CISCO
SECURE

Nghiên cứu kết quả bảo mật

Tập 2

Tối đa hóa năm phương thức bảo mật hàng đầu

Mục lục

Giới thiệu (lại) về Fab Five

Nghiên cứu kết quả bảo mật của Cisco 2021 tìm cách đo lường những gì quan trọng nhất trong quản lý an ninh mạng. Để đạt được mục tiêu đó, chúng tôi đã kiểm tra 25 biện pháp bảo mật chung và thử nghiệm xem mỗi phương pháp tương quan như thế nào với việc đạt được 11 kết quả cấp chương trình. Bạn có thể xem các mối tương quan giữa biện pháp và kết quả này thông qua hình ảnh tương tác trên trang web Nghiên cứu kết quả bảo mật của Cisco 2021 hoặc tải xuống báo cáo đầy đủ.

Từ thử nghiệm, chúng tôi nhận ra rằng 5 trong số 25 biện pháp nổi bật nhất về mức độ đóng góp cho chương trình bảo mật đạt giá trị cao nhất trong số tất cả các kết quả đã đo lường.

Trong các trang tiếp theo, chúng tôi tập trung vào các yếu tố “Fab Five” thúc đẩy sự thành công của chương trình bảo mật để xác định các chiến lược tối đa hóa hiệu quả của chúng. “Fab Five” bao gồm:

Chủ động làm mới công nghệ	Tổ chức có chiến lược chủ động làm mới công nghệ để luôn cập nhật các công nghệ bảo mật và CNTT tốt nhất hiện có.
Tích hợp công nghệ hiệu quả	Các công nghệ bảo mật được tích hợp tốt và hoạt động hiệu quả với nhau.
Ứng phó kịp thời với sự cố	Khả năng ứng phó sự cố giúp có thể điều tra và khắc phục các sự kiện an ninh kịp thời và hiệu quả.
Phát hiện đúng mối đe dọa	Khả năng phát hiện mối đe dọa giúp nắm bắt chính xác các sự kiện bảo mật tiềm ẩn không có điểm mù đáng kể.
Nhanh chóng khôi phục sau sự cố	Khả năng phục hồi giúp giảm thiểu tác động và đảm bảo khả năng phục hồi của các chức năng kinh doanh chịu ảnh hưởng từ sự cố bảo mật.

Hiệu quả rộng rãi của những phương pháp này đặt ra câu hỏi "Tại sao?" Điều gì khiến các phương pháp này trở thành yếu tố then chốt để gặt hái thành công? Những yếu tố nào làm tăng hoặc giảm hiệu quả của các phương pháp này? Các công ty nên thực hiện những phương pháp này như thế nào để đạt kết quả tốt nhất? Đây là những loại câu hỏi mà chúng tôi muốn tìm hiểu trong phần tiếp theo về Nghiên cứu kết quả bảo mật này.

Trong các trang tiếp theo, chúng tôi tập trung vào các yếu tố “Fab Five” thúc đẩy sự thành công của chương trình bảo mật để xác định các chiến lược tối đa hóa hiệu quả của chúng. Chúng tôi thực hiện điều này thông qua một cuộc khảo sát "giấu kín kép", được tiến hành độc lập với hơn 5.100 chuyên gia bảo mật và CNTT trên khắp thế giới. Chúng tôi tìm hiểu chi tiết về dữ liệu, đúc rút những phát hiện nổi bật và chia sẻ những điểm đáng chú ý đã xem xét để giúp mở ra những đỉnh cao mới về thành tựu bảo mật cho tổ chức của bạn.

Những phát hiện chính

Chúng tôi đã hỏi hơn 5.100 chuyên gia bảo mật và CNTT tại 27 quốc gia về cách tiếp cận mà tổ chức của họ áp dụng đối với việc cập nhật và tích hợp kiến trúc bảo mật, phát hiện và ứng phó với các mối đe dọa cũng như việc luôn kiên cường khi xảy ra sự cố. Bạn có thể hình dung họ đã chia sẻ nhiều thông tin chi tiết, những nỗ lực, chiến lược và sự thành công. Chúng tôi đã phân tích mọi phản hồi theo nhiều cách, đúc rút những phát hiện chính như những phát hiện được nêu bên dưới.

Cập nhật và tích hợp kiến trúc

- CNTT hiện đại và tích hợp tốt là yếu tố góp phần vào thành công chung của chương trình, hiệu quả hơn bất kỳ phương thức bảo mật hoặc kiểm soát nào khác.
- Đối với các kiến trúc mới hơn, dựa trên đám mây, việc làm mới thường xuyên sẽ dễ dàng hơn nhiều để bắt kịp với công việc kinh doanh.
- Những tổ chức chủ yếu lấy nguồn từ một nhà cung cấp duy nhất sẽ tăng gấp đôi cơ hội xây dựng hệ thống công nghệ tích hợp.
- Các công nghệ bảo mật tích hợp có khả năng đạt được mức độ tự động hóa quy trình cao hơn gấp 7 lần.

Phát hiện và ứng phó đối với các mối đe dọa trên mạng

- Những chương trình hoạt động bảo mật (SecOps) được xây dựng dựa trên con người, quy trình và công nghệ hiệu quả sẽ đạt được hiệu quả tăng gấp 3,5 lần so với những chương trình có nguồn lực yếu kém hơn.
- Các nhóm phát hiện và ứng phó thuê ngoài thể hiện năng lực vượt trội hơn, nhưng các nhóm nội bộ lại có thời gian ứng phó trung bình nhanh hơn (6 ngày so với 13 ngày).
- Những nhóm sử dụng thông tin về mối đe dọa một cách rộng rãi sẽ có khả năng phát hiện và ứng phó hiệu quả gấp 2 lần.
- Quy trình tự động hóa giúp tăng gấp đôi hiệu suất của những người ít kinh nghiệm và giúp các nhóm có năng lực gần như chắc chắn (95%) đạt được thành công trong hoạt động bảo mật (SecOps).

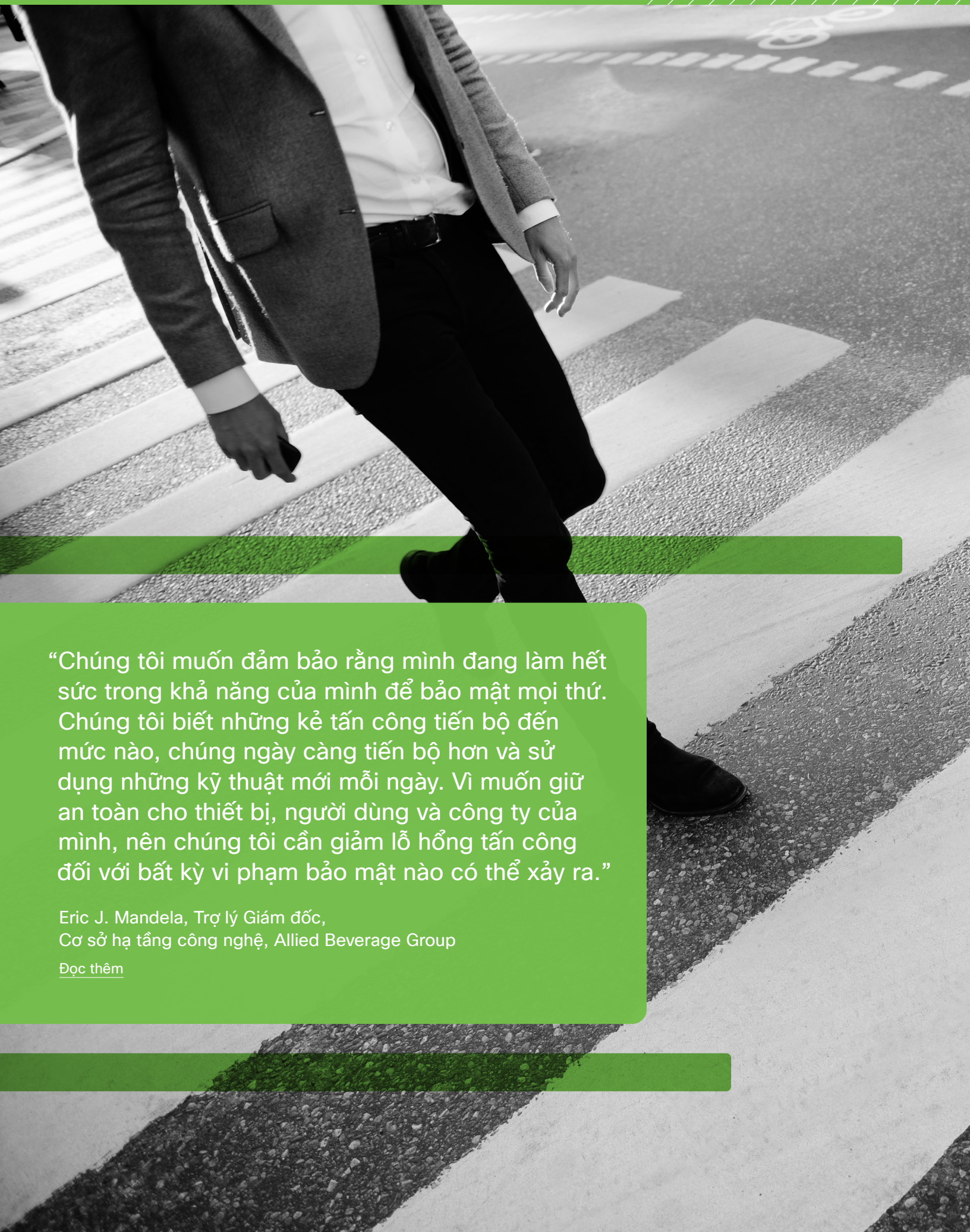
Luôn kiên cường khi xảy ra sự cố

- Những tổ chức có sự giám sát của hội đồng quản trị về tính liên tục của hoạt động kinh doanh và khả năng khắc phục sự cố sẽ có nhiều khả năng (trên mức trung bình 11%) có các chương trình hiệu quả nhất.
- Việc có thể duy trì khả năng phục hồi của doanh nghiệp chỉ cải thiện khi ít nhất 80% hệ thống quan trọng đảm bảo được tính liên tục của hoạt động kinh doanh và có khả năng khôi phục sau sự cố.
- Những tổ chức thường xuyên kiểm tra tính liên tục của hoạt động kinh doanh và khả năng khôi phục sau sự cố bằng nhiều cách sẽ có thể duy trì khả năng phục hồi của doanh nghiệp cao hơn gấp 2,5 lần.
- Những tổ chức xem kỹ thuật hỗn loạn là giải pháp tiêu chuẩn sẽ có khả năng đạt được mức độ phục hồi cao hơn gấp 2 lần.

Giới thiệu về cuộc khảo sát này

Lấy mẫu	Người trả lời	Phân tích
Cisco đã hợp tác với công ty nghiên cứu khảo sát YouGov để thực hiện một cuộc khảo sát hoàn toàn ẩn danh vào giữa năm 2021, sử dụng kỹ thuật lấy mẫu ngẫu nhiên phân tầng.	5.123 chuyên gia CNTT, bảo mật và quyền riêng tư đang làm việc tại 27 quốc gia đã tham gia khảo sát. Bạn có thể xem mẫu thông tin nhân khẩu học trong phần phụ lục.	Viện Cyentia đã thay mặt Cisco tiến hành phân tích độc lập dữ liệu khảo sát và thu được toàn bộ các kết quả trình bày trong nghiên cứu này.

5.123 chuyên gia CNTT, bảo mật và quyền riêng tư đang làm việc tại **27** quốc gia đã tham gia khảo sát



“Chúng tôi muốn đảm bảo rằng mình đang làm hết sức trong khả năng của mình để bảo mật mọi thứ. Chúng tôi biết những kẻ tấn công tiến bộ đến mức nào, chúng ngày càng tiến bộ hơn và sử dụng những kỹ thuật mới mỗi ngày. Vì muốn giữ an toàn cho thiết bị, người dùng và công ty của mình, nên chúng tôi cần giảm lỗ hổng tấn công đối với bất kỳ vi phạm bảo mật nào có thể xảy ra.”

Eric J. Mandela, Trợ lý Giám đốc,
Cơ sở hạ tầng công nghệ, Allied Beverage Group

Đọc thêm

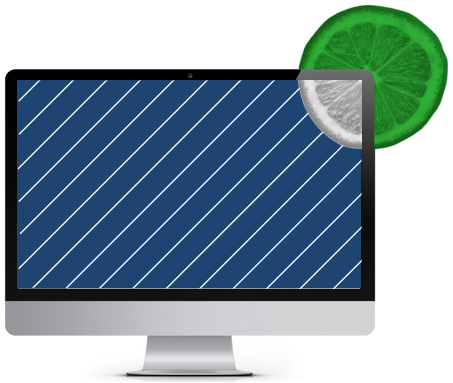
Các chiến lược chủ động làm mới công nghệ

Nghiên cứu trước đây của chúng tôi cho thấy rằng cách tiếp cận chủ động để làm mới cũng như duy trì các công nghệ bảo mật và CNTT tốt nhất đã góp phần mang lại thành công cho chương trình an ninh mạng hơn bất kỳ phương pháp nào khác. Đó là một thành tích không nhỏ vì toàn bộ 25 phương pháp mà chúng tôi đã thử nghiệm đều được công nhận rộng rãi là "phương pháp hay nhất" theo đúng nghĩa. Vì vậy, chúng tôi rất muốn tìm hiểu cách làm cho phương pháp này trở nên hiệu quả trong nghiên cứu tiếp theo này.

Khi bắt đầu tìm hiểu sâu hơn về các chiến lược làm mới công nghệ, chúng tôi thực hiện một bài kiểm tra đánh giá nhanh về "độ mới" của cơ sở hạ tầng hiện có. Chúng tôi đã hỏi những người tham gia về tỷ lệ công nghệ bảo mật đang hoạt động của họ đã lỗi thời. Trung bình, 39% công nghệ bảo mật mà các tổ chức sử dụng bị xem là công nghệ lỗi thời. Gần 13% người được hỏi khẳng định rằng ít nhất 8 trong số 10 công cụ bảo mật mà họ sử dụng đã cũ.

Chỉ riêng thực tế này cũng có thể chỉ ra rất nhiều lợi ích mà chúng ta nhận được từ chiến lược chủ động làm mới công nghệ. Rõ ràng, các công nghệ mới hơn mang đến các khả năng tiên tiến để chống lại loạt mối đe dọa mạng ngày càng tiến bộ. Nhưng còn nhiều điều hơn thế nữa, vì vậy, chúng ta hãy tiếp tục tìm hiểu các câu hỏi về dữ liệu mà chúng tôi đã đưa ra.

Trung bình, 39% công nghệ bảo mật mà các tổ chức sử dụng bị xem là công nghệ lỗi thời.



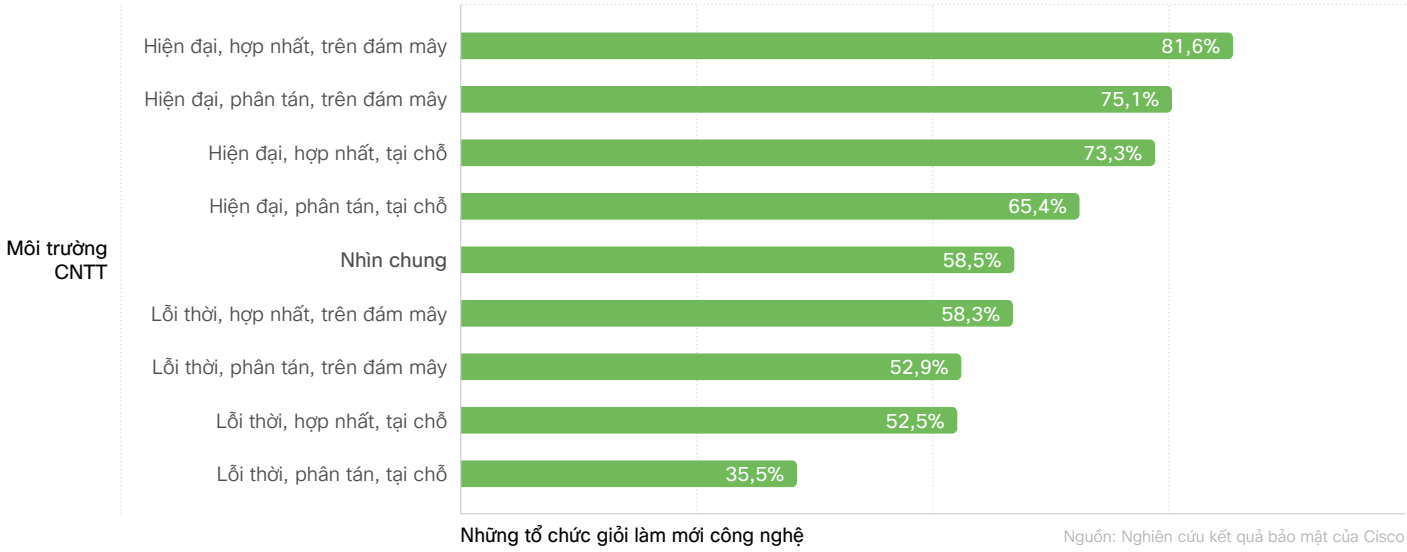
Các đặc điểm cơ sở hạ tầng có ảnh hưởng đến sáng kiến làm mới không?

Trong nghiên cứu ban đầu, chúng tôi suy đoán rằng các kiến trúc dựa trên đám mây, hiện đại hơn có thể hiệu quả hơn vì chúng dễ quản lý hơn và được tích hợp sẵn các biện pháp bảo mật gốc. Để kiểm tra giả thuyết đó, chúng tôi yêu cầu người trả lời mô tả chung về cơ sở hạ tầng công nghệ của họ bằng cách chọn một nhóm yếu tố mô tả theo tỷ lệ, bao gồm:

- Trên đám mây hay Tại chỗ
- Hiện đại hay Lỗi thời
- Hợp nhất hay Phân tán

Những đặc điểm kiến trúc khác nhau này có góp phần vào hiệu quả của khả năng làm mới công nghệ không? Theo hình 1 thì ảnh hưởng rất nhiều đó. **Những tổ chức có kiến trúc hiện đại, hợp nhất, dựa trên đám mây có khả năng làm mới công nghệ hiệu quả cao hơn gấp 2 lần so với những tổ chức sử dụng công nghệ lỗi thời, phân tán, tại chỗ.** Tuy nhiên, trước khi đưa ra biểu đồ đó trong cuộc họp chiến lược tiếp theo về di chuyển sang đám mây, hãy lưu ý rằng những tổ chức có môi trường chủ yếu là tại chỗ vẫn hoạt động tốt hơn mức bình thường, miễn là họ đã hiện đại hóa CNTT.

Chắc chắn, việc chuyển sang đám mây giúp bạn dễ dàng triển khai chiến lược làm mới công nghệ của mình hơn, nhưng lỗi thời là vấn đề cấp bách hơn ở đây. Khi việc làm mới cơ sở hạ tầng cũ trở nên khó khăn, bạn có thể đạt được nhiều tiến bộ hơn khi chuyển sang một kiến trúc mới hơn là việc tiếp tục trang bị thêm cho kiến trúc cũ. Tất nhiên, điều đó không phải lúc nào cũng khả thi hoặc tiết kiệm chi phí với cơ sở hạ tầng cũ hoặc quan trọng, nhưng nguyên tắc chung vẫn được áp dụng.



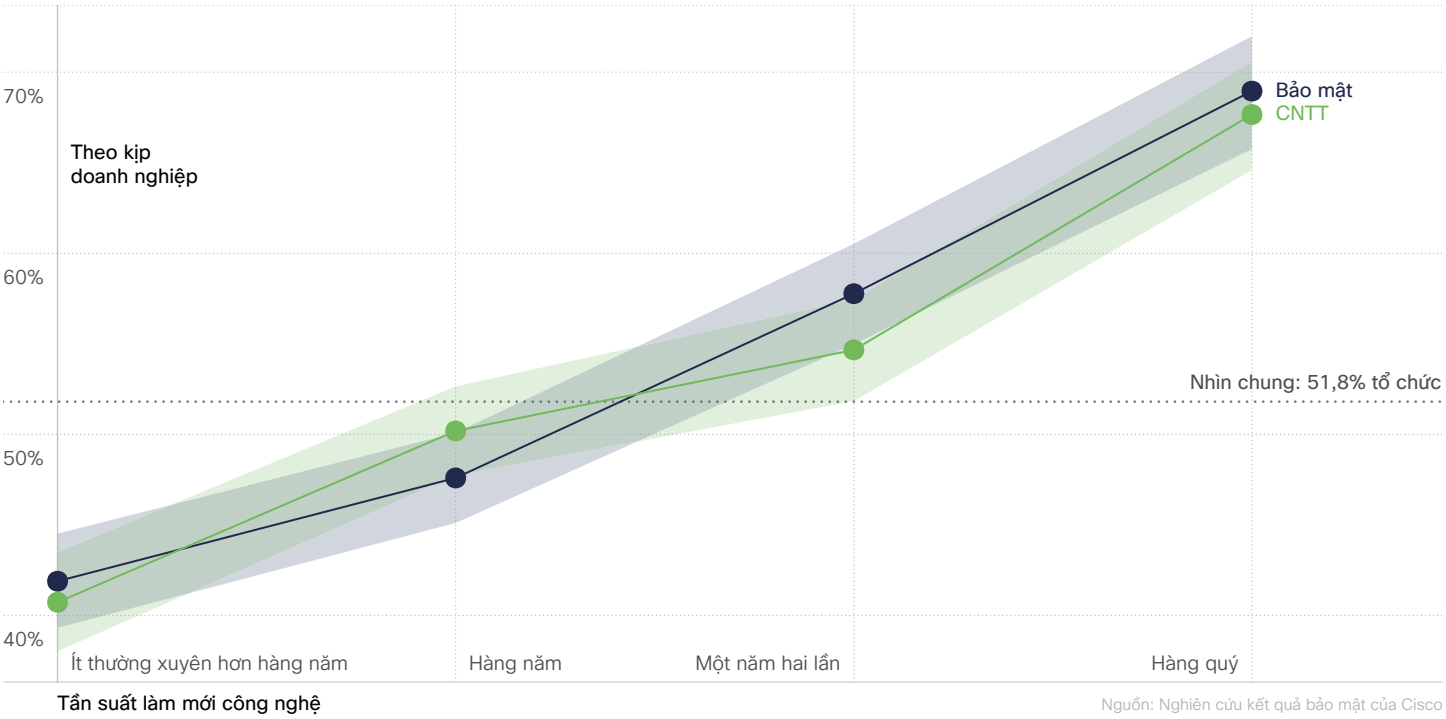
Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 1: Ảnh hưởng của các đặc điểm kiến trúc CNTT đến hiệu suất làm mới công nghệ

81,6% số tổ chức có kiến trúc hiện đại, hợp nhất, dựa trên đám mây có khả năng làm mới công nghệ mạnh mẽ

Việc nâng cấp thường xuyên có giúp hệ thống bảo mật theo kịp doanh nghiệp không?

Theo Nghiên cứu kết quả bảo mật 2021, kết quả tương quan chặt chẽ nhất với chiến lược chủ động làm mới công nghệ đang hỗ trợ chương trình bảo mật theo kịp với nhu cầu và sự tăng trưởng của doanh nghiệp. Trên thực tế, đó là sự kết hợp hiệu quả nhất giữa phương pháp và kết quả trong toàn bộ nghiên cứu.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 2: Ảnh hưởng của tần suất làm mới công nghệ đến khả năng bắt kịp doanh nghiệp của chương trình bảo mật[1]

Chúng tôi đã hỏi các tổ chức về tần suất nâng cấp CNTT và bảo mật của họ, đồng thời so sánh những câu trả lời đó với khả năng theo kịp doanh nghiệp của chương trình bảo mật. 2 biến này có mối quan hệ với nhau không? Quả nhiên là có; chúng tôi nhận thấy kết quả quan trọng này có sự cải thiện ổn định khi nhịp độ nâng cấp tăng lên. **Nhìn chung, những tổ chức nâng cấp công nghệ bảo mật và CNTT hàng quý có khả năng theo kịp doanh nghiệp cao hơn 30% so với những tổ chức vài năm mới nâng cấp một lần.** Nghe có vẻ như tấm áp phích khích lệ tinh thần cho các nhóm CNTT đang căng thẳng: Hãy cập nhật và tiếp tục phát huy.

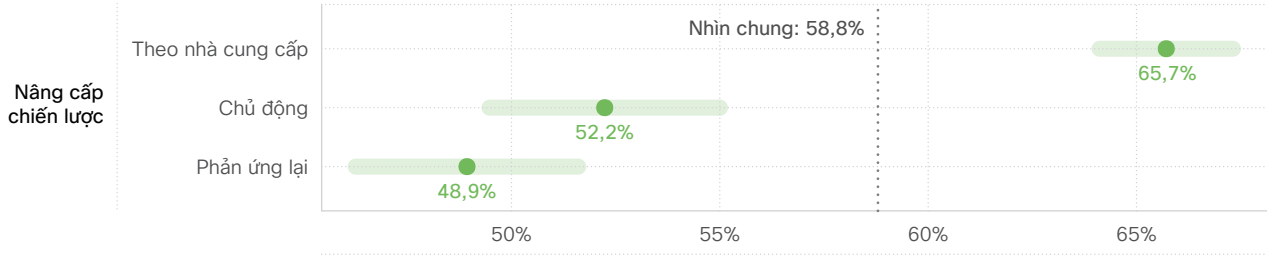
[1] Trong suốt báo cáo, chúng tôi sẽ gắn nhãn giá trị "Nhìn chung" cho các số liệu đối với một thực tiễn hoặc kết quả cụ thể. Đây là giá trị trung bình của tất cả những người tham gia trả lời nhóm câu hỏi cụ thể đó. Giá trị này mang tính tham khảo và cho bạn biết ai đang làm tốt hơn mức trung bình và ai không đạt tiêu chuẩn. Chúng tôi cũng thể hiện sự không chắc chắn thông qua các thanh lỗi hoặc vùng bóng mờ trên một số biểu đồ. Khi các khu vực đó chồng lên dòng "Nhìn chung", điều đó có nghĩa là chúng tôi không thể suy ra rằng khía cạnh cụ thể của chương trình bảo mật có bất kỳ ảnh hưởng nào đến kết quả hoặc phương pháp mà chúng tôi đang kiểm tra.

Điều gì (hoặc ai) sẽ thúc đẩy nỗ lực làm mới công nghệ?

Chúng tôi nhận thấy rằng việc nâng cấp thường xuyên sẽ góp phần tạo điều kiện cho doanh nghiệp, nhưng điều gì – hoặc ai – sẽ thúc đẩy hoàn thành các hoạt động nâng cấp đó? Chúng tôi đã yêu cầu những người tham gia chọn ra động lực chính thúc đẩy tổ chức của họ làm mới công nghệ bảo mật và câu trả lời của họ được chia thành 3 loại chính:

- **Theo nhà cung cấp:** Lịch trình do nhà cung cấp phần mềm dưới dạng dịch vụ (SaaS) xác định hoặc là một phần của sáng kiến hợp nhất nhà cung cấp lớn hơn (yếu tố phổ biến nhất)
- **Chủ động:** Theo lịch trình định trước hoặc khi các trường hợp sử dụng hoặc tính năng mới cho phép nâng cấp (yếu tố phổ biến thứ hai)
- **Phản ứng lại:** Để ứng phó với sự cố, khi công nghệ trở nên lỗi thời hoặc để đáp ứng các yêu cầu tuân thủ (yếu tố ít phổ biến nhất)

Những yếu tố này vốn thú vị, nhưng điều chúng tôi thực sự muốn biết là liệu những động cơ như vậy có tương quan với cách tiếp cận hiệu quả hơn đối với làm mới công nghệ hay không. Câu trả lời có ở Hình 3. Về cơ bản, các sáng kiến làm mới công nghệ sẽ thành công hơn khi nhà cung cấp thực hiện (hoặc ít nhất là tích cực tham gia vào việc hiện thực hóa các sáng kiến đó). **Chưa đến một nửa số người có cách tiếp cận phản ứng cho thấy họ có khả năng làm mới hiệu quả, so với gần 2/3 số người tuân theo chu kỳ làm mới của nhà cung cấp.**



Những tổ chức giỏi làm mới công nghệ

Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 3: Ảnh hưởng của các yếu tố chính thúc đẩy nâng cấp đối với hiệu quả làm mới công nghệ bảo mật

Chúng tôi hiểu điều đó – tất cả điều này nghe có vẻ thực sự đáng ngờ khi ở đây nhắc đến một nhà cung cấp các sản phẩm CNTT và bảo mật. Nhưng thành thật mà nói, chúng tôi không tác động đến kết quả này. Cuộc khảo sát do một công ty nghiên cứu độc lập, có uy tín thực hiện, những người trả lời không biết Cisco tài trợ cho cuộc khảo sát và Viện Cyentia có uy tín đã phân tích dữ liệu để đúc rút ra dữ liệu mà bạn thấy ở Hình 3. Và để đánh giá chính xác, chúng tôi sẽ hết sức thận trọng khi diễn giải những kết quả này.

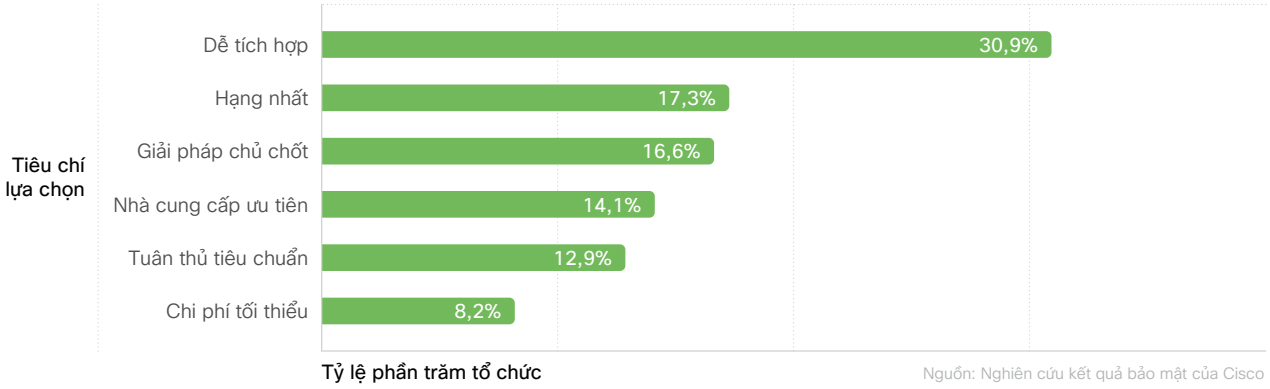
Chúng tôi nghi ngờ rằng phần lớn sự cải tiến đến từ cách tiếp cận theo nhà cung cấp có liên quan đến các kiến trúc đám mây/SaaS thân thiện hơn với các bản nâng cấp thường xuyên. Chúng tôi cũng nhận thấy rằng vấn đề không phải là các nhà cung cấp có năng lực mà là việc thoát khỏi những rào cản nội bộ và vũng lầy chính trị có xu hướng cản trở lịch trình làm mới công nghệ.

Rob Base và DJ E-Z Rock nói rằng "Cần 2 người để làm cho một việc đi đúng hướng. Cần 2 người để việc đó gặt hái thành công". Ai mà biết được họ có phải kiến trúc sư bảo mật hay không! Triển khai chiến lược làm mới của bạn thật thành công bằng cách phát huy khả năng của đối tác giải pháp công nghệ để cải thiện kết quả của nhiệm vụ.

65,7% số tổ chức đồng bộ với chu kỳ làm mới của nhà cung cấp có khả năng làm mới công nghệ hiệu quả

Nâng cấp vì mục tiêu khả năng hay khả năng tương thích?

Phần trước đề cập đến tình huống nào thúc đẩy các tổ chức nâng cấp công nghệ và bây giờ, chúng ta sẽ xem xét lý do họ nên chọn giải pháp này thay vì giải pháp khác. Hình 4 thể hiện tiêu chí lựa chọn mà những người trả lời cho chúng tôi biết. Tích hợp hiệu quả với công nghệ hiện có là ưu tiên rõ ràng, tiếp theo là các giải pháp mang đến những khả năng tốt nhất hoặc đáp ứng các nhu cầu cụ thể. Thật bất ngờ, việc giảm thiểu chi phí lại ở vị trí cuối cùng.



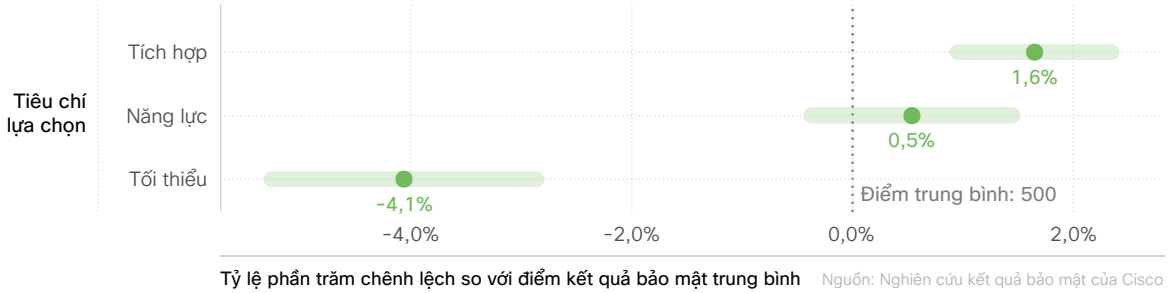
Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 4: Tiêu chí lựa chọn chính khi làm mới các sản phẩm bảo mật

Tất cả tiêu chí đều hợp lý, nhưng tiêu chí nào đóng vai trò quan trọng nhất để xây dựng một chương trình bảo mật thành công? Để trả lời câu hỏi này, chúng tôi đã nhóm các tiêu chí lựa chọn ở Hình 4 thành 3 loại:

- **Tối thiểu:** Giải pháp chi phí tối thiểu; Tuân thủ tiêu chuẩn
- **Dễ tích hợp:** Tích hợp với công nghệ hiện có; Sử dụng các nhà cung cấp ưu tiên
- **Khả năng:** Tốt nhất; Giải pháp chủ chốt

Sau đó, chúng tôi kiểm tra các danh mục này dựa trên điểm tổng hợp cho từng tổ chức dựa trên cấp độ thành tích của họ trên 11 kết quả bảo mật. Giá trị tuyệt đối của điểm số này không có ý nghĩa cụ thể, nhưng là cơ sở để so sánh các chiến lược làm mới công nghệ khác nhau. **Như trong Hình 5, việc ưu tiên tiêu chí tích hợp và khả năng đều mang lại kết quả tốt hơn là việc lựa chọn sản phẩm dựa trên tiêu chí giảm thiểu chi phí hoặc đáp ứng các yêu cầu tuân thủ cơ bản. Tuy nhiên, cách tiếp cận dựa trên sự tích hợp là phương pháp duy nhất vượt trội hơn đáng kể so với trung bình.**



Hình 5: Ảnh hưởng của tiêu chí lựa chọn công nghệ đến điểm số kết quả bảo mật chung

Lưu ý rằng sự khác biệt ở đây là không đáng kể xét về mức độ thành công chung của chương trình. Có vẻ như những gì chúng ta đang thực sự thấy ở đây là cánh cửa dẫn đến các ưu tiên và thực tiễn rộng lớn hơn của chương trình bảo mật. Nhưng điều này cho thấy rằng các vấn đề ít chú ý hơn như lý do chúng ta chọn sản phẩm này mà không chọn sản phẩm khác là điều đáng xem xét. Và nếu bạn muốn xếp hạng các đặc điểm khi làm mới hoặc nâng cấp giải pháp bảo mật, hãy xem đây là lý do hợp lý để thúc đẩy khả năng tương thích và khả năng hơn là giảm thiểu chi phí.

Điểm kết quả bảo mật là gì?

Chúng tôi đã hỏi những người tham gia về mức độ thành công mà tổ chức của họ đạt được thông qua 12 kết quả chương trình bảo mật khác nhau. Ấn bản đầu tiên của Nghiên cứu kết quả bảo mật đã phân tích chi tiết những kết quả này và bạn cũng sẽ thấy một vài kết quả trong số được nghiên cứu riêng trong nghiên cứu này. Nhưng chúng tôi cũng muốn tạo một điểm số tổng hợp để đánh giá mức độ thành công của mỗi tổ chức trên tất cả 12 kết quả như một thước đo về hiệu quả chung của chương trình bảo mật. Chúng tôi gọi đó là "điểm kết quả bảo mật" và bạn sẽ thấy điểm số này được nhắc đến một vài lần trong báo cáo này.

Để có được điểm số này, chúng tôi đã sử dụng một kỹ thuật thống kê ưa thích là “Lý thuyết ứng đáp câu hỏi”. Bằng kỹ thuật này, chúng tôi có thể chấm điểm các tổ chức dựa trên mức độ hiệu quả của họ ở tất cả các kết quả, đồng thời tính đến thực tế là một số kết quả có thể khó đạt được hơn những kết quả khác. Kỹ thuật đã qua kiểm chứng này là cách tạo điểm thử nghiệm tiêu chuẩn. Giá trị tuyệt đối của điểm số này không có ý nghĩa cụ thể, nhưng là cơ sở để so sánh giữa các chương trình.

"Giám đốc an ninh thông tin phải vừa là người có tầm ảnh hưởng vừa là người hướng dẫn. Để hoạt động hiệu quả nhất có thể, chúng ta cần phải đi đầu trong các quyết định chiến lược được đưa ra trong tổ chức của mình. Tuy nhiên, chẳng những cố gắng thuyết phục mọi người rằng bảo mật là vấn đề quan trọng, rằng chúng tôi cần đầu tư hợp lý để thực hiện tốt điều đó và rằng chúng tôi nên tham gia vào mọi khía cạnh của doanh nghiệp, chúng tôi còn phải hướng dẫn cho họ. Hầu hết các giám đốc điều hành không có kiến thức cơ bản về bảo mật, vì vậy, chúng tôi cần liên tục thông báo cho họ về các loại rủi ro đi kèm khi đưa ra mỗi quyết định."

Helen Patton, Giám đốc tư vấn an toàn thông tin,
Cisco @CisoHelen

Nghe Helen chia sẻ về vai trò CISO ngày càng phát triển trong tập podcast Câu chuyện bảo mật đầy hấp dẫn này của chúng tôi

Tích hợp hiệu quả Công nghệ bảo mật

Theo Nghiên cứu kết quả bảo mật mới nhất của chúng tôi, các công nghệ bảo mật được tích hợp tốt hoạt động hiệu quả với cơ sở hạ tầng CNTT rộng lớn hơn sẽ góp phần mang lại thành công cho tất cả các kết quả của chương trình. Chúng tôi đã đặt ra một loạt câu hỏi nhằm tìm hiểu sâu hơn về các yếu tố mang lại thành tích đáng khen đó, bắt đầu từ những ý định về việc tích hợp công nghệ bảo mật.

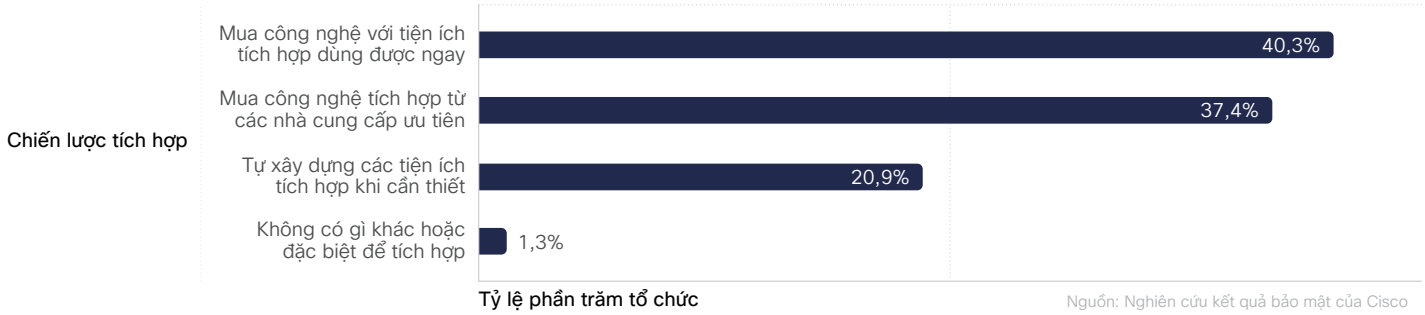
Theo những người trả lời, động lực phổ biến nhất để tích hợp các công nghệ bảo mật là nâng cao hiệu quả giám sát và kiểm toán. Điều là điều mà chúng tôi mong muốn, bởi lẽ chúng tôi vốn mệt mỏi và thất vọng khi phải kiểm tra nhiều bảng điều khiển hoặc trang tổng quan để tổng hợp một số thông tin liên quan đến những gì đang xảy ra trên mạng. Sự cộng tác và tự động hóa dễ dàng hơn cũng là những động lực phổ biến để tích hợp công nghệ bảo mật (và sau này sẽ còn nhiều hơn nữa). Chúng tôi đã đối chiếu những động lực này so với kết quả của chương trình và mức độ tích hợp công nghệ được báo cáo, nhưng mối tương quan không quá chặt chẽ. Có lẽ câu hỏi "điều gì" hoặc "cách nào" quan trọng hơn "tại sao" khi tích hợp các công nghệ bảo mật? Hãy tìm hiểu kỹ hơn một chút về chủ đề đó trong các câu hỏi sau.

Theo những người trả lời, động lực phổ biến nhất để tích hợp các công nghệ bảo mật là nâng cao hiệu quả giám sát và kiểm toán.

Mua hay xây dựng cho công nghệ được tích hợp hiệu quả?

Từ nghiên cứu trước, chúng tôi biết rằng việc tích hợp công nghệ bảo mật sẽ thúc đẩy kết quả, nhưng cách tốt nhất để có được một hệ thống công nghệ tích hợp cao là gì? Mua như đề xuất? Xây dựng cho phù hợp? Giữ nguyên trạng? Hãy xem liệu chúng tôi có tìm ra đáp án hay không nhé.

Chúng tôi đã hỏi các tổ chức về cách tiếp cận điển hình của họ đối với việc tích hợp công nghệ bảo mật và Hình 6 sẽ minh họa các câu trả lời. **Nhìn chung, hơn 3/4 tổ chức muốn mua các giải pháp tích hợp hơn là tự xây dựng.** Trong số các tổ chức đó, hơn 40% chọn các công nghệ có thể tích hợp ngay vào cơ sở hạ tầng hiện có của họ. Hơn 37% tổ chức thực hiện thêm một bước nữa và muốn tìm các giải pháp của một nhà cung cấp duy nhất để tích hợp hiệu quả một cách tự nhiên hoặc đưa các giải pháp đó vào một nền tảng lớn hơn. Chỉ hơn 20% tổ chức sẵn sàng tự xây dựng các tiện ích tích hợp, miễn là sản phẩm phù hợp với nhu cầu của họ. Rất ít người áp dụng cách tiếp cận theo kiểu tự do.



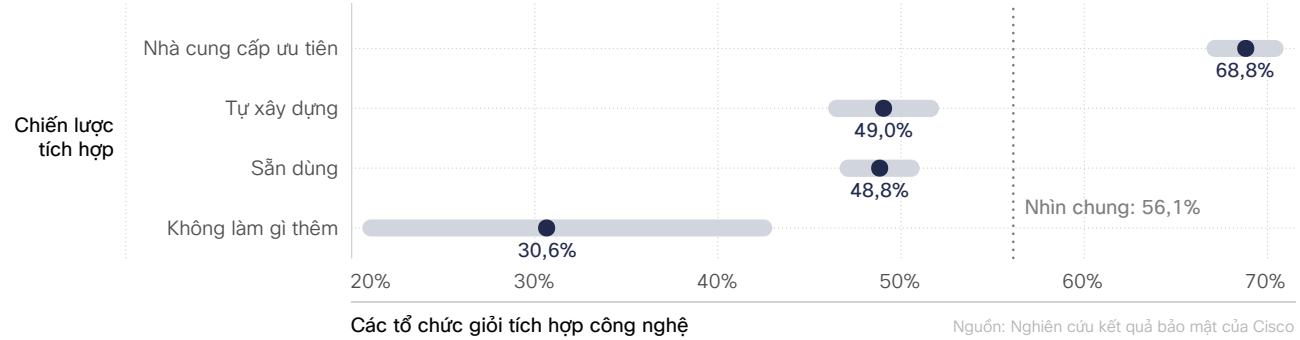
Hình 6: Các cách tiếp cận phổ biến để tích hợp công nghệ bảo mật tại tất cả các tổ chức

Nhìn chung, hơn **3/4** tổ chức muốn mua các giải pháp tích hợp hơn là tự xây dựng

Hình 7 đánh giá liệu bất kỳ cách tiếp cận tích hợp nào trong số này có tạo ra sự khác biệt hay không. Ở đây, chúng ta lại tìm hiểu một chủ đề về lợi ích từ việc cộng tác với các nhà cung cấp để giúp công nghệ luôn hiện đại và được tích hợp hiệu quả. **Như bạn thấy trong biểu đồ, việc gắn bó với một nhà cung cấp ưu tiên sẽ giúp bạn có khả năng tích hợp hiệu quả công nghệ bảo mật hơn gấp đôi so với lựa chọn không làm gì thêm (~ 69% so với ~ 31%).** Hơn nữa, theo nghiên cứu của chúng tôi, phát hiện này đúng với tất cả các quy mô tổ chức, mặc dù việc sử dụng nhà cung cấp ưu tiên mang lại nhiều lợi ích hơn một chút cho doanh nghiệp vừa và nhỏ so với doanh nghiệp lớn.

Chúng tôi còn phát hiện ra một điểm đáng ngờ khác về công ty có danh mục bảo mật tích hợp, phong phú. Chắc chắn, chúng tôi rất vui khi thấy rằng kết quả này hỗ trợ chiến lược của Cisco... nhưng hãy nhớ rằng đây là một nghiên cứu "giấu kín kép" và chúng tôi hoàn toàn không tác động đến kết quả đó.

Không có gì ngạc nhiên khi những tổ chức không làm gì thêm để tích hợp công nghệ bảo mật đã cho thấy kết quả đúng như dự đoán. **Tuy nhiên, chúng tôi cho rằng một số người sẽ ngạc nhiên khi biết rằng hầu như không có sự khác biệt giữa những người mua sản phẩm có tiện ích tích hợp sẵn và những người tự xây dựng tiện ích tích hợp.** Chưa đến một nửa (~49%) số tổ chức sử dụng một cách tiếp cận trong số này cho thấy mức độ tích hợp mạnh mẽ.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 7: Ảnh hưởng của các cách tiếp cận tích hợp phổ biến đối với khả năng tích hợp công nghệ bảo mật

Chuyển sang đám mây để có nhiều cơ hội tích hợp

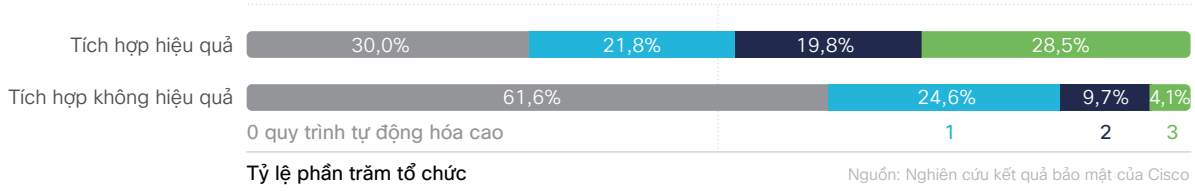
Nhiều tổ chức cho chúng tôi biết họ đang băn khoăn không biết nên bắt đầu (hoặc mở rộng) nỗ lực tích hợp công nghệ bảo mật trong môi trường đám mây hay tại chỗ. Nếu bạn cũng vậy, chúng tôi sẽ cung cấp cho bạn một số dữ liệu để giúp đánh giá một cách đúng đắn. Tin vui là nhiều người tham gia khảo sát cho biết họ thu được kết quả tốt trong cả môi trường tại chỗ và đám mây. Điều đó cho thấy, việc tích hợp công nghệ mạnh mẽ trên đám mây có vẻ trở nên dễ dàng hơn rất nhiều.

Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 8: Ảnh hưởng của môi trường đám mây so với môi trường tại chỗ đến mức độ tích hợp công nghệ bảo mật

Tích hợp có hỗ trợ tự động hóa không?

Theo nội dung ở đầu phần này, tự động hóa không phải là động lực phổ biến nhất để tích hợp công nghệ. Nhưng 44% số tổ chức đã xem đây là động lực. Ngoài các động lực, có bằng chứng cho thấy việc tích hợp hiệu quả công nghệ sẽ mang đến cơ hội tự động hóa các quy trình bảo mật tốt hơn không? Bằng chứng được đưa ra trong Hình 9 chỉ ra rằng thực sự là như vậy.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

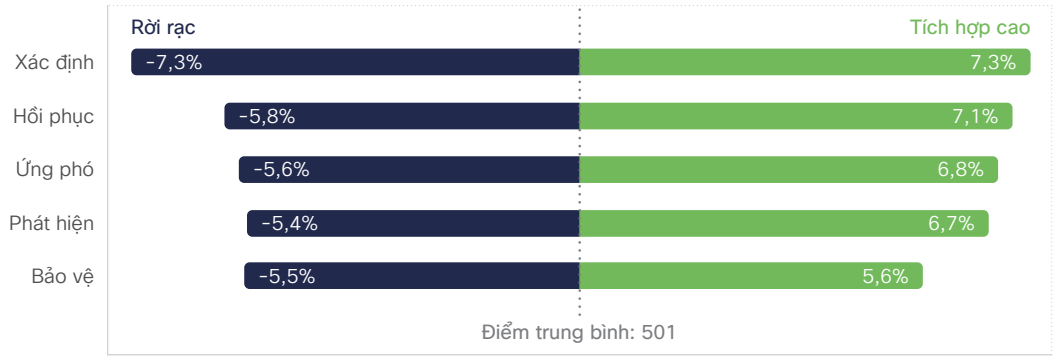
Hình 9: Ảnh hưởng của tích hợp công nghệ đến mức độ tự động hóa quy trình bảo mật

2 thanh ngang trong Hình 9 thể hiện sự khác biệt giữa các tổ chức về mức độ tích hợp công nghệ bảo mật (tốt so với kém). Các phân đoạn màu thể hiện số lượng quy trình bảo mật chính (giám sát sự kiện, phân tích sự cố và ứng phó sự cố) được hỗ trợ bởi tự động hóa kỹ lưỡng. Tỷ lệ tổ chức không áp dụng tự động hóa cao gấp hơn 2 lần so với số tổ chức có khả năng tích hợp kém. **Ngược lại, số tổ chức tích hợp hiệu quả công nghệ bảo mật có khả năng đạt được mức độ tự động hóa cao cho cả 3 quy trình này cao hơn gần 7 lần (4,1% so với 28,5%).** Đó thực sự là một động lực hấp dẫn!

Nên tích hợp những chức năng nào?

Tiếp theo, chúng tôi hỏi những người tham gia về mức độ họ tích hợp các công nghệ hỗ trợ 5 chức năng cốt lõi của Khung an ninh mạng NIST (CSF). Chúng tôi đưa ra thang đáp án từ phân tán cao (công nghệ tách biệt hoạt động chủ yếu cô lập) đến tích hợp cao (công nghệ phối hợp hoạt động như một đơn vị chức năng). Sau đó, chúng tôi tạo một mô hình để xác định mức độ ảnh hưởng đến điểm số bảo mật chung cho mỗi tổ chức.

Các kết quả trong Hình 10 khá nhất quán giữa 5 chức năng. **Nỗ lực hợp nhất và tích hợp bất kỳ khía cạnh chức năng nào theo Khung an ninh mạng NIST sẽ góp phần mang đến thành công ấn tượng hơn cho chương trình bảo mật (+11% đến ~15%).** Vì vậy, câu trả lời cho câu hỏi trên của chúng tôi sẽ là "tất cả các chức năng". Tuy nhiên, chức năng "Xác định" được tích hợp cao sẽ là yếu tố thúc đẩy lớn nhất nếu bạn đang băn khoăn không biết bắt đầu từ đâu.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

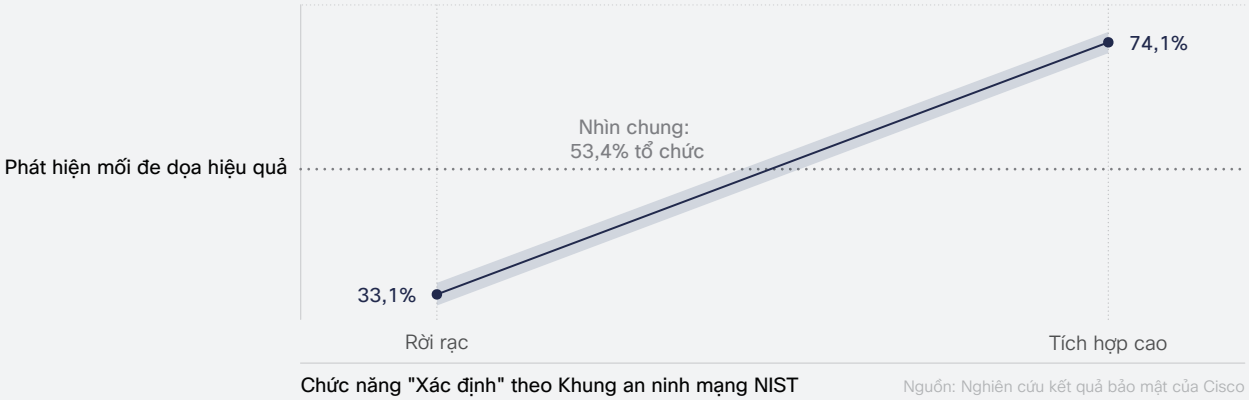
Hình 10: Tác động của việc tích hợp các chức năng theo Khung an ninh mạng NIST đối với điểm số bảo mật chung

Có mối liên hệ rõ ràng giữa thực tế này và những gì chúng ta đã học được ở phần trước về việc giám sát, kiểm tra và cộng tác là các động lực lớn nhất để tích hợp công nghệ. Tất cả các động lực này hợp lại thể hiện được tầm quan trọng cơ bản của tầm nhìn tốt trong toàn doanh nghiệp. Điều này đồng nghĩa với việc cách tiếp cận phân tán đối với "trau dồi sự hiểu biết có tổ chức để quản lý rủi ro an ninh mạng với hệ thống, con người, tài sản, dữ liệu và khả năng" (ngôn ngữ CSF) sẽ không mang lại kết quả tốt. Bạn sẽ được tìm hiểu thêm về chủ đề này ở phần Phát hiện mối đe dọa và ứng phó với sự cố.

Tích hợp, xác định và thông tin

Ngoài biểu đồ mà chúng ta vừa thảo luận, dữ liệu trong suốt nghiên cứu này đều chỉ ra mối quan hệ cốt yếu giữa tích hợp, xác định và thông tin. Nếu không thể xác định một tài sản hoặc mối đe dọa, bạn sẽ không biết mối nguy hiểm đang hiện hữu, do đó, sẽ không đủ cảnh giác để thiết lập một biện pháp bảo vệ sáng suốt cho đến khi quá muộn.

Hình 11 minh họa rõ ràng khía cạnh này. Chúng tôi đã so sánh mức độ tích hợp của mỗi tổ chức trong chức năng "Xác định" theo Khung an ninh mạng NIST với khả năng của họ trong việc phát hiện chính xác các mối đe dọa một cách kịp thời. **Những tổ chức có hệ thống tích hợp cao để xác định các tài sản và rủi ro nghiêm trọng có khả năng phát hiện mối đe dọa tốt hơn nhiều (+41%).** Vì vậy, trong thực tế, chống phân tán và chống kẻ tấn công là 2 yếu tố song hành!



Hình 11: Hiệu quả của việc tích hợp chức năng Xác định theo Khung an ninh mạng NIST đối với khả năng phát hiện mối đe dọa

Những tổ chức có hệ thống tích hợp cao để xác định các tài sản và rủi ro nghiêm trọng đạt hiệu quả cao hơn **41%** xét về khả năng phát hiện mối đe dọa

“Tự động hóa giúp các kỹ sư của chúng tôi ứng phó kịp thời với các mối đe dọa mới xuất hiện. Giờ đây, chúng tôi có thể tập trung vào việc hiểu đúng các khái niệm bảo mật thay vì liên tục cập nhật các quy tắc và giám sát mạng 24/7. Cisco đào sâu nghiên cứu và trích xuất thông tin chúng tôi cần để có thể làm tốt hơn công việc bảo mật và duy trì cơ sở hạ tầng mà chúng tôi có. Cisco đã mang đến cho chúng tôi sự kết hợp hoàn hảo giữa trí tuệ con người và máy móc”.

Steve Erzberger, Giám đốc công nghệ, Frankfurter Bankgesellschaft (Schweiz) AG

Đọc thêm

Phát triển khả năng phát hiện mối đe dọa và ứng phó với sự cố

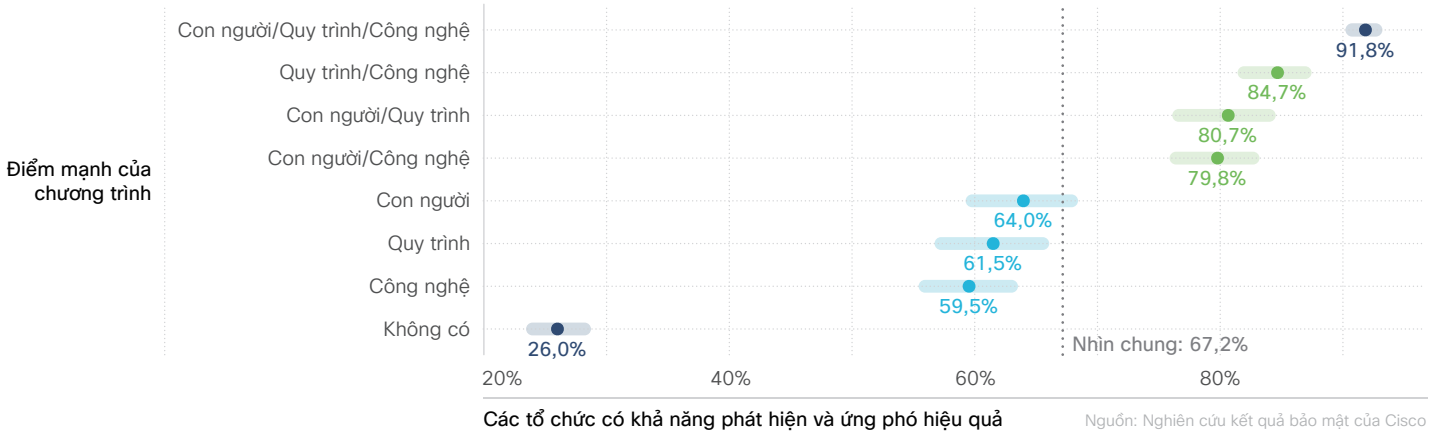
Phần này bao gồm 2 khía cạnh biện pháp bảo mật riêng mà cả hai đều đã tạo ra quy tắc Fab Five theo đúng nghĩa. Vì chức năng phát hiện mối đe dọa và ứng phó với sự cố (IR) thường là sự kết hợp giữa con người, quy trình và công nghệ dưới cái tên hoạt động bảo mật (SecOps), nên chúng tôi đã đặt ra một loạt câu hỏi phổ biến liên quan. Vì vậy, sẽ hợp lý khi phân tích các yếu tố đó trong cùng một phần của nghiên cứu này.

Gần như tất cả (khoảng 92%) các tổ chức có con người, quy trình và công nghệ hiệu quả đều đạt được khả năng phát hiện và ứng phó với mối đe dọa ấn tượng.

Ưu tiên con người, quy trình hay công nghệ?

Chúng ta hay cùng tìm hiểu về các yếu tố con người, quy trình và công nghệ (hay còn gọi là bộ ba p-p-t). Các chức năng bảo mật thường được mô tả là sự kết hợp của cả 3 yếu tố này, đặc biệt là ở khía cạnh phát hiện mối đe dọa và ứng phó với sự cố. Nhưng yếu tố nào trong bộ 3 bảo mật này là quan trọng nhất? Vấn đề là thế đó; chúng ta hãy bắt đầu phân tích nhé.

Bắt đầu từ cuối của Hình 12, chúng ta thấy rằng chỉ có khoảng 1/4 chương trình không hiệu quả ở tất cả các khía cạnh của bộ 3 p-p-t là thể hiện sự tin tưởng vào SecOps của họ. Khi đạt được hiệu quả ở bất kỳ khía cạnh nào - con người, quy trình hay công nghệ - tỷ lệ phần trăm đó sẽ tăng tới khoảng 60% đến 64%, tùy thuộc vào khía cạnh nào. Yếu tố con người có năng lực dường như mang lại một chút lợi thế, nhưng vì các khoảng tin cậy chồng chéo nhau, nên hãy thận trọng để không quá xem trọng dữ kiện đó. Điểm mấu chốt quan trọng là bất kỳ điều nào trong số này đều cung cấp một điểm khởi đầu tốt để xây dựng khả năng phát hiện và phản hồi tốt hơn.



Hình 12: Ảnh hưởng của con người, quy trình và công nghệ mạnh đến khả năng phát hiện mối đe dọa và ứng phó sự cố

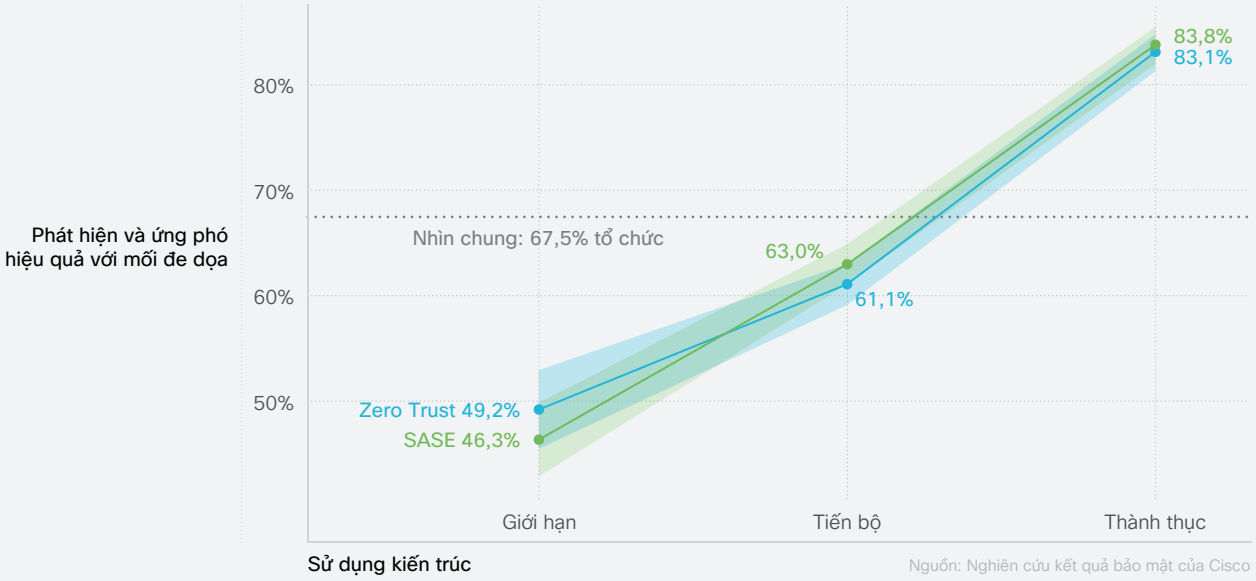
Tiếp tục đến Hình 12, làm tốt hai điều sẽ giúp các chương trình SecOps vượt trội hơn mức trung bình một cách vững chắc và cải thiện khả năng khoảng 15% đến 20% so với những chương trình chỉ làm tốt một việc. Xin nhắc lại, việc bạn kết hợp yếu tố con người, quy trình hay công nghệ như thế nào không quá quan trọng. Bạn chỉ cần làm tốt 2 yếu tố mà thôi. Thật vui khi biết rằng bạn có quyền tự do lựa chọn trong việc điều chỉnh lộ trình SecOps cho tổ chức của mình, đúng không nào?

Và khi đó chúng ta sẽ đạt được các chương trình ấn tượng như trong Hình 12 với khả năng nắm chắc bộ ba SecOps trong tay. **Gần như tất cả (khoảng 92%) các tổ chức có con người, quy trình và công nghệ hiệu quả đều đạt được khả năng phát hiện và ứng phó với mối đe dọa ấn tượng.** Hiệu suất của họ cao hơn gấp 3,5 lần so với những chương trình SecOps không đạt được bất kỳ yếu nào kể trên! Vì vậy, hãy bắt đầu ở bất cứ đâu để đạt được nhiều thành tựu nhất, nhưng đừng dừng lại cho đến khi bạn đạt đến đỉnh cao của p-p-t.

Với những tổ chức có con người, quy trình và công nghệ hiệu quả, khả năng phát hiện và ứng phó với mối đe dọa hiệu quả hơn **3,5 lần** so với những tổ chức yếu kém ở cả 3 phương diện này

Mô hình Zero Trust và SASE có góp phần cải thiện SecOps không?

Chúng tôi hiểu rằng các yếu tố mô tả trừu tượng như "công nghệ hiệu quả" gây khó khăn cho việc hình thành các kết quả cụ thể từ những phát hiện ở trên. Đó là lý do tại sao chúng tôi đặt ra một số câu hỏi tiếp theo về các kiến trúc cụ thể. Chúng tôi đã hỏi những người tham gia về việc họ áp dụng mô hình Zero Trust và Cạnh dịch vụ truy cập an toàn (SASE) để hiểu rõ hơn các cách tiếp cận đó ảnh hưởng ra sao đến khả năng phát hiện mối đe dọa và ứng phó với sự cố (do đó, ảnh hưởng đến kết quả của chương trình bảo mật).



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

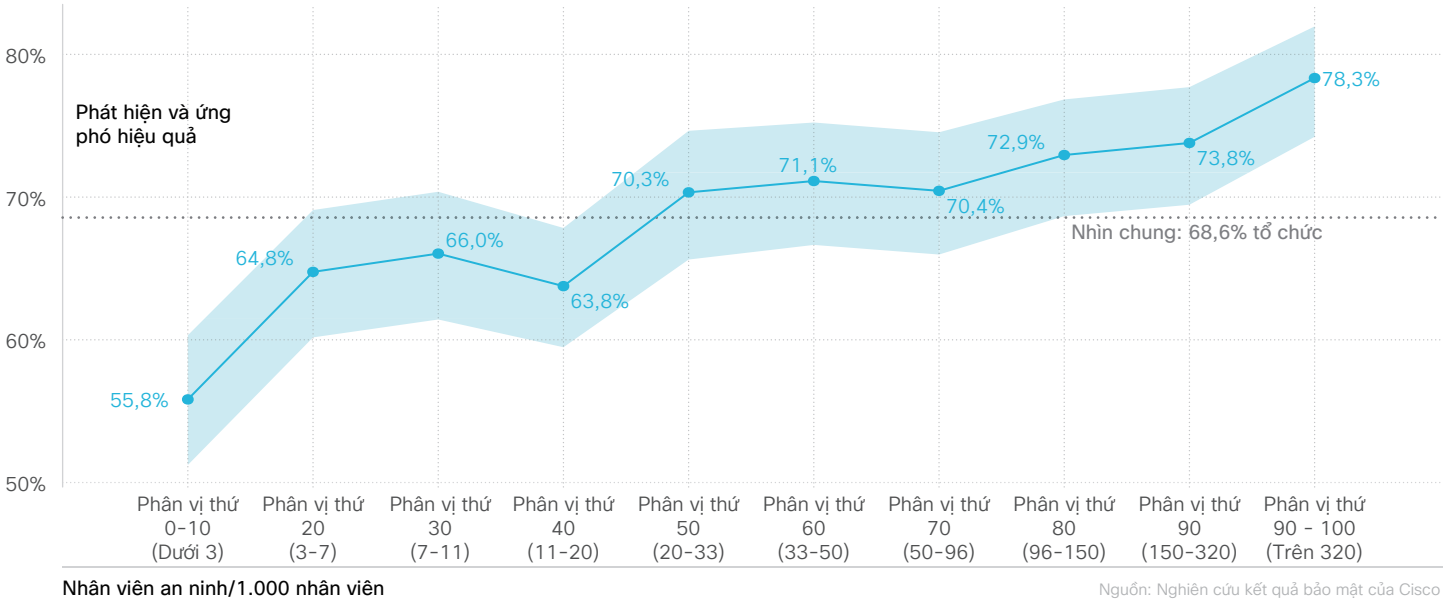
Hình 13: Ảnh hưởng của kiến trúc SASE và Zero Trust đối với khả năng phát hiện mối đe dọa và ứng phó với sự cố

Những tổ chức cho biết triển khai thuần thục kiến trúc Zero Trust hoặc SASE có khả năng đạt được SecOps hiệu quả cao hơn khoảng 35% so với những tổ chức triển khai chưa tốt. Những kết quả này là minh chứng cho những gì mà chúng tôi đã chia sẻ trước đó về nhiều lợi ích mà kiến trúc hiện đại có thể mang lại cho các chương trình an ninh mạng.

Thêm nhân lực đồng nghĩa với việc tăng hiệu quả công việc ư?

Chúng tôi biết rằng những người có năng lực đóng vai trò quan trọng trong việc xây dựng khả năng phát hiện mối đe dọa và ứng phó với sự cố hiệu quả. Nhưng nên tập trung vào việc bổ sung nhân lực hay trau dồi kỹ năng cho nhân lực bạn hiện có? Rõ ràng, không nhất thiết phải chọn một trong hai, nhưng câu hỏi vẫn còn bỏ ngỏ - có bằng chứng nào cho thấy số lượng hay chất lượng quan trọng hơn khi phát triển các đội ngũ SecOps thành công không?

Để trả lời câu hỏi này, trước tiên, chúng tôi tính toán tỷ lệ nhân viên SecOps trên tổng số nhân viên đối với tất cả các tổ chức. Sau đó, chúng tôi so sánh tỷ lệ đó với khả năng phát hiện và ứng phó được báo cáo. Hình 14 mô tả kết quả của các phép tính đó. Mặc dù hình này không giải đáp hoàn toàn được câu hỏi về số lượng hay chất lượng, nhưng thể hiện được một số điểm quan trọng.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 14: Ảnh hưởng của tỷ lệ nhân viên bảo mật đến khả năng phát hiện mối đe dọa và ứng phó với sự cố

Điểm đầu tiên đúc rút được là tỷ lệ nhân viên bảo mật tương quan với khả năng phát hiện và ứng phó tốt hơn với mối đe dọa. So với các tổ chức có tỷ lệ này thấp nhất, những tổ chức có tỷ lệ cao nhất đạt được khả năng tốt hơn chỉ cao hơn 20%. NHƯNG – hãy xem đường chấm thể hiện mức trung bình tổng thể cắt qua phần lớn khoảng tin cậy được tô bóng như thế nào trong Hình 14? Về cơ bản, điều đó có nghĩa là (phần lớn) những tổ chức có quy mô nhân sự hợp lý đều có khả năng như nhau trong việc đạt được chương trình SecOps hiệu quả.

Tất cả những điều đó thực sự có ý nghĩa gì? Về năng lực phát hiện và ứng phó hiệu quả, chúng tôi có thể tự tin nói rằng những tổ chức có đội ngũ bảo mật hùng hậu có nhiều khả năng đạt được điều đó hơn đáng kể so với những tổ chức có đội ngũ bảo mật ít ỏi. Nhưng chỉ riêng số lượng nhân viên sẽ không giải quyết được mọi vấn đề về SecOps của hoặc đảm bảo sự thành công. Hơn nữa, ngay cả sự khác biệt giữa tỷ lệ nhân sự thấp nhất và cao nhất cũng không giải thích cho việc sự cải thiện hiệu suất có liên quan đến việc có nguồn nhân lực mạnh mà chúng ta nhắc đến ở phần trước. **Do đó, chúng tôi suy ra rằng chất lượng tương đương – có lẽ còn quan trọng hơn số lượng – khi nói đến việc xây dựng các đội ngũ phát hiện và ứng phó hiệu quả với mối đe dọa.**

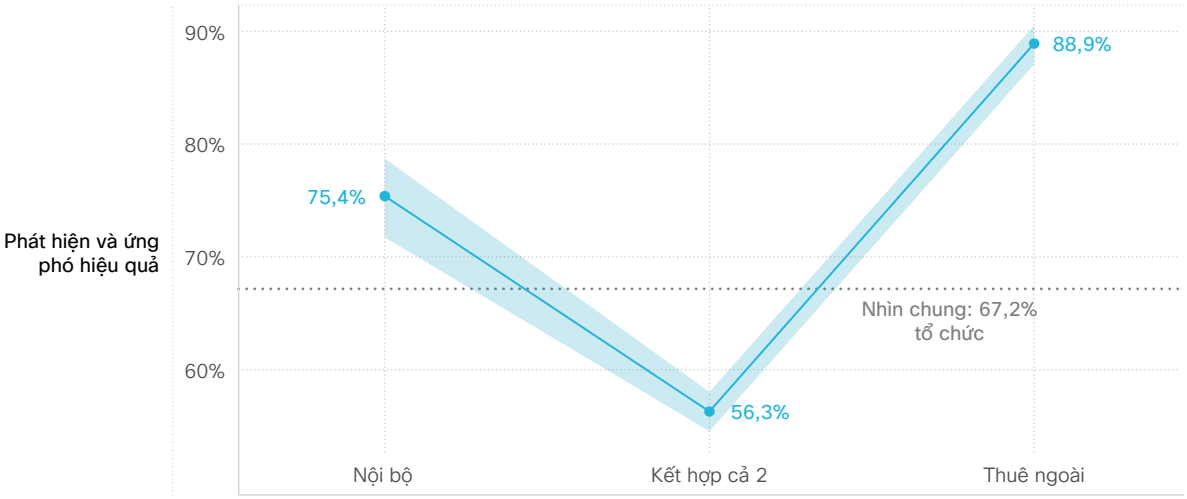
Đội ngũ bảo mật tiếp tục đối mặt với tình trạng thiếu nhân sự trầm trọng.

Với nguồn lực bị thu hẹp và các mối đe dọa ngày càng tăng, nhiều chuyên gia an ninh mạng đang trở nên cực kỳ căng thẳng và kiệt sức. Chúng ta có thể thực hiện những biện pháp chủ động nào để giúp họ? Trong cuốn sách điện tử này, chúng tôi đã mời các nhà lãnh đạo và chuyên gia trong ngành chia sẻ những hiểu biết và câu chuyện của họ về việc kiểm soát sức khỏe tâm thần.

Nhân sự SecOps: Của bạn, của tôi hay của chúng ta?

Vì vậy, sự thành công về SecOps không chỉ đơn thuần là nhờ số lượng nhân viên, nhưng các mô hình nhân sự có ảnh hưởng đến kết quả không? Tất cả mọi thứ đều như nhau, tốt hơn nên thuê ngoài, dùng nguồn lực nội bộ hay chia sẻ trách nhiệm phát hiện và ứng phó với mối đe dọa? Hãy xem dữ liệu trả lời câu hỏi đó như thế nào – nhưng hãy nhớ – dữ liệu cũng thể hiện cả 2 mặt.

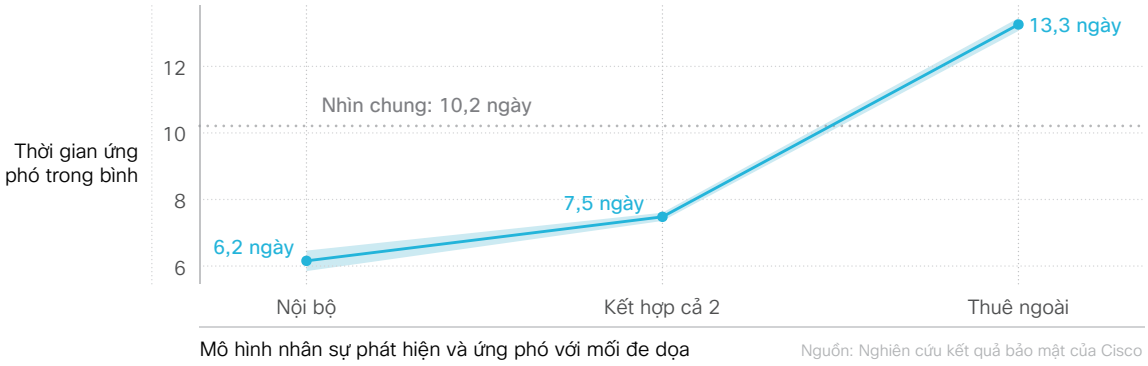
Chúng tôi đã hỏi những người tham gia về mô hình nhân sự của họ và sau đó, so sánh yếu tố đó với khả năng phát hiện và ứng phó. **Như bạn thấy trong Hình 15, những tổ chức có đội ngũ chủ yếu thuê ngoài hoặc sử dụng nguồn lực nội bộ sẽ có nhiều khả năng hơn (tương ứng +20% đến 30%) trong việc đạt được chương trình SecOps hiệu quả so với những tổ chức có mô hình nhân sự hỗn hợp.** Vì hầu hết các tổ chức cho biết họ sử dụng một số dạng mô hình hỗn hợp, chúng tôi nghĩ nên xem xét điều này từ một góc độ khác, chứ không nên chỉ dựa vào kết quả (dường như) từ cuộc khảo sát mà đưa ra kết luận về sự thất bại của họ.



Hình 15: Ảnh hưởng của các mô hình nhân sự đối với khả năng phát hiện mối đe dọa và ứng phó với sự cố được nhận thấy

Về khía cạnh có chương trình SecOps hiệu quả, những tổ chức có nhân lực chủ yếu thuê ngoài hoặc chủ yếu nội bộ sẽ có nhiều khả năng hơn **20 - 30%** so với những tổ chức dùng mô hình nhân sự hỗn hợp

Ngoài việc yêu cầu người trả lời đánh giá khả năng phát hiện và ứng phó được nhận thấy, chúng tôi cũng cố gắng thu thập các số liệu khách quan hơn để so sánh. Một trong số đó là Thời gian phản hồi trung bình (MTTR) hoặc thời gian trung bình để khắc phục hoặc ngăn chặn sự cố bảo mật. Trong phân tích cơ bản của chúng tôi bên ngoài báo cáo này, các số liệu này thường có xu hướng thể hiện các đánh giá chủ quan. Nhưng 2 quan điểm mâu thuẫn với nhau trong trường hợp này, như được thể hiện rõ trong Hình 16.



Hình 16: Ảnh hưởng của các mô hình nhân sự đến Thời gian ứng phó trung bình với sự cố bảo mật[2]

Dựa trên khía cạnh thể hiện trong Hình 16, những tổ chức có đội ngũ phát hiện và ứng phó với mối đe dọa nội bộ sẽ có MTTR thấp hơn một nửa so với những tổ chức sử dụng mô hình thuê ngoài (khoảng 6 ngày so với 13 ngày). Những tổ chức có mô hình nhân sự kết hợp sẽ có MTTR ở mức trung bình (khoảng 8 ngày), tức là không nhanh bằng các đội ngũ có mô hình nội bộ nhưng nhanh hơn nhiều so với các đối tác chủ yếu được thuê ngoài.

Rõ ràng, chúng tôi gặp một vấn đề nan giải ở đây. Thước đo nào (quan điểm hay số liệu) là đúng và quan trọng hơn là bạn nên dựa vào thước đo nào khi đưa ra quyết định tìm nguồn cung ứng. Chúng tôi sẽ cố ý bỏ qua câu hỏi này ở đây, đồng thời xem như "cả hai" hoặc "không thước đo nào cả" (đừng trách chúng tôi vì đã làm theo hướng dẫn xung đột về dữ liệu ở đây nhé).

Tất nhiên, khả năng khắc phục gồm nhiều yếu tố và phụ thuộc vào điều đó. Tổ chức có thể yêu cầu nhà cung cấp đưa ra bản vá/bản sửa lỗi nhằm giải quyết hoàn toàn lỗ hổng bảo mật. Sau đó, bản vá cần được kiểm tra tại phòng thí nghiệm trong môi trường của chúng trước khi được triển khai chính thức. Tóm lại, có rất nhiều bộ phận chuyển động liên quan.

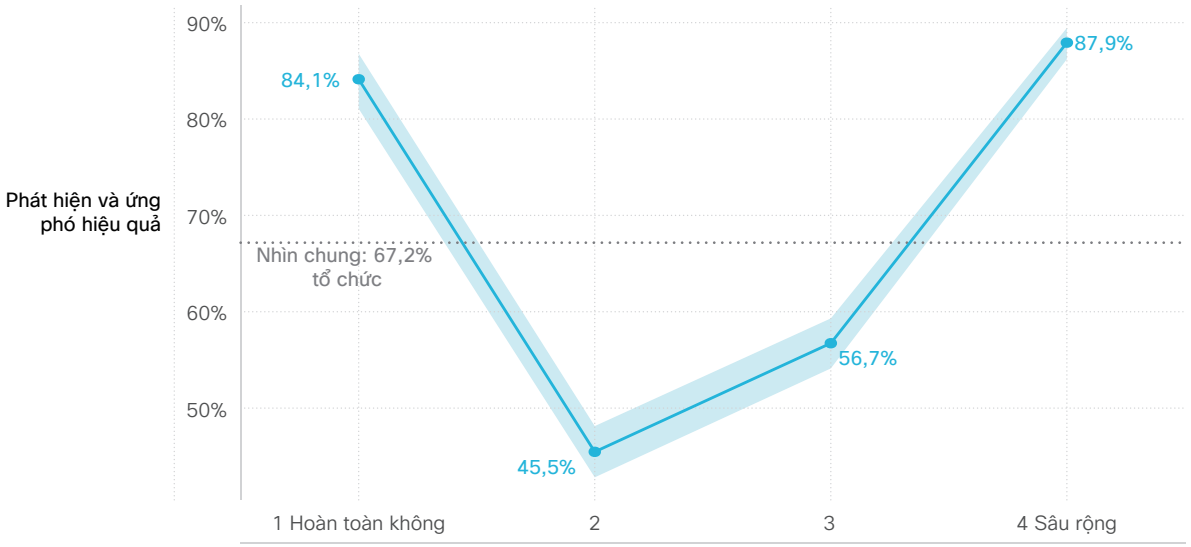
Trên thực tế, thật khó để biết chắc chắn điều gì đang xảy ra ở đây. Có thể việc cố gắng thu thập số liệu thông qua một cuộc khảo sát là sai lầm. Có thể MTTR và xếp hạng khả năng đủ khác nhau để có thể có một chương trình phát hiện và ứng phó "hiệu quả" về tổng thể, nhưng tỷ lệ khắc phục chậm hơn. Có thể những chương trình đó chậm hơn vì chúng kỹ lưỡng hơn. Có thể việc phối hợp với nhân viên thuê ngoài chỉ làm mất nhiều thời gian hơn. Có thể cảm giác tự tin có được vì "chúng tôi đang thuê các chuyên gia làm điều này và họ đã hoàn thành công việc". Có thể chúng ta đang thấy phiên bản SecOps của Hiệu ứng Dunning-Kruger. Đó có thể là tất cả những điều này và hơn thế nữa. Và vì lý do đó, bạn nên sử dụng phần này để tổ chức các cuộc thảo luận hơn là đưa ra quyết định.

[2] Chúng tôi sử dụng giá trị trung bình hình học trong biểu đồ này vì giá trị này tiêu biểu hơn cho giá trị "điển hình". Người trả lời báo cho biết MTTR thường chưa đến 2-3 tuần, nhưng đôi khi là vài tháng (hoặc vài năm!). Sử dụng giá trị trung bình hình học giúp thể hiện tính "điển hình" tốt hơn mà không bị sai lệch do những giá trị cực kỳ lớn đó.

Có nên sử dụng thông tin không?

Khi nói về Hiệu ứng Dunning-Kruger, đó là sự thiết lập hoàn hảo cho phần này. Chúng tôi đã hỏi những người tham gia về việc sử dụng thông tin liên quan đến mối đe dọa mạng trong chương trình SecOps của họ. Hầu hết các tổ chức (85%) nói rằng họ đang sử dụng thông tin ở một mức độ nào đó, nhưng chưa đến 1/3 (31%) tổ chức cho biết họ đang sử dụng thông tin một cách rộng rãi. Thông tin đó có giúp phát hiện và ứng phó với mối đe dọa hiệu quả hơn, thông minh hơn, nhanh hơn không? Chà ... hãy nhìn vào Hình 17.

Thật kỳ lạ, hầu hết các tổ chức hoàn toàn không sử dụng thông tin về mối đe dọa dường như nghĩ rằng họ đang hoạt động khá tốt. Câu ngạn ngữ cổ "bơ đi mà sống" quả là đúng trong trường hợp này, đặc biệt là khi việc thử sử dụng thông tin sẽ bác bỏ những quan niệm đó (độ tin cậy giảm từ khoảng 84% xuống còn 46%). **Những tổ chức sử dụng thông tin về mối đe dọa một cách rộng rãi sẽ có khả năng phát hiện và ứng phó hiệu quả cao gấp gần 2 lần so với những tổ chức ít sử dụng hơn. Trong một ví dụ thể hiện sự phù hợp giữa thứ hạng khả năng và số liệu, những tổ chức sử dụng thông tin nhiều hơn sẽ có MTTR bằng khoảng một nửa so với những người tổ chức không sử dụng thông tin.**



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 17: Ảnh hưởng của việc sử dụng thông tin đến khả năng phát hiện mối đe dọa và ứng phó với sự cố

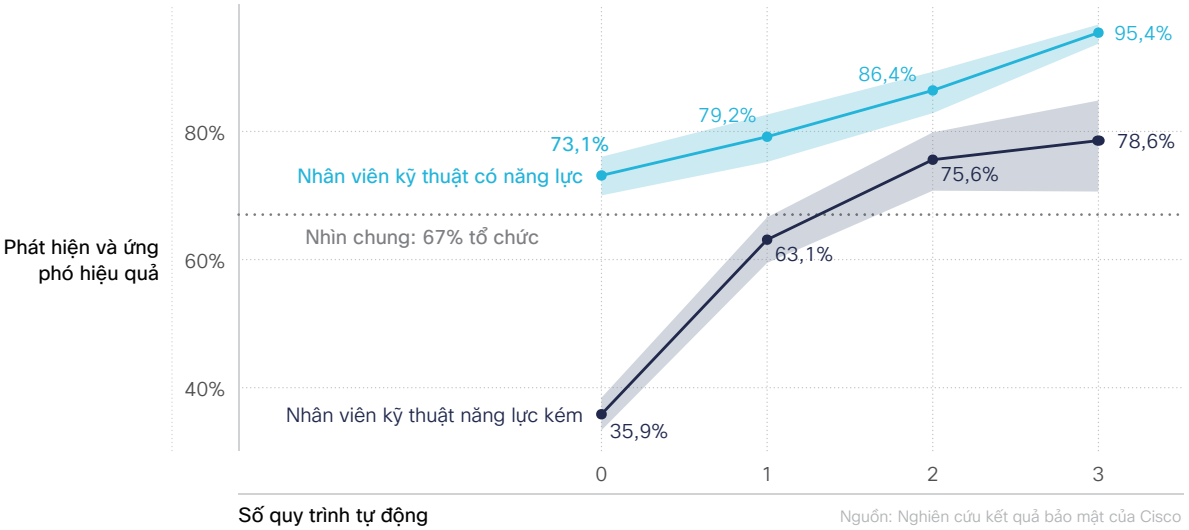
Nhà tâm lý học và tác giả cuốn sách bán chạy nhất Daniel Kahneman từng nói: "Chúng ta mù quáng về chính bản thân mình. Chúng ta không nhận ra sự hạn chế của bản thân". Hình 17 gợi ý rằng khi các tổ chức biết một chút về các mối đe dọa mà mình gặp phải, họ sẽ nhận ra có rất nhiều điều họ không biết. Việc sử dụng rộng rãi hơn thông tin về mối đe dọa sẽ bắt đầu tạo dựng lại sự tự tin đó – trừ khi hiện tại họ không mù quáng đến thế.

Những tổ chức sử dụng rộng rãi thông tin về mối đe dọa sẽ có nhiều khả năng hơn gần **2 lần** xét về năng lực phát hiện và ứng phó hiệu quả với mối đe dọa

Tự động hóa có thay thế được con người không?

Sau khi đọc tiêu đề này, bạn có thể cho rằng đó là một câu hỏi tu từ. Hãy đọc kỹ hơn nhé. Dù có thể không làm hài lòng toàn bộ cộng đồng bảo mật, nhưng chúng tôi xin mạnh dạn đề xuất rằng trên thực tế, tự động hóa có thể thay thế con người. NHƯNG hãy tiếp tục đọc trước khi bạn quyết định xóa báo cáo này và thêm chúng tôi vào danh sách liên hệ bị chặn của bạn. <hít thở sâu>

Hình 18 kết hợp các yếu tố bạn đã thấy trước đây trong các biểu đồ riêng biệt – nhân viên bảo mật và tự động hóa. 2 dòng này so sánh 2 loại chương trình SecOps khác nhau. Dòng đầu tiên (đường màu lam đậm) đại diện cho các tổ chức KHÔNG có nguồn nhân lực mạnh, trong khi đó những tổ chức CÓ nhân lực mạnh được thể hiện bằng đường màu lam nhạt. Trong cả 2 tình huống, việc di chuyển từ trái sang phải cho thấy tác động của việc tăng mức độ tự động hóa đối với khả năng phát hiện mối đe dọa và ứng phó với sự cố.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 18: Ảnh hưởng của sức mạnh nhân lực và tự động hóa đến khả năng phát hiện mối đe dọa và ứng phó với sự cố

Hãy xem xét trường hợp của Have Nots. Chỉ khoảng 1/3 tổ chức thiếu nhân viên bảo mật hiệu quả và không tự động hóa bất kỳ quy trình chính nào có khả năng phát hiện và ứng phó tốt. Tỷ lệ đó sẽ tăng lên rất nhiều khi một trong ba khía cạnh quy trình mà chúng tôi yêu cầu (giám sát mối đe dọa, phân tích sự kiện, ứng phó với sự cố) được tự động hóa. Việc tự động hóa 2 khía cạnh trong số đó sẽ nâng cao giá trị hơn nữa, còn việc tự động hóa cả 3 sẽ giúp tăng gấp đôi hiệu quả làm việc của riêng nhân viên ít kinh nghiệm. **Hơn 3/4 chương trình SecOps không có nguồn nhân lực mạnh vẫn có thể đạt được các khả năng mạnh mẽ nhờ có mức độ tự động hóa cao.**

Bây giờ, hãy theo dõi từ điểm ngoài cùng bên phải của đường màu lam đậm đến điểm đầu tiên của đường màu lam nhạt. Bạn có nắm bắt được điều gì không? **Một chương trình SecOps với đội ngũ nhân viên yếu kém có tỷ lệ tự động hóa nâng cao gần bằng với chương trình có đội ngũ nhân viên vững mạnh và khả năng tự động hóa kém.** Hay nói cách khác, tự động hóa mạnh mẽ là yếu tố có thể thay thế cho đội ngũ nhân viên hùng hậu. Hãy xem – điều chúng tôi nói là đúng đắn!

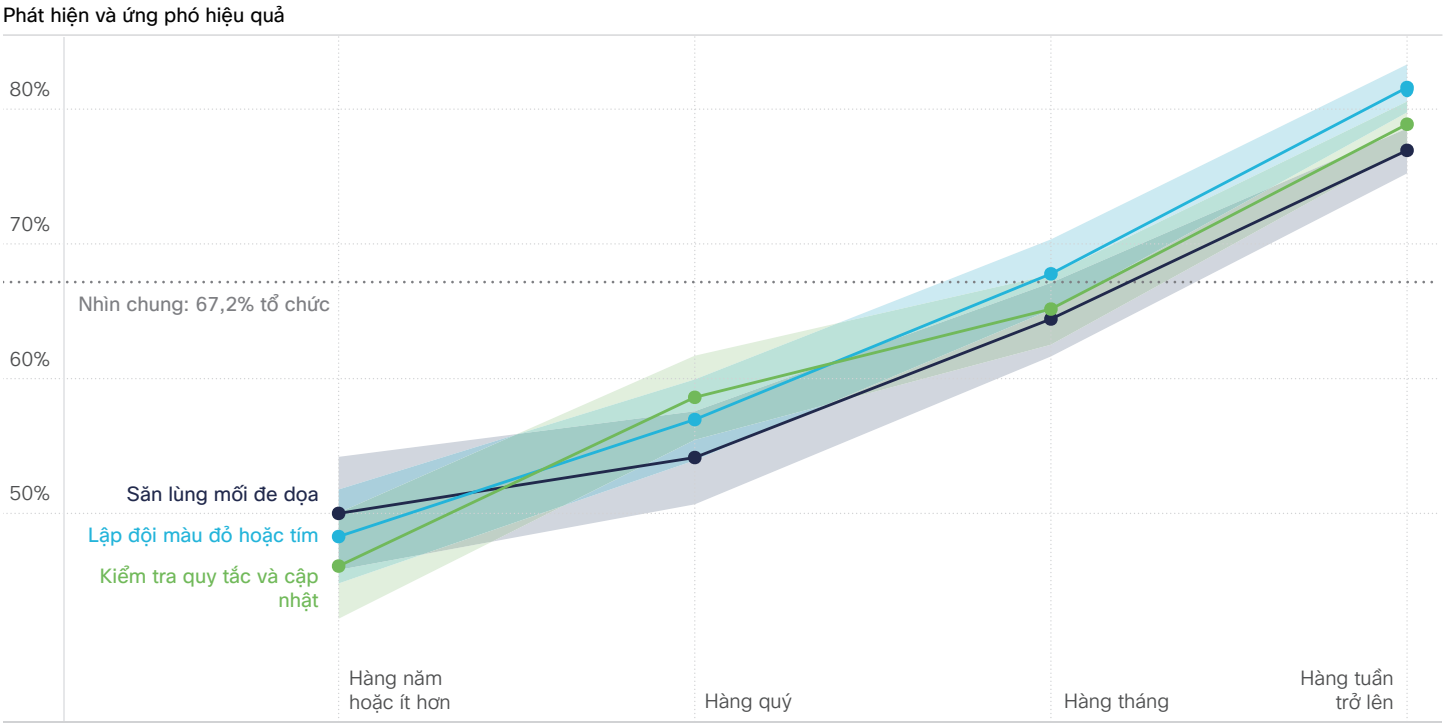
Nhưng con người so với máy móc không thực sự là điểm chính hay bài học quan trọng nhất rút ra từ Hình 18. Khi theo dõi đường màu lam qua các cấp độ tự động hóa liên tiếp, bạn sẽ lý do rất thuyết phục cho việc theo đuổi cả 2 mục tiêu này. Các chương trình bảo mật có sự hợp sức của một đội ngũ vững mạnh VÀ sự tự động hóa các quy trình phát hiện & ứng phó với mối đe dọa lớn gần như đảm bảo (hơn 95%) sẽ đạt được thành công về SecOps. Vì vậy, đừng sử dụng yếu tố tự động hóa để thay thế cho lực lượng lao động tài năng. Hãy sử dụng quy trình tự động hóa để nâng cao tài năng của con người bằng cách cho phép họ tập trung vào các hoạt động có mức độ ưu tiên cao.

Bao lâu chúng ta nên chỉnh sửa, xâm nhập và săn tìm?

Chúng ta có thể tiến hành hoạt động có khả năng cải thiện các chương trình phát hiện và ứng phó với mối đe dọa ở tần suất bất kỳ. Theo một cuộc thăm dò không chính thức mà chúng tôi đã thực hiện về chủ đề đó, sau đây là 3 hoạt động người được đề xuất nhiều nhất:

- Kiểm tra và cập nhật các quy tắc phát hiện và các trường hợp sử dụng
- Chủ động tìm kiếm các dấu hiệu của hoạt động gây hại
- Tham gia các bài tập đội đỏ và/hoặc tím

Chúng tôi đã hỏi những người tham gia về tần suất tổ chức của họ tiến hành từng hoạt động đó, sau đó đối chiếu dữ liệu đó với khả năng phát hiện và ứng phó với mối đe dọa được cho biết. Xu hướng thu được trong Hình 19 đã thể hiện rõ nhất vấn đề.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 19: Ảnh hưởng của tần suất tiến hành hoạt động đến khả năng phát hiện mối đe dọa và ứng phó với sự cố

Điều chỉnh quy tắc, lập đội đỏ/tím và săn lùng mối đe dọa, tất cả đều tuân theo một quỹ đạo tương tự. Càng nhiều việc được hoàn thành, thì càng góp phần cải thiện hiệu quả cho các chương trình SecOps. **Những tổ chức thực hiện các hoạt động này ít nhất hàng tuần sẽ thu được hiệu quả tăng khoảng 30% so với những tổ chức thực hiện hàng năm hoặc ít hơn.** Vậy thì, tổ chức của bạn nên thực hiện các hoạt động đó bao lâu một lần? Câu trả lời đơn giản là "càng thường xuyên càng tốt".

Những tổ chức tiến hành các hoạt động này ít nhất hàng tuần sẽ đạt được mức tăng gần **30%** xét về hiệu quả

“Bảo mật luôn thay đổi và chúng ta cần tuân theo những xu hướng bảo mật này. [Trước đây], chúng tôi đã mất rất nhiều thời gian để giải quyết các vấn đề và sự cố bảo mật. Giờ đây, khi đã đơn giản hóa quy trình và tiết kiệm được thời gian điều tra, chúng tôi có thể tuân theo các xu hướng bảo mật mới và tích hợp các giải pháp bảo mật mới để cung cấp cơ sở hạ tầng an toàn hơn cho mạng giáo dục của mình.”

Bahruz Ibrahimov, Kỹ sư bảo mật thông tin cao cấp, AzEduNet

Đọc thêm

Đảm bảo tính kiên cường và khả năng khôi phục nhanh chóng sau sự cố

Thật thú vị về cách "mối quan tâm hàng đầu" về các khía cạnh khác nhau của an ninh mạng thường xuyên thay đổi theo thời gian. Sau một vài năm tạm lắng xuống để nhường chỗ cho vấn đề vi phạm dữ liệu và gián điệp mạng, chủ đề về tính liên tục của hoạt động kinh doanh và khả năng khôi phục sau sự cố (BCDR) lại một lần nữa giữ vị trí trung tâm. Tất nhiên là có lý do chính đáng cho điều đó. Phần mềm tống tiền tràn lan, sự ngừng hoạt động của các nhà cung cấp dịch vụ lưu trữ lớn, v.v. đã buộc chúng ta phải thay đổi đáng kể trong chiến lược đảm bảo khả năng phục hồi khi đối mặt với các mối đe dọa nguy hiểm.

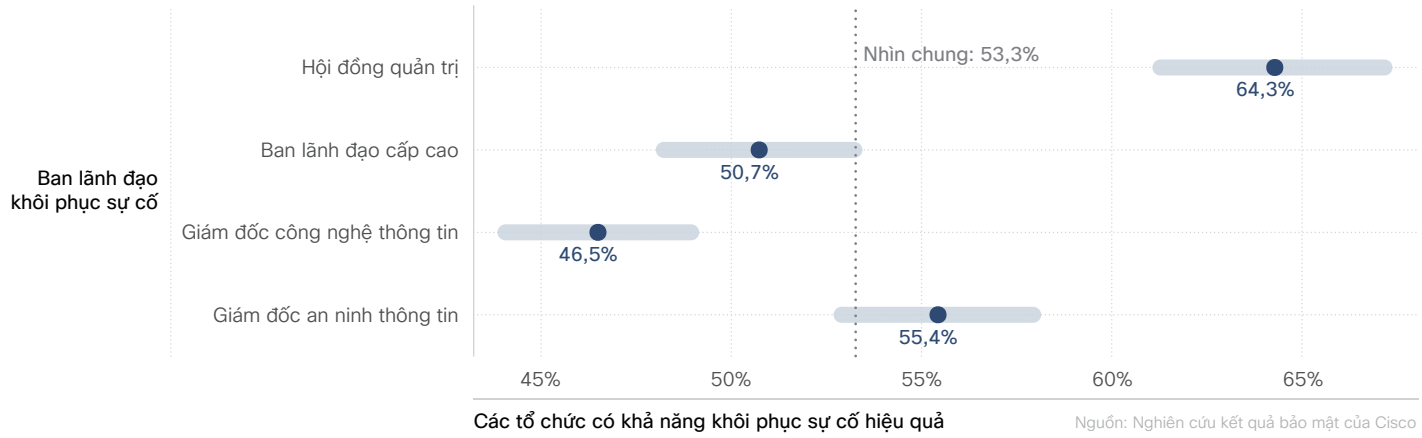
Nghiên cứu kết quả bảo mật năm 2021 đã xếp hạng khả năng khôi phục nhanh chóng sau sự cố là yếu tố quan trọng thứ 4 đối với việc xây dựng chương trình an ninh mạng thành công. Yếu tố này cho thấy mối tương quan đáng kể với toàn bộ 11 kết quả ngoại trừ khía cạnh văn hóa bảo mật. Theo đó, chúng ta hãy xem xét các chiến lược để tối đa hóa hiệu quả cho phương pháp này và đảm bảo khả năng phục hồi.

Phần mềm tống tiền tràn lan, sự ngừng hoạt động của các nhà cung cấp dịch vụ lưu trữ lớn, v.v. đã buộc chúng ta phải thay đổi đáng kể trong chiến lược đảm bảo khả năng phục hồi khi đối mặt với các mối đe dọa nguy hiểm.

Có nên đặt khả năng khôi phục sau sự cố dưới sự giám sát của hội đồng quản trị không?

Chúng tôi rất tò mò muốn biết ai là người có khả năng giám sát cuối cùng về khả năng khôi phục sau sự cố. Quyền hạn này được chia đều cho Giám đốc công nghệ thông tin, Giám đốc an ninh thông tin và các thành viên khác không am hiểu về CNTT trong Ban lãnh đạo cấp cao, với khoảng 1/4 quy trình BCDR của tổ chức được báo cáo cho từng vị trí. Khả năng nắm bắt của hội đồng quản trị ít phổ biến hơn một chút so với các vị trí trên, nhưng vẫn xuất hiện ở 18% tổ chức tham gia cuộc khảo sát của chúng tôi.

Khi chúng tôi so sánh những câu trả lời này với đánh giá của mỗi người tham gia về tính liên tục của hoạt động kinh doanh và khả năng khắc phục sau sự cố, rõ ràng câu hỏi về quyền giám sát không chỉ là sự tò mò. **Theo Hình 20, những tổ chức có sự giám sát của hội đồng quản trị về BCDR sẽ có nhiều khả năng (trên mức trung bình 11%) đạt được các chương trình hiệu quả nhất.** Xét về chức năng tính liên tục của hoạt động kinh doanh và khả năng khắc phục sau sự cố, đầu tiên là CIO với tỷ lệ thấp nhất, thấp hơn đáng kể so với mức trung bình.



Hình 20: Ảnh hưởng của việc giám sát có tổ chức ở cấp cao nhất đối với khả năng khôi phục sau sự cố

Có nhiều cách giải thích hợp lý cho kết quả trong Hình 20. Chúng tôi nghi ngờ rằng tổ chức báo cáo lên hội đồng về các vấn đề khôi phục sau sự cố có thể đã làm gia tăng mối quan ngại về rủi ro hoạt động và khả năng phục hồi. Từ đó, ban lãnh đạo sẽ giám sát chặt chẽ hơn, hỗ trợ tích cực hơn và chi ngân sách lớn hơn. Vì vậy, nếu tổ chức của bạn đang gặp khó khăn trong việc cải thiện khả năng khôi phục sau sự cố, thì việc tiếp cận theo hướng từ trên xuống thay vì từ dưới lên có thể cách hợp lý.

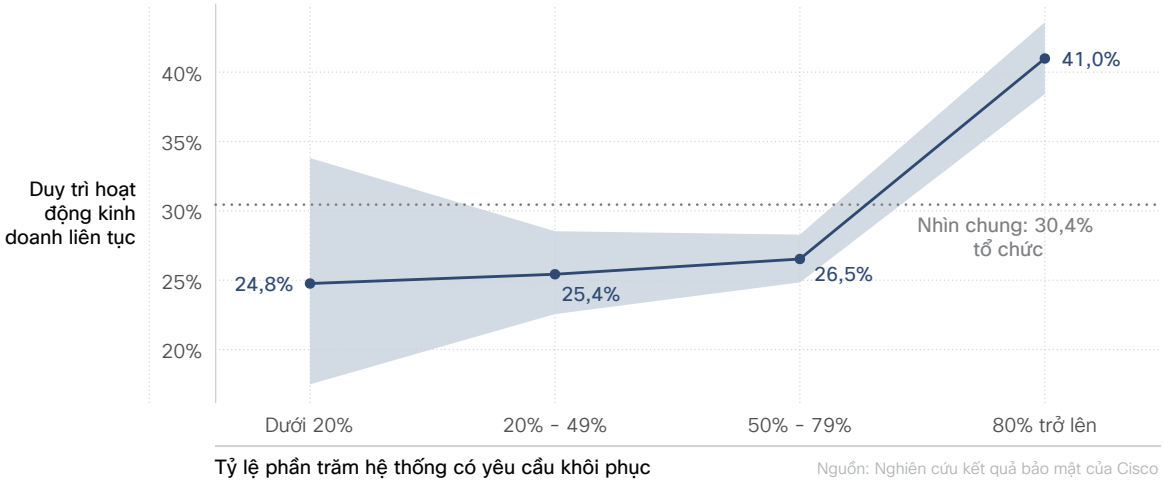
Còn về hoạt động khôi phục sau sự cố hàng ngày thì sao?

Ngoài quyền giám sát cuối cùng, chúng tôi cũng hỏi ai là người chịu trách nhiệm điều hành các khía cạnh mang tính chiến thuật hơn của việc khôi phục sau sự cố. **Các hoạt động của đội ngũ an ninh mạng hoặc chuyên đảm bảo tính liên tục của hoạt động kinh doanh thường đạt được hiệu quả cao nhất.** Các chương trình do đội ngũ CNTT điều hành thường có hiệu quả thấp hơn. Điều thú vị là khả năng nắm bắt của ban lãnh đạo chẳng khác nào cơn thủy triều nổi có thể nâng tất cả các con thuyền lên. Tỷ lệ thành công là ngang nhau về mặt thống kê, bất kể trách nhiệm hàng ngày nằm ở đâu miễn là có sự giám sát cuối cùng của ban lãnh đạo.

Phạm vi khôi phục sau sự cố có quan trọng không?

Có lẽ bạn sẽ không ngạc nhiên khi biết rằng sự cố không chỉ xảy ra ở địa điểm và vào thời gian mà bạn đã biết trước. Các sự cố an ninh mạng cũng không ngoại lệ, đó là lý do tại sao ở phương diện này, bạn nên chuẩn bị cho mọi tình huống xảy ra một cách tốt nhất có thể. Tất nhiên, nói thì dễ hơn làm.

Nhận thức được vấn đề đó, chưa đến 3 trong số 10 tổ chức nói rằng họ triển khai chức năng khôi phục sau sự cố cho ít nhất 80% số hệ thống quan trọng. Một nửa số tổ chức có tỷ lệ triển khai là 50% - 79%, và xấp xỉ 20% thừa nhận tỷ lệ triển khai thấp hơn mức đó. Thoạt nhìn, điều đó có vẻ không quá tệ. Nhìn chung, hầu hết các tổ chức đều triển khai cho phần lớn các hệ thống quan trọng của họ. Tiếc rằng, họ lại bỏ qua thực tế rằng sự cố thường xảy ra ở những nơi không ngờ đến. Dữ liệu của chúng tôi cho thấy rằng điều này xảy ra thường xuyên hơn dự đoán của chúng tôi.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 21: Ảnh hưởng của phạm vi triển khai cho tài sản quan trọng đối với khả năng phục hồi sau sự cố

Hình 21 đo lường một kết quả mới được bổ sung cho nghiên cứu này nhằm đánh giá khả năng của tổ chức trong việc duy trì tính liên tục của hoạt động kinh doanh thông qua các sự kiện gây gián đoạn. Nghiên cứu chỉ ra rằng đó là một trong 3 kết quả mà người trả lời cho biết họ gặp nhiều khó khăn nhất Điều đó làm cho việc tìm ra những cách hiệu quả để cải thiện khả năng thành công càng trở nên quan trọng hơn.

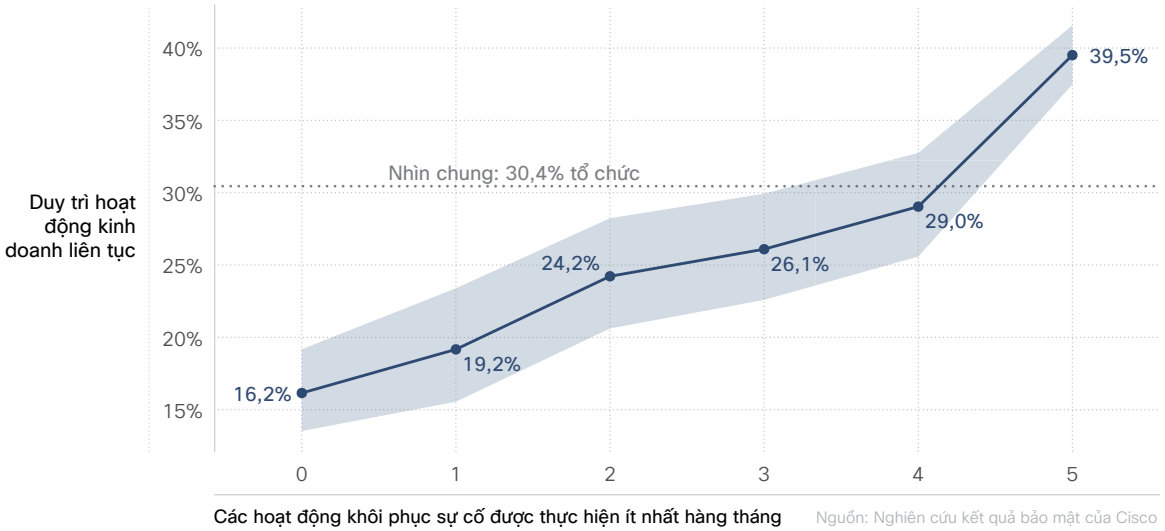
Hình 21 thể hiện một thông điệp quan trọng về việc duy trì tính liên tục của hoạt động kinh doanh. **Cụ thể, hầu như không có sự cải thiện nào về xác suất đạt được kết quả này cho đến khi có khả năng BCDR với ít nhất 80% số hệ thống quan trọng.**

Điều này gần như chắc chắn chỉ ra xu hướng kỳ lạ của sự cố, đó là chúng tấn công ở nơi mà chúng ta chưa chuẩn bị sẵn sàng. Bài học rút ra là chúng ta không thể mong đợi các khoản đầu tư để duy trì hoạt động kinh doanh liên tục và khôi phục sau sự cố sẽ mang lại kết quả tức thì hoặc tương đương. Đó có thể không phải là một thông điệp vui, nhưng sự thật thì sự cố có bao giờ là chuyện vui đâu.

Thực hành có giúp khôi phục sau sự cố một cách hoàn hảo không?

Chúng tôi sẽ giải thích về câu hỏi này và trước tiên sẽ đưa ra câu trả lời. Câu trả lời là Không, rất tiếc là không. Nhưng thực hành vẫn tốt hơn nhiều so với việc không làm gì cả. Tốt hơn thế nào? Hãy đọc tiếp...

Một câu ngạn ngữ nổi tiếng trong ngành quân sự là "Biết người biết ta, trăm trận trăm thắng". Câu nói này khá đúng với chiến trường mạng và có nhiều cách để thử khả năng BCDR, bao gồm hướng dẫn kế hoạch, diễn tập trong phòng họp, thử nghiệm trực tiếp, thử nghiệm song song và thử nghiệm sản xuất đầy đủ. Chúng tôi đã hỏi những người tham gia về tần suất tổ chức của họ tham gia vào các bài diễn tập như vậy, rồi so sánh tần suất đó với khả năng họ duy trì hoạt động kinh doanh liên tục.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 22: Ảnh hưởng của các bài diễn tập thử nghiệm đến khả năng khắc phục sự cố

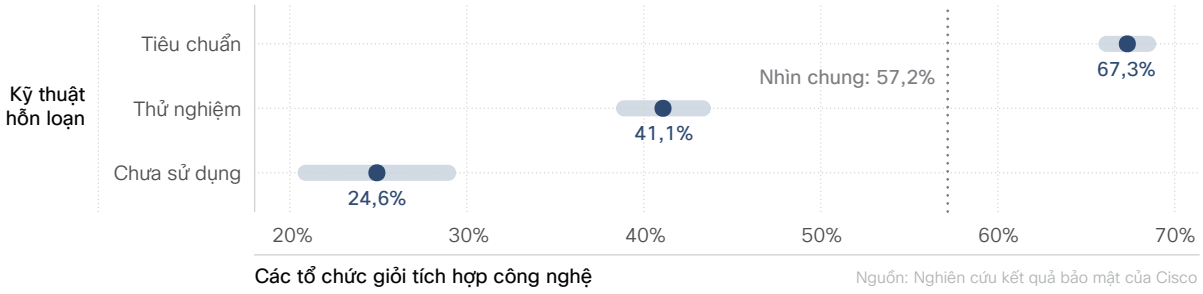
Không có bài thực hành nào trong số này là vượt trội nhất về hiệu quả, nhưng tất cả chúng đều góp phần chung vào việc cải thiện khả năng phục hồi. **Xét về khả năng duy trì thành công sự liên tục của hoạt động kinh doanh, những tổ chức thường xuyên tiến hành toàn bộ 5 loại hình thử nghiệm khôi phục sau sự cố sẽ có nhiều khả năng hơn gần 2,5 lần so với những tổ chức không thực hiện.** Điểm mấu chốt là gì? Đừng phó mặc số mệnh. Hãy thử nghiệm sức chịu đựng xét về khả năng duy trì sự liên tục của hoạt động kinh doanh và khả năng khôi phục sau sự cố một cách thường xuyên từ nhiều góc độ.

Những tổ chức thường xuyên tiến hành toàn bộ 5 loại hình thử nghiệm khôi phục sau sự cố sẽ có nhiều khả năng hơn **2,5 lần** trong việc duy trì thành công sự liên tục của hoạt động kinh doanh

Chúng ta có nên áp dụng kỹ thuật hỗn loạn không?

Về chủ đề thử nghiệm sức chịu đựng trong kế hoạch khôi phục sau sự cố, hãy tối đa hóa "sự căng thẳng". Chúng ta đang nói về kỹ thuật hỗn loạn, theo đó các hệ thống bị gián đoạn định kỳ (có chủ ý) để kiểm tra khả năng chịu đựng với các điều kiện và sự kiện không mong muốn. Việc tạo ra tình huống sự cố cho hệ thống CNTT và bảo mật có thể giúp tổ chức của bạn thêm kiên cường không? Bạn đã đến đúng nơi rồi.

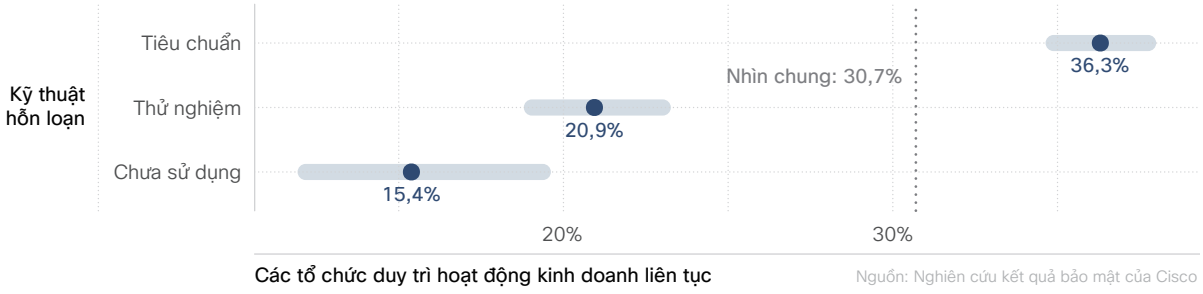
Chúng tôi đã hỏi những người tham gia về mức độ mà tổ chức của họ tham gia vào kỹ thuật hỗn loạn và nhận thấy điều này phổ biến hơn chúng tôi nghĩ. Đáng chú ý, chúng tôi nhận thấy mối quan hệ giữa giải pháp này và việc tích hợp công nghệ. Theo Hình 23, hơn 2/3 số tổ chức xem kỹ thuật hỗn loạn là giải pháp tiêu chuẩn có sử dụng công nghệ tích hợp cao để hỗ trợ cho khả năng phục hồi của họ. Vẫn chưa rõ tích hợp là việc bắt buộc hay hỗ trợ cho kỹ thuật hỗn loạn. Cũng như rất nhiều vấn đề trong lĩnh vực này, có lẽ câu trả lời sẽ là cả 2. Hãy theo dõi kỷ luật mới nổi này – đặc biệt nếu bạn chịu trách nhiệm về BCDR trong một môi trường CNTT phức tạp và có tính tích hợp cao.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 23: Mối quan hệ giữa kỹ thuật hỗn loạn và mức độ tích hợp CNTT

Sự so sánh mức độ của kỹ thuật hỗn loạn với kết quả duy trì khả năng phục hồi kinh doanh trong Hình 24 đưa ra lý do thuyết phục rằng nên áp dụng kỹ thuật hỗn loạn cho mạng lưới của bạn. **Những tổ chức xem kỹ thuật hỗn loạn là giải pháp tiêu chuẩn sẽ có khả năng đạt được thành công vang dội ở khía cạnh này cao hơn gấp 2 lần so với những tổ chức không áp dụng kỹ thuật hỗn loạn.** Thật dễ hiểu nếu bạn bất ngờ về kết quả này. Tin tốt là để không bất ngờ, bạn hãy áp dụng kỹ thuật hỗn loạn để gặt hái kết quả cho chính mình nhé.



Nguồn: Nghiên cứu kết quả bảo mật của Cisco

Hình 24: Ảnh hưởng của kỹ thuật hỗn loạn đối với việc duy trì khả năng phục hồi kinh doanh

Kết luận và đề xuất

Chúng tôi đã bắt đầu áp dụng các biện pháp bảo mật được xác định là có hiệu quả cao trong một nghiên cứu trước đó, thu thập thêm thông tin qua một cuộc khảo sát mới để biết điều gì làm cho các giải pháp đó hiệu quả nhất và chia sẻ những bài học đó với bạn. Chúng tôi hy vọng rằng thông qua báo cáo này, bạn sẽ chia sẻ một số bí quyết thiết thực về cách triển khai chương trình an ninh mạng thành công hơn.

Ngoài ra, bạn cũng nên tham khảo các kết quả của nghiên cứu này và đúc kết của những người khác từ kết quả đó. Chúng tôi đã yêu cầu đội ngũ Cố vấn CISO giàu kinh nghiệm của mình xem xét từng phương diện biện pháp đã nghiên cứu. Dưới đây là các đề xuất hàng đầu của họ. Bạn có thể tìm xem thông tin chi tiết và bài học trong loạt blog Nghiên cứu kết quả bảo mật của chúng tôi.

Chủ động làm mới công nghệ

"Tình trạng tích lũy lỗ hổng bảo mật rất nghiêm trọng. Đối với CISO, kế hoạch trong tương lai là phát triển chiến lược "Mua, Giữ, Bán". Nhận ra những gì bạn có, xác định kiến trúc có thể thích ứng, giảm rủi ro phụ thuộc và triển khai vòng xem xét cho các chu kỳ làm mới trong tương lai."

Richard Archdeacon, Giám đốc tư vấn an toàn thông tin, Cisco

Tích hợp công nghệ hiệu quả

"Chúng tôi biết CNTT hiện đại, được tích hợp tốt góp phần vào thành công chung của chương trình bảo mật, vì vậy, đây là một số hành động bạn có thể thực hiện để cải thiện môi trường của mình: Tìm kiếm các giải pháp bảo mật dựa trên đám mây, tìm hiểu các cơ hội tự động hóa, đảm bảo các yêu cầu mua hàng bao gồm khả năng tích hợp công nghệ".

Helen Patton, Giám đốc tư vấn an toàn thông tin, Cisco @CisoHelen

Ứng phó kịp thời với sự cố

"Đội ngũ nhân viên hùng hậu mang lại lợi thế cho các nhóm ứng phó với sự cố. Đây là một điểm khởi đầu tốt nhưng cần được thực hiện kết hợp với các yếu tố khác. Khi doanh nghiệp kết hợp con người, quy trình và công nghệ mạnh mẽ, họ sẽ đạt được khả năng tiên tiến trong việc phát hiện và ứng phó với mối đe dọa".

Dave Lewis, Giám đốc tư vấn an toàn thông tin, Cisco @gattaca

Phát hiện đúng mối đe dọa

“Hãy chọn ra những người có chuyên môn cao nhất cho đội ngũ điều hành an toàn thông tin của bạn, chất lượng hơn số lượng. Nếu bạn không thể đạt được trình độ chuyên môn mà mình cần, thì tự động hóa có thể giúp bạn thu hẹp khoảng cách với nhân viên cấp thấp của mình để kết quả đạt được không chênh lệch so với nhân viên cấp cao.”

Wendy Nather, Giám đốc tư vấn an toàn thông tin, Cisco @wendynather

Nhanh chóng khôi phục sau sự cố

“Những phát hiện trong báo cáo này giúp nêu bật giá trị của khả năng duy trì sự liên tục trong hoạt động kinh doanh và khôi phục sau sự cố, nhưng không được tách biệt khả năng này với các chức năng bảo mật khác. Việc ưu tiên và xếp hạng rủi ro các nguồn lực nên được chia sẻ với các chức năng quản lý rủi ro khác. Tương tự, tích hợp chặt chẽ hoạt động quản lý tài sản và quản lý mối đe dọa để đảm bảo tất cả các đội ngũ đều có chung chí hướng.”

Wolfgang Goerlich, Giám đốc tư vấn an toàn thông tin, Cisco @jwgoerlich

Giới thiệu về Cisco Secure

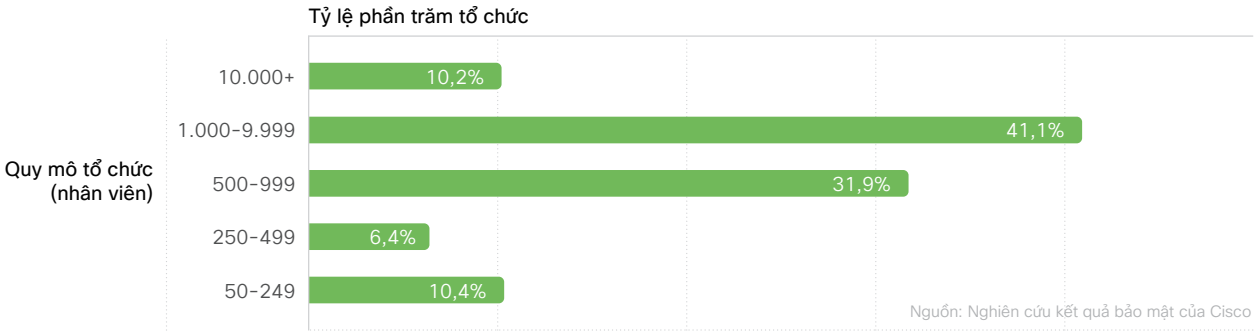
Cisco từ lâu đã khẳng định mình là công ty hàng đầu trên toàn thế giới về công nghệ hỗ trợ Internet, đồng thời xây dựng một danh mục tích hợp, mở gồm các giải pháp an ninh mạng. Chúng tôi tin rằng các giải pháp bảo mật nên được thiết kế để hoạt động như một nhóm. Mọi người nên học hỏi lẫn nhau. Họ nên lắng nghe và phản hồi như một đơn vị điều phối. Khi có chuyện, giải pháp bảo mật trở nên hiệu quả và có hệ thống hơn. Chúng tôi đã gây dựng được niềm tin của khách hàng trong nhiều năm qua với tư cách là nhà cung cấp dịch vụ mạng và cơ sở hạ tầng CNTT, cũng như công ty an ninh mạng doanh nghiệp lớn nhất thế giới.

Cisco Secure được xây dựng dựa trên nguyên tắc bảo mật hiệu quả hơn, chứ không phải nhiều hơn. Giải pháp này mang đến cách tiếp cận hợp lý, lấy khách hàng làm trung tâm đối với vấn đề bảo mật, để đảm bảo dễ dàng triển khai, quản lý và sử dụng – tất cả đều hoạt động cùng nhau. Động lực của chúng tôi là lấy mọi người và khách hàng làm trọng tâm trong mọi hành động. Chúng tôi hiểu rằng khách hàng muốn loại bỏ sự phức tạp, ồn ào, đồng thời muốn cảm thấy tin tưởng khả năng bảo mật của họ, tập trung vào kết quả. Điều này đòi hỏi sự đơn giản hóa mà không phải là đơn giản thái quá. Nền tảng gốc đám mây của chúng tôi là một bước tiến vượt bậc về điều đó.

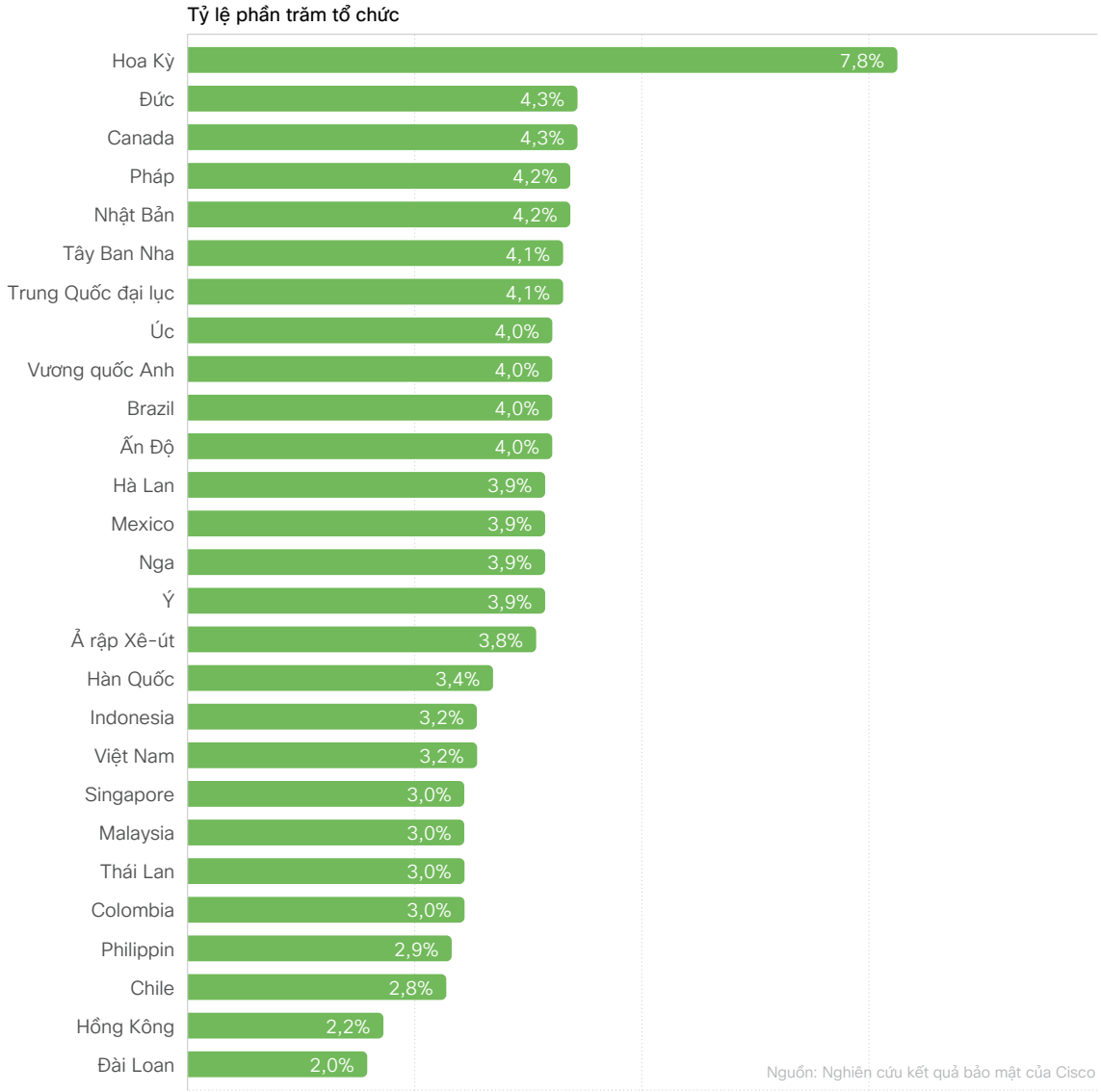
Chúng tôi mang đến cho cộng đồng bảo mật sự tin cậy và đảm bảo rằng họ an toàn trước các mối đe dọa ở hiện tại và trong tương lai nhờ có nền tảng Cisco SecureX. Chúng tôi giúp 100% công ty trong danh sách Fortune 100 đảm bảo an toàn cho công việc – bất kể nơi đâu xảy ra sự cố – nhờ nền tảng tích hợp, rộng nhất. Tìm hiểu thêm về cách chúng tôi đơn giản hóa trải nghiệm, tăng tốc để đạt được thành công và bảo vệ tương lai trên trang cisco.com/go/secure.

Phụ lục: Khảo sát theo mẫu thông tin nhân khẩu học

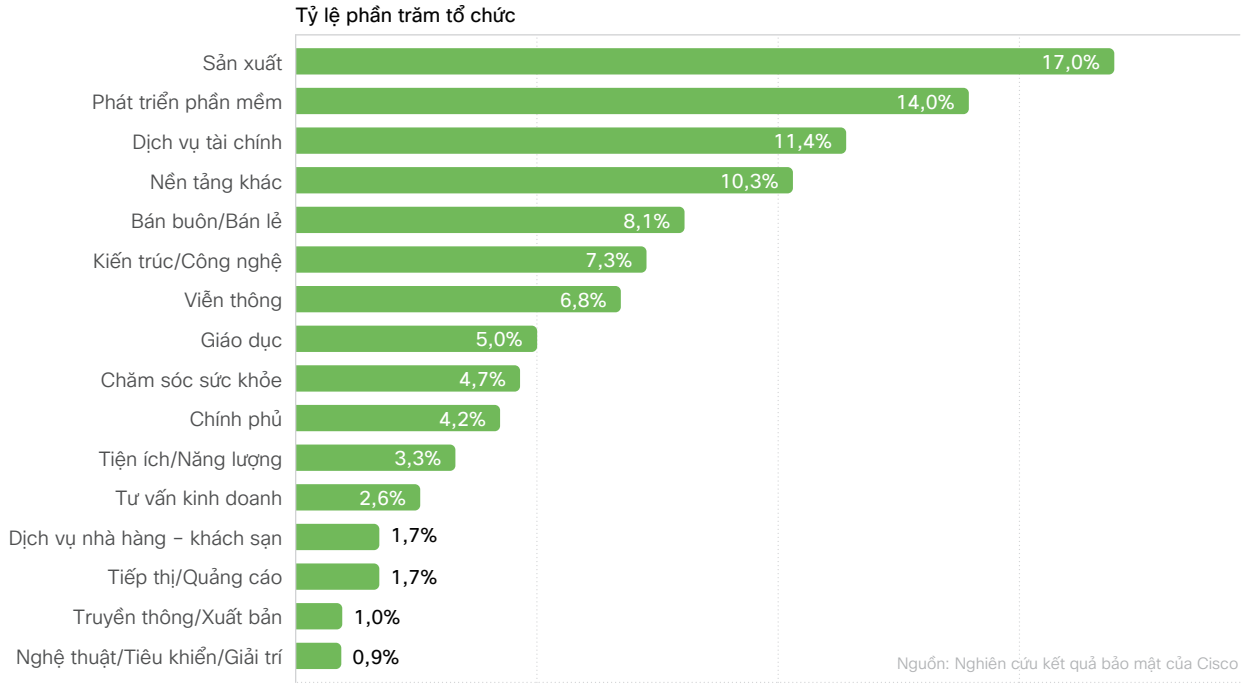
Trong phụ lục này, chúng tôi đã đưa ra thông tin nhân khẩu học mẫu từ 5.123 người tham gia đủ điều kiện cho cuộc khảo sát này. Chúng tôi hy vọng điều này sẽ giúp những người đang cố gắng phân biệt tính tiêu biểu của những phát hiện này.



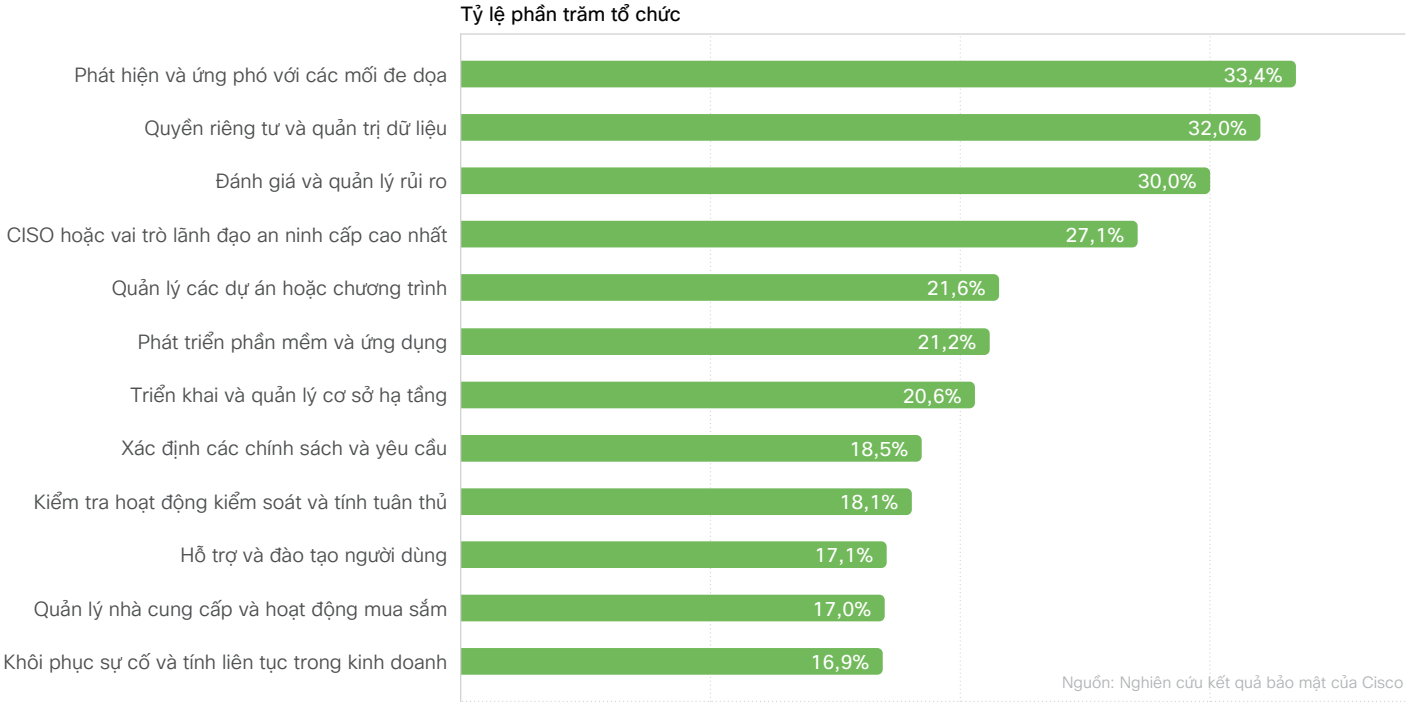
Hình A1: Số lượng nhân viên của các tổ chức tham gia



Hình A2: Các thị trường đặt trụ sở chính của các tổ chức tham gia



Hình A3: Những ngành đại diện theo các tổ chức tham gia



Hình A4: Trách nhiệm công việc chính của những người tham gia

CISCO
SECURE

Trụ sở tại Châu Mỹ
Cisco Systems, Inc.
San Jose, CA

Trụ sở tại Châu Á Thái Bình Dương
Cisco Systems (USA), Pte. Ltd.
Singapore

Trụ sở chính tại Châu Âu
Cisco Systems International BV
Amsterdam, Hà Lan

Published December 2021