BkavPro TI

Phần mềm Nền tảng tri thức mối đe dọa an toàn thông tin BkavPro TI

Giới thiệu

Ngày nay, các cuộc tấn công mạng được thực hiện bởi những kẻ xâm nhập có hiểu biết và nhận thức cao hơn. Chúng thường sử dụng các kỹ thuật khai thác tiên tiến để thực hiện các cuộc tấn công khác nhau vào các những tổ chức, khiến các tổ chức khó dự đoán ý định, đặc điểm và phương pháp của chúng được sử dụng để thực hiện cuộc tấn công. Trong trường hợp này, cách tiếp cận an ninh mạng truyền thống sẽ không đủ. Do đó, việc nắm bắt và cập nhật sớm những thông tin liên quan đến các mối đe dọa mới là một chiến lược cần thiết cho các tổ chức, doanh nghiệp trong nhiệm vụ phòng ngừa và đảm bảo an toàn thông tin (ATTT) cho đơn vị.

BkavPro TI là hệ thống thu thập và xử lý dữ liệu, cung cấp tri thức về các mối đe dọa an ninh mạng, hỗ trợ trong việc phát hiện, cảnh báo và ngăn chặn sớm các mối đe dọa.

Dịch vụ **BkavPro TI** cung cấp các thông tin được thu thập từ rất nhiều nguồn khác nhau về các mối đe dọa trên không gian mạng cho các tổ chức. Cung cấp nguồn dữ liệu cho các giải pháp đảm bảo ATTT như: SIEM, IPS/IDS, Network APT, EDR... cập nhật tự động - hỗ trợ các giải pháp trong việc tăng khả năng phát hiện các mối đe dọa về ATTT cho tổ chức. Hệ thống hỗ trợ API và dữ liệu theo định dạng chuẩn (STIX/TAXII).

Ưu điểm nổi bật

Dễ dàng triển khai và sử dụng	Cấu hình và giám sát an toàn thông tin từ xa với hệ thống của mình qua giao diện Web. Không yêu cầu đầu tư thêm thiết bị phần cứng hay chi phí vận hành.
Cảnh báo sớm rủi ro, nguy cơ	Hệ thống sẽ thực hiện cảnh báo sớm các nguy cơ, rủi ro tấn công mạng vào tổ chức ngay sau khi phát hiện hoặc có các công bố mới qua email.
Nguồn dữ liệu đa dạng, phong phú	Dữ liệu được tổng hợp từ các tổ chức Quốc tế, Việt Nam, từ các sensor, honeypot... tích hợp trí tuệ nhân tạo AI và Machine Learning giúp nâng cao khả năng tìm kiếm mối đe dọa, từ đó phân tích để có các cảnh báo sớm nhất, cụ thể nhất.
Thông tin kỹ thuật nóng liên tục cập nhật	Liên tục cập nhật các thông tin kỹ thuật mới về nguy cơ tấn công mạng đối với Việt Nam. Đặc biệt luôn theo dõi và giám sát hoạt động của các nhóm tin tặc trên thế giới, cung cấp thông tin liên quan cho khách hàng trước khi các cuộc tấn công diễn ra.
Hỗ trợ 24/7/365	Thực hiện giám sát liên tục theo thời gian thực. Đội ngũ hỗ trợ kỹ thuật sẵn sàng hỗ trợ khi có các yêu cầu bổ sung của dịch vụ.

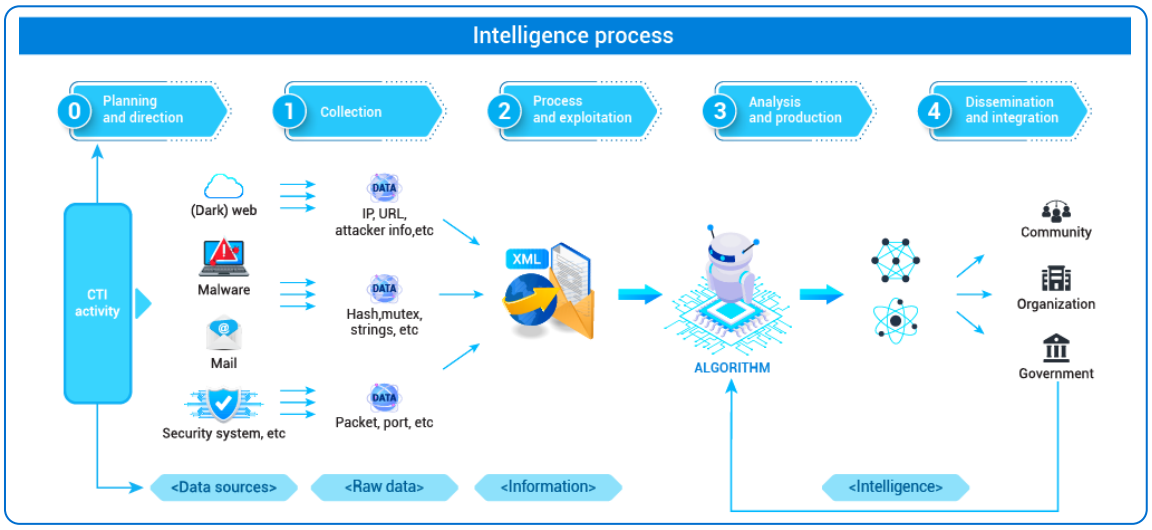
Tính năng chi tiết

Tra cứu các tri thức nguy cơ (Threat Lookups)	Dịch vụ **BkavPro TI** cung cấp các thông tin được thu thập từ rất nhiều nguồn khác nhau về các mối đe dọa trên không gian mạng cho các tổ chức. Hỗ trợ tìm kiếm, tra cứu tri thức nguy cơ theo từ khóa, thời gian (real-time information), giúp người dùng tra cứu các thông tin nguy cơ một cách nhanh chóng.
Nguồn cấp dữ liệu mối đe dọa (Threat data feeds)	Cung cấp nguồn dữ liệu (IP, domain, hash...) tích hợp cho các giải pháp ATTT như SIEM, IPS/IDS, Network APT, EDR... cập nhật tự động - hỗ trợ các giải pháp trong việc tăng khả năng phát hiện các mối đe dọa về ATTT cho tổ chức. Hệ thống cung cấp API và dữ liệu ở các định dạng chuẩn (STIX / TAXII)
Cảnh báo (Real-time information and alerts)	**BkavPro TI** hỗ trợ cảnh báo thời gian thực các mối đe dọa về ATTT: **(1)** Cảnh báo thông tin về các nguy cơ ảnh hưởng trực tiếp đến tổ chức, doanh nghiệp như: Thông tin về các nguy cơ lạm dụng thương hiệu của tổ chức: Domain, IP, ứng dụng, các chứng chỉ số (SSL Certificates) giả mạo thương hiệu. Thông tin về dữ liệu bị đánh cắp, rò rỉ của tổ chức (compromised/leak data): Logindetails, bank cards, IMEIs, public leaks, Git Leaks... có thể gây hại cho khách hàng, yêu cầu phản hồi và hành động ngay lập tức. **(2)** Cảnh báo thông tin về các lỗ hổng an ninh bảo mật, lỗ hổng dịch vụ của tổ chức. **(3)** Cảnh báo các thông tin liên quan đến kỹ thuật, chiến dịch, thông tin liên quan đến các nhóm tấn công. **(4)** Các thông tin liên quan đến mã độc, thông tin về domain, IP của khách hàng có kết nối đến cơ sở hạ tầng của mã độc. Cảnh báo về các mối đe doạ an ninh mạng cho khách hàng ngay khi nguy cơ vừa xuất hiện kèm theo đầy đủ phân tích kỹ thuật, đánh giá chi tiết của chuyên gia về cách phát hiện, phòng chống. Hệ thống cho phép cấu hình lĩnh vực/chủng loại/từ khóa/mức độ nguy hiểm, thời gian về các cảnh báo sẽ nhận. Cho phép thiết lập các từ khóa cần theo dõi, quan tâm. Bất kỳ thông tin nào xuất hiện liên quan đến các từ khóa thiết lập sẽ được cảnh báo. Hỗ trợ nhận cảnh báo qua giao diện website và email. Cho phép tải cảnh báo nguy cơ dưới dạng file.
Điều tra mối đe dọa (Threat Investigation)	Hệ thống cung cấp tính năng Network Analytics Graph – một công cụ phân tích mạnh mẽ, kết hợp các công cụ săn tìm, phân tích mối đe dọa của Bkav, chủ động thực hiện tìm kiếm, nghiên cứu, phân tích và khám phá các mối quan hệ, mối tương quan giữa các sự kiện, các đối tượng liên quan đến mối đe dọa. Hệ thống thu thập một lượng lớn dữ liệu (bao gồm thông tin được thu thập từ các diễn đàn ngầm – Dark Web monitoring, Malware Analysis, Internet snapshots và các thông tin được thu thập qua nhiều năm theo dõi và phân tích), sử dụng các thuật toán độc đáo để xây dựng liên kết, tiết lộ các kết nối ngầm, cung cấp thông tin chi tiết nhất về các đối tượng liên quan đến mối đe dọa. Sử dụng hệ thống phân tích biểu đồ mạng Graph, người dùng có thể xây dựng và khám phá các mối quan hệ giữa các tên miền; các địa chỉ ip; địa chỉ liên hệ được gửi bằng email, số điện thoại, bút danh; Chứng chỉ SSL và khóa SSH; các tệp, dựa trên mã hash (hàm băm) của chúng, được xác định bằng cách sử dụng thuật toán SHA-1; tài khoản sử dụng và các chủ đề được thảo luận trên dark web. Hệ thống cho phép lưu trữ, trích xuất và chia sẻ các thông tin tìm được dưới dạng file.

Tính năng chi tiết

Phân tích phần mềm độc hại (Malware Analysis)	Malware Analysis – Công cụ khởi chạy và phân tích phần mềm độc hại, tích hợp trong nền tảng **BkavPro TI** được thiết kế để quét các file, tệp đính kèm và các liên kết, cung cấp các thông tin phân tích chuyên sâu, bao gồm video về quá trình thực thi và đánh giá mức độ nguy hại. Trên nền tảng Malware Analysis, các tệp được khởi chạy trong một môi trường cô lập và được phân tích động. Từ kết quả phân tích, báo cáo chi tiết nhất về phần mềm độc hại, các dấu hiệu hành vi... sẽ được ghi lại và cảnh báo tới người dùng.
Giám sát Dark Web (Dark Web Monitoring)	Hỗ trợ thu thập dữ liệu trên Deep-web, Dark-web: theo dõi các diễn đàn của tin tặc, thu thập dữ liệu và các thông tin cá nhân của khách hàng có thể bị rao bán.
Theo dõi các nhóm tấn công (Threat Actors Data feeds & reports)	Cung cấp thông tin liên quan đến các chiến dịch, nhóm tấn công (từ các nhóm thông thường đến các nhóm được nhà nước bảo trợ) bao gồm các thông tin: mô tả, kỹ thuật tấn công, đối tượng tấn công, các chiến dịch tấn công... và các báo cáo liên quan. Cung cấp danh sách các cuộc tấn công và các báo cáo gần nhất (Tháng/Quý/Năm)
Báo cáo mối đe dọa (Threat Intelligence Report)	Bên cạnh thông tin về các nguy cơ nguy hiểm được cảnh bảo trực tiếp, **BkavPro TI** còn cung cấp báo cáo về tình hình an ninh mạng đang diễn ra trên toàn cầu: Top các sự kiện, nguy cơ mất ATTT trên toàn thế giới; các nhóm tấn công đang hoạt động mạnh; mã độc, phương thức tấn công thịnh hành; các lỗ hổng đang được sử dụng, khai thác hoặc được quan tâm, chú ý. Cung cấp một bức tranh toàn cảnh giúp cho doanh nghiệp nắm bắt được các xu hướng, tình hình an ninh mạng trên thế giới. Cho phép xem xu hướng nguy cơ toàn cầu theo: ngày, tháng, quý, năm...

Sơ đồ quy trình



Mô tả, diễn giải quy trình

Lập kế hoạch và định hướng	Trong giai đoạn này, một kế hoạch phù hợp được phát triển dựa trên yêu cầu tình báo chiến lược, chẳng hạn các yêu cầu để phát triển thông tin tình báo về mối đe dọa là gì, thông tin tình báo nào nên được ưu tiên... Giai đoạn này xác định toàn bộ chương trình tình báo từ thu thập dữ liệu đến phân phối sản phẩm tình báo cuối cùng và đóng vai trò là cơ sở cho quá trình tình báo hoàn chỉnh. Nó cũng bao gồm việc xác định các yêu cầu của dữ liệu, các phương pháp được sử dụng để thu thập dữ liệu và thiết lập một kế hoạch thu thập. Trong giai đoạn này, một đội tình báo sẽ được thành lập, vai trò và trách nhiệm chính của họ cũng được hình thành. Ngoài ra, việc lập kế hoạch và các yêu cầu được đặt ra cho các giai đoạn sau của chu trình cũng được thực hiện.
Thu thập dữ liệu	Giai đoạn này tập trung vào việc thu thập dữ liệu thỏa mãn các yêu cầu đã đặt ra ở giai đoạn một. Dữ liệu có thể được thu thập theo những cách khác nhau thông qua phương tiện kỹ thuật hoặc con người. Việc thu thập thông tin có thể được thực hiện trực tiếp hoặc bí mật dựa trên tính bảo mật của thông tin. Công ty cổ phần phần mềm diệt virus Bkav là đơn vị hàng đầu trong việc cung cấp các dịch vụ về **BkavPro TI**. Các nguồn dữ liệu của Bkav rất đa dạng bao gồm các nguồn dữ liệu được thu thập từ các tổ chức trong và ngoài nước, từ quá trình thực hiện các nhiệm vụ giám sát an ninh mạng, cung cấp các dịch vụ giám sát ATTT, các hệ thống giám sát mạng xã hội, các diễn đàn ngầm - DarkWeb monitoring, các nền tảng phân tích mối đe dọa. Đặc biệt, là nguồn dữ liệu từ các nghiên cứu nội bộ do các chuyên gia hàng đầu của Bkav thực hiện.
Một số nguồn dữ liệu của Bkav	**National Cyber Security Center (NCSC)**: Bkav kết hợp với Trung tâm Giám sát an toàn không gian mạng quốc gia Việt Nam trong trong việc thu thập, phân tích và chia sẻ dữ liệu nguy cơ an ninh mạng. **GROUP-IB**: Bkav đã thực hiện ký kết thoả thuận hợp tác chiến lược với Group-IB trong việc chia sẻ thông tin tình báo mối đe dọa... **Trung tâm Giám sát mã độc (AMC)**: Bkav xây dựng Trung tâm Giám sát mã độc với nhiệm vụ chính là thực hiện theo dõi, phát hiện và phân tích các loại mã độc trong nước và trên thế giới. Ngoài ra hệ thống còn thu thập ở rất nhiều các nguồn khác. Hiện tại hệ thống đang thực hiện thu thập khoảng trên 200 các nguồn dữ liệu khác nhau bao gồm các nguồn feeds, sources, frameworks & platforms... như: CIRCL, TOR, Botvrij, openphish, AbuseIPDB, APT Groups and Operations, Kaspersky, OpenPhish, MISP, OpenTAXII... Để có được những nguồn dữ liệu đáng tin cậy và có thể cảnh báo kịp thời tới khách hàng, Bkav còn thực hiện xây dựng đội điểm tin và quy trình thực hiện giám sát an ninh mạng, luôn cập nhật các thông tin, tình an ninh mạng mới nhất trên thế giới. Sau khi quá trình thu thập được thực hiện, dữ liệu sẽ được chuyển để xử lý trong giai đoạn tiếp theo.

Mô tả, diễn giải quy trình

Khai thác và xử lý	Giai đoạn này, dữ liệu chưa có định dạng thích hợp và ở dạng thô (Raw data). Dữ liệu thu được từ các giai đoạn trước được xử lý để khai thác và chuyển thành thông tin hữu ích mà người dùng có thể hiểu được. Dữ liệu thô được chuyển đổi thành thông tin có ý nghĩa bởi các chuyên gia được đào tạo chuyên sâu bằng cách sử dụng công nghệ và công cụ tinh vi. Dữ liệu đã diễn giải này được chuyển đổi thành một định dạng có thể sử dụng được và có thể được sử dụng trực tiếp trong giai đoạn phân tích dữ liệu. Việc xử lý để có hiệu quả đòi hỏi phải hiểu đúng về kế hoạch thu thập dữ liệu, các yêu cầu của người tiêu dùng, chiến lược phân tích và các loại dữ liệu đang được xử lý. Nhiều công cụ tự động được sử dụng để áp dụng các chức năng xử lý dữ liệu như cấu trúc, giải mã, phân tích cú pháp, giảm dữ liệu, lọc, tương quan dữ liệu và tổng hợp dữ liệu.
Phân tích và sản xuất	Sau khi thông tin được xử lý thành một định dạng thích hợp, phân tích dữ liệu để lấy thông tin tinh chỉnh được thực hiện trong giai đoạn này. Phân tích bao gồm các dữ kiện, phát hiện và dự báo, cho phép ước tính và dự đoán các cuộc tấn công và kết quả. Việc phân tích phải khách quan, kịp thời, chính xác và có thể hành động được. Do thông tin được thu thập từ các nguồn khác nhau, phải thực hiện kết hợp các nguồn khác nhau này thành một thực thể duy nhất trong giai đoạn này. Dữ liệu thô được chuyển đổi thành thông tin bằng cách áp dụng các kỹ thuật phân tích dữ liệu khác nhau như phân tích định tính và định lượng, kỹ thuật dựa trên máy và phương pháp thống kê. Khi thông tin được phân tích cung cấp đủ bối cảnh để xác định mối đe dọa, thì nó sẽ được nâng lên thành tình báo. Giai đoạn này xác định các mối đe dọa tiềm ẩn đối với tổ chức và hỗ trợ thêm trong việc phát triển các biện pháp đối phó thích hợp để ứng phó với các mối đe dọa đã xác định.
Phổ biến và tích hợp	Các thông tin được phân tích sẵn sàng để tích hợp và phân phối cho người dùng, được thực hiện bằng phương tiện tự động hoặc bằng phương pháp thủ công. Các loại thông tin về mối đe dọa chính thường được sử dụng để phổ biến bao gồm chỉ báo mối đe dọa, TTP của đối thủ, cảnh báo bảo mật, báo cáo tình báo về mối đe dọa và thông tin cấu hình công cụ để sử dụng các công cụ tự động hóa tất cả các giai đoạn của thông tin tình báo về mối đe dọa. Các báo cáo tình báo khác nhau được tạo ra để đáp ứng các yêu cầu khác nhau các cấp: cấp chiến lược, tác chiến, chiến thuật và kỹ thuật Tình báo mối đe dọa chiến lược được sử dụng bởi các nhà điều hành và quản lý cấp cao, tập trung vào các chiến lược kinh doanh cấp cao. Thông tin tình báo về mối đe dọa hoạt động được sử dụng bởi các chuyên gia an ninh mạng như các nhà quản lý bảo mật và người bảo vệ mạng và chủ yếu tập trung vào các mối đe dọa cụ thể đối với các tổ chức.

Mô tả, diễn giải quy trình

Phổ biến và tích hợp	Tình báo mối đe dọa chiến thuật được sử dụng bởi các chuyên gia an ninh mạng như dịch vụ CNTT và các nhà quản lý SOC, quản trị viên và kiến trúc sư và tập trung vào các TTPs đối thủ. Tình báo mối đe dọa kỹ thuật được sử dụng bởi các nhân viên SOC và các nhóm IR, bao gồm thông tin liên quan đến các IoC đã được xác định. Việc phổ biến thông tin giúp các tổ chức xây dựng chiến lược phòng thủ và giảm thiểu cho các mối đe dọa đã được xác định. Chia sẻ mối đe dọa tình báo trong và ngoài giúp các tổ chức có được nhận thức tình huống và cũng để tăng cường các quy trình quản lý rủi ro và quản lý rủi ro hiện tại. Giai đoạn này cũng cung cấp thông tin phản hồi cung cấp thêm đầu vào cho các yêu cầu thông tin do đó lặp lại vòng đời tình báo mối đe dọa. Phản hồi là một đánh giá mô tả liệu trí thông minh được trích xuất có đáp ứng các yêu cầu của người tiêu dùng thông minh hay không. Phản hồi này giúp tạo ra tình báo chính xác hơn thông qua các đánh giá liên quan và kịp thời.

Phân loại dịch vụ

Tính năng	Nội dung	Gói dịch vụ Basic	Gói dịch vụ Advanced
Tra cứu tri thức nguy cơ	Sản phẩm cho phép tìm kiếm, tra cứu tri thức nguy cơ theo từ khóa, thời gian	✓	✓
Alerts	Cảnh báo thông tin về các lỗ hổng an ninh bảo mật, mã độc, chiến dịch tấn công	✓	✓
	Cảnh báo thông tin liên quan đến kỹ thuật tấn công	✓	✓
	Cảnh báo thông tin liên quan đến nhóm tấn công	✓	✓
	Cảnh báo thông tin về dữ liệu bị đánh cắp, rò rỉ (compromised/leak data)	✓	✓
	Cảnh báo thông tin về domain, IP của khách hàng có kết nối đến cơ sở hạ tầng của mã độc		✓
	Cảnh báo thông tin về các nguy cơ lạm dụng thương hiệu của tổ chức: domain, Domain, IP giả mạo thương hiệu, ứng dụng giả mạo thương hiệu, các chứng chỉ số (SSL Certificates) giả mạo thương hiệu		✓
	Cảnh báo lỗ hổng dịch vụ, các port mở bất thường của tổ chức		
	Cảnh báo qua portal và email		✓
Compro-mise and Leaks	Cung cấp các thông tin liên quan dữ liệu bị đánh cắp, rò rỉ của tổ chức: Compromised accounts, Bank cards, Mules, IMEI, Public Leaks, Git Leaks, Breached Databases	✓	✓

Phân loại dịch vụ

Tính năng	Nội dung	Gói dịch vụ Basic	Gói dịch vụ Advanced
Threat Actors Data feeds & reports	Cung cấp các nguồn thông tin được thu thập từ rất nhiều nguồn khác nhau về mối đe dọa cho tổ chức, lỗ hổng dịch vụ, các port mở bất thường của tổ chức...	✓	✓
	Cung cấp thông tin liên quan đến các chiến dịch, nhóm tấn công, từ các nhóm thông thường đến các nhóm được nhà nước bảo trợ bao gồm các thông tin: mô tả, kỹ thuật tấn công, đối tượng tấn công, các chiến dịch tấn công	✓	✓
	Cung cấp danh sách các cuộc tấn công và các báo cáo gần nhất (Tháng/Quý/Năm)	✓	✓
Malware & Attacks Data feeds	Malware data- Phishing kits\Vulnerabilities\Targeted Trojans: Cung cấp thông tin về các phần mềm độc hại có khả năng nhắm vào khách hàng, trích xuất dữ liệu từ các bộ công cụ lừa đảo. Cập nhật thông tin về các lỗ hổng và cách khai thác mới nhất.	✓	✓
	Attacks data - Phishing, DDoS & Defacement: Dữ liệu về các tên miền lừa đảo, các cuộc tấn công DDoS, Deface trang web	✓	✓
	Suspicious IP: Danh sách các ip độc hại	✓	✓
Malware Detonation	Một công cụ khởi chạy và phân tích phần mềm độc hại, được thiết kế để quét các file, tệp đính kèm và các liên kết, cung cấp các thông tin phân tích chuyên sâu, bao gồm video về quá trình thực thi và đánh giá mức độ nguy hại		✓
Network Analytics Graph	Một công cụ phân tích mạnh mẽ, kết hợp với các công cụ săn tìm mối đe dọa bên ngoài của Bkav. Hệ thống thu thập một lượng lớn dữ liệu và sử dụng các thuật toán độc đáo để xây dựng các liên kết, tiết lộ các kết nối ngầm và cung cấp các thông tin chi tiết quan hệ với nguy cơ		✓
DarkWeb monitoring	Công cụ cho phép truy cập theo dõi tổng quan tất cả các hoạt động trong DarkWeb: theo dõi các diễn đàn của tin tặc, thu thập dữ liệu và các thông tin cá nhân của khách hàng có thể bị giao bán		✓
Báo cáo mỗi đe dọa	Cung cấp các báo cáo về tình hình an ninh mạng đang diễn ra trên thế giới: Top các sự kiện, nguy cơ mất ATTT trên toàn thế giới; các nhóm tấn công đang hoạt động mạnh; mã độc, phương thức tấn công thịnh hành; các lỗ hổng đang được sử dụng, khai thác hoặc được quan tâm, chú ý (tháng/quý/năm)	✓	✓
Hỗ trợ	Hỗ trợ support 24/7/365	✓	✓

Trụ sở chính: Tòa nhà Bkav, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội
Điện thoại: (024) 37 677 090/ Ext: 1013 Số fax: (024) 3868 4755
Website: security.bkav.com Email: security@bkav.com
Bkav TP. HCM: Số 67, Đường số 3, Khu dân cư City Land, P. 7, Q. Gò Vấp, TP HCM
Điện thoại: (028) 6296 6626 Số fax: (028) 2253 6103

Bkav Pro