DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN

SECURITY OPERATIONS CENTER

Giới thiệu

Trong những năm gần đây, khi tần suất các cuộc tấn công mạng trên thế giới nói chung và ở Việt Nam nói riêng gia tăng ngày càng nhiều, mức độ nghiêm trọng và tinh vi ngày càng cao, các biện pháp đảm bảo An toàn thông tin (ATTT) cũng được các tổ chức, đơn vị chú ý và đầu tư bài bản hơn trước. Thay vì các giải pháp độc lập, chuyên biệt chỉ xử lý được một khía cạnh của cuộc tấn công, các cơ quan, tổ chức bị thuyết phục bởi các giải pháp tổng thể, đa tầng, nhiều lớp nhằm phát hiện và giải quyết triệt để các mối nguy hại chưa từng có tiền lệ. Và để có thể phát hiện sớm các vấn đề, sự cố an ninh mạng thì việc chủ động giám sát là việc quan trong phương án phòng ngừa, bảo vệ, cảnh báo sớm các cuộc tấn công mạng với mục tiêu đảm bảo các sự cố về an ninh mạng tiềm ẩn luôn được xác định, phân tích, điều tra và báo cáo một cách chính xác. Chính vì vậy, **dịch vụ giám sát ATTT của Bkav** được sinh ra với sứ mệnh nhằm đảm bảo an toàn thông tin cho các tổ chức một cách chủ động.

Mô tả dịch vụ

Dịch vụ giám sát an toàn thông tin của Bkav được thực hiện bởi **Trung tâm Giám sát và Điều hành an ninh không gian mạng Bkav** cung cấp:

- Giám sát 24x7x365
- Thu thập, theo dõi, phân tích, xác minh về các nguy cơ, sự cố về an ninh mạng, các cuộc tấn công vào các đối tượng được giám sát
- Phân tích nhật ký (log) từ nhiều nguồn dữ liệu: thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng, thiết bị đầu cuối
- Cảnh báo sự cố an ninh mạng thông qua nhiều kênh liên lạc (App SOC, SMS, Email, Điện thoại)
- Phối hợp ứng cứu sự cố theo quy trình ứng cứu chuẩn
- Tư vấn chuẩn hóa luật (rule) của các thiết bị bảo mật
- Định kỳ gửi báo cáo giám sát an ninh mạng
- Tư vấn, đề xuất biện pháp giúp đảm bảo an toàn, an ninh thông tin cho tổ chức

Ưu điểm

- Được đảm bảo về sự an toàn của hệ thống thông tin 24/7 trước các mối đe dọa
- Nhanh chóng phát hiện mối đe dọa từ đó có những giải pháp ngăn chặn và giảm thiểu rủi ro liên quan đến sự cố an ninh mạng
- Giảm chi phí đầu tư cho nhân sự chuyên trách về an toàn thông tin
- Hạn chế các cảnh báo giả, thời gian phân tích và cảnh báo sự cố một cách nhanh chóng
- Tận dụng được đội ngũ chuyên gia chuyên nghiệp có trình độ cao
- Thường xuyên được cập nhật về thông tin tình báo mạng, công nghệ mới nhất trong việc phân tích, giám sát

Quy trình

Giám sát lớp mạng

- ✓ Giám sát hoạt động của các thiết bị mạng, thiết bị bảo mật trong hệ thống thuộc phạm vi giám sát
- ✓ Phát hiện các kết nối, truy vấn tới các máy chủ điều khiển mạng botnet (C&C Server)
- ✓ Phát hiện các file mã độc, URL nguy hiểm được truyền qua môi trường mạng của tổ chức (với các giao thức không mã hóa)
- ✓ Phát hiện hiện các shellcode, payload tấn công khai thác lỗ hổng phần mềm, dịch vụ trong dữ liệu truyền tải trên mạng thông qua việc phân tích các dấu hiệu đặc trưng
- ✓ Phát hiện các hành vi bất thường như dò quét mạng, thăm dò hệ thống bằng các công cụ Nmap, Nessus, Acunetix,...
- ✓ Phát hiện các hoạt động của mã độc trong hệ thống
  - Phát hiện các hoạt động khai thác, lây nhiễm mã độc trong tổ chức
  - Phát hiện mã độc được tải về từ internet
- ✓ Phát hiện các cuộc tấn công khai thác lỗ hổng trên các thiết bị mạng: Cisco, TPLink,...
- ✓ Phát hiện các thông tin liên quan tới mật khẩu không được mã hóa hoặc mật khẩu yếu được truyền đi trong mạng
- ✓ Hỗ trợ xuất báo cáo thống kê theo các chỉ số:
  - Top dấu hiệu
  - Top IP
  - Top port
  - Top quốc gia

Giám sát lớp máy chủ

- ✓ Giám sát hoạt động của các máy chủ trong hệ thống thuộc phạm vi giám sát
- ✓ Thu thập giám sát nhật ký (log) của các máy chủ Windows/Linux/Unix
- ✓ Phát hiện các hành vi vi phạm chính sách truy cập, quản lý, thiết lập cấu hình hệ điều hành
- ✓ Phát hiện các kết nối của máy chủ ra các địa chỉ IP độc hại
- ✓ Phát hiện các cuộc tấn công, khai thác lỗ hổng của hệ điều hành (Windows, Linux, Unix)
- ✓ Phát hiện hoạt động của các tiến trình độc hại hoặc phần mềm độc hại trên máy chủ Windows/Linux
- ✓ Giám sát tính toàn vẹn của các file/thư mục hệ thống trên máy chủ Windows/Linux
- ✓ Phát hiện lỗ hổng bảo mật hệ điều hành
- ✓ Phát hiện thời gian, tần suất bất thường khi truy cập máy chủ

Giám sát lớp ứng dụng

- ✓ Giám sát hoạt động của các ứng dụng trong hệ thống thuộc phạm vi giám sát
- ✓ Thu thập giám sát log của các webserver như Nginx, Apache, IIS, ...
- ✓ Phát hiện các cuộc tấn công, khai thác lỗ hổng đối với các ứng dụng như: web, FTP, SQL, DNS, Telnet, SMTP,...
- ✓ Phát hiện các cuộc tấn công từ chối dịch vụ DoS, DDoS
- ✓ Phát hiện các dạng tấn công vào lớp ứng dụng SQL Injection, XSS, ...
- ✓ Phát hiện tấn công thay đổi giao diện
- ✓ Phát hiện tấn công Phishing

Giám sát lớp thiết bị đầu cuối

- ✓ Phát hiện các kết nối của thiết bị đầu cuối ra các địa chỉ IP độc hại
- ✓ Phát hiện hoạt động của các tiến trình/mã độc trên các máy Windows/Linux
- ✓ Thu thập, phân tích các IoC (Indicator of Compromise) từ các mối nguy hại
- ✓ Phát hiện hoạt động khai thác, leo thang đặc quyền trong các máy Windows/-Linux
- ✓ Phát hiện các hành vi vi phạm chính sách ATTT của tổ chức:
  - Phát hiện truy cập các website bị cấm
  - Phát hiện sử dụng các phần mềm bị cấm
  - Phát hiện việc sử dụng trái phép các thiết bị ngoại vi
  - Phát hiện việc chưa cập nhật bản vá trên các máy tính...
- ✓ Phát hiện lỗ hổng hệ điều hành của các máy Windows/Linux

Các gói dịch vụ

STT	Gói dịch vụ	Loại ngày làm việc	Giờ làm việc	Ngày làm việc/tuần	Ngày làm việc/năm
1	Gói **Copper** (Giám sát theo giờ làm việc hành chính) - 8h	Ngày thường	Giờ hành chính	5	250
2	Gói **Silver** (Giám sát ngoài giờ hành chính bao gồm cả thứ 7, chủ nhật nhưng trừ ngày lễ tết) - 16h	Ngày thường	Ngoài giờ Giờ làm đêm	5	250
		Ngày nghỉ cuối tuần	Giờ hành chính Ngoài giờ Giờ làm việc đêm	2	104
3	Gói **Gold** (Giám sát 24*7*365) - 24h	Ngày thường	Giờ hành chính Ngoài giờ Giờ làm việc đêm	7	250
		Ngày nghỉ cuối tuần	Giờ hành chính Ngoài giờ Giờ làm việc đêm		104
		Ngày nghỉ lễ	Giờ hành chính Ngoài giờ Giờ làm việc đêm		10

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