BKAV TI

Mục lục

1. Tổng quan

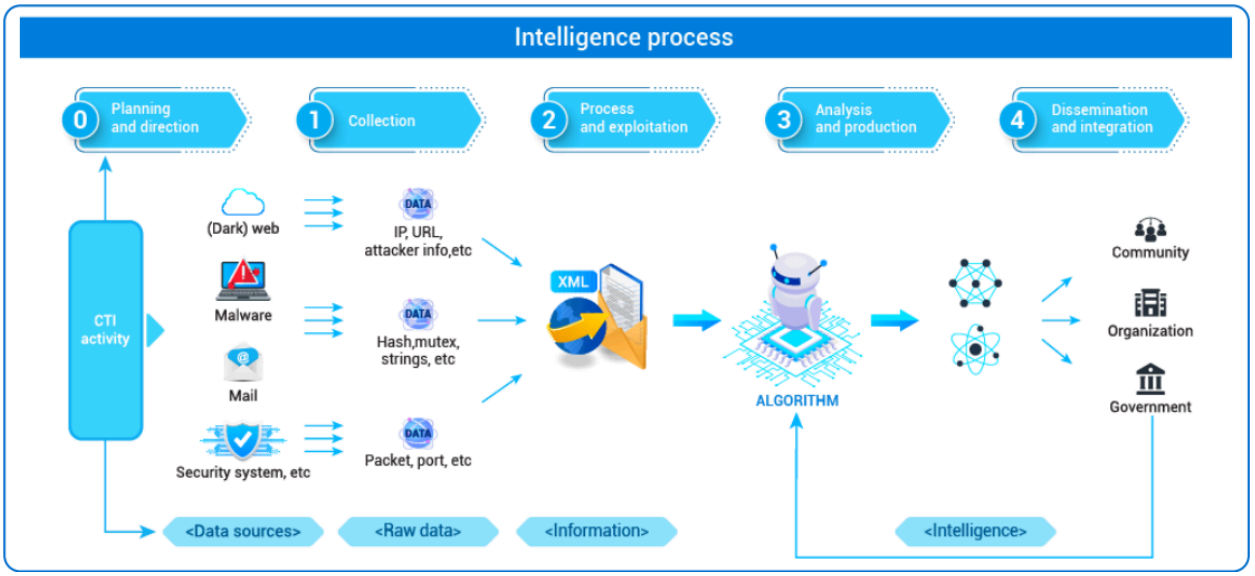
- Ngày nay, các cuộc tấn công mạng được thực hiện bởi những kẻ xâm nhập có hiểu biết và nhận thức cao hơn. Chúng thường sử dụng các kỹ thuật khai thác tiên tiến để thực hiện các cuộc tấn công khác nhau vào các những tổ chức, khiến các tổ chức khó dự đoán ý định, đặc điểm và phương pháp của chúng được 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.
- Bkav 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 Bkav 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).

2. Tính năng nổi bật và lợi ích của Hệ thống

- **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.

3.Sơ đồ hoạt động và cách hoạt động



4.Chi tiết tính năng

STT	Tên Tính năng	Mô tả
1	Tra cứu các tri thức nguy cơ (Threat Lookups)	Dịch vụ Bkav 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.
2	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)
3	Cảnh báo (Real-time information and alerts)	Bkav 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.
4	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 BkavCS, 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 hoản 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.
5	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 Bkav 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
6	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
7	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)
8	Báo cáo mối đe dọa (Threat Intelligence Report)	Bên cạnh thông tin về các nguy cơ nguy hiểm được cảnh bảo trực tiếp, Bkav 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

5.Yêu cầu về phần cứng

Cấu hình: 16 core, 64 GB Ram, Dung lượng ổ cứng tối thiểu 2T

6.Yêu cầu về Hạ tầng kỹ thuật

STT	Hợp phần	OS	Số lượng máy chủ	Cấu hình máy chủ	Đường truyền
1	Website TI	Ubuntu	01 Máy	CPU: 8 Core Memory: 16G Storage: 2T	250 Mbps / 500Users

7.Môi trường triển khai

- Triển khai trên hệ điều hành Ubuntu.