EDR
Bkav Endpoint Detection Response

Giới thiệu

Giải pháp giám sát an ninh hệ thống Bkav Endpoint Detection Response (Bkav EDR) là giải pháp đảm bảo an ninh thông tin tổng thể, kết hợp các hoạt động theo dõi, phân tích, điều tra những nguy cơ về bảo mật trong hệ thống mạng máy tính, đồng thời cho phép ứng phó nhanh chóng, hiệu quả với các mối đe dọa được phát hiện

Tính năng nổi bật

Phát hiện các hành vi bất thường

Bkav EDR với các agent trên các máy tính sẽ thực hiện theo dõi thường xuyên, đầy đủ các hoạt động liên quan tới an ninh thông tin trên toàn hệ thống. Khi phát hiện các hành vi bất thường của các thành phần agent trên máy sẽ gửi cảnh báo về server quản lý tập trung.

Điều tra cảnh báo và ứng phó với mối đe dọa, Săn tìm mối đe dọa

Bkav EDR cung cấp giao diện quản trị tiện lợi để theo dõi các cảnh báo về an ninh trong hệ thống, đồng thời có thể đặt các lệnh để thu thập thêm thông tin, tìm kiếm các thành phần tấn công trên toàn hệ thống. Kết quả tìm kiếm bao gồm các mẫu, các log hoạt động của máy tính... sẽ được cập nhật theo thời gian thực, giúp phát hiện sớm và chính xác các mối đe dọa về an ninh thông tin.

Thống kê báo cáo

Giao diện quản trị của **Bkav EDR** cũng hỗ trợ việc thiết lập các quy tắc và mệnh lệnh để ứng phó với các nguy cơ trong hệ thống một cách nhanh chóng, hiệu quả. Các thiết lập có thể thực hiện bao gồm: Chặn các mẫu virus, cách ly hoặc ngăn chặn các thao tác từ máy tính bị tấn công.

Tính năng chi tiết

Tính năng	Bkav EDR phiên bản Standard	Bkav EDR
Thu thập toàn bộ thông tin dữ liệu điểm cuối		
Thu thập dữ liệu các thành phần khởi động cùng máy	✓	✓
Thu thập lịch sử thay đổi nội dung và thuộc tính các file thực thi	✓	✓
Thu thập lịch sử tiến trình sử dụng các thư viện (Dll)	✓	✓
Thu thập lịch sử sử dụng các thiết bị ngoại vi: USB,máy in…	✓	✓
Thu thập dữ liệu các tiến trình đang chạy trên máy tính của người sử dụng	✓	✓
Thu thập lịch sử kết nối vào/ra của máy tính của người sử dụng	✓	✓
Thu thập lịch sử khởi tạo, kết thúc các tiến trình	✓	✓
Thu thập lịch sử tạo, xóa, thay đổi các dịch vụ	✓	✓
Thu thập lịch sử tác động vào các registry nhạy cảm của hệ thống	✓	✓
Thu thập lịch sử đăng nhập, đăng xuất máy tính	✓	✓
Thu thập lịch sử về sự thay đổi quyền hạn của các tiến trình	✓	✓
Thu thập dữ liệu về sự thay đổi cấu hình bảo mật điểm cuối (UAC, Firewall, Remote…)	✓	✓
Thu thập dữ liệu về thông số điểm cuối (OS, version, netwword interface, harware…)		✓
Thu thập lịch sử tác động vào database		✓
Thu thập lịch sử tác động vào các cấu hình dịch vụ web		✓
Thu thập lịch sử truy cập vào các cổng dịch vụ (RDP, FTP, SMTP, POP3, HTTP, SSH...)		✓
Thu thập lịch sử đóng, mở cổng		✓
Phát hiện và cảnh báo các mối đe dọa		
Phát hiện các tiến trình bất thường theo các quy tắc học máy dựa trên các đặc điểm đặc trưng của file	✓	✓
Phát hiện, cảnh báo phần mềm gián điệp	✓	✓
Phát hiện, cảnh báo mã độc, virus lây nhiễm qua USB	✓	✓
Phát hiện, cảnh báo mã độc mã hóa dữ liệu	✓	✓
Phát hiện, cảnh báo tấn công dò quét mật khẩu máy tính (brute force)	✓	✓
Phát hiện, cảnh báo tấn công SMB (khai thác lỗ hổng trong cơ chế chia sẻ thư mục của hệ điều hành)	✓	✓
Phát hiện, cảnh báo tấn công mã độc Fileless (các mã độc hoạt động mà không cần tớ sự tồn tại của file nhị phân)	✓	✓
Phát hiện, cảnh báo tấn công APT (tấn công có chủ đích)	✓	✓
Phát hiện, cảnh báo kết nối tới mạng Botnet	✓	✓

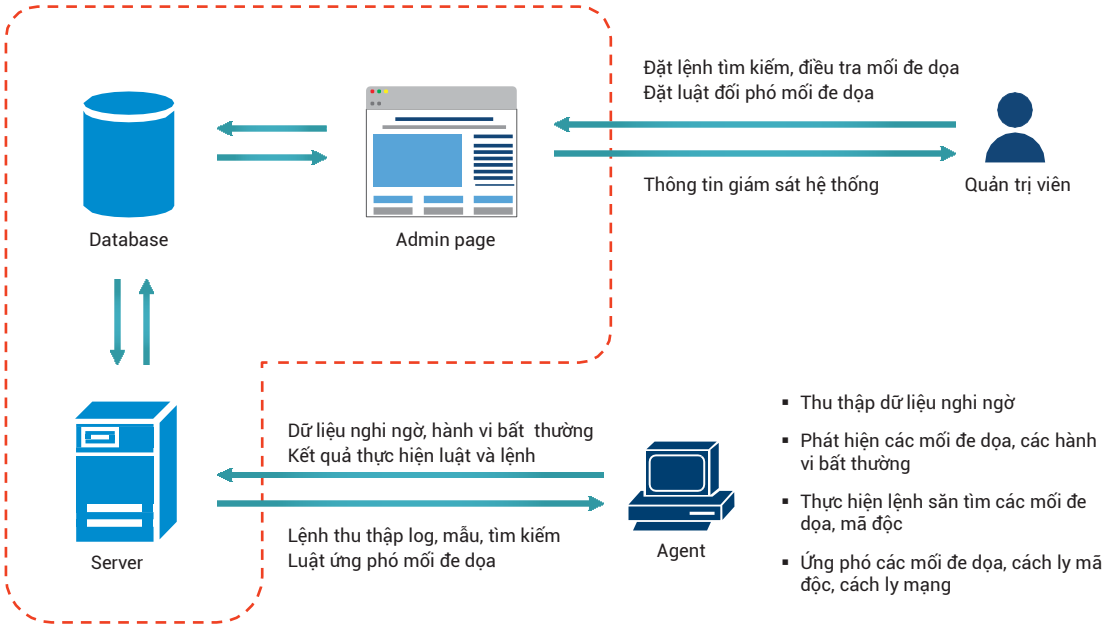
Tính năng chi tiết

Tính năng	Bkav EDR phiên bản Standard	Bkav EDR
Phát hiện và cảnh báo các mối đe dọa (tiếp)		
Phát hiện, cảnh báo mã độc tải về từ Internet	✓	✓
Phát hiện, cảnh báo các tiến trình có hành vi bất thường: Chèn mã thực thi vào tiến trình khác, tác động vào vùng nhạy cảm của hệ thống…	✓	✓
Phát hiện, cảnh báo báo các tiến trình bất thường theo các quy tắc kết hợp học máy, dựa trên các dữ liệu về hoạt động của máy tính được thu thập	✓	✓
Phát hiện, cảnh báo tấn công dò mật khẩu server		✓
Phát hiện, cảnh báo tấn công dò mật khẩu database		✓
Phát hiện, cảnh báo đọc ghi trái phép vào database		✓
Phát hiện, cảnh báo khai thác lỗ hổng database		✓
Phát hiện, cảnh báo remote vào server		✓
Phát hiện, cảnh báo thay đổi cấu hình bảo mật (firewall, taskcheduler, remote, port...) server		✓
Phát hiện, cảnh báo tấn công dịch vụ web		✓
Điều tra, săn tìm mối đe dọa		
Cho phép tìm kiếm file trên các điểm cuối	✓	✓
Cho phép tìm kiếm thông tin trên bộ nhớ các điểm cuối	✓	✓
Cho phép tìm kiếm thông qua các luật của Yara	✓	✓
Cho phép ghi lại thông tin bộ nhớ tiến trình	✓	✓
Cho phép ghi lại thông tin bộ nhớ điểm cuối	✓	✓
Cho phép thực hiện các lệnh, các thao tác với file, tiến trình, registry trên điểm cuối phục vụ điều tra chuyên sâu	✓	✓
Ứng phó với mối đe dọa		
Cho phép cách ly máy tính bị tấn công	✓	✓
Cho phép chặn thao tác trên máy tính bị tấn công	✓	✓
Cho phép chặn tiến trình mã độc	✓	✓
Cho phép xóa file mã độc	✓	✓
Cho phép xử lý các Registry, WMI, Taskcheduler	✓	✓
Cho phép ngăn tiến trình đang chạy thực hiện kết nối mạng	✓	✓
Cho phép thay đổi trạng thái của điểm cuối (như tắt, khởi động lại hoặc chuyển sang chế độ ngủ)	✓	✓

Tính năng chi tiết

Tính năng	Bkav EDR phiên bản Standard & Bkav EDR
Tính năng Hệ thống quản lý tập trung Bkav Endpoint Security Detection & Response MNG (Bkav EDR MNG)	
Giao diện quản trị thông minh, chuyên nghiệp	✓
Cung cấp giao diện khép kín điều tra các cuộc tấn công: Phát hiện các mối đe dọa – Điều tra - Ứng phó	✓
Cung cấp giao diện hiển thị tổng quan về các mối đe dọa, các cảnh báo bất thường	✓
Cung cấp gia diện hiển thị tổng quan về các dải mạng đang có cảnh báo, số lượng các điểm cuối đang cần xử lý	✓
Tự động điều tra các cảnh báo và hiển thị trực quan trên sơ đồ điều tra: Nguồn gốc lây nhiễm, phạm vi ảnh hưởng, C&C của mã độc	✓
Cho phép quản trị viên ra lệnh tìm kiếm file theo mã hash trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên ra lệnh tìm kiếm file luật Yara trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên ra lệnh chụp lại thông tin bộ nhớ RAM hoặc của tiến trình trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên điều tra dựa trên log thu thập được lưu trữ hệ thống big data ngay cả khi điểm cuối offline, dữ liệu được lưu trữ lên đến 6 tháng	✓
Cho phép quản trị viên remote xuống điểm cuối thực hiện các lệnh, các tác động vào file, registry phục vụ quá trình điều tra chuyên sâu	✓
Hệ thống đưa ra các gợi ý phương án xử lý đối với từng cảnh báo, sự cố	✓
Cho phép quản trị viên đặt lệnh chặn điểm cuối kết nối mạng	✓
Cho phép quản trị viên đặt lệnh chặn thao tác chuột, bản phím trên điểm cuối	✓
Cho phép quản trị viên đặt lệnh chặn tiến trình kết nối mạng trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên đặt lệnh chặn tiến trình thực thi trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên đặt lệnh xóa file trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên đặt lệnh xóa registry, wmi, taskcheduler trên một điểm cuối hoặc toàn bộ hệ thống	✓
Cho phép quản trị viên đặt lệnh shutdown, restart, sleep trên điểm cuối	✓
Quản lý tài khoản quản trị phân cấp: Cho phép thiết lập các tài khoản quản trị với các mức độ quyền hạn khác nhau	✓
Cho phép quản lý các điểm cuối theo nhóm, có thể đưa các điểm cuối vào nhóm phù hợp với cơ cấu tổ chức	✓
Thống kê báo cáo: Quản trị viên dễ dàng thống kê xuất báo cáo, nắm bắt được tình hình an ninh trên hệ thống	✓

Sơ đồ



Thông số kỹ thuật

	Bkav Endpoint Security Detection & Respone Phiên bản Standard	Bkav Endpoint Security Detection & Respone (Bkav EDR)
Server	01	01
Core	8 Cores	8 Cores
Memory	8 GB	16 GB
Disk	500 GB	1 TB

Các phiên bản

Giải pháp EDR gồm bộ 02 sản phẩm:

- Giải pháp phát hiện và ứng phó - Bkav Endpoint Security Detection & Respone (Phiên bản Standard)
- Giải pháp phát hiện và ứng phó - Bkav Endpoint Security Detection & Respone (Bkav EDR)

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: DuAn@bkav.com
Bkav TP. HCM: Số 67, Đường số 3, Khu dân cư City Land, P.7, Q. Gò Vấp, TPHCM
Điện thoại: (028) 6296 6626 Số fax: (028) 2253 6103