Bkav
Security Operations Center (SOC)

Giới thiệu

Bkav Security Operations Center (Bkav SOC) là Trung tâm giám sát và điều hành An ninh mạng. Bkav SOC sử dụng công nghệ xử lý dữ liệu thông minh, bên cạnh việc giám sát tính sẵn sàng của các dịch vụ quan trọng trong hệ thống Bkav SOC còn có khả năng phát hiện sớm kiểu tấn công nằm vùng đặc trưng của các cuộc tấn công APT, tấn công DDoS, tấn công XSS… từ đó cảnh báo để quản trị hệ thống cách ly, xử lý các máy tính đã bị xâm nhập, ngăn chặn hacker có thể truy cập sâu vào hệ thống.

Bkav SOC - cung cấp thông tin cập nhật 24/7 về hiện trạng an ninh của toàn bộ hệ thống, kết nối dữ liệu của tất cả các thành phần quan trọng trong hệ thống như thiết bị tường lửa, các thiết bị mạng, máy chủ, máy trạm, đồng thời giám sát toàn bộ lưu lượng mạng… Các dữ liệu này sẽ được xử lý, phân tích để phát hiện ra các bất thường, từ đó hiển thị các cảnh báo cho người quản lý để kịp thời xử lý. Trung tâm điều hành SOC sẽ giúp nhanh chóng phát hiện mọi dấu hiệu tấn công vào hệ thống mạng, chủ động ứng phó, từ đó giảm thiểu các thiệt hại.

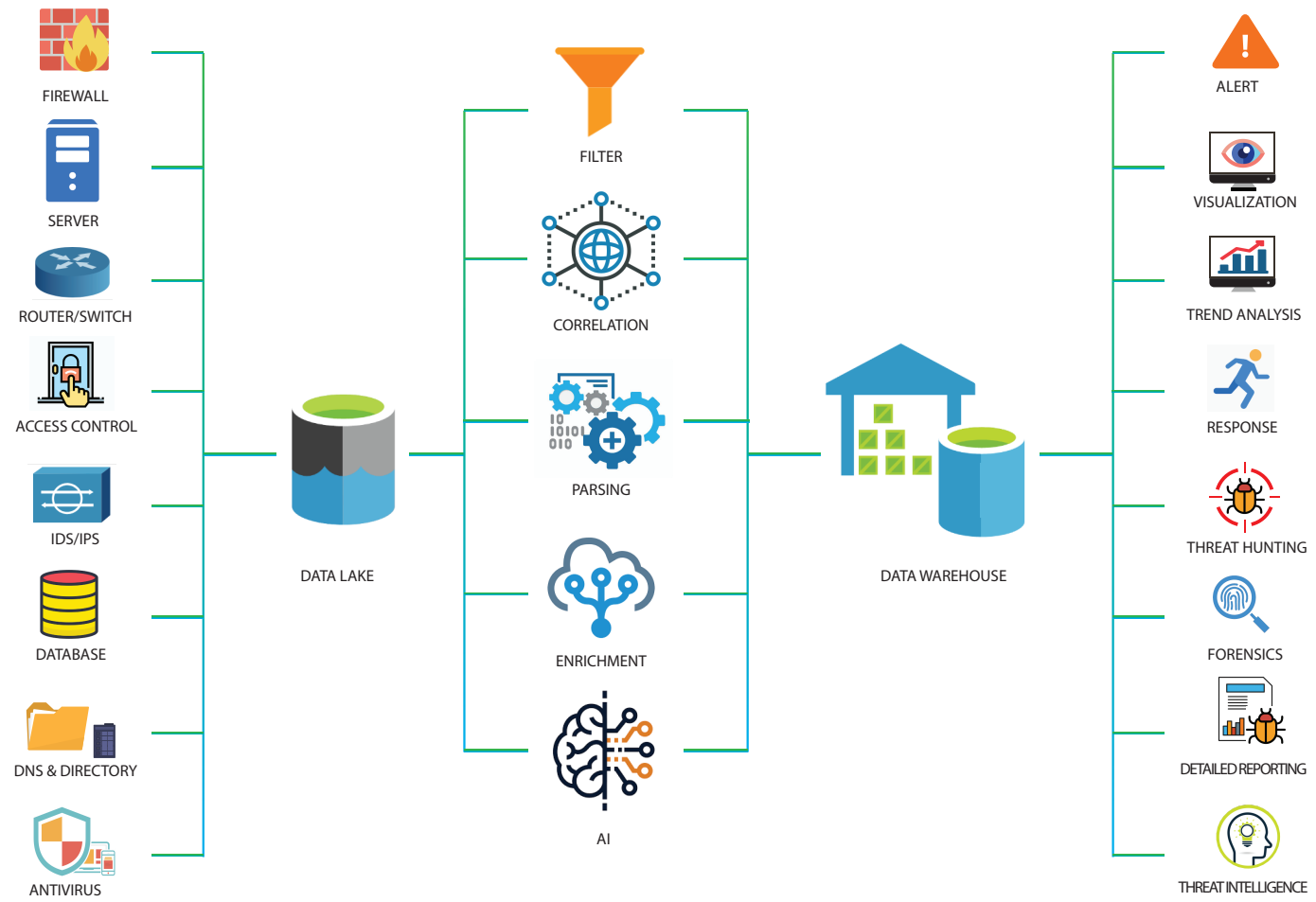
Các thành phần chính :

- Hệ thống thu thập, bắt toàn bộ gói tin.
- Phát hiện xâm nhập dựa trên network-based và host-based.
- Công cụ phân tích mạnh.
- Forensic.

Tính năng

- Giám sát, phát hiện và cảnh báo các cuộc tấn công DDoS.
  Giám sát, phát hiện và cảnh báo các tấn công APT trong hệ thống.
  Giám sát, phát hiện và cảnh báo các máy tính, server trong hệ thống nội bộ bị điều khiển bởi hacker.
- Giám sát, phát hiện và cảnh báo các máy tính, server, thiết bị mạng trong hệ thống có nguy cơ bị nhiễm mã độc có các hành vi rà quét thăm dò trong mạng nội bộ.
- Phát hiện các cuộc tấn công Web: SQL Injection, XSS …
- Phát hiện nguy cơ tiềm ẩn từ việc phân tích event log
- Giám sát, phát hiện và cảnh báo các máy tính, server, thiết bị mạng trong hệ thống đang hoạt động có lưu lượng bất thường.
- Giám sát, phát hiện và cảnh báo các máy tính, server có kết nối tới các dịch vụ không được phép.
- Giám sát theo thời gian thực và cảnh báo ngay lập tức cho quản trị qua SMS, Email.
- Gửi báo cáo định kỳ qua email cho đội ngũ quản trị và lãnh đạo về tình hình giám sát an ninh trong toàn hệ thống.
- Theo dõi, phát hiện, phân tích các cuộc xâm nhập tiềm năng trong thời gian thực qua lịch sử người dùng dữ liệu.
- Có các công nghệ để thu thập, phân tích dữ liệu, tiến hành điều tra
- Giám sát, phát hiện và cảnh báo các biểu hiện bất thường trên các máy tính, server: đăng nhập nhiều lần, hết dung lượng ổ cứng, …
- Phát hiện, ngăn chặn các phần mềm, hành vi nguy hiểm

Sơ đồ



Phát hiện

Giám sát 24/7: mạng, máy chủ, thiết bị đầu cuối, cơ sở dữ liệu, ứng dụng, website...

Phân tích

Phân tích hành vi độc hại, đáng ngờ với phân tích tự động nâng cao và phân tích tự động hóa dựa trên AI

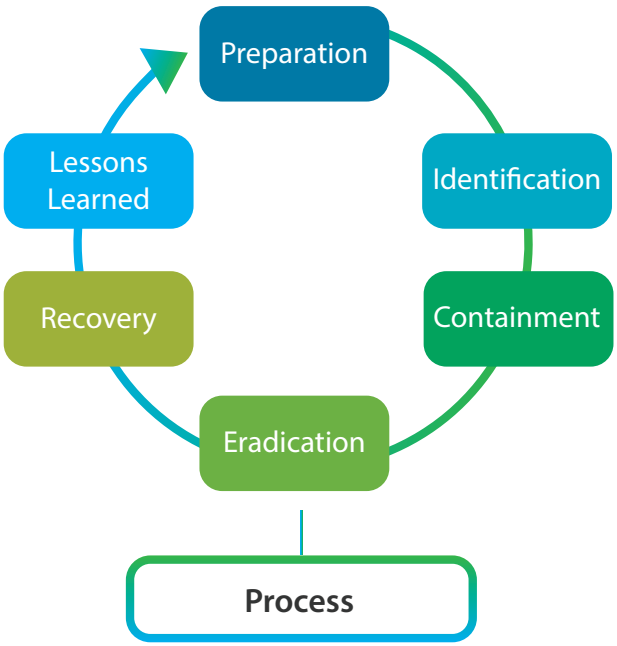
Phản ứng

Xác định chính xác, ưu tiên xác định các rủi ro, ngăn chặn và phục hồi nhanh, điều tra và xác định các mối đe dọa bảo mật

Thông số kĩ thuật

	CPU	Ram	Storage
• Master Server	4-8 CPU cores	8-16GB RAM	100GB - 1TB
• Storage Node	4-8 CPU cores	8-16GB RAM	100GB - 1TB
• Forward Node	1Gbps - ít nhất 10 cores	(Băng thông 50Mbps or less) - 4Gb	1TB
		(Băng thông 50Mbps - 500Mbps) - (16GB - 128GB)	4TB
		(Băng thông 500Mbps - 1000Mbps) - (128GB - 256GB	8TB

Quy trình xử lý sự cố



- **Prepation:** Chuẩn bị trước về con người, chính sách, dữ liệu, phần cứng phần mềm, phương tiện liên lạc, tài nguyên, tài liệu và các yếu tố cơ sở vật chất phát sinh khác.
- **Identication:** khi có những nhận biết ban đầu về sự cố thì cần thực hiện các bước như cảnh báo sớm, tiến hành giao việc cho các đơn vị chuyên trách và đưa ra các lưu ý, cảnh báo đối với người dùng.
- **Containment:** Được chia làm 3 giai đoạn là ngăn chặn ngắn hạn, tạo và lưu trữ images và ngăn chặn dài hạn. Đối với từng đối tượng thì sẽ bắt đầu ở các giai đoạn khác nhau.
- **Eradication:** Quá trình loại bỏ các thành phần nguy hiểm, nguy cơ và rủi ro sau khi thực hiện các bước ngăn chặn.
- **Recovery:** Đưa hệ thống quay về hoạt động bình thường như lúc chưa xảy ra sự cố.
- **Lessons Learned:** Sau khi các sự cố xảy ra thì có thể rút ra được các bài học kinh nghiệm, viết ra được tài liệu cho bước chuẩn bị.

Trụ sở chính: Tòa nhà Bkav, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội
Điện thoại: (024) 3763 2552 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