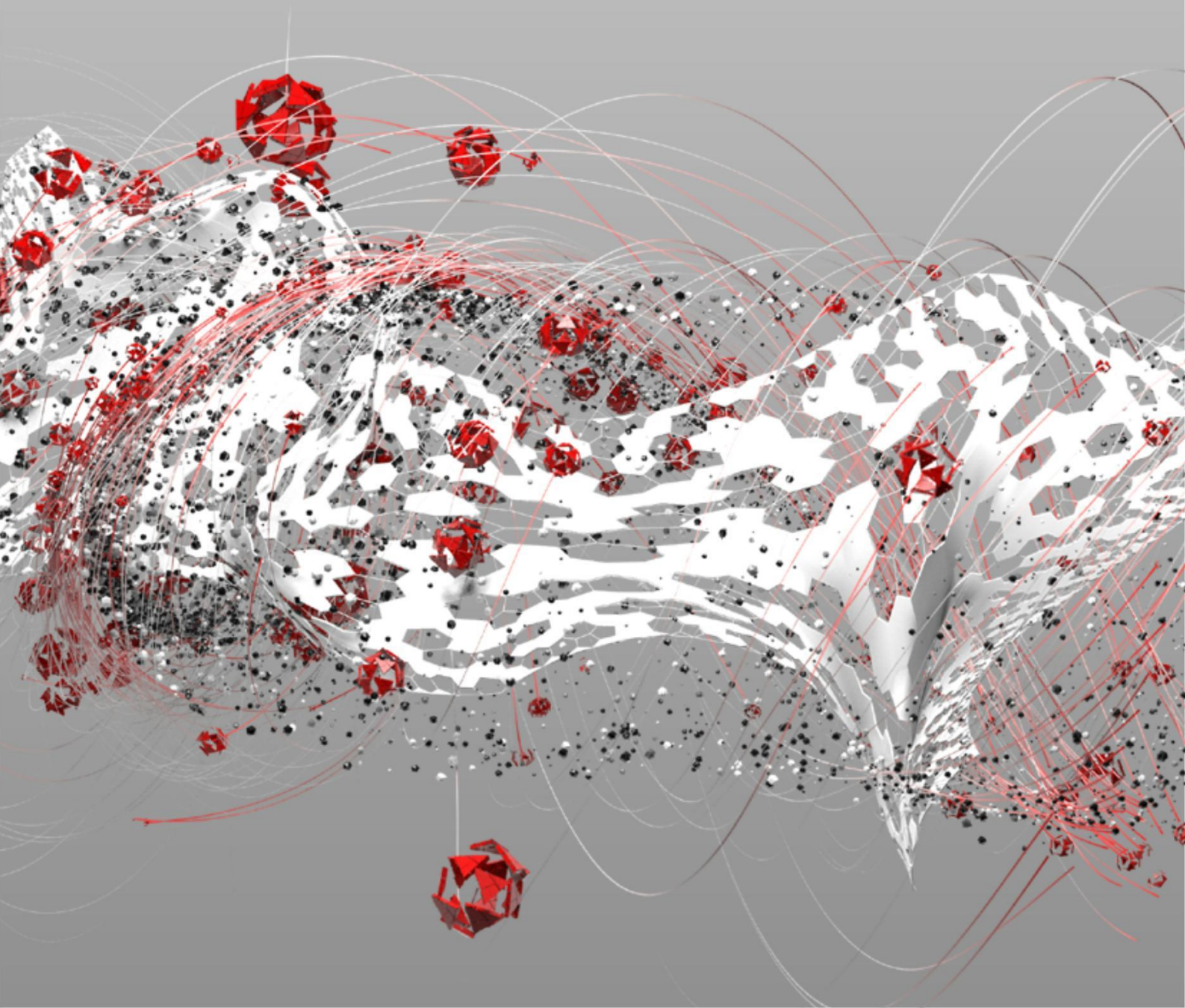
TREND MICRO

PACISOFT.vn

Theo nghiên cứu toàn cầu

CÁC HỆ LỤY CỦA HOẠT ĐỘNG BẢO MẬT AN NINH MẠNG :

Sử dụng công cụ kém hiệu quả gây tác động gì đến các chuyên gia bảo mật



Trong những năm gần đây, các nhà lãnh đạo bảo mật và doanh nghiệp đã thay đổi kì vọng về an ninh mạng hiệu quả có thể mang lại điều gì. Những ngày tháng tất cả nguồn lực đều đổ dồn vào việc bảo vệ vành đai hệ thống mạng của tập đoàn đã là quá khứ. Nhờ vào sự áp dụng rộng rãi các cơ sở hạ tầng và dịch vụ đám mây. BYOD và hiện trạng làm việc tại nhà, vành đai ấy hiện dễ dàng luân chuyển, linh hoạt và nhiều lỗ hổng hơn.

Các nhân tố nguy hiểm có thể và thường xuyên xâm nhập vào hệ thống mạng tập đoàn bằng cách đánh cắp, lừa đảo hoặc bẻ khóa thông tin đăng nhập, hoặc bằng cách khai thác các lỗ hổng chưa được vá mà trên thực tế là bọn chúng có vô số để chọn lựa. Điều này có nghĩa, các CISO và CEO phải nhìn nhận rằng tổ chức của họ sẽ bị xâm nhập, hoặc có thể trường hợp đó đã xảy ra rồi. Mấu chốt chính là tìm những tên tấn công trước khi chúng có cơ hội để gây ra thiệt hại nghiêm trọng.

Đây chính là lúc trung tâm Security Operations Center (SOC) vào cuộc. Chức năng nó cung cấp là định vị, luôn luôn giám sát, phát hiện và phản hồi với các mối đe dọa mạng. Trên lí thuyết, đây là một cách hiệu quả để giám sát sự tăng trưởng của các mối đe dọa có liên quan đến tội phạm mạng. Nhưng trên thực tế, rất nhiều đội đang phải nỗ lực để cung cấp dịch vụ hỗ trợ mà CISO yêu cầu từ họ, đồng thời bị ảnh hưởng tiêu cực đến đời sống không chỉ trong công việc mà còn ở đời sống cá nhân.

Để tìm hiểu thêm, Trend Micro đã thực hiện một nghiên cứu toàn cầu, dựa trên các cuộc phỏng vấn với 2.303 nhà quyết định bảo mật CNTT trên 21 quốc gia. Phỏng vấn này bao gồm các nhà lãnh đạo điều hành các nhóm SOC (85%) và nhà quản lí SecOps trong đội ngũ bảo mật CNTT của họ (15%). Tất cả đến từ các công ty có trên 250 nhân viên, với riêng Na Uy (trên 10), Đan Mạch (trên 25), Úc và Bỉ (cả hai trên 100).

2,303
Nhà quyết định bảo mật CNTT

21
Quốc gia

85% bao gồm các nhà lãnh đạo có các nhóm SOC

15% quản lí SecOps nhóm bảo mật CNTT trong tổ chức của họ

Công ty có lượng nhân viên

TRÊN 250 NGƯỜI

Nhiều cuộc xâm nhập đang diễn ra

Hãy làm rõ về quy mô thách thức mà các nhóm SecOps đang phải đối mặt. Chúng tôi nhận thấy rằng ¾ (74%) trong số họ trả lời đã phải đối phó với cuộc xâm phạm hoặc dự đoán việc đó sẽ xảy ra trong vòng một năm. Điều này không đồng nghĩa với việc họ thất bại trong công việc của họ, chìa khóa chính là phản ứng nhanh với các xâm phạm từ ban đầu, để đảm bảo các nhân tố nguy hiểm không tìm thấy các ổ dữ liệu nhạy cảm hoặc tài sản quan trọng khác. Tuy nhiên, việc này minh họa được cường độ hoạt động mà có nhóm SecOps phải đối mặt.

Việc này tạo nên sự cố tăng áp lực. Khác với vai trò hằng ngày của đa số nhân viên, các chuyên viên bảo mật tham gia vào việc phát hiện và đối phó với mối đe dọa bị áp lực trong tâm trí rằng, nếu họ thất bại, tổ chức đó sẽ chịu ảnh hưởng tài chính và danh tiếng nghiêm trọng. Người được phỏng vấn ước tính trung bình mỗi lần bị xâm hại GDPR sẽ tốn 235.000 đô-la Mỹ. Nhưng trên thực tế con số này có thể cao hơn rất nhiều. Ví dụ, một số tập đoàn là nạn nhân của ransomware tiết lộ đã tổn thất hàng chục triệu đô-la.

Một vài nhân tố chính khiến SecOps gặp nhiều vấn đề:

• **Đại dịch ransomware**: Nhờ vảo sự phổ biến của mô hình liên kết cùng với các phương thức ngày càng cụ thể hóa và tinh tế, cũng như bao gồm cả việc thẩm thấu dữ liệu. Trend Micro đã phát hiện các nhánh ransomware mới trong năm 2020 tăng 34% tính theo năm.

• **Sơ suất nội bộ:** Như đã nêu chi tiết trong báo cáo "Làm việc trên mây" của chúng tôi, làm việc tại nhà đã khiến nhân viên đối mặt với các hành vi nguy hiểm mà họ nghĩ là không có vấn đề gì, như là tải dữ liệu công ty vào ứng dụng chưa được duyệt.

• **Làm việc từ xa** : Chuyển sang làm việc từ xa hàng loạt cũng ảnh hưởng đến hiệu quả của các nhóm SecOps đã quen làm việc tại cùng một văn phòng.

• **Sử dụng công cụ hợp pháp** : Các tác nhân nguy hiểm đang ngày càng tận dụng các tính năng và công cụ hợp pháp để di chuyển ngang cũng như lọc dữ liệu, khiến việc phát hiện chúng gặp nhiều khó khăn.

• **Có quá nhiều công cụ**: Sau đây chúng ta sẽ thấy, một trong những nguyên nhân lớn khiến SecOps nhức nhối chính là số lượng ứng dụng bảo mật đang hiện hữu trong hệ thống tập đoàn, dẫn đến lượng tin cảnh báo cao ngất ngưỡng.

Hoạt động bảo mật an ninh bị choáng ngợp bởi các tin cảnh báo

Kết quả của việc bành trướng tội phạm mạng ngầm và quá nhiều công cụ, cùng với sự thiếu hụt công nghệ để tương quan và tối ưu cảnh báo, là các nhóm SecOps đang phải chịu áp lực. Hơn phân nửa (51%) cho biết họ bị chìm trong tin báo, tăng lên 54% đối với các nhóm SOC và thậm chí cao hơn trong các mảng như bất động sản (70%), pháp lí (69%), nhà hàng khách sạn (65%) và bán lẻ (61%).

Hơn một nửa (55%) người được phỏng vấn thừa nhận họ không tự tin về khả năng tối ưu hay ứng phó trước những báo động. Vì vậy, không ngạc nhiên khi họ dành trung bình hơn ¼ (27%) thời gian xử lí các tín hiệu giả. Một thách thức không kém xuất phát từ tình hương này là khả năng có cảnh báo không có lỗi giả từ mối đe dọa thật đang lẩn trốn trong hệ thống.

Chuyên viên bảo mật bị áp lực và không hài lòng với công việc

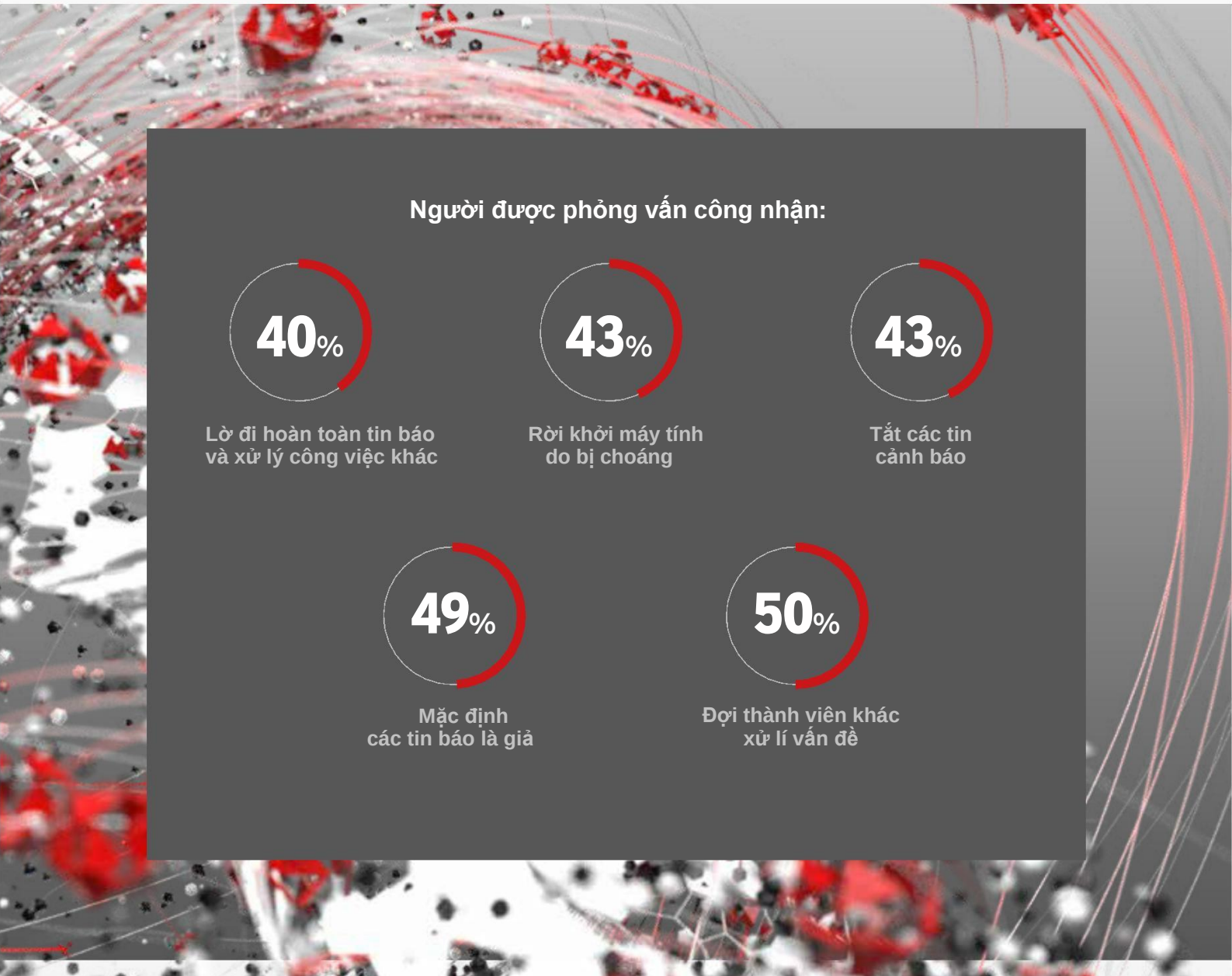
Tin xấu cho các nhà quản lí SecOps rằng báo động quá tải này đang có tác động đáng kể đến chất lượng sống nhân viên của họ. Khoảng 70% người trả lời cho biết họ cảm thấy bị ảnh hưởng tâm lý bởi công việc của mình. Nhiều người thừa nhận:

- Họ không thể thư giản do căng thẳng
- Thời gian nghỉ ngơi của họ bị ảnh hưởng do không thể ngừng nghĩ về công việc
- Họ khó chịu với bạn bè và gia đình.

Chỉ 28% trong các nhóm SOC cho biết họ có thể hoàn toàn nghỉ ngơi và quên công việc khi hết giờ làm việc.

Số lượng tin cảnh báo ồ ạt đến các nhóm SecOps đến mức, phần lớn người trả lời cho biết, họ thường xuyên hoặc đôi khi xảy ra tình trạng:

- Lờ đi hoàn toàn tin báo và xử lí công việc khác (40%)
- Rời khỏi máy tính do bị choáng (43%)
- Tắt các tin cảnh báo (43%)
- Mặc định nghĩ các tin báo đó là giả (49%)
- Đợi thành viên khác xử lí vấn đề (50%)



Tiếp cận dễ dàng hơn với Trend Micro Vision One™

Rõ ràng các căng thẳng trên không chỉ khiến tổ chức rơi vào thế khó khi đối mặt với các mối nguy hiểm mạng nghiêm trọng, mà còn đồng thời đe dọa đến tinh thần và phúc lợi của đội ngũ bảo mật an ninh mạng.

Nhưng tin tốt là, các nền tảng công nghệ hiện nay có thể giảm tải áp lực cho nhóm SecOps bằng cách cải thiện khả năng phát hiện và ứng phó với mối đe dọa. Trend Micro Vision One là nền tảng phát hiện mối đe dọa được xây dựng vượt xa XDR để cung cấp cái nhìn tối ưu và tăng tốc độ ứng phó với các mối đe doạn trong hệ thống tập đoàn. Không giống với các giải pháp phát hiện và đối phó khác chỉ quan sát điểm cuối, Vision One tương quan các cảnh báo trên toàn email, máy chủ, đám mây công việc kể cả mạng để tối ưu hiển thị và phản hồi thông minh.

Với Vision One, tổ chức của bạn sẽ nhận được:

• Thời gian phát hiện và đối phó nhanh hơn, nhờ vào cảnh báo ít hơn và được tối ưu để hành động.

• Khả năng hiển thị và bảo vệ xuyên suốt điểm cuối, mạng, email, trung tâm dữ liệu và đám mây để tự động chặn các đợt tấn công.

• Khắc phục tự động để loại bỏ phần mềm độc hại và giải phóng thời gian cho chuyên viên phân tích.

• Tập trung nguồn các cảnh báo, điều tra, ngăn ngặn để hỗ trợ ứng phó nhanh và sử dụng it 0nguồn lực hơn.

• Cải thiện năng suất của chuyên viên phân tích SOC

• Giảm thiểu rủi ro tài chính và ảnh hưởng danh tiếng.

• Các nhóm SecOps hạnh phúc hơn.

Với một nền tảng như Vision One, các tổ chức có thể đối phó với sự cố nhanh hơn để chặn đứng nhân tố nguy hiểm trước khi chúng có thể gây hậu quả dài hạn. Bằng cách giúp SecOps tối ưu hóa cảnh báo, họ có thể giảm thiểu nguy cơ kiệt sức, cải thiện mức độ hài lòng trong công việc và tăng năng suất lao động của các chuyên viên.

Để biết thêm thông tin, hãy truy cập www.trendmicro.com

Các mối đe dọa tiềm ẩn do các chuyên gia về mối đe dọa mạng của Trend Micro chủ động phát hiện và khắc phục.
Được viết bởi dữ liệu thực bởi tác giả Brendan Dawes.

Biên dịch bởi Thanh Hiền – Iworld.com.vn