhận được kết quả ngay lập tức.

Một số ví dụ về cách XDR cung cấp các khả năng cần thiết để hỗ trợ các phương pháp săn lùng mối đe dọa khác nhau bao gồm:

- **Dựa trên thông tin tình báo (Intel-based):** Đây là loại hoạt động săn lùng mối đe dọa phổ biến nhất, trong đó thợ săn đã được cung cấp một manh mối về một mối đe dọa tiềm tàng trước khi tìm kiếm nó. Cho dù đó là một đầu mối từ thông tin tình báo về mối đe dọa, một chỉ số xâm phạm (IOC) mới được tìm thấy, một mẹo từ ai đó trong tổ chức, hay chỉ là sự nghi ngờ, sự phức tạp của việc săn lùng mối đe dọa dựa trên thông tin tình báo sẽ phụ thuộc vào mức độ chi tiết mà thông tin tình báo cung cấp. Rút ra từ một nguồn dữ liệu tích hợp được liên kết với nhiều nhà cung cấp thông tin tình báo về mối đe dọa, một giải pháp XDR có thể nhập thủ công các tạo tác hoặc IOC từ các tiêu chuẩn khác nhau để cung cấp kết quả tìm kiếm nhanh chóng và mạnh mẽ.

- **Không có manh mối (Leadless-based):** Xếp thứ hai về các phương pháp tiếp cận phổ biến để săn lùng mối đe dọa, không có manh mối là nơi thợ săn sử dụng kiến thức của riêng mình hoặc tìm kiếm về cách một máy tính, ứng dụng, người dùng, dữ liệu hoặc mạng được sử dụng và nhằm mục đích xác định việc sử dụng bất thường hoặc không bình thường. Loại săn lùng mối đe dọa nâng cao này thường được dành cho các thành viên có kinh nghiệm nhất trong nhóm, những người sử dụng các kỹ thuật như khắc dữ liệu và phân tích để đạt được kết quả. Một giải pháp XDR đơn giản hóa quy trình này bằng cách xây dựng các kỹ thuật nâng cao này vào giao diện của nó. Nó cho phép các thợ săn ở mọi cấp độ kinh nghiệm tận dụng các kỹ thuật này mà không cần kịch bản hoặc các công cụ bổ sung.

- **Dựa trên kết quả (Outcome-based):** Trong phương pháp này, thợ săn xem xét các cảnh báo đã được cách ly trong quá khứ, các cuộc điều tra đã hoàn thành, hoặc bất kỳ mối đe dọa nào đã được giải quyết và sử dụng chúng để xác định các biến thể của mối đe dọa, các mối đe dọa mới tiềm tàng, hoặc các vector tấn công mở. Một giải pháp XDR chất lượng có thể tự động và liên tục kết hợp việc săn lùng mối đe dọa dựa trên kết quả trực tiếp vào quy trình xử lý cảnh báo và sự cố bảo mật. Các bài học kinh nghiệm từ mỗi cuộc điều tra được áp dụng để đảm bảo bạn không bị tấn công bởi các cuộc tấn công lặp lại.

- **Dựa trên tuân thủ (Compliance-based):** Phương pháp săn lùng mối đe dọa này tập trung vào việc đảm bảo tuân thủ các yêu cầu nội bộ, ngành và chính phủ bằng cách thực hiện các tìm kiếm định kỳ chỉ ra sự không tuân thủ, chẳng hạn như dữ liệu nhạy cảm được lưu trữ trên các hệ thống trái phép hoặc leo thang đặc quyền của người dùng quản trị. Một giải pháp XDR có thể được cấu hình để cảnh báo các nhà phân tích bảo mật về loại hoạt động này và cung cấp một phương tiện để điều tra tình hình một cách nhanh chóng.

- **Dựa trên học máy (Machine learning-based):** Các hệ thống học máy thiết

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

lập đường cơ sở cho các hành vi điển hình của một tổ chức để hiểu những gì là bình thường và những gì không. Sử dụng các phân tích quy mô lớn, các giải pháp XDR sử dụng học máy để giám sát các hành vi và xác định các bất thường đi chệch khỏi các đường cơ sở này. Các chỉ số xâm phạm hành vi (BIOCs) này phát hiện nhiều mối đe dọa lén lút mà một nhà phân tích có thể không thể xác định thủ công và được tối ưu hóa liên tục theo thời gian để cải thiện mô hình học máy. Hình thức săn lùng mối đe dọa này đại diện cho sự tiết kiệm thời gian tối đa cho các nhà phân tích và rất quan trọng để tối ưu hóa các kết quả bảo mật.

- Với XDR, các thợ săn mối đe dọa có khả năng tăng cường để:

- Tận dụng dữ liệu mạng, điểm cuối và đám mây cho các tìm kiếm và phân tích.

- Tận dụng tự động hóa để săn lùng trên tất cả các hoạt động mạng, điểm cuối và đám mây.

- Sử dụng các tìm kiếm và trình hướng dẫn có thể cấu hình cao để tìm cả các mối đe dọa nội bộ và bên ngoài được xác định bởi các IOC truyền thống và BIOC được lưu trữ trong thư viện mối đe dọa của bạn.

- Khắc phục các cuộc tấn công thông qua tích hợp với các kiểm soát bảo mật.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

CHƯƠNG 5: MƯỜI NĂNG LỰC VÀ TÍNH NĂNG CHÍNH CỦA XDR

Phát hiện và Phản hồi Mở rộng (XDR) cho phép các tổ chức ngăn chặn các cuộc tấn công mạng thành công và đơn giản hóa cũng như tăng cường các quy trình bảo mật của họ bằng cách sử dụng một phương pháp tiếp cận chủ động để phát hiện và phản hồi mối đe dọa. XDR ngăn chặn các cuộc tấn công hiện đại bằng cách thu thập và phân tích dữ liệu từ bất kỳ nguồn nào. Nó hợp nhất việc phòng chống, phát hiện, điều tra và phản hồi để mang lại hiệu quả bảo mật và hoạt động vô song.

Chương này trình bày mười điều "bắt buộc phải có" cần tìm kiếm trong một giải pháp XDR cho tổ chức của bạn. Nó cũng giải thích cách Cortex XDR, nền tảng phát hiện và phản hồi mở rộng được điều khiển bởi AI, cung cấp các tính năng thiết yếu này.

1. Phòng chống Mối đe dọa Điểm cuối Tốt nhất

Việc bảo vệ tổ chức của bạn bắt đầu bằng khả năng phòng chống mối đe dọa điểm cuối tốt nhất, chặn phần mềm độc hại đã biết và chưa biết, ransomware, các cuộc tấn công không dùng tệp và khai thác.

Cortex XDR cung cấp mọi thứ bạn cần để phòng chống, phát hiện và phản hồi mối đe dọa với một tác nhân duy nhất được quản lý từ đám mây. Nó bảo vệ các điểm cuối của bạn bằng phân tích cục bộ được điều khiển bởi trí tuệ nhân tạo (AI) và bảo vệ dựa trên hành vi tốt nhất trong ngành.

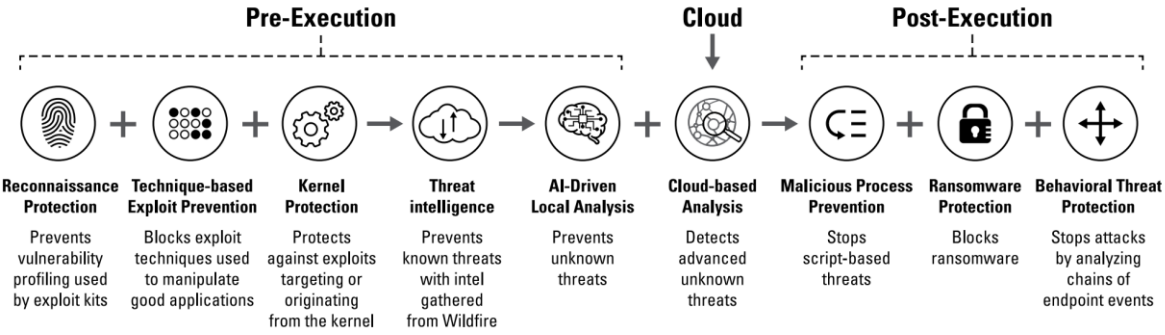

Figure 11: Cortex XDR cung cấp khả năng phòng chống mối đe dọa điểm cuối hoàn chỉnh.

Sơ đồ mô tả các lớp phòng thủ của Cortex XDR, từ giai đoạn Trước-Thực thi (Pre-Execution) đến Sau-Thực thi (Post-Execution). Các lớp này bao gồm: Phân tích Cục bộ do AI điều khiển, Thông tin tình báo về mối đe dọa từ đám mây, Phòng chống Khai thác dựa trên Kỹ thuật, Bảo vệ Chống Phần mềm độc hại, Bảo vệ Chống Ransomware, Bảo vệ Mối đe dọa Hành vi, và Bảo vệ Kernel.

Hãy tìm kiếm khả năng phòng chống mối đe dọa điểm cuối cung cấp:

- Chống virus thế hệ mới
- Bảo vệ chống phần mềm độc hại, ransomware và mối đe dọa không dùng tệp
- Thông tin tình báo về mối đe dọa toàn cầu theo thời gian thực dựa trên đám

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

mây
- Phân tích cục bộ thông qua học máy
- Bảo vệ mối đe dọa hành vi
- Bảo vệ quy trình con chi tiết
- Phòng chống khai thác trước khi xảy ra và dựa trên kỹ thuật
- Phòng chống khai thác kernel
- Phòng chống tấn công shellcode
- Bảo vệ chống đánh cắp thông tin xác thực

2. Bộ Tính năng Bảo vệ Điểm cuối Linh hoạt

Bạn cần một cách dễ dàng để xác định và ưu tiên các rủi ro điểm cuối, giảm bề mặt tấn công và ngăn chặn mất mát dữ liệu. Hãy tìm kiếm một bộ tính năng bảo vệ điểm cuối hoàn chỉnh, bao gồm:

- **Đánh giá lỗ hổng:** Tận dụng đánh giá lỗ hổng, hiển thị ứng dụng trên các điểm cuối được quản lý và không được quản lý, và nhiều hơn nữa để có được một cái nhìn toàn doanh nghiệp về tài sản kỹ thuật số của bạn.
- **Tường lửa máy chủ:** Quản lý tập trung các giao tiếp vào và ra trên các điểm cuối của bạn từ bảng điều khiển quản lý.
- **Mã hóa đĩa:** Áp dụng các chính sách mã hóa hoặc giải mã trên các điểm cuối của bạn và xem danh sách tất cả các ổ đĩa được mã hóa.
- **Kiểm soát thiết bị:** Giám sát và kiểm soát chi tiết quyền truy cập USB để bảo vệ các điểm cuối của bạn.

3. Tầm nhìn Mở rộng đến các Nguồn dữ liệu từ khắp Tổ chức của Bạn

Để giảm rủi ro của một cuộc tấn công thành công, bạn cần một phương pháp tiếp cận toàn diện để phát hiện và phản hồi nhằm loại bỏ các điểm mù, tăng độ chính xác và hợp lý hóa các cuộc điều tra trên tất cả các môi trường, bao gồm mạng, đám mây, định danh và điểm cuối.

Cortex XDR tích hợp tự nhiên dữ liệu điểm cuối, mạng, định danh và đám mây để ngăn chặn các cuộc tấn công tinh vi. Cortex XDR cung cấp tất cả các khả năng của phát hiện và phản hồi mạng (NDR), phát hiện và phản hồi điểm cuối (EDR), bảo vệ điểm cuối (EPP), phát hiện và phản hồi đám mây (CDR), và phân tích hành vi người dùng và thực thể (UEBA), như được hiển thị trong Hình.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

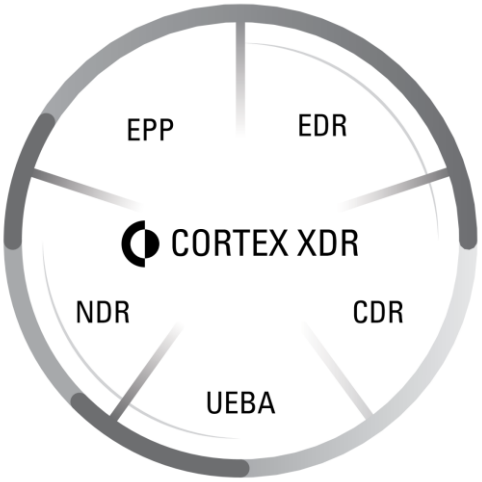

Figure 12: Cortex XDR thu thập và phân tích dữ liệu phong phú để cung cấp các khả năng thường được cung cấp bởi các công cụ EPP, EDR, NDR, CDR và UEBA.

Sơ đồ cho thấy các công cụ riêng lẻ như NDR, EPP, EDR, UEBA, CDR được hợp nhất thành một nền tảng duy nhất là CORTEX XDR.

4. Đơn giản hóa Điều tra

Các công cụ bảo mật riêng lẻ ngày nay tạo ra vô số cảnh báo với bối cảnh hạn chế. Theo Báo cáo Chi phí của một Vụ vi phạm Dữ liệu năm 2023 của IBM và Viện Ponemon, thời gian trung bình để xác định và ngăn chặn một vụ vi phạm là 277 ngày. Các công cụ bảo mật phải cung cấp một bức tranh hoàn chỉnh về các sự cố với các chi tiết điều tra phong phú để giảm thời gian phản hồi.

Cortex XDR đơn giản hóa các cuộc điều tra bằng cách tự động tiết lộ nguyên nhân gốc rễ, chuỗi sự kiện và các chi tiết thông tin tình báo về mối đe dọa của các cảnh báo. Nó giảm thời gian điều tra tới 88% bằng cách tiết lộ nguyên nhân gốc rễ và bối cảnh phong phú của các cảnh báo mạng, điểm cuối, định danh và đám mây, và giảm số lượng cảnh báo tới 98% bằng cách nhóm các cảnh báo một cách thông minh thành các sự cố được ưu tiên kể lại toàn bộ câu chuyện của một cuộc tấn công.

5. Phân tích và Học máy

Các tác nhân đe dọa tận dụng công nghệ đám mây và học máy để tăng quy mô và hiệu quả của các cuộc tấn công của chúng. Bạn cần một bộ toàn diện các kỹ thuật học máy và phân tích để đi trước các mối đe dọa đang phát triển nhanh chóng và chống lại các cuộc tấn công tinh vi.

Cortex XDR cung cấp:

- Phân tích cục bộ do AI điều khiển để chặn phần mềm độc hại
- Phân tích hành vi để phát hiện các cuộc xâm nhập và tấn công đang hoạt động
- Phân tích toàn cầu để cải thiện độ chính xác và phạm vi phát hiện

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

6. Phản hồi Phối hợp

Sau khi bạn xác định các mối đe dọa trong môi trường của mình, bạn cần phải ngăn chặn chúng một cách nhanh chóng. Đội ngũ của bạn cần các tùy chọn phản hồi tích hợp và linh hoạt để dập tắt các cuộc tấn công một cách nhanh chóng và hiệu quả trước khi chúng có thể gây ra nhiều thiệt hại hơn. Một giải pháp XDR phải cho phép đội ngũ của bạn ngăn chặn sự lây lan của phần mềm độc hại từ xa, hạn chế hoạt động mạng đến và đi từ các thiết bị, và cập nhật danh sách phòng chống mối đe dọa, chẳng hạn như các tên miền xấu, thông qua tích hợp chặt chẽ với các điểm thực thi của bạn.

Cortex XDR cho phép đội ngũ bảo mật của bạn loại bỏ ngay lập tức các mối đe dọa điểm cuối, mạng, định danh và đám mây từ một bảng điều khiển duy nhất.

7. Tự động hóa các Tác vụ An ninh

Các nhiệm vụ và quy trình thủ công làm chậm quá trình ứng phó sự cố và tăng chi phí hoạt động bảo mật. XDR giảm đáng kể công việc thủ công, tự động hóa nhiều nhiệm vụ nặng nhọc cho các đội ngũ bảo mật.

XDR có thể giảm thời gian các nhà phân tích dành để sàng lọc các cảnh báo, bằng cách tự động nhóm các cảnh báo liên quan thành các sự cố kết hợp, giảm tổng khối lượng cảnh báo tới 98%. Hãy tìm các giải pháp XDR được xây dựng sẵn với các quy tắc phát hiện, phân tích các sự kiện bằng học máy để tự động phát hiện các cuộc tấn công đang diễn ra, vì vậy các nhà phân tích không phải viết các quy tắc phát hiện tùy chỉnh.

Các giải pháp XDR sau đó có thể nhanh chóng ngăn chặn các mối đe dọa bằng cách thực hiện một loạt các hành động phản hồi tự nhiên đối với điểm cuối và các điểm thực thi quan trọng khác. Các SOC tiên tiến có thể yêu cầu các quy trình bao gồm logic quyết định và điều phối quy trình làm việc được kiểm soát bởi các playbook và bao gồm một loạt các hành động trên một loạt các công cụ bảo mật và CNTT từ các nhà cung cấp khác nhau. Một giải pháp tự động hóa và điều phối an ninh đầy đủ tính năng cung cấp logic điều phối và có các tích hợp đối tác rộng rãi và nội dung và playbook được xây dựng sẵn có thể giải quyết các yêu cầu này. Do đó, hãy tìm một giải pháp XDR tích hợp chặt chẽ với một nền tảng SOAR hàng đầu trong ngành.

Cortex XDR tích hợp chặt chẽ với Cortex XSOAR để quản lý thông tin tình báo về mối đe dọa hoàn chỉnh và cung cấp hơn 850 tích hợp đối tác và 1,000 gói nội dung để bạn có thể đưa hoạt động bảo mật của mình lên một tầm cao mới.

8. Kiểm định và Xác thực Độc lập

Khi chọn một giải pháp XDR, bạn nên luôn xem xét các thử nghiệm của bên thứ ba, xác thực của các nhà phân tích và lời chứng thực của khách hàng để có được một góc nhìn độc lập và khách quan.

Cortex XDR đã đạt được các kết quả kiểm tra đặc biệt bao gồm việc đạt được sự kết hợp tốt nhất giữa phát hiện và bảo vệ trong đánh giá MITRE ATT&CK Vòng

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

Năm, và xếp hạng "Strategic Leader" trong bài kiểm tra Endpoint Prevention and Response (EPR) của AV-Comparatives. Nhận được lời khen ngợi từ cả khách hàng và các nhà đánh giá, Cortex XDR có thể được tin cậy để bảo vệ các điểm cuối và dữ liệu của bạn.

9. Tốc độ Đổi mới Nhanh chóng

Để vượt qua các đối thủ di chuyển nhanh, hãy tìm kiếm các nhà cung cấp liên tục tăng cường hoặc mở rộng khả năng của sản phẩm của họ.

Cortex XDR tiếp tục định nghĩa lại cách các đội ngũ vận hành an ninh giải quyết các mối đe dọa hiện đại phức tạp và thúc đẩy hiệu quả cao hơn. Bằng cách giải quyết vấn đề tích hợp hệ thống trong việc thu thập, tích hợp và phân tích dữ liệu và kết hợp điều đó với khả năng khởi động các quy trình làm việc được tối ưu hóa và tự động hóa cao, XDR giúp giải quyết các thách thức về phát hiện, điều tra và phản hồi ở quy mô lớn một cách hợp nhất.

10. Lợi tức Đầu tư Vượt trội

Khi lựa chọn một yếu tố quan trọng trong cơ sở hạ tầng bảo mật của bạn, bạn muốn đảm bảo rằng nó sẽ cung cấp giá trị thực sự có thể dễ dàng chứng minh cho các bên liên quan của bạn.

Cortex XDR giảm tổng chi phí sở hữu (TCO) trung bình 44% so với các công cụ truyền thống, bằng cách:

- Tận dụng các công cụ bảo mật hiện có của bạn làm cảm biến để phát hiện và phản hồi
- Loại bỏ các máy chủ nhật ký tại chỗ với việc triển khai trên đám mây
- Đơn giản hóa hoạt động với việc xâu chuỗi dữ liệu, nhóm cảnh báo và phân tích nguyên nhân gốc rễ

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn

THÔNG TIN CORTEX XDR

CORTEX XDR Đã được kiểm tra. Đã được đánh giá. Đã được chứng minh.

Cortex XDR Cung cấp: Bảo mật điểm cuối đoạt giải thưởng, được các nhà phân tích công nhận: Cortex XDR đã được công nhận là Đơn vị Dẫn đầu trong "The Forrester Wave™: Extended Detection and Response (XDR) Platforms, Q2 2024."

FORRESTER WAVE LEADER 2024 - Nền tảng Phát hiện và Phản hồi Mở rộng

Độ chính xác phát hiện hàng đầu trong ngành: Trong các đánh giá MITRE ATT&CK® năm 2023, Cortex XDR® đảm bảo tầm nhìn 100% về các hành động có khả năng độc hại, trao quyền cho việc giảm thiểu mối đe dọa chủ động và chặn tất cả các bước phụ, giảm đáng kể thời gian và chi phí.

HQ: 136A + 136B, Residential No.2, Hai An Ward, Hai Phong City, Vietnam.
BO: 12/49 Lu Gia Str., Phu Tho Ward, Ho Chi Minh City, Vietnam.
Tel: +84-0225-7308688/3630888
Email: info@ktd.vn | https://ktd.vn