|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA AN TOÀN THÔNG TIN**  Logo HvKTMM  BÁO CÁO MÔN HỌC  **QUẢN LÝ AN TOÀN THÔNG TIN**  **Đề tài:**  **Tìm hiểu công cụ để tự động đánh giá rủi ro**  *Sinh viên thực hiện:*  **Bàn Văn Cường** - AT160210  **Vũ Hồng Phúc** - AT160245  **Nguyễn Thế Phong** - AT160244  **Nguyễn Minh Đức** - AT160218  *Giảng viên hướng dẫn:*  **ThS. Trần Thị Thanh Liêm**  Khoa An toàn Thông tin – Học viện Kỹ thuật Mật mã  Hà Nội, 02-2023 |

**MỤC LỤC**

[DANH MỤC HÌNH VẼ iv](#_Toc128606884)

[CHƯƠNG 1. KHÁI QUÁT VỀ CÁC CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO 1](#_Toc128606885)

[1.1 Tổng quan công cụ đánh giá rủi ro 1](#_Toc128606886)

[1.1.1 Khái niệm công cụ tự động đánh giá rủi ro 1](#_Toc128606887)

[1.1.2 Một số loại rủi ro an toàn thông tin 1](#_Toc128606888)

[1.1.3 Nguyên nhân rủi ro an toàn thông tin 2](#_Toc128606889)

[1.2 Các bước đánh giá rủi ro 3](#_Toc128606890)

[1.2.1 Xác định các rủi ro 3](#_Toc128606891)

[1.2.2 Đánh giá rủi ro 4](#_Toc128606892)

[1.2.3 Phân tích rủi ro 4](#_Toc128606893)

[1.2.4 Giảm thiểu rủi ro 5](#_Toc128606894)

[1.2.5 Đánh giá lại rủi ro lần nữa 6](#_Toc128606895)

[1.3 Thực trạng rủi ro ở các doanh nghiệp 8](#_Toc128606896)

[1.3.1 Thực trạng ở các doanh nghiệp 8](#_Toc128606897)

[1.3.2 Ưu nhược điểm của công cụ tự động đánh giá rủi ro 9](#_Toc128606898)

[1.4 Biện pháp kiểm soát rủi ro 10](#_Toc128606899)

[1.4.1 Hướng dẫn chung 10](#_Toc128606900)

[1.4.2 Biện pháp kiểm soát về quản lý 12](#_Toc128606901)

[1.4.3 Biện pháp kiểm soát về kỹ thuật 15](#_Toc128606902)

[CHƯƠNG 2. MỘT SỐ CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO 19](#_Toc128606903)

[2.1 RSA Archer (Nền tảng GRC) 19](#_Toc128606904)

[2.1.1 Chi tiết 19](#_Toc128606905)

[2.1.2 Tính năng 19](#_Toc128606906)

[2.1.3 Ưu điểm 21](#_Toc128606907)

[2.1.4 Nhược điểm 21](#_Toc128606908)

[2.2 Qualys (Công cụ quét lỗ hổng) 22](#_Toc128606909)

[2.2.1 Chi tiết 22](#_Toc128606910)

[2.2.2 Tính năng 22](#_Toc128606911)

[2.2.3 Ưu điểm 25](#_Toc128606912)

[2.2.4 Nhược điểm 26](#_Toc128606913)

[2.3 Metasploit (Công cụ kiểm tra thâm nhập) 26](#_Toc128606914)

[2.3.1 Chi tiết 26](#_Toc128606915)

[2.3.2 Tính năng 28](#_Toc128606916)

[2.3.3 Ưu điểm 29](#_Toc128606917)

[2.3.4 Nhược điểm 29](#_Toc128606918)

[2.4 ThreatConnect (Nền tảng tình báo mối đe dọa) 30](#_Toc128606919)

[2.4.1 Chi tiết 30](#_Toc128606920)

[2.4.2 Tính năng 30](#_Toc128606921)

[2.4.3 Ưu điểm 31](#_Toc128606922)

[2.4.4 Nhược điểm 31](#_Toc128606923)

[2.5 Splunk (Hệ thống quản lý sự kiện và thông tin bảo mật (SIEM)) 32](#_Toc128606924)

[2.5.1 Chi tiết 32](#_Toc128606925)

[2.5.2 Tính năng 33](#_Toc128606926)

[2.5.3 Ưu điểm 35](#_Toc128606927)

[2.5.4 Nhược điểm 35](#_Toc128606928)

[2.6 Symantec DLP (Giải pháp ngăn ngừa mất dữ liệu (DLP)) 36](#_Toc128606929)

[2.6.1 Chi tiết 36](#_Toc128606930)

[2.6.2 Tính năng 37](#_Toc128606931)

[2.6.3 Ưu điểm 37](#_Toc128606932)

[2.6.4 Nhược điểm 38](#_Toc128606933)

[2.7 Microsoft Defender ATP (Công cụ đánh giá trạng thái bảo mật) 38](#_Toc128606934)

[2.7.1 Chi tiết 38](#_Toc128606935)

[2.7.2 Tính năng 39](#_Toc128606936)

[2.7.3 Ưu điểm 40](#_Toc128606937)

[2.7.4 Nhược điểm 40](#_Toc128606938)

[2.8 Checkmarx (Công cụ kiểm tra bảo mật ứng dụng) 41](#_Toc128606939)

[2.8.1 Chi tiết 41](#_Toc128606940)

[2.8.2 Tính năng 41](#_Toc128606941)

[2.8.3 Ưu điểm 41](#_Toc128606942)

[2.8.4 Nhược điểm 42](#_Toc128606943)

[2.9 Prisma Cloud (Giải pháp quản lý tư thế bảo mật đám mây (CSPM)) 42](#_Toc128606944)

[2.9.1 Chi tiết 42](#_Toc128606945)

[2.9.2 Tính năng 43](#_Toc128606946)

[2.9.3 Ưu điểm 44](#_Toc128606947)

[2.9.4 Nhược điểm 44](#_Toc128606948)

[2.10 Okta (Giải pháp quản lý truy cập và nhận dạng (IAM)) 44](#_Toc128606949)

[2.10.1 Chi tiết 44](#_Toc128606950)

[2.10.2 Tính năng 45](#_Toc128606951)

[2.10.3 Ưu điểm 46](#_Toc128606952)

[2.10.4 Nhược điểm 46](#_Toc128606953)

[KẾT LUẬN 47](#_Toc128606954)

# DANH MỤC HÌNH VẼ

|  |  |
| --- | --- |
| Hình 1 | Giao diện Archer |
| Hình 2 | Tính năng quản lý rủi ro của Archer |
| Hình 3 | Tính năng quản lý kiểm toán của Archer |
| Hình 4 | Giao diện Qualys |
| Hình 5 | Tính năng quản lý lỗ hổng của Qualys |
| Hình 6 | Tính năng quản lý tuân thủ của Qualys |
| Hình 7 | .Tính năng quản lý tài sản của Qualys |
| Hình 8 | Tính năng đánh giá bảo mật của Qualys |
| Hình 9 | Metasploit phiên bản câu lệnh |
| Hình 10 | Metasploit phiên bản Pro |
| Hình 11 | Kiểm tra thâm nhập bằng Metasploit dòng lệnh |
| Hình 12 | Đánh giá lỗ hổng sử dụng Metasploit Pro |
| Hình 13 | Giao diện ThreatConnect |
| Hình 14 | Giao diện Spunk |
| Hình 15 | Tính năng quản lý và phân tích nhật ký của Splunk |
| Hình 16 | Tính năng trực quan hoá dữ liệu máy của Splunk |
| Hình 17 | Tính năng cảnh báo và giám sát của Slunk |
| Hình 18 | Tổng quan chính sách |
| Hình 19 | Tích hợp Symantec DLP với Microsoft Information Protection |
| Hình 20 | Microsoft Defender for Endpoint |
| Hình 21 | Giao diện Prisma Cloud |
| Hình 22 | Ứng dụng dành cho Okta SWA |

# KHÁI QUÁT VỀ CÁC CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO

## Tổng quan công cụ đánh giá rủi ro

### Khái niệm công cụ tự ***động*** đánh giá rủi ro

Công cụ tự động đánh giá rủi ro là một phần mềm hoặc hệ thống tự động hóa được sử dụng để đánh giá, phân loại và ưu tiên các rủi ro trong một doanh nghiệp hoặc tổ chức. Công cụ này giúp cho doanh nghiệp đánh giá và phân tích các rủi ro một cách tự động, nhanh chóng và chính xác hơn so với các phương pháp đánh giá rủi ro thủ công.

Các công cụ đánh giá rủi ro thường tích hợp các thuật toán, phương pháp và tiêu chuẩn quốc tế để đánh giá rủi ro theo các tiêu chí khác nhau. Các công cụ này có thể thực hiện đánh giá rủi ro trong nhiều lĩnh vực khác nhau, bao gồm thông tin, tài chính, bảo mật mạng, an toàn, sức khỏe và môi trường.

Các công cụ đánh giá rủi ro có thể có các tính năng khác nhau, bao gồm tạo và quản lý danh sách rủi ro, cung cấp điều kiện để đánh giá rủi ro, phân loại rủi ro theo mức độ và ưu tiên hóa các rủi ro quan trọng nhất. Công cụ đánh giá rủi ro cũng có thể cung cấp cho người dùng các thông tin liên quan đến các biện pháp phòng ngừa và giảm thiểu rủi ro.

Các công cụ đánh giá rủi ro cũng có thể kết hợp với các công cụ khác để đảm bảo tính toàn vẹn của dữ liệu, bảo mật thông tin và phân tích dữ liệu một cách chính xác và hiệu quả. Trong tổng thể, công cụ đánh giá rủi ro là một phần quan trọng của việc quản lý rủi ro trong một doanh nghiệp hoặc tổ chức.

### Một số loại rủi ro an toàn thông tin

Tấn công từ bên ngoài: Đây là một trong những rủi ro an toàn thông tin phổ biến nhất, khi kẻ tấn công cố gắng truy cập vào hệ thống hoặc dữ liệu của một tổ chức bằng cách sử dụng các kỹ thuật tấn công mạng.

Mất dữ liệu: Rủi ro này có thể xảy ra do lỗi kỹ thuật, thiết bị hỏng hoặc thất thoát dữ liệu. Khi dữ liệu quan trọng của doanh nghiệp bị mất, nó có thể dẫn đến mất cơ hội kinh doanh, mất tiền bạc và mất uy tín.

Mất thông tin cá nhân: Rủi ro này xảy ra khi thông tin cá nhân của khách hàng hoặc nhân viên bị rò rỉ hoặc bị đánh cắp. Điều này có thể dẫn đến hậu quả nghiêm trọng như việc phá vỡ sự riêng tư và bị tội phạm sử dụng thông tin cá nhân để gian lận hoặc tấn công.

Sự cố hệ thống: Rủi ro này có thể xảy ra khi hệ thống máy tính hoặc các ứng dụng của doanh nghiệp bị gián đoạn, dẫn đến mất kết nối và gián đoạn các hoạt động kinh doanh.

Rủi ro từ bên trong: Rủi ro này xảy ra khi nhân viên, cộng tác viên hoặc nhà cung cấp đối tác gây ra thiệt hại cho doanh nghiệp bằng cách lợi dụng thông tin quan trọng hoặc vi phạm các chính sách bảo mật của doanh nghiệp.

Sự thiếu hiểu biết về an toàn thông tin: Rủi ro này xảy ra khi các nhân viên hoặc người dùng cuối không hiểu rõ về an toàn thông tin và không tuân thủ các quy định và chính sách của doanh nghiệp, dẫn đến tình trạng dễ bị tấn công hoặc lỗ hổng an ninh.

### Nguyên nhân rủi ro an toàn thông tin

Sự thiếu thông tin và giáo dục an toàn thông tin: Đây là nguyên nhân phổ biến nhất. Nhiều người không nhận thức được tầm quan trọng của việc bảo vệ thông tin và cách để bảo vệ chúng. Do đó, họ dễ dàng bị lừa đảo, tấn công hoặc để lộ thông tin quan trọng.

Phần mềm độc hại: Sự phát triển của phần mềm độc hại là một nguyên nhân rủi ro lớn cho an toàn thông tin. Phần mềm độc hại bao gồm virus, spyware, trojan và malware có thể tấn công hệ thống của bạn, lấy cắp thông tin cá nhân hoặc tiêm vào mã độc để làm hỏng hệ thống.

Sự thiếu bảo mật của thiết bị: Thiết bị của bạn có thể bị tấn công nếu chúng không được bảo mật đầy đủ. Mật khẩu yếu hoặc không có mật khẩu, thiết lập mạng không đúng cách, hoặc cập nhật phần mềm không đầy đủ đều làm cho thiết bị của bạn trở nên dễ bị tấn công.

Tấn công từ bên ngoài: Bên ngoài nhà mạng của bạn, hacker, tội phạm mạng hoặc chính phủ có thể tấn công vào hệ thống của bạn để đánh cắp thông tin hoặc tạo ra những vấn đề an ninh.

Sự thiếu nhạy cảm với vấn đề an toàn thông tin: Nhiều tổ chức không chấp nhận vấn đề an toàn thông tin là một vấn đề quan trọng và không đầu tư đủ nguồn lực để giải quyết nó. Điều này làm cho họ trở nên dễ bị tấn công hoặc để lộ thông tin quan trọng.

## Các bước đánh giá rủi ro

### Xác định các rủi ro

Các rủi ro an toàn thông tin là các tình huống có thể gây tổn hại hoặc mất mát đối với thông tin quan trọng, bao gồm các thông tin như thông tin cá nhân, dữ liệu doanh nghiệp, tài sản trí tuệ, v.v. Dưới đây là một số ví dụ về các rủi ro an toàn thông tin:

* *Tấn công mạng*: Các tấn công mạng bao gồm các phương thức tấn công như tấn công từ chối dịch vụ (DDoS), phishing, malware, virus, rootkit, v.v. Tấn công mạng có thể gây mất mát dữ liệu, tiền bạc, tài sản trí tuệ hoặc ảnh hưởng đến hoạt động kinh doanh của một tổ chức.
* *Đánh cắp thông tin cá nhân*: Đánh cắp thông tin cá nhân là một rủi ro an toàn thông tin phổ biến. Khi thông tin cá nhân của người dùng bị đánh cắp, tin tặc có thể sử dụng các thông tin này để thực hiện các hành động giả mạo hoặc lừa đảo.
* *Lỗ hổng bảo mật*: Lỗ hổng bảo mật là những điểm yếu trong hệ thống bảo mật của một tổ chức, mà tin tặc có thể khai thác để truy cập vào dữ liệu và thông tin quan trọng. Lỗ hổng bảo mật có thể do phần mềm không được cập nhật, mật khẩu yếu, cấu hình sai, v.v.
* *Thiếu nhân viên được đào tạo về an toàn thông tin*: Nếu nhân viên của một tổ chức không được đào tạo về an toàn thông tin, họ có thể mắc phải các sai sót, không biết phản ứng khi bị tấn công hoặc không hiểu cách sử dụng các công cụ bảo mật.
* *Thất thoát dữ liệu*: Thất thoát dữ liệu xảy ra khi thông tin quan trọng bị mất hoặc bị đánh cắp. Các nguyên nhân của thất thoát dữ liệu bao gồm thiết bị bị mất hoặc đánh cắp, phần mềm lỗi, lỗi người dùng,...

### Đánh giá rủi ro

Đánh giá rủi ro an toàn thông tin là một quá trình đánh giá các rủi ro có thể ảnh hưởng đến an toàn thông tin của một tổ chức hoặc cá nhân. Việc đánh giá rủi ro là quan trọng để xác định các rủi ro, đánh giá mức độ nghiêm trọng và ưu tiên các biện pháp bảo vệ để giảm thiểu các rủi ro đó.

Các bước đánh giá rủi ro an toàn thông tin thường bao gồm:

* *Xác định các tài sản quan trọng*: Đầu tiên, cần xác định các tài sản quan trọng như dữ liệu, hệ thống, ứng dụng, v.v.
* *Xác định các rủi ro*: Dựa trên các tài sản đã xác định, cần xác định các rủi ro tiềm ẩn có thể ảnh hưởng đến các tài sản đó. Các rủi ro bao gồm các mối đe dọa từ bên ngoài, các lỗ hổng bảo mật, các lỗi thiết kế, v.v.
* *Đánh giá mức độ nghiêm trọng của rủi ro*: Các rủi ro được đánh giá về mức độ nghiêm trọng của chúng, bao gồm khả năng xảy ra, mức độ ảnh hưởng và tầm quan trọng của tài sản bị ảnh hưởng.
* *Xác định các biện pháp bảo vệ*: Sau khi đánh giá các rủi ro, cần xác định các biện pháp bảo vệ để giảm thiểu các rủi ro đó. Các biện pháp bảo vệ bao gồm việc cập nhật phần mềm, sử dụng mật khẩu mạnh, sử dụng phần mềm bảo mật, đào tạo nhân viên về an toàn thông tin, v.v.
* *Xác nhận lại lại các rủi ro*: Cuối cùng, cần đánh giá lại các rủi ro và các biện pháp bảo vệ đã thực hiện để đảm bảo hiệu quả của chúng và cập nhật lại các biện pháp bảo vệ nếu cần thiết.

Việc đánh giá rủi ro an toàn thông tin là một phần quan trọng của việc bảo vệ an toàn thông tin. Nó giúp các tổ chức xác định các rủi ro và ưu tiên các biện pháp bảo vệ để giảm thiểu các rủi ro đó.

### Phân tích rủi ro

Phân tích rủi ro bảo mật thông tin là quá trình xác định, đánh giá và ưu tiên các rủi ro và mối đe dọa tiềm tàng đối với tính bảo mật, tính toàn vẹn và tính khả dụng của hệ thống thông tin và thông tin của tổ chức. Mục tiêu của phân tích rủi ro bảo mật thông tin là xác định và ưu tiên các rủi ro quan trọng nhất và thực hiện các bước để giảm thiểu hoặc quản lý chúng. Các bước liên quan đến phân tích rủi ro bảo mật thông tin bao gồm:

* *Nhận dạng tài sản*: Xác định các hệ thống thông tin và thông tin quan trọng đối với tổ chức. Xác định mối đe dọa: Xác định các mối đe dọa tiềm năng đối với hệ thống thông tin và thông tin của tổ chức. Các mối đe dọa có thể đến từ các nguồn bên trong và bên ngoài.
* *Nhận dạng lỗ hổng*: Xác định các lỗ hổng trong hệ thống thông tin và thông tin của tổ chức. Các lỗ hổng có thể phát sinh từ phần mềm, phần cứng hoặc lỗi của con người.
* *Đánh giá lỗ hổng:* Đánh giá khả năng và tác động tiềm năng của từng mối đe dọa và tính dễ bị tổn thương đối với hệ thống thông tin và thông tin của tổ chức. Chỉ định xếp hạng rủi ro cho từng rủi ro được xác định.
* *Ưu tiên rủi ro*: Ưu tiên rủi ro dựa trên xếp hạng rủi ro và tác động tiềm năng của họ đối với tổ chức.
* *Điều trị rủi ro*: Phát triển và thực hiện kế hoạch quản lý rủi ro để giảm, chuyển hoặc chấp nhận rủi ro. Kế hoạch quản lý rủi ro nên bao gồm các biện pháp để giải quyết các rủi ro được xác định và dòng thời gian để thực hiện.
* *Giám sát và xem xét rủi ro*: Thường xuyên giám sát và xem xét hiệu quả của kế hoạch quản lý rủi ro và thực hiện các điều chỉnh cần thiết theo yêu cầu.

Phân tích rủi ro bảo mật thông tin là một thành phần thiết yếu của quy trình quản lý rủi ro tổng thể của tổ chức. Bằng cách xác định và ưu tiên rủi ro, các tổ chức có thể thực hiện các biện pháp phù hợp để bảo vệ hệ thống thông tin và thông tin của họ khỏi các mối đe dọa và lỗ hổng tiềm năng.

### Giảm thiểu rủi ro

Có một số bước mà các tổ chức có thể thực hiện để giảm rủi ro bảo mật thông tin:

* *Tiến hành đánh giá rủi ro*: các tổ chức nên thường xuyên tiến hành đánh giá rủi ro để xác định rủi ro và lỗ hổng tiềm năng đối với hệ thống thông tin và thông tin của họ. Điều này sẽ cho phép họ ưu tiên và phát triển một kế hoạch để giảm thiểu rủi ro.
* *Thực hiện các chính sách và thủ tục bảo mật*: Các tổ chức nên phát triển và thực hiện các chính sách và quy trình bảo mật chi phối cách nhân viên truy cập, sử dụng và bảo vệ hệ thống thông tin và thông tin.
* *Cung cấp đào tạo nhận thức bảo mật*: Các tổ chức nên cung cấp đào tạo nhận thức bảo mật thường xuyên cho nhân viên để giúp họ hiểu tầm quan trọng của bảo mật và cách bảo vệ hệ thống thông tin và thông tin.
* *Sử dụng mật khẩu mạnh*: Các tổ chức nên yêu cầu nhân viên sử dụng mật khẩu mạnh và thay đổi chúng thường xuyên để ngăn chặn truy cập trái phép.
* *Thực hiện kiểm soát truy cập:* Các tổ chức nên thực hiện các điều khiển truy cập để giới hạn quyền truy cập vào hệ thống thông tin và thông tin cho nhân viên được ủy quyền.
* *Giữ cho phần mềm và hệ thống cập nhật:* Các tổ chức nên đảm bảo rằng phần mềm và hệ thống được cập nhật thường xuyên với các bản vá và cập nhật bảo mật mới nhất để ngăn chặn các lỗ hổng.
* *Dữ liệu sao lưu thường xuyên*: Các tổ chức nên thường xuyên sao lưu dữ liệu quan trọng để đảm bảo rằng nó có thể được phục hồi trong trường hợp xảy ra sự cố bảo mật.
* *Tiến hành kiểm toán bảo mật thường xuyên*: Các tổ chức nên tiến hành kiểm toán bảo mật thường xuyên để đảm bảo rằng các biện pháp bảo mật của họ có hiệu lực và cập nhật.
* *Sử dụng mã hóa*: Các tổ chức nên sử dụng mã hóa để bảo vệ thông tin nhạy cảm và ngăn chặn truy cập trái phép.

Bằng cách thực hiện các bước này, các tổ chức có thể giảm rủi ro bảo mật thông tin của họ và bảo vệ tốt hơn hệ thống thông tin và thông tin của họ khỏi các mối đe dọa và lỗ hổng tiềm năng.

### Đánh giá lại rủi ro lần nữa

Đánh giá lại rủi ro bảo mật thông tin là một quá trình quan trọng cần được thực hiện định kỳ để đảm bảo rằng tư thế bảo mật của một tổ chức được cập nhật và hiệu quả trong việc giải quyết các mối đe dọa mới và phát triển. Dưới đây là một số bước bạn có thể thực hiện để đánh giá lại rủi ro bảo mật thông tin:

* *Xem lại các đánh giá rủi ro hiện tại*: Bắt đầu bằng cách xem xét các đánh giá rủi ro hiện tại của tổ chức để xác định xem chúng có còn liên quan và cập nhật hay không. Đảm bảo đánh giá cả rủi ro bên ngoài và bên trong cho tổ chức, bao gồm các mối đe dọa đối với bảo mật vật lý, bảo mật mạng, bảo mật dữ liệu và bảo mật nhân sự.
* *Xác định các rủi ro mới:* Luôn cập nhật các xu hướng và tin tức mới nhất về an ninh mạng để xác định các rủi ro mới và mới nổi. Được thông báo về các loại mối đe dọa mới, chẳng hạn như ransomware, kỹ thuật xã hội và các cuộc tấn công chuỗi cung ứng và cách chúng có thể tác động đến tổ chức của bạn.
* *Tiến hành đánh giá lỗ hổng*: Thực hiện các đánh giá lỗ hổng trên hệ thống và mạng của bạn để xác định các điểm yếu tiềm năng có thể được khai thác bởi những kẻ tấn công. Điều này có thể giúp bạn ưu tiên các nỗ lực bảo mật của bạn và giải quyết các lỗ hổng quan trọng nhất trước tiên.
* *Xem xét các chính sách và quy trình bảo mật:* Xem lại các chính sách và quy trình bảo mật của tổ chức của bạn để đảm bảo chúng được cập nhật và hiệu quả trong việc giải quyết các rủi ro hiện tại. Hãy chắc chắn rằng tất cả nhân viên đều biết về các chính sách này và đã được đào tạo phù hợp.
* *Thực hiện kiểm tra bảo mật*: Tiến hành kiểm tra bảo mật, chẳng hạn như kiểm tra thâm nhập hoặc tập thể dục nhóm màu đỏ, để xác định điểm yếu trong phòng thủ bảo mật của bạn. Điều này có thể giúp bạn xác định các lỗ hổng trong các điều khiển bảo mật của bạn và giải quyết chúng trước khi chúng có thể được khai thác bởi những kẻ tấn công.
* *Lập kế hoạch cho các sự cố*: Phát triển và xem xét các kế hoạch ứng phó sự cố để đảm bảo rằng bạn sẵn sàng ứng phó với các sự cố an ninh một cách nhanh chóng và hiệu quả. Hãy chắc chắn rằng tất cả nhân viên đều biết phải làm gì trong trường hợp xảy ra sự cố và kế hoạch thường xuyên được kiểm tra.

Bằng cách làm theo các bước này, bạn có thể đánh giá lại rủi ro bảo mật thông tin của tổ chức và đảm bảo rằng tư thế bảo mật của bạn được cập nhật và hiệu quả trong việc giải quyết các mối đe dọa mới và phát triển.

## Thực trạng rủi ro ở các doanh nghiệp

### Thực trạng ở các doanh nghiệp

Theo Tổng cục Thống Kê năm 2019, Việt Nam hiện có khoảng trên 800 nghìn doanh nghiệp đang hoạt động, trong đó số doanh nghiệp vừa và nhỏ chiếm 98,95% tổng số doanh nghiệp cả nước. Trong những năm qua, doanh nghiệp vừa và nhỏ tại Việt Nam có vai trò vô cùng quan trọng đối với sự phát triển của nền kinh tế.

Tuy nhiên thực tế hoạt động của các doanh nghiệp này còn gặp nhiều khó khăn do tác động từ các yếu tố chủ quan và khách quan. Bên cạnh đó, các rủi ro xuất hiện ngày càng nhiều gây cản trở đến sự phát triển của các doanh nghiệp này. Cũng bởi vậy, vấn đề quản trị rủi ro trong hoạt động của các doanh nghiệp ngày càng được quan tâm với mong muốn đưa ra được các giải pháp nâng cao hiệu quả quản trị rủi ro trong doanh nghiệp và tạo tiền đề cho sự phát triển vượt bậc của doanh nghiệp vừa và nhỏ nói riêng cũng như cả nền kinh tế Việt Nam nói chung.

Quản trị rủi ro trong hoạt động kinh doanh của các doanh nghiệp là quá trình tiếp cận vấn đề rủi ro một cách khoa học và có hệ thống nhằm nhận dạng, kiểm soát, phòng tránh và giảm thiểu những tổn thất, mất mát hay những ảnh hưởng bất lợi của các rủi ro này, qua đó tìm cách biến rủi ro thành cơ hội để phát triển.

Hiện nay tồn tại nhiều loại rủi ro trong các tổ chức, bao gồm:

* *Rủi ro mang tính chủ quan*: Đây là những rủi ro bắt nguồn từ sai lầm chủ quan của người quản lý và các nhân viên làm việc trong doanh nghiệp. Vấn đề này cũng thường xuất hiện trong việc quản lý nguồn lực của công ty.
* *Rủi ro mang tính khách quan*: Loại rủi ro này xuất phát từ bên ngoài và được tạo ra từ các vấn đề mang tính bất khả kháng và nằm ngoài tầm kiểm soát của doanh nghiệp.
* *Rủi ro tài chính*: Rủi ro tài chính xuất hiện khá phổ biến trong các doanh nghiệp, liên quan trực tiếp đến tài sản của tổ chức. Rủi ro tài chính bao gồm: Rủi ro vốn đầu tư, lợi nhuận, tiền lương,…
* *Rủi ro về nhân lực*: Đây là loại rủi ro bắt nguồn từ chính nội tại của các mối quan hệ bất đồng trong nội bộ tổ chức, đặc biệt ở vị trí quản lý. Ngoài ra, rủi ro về nhân lực cũng có một số nguyên nhân khác như: Tổn thất khi người lao động gặp tai nạn, tử vong, bỏ việc,… Từ đó gây tổn thất lớn về nhân sự và ảnh hưởng trực tiếp tới tiến độ làm việc cũng như hiệu quả kinh doanh của tổ chức.
* *Rủi ro về năng suất*: Năng suất là yếu tố ảnh hưởng trực tiếp đến tốc độ phát triển, doanh thu và lợi nhuận của doanh nghiệp. Do đó những doanh nghiệp không thể duy trì tốt hay không tăng được năng suất được xem là yếu tố rủi ro kìm hãm sự phát triển.

### Ưu nhược điểm của công cụ tự động đánh giá rủi ro

Rủi ro có thể tồn tại ở bất kỳ giai đoạn nào của tổ chức, gây ra nhiều ảnh hưởng tiêu cực và có thể làm chậm quá trình kinh doanh. Trong môi trường kinh doanh hiện nay, các doanh nghiệp được yêu cầu phải có nhận thức tốt về các loại rủi ro, tuy nhiên đa số các tổ chức lại thiếu một bức tranh toàn cảnh cho các loại rủi ro này. Để đảm bảo sự phát triển lâu dài, bền vững và đạt được hiệu suất như mong đợi, tổ chức cần nhanh chóng tìm ra rủi ro và ngăn chặn hiệu quả trong thực tế.

Trong trường hợp này, sử dụng phần mềm quản lý rủi ro là giải pháp tối ưu nhất. Đây là các loại phần mềm có khả năng tự động hóa việc thu thập tài liệu và cho phép tổ chức đào sâu vào báo cáo. Từ đó, phần mềm sẽ phân tích chi tiết để truy cập vào thông tin quản lý rủi ro theo thời gian trong toàn bộ tổ chức, xem xét rủi ro theo sản phẩm, quy trình hoặc danh mục rủi ro. Phần mềm quản lý rủi ro được xem như công cụ quản trị trong doanh nghiệp mà thông qua đó, các doanh nghiệp có thể quan sát một cách tổng thể tình hình kinh doanh của tổ chức để đưa ra hướng giải quyết phù hợp. Tuy nhiên không có công cụ nào là hoàn hảo và chúng cũng có những ưu điểm, nhược điểm riêng.

**Ưu điểm:**

* *Tăng tính chính xác*: Công cụ tự động đánh giá rủi ro sử dụng các thuật toán và phương pháp tính toán để đưa ra kết quả đánh giá rủi ro, giúp tăng tính chính xác và khả năng dự đoán các rủi ro tiềm năng.
* *Tiết kiệm thời gian*: Việc đánh giá rủi ro thủ công có thể tốn rất nhiều thời gian, đặc biệt là đối với các doanh nghiệp hoặc tổ chức có quy mô lớn. Sử dụng công cụ tự động giúp tiết kiệm thời gian đánh giá, giảm thiểu sự mệt mỏi và tăng hiệu quả làm việc.
* *Đồng bộ hóa dữ liệu*: Công cụ tự động đánh giá rủi ro giúp tổ chức đồng bộ hóa dữ liệu, giảm thiểu các sai sót hoặc thiếu sót trong quá trình thu thập và phân tích dữ liệu.
* *Dễ dàng quản lý*: Các công cụ tự động đánh giá rủi ro thường được thiết kế để dễ dàng quản lý và sử dụng, giúp các tổ chức có thể quản lý rủi ro hiệu quả hơn.
* *Phát hiện rủi ro nhanh chóng*: Các công cụ tự động đánh giá rủi ro có thể phát hiện các rủi ro tiềm năng nhanh chóng, giúp tổ chức có thể đưa ra các biện pháp phòng ngừa và giảm thiểu tác động tiêu cực của rủi ro đối với hoạt động kinh doanh.

**Nhược điểm:**

* *Giới hạn của mô hình:* Các công cụ tự động đánh giá rủi ro phải dựa trên các mô hình và thuật toán để đưa ra dự đoán, vì vậy chúng có thể không đủ linh hoạt để xử lý các tình huống đặc biệt và có thể không chính xác trong việc đánh giá các rủi ro hiếm.
* *Phụ thuộc vào chất lượng dữ liệu*: Công cụ tự động đánh giá rủi ro có thể phụ thuộc vào chất lượng dữ liệu đầu vào. Nếu dữ liệu không chính xác hoặc không đầy đủ, kết quả đánh giá rủi ro cũng sẽ không chính xác.
* *Yêu cầu kỹ năng chuyên môn*: Việc sử dụng công cụ tự động đánh giá rủi ro yêu cầu kỹ năng chuyên môn để cấu hình, hiểu và sử dụng một số công cụ này, đặc biệt là trong các trường hợp phức tạp.
* *Chi phí đầu tư ban đầu*: Để triển khai các công cụ tự động đánh giá rủi ro, tổ chức sẽ cần phải đầu tư chi phí đầu tư ban đầu để mua các phần mềm, thiết bị và huấn luyện nhân viên.
* *Không thể thay thế hoàn toàn cho con người*: Công cụ tự động đánh giá rủi ro có thể giúp tổ chức tiết kiệm thời gian và tăng tính chính xác, nhưng chúng không thể thay thế hoàn toàn cho con người trong việc đánh giá rủi ro. Con người vẫn cần phải đưa ra quyết định cuối cùng và có vai trò quan trọng trong việc giám sát và đánh giá rủi ro trong các hoạt động kinh doanh.

## Biện pháp kiểm soát rủi ro

### Hướng dẫn chung

Theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, hệ thống thông tin phải đáp ứng các yêu cầu an toàn cơ bản, tối thiểu. Tuy nhiên, mỗi hệ thống thông tin khác nhau sẽ có sẽ có đặc thù riêng và yêu cầu mức độ an toàn khác nhau phù hợp với yêu cầu thực tế của mỗi cơ quan, tổ chức. Do đó, trên cơ sở đánh giá và quản lý rủi ro, cơ quan, tổ chức cần rà soát, bổ sung các yêu cầu an toàn (sau đây gọi là biện pháp kiểm soát rủi ro) cho phù hợp với yêu cầu thực tế. Khi triển khai các biện pháp kiểm soát rủi ro, trước hết cơ quan, tổ chức cần xem xét các biện pháp cần thiết đã có trong yêu cầu cơ bản hay chưa.

Trường hợp, biện pháp kiểm soát đã nằm trong yêu cầu cơ bản thì cần thực hiện theo quy định. Trường hợp cần bổ sung các yêu cầu an toàn mới để đáp ứng yêu cầu thực tế thì cần đưa ra phương án cụ thể để thực hiện.

Các biện pháp kiểm soát cơ bản đối với hệ thống thông tin được quy định tại

Điều 19 Nghị định 85/2016/NĐ-CP ngày 10/7/2016, Điều 8, 9 Thông tư

03/2017/TT-BTTTT ngày 24/4/2017 và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017. Các yêu cầu an toàn được chia làm nhóm các yêu cầu về quản lý và các yêu cầu về kỹ thuật. Trong đó, các yêu cầu về kỹ thuật đưa ra các yêu cầu liên quan đến thiết kế, thiết lập, các biện pháp, giải pháp công nghệ đối với hệ thống trong quá trình xây dựng và thiết lập. Các yêu cầu về quản lý đưa ra chính sách, quy chế, quy trình, tổ chức bộ máy bảo đảm an toàn thông tin nhằm bảo đảm an toàn thông tin cho hệ thống thông tin trong quá trình vận hành, khai thác.

Các biện pháp kiểm soát đưa ra trong TCVN 11930:2017 được phân thành 05 mức theo cấp độ của hệ thống thông tin cần bảo vệ. Do đó, biện pháp kiểm soát rủi ro khi lựa chọn cần dựa vào mức rủi ro để xác định các biện pháp kiểm soát phù hợp trong TCVN 11930:2017 và các tiêu chuẩn khác liên quan. Ví dụ, mức ảnh hưởng được xác định là mức 5 thì biện pháp kiểm soát được lựa chọn sẽ là các biện pháp tương ứng với cấp độ 5 trong TCVN 11930:2017.

Các biện pháp bổ sung được xác định là các biện pháp được yêu cầu ở hệ

thống thông tin ở cấp độ cao hơn. Ví dụ hệ thống thông tin được xác định là cấp

độ 3, cần áp dụng các biện pháp kiểm soát yêu cầu với hệ thống thông tin cấp độ

4, thì các biện pháp này được coi là biện pháp bổ sung. 22 Bên cạnh đó, các biện pháp kiểm soát bổ sung, cơ quan, tổ chức có thể tham khảo từ hai bộ tiêu chuẩn ISP/IEC 27000 đối với các biện pháp về quản lý và SP800-53 đối với các biện pháp về kỹ thuật. Các biện pháp kiểm soát kiểm soát cơ bản và bổ sung được hướng dẫn cụ thể như dưới đây.

### Biện pháp kiểm soát về quản lý

***1.4.2.1. Các yêu cầu an toàn cơ bản theo TCVN 11930***

*1.4.2.1.1. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin*

Đưa ra mục tiêu, nguyên tắc bảo đảm an toàn thông tin của tổ chức.

*1.4.2.1.2. Trách nhiệm bảo đảm an toàn thông tin.*

Đưa ra các quy định về trách nhiệm bảo đảm an toàn thông tin của đơn vị

chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối

tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.

*1.4.2.1.3. Phạm vi chính sách an toàn thông tin*

Đưa ra phạm vi chính sách, đối tượng áp dụng chính sách bảo đảm an toàn thông tin của tổ chức.

*1.4.2.1.4. Tổ chức bảo đảm an toàn thông tin*

Cung cấp thông tin về cơ cấu, tổ chức bảo đảm an toàn thông tin của tổ chức, bao gồm: Đơn vị chuyên trách về an toàn thông tin; Cơ chế, đầu mối phối hợp với cơ quan/tổ chức có thẩm quyền trong hoạt động bảo đảm an toàn thông tin.

*1.4.2.1.5. Bảo đảm nguồn nhân lực*

Đưa ra chính sách/quy trình thực hiện quản lý bảo đảm nguồn nhân lực an

toàn thông tin của tổ chức, bao gồm: Tuyển dụng cán bộ; quy chế/quy định bảo

đảm an toàn thông tin trong quá trình làm việc và chấm dứt hoặc thay đổi công

việc.

*1.4.2.1.6. Quản lý thiết kế, xây dựng hệ thống*

Đưa ra chính sách/quy trình thực hiện quản lý thiết kế, xây dựng hệ thống

của tổ chức, bao gồm: Thiết kế an toàn hệ thống thông tin; Phát triển phần mềm

thuê khoán; Thử nghiệm và nghiệm thu hệ thống.

*1.4.2.1.7. Quản lý vận hành hệ thống*

a) Quản lý an toàn mạng: Đưa ra chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường 23 của hệ thống; Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố; Truy cập và quản lý cấu hình hệ thống; Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

b) Quản lý an toàn máy chủ và ứng dụng: Đưa ra chính sách/quy trình thực hiện quản lý an toàn máy chủ và ứng dụng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ; Truy cập mạng của máy chủ; Truy cập và quản trị máy chủ và ứng dụng; Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố; Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống; Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

c) Quản lý an toàn dữ liệu: Đưa ra chính sách/quy trình thực hiện quản lý an toàn dữ liệu của tổ chức, bao gồm: Yêu cầu an toàn đối với phương pháp mã hóa; Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa; Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu; Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ; Sao lưu dự phòng và khôi phục dữ liệu; Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

d) Quản lý an toàn thiết bị đầu cuối: Đưa ra chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường cho thiết bị đầu cuối; Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa; Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng; Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối.

đ) Quản lý phòng chống phần mềm độc hại: Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng; Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động; Thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Kiểm tra và xử lý phần mềm độc hại.

e) Quản lý giám sát an toàn hệ thống thông tin: Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; 24 Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

g) Quản lý điểm yếu an toàn thông tin: Đưa ra chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin của tổ chức, bao gồm: Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin; Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; Phân nhóm và mức độ của điểm yếu; Cơ chế phối hợp với các nhóm chuyên gia; Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin trước khi đưa hệ thống vào sử dụng; Quy trình khôi phục lại hệ thống.

h) Quản lý sự cố an toàn thông tin: Đưa ra chính sách/quy trình thực hiện

quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn

thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

i) Quản lý an toàn người sử dụng đầu cuối: Đưa ra chính sách/quy trình thực hiện quản lý an toàn người sử dụng đầu cuối của tổ chức, bao gồm: Quản lý truy cập, sử dụng tài nguyên nội bộ; Quản lý truy cập mạng và tài nguyên trên Internet; Cài đặt và sử dụng máy tính an toàn.

***1.4.2.2. Các yêu cầu an toàn bổ sung***

Cơ quan, tổ chức có thể tham khảo các biện pháp kiểm sát được đưa ra tại

tiêu chuẩn TCVN ISO/IEC 27002:2020, bao gồm các biện pháp kiểm soát được

chia thành 15 nhóm như sau: Chính sách an toàn thông tin; Tổ chức bảo đảm an

toàn thông tin; An toàn nguồn nhân lực; Quản lý tài sản; Kiểm soát truy cập; Mật mã; An toàn vật lý và môi trường; An toàn vận hành; An toàn truyền thông; Tiếp nhận, phát triển và bảo trì hệ thống; Các mối quan hệ với nhà cung cấp; Quản lý sự cố an toàn thông tin; Các khía cạnh an toàn thông tin trong quản lý hoạt động nghiệp vụ liên tục; Soát xét về an toàn thông tin.

### Biện pháp kiểm soát về kỹ thuật

***1.4.3.1. Các yêu cầu an toàn cơ bản theo TCVN 11930***

*1.4.3.1.1. Bảo đảm an toàn mạng*

a) Thiết kế hệ thống 25

- Đưa ra yêu cầu về thiết kế các vùng mạng trong hệ thống theo chức năng,

các vùng mạng.

- Đưa ra yêu cầu về các biện pháp bảo vệ cụ thể bao gồm: Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn, Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng, Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu, Có phương án chặn lọc phần mềm độc hại trên môi trường mạng, Phương án phòng chống tấn công từ chối dịch vụ, Phương án giám sát hệ thống thông tin tập trung, Phương án giám sát an toàn hệ thống thông tin tập trung, Phương án quản lý sao lưu dự phòng tập trung, Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung, Phương án phòng, chống thất thoát dữ liệu, Phương án bảo đảm an toàn cho mạng không dây, Phương án quản lý tài khoản đặc quyền, Phương án dự phòng hệ thống ở vị trí địa lý khác nhau.

b) Kiểm soát truy cập từ bên ngoài mạng: Đưa ra biện pháp quản lý truy cập từ các mạng bên ngoài theo chiều đi vào hệ thống tới các máy chủ dịch vụ bên trong mạng, bao gồm: Các dịch vụ/ứng dụng cho phép từ truy cập từ bên ngoài; Thời gian mất kết nối; Phân quyền truy cập; Giới hạn kết nối; Thiết lập chính sách ưu tiên. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

c) Kiểm soát truy cập từ bên trong mạng: Đưa ra biện pháp quản lý truy cập

từ các máy tính/máy chủ bên trong mạng theo chiều đi ra các mạng bên ngoài và

các mạng khác bên trong mạng, bao gồm: Các ứng dụng/dịch vụ nào được truy

cập; Quản lý truy cập theo địa chỉ thiết bị; phương án ưu tiên truy cập. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

d) Nhật ký hệ thống: Đưa ra biện pháp quản lý nhật ký hệ thống (log) trên

các thiết bị hệ thống về bật chức năng ghi log; thông tin ghi log; thời gian, dung

lượng ghi log; quản lý log.

đ) Phòng chống xâm nhập: Đưa ra biện pháp triển khai/thiết lập cấu hình của thiết bị phòng, chống xâm nhập IDS/IPS hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống nhằm đáp ứng yêu cầu an toàn.

e) Phòng chống phần mềm độc hại trên môi trường mạng: Đưa ra biện pháp triển khai/thiết lập cấu hình của thiết bị để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng đáp ứng yêu cầu an toàn. 26

g) Bảo vệ thiết bị hệ thống: Đưa ra biện pháp triển khai/thiết lập cấu hình

chức năng bảo mật trên các thiết bị có trong hệ thống nhằm bảo đảm bảo đảm an

toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành.

*1.4.3.1.2. Bảo đảm an toàn máy chủ*

a) Xác thực: Đưa ra biện pháp cấu hình/thiết lập chính sách xác thực trên

máy chủ để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

b) Kiểm soát truy cập: Đưa ra biện pháp cấu hình/thiết lập chính sách kiểm soát truy cập trên máy chủ để bảo đảm việc truy cập, sử dụng máy chủ an toàn sau khi đăng nhập thành công.

c) Nhật ký hệ thống: Đưa ra biện pháp quản lý nhật ký hệ thống (log) trên

các máy chủ về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, Dung lượng ghi log; Quản lý log.

d) Phòng chống xâm nhập: Đưa ra biện pháp cấu hình/thiết lập cấu hình bảo mật trên máy chủ để bảo bảo vệ tấn công xâm nhập từ bên ngoài.

đ) Phòng chống phần mềm độc hại: Đưa ra biện pháp cấu hình/thiết lập cấu hình bảo mật trên máy chủ về: Cài đặt phần mềm phòng chống mã độc; Dò quét mã độc; Xử lý mã độc; Quản lý tập trung phần mềm phòng chống mã độc...để phòng chống mã độc cho máy chủ.

e) Xử lý máy chủ khi chuyển giao: Đưa ra biện pháp xóa sạch dữ liệu; sao

lưu dự phòng dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

*1.4.3.1.3. Bảo đảm an toàn ứng dụng*

a) Xác thực Đưa ra biện pháp cấu hình/thiết lập chính sách xác thực trên ứng dụng để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

b) Kiểm soát truy cập: Đưa ra biện pháp cấu hình/thiết lập chính sách kiểm soát truy cập trên ứng dụng để bảo đảm việc truy cập, sử dụng ứng dụng an toàn sau khi đăng nhập thành công.

c) Nhật ký hệ thống: Đưa ra biện pháp quản lý nhật ký hệ thống (log) trên

các ứng dụng về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, dung lượng ghi log; Quản lý log.

d) Bảo mật thông tin liên lạc: Đưa ra biện pháp mã hóa và sử dụng giao thức mạng hoặc kênh kết nối mạng an toàn khi trao đổi dữ liệu qua môi trường mạng.

đ) Chống chối bỏ: Đưa ra biện pháp sử dụng và bảo vệ chữ ký số để bảo vệ tính bí mật và chống chối bỏ khi gửi/nhận thông tin quan trọng qua mạng. 27

e) An toàn ứng dụng và mã nguồn: Đưa ra biện pháp cấu hình/thiết lập chức năng bảo mật cho ứng dụng và phương án bảo vệ mã nguồn ứng dụng.

*1.4.3.1.4. Bảo đảm an toàn dữ liệu*

a) Nguyên vẹn dữ liệu: Đưa ra biện pháp lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính nguyên vẹn của dữ liệu.

b) Bảo mật dữ liệu: Đưa ra biện pháp lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính bí mật của dữ liệu.

c) Sao lưu dự phòng: Đưa ra biện pháp sao lưu dự phòng dữ liệu: Các thông tin yêu cầu sao lưu dự phòng; Phân loại dữ liệu sao lưu dự phòng; Hệ thống sao lưu dự phòng…

***1.4.3.2. Các yêu cầu an toàn bổ sung***

Cơ quan, tổ chức có thể tham khảo các tiêu chuẩn quốc tế dưới đây để xác

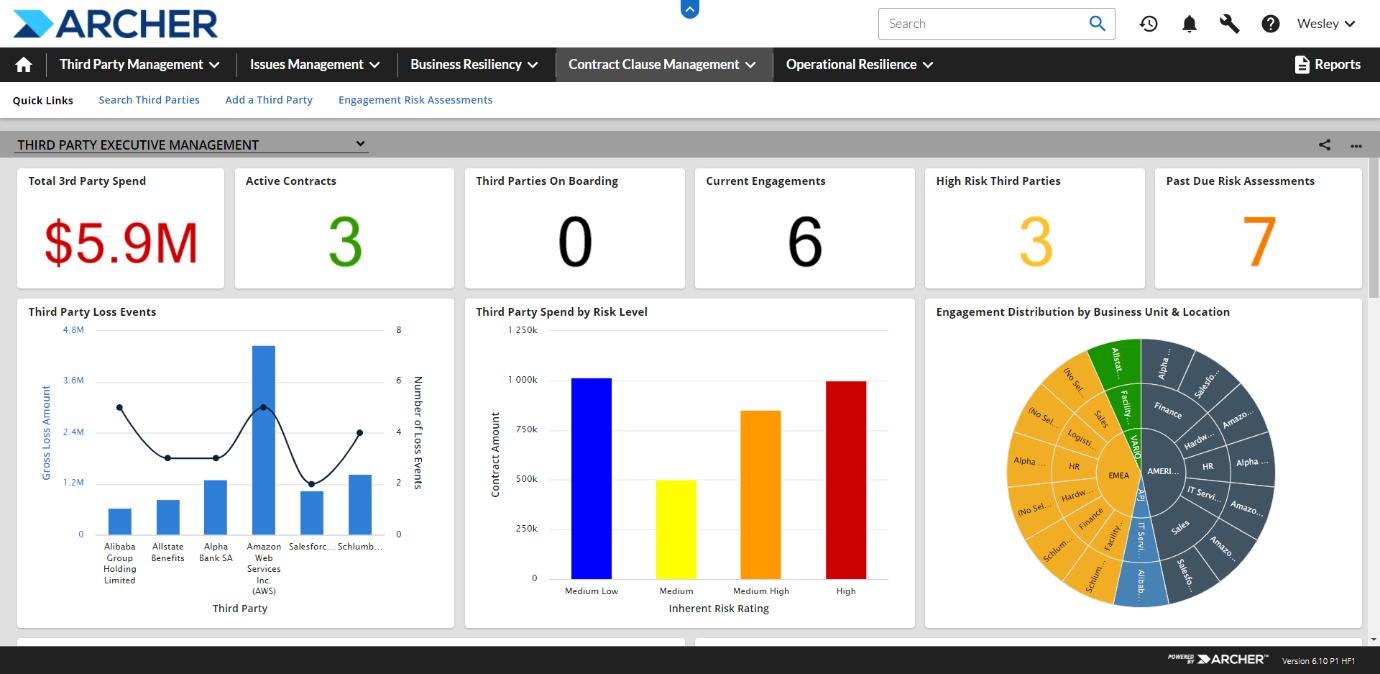
định các biện pháp bổ sung, bao gồm nhưng không giới hạn các nhóm, tiêu chuẩn sau: Quản lý sự cố an toàn thông tin, Quản lý giám sát, Kiểm tra, đánh giá an toàn thông tin, Kỹ thuật an toàn mạng, Kỹ thuật an toàn máy chủ, Kỹ thuật an toàn thông tin cho ứng dụng, Kỹ thuật an toàn dữ liệu, Kỹ thuật an toàn thiết bị đầu cuối. Danh mục các tiêu chuẩn cụ thể tại Phụ lục 4 hướng dẫn này.

# MỘT SỐ CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO

## RSA Archer (Nền tảng GRC)

### Chi tiết

RSA Archer là một nền tảng Quản trị, Rủi ro và Tuân thủ (GRC) cung cấp cho các tổ chức một nền tảng tập trung để quản lý rủi ro, tuân thủ và các hoạt động kiểm toán.

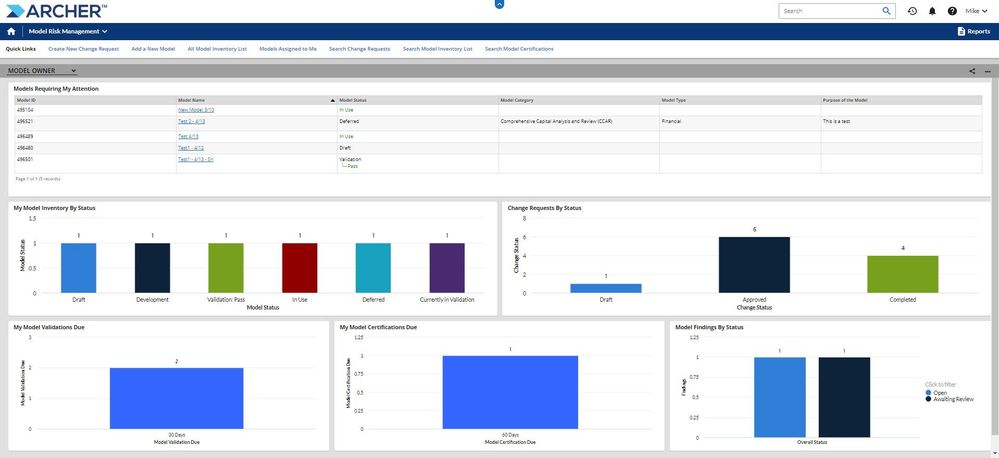


Hình 1. Giao diện Archer

Chi phí của RSA Archer khác nhau tùy thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức, nhưng thường bắt đầu ở mức khoảng 40.000 đô la mỗi năm cho triển khai cơ bản và mở rộng quy mô cho các triển khai lớn hơn hoặc khả năng nâng cao. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai cũng như các tính năng và khả năng cụ thể được yêu cầu.

### Tính năng

* Quản lý rủi ro: RSA Archer cung cấp một nền tảng tập trung để quản lý rủi ro, bao gồm khả năng xác định, đánh giá và ưu tiên rủi ro cũng như phát triển và triển khai các chiến lược giảm thiểu.



Hình 2. Tính năng quản lý rủi ro của Archer

* Quản lý tuân thủ: RSA Archer cung cấp một nền tảng tập trung để quản lý tuân thủ, bao gồm khả năng theo dõi và quản lý các yêu cầu tuân thủ quy định cũng như giám sát các hoạt động tuân thủ.
* Quản lý kiểm toán: RSA Archer cung cấp một nền tảng tập trung để quản lý các hoạt động kiểm toán, bao gồm khả năng lập kế hoạch, thực hiện và theo dõi kiểm toán cũng như quản lý các phát hiện và đề xuất kiểm toán.



Hình 3. Tính năng quản lý kiểm toán của Archer

* Quản lý sự cố: RSA Archer cung cấp khả năng quản lý sự cố, cho phép các tổ chức quản lý và ứng phó với các sự cố bảo mật cũng như các rủi ro khác một cách tập trung và có tổ chức.
* Báo cáo và phân tích: RSA Archer cung cấp nhiều khả năng báo cáo và phân tích, cho phép các tổ chức tạo báo cáo và phân tích dữ liệu để hiểu rõ hơn về các hoạt động kiểm toán, tuân thủ và rủi ro của họ.

### Ưu điểm

* Nền tảng tập trung: RSA Archer cung cấp một nền tảng tập trung để quản lý các chương trình rủi ro, tuân thủ và bảo mật, cho phép các tổ chức có một nguồn thông tin xác thực duy nhất về rủi ro và thông tin tuân thủ.
* Tự động hóa: RSA Archer tự động hóa nhiều quy trình quản lý rủi ro, giảm công sức thủ công và tăng hiệu quả.
* Tích hợp: RSA Archer tích hợp với các công cụ và hệ thống bảo mật khác, cung cấp cái nhìn toàn diện về tình trạng rủi ro của tổ chức và cho phép các nhóm ứng phó với rủi ro và sự cố hiệu quả hơn.
* Cộng tác: RSA Archer hỗ trợ cộng tác giữa các bộ phận và các bên liên quan khác nhau, cho phép các tổ chức quản lý rủi ro và tuân thủ trong toàn doanh nghiệp.
* Các mẫu và trường hợp sử dụng dựng sẵn: RSA Archer cung cấp một số mẫu và trường hợp sử dụng dựng sẵn, cho phép các tổ chức bắt đầu nhanh chóng và giảm thời gian triển khai.

### Nhược điểm

* Độ phức tạp: RSA Archer là một nền tảng phức tạp và đường cong học tập có thể dốc, đặc biệt đối với các tổ chức mới làm quen với quản lý rủi ro và GRC.
* Chi phí: RSA Archer có thể tốn kém, đặc biệt đối với các tổ chức có ngân sách hạn chế.
* Triển khai: Triển khai RSA Archer có thể là một quy trình phức tạp và tốn thời gian, đặc biệt đối với các tổ chức có yêu cầu quản lý rủi ro phức tạp.
* Tùy chỉnh hạn chế: Mặc dù RSA Archer hỗ trợ cấu hình tùy chỉnh, nhưng có thể có những hạn chế về mức độ nền tảng có thể được tùy chỉnh để đáp ứng nhu cầu cụ thể của tổ chức.
* Hiệu suất: Hiệu suất của RSA Archer có thể bị ảnh hưởng bởi lượng dữ liệu và số lượng người dùng truy cập nền tảng, điều này có thể dẫn đến chậm và ngừng hoạt động.

## Qualys (Công cụ quét lỗ hổng)

### Chi tiết

Qualys là một nền tảng tuân thủ và bảo mật dựa trên đám mây, cung cấp cho các tổ chức một nền tảng tập trung để quản lý các hoạt động tuân thủ và bảo mật của họ.

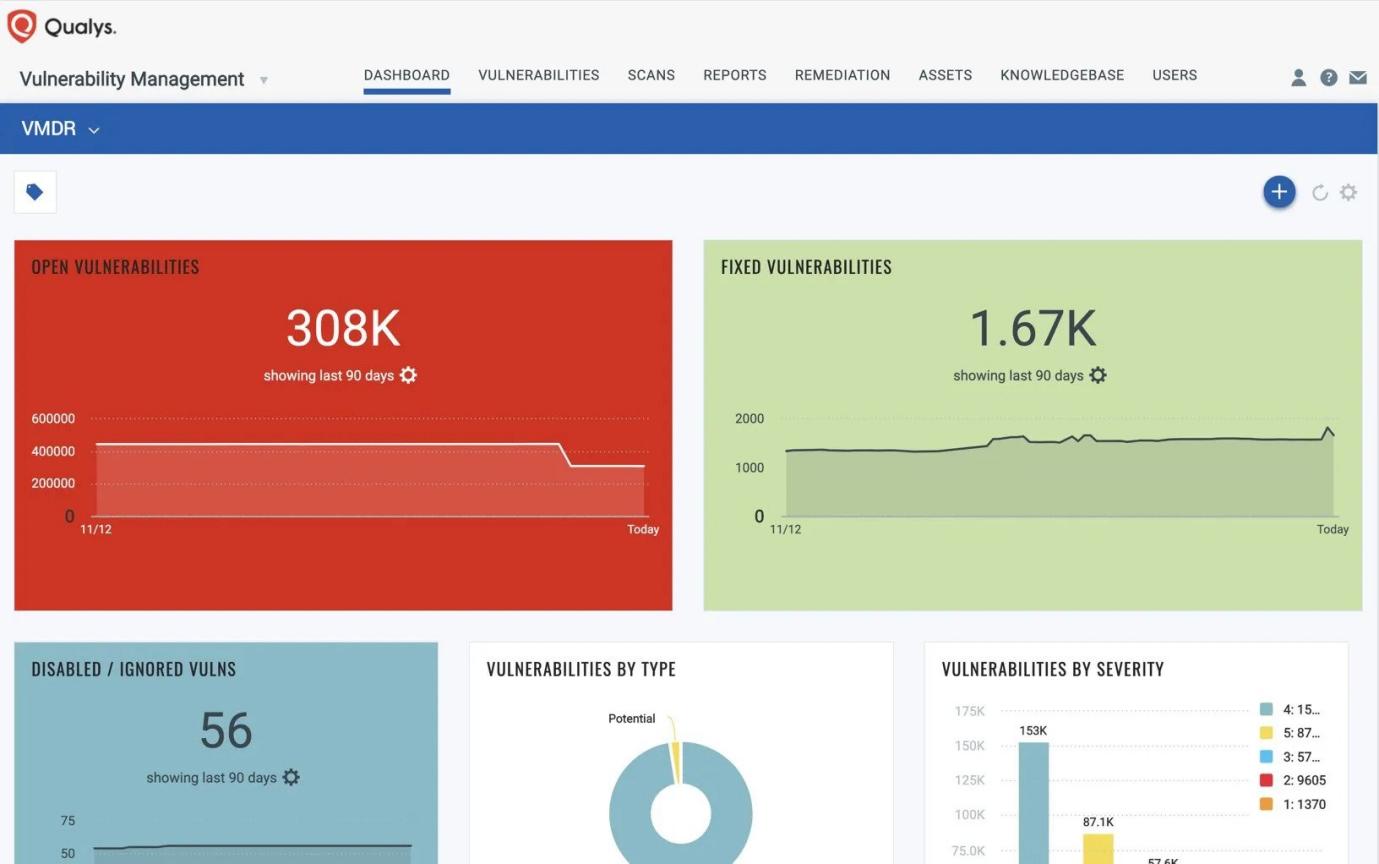


Hình 4. Giao diện Qualys

Chi phí của Qualys khác nhau tùy thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức, nhưng thường bắt đầu ở mức khoảng 1.000 đô la mỗi năm cho triển khai cơ bản và mở rộng quy mô cho triển khai lớn hơn hoặc khả năng nâng cao. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai cũng như các tính năng và khả năng cụ thể được yêu cầu.

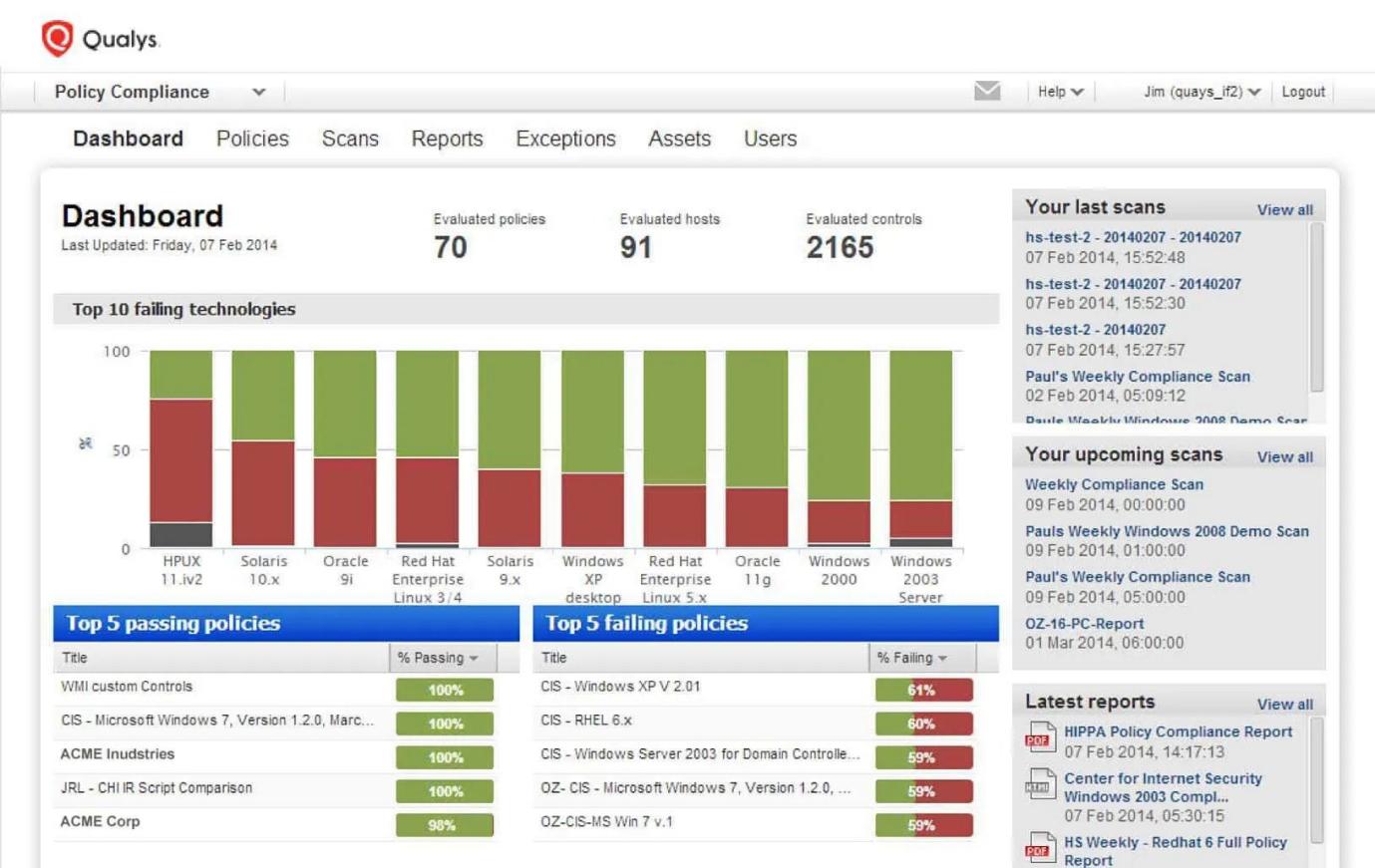
### Tính năng

* Quản lý lỗ hổng: Qualys cung cấp khả năng quản lý lỗ hổng, bao gồm quét lỗ hổng và đánh giá lỗ hổng, để giúp các tổ chức xác định và giảm thiểu rủi ro bảo mật.



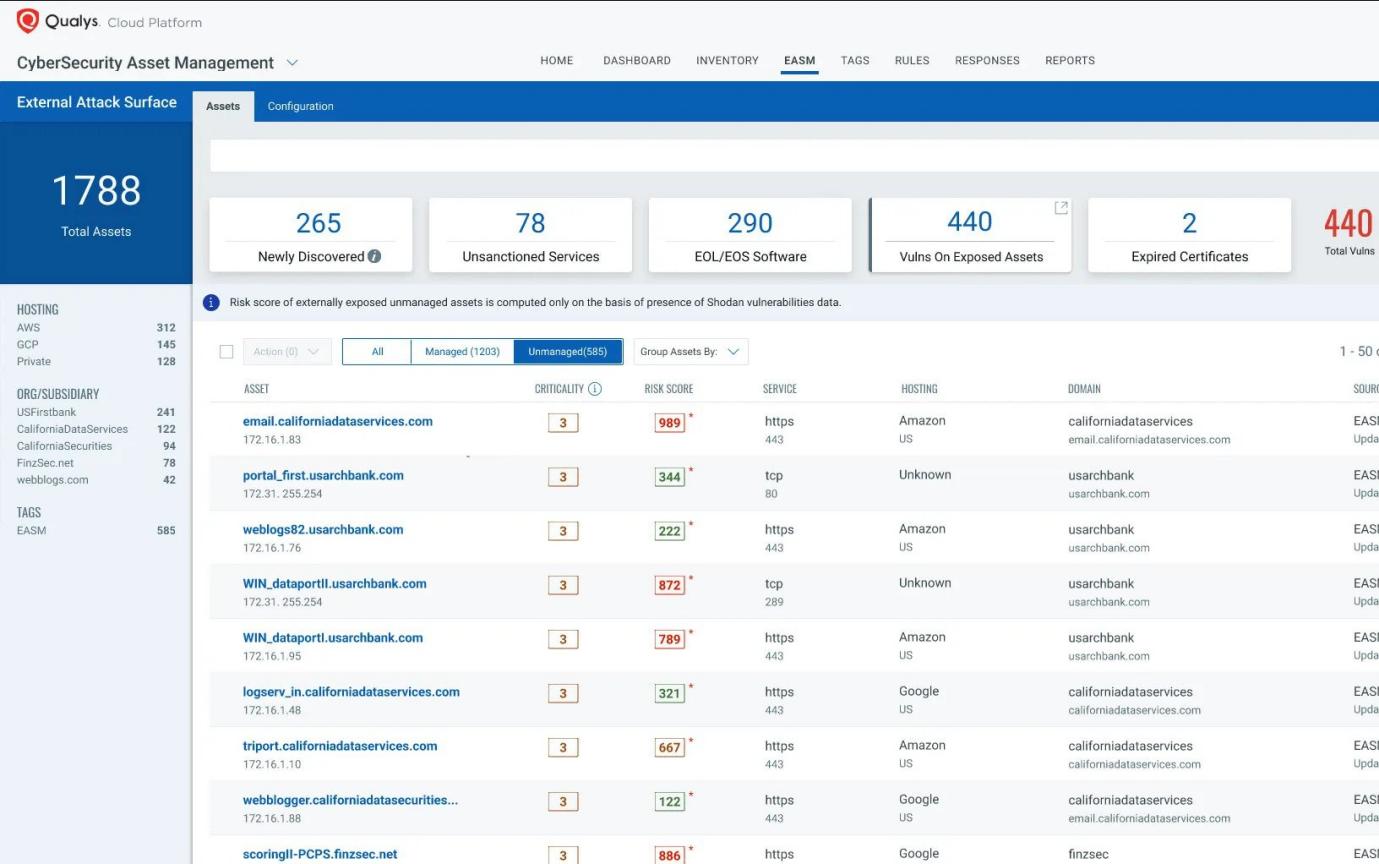
Hình 5. Tính năng quản lý lỗ hổng của Qualys

* Quản lý tuân thủ: Qualys cung cấp khả năng quản lý tuân thủ, bao gồm giám sát tuân thủ chính sách và quy định, để giúp các tổ chức duy trì việc tuân thủ các quy định của ngành và chính phủ.



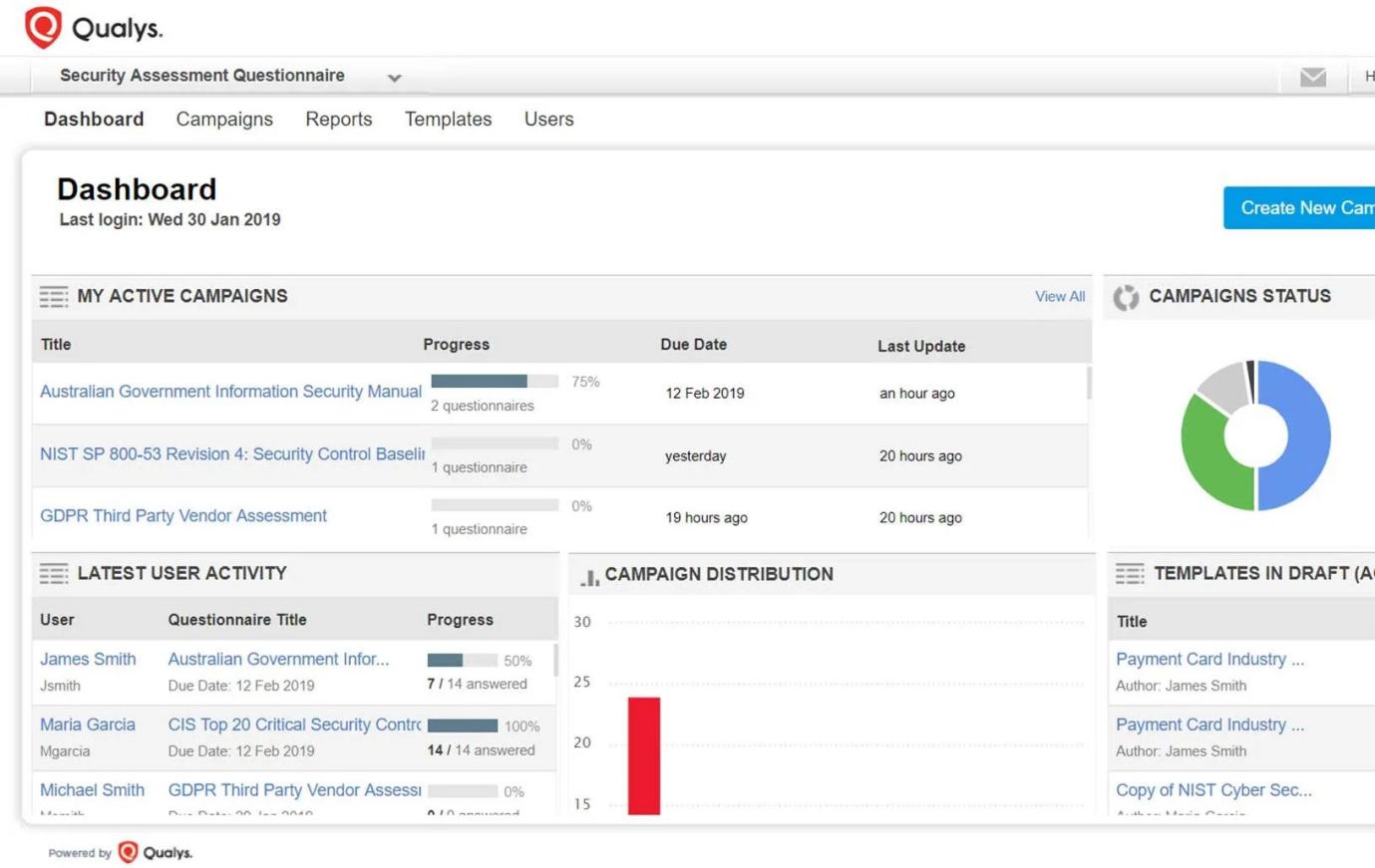
Hình 6. Tính năng quản lý tuân thủ của Qualys

* Quản lý tài sản: Qualys cung cấp khả năng quản lý tài sản, bao gồm quản lý hàng tồn kho và quản lý tài sản phần mềm, để giúp các tổ chức hiểu rõ hơn và quản lý tài sản của họ.



Hình 7. Tính năng quản lý tài sản của Qualys

* Đánh giá bảo mật: Qualys cung cấp khả năng đánh giá bảo mật, bao gồm đánh giá bảo mật mạng và đánh giá bảo mật ứng dụng web, để giúp các tổ chức xác định và giảm thiểu rủi ro bảo mật.



Hình 8. Tính năng đánh giá bảo mật của Qualys

* Báo cáo và phân tích: Qualys cung cấp nhiều khả năng báo cáo và phân tích, cho phép các tổ chức tạo báo cáo và phân tích dữ liệu để hiểu rõ hơn về các hoạt động bảo mật và tuân thủ của họ.

### Ưu điểm

* Dựa trên đám mây: Qualys dựa trên đám mây, do đó không cần cài đặt phần mềm tại chỗ, giảm nỗ lực cần thiết để triển khai và bảo trì nền tảng.
* Tự động hóa: Qualys tự động hóa nhiều quy trình tuân thủ và bảo mật, bao gồm quét lỗ hổng bảo mật, đánh giá bảo mật và quản lý tuân thủ, giúp giảm nỗ lực thủ công và tăng hiệu quả.
* Tích hợp: Qualys tích hợp với các công cụ và hệ thống bảo mật khác, cung cấp cái nhìn toàn diện về tình hình bảo mật của tổ chức và cho phép các nhóm ứng phó với rủi ro và sự cố hiệu quả hơn.
* Khả năng mở rộng: Qualys có khả năng mở rộng cao, vì vậy các tổ chức có thể dễ dàng thêm nhiều tài sản và người dùng hơn khi nhu cầu tuân thủ và bảo mật của họ tăng lên.
* Báo cáo: Qualys cung cấp khả năng báo cáo toàn diện, bao gồm báo cáo theo thời gian thực, báo cáo lịch sử và phân tích xu hướng, cho phép các tổ chức đưa ra quyết định sáng suốt về tình hình tuân thủ và bảo mật của họ.

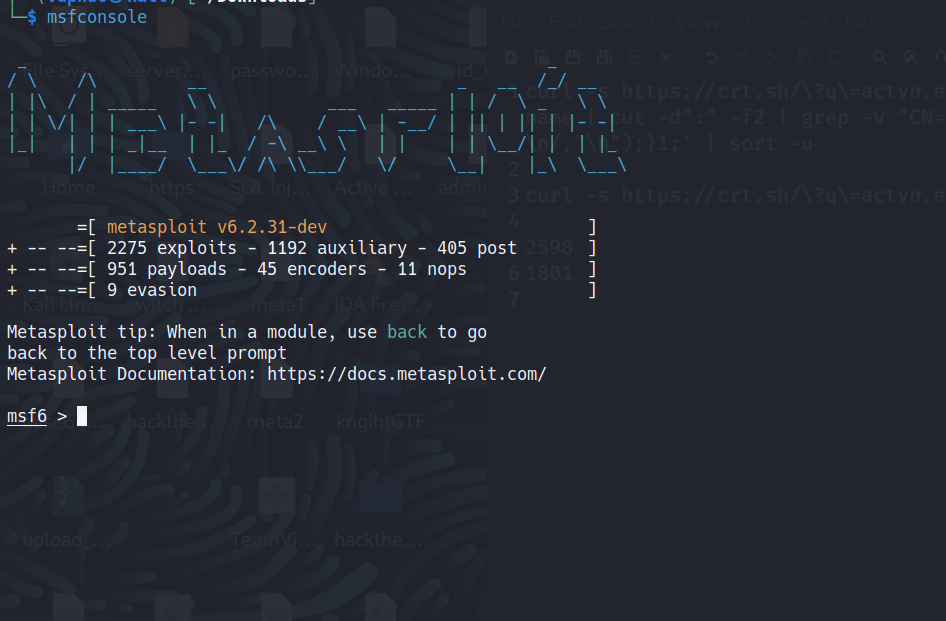
### Nhược điểm

* Chi phí: Qualys có thể tốn kém đối với các tổ chức có ngân sách hạn chế, đặc biệt đối với các tổ chức lớn hơn có nhiều nội dung cần quét.
* Kết quả nhận diện sai: Qualys có thể tạo ra kết quả nhận diện sai, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
* Tùy chỉnh hạn chế: Mặc dù Qualys hỗ trợ cấu hình tùy chỉnh, nhưng có thể có những hạn chế về mức độ nền tảng có thể được tùy chỉnh để đáp ứng nhu cầu cụ thể của tổ chức.
* Hiệu suất: Hiệu suất của Qualys có thể bị ảnh hưởng bởi số lượng nội dung được quét và tần suất quét, điều này có thể dẫn đến chậm và ngừng hoạt động.
* Trải nghiệm người dùng: Trải nghiệm người dùng của Qualys có thể là một thách thức, đặc biệt đối với những người dùng mới sử dụng các công cụ tuân thủ và bảo mật, đồng thời quá trình học tập có thể khó khăn.

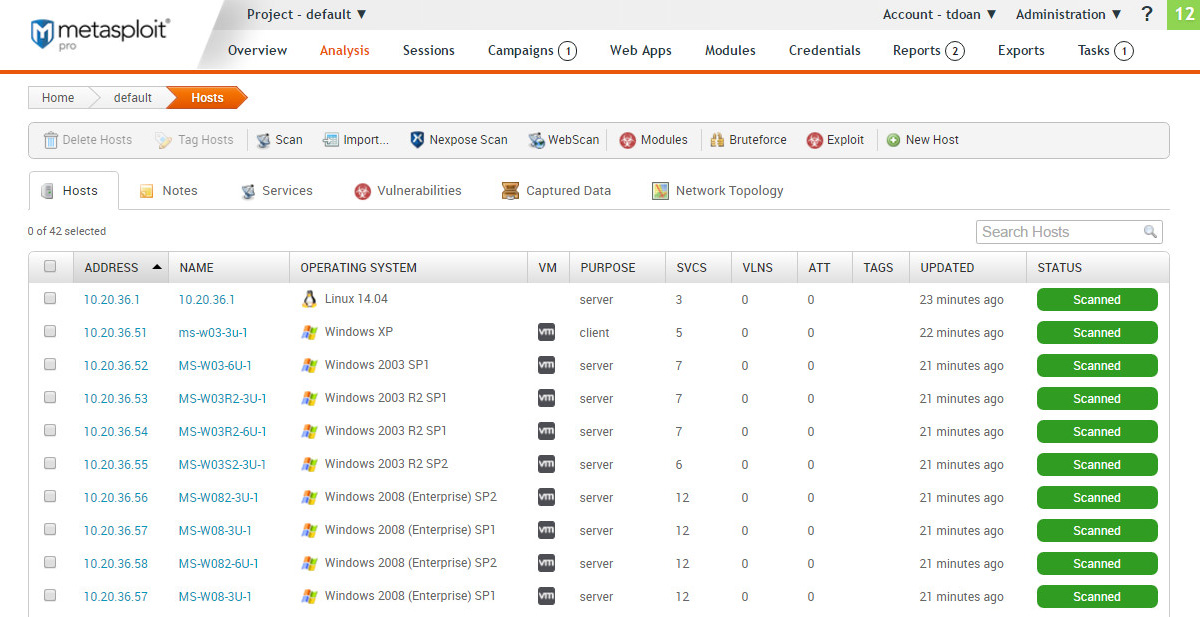
## Metasploit (Công cụ kiểm tra thâm nhập)

### Chi tiết

Chi tiết: Metasploit là nền tảng thử nghiệm bảo mật nguồn mở cung cấp cho các tổ chức giải pháp toàn diện để thử nghiệm thâm nhập và đánh giá lỗ hổng.



Hình 9. Metasploit phiên bản câu lệnh

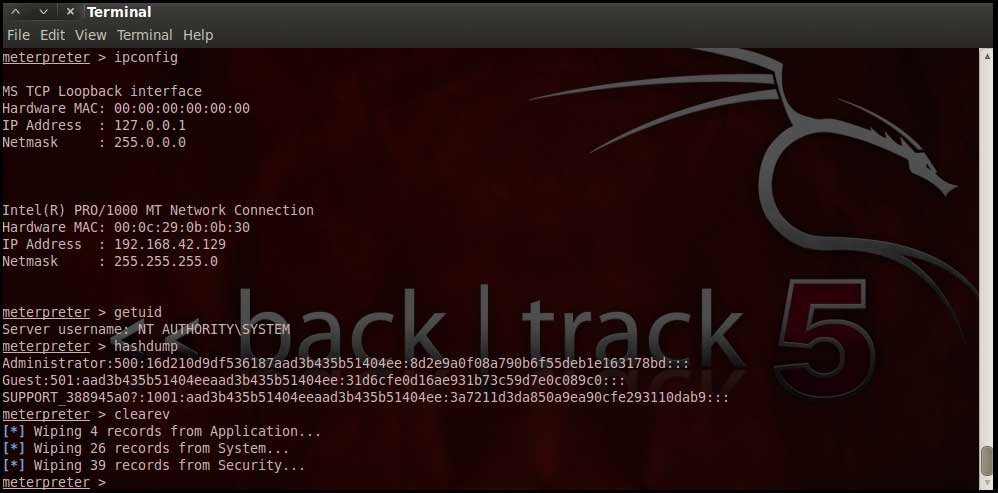


Hình 10. Metasploit phiên bản Pro

Metasploit là phần mềm nguồn mở và miễn phí, làm cho nó trở thành một lựa chọn hấp dẫn cho các tổ chức có ngân sách hạn chế hoặc những người đang tìm kiếm một giải pháp chi phí thấp để kiểm tra bảo mật. Tuy nhiên, hỗ trợ thương mại và các tính năng nâng cao có thể yêu cầu phí cấp phép bổ sung.

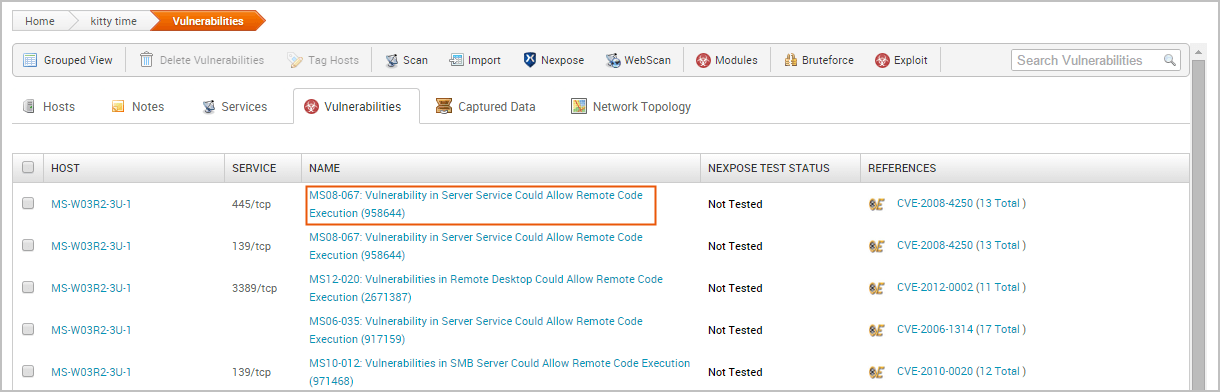
### Tính năng

* Kiểm tra thâm nhập: Metasploit cung cấp khả năng kiểm tra thâm nhập toàn diện, bao gồm kiểm tra thâm nhập mạng và kiểm tra thâm nhập ứng dụng web.



Hình 11. Kiểm tra thâm nhập bằng Metasploit dòng lệnh

* Đánh giá lỗ hổng: Metasploit cung cấp khả năng đánh giá lỗ hổng, bao gồm quét lỗ hổng và khai thác lỗ hổng, để giúp các tổ chức xác định và giảm thiểu rủi ro bảo mật.



Hình 12. Đánh giá lỗ hổng sử dụng Metasploit Pro

* Phát triển khai thác: Metasploit cung cấp khả năng phát triển khai thác, cho phép các nhà nghiên cứu và nhà phát triển bảo mật phát triển và thử nghiệm khai thác các lỗ hổng đã xác định.
* Báo cáo và phân tích: Metasploit cung cấp nhiều khả năng báo cáo và phân tích, bao gồm báo cáo chi tiết về kiểm tra thâm nhập và kết quả đánh giá lỗ hổng.

### Ưu điểm

* Mã nguồn mở: Metasploit là phần mềm mã nguồn mở, có nghĩa là nó được cung cấp miễn phí và có thể được sửa đổi để đáp ứng các nhu cầu cụ thể.
* Cộng đồng lớn: Metasploit có một cộng đồng người dùng và cộng tác viên lớn, dẫn đến việc cập nhật thường xuyên và vô số kiến thức cũng như tài nguyên.
* Tích hợp: Metasploit tích hợp với các công cụ và hệ thống bảo mật khác, cung cấp cái nhìn toàn diện về tình hình bảo mật của tổ chức và cho phép các nhóm ứng phó với rủi ro và sự cố hiệu quả hơn.
* Kiểm tra: Metasploit cho phép các chuyên gia bảo mật và tin tặc có đạo đức kiểm tra các hệ thống và mạng của họ để tìm các lỗ hổng trong một môi trường an toàn và được kiểm soát.
* Tự động hóa: Metasploit tự động hóa nhiều quy trình kiểm tra bảo mật, giảm nỗ lực thủ công và tăng hiệu quả.

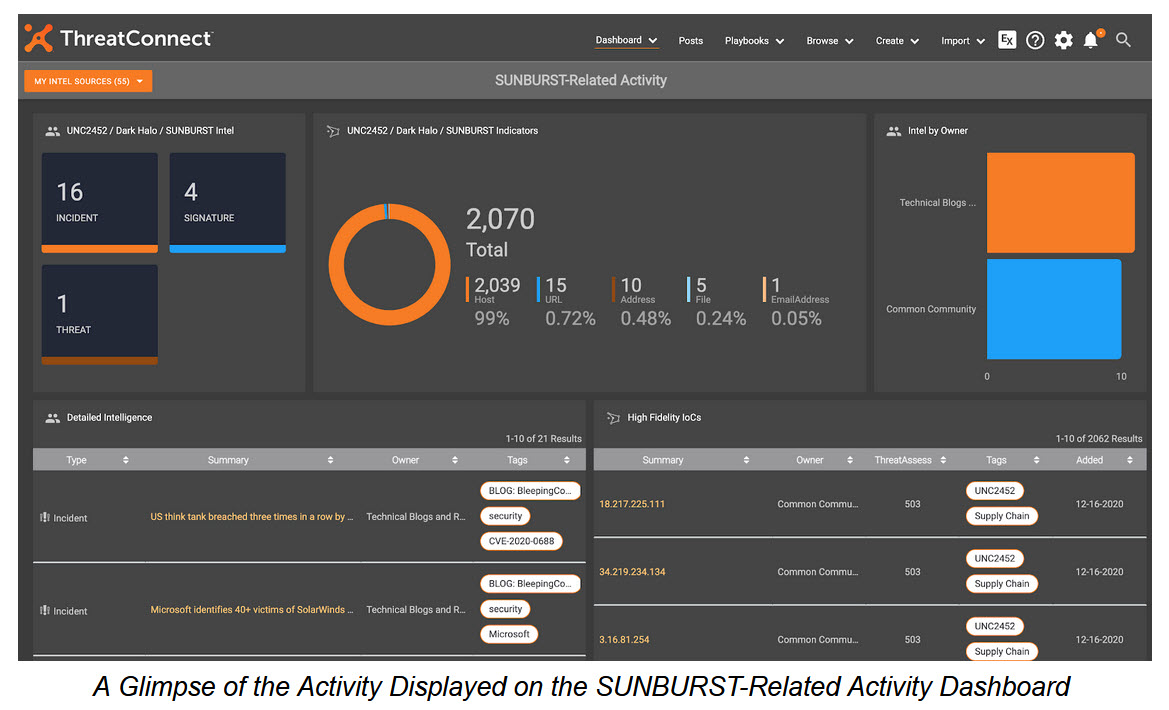
### Nhược điểm

* Độ phức tạp: Metasploit là một nền tảng phức tạp và đường cong học tập có thể dốc, đặc biệt đối với những người dùng mới thử nghiệm bảo mật.
* Thiếu hỗ trợ: Metasploit là phần mềm nguồn mở, có nghĩa là không có hỗ trợ thương mại.
* Nguy cơ lạm dụng: Metasploit có thể được sử dụng một cách độc hại để khai thác các lỗ hổng, vì vậy điều quan trọng là phải sử dụng nền tảng một cách có trách nhiệm và chỉ trong các môi trường an toàn và được kiểm soát.
* Kết quả nhận diện sai: Metasploit có thể tạo ra kết quả nhận diện sai, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
* Hiệu suất: Hiệu suất của Metasploit có thể bị ảnh hưởng bởi số lượng nội dung được kiểm tra và mức độ phức tạp của các bài kiểm tra, điều này có thể dẫn đến tình trạng chậm lại và ngừng hoạt động.

## ThreatConnect (Nền tảng tình báo mối đe dọa)

### Chi tiết

ThreatConnect là một nền tảng tình báo về mối đe dọa cung cấp cho các tổ chức một giải pháp tập trung để quản lý và phân tích dữ liệu tình báo về mối đe dọa.



Hình 13. Giao diện ThreatConnect

Chi phí của ThreatConnect thay đổi tùy thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức, nhưng nó thường bắt đầu ở mức khoảng 10.000 đô la mỗi năm cho triển khai cơ bản và mở rộng quy mô cho các triển khai lớn hơn hoặc khả năng nâng cao. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai cũng như các tính năng và khả năng cụ thể được yêu cầu.

### Tính năng

* Quản lý thông tin về mối đe dọa: ThreatConnect cung cấp một nền tảng tập trung để quản lý và phân tích dữ liệu thông minh về mối đe dọa, bao gồm khả năng thu thập, lưu trữ và phân tích dữ liệu thông minh về mối đe dọa từ nhiều nguồn.
* Phân tích mối đe dọa: ThreatConnect cung cấp khả năng phân tích mối đe dọa nâng cao, bao gồm khả năng tiến hành phân tích chuyên sâu về dữ liệu mối đe dọa để xác định các mối đe dọa tiềm ẩn và hiểu tác động của các mối đe dọa này đối với tổ chức.
* Cộng tác: ThreatConnect cung cấp khả năng cộng tác, cho phép các tổ chức chia sẻ dữ liệu và thông tin tình báo về mối đe dọa với các tổ chức khác hoặc với người dùng cá nhân.
* Tích hợp: ThreatConnect tích hợp với nhiều giải pháp CNTT và bảo mật, bao gồm giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), giải pháp phát hiện mối đe dọa và giải pháp phối hợp bảo mật, tự động hóa và phản hồi (SOAR).

### Ưu điểm

* + - Thông tin về mối đe dọa: ThreatConnect cung cấp cho các tổ chức cái nhìn toàn diện về tình trạng thông minh về mối đe dọa của họ, cho phép các nhóm xác định và ứng phó với các mối đe dọa nhanh chóng và hiệu quả hơn.
    - Tích hợp: ThreatConnect tích hợp với các công cụ và hệ thống bảo mật khác, cung cấp một nguồn thông tin chính xác duy nhất cho dữ liệu tình báo về mối đe dọa và cho phép các nhóm ứng phó với rủi ro và sự cố hiệu quả hơn.
    - Tự động hóa: ThreatConnect tự động hóa nhiều quy trình thông minh về mối đe dọa, giảm nỗ lực thủ công và tăng hiệu quả.
    - Khả năng mở rộng: ThreatConnect có khả năng mở rộng cao, vì vậy các tổ chức có thể dễ dàng thêm nhiều người dùng và nguồn dữ liệu tình báo về mối đe dọa hơn khi nhu cầu của họ tăng lên.
    - Trải nghiệm người dùng: ThreatConnect cung cấp giao diện thân thiện với người dùng, giúp người dùng quản lý và phân tích dữ liệu tình báo về mối đe dọa dễ dàng hơn.

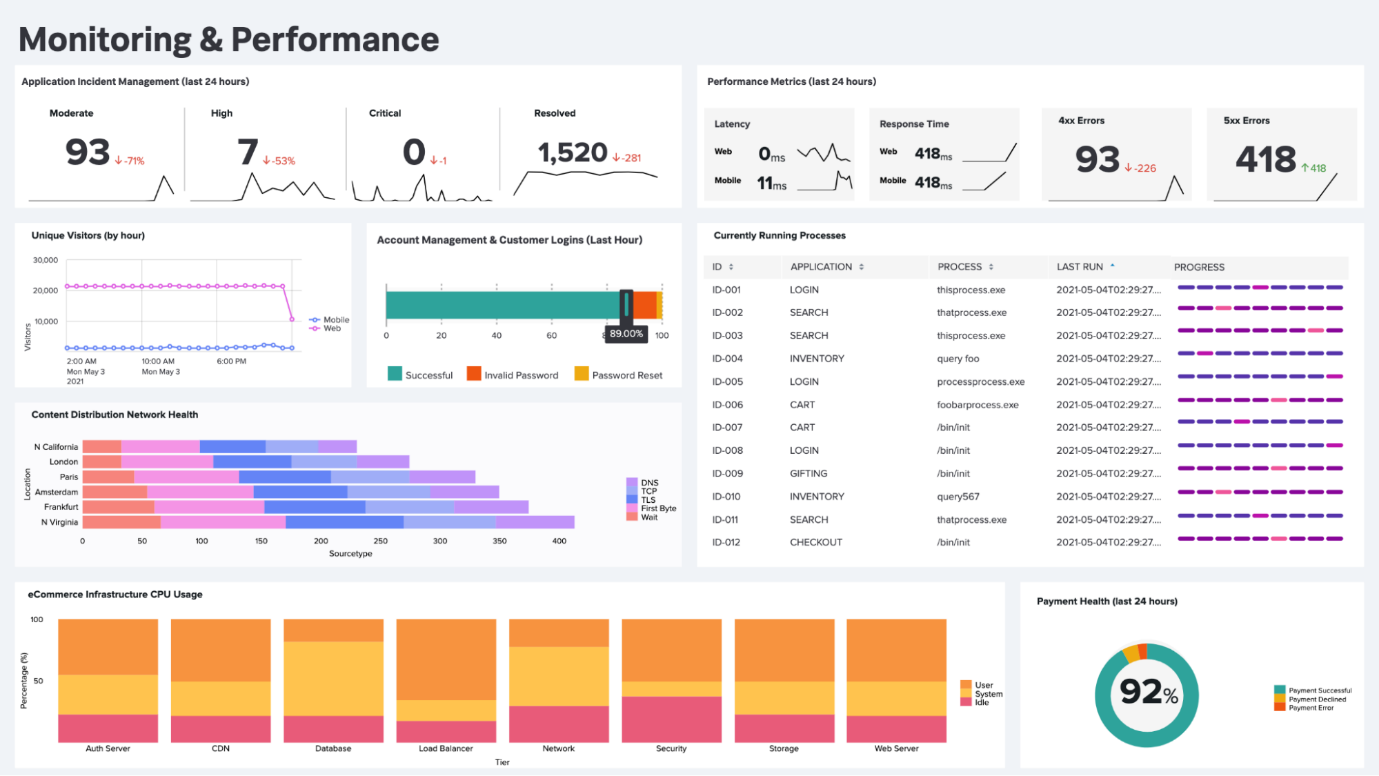
### Nhược điểm

* + - Chi phí: ThreatConnect có thể tốn kém đối với các tổ chức có ngân sách hạn chế, đặc biệt là đối với các tổ chức lớn hơn có nhiều người dùng và nguồn dữ liệu tình báo về mối đe dọa.
    - Kết quả nhận diện sai: ThreatConnect có thể tạo ra kết quả nhận diện sai, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
    - Tùy chỉnh hạn chế: Mặc dù ThreatConnect hỗ trợ cấu hình tùy chỉnh, nhưng có thể có những hạn chế về mức độ nền tảng có thể được tùy chỉnh để đáp ứng nhu cầu cụ thể của tổ chức.
    - Hiệu suất: Hiệu suất của ThreatConnect có thể bị ảnh hưởng bởi khối lượng dữ liệu thông minh về mối đe dọa đang được xử lý, điều này có thể dẫn đến tình trạng chậm và ngừng hoạt động.
    - Trải nghiệm người dùng: Trải nghiệm người dùng của ThreatConnect có thể là một thách thức, đặc biệt đối với những người dùng chưa quen với các nền tảng tình báo về mối đe dọa và quá trình học tập có thể dốc

## Splunk (Hệ thống quản lý sự kiện và thông tin bảo mật (SIEM))

### Chi tiết

Splunk là một nền tảng phân tích nhật ký và dữ liệu máy cung cấp cho các tổ chức một giải pháp tập trung để thu thập, phân tích và trực quan hóa khối lượng lớn dữ liệu máy.

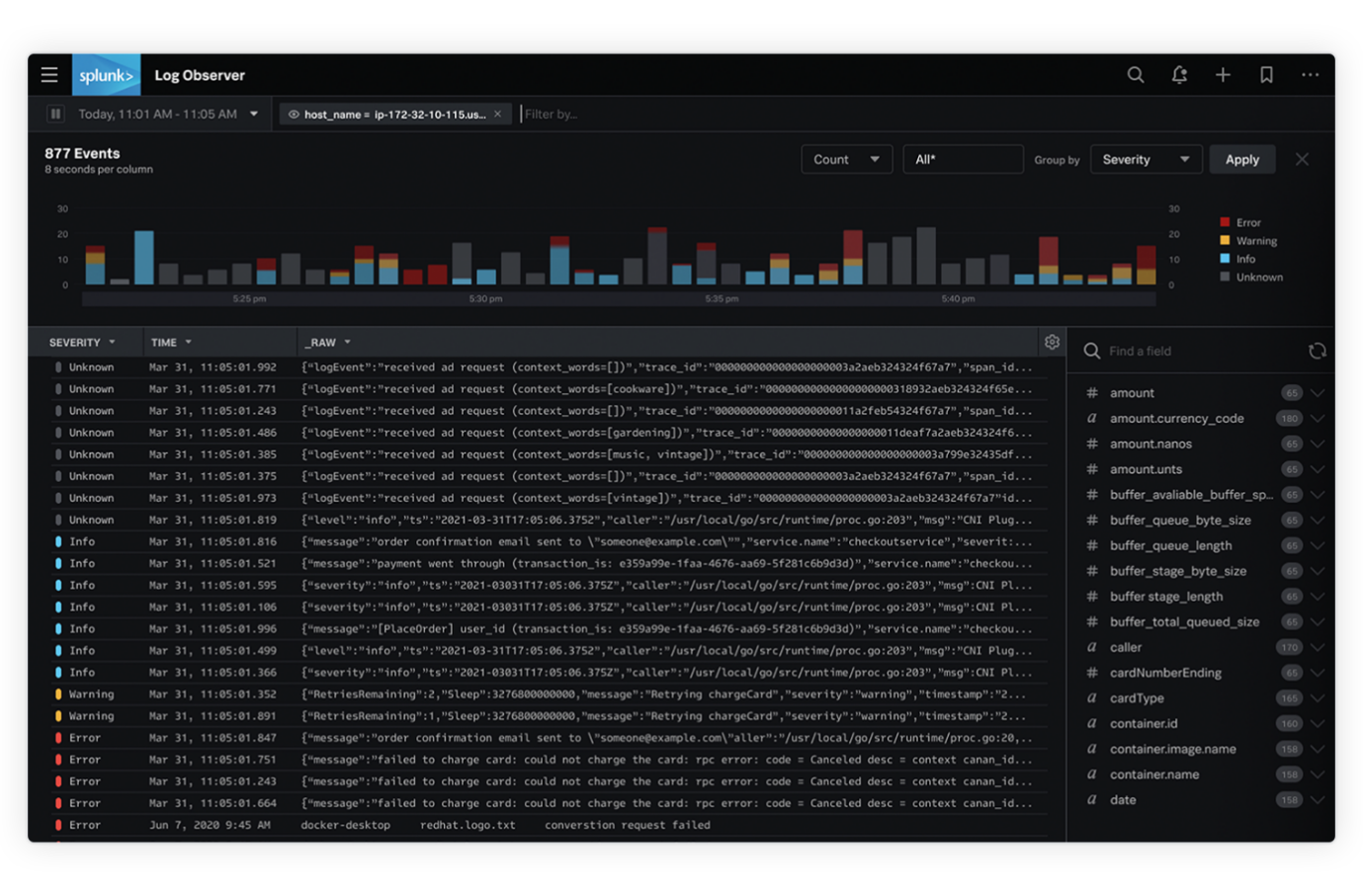


Hình 14. Giao diện Spunk

Chi phí của Splunk phụ thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức, nhưng nó thường bắt đầu ở mức khoảng 150 USD/người dùng/năm cho triển khai cơ bản và mở rộng quy mô cho các triển khai lớn hơn hoặc khả năng nâng cao. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai, các tính năng và khả năng cụ thể được yêu cầu cũng như mức độ hỗ trợ cần thiết.

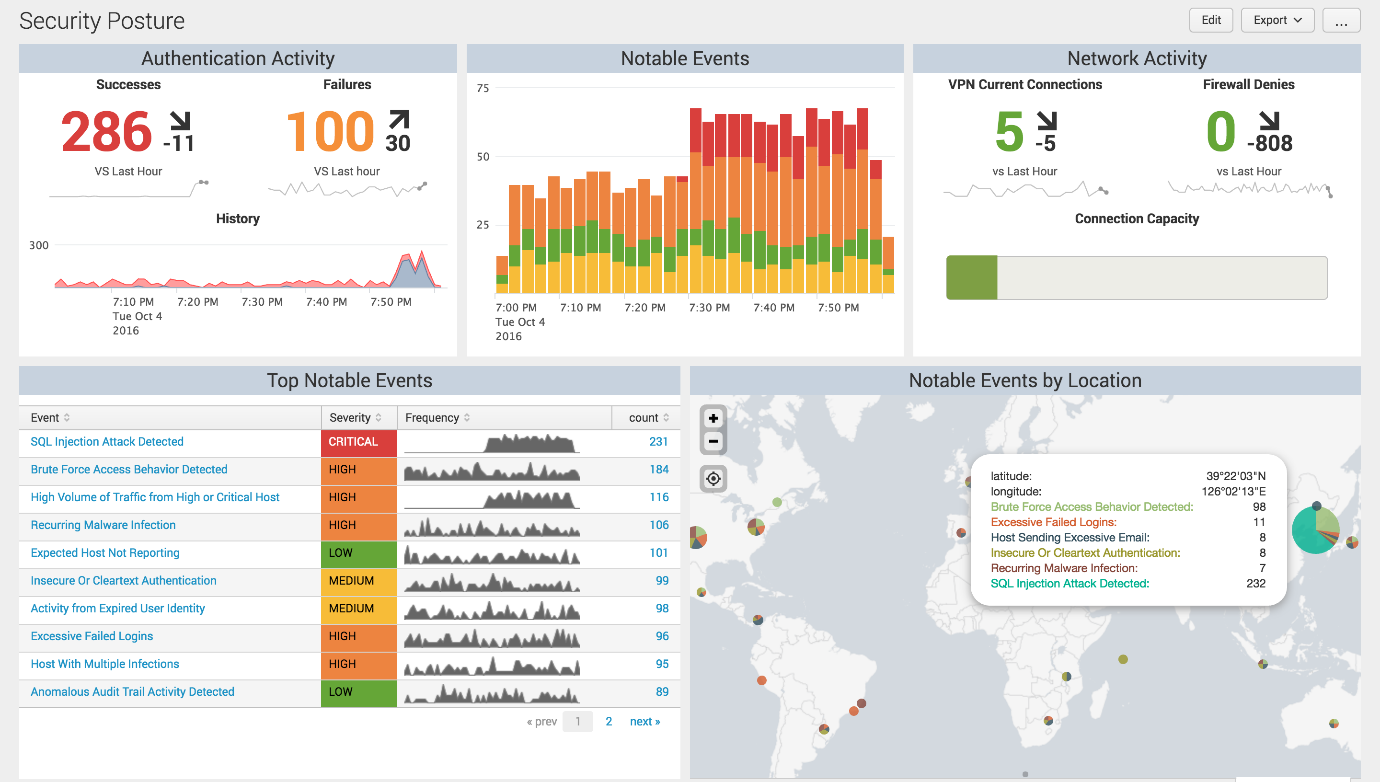
### Tính năng

* Quản lý và phân tích nhật ký: Splunk cung cấp khả năng quản lý và phân tích nhật ký, cho phép các tổ chức thu thập, lập chỉ mục và phân tích khối lượng lớn dữ liệu máy từ nhiều nguồn khác nhau.



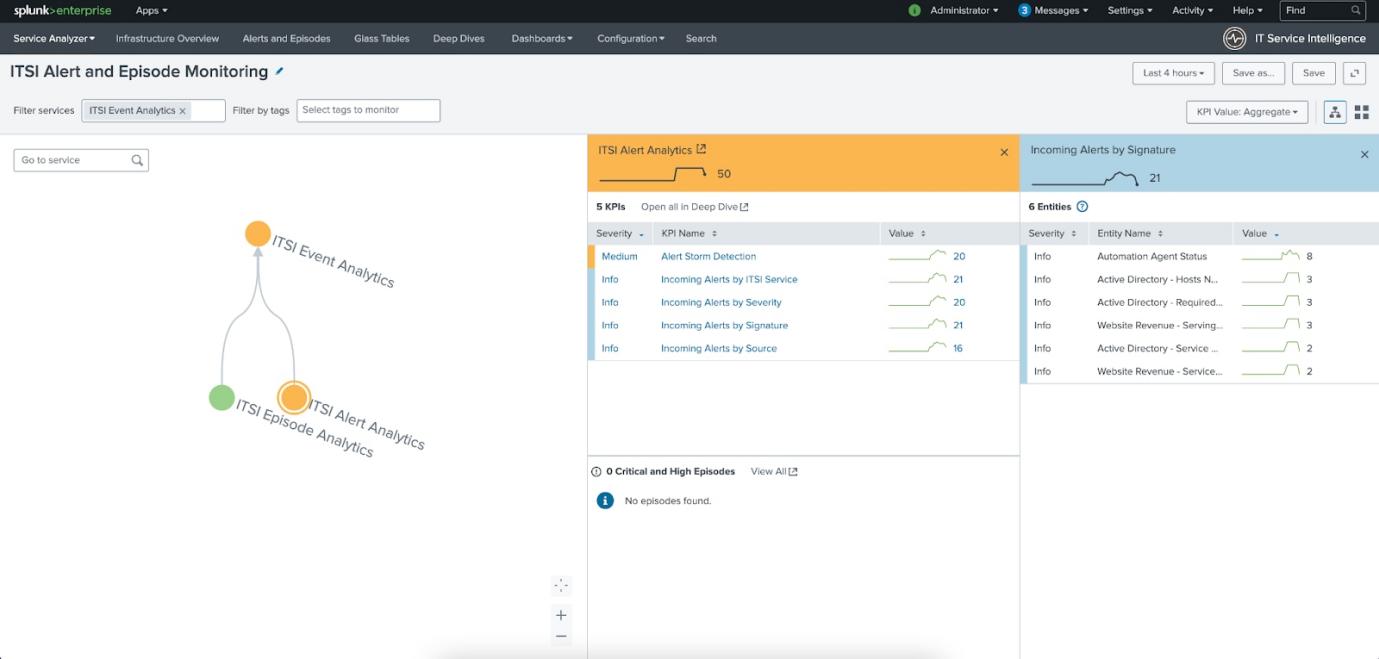
Hình 15. Tính năng quản lý và phân tích nhật ký của Splunk

* Trực quan hóa dữ liệu máy: Splunk cung cấp khả năng trực quan hóa dữ liệu máy, bao gồm khả năng trực quan hóa dữ liệu máy trong thời gian thực, tạo bảng điều khiển tương tác và tạo báo cáo tùy chỉnh.



Hình 16. Tính năng trực quan hoá dữ liệu máy của Splunk

* Cảnh báo và giám sát: Splunk cung cấp khả năng cảnh báo và giám sát, cho phép các tổ chức giám sát dữ liệu máy trong thời gian thực, để phát hiện các sự cố bảo mật và phản hồi chúng một cách nhanh chóng và hiệu quả.



Hình 17. Tính năng cảnh báo và giám sát của Slunk

* Tích hợp: Splunk tích hợp với nhiều giải pháp CNTT và bảo mật, bao gồm giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), giải pháp phát hiện mối đe dọa và giải pháp phối hợp bảo mật, tự động hóa và phản hồi (SOAR).
* Học máy: Splunk cung cấp khả năng học máy, bao gồm khả năng sử dụng các thuật toán học máy để phân tích dữ liệu máy và xác định các mẫu cũng như mối tương quan.

### Ưu điểm

* + - Phân tích dữ liệu lớn: Splunk cung cấp cho các tổ chức cái nhìn toàn diện về dữ liệu lớn của họ, cho phép các nhóm xác định và ứng phó với các rủi ro bảo mật cũng như các vấn đề về hiệu suất nhanh chóng và hiệu quả hơn.
    - Tích hợp: Splunk tích hợp với các công cụ và hệ thống quản lý hiệu suất và bảo mật khác, cung cấp một nguồn thông tin chính xác duy nhất cho dữ liệu máy và cho phép các nhóm ứng phó với rủi ro và sự cố hiệu quả hơn.
    - Tự động hóa: Splunk tự động hóa nhiều quy trình phân tích dữ liệu lớn, giảm nỗ lực thủ công và tăng hiệu quả.
    - Khả năng mở rộng: Splunk có khả năng mở rộng cao, vì vậy các tổ chức có thể dễ dàng thêm nhiều nguồn dữ liệu và người dùng hơn khi nhu cầu của họ tăng lên.
    - Trải nghiệm người dùng: Splunk cung cấp giao diện thân thiện với người dùng, giúp người dùng quản lý và phân tích dữ liệu máy dễ dàng hơn.

### Nhược điểm

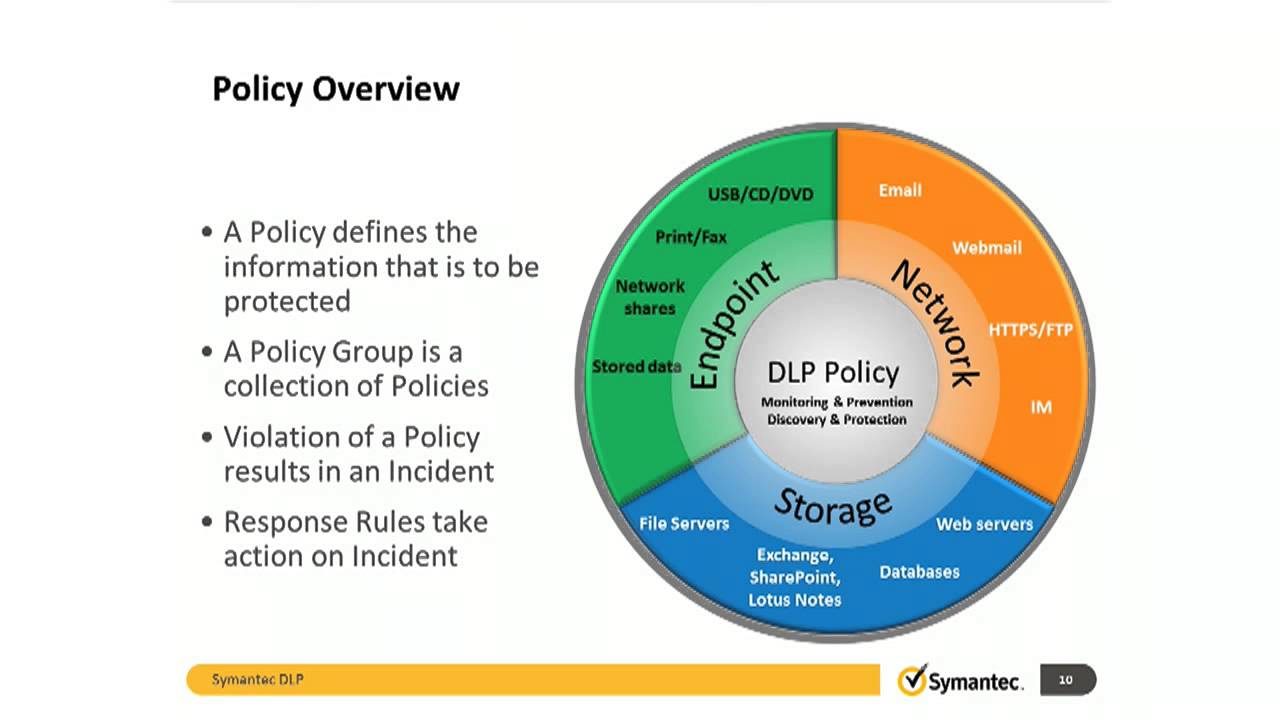
* + - Chi phí: Splunk có thể tốn kém đối với các tổ chức có ngân sách hạn chế, đặc biệt đối với các tổ chức lớn hơn có nhiều nguồn dữ liệu và người dùng.
    - Kết quả dương tính giả: Splunk có thể tạo ra kết quả dương tính giả, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
    - Độ phức tạp: Splunk là một nền tảng phức tạp và đường cong học tập có thể dốc, đặc biệt đối với người dùng chưa quen với phân tích dữ liệu lớn.
    - Hiệu suất: Hiệu suất của Splunk có thể bị ảnh hưởng bởi khối lượng dữ liệu máy đang được xử lý, điều này có thể dẫn đến chậm và ngừng hoạt động.
    - Tích hợp: Mặc dù Splunk tích hợp với các công cụ và hệ thống khác, mức độ tích hợp có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để tận dụng tối đa nền tảng.

## Symantec DLP (Giải pháp ngăn ngừa mất dữ liệu (DLP))

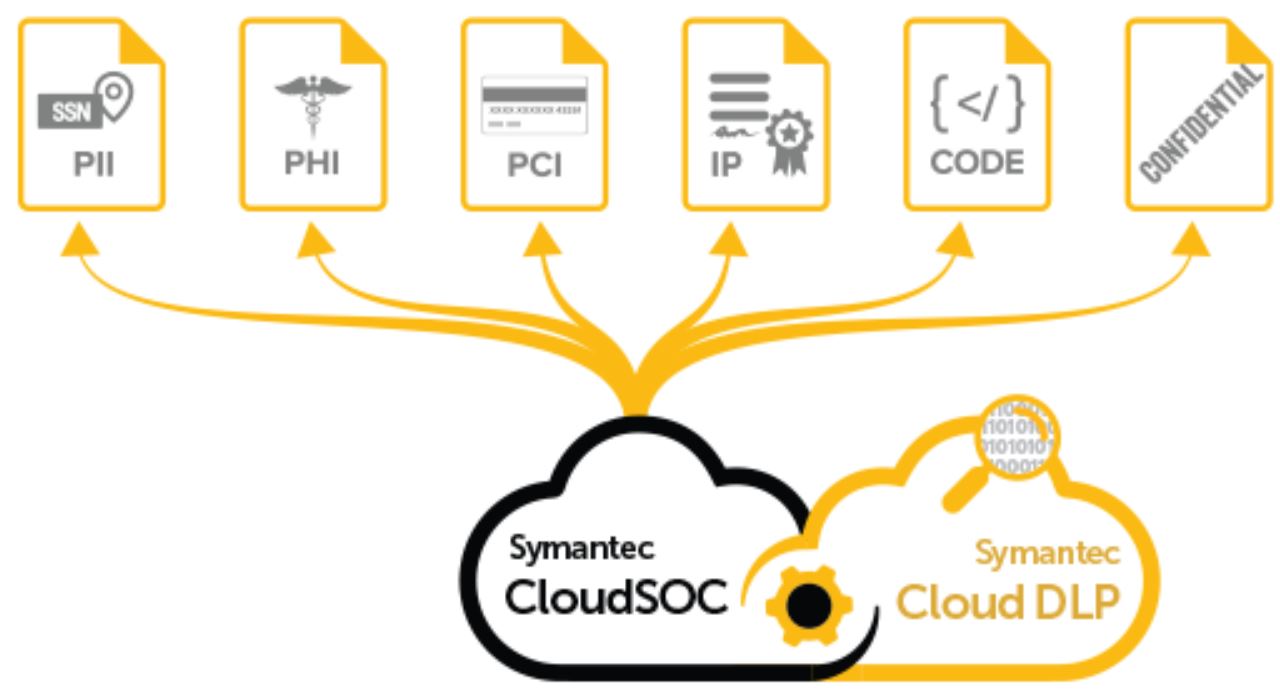
### Chi tiết

Symantec Data Loss Prevention (DLP) là một giải pháp bảo vệ dữ liệu giúp các tổ chức ngăn ngừa dữ liệu nhạy cảm bị mất hoặc bị đánh cắp.

Chi phí của Symantec DLP khác nhau tùy thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức, nhưng nó thường bắt đầu ở mức khoảng 50 USD/người dùng/năm đối với triển khai cơ bản và mở rộng quy mô cho các triển khai lớn hơn hoặc khả năng nâng cao. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai, các tính năng và khả năng cụ thể được yêu cầu cũng như mức độ hỗ trợ cần thiết.



Hình 18: Tổng quan chính sách



Hình 19: Tích hợp Symantec DLP với Microsoft Information Protection

### Tính năng

* + - Khám phá dữ liệu: Symantec DLP cung cấp khả năng khám phá dữ liệu, cho phép các tổ chức định vị và xác định dữ liệu nhạy cảm trong mạng và điểm cuối của họ.
    - Phân loại dữ liệu: Symantec DLP cung cấp khả năng phân loại dữ liệu, cho phép các tổ chức phân loại dữ liệu nhạy cảm và áp dụng các mức bảo vệ khác nhau cho các loại dữ liệu khác nhau.
    - Bảo vệ dữ liệu: Symantec DLP cung cấp khả năng bảo vệ dữ liệu, bao gồm khả năng mã hóa dữ liệu nhạy cảm, theo dõi và kiểm soát luồng dữ liệu nhạy cảm cũng như ngăn dữ liệu nhạy cảm bị mất hoặc bị đánh cắp.
    - Tuân thủ: Symantec DLP cung cấp khả năng tuân thủ, giúp các tổ chức đáp ứng các tiêu chuẩn và quy định bảo vệ dữ liệu, bao gồm GDPR, HIPAA và PCI DSS.
    - Tích hợp: Symantec DLP tích hợp với nhiều giải pháp CNTT và bảo mật, bao gồm giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), giải pháp phát hiện mối đe dọa và giải pháp phối hợp bảo mật, tự động hóa và phản hồi (SOAR).
    - Phát hiện mối đe dọa: Symantec DLP cung cấp khả năng phát hiện mối đe dọa, bao gồm khả năng phát hiện và ngăn chặn vi phạm dữ liệu cũng như xác định và ứng phó với các sự cố bảo mật.

### Ưu điểm

* + - Bảo vệ dữ liệu: Symantec DLP cung cấp cho các tổ chức giải pháp toàn diện để bảo vệ dữ liệu nhạy cảm, giảm nguy cơ vi phạm dữ liệu và đảm bảo tuân thủ các quy định như GDPR.
    - Thực thi chính sách: Symantec DLP cung cấp cho các tổ chức một bộ công cụ để quản lý và thực thi các chính sách bảo mật dữ liệu, giảm nguy cơ truy cập trái phép, sử dụng hoặc đánh cắp dữ liệu nhạy cảm.
    - Tích hợp: Symantec DLP tích hợp với các công cụ và hệ thống bảo mật khác, cung cấp cái nhìn toàn diện về tình trạng bảo mật của tổ chức và cho phép các nhóm ứng phó với rủi ro và sự cố hiệu quả hơn.
    - Giao diện thân thiện với người dùng: Symantec DLP có giao diện thân thiện với người dùng, giúp người dùng dễ dàng quản lý và thực thi các chính sách bảo mật dữ liệu.
    - Khả năng mở rộng: Symantec DLP có khả năng mở rộng cao, vì vậy các tổ chức có thể dễ dàng thêm nhiều người dùng và nguồn dữ liệu hơn khi nhu cầu của họ tăng lên.

### Nhược điểm

* + - Chi phí: Symantec DLP có thể tốn kém, đặc biệt đối với các tổ chức có ngân sách hạn chế hoặc đối với những tổ chức có số lượng lớn người dùng hoặc nguồn dữ liệu.
    - Độ phức tạp: Symantec DLP có thể là một giải pháp phức tạp và đường cong học tập có thể dốc, đặc biệt đối với người dùng chưa quen với việc ngăn ngừa mất dữ liệu.
    - Kết quả dương tính giả: Symantec DLP có thể tạo ra kết quả dương tính giả, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
    - Tích hợp: Mặc dù Symantec DLP tích hợp với các công cụ và hệ thống bảo mật khác, mức độ tích hợp có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để tận dụng tối đa giải pháp.
    - Hiệu suất: Hiệu suất của Symantec DLP có thể bị ảnh hưởng bởi khối lượng dữ liệu được xử lý, điều này có thể dẫn đến chậm và thời gian ngừng hoạt động.

## Microsoft Defender ATP (Công cụ đánh giá trạng thái bảo mật)

### Chi tiết

Tính năng Chống Mối đe dọa Nâng cao của Bộ bảo vệ Microsoft (ATP) là một giải pháp bảo mật điểm cuối cung cấp cho các tổ chức khả năng bảo vệ chống lại các mối đe dọa nâng cao, bao gồm cả phần mềm độc hại và các sự cố bảo mật khác.

Chi phí của ATP của Bộ bảo vệ Microsoft thay đổi tùy theo nhu cầu và yêu cầu cụ thể của tổ chức, nhưng nó thường được bao gồm như một phần của bộ Enterprise Mobility + Security (EMS) của Microsoft hoặc dưới dạng một dịch vụ độc lập. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai, các tính năng và khả năng cụ thể được yêu cầu cũng như mức độ hỗ trợ cần thiết.



Hình 20: Microsoft Defender for Endpoint

### Tính năng

* + - Bảo vệ điểm cuối: ATP của Bộ bảo vệ Microsoft cung cấp khả năng bảo vệ điểm cuối, bao gồm bảo vệ thời gian thực chống lại phần mềm độc hại và các sự cố bảo mật khác.
    - Thông tin về Mối đe dọa: ATP của Bộ bảo vệ Microsoft cung cấp các chức năng thông tin về mối đe dọa, bao gồm khả năng phát hiện và ứng phó với các mối đe dọa mới và đang phát triển.
    - Tìm kiếm mối đe dọa: ATP của Bộ bảo vệ Microsoft cung cấp khả năng tìm kiếm mối đe dọa, cho phép các nhóm bảo mật chủ động tìm kiếm và ứng phó với các sự cố bảo mật.
    - Điều tra và ứng phó: ATP của Bộ bảo vệ Microsoft cung cấp các khả năng điều tra và ứng phó, bao gồm khả năng thực hiện điều tra pháp y, ứng phó với các sự cố bảo mật và ngăn chặn các mối đe dọa bảo mật.
    - Tích hợp: ATP của Bộ bảo vệ Microsoft tích hợp với nhiều giải pháp CNTT và bảo mật, bao gồm giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), giải pháp phát hiện mối đe dọa và giải pháp điều phối, tự động hóa và phản hồi (SOAR) bảo mật.
    - Quản lý dựa trên đám mây: Microsoft Defender ATP là giải pháp dựa trên đám mây, cung cấp khả năng quản lý và báo cáo tập trung cho các tổ chức có nhiều điểm cuối.

### Ưu điểm

* + - Tích hợp: ATP của Bộ bảo vệ Microsoft tích hợp với các công cụ và hệ thống bảo mật khác của Microsoft, chẳng hạn như Microsoft 365 và Azure, mang đến cái nhìn toàn diện về tình hình bảo mật của một tổ chức.
    - Bảo mật điểm cuối: ATP của Bộ bảo vệ Microsoft cung cấp cho các tổ chức khả năng bảo mật điểm cuối toàn diện, bao gồm khả năng bảo vệ theo thời gian thực chống lại phần mềm độc hại và vi rút.
    - Bảo mật đám mây: ATP của Bộ bảo vệ Microsoft cung cấp cho các tổ chức khả năng bảo mật đám mây, bao gồm khả năng bảo vệ chống lại các cuộc tấn công vào dữ liệu và hệ thống dựa trên đám mây.
    - Giao diện thân thiện với người dùng: Microsoft Defender ATP có giao diện thân thiện với người dùng, giúp người dùng dễ dàng quản lý và thực thi các chính sách bảo mật.
    - Khả năng mở rộng: ATP của Bộ bảo vệ Microsoft có khả năng mở rộng cao, vì vậy các tổ chức có thể dễ dàng thêm nhiều người dùng và thiết bị hơn khi nhu cầu của họ tăng lên.

### Nhược điểm

* + - Tích hợp hạn chế: Mặc dù ATP của Bộ bảo vệ Microsoft tích hợp với các công cụ và hệ thống bảo mật khác của Microsoft, mức độ tích hợp có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để tận dụng tối đa giải pháp.
    - Kết quả dương tính giả: ATP của Bộ bảo vệ Microsoft có thể tạo ra kết quả dương tính giả, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
    - Hiệu suất: Hiệu suất của ATP của Bộ bảo vệ Microsoft có thể bị ảnh hưởng bởi khối lượng dữ liệu được xử lý, điều này có thể dẫn đến tình trạng chậm và ngừng hoạt động.
    - Độ phức tạp: ATP của Bộ bảo vệ Microsoft có thể là một giải pháp phức tạp và quá trình học hỏi có thể khó khăn, đặc biệt đối với người dùng mới sử dụng các giải pháp bảo mật.
    - Chi phí: ATP của Bộ bảo vệ Microsoft có thể tốn kém đối với các tổ chức có ngân sách hạn chế, đặc biệt đối với những tổ chức có số lượng lớn người dùng hoặc thiết bị.

## Checkmarx (Công cụ kiểm tra bảo mật ứng dụng)

### Chi tiết

Checkmarx là một giải pháp bảo mật phần mềm giúp các tổ chức xác định và khắc phục các lỗ hổng bảo mật trong ứng dụng của họ.

Chi phí của Checkmarx khác nhau tùy thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức, nhưng nó thường bắt đầu ở mức khoảng 5.000 đô la mỗi năm cho triển khai cơ bản và mở rộng quy mô cho các triển khai lớn hơn hoặc khả năng nâng cao. Chi phí chính xác sẽ phụ thuộc vào quy mô triển khai, các tính năng và khả năng cụ thể được yêu cầu cũng như mức độ hỗ trợ cần thiết.

### Tính năng

* + - Kiểm tra bảo mật ứng dụng: Checkmarx cung cấp khả năng kiểm tra bảo mật ứng dụng, bao gồm phân tích mã tĩnh, kiểm tra bảo mật ứng dụng động (DAST) và kiểm tra bảo mật ứng dụng tương tác (IAST).
    - Quản lý lỗ hổng: Checkmarx cung cấp khả năng quản lý lỗ hổng, bao gồm khả năng xác định, ưu tiên và khắc phục lỗ hổng bảo mật trong ứng dụng.
    - Tích hợp: Checkmarx tích hợp với một loạt các công cụ và quy trình phát triển, bao gồm các công cụ vòng đời phát triển phần mềm (SDLC), công cụ quản lý mã nguồn (SCM) và các công cụ tích hợp/phân phối liên tục (CI/CD) liên tục.
    - Báo cáo và phân tích: Checkmarx cung cấp khả năng báo cáo và phân tích, bao gồm các báo cáo và bảng điều khiển có thể tùy chỉnh để cung cấp khả năng hiển thị trạng thái bảo mật của ứng dụng.
    - Phát hiện mối đe dọa: Checkmarx cung cấp khả năng phát hiện mối đe dọa, bao gồm khả năng phát hiện và ứng phó với các mối đe dọa mới và đang phát triển.
    - Tự động hóa: Checkmarx cung cấp các khả năng tự động hóa, bao gồm khả năng tự động hóa quy trình kiểm tra bảo mật và quản lý lỗ hổng.

### Ưu điểm

* + - Phân tích mã: Checkmarx cung cấp cho các tổ chức giải pháp phân tích mã toàn diện, bao gồm quét thời gian thực để tìm các lỗ hổng và vấn đề bảo mật.
    - Kiểm tra bảo mật ứng dụng: Checkmarx cung cấp cho các tổ chức giải pháp kiểm tra bảo mật ứng dụng toàn diện, bao gồm kiểm tra tự động và thủ công, để giúp các tổ chức xác định và giải quyết các vấn đề bảo mật.
    - Phân tích thành phần phần mềm: Checkmarx cung cấp cho các tổ chức giải pháp phân tích thành phần phần mềm toàn diện, giúp các tổ chức xác định và giải quyết các lỗ hổng và vấn đề bảo mật trong các thành phần phần mềm của bên thứ ba.
    - Giao diện thân thiện với người dùng: Checkmarx có giao diện thân thiện với người dùng, giúp người dùng dễ dàng quản lý và thực thi các chính sách bảo mật.
    - Tích hợp: Checkmarx tích hợp với các công cụ và hệ thống bảo mật khác, chẳng hạn như các đường ống tích hợp liên tục và triển khai liên tục (CI/CD), cung cấp một cái nhìn toàn diện về tình hình bảo mật của một tổ chức.

### Nhược điểm

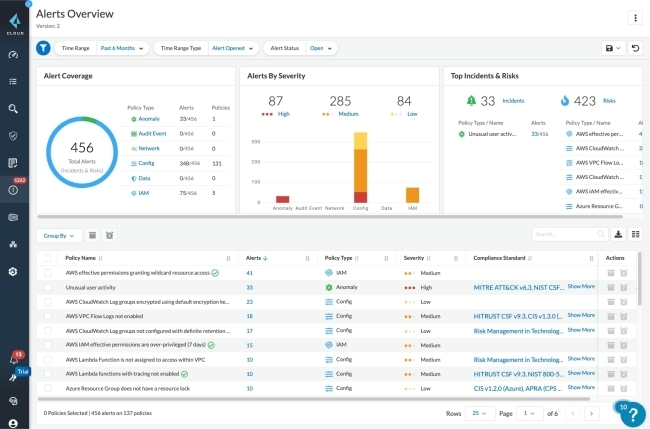
* + - Chi phí: Checkmarx có thể tốn kém, đặc biệt đối với các tổ chức có ngân sách hạn chế hoặc đối với những tổ chức có số lượng lớn người dùng hoặc cơ sở mã.
    - Kết quả dương tính giả: Checkmarx có thể tạo ra kết quả dương tính giả, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
    - Độ phức tạp: Checkmarx có thể là một giải pháp phức tạp và đường cong học tập có thể dốc, đặc biệt đối với người dùng mới sử dụng bảo mật phần mềm.
    - Hiệu suất: Hiệu suất của Checkmarx có thể bị ảnh hưởng bởi khối lượng mã được quét, điều này có thể dẫn đến chậm và ngừng hoạt động.
    - Tích hợp hạn chế: Mặc dù Checkmarx tích hợp với các công cụ và hệ thống bảo mật khác, mức độ tích hợp có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để tận dụng tối đa giải pháp.

## Prisma Cloud (Giải pháp quản lý tư thế bảo mật đám mây (CSPM))

### Chi tiết

Prisma Cloud là giải pháp bảo mật đám mây cung cấp cho các tổ chức giải pháp bảo mật toàn diện, bao gồm bảo mật cơ sở hạ tầng đám mây, bảo mật ứng dụng đám mây và bảo mật dữ liệu đám mây.

Chi phí của Prisma Cloud thay đổi tùy thuộc vào nhu cầu cụ thể của tổ chức, chẳng hạn như số lượng người dùng, số lượng tài khoản đám mây và mức độ phức tạp của giải pháp. Mô hình định giá thường dựa trên đăng ký mỗi người dùng, mỗi năm, với chi phí bắt đầu từ khoảng 1.000 USD mỗi năm



Hình 21: Giao diện Prisma Cloud

### Tính năng

* + - Quản lý trạng thái bảo mật đám mây (CSPM): Prisma Cloud cung cấp các khả năng CSPM, bao gồm khả năng giám sát và quản lý trạng thái bảo mật đám mây, xác định các rủi ro và lỗ hổng bảo mật cũng như khắc phục các sự cố bảo mật.
    - Phát hiện và phản hồi mối đe dọa: Prisma Cloud cung cấp khả năng phát hiện và phản hồi mối đe dọa, bao gồm phát hiện và phản hồi mối đe dọa theo thời gian thực, điều tra và phản hồi sự cố bảo mật cũng như phân tích bảo mật.
    - Quản lý tuân thủ: Prisma Cloud cung cấp khả năng quản lý tuân thủ, bao gồm khả năng đánh giá và quản lý việc tuân thủ các tiêu chuẩn bảo mật khác nhau, chẳng hạn như PCI DSS, HIPAA và SOC 2.
    - Bảo vệ khối lượng công việc trên đám mây: Prisma Cloud cung cấp khả năng bảo vệ khối lượng công việc trên đám mây, bao gồm bảo vệ chống lại các mối đe dọa đối với khối lượng công việc dựa trên đám mây, chẳng hạn như tấn công mạng, vi phạm dữ liệu và phần mềm độc hại.
    - Tích hợp: Prisma Cloud tích hợp với nhiều giải pháp bảo mật và cơ sở hạ tầng đám mây, bao gồm các nền tảng đám mây, chẳng hạn như Amazon Web Services (AWS), Microsoft Azure và Google Cloud Platform (GCP) cũng như các giải pháp quản lý sự kiện và thông tin bảo mật (SIEM).
    - Quản lý dựa trên đám mây: Prisma Cloud là giải pháp dựa trên đám mây, cung cấp khả năng quản lý và báo cáo tập trung cho các tổ chức có nhiều tài sản đám mây.

### Ưu điểm

* + - Bảo mật cơ sở hạ tầng đám mây: Prisma Cloud cung cấp cho các tổ chức bảo mật cơ sở hạ tầng đám mây toàn diện, bao gồm bảo vệ chống lại các mối đe dọa như phần mềm độc hại và các nỗ lực hack.
    - Bảo mật ứng dụng đám mây: Prisma Cloud cung cấp cho các tổ chức khả năng bảo mật ứng dụng đám mây toàn diện, bao gồm bảo vệ chống lại các mối đe dọa như tấn công cross-site scripting (XSS) và SQL injection.
    - Bảo mật dữ liệu đám mây: Prisma Cloud cung cấp cho các tổ chức bảo mật dữ liệu đám mây toàn diện, bao gồm bảo vệ chống vi phạm và trộm cắp dữ liệu.
    - Tích hợp: Prisma Cloud tích hợp với các công cụ và hệ thống bảo mật khác, chẳng hạn như nhà cung cấp cơ sở hạ tầng đám mây và giải pháp bảo mật đám mây, cung cấp cái nhìn toàn diện về tình hình bảo mật của tổ chức.
    - Giao diện thân thiện với người dùng: Prisma Cloud có giao diện thân thiện với người dùng, giúp người dùng dễ dàng quản lý và thực thi các chính sách bảo mật.

### Nhược điểm

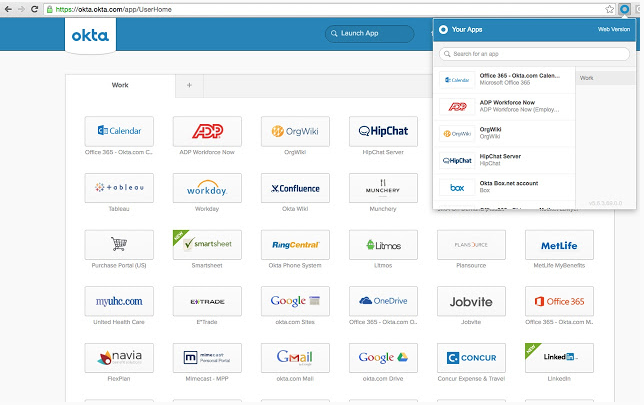
* + - Chi phí: Prisma Cloud có thể tốn kém, đặc biệt đối với các tổ chức có ngân sách hạn chế hoặc những tổ chức có số lượng lớn tài khoản đám mây.
    - Kết quả dương tính giả: Prisma Cloud có thể tạo ra kết quả dương tính giả, điều này có thể dẫn đến lãng phí thời gian và công sức nếu kết quả không được xác thực đúng cách.
    - Độ phức tạp: Prisma Cloud có thể là một giải pháp phức tạp và đường cong học tập có thể dốc, đặc biệt đối với người dùng mới sử dụng bảo mật đám mây.
    - Hiệu suất: Hiệu suất của Prisma Cloud có thể bị ảnh hưởng bởi khối lượng dữ liệu được xử lý, điều này có thể dẫn đến chậm và ngừng hoạt động.
    - Tích hợp hạn chế: Mặc dù Prisma Cloud tích hợp với các công cụ và hệ thống bảo mật khác, mức độ tích hợp có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để tận dụng tối đa giải pháp.

## Okta (Giải pháp quản lý truy cập và nhận dạng (IAM))

### Chi tiết

Okta là giải pháp quản lý danh tính và quyền truy cập (IAM) cung cấp cho các tổ chức một nền tảng tập trung để quản lý và bảo mật quyền truy cập của người dùng vào các ứng dụng và tài nguyên.

Chi phí: Giá của Okta dựa trên đăng ký mỗi người dùng, mỗi tháng, với giá khởi điểm khoảng 4 đô la mỗi người dùng mỗi tháng cho các khả năng quản lý danh tính cơ bản và mở rộng quy mô cho các tính năng và khả năng bổ sung. Chi phí chính xác sẽ phụ thuộc vào nhu cầu và yêu cầu cụ thể của tổ chức.



Hình 22: Ứng dụng dành cho Okta SWA

### Tính năng

* + - Đăng nhập một lần (SSO): Okta cung cấp khả năng đăng nhập một lần (SSO), cho phép người dùng truy cập tất cả các ứng dụng và tài nguyên của họ từ một nơi bằng một bộ thông tin xác thực.
    - Quản lý người dùng: Okta cung cấp một nền tảng tập trung để quản lý danh tính người dùng, bao gồm khả năng thêm, cập nhật và xóa người dùng cũng như quản lý quyền truy cập của người dùng vào các ứng dụng và tài nguyên.
    - Quản lý truy cập: Okta cung cấp khả năng quản lý truy cập, bao gồm kiểm soát truy cập dựa trên vai trò (RBAC), kiểm soát truy cập dựa trên chính sách và khả năng xác thực đa yếu tố (MFA).
    - Quản lý thiết bị di động: Okta cung cấp khả năng quản lý thiết bị di động (MDM), cho phép các tổ chức quản lý và bảo mật các thiết bị di động được nhân viên sử dụng.
    - Tích hợp: Okta tích hợp với nhiều ứng dụng và hệ thống, giúp các tổ chức dễ dàng truy cập an toàn hơn vào các tài nguyên này.

### Ưu điểm

* + - Tăng cường bảo mật: Okta giúp các tổ chức tăng cường bảo mật bằng cách cung cấp một nền tảng tập trung để quản lý quyền truy cập của người dùng vào các ứng dụng và tài nguyên.
    - Trải nghiệm người dùng được cải thiện: Okta cung cấp trải nghiệm người dùng liền mạch bằng cách cho phép người dùng truy cập tất cả các ứng dụng và tài nguyên của họ từ một nơi bằng một bộ thông tin xác thực.
    - Giảm chi phí CNTT: Okta giúp giảm chi phí CNTT bằng cách cung cấp một nền tảng tập trung để quản lý danh tính và quyền truy cập của người dùng, giảm nhu cầu về các quy trình thủ công và giảm nguy cơ xảy ra lỗi.
    - Cải thiện tuân thủ: Okta giúp các tổ chức cải thiện tuân thủ bằng cách cung cấp một nền tảng tập trung để quản lý quyền truy cập của người dùng vào các ứng dụng và tài nguyên, giảm nguy cơ vi phạm và không tuân thủ.

### Nhược điểm

* + - Chi phí: Okta có thể tốn kém, đặc biệt đối với các tổ chức có số lượng người dùng lớn hoặc đối với những tổ chức yêu cầu khả năng nâng cao.
    - Độ phức tạp: Okta có thể phức tạp để thiết lập và sử dụng, đặc biệt là đối với các tổ chức chưa quen với việc quản lý danh tính và quyền truy cập.
    - Tích hợp: Mặc dù Okta tích hợp với nhiều ứng dụng và hệ thống, nhưng mức độ tích hợp có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để tận dụng tối đa giải pháp.
    - Hiệu suất: Hiệu suất của Okta có thể bị ảnh hưởng bởi khối lượng dữ liệu đang được xử lý, điều này có thể dẫn đến chậm và ngừng hoạt động.
    - Tùy chỉnh có giới hạn: Mặc dù Okta cung cấp nhiều tính năng và khả năng, nhưng mức độ tùy chỉnh có thể bị hạn chế và các tổ chức có thể cần đầu tư vào các công cụ hoặc dịch vụ bổ sung để đáp ứng các yêu cầu cụ thể của họ.

# KẾT LUẬN

Ba chương của bài tập đã thể hiện được rằng những mục tiêu được đặt ra khi thực hiện bài tập đều đã đạt được. Cụ thể:

Chương 1 đã hệ thống lại kiến thức tổng quan về các công cụ tự động về đánh giá rủi ro.

Chương 2 đã giới thiệu từng công cụ thực hiện. Khái niệm, chi tiết, ưu điểm , nhược điểm của từng công cụ, đem đến cho người đọc những cái nhìn khách quan của từng công cụ.

Trong khi thực hiện bài tập này, do hạn chế về thời gian và trình độ nên không tránh khỏi những thiếu sót và hạn chế nhất định, chúng em rất mong có sự góp ý và bổ sung của cô để nhóm có thêm kinh nghiệm hoàn thành tốt hơn trong những đề tài tiếp theo.

Chúng em xin chân thành cảm ơn!