1. **Phân tích những điểm yếu trong mô hình mạng hiện tại (tối thiểu phân tích 10 rủi ro liên quan tới ATTT).**
    - Chưa có chính sách sao lưu và phục hồi dữ liệu nên sẽ dễ bị mất tài liệu hoặc không thể khôi phục tài liệu về phiên bản trước nếu có sự cố xảy ra
    - Chưa có chính sách bảo mật dữ liệu nên thông tin nội bộ, thông tin quan trọng, mang tính chiến lược có khả năng bị tiết lộ ra bên ngoài
    - Chưa có chính sách về vấn đề an toàn thông tin trong hệ thống nên thông tin nội bộ, quan trọng dễ dàng bị tiết lộ ra bên ngoài. Nhân viên dễ trở thành đối tượng bị attacker lợi dụng
    - Chưa có chính sách và triển khai hệ thống access control dẫn tới nhận viên có thể vượt quá quyền hạn của mình trong việc truy cập database
    - Chưa có firewall chuyên dụng nên dễ bị tấn công từ bên ngoài và cả bên trong
    - Chưa có phần mềm antivirus nên dễ bị nhiễm và lây nhiễm malware trong công ty
    - Chưa có hệ thống IDS/IPS, SIEM hay các hệ thống khác có chức năng bảo vệ mạng, các thiết bị đầu cuối khỏi các cuộc tấn công physical và digital
    - Chưa phân vùng mạng cho các bộ phận trong office nên dữ liệu từ phòng ban này có bị phòng ban khác biết được và các nhân viên cũng có thể vượt quyền hạn của mình trong việc truy cập dữ liệu công ty.
    - Chưa có hệ thống giám sát và phân tích lưu lượng mạng hoặc hành vi truy cập của người dùng cả trong mạng nội bộ và mạng Internet nói chung
    - Sử dụng DataCenter từ nhà cung cấp khác nên có khả năng rò rỉ, mất mát thông tin nếu phía nhà cung cấp không đáng tin hoặc bị attacker tấn công hoặc có thiên tai xảy ra ở nơi đặt DataCenter.
    - Dùng vSphere để chạy DHCP Server, File Server, HR Server, CRM Server (Customer relationship manager server) do đó nếu vSphere có lỗ hổng thì các server này đều có thể bị chiếm đạt.
    - Chưa triển khai hệ thống backup data để đối phó với các cuộc tấn công nhằm vào data như ransomware, wiper attack, hoặc trường hợp các thiết bị trong công ty bị tác động vật lý, xảy ra thiên tai,…
2. **Phân tích những rủi ro liên quan tới mất mát dữ liệu**
    a. **Attacker (5 rủi ro)**

- Attacker tấn công vào các lỗ hổng hiện có trong công ty
  Việc chưa có phần mềm firewall chuyên dụng, IPS/IDS hay các hệ thống bảo vệ có chức năng ngăn chặn scanning dẫn tới attacker có thể sử dụng nmap, nessus, open VAS để phát hiện các thông tin như port đang mở, OS, service đang chạy trên các endpoint từ đó phát hiện các lỗ hổng mà attacker có thể khai thác để chiếm quyền truy cập, kiểm soát hay lấy trộm dữ liệu.
  VD: attacker khai thác lỗ hổng trên Webserver để thực hiện tấn công SQL injection nhằm truy cập database trái phép trên server này.

- Attacker tiêm nhiễm mã độc vào các endpoint hoặc server trong công ty
  Việc không có phần mềm Anti-virus, EDR, NDR, firewall tích hợp antivirus… tạo cơ hội cho các attacker thực hiện các cuộc tấn công bằng các malware như trojan, spyware để thu thập dữ liệu; tiêm nhiễm ransomware để tống tiền công ty; dùng worm, rootkit để tạo botnet, chiếm quyền truy cập và điều khiển các thiết bị,…

- Attacker đánh cắp dữ liệu trong quá trình truyền tải
  Không có phần mềm firewall chuyên dụng, hệ thống phát hiện xâm nhập (IDS), hệ thống phòng ngừa xâm nhập (IPS) tạo cơ hội cho các attacker sử dụng các kỹ thuật như Man-in-the-Middle, Sniffing (nghe lén) để đánh cắp dữ liệu trong quá trình truyền tải

- Attacker giả mạo danh tính và có quyền truy cập dữ liệu
  Không có DNS Server triển khai DNSSEC (DNS Security Extensions) các attacker có thể sử dụng IP Spoofing hoặc DNS Spoofing để làm giả mạo danh tính và có quyền truy cập vào dữ liệu

- Attacker lấy được những thông tin nhạy cảm như tên đăng nhập, mật khẩu, dữ liệu nội bộ để kiểm soát hệ thống
  Không có chính sách đào tạo bảo mật cho nhân viên, kẻ tấn công có thể giả mạo email từ đối tác hoặc khách hàng để yêu cầu nhân viên cung cấp thông tin đăng nhập, mật khẩu hoặc tải xuống các tệp độc hại. Những email này thường sử dụng các công cụ tinh vi như phần mềm tạo email giả mạo (Email Spoofing Tools).

- Attacker xâm nhập vào cơ sở dữ liệu

  Chưa có chính sách bảo mật web, attacker có thể thực hiện các cuộc tấn công web bằng cách sử dụng các kỹ thuật như SQL Injection, Cross-Site Scripting (XSS) hoăcj Cross-site Request Forgery (CSRF) để xâm nhập vào cơ sở dữ liệu.

b. Nhân viên (5 rủi ro)

- Nhân viên tiết lộ thông tin nội bộ, quan trọng hay mang tính chiến lược ra bên ngoài

  Việc không phân vùng mạng và cấu hình firewall theo chính sách bảo mật, không có hệ thống giám sát hành vi người dùng như HIDS, NDR dẫn tới nhân viên dễ dàng chụp ảnh, nhắn tin và đính kèm tài liệu của công ty rồi gửi nó ra bên ngoài thông qua các ứng dụng nhắn tin như zalo, messenger, gmail,…

- Nhân viên tải phần mềm hoặc các file từ nguồn không đáng tin cậy

  Việc không có phần mềm Anti-virus, EDR, NDR,…để bảo vệ endpoint khiến chúng rất dễ bị chiếm đoạt khi nhân viên tải các mã độc của attacker về máy tính. Ngoài ra việc không có các chính sách tập huấn để nâng cao nhận thức nhân viên về vấn đề rủi ro và an toàn thông tin cũng khiến attacker dễ lợi dụng nhân viên để tiêm nhiễm mã độc và lay lan chúng trong công ty.

- Nhân viên click vào các link lạ, truy cập tới các trang web độc hại, giả mạo do attacker tạo ra

  Việc không triển khai hệ thống giám sát mạng như IDS, NSM, các hệ thống phân tích và phát hiện sự cố như SIEM, NDR,… khiến nhân viên có thể bị attacker lừa để lấy thông tin về công ty hay thông tin về nhân viên (như tài khoản, ID nhân viên, chức vụ,…) để phục vụ mục đích giả mạo của chúng; trở thành nạn nhân trong các cuộc tấn công Browser-Based Attacks như CSRF, XSS, Drive-By Downloads, ,Clickjacking,…

- Nhân viên vô ý làm mất dữ liệu

Nhân viên không được đào tạo đầy đủ về quy trình quản lý dữ liệu hoặc bảo mật thông tin. Việc sao chép, di chuyển, hoặc xóa dữ liệu quan trọng một cách không cẩn thận có thể gây mất mát dữ liệu. Hoặc bị đánh cắp các thiết bị như điện thoại, máy tính xách tay, USB, có chứa dữ liệu nhạy cảm và không có các phương pháp bảo vệ phù hợp dẫn đến dữ liệu công ty có thể bị đánh cắp

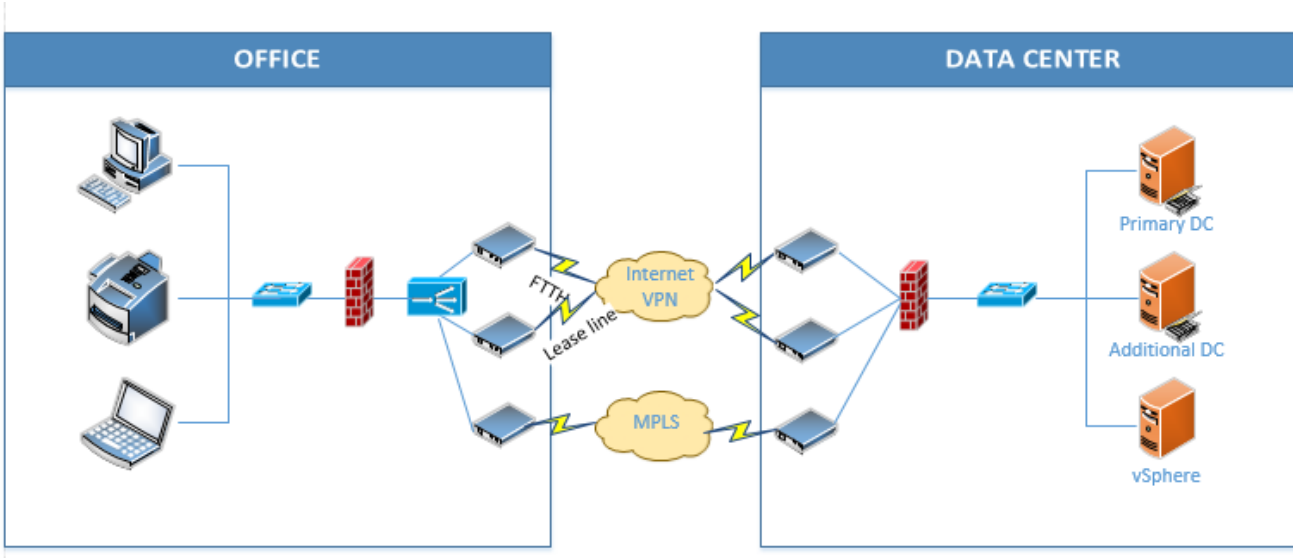
- Không có chính sách đào tạo cho nhân viên về an toàn thông tin, dẫn đến việc nhân viên có thể vô tình khiến dữ liệu gặp rủi ro, chẳng hạn như tấn công Social Engineering, tấn công Phishing, sử dụng mật khẩu yếu,...

☐ **Phương pháp và công cụ assessment**

	Rủi ro liên quan tới mất mát dữ liệu	**Phương pháp đánh giá**	
Attacker	Attacker tấn công vào các lỗ hổng hiện có trong công ty	- **Scanning và kiểm tra lỗ hổng:** Sử dụng các công cụ kiểm tra lỗ hổng như **Nmap**, **Nessus**, **OpenVAS** để xác định các cổng mở, dịch vụ đang chạy, và lỗ hổng trên hệ thống. - **Phân tích cấu hình hệ thống:** Đánh giá các dịch vụ đang chạy (OS, web server, database server) để phát hiện các điểm yếu.	- **Nmap** định các - **Nessus** đã biết t thống. - **OpenV** lỗ hổng liệu lỗ h
	Attacker tiêm nhiễm mã độc vào các endpoint hoặc server trong công ty	- **Kiểm tra khả năng phòng chống mã độc:** Xác định mức độ bảo vệ hiện tại, ví dụ, có sử dụng phần mềm **Anti-virus**, **EDR** hay không. - **Phân tích hành vi endpoint:** Sử dụng các công cụ mô phỏng tấn công (malware simulation tools) để đánh giá khả năng phát hiện và ngăn chặn.	- **Metas** để kiểm phát tán - **Cucko** hoạt độn tích khả
	Attacker đánh cắp dữ liệu trong quá trình truyền tải	- **Kiểm tra bảo mật truyền tải:** Sử dụng các công cụ để kiểm tra việc triển khai mã hóa và phát hiện các dữ liệu truyền tải không được bảo vệ.	- **Wiresh** kiểm tra tải qua n

		- **Mô phỏng tấn công MITM (Man-in-the-Middle):** Để xác định khả năng hệ thống chống lại các kỹ thuật nghe lén.	- **Etterc** MITM đ mạng.
	Attacker giả mạo danh tính và có quyền truy cập dữ liệu	- **Đánh giá bảo mật DNS:** Kiểm tra việc triển khai **DNSSEC** hoặc các phương pháp ngăn chặn tấn công DNS Spoofing. - **Mô phỏng tấn công giả mạo:** Sử dụng các công cụ để mô phỏng tấn công như **IP Spoofing** hoặc **DNS Spoofing**	- **dnsspo** bảo vệ c . - **Scapy:** chỉnh ph Spoofing
	attacker lấy được những thông tin nhạy cảm như tên đăng nhập, mật khẩu, dữ liệu nội bộ để kiểm soát hệ thống	- **Kiểm tra nhận thức nhân viên:** Tạo các chiến dịch giả lập tấn công email (phishing simulation). - **Phân tích luồng email:** Xác định các lỗ hổng trong cấu hình bảo mật email.	- **PhishM** phishing bảo mật - **Social-** **(SET):** giả mạo
	attacker xâm nhập vào cơ sở dữ liệu	- **Kiểm tra lỗ hổng web:** Dò quét và kiểm tra các lỗ hổng như **SQL Injection**, **XSS**, và **CSRF**. - **Mô phỏng tấn công:** Sử dụng các công cụ tấn công để đánh giá tính bảo mật của ứng dụng web.	- **Burp S** thác lỗ h - **OWAS** đánh giá
Nhân viên	Nhân viên tiết lộ thông tin nội bộ, quan trọng hay mang tính chiến lược ra bên ngoài	- **Giám sát hành vi người dùng:** Đánh giá khả năng giám sát hoạt động của người dùng để phát hiện hành vi gửi dữ liệu nhạy cảm ra ngoài qua các ứng dụng hoặc thiết bị. - **Đánh giá phân quyền và kiểm soát truy cập:** Kiểm tra các chính sách về phân quyền truy cập và cấu hình firewall	- **HIDS** **Detectio** hành vi endpoint - **DLP (** Ngăn ch gửi dữ li ngoài. - **SIEM** **and Eve** tích và p

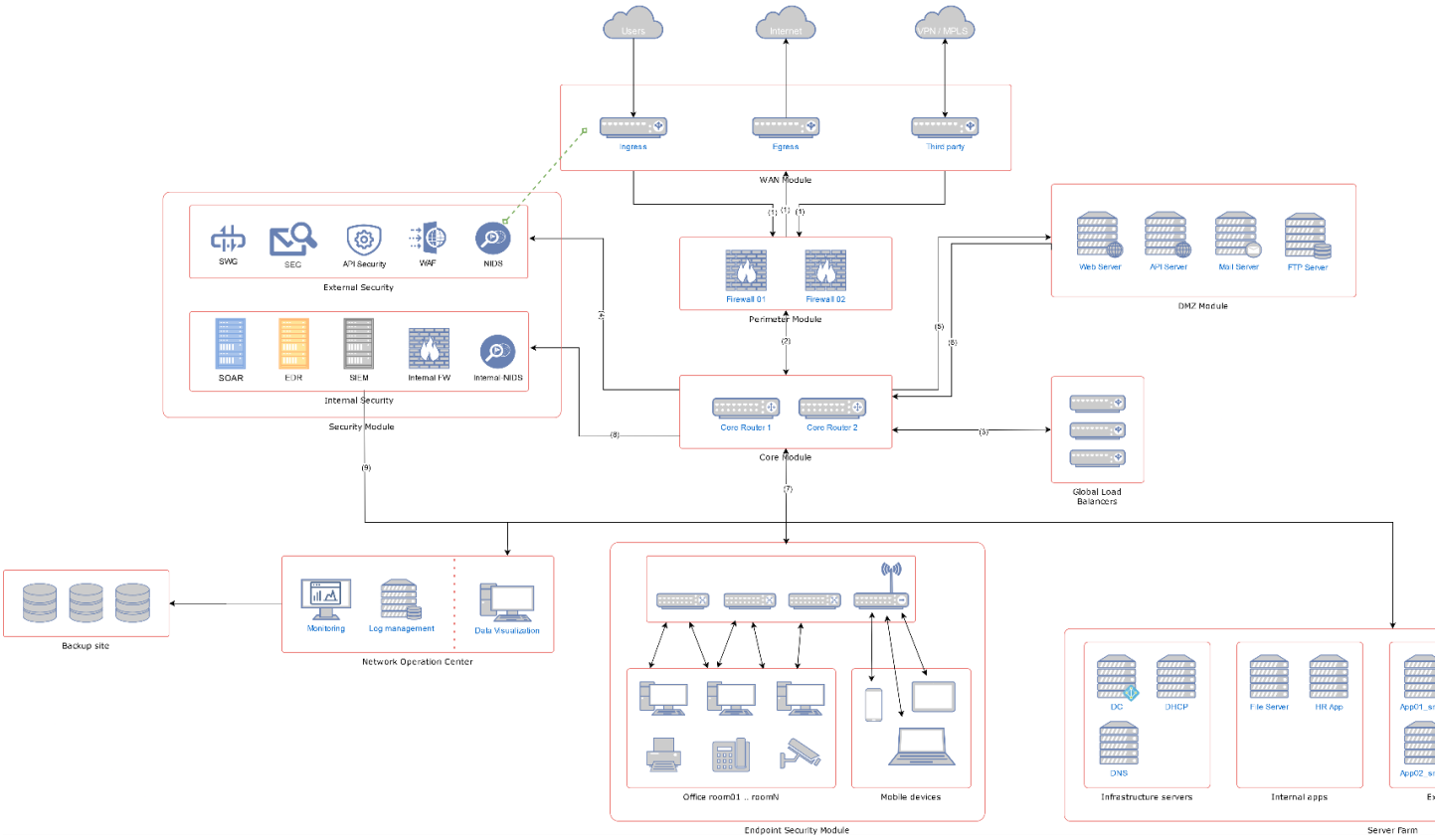
			thường c
	Nhân viên tải phần mềm hoặc các file từ nguồn không đáng tin cậy	- **Kiểm tra bảo vệ endpoint:** Xác định sự hiện diện của phần mềm bảo mật như **Anti-virus**, **EDR**, **NDR** để ngăn chặn mã độc xâm nhập qua phần mềm tải về. - **Đánh giá chính sách bảo mật và đào tạo nhân viên:** Kiểm tra các chương trình đào tạo và nhận thức bảo mật cho nhân viên về rủi ro khi tải phần mềm và file từ các nguồn không rõ ràng.	
	Nhân viên click vào các link lạ, truy cập tới các trang web độc hại, giả mạo do attacker tạo ra	- **Kiểm tra nhận thức nhân viên:** Sử dụng các chiến dịch mô phỏng tấn công phishing hoặc link độc hại để đánh giá phản ứng. - **Đánh giá hệ thống giám sát mạng:** Kiểm tra hiệu quả của các công cụ như IDS, NSM trong việc phát hiện truy cập vào các trang web độc hại.	- **IDS (I** **System)** các hành lượng m - **SIEM** **and Eve** tích các hiện tấn hại. - **Phishi** công cụ kết hoặc
	Nhân viên vô ý làm mất dữ liệu	- **Đánh giá bảo vệ thiết bị di động và di chuyển dữ liệu:** Xem xét việc bảo vệ các thiết bị như laptop, USB và các phương tiện lưu trữ di động khỏi việc mất mát dữ liệu.	- **Cloud** dữ liệu đ khôi phụ - **DLP (** Giám sá chép dữ bảo mật.
	Không có chính sách đào tạo cho nhân viên về an toàn thông tin	- **Đánh giá chương trình đào tạo và nhận thức bảo mật:** Kiểm tra xem công ty có chương trình đào tạo bảo mật định kỳ cho nhân viên không và mức độ hiệu quả của các khóa đào tạo này	- **Securi** **Platform** nhận thú giúp nhâ nhận diệ



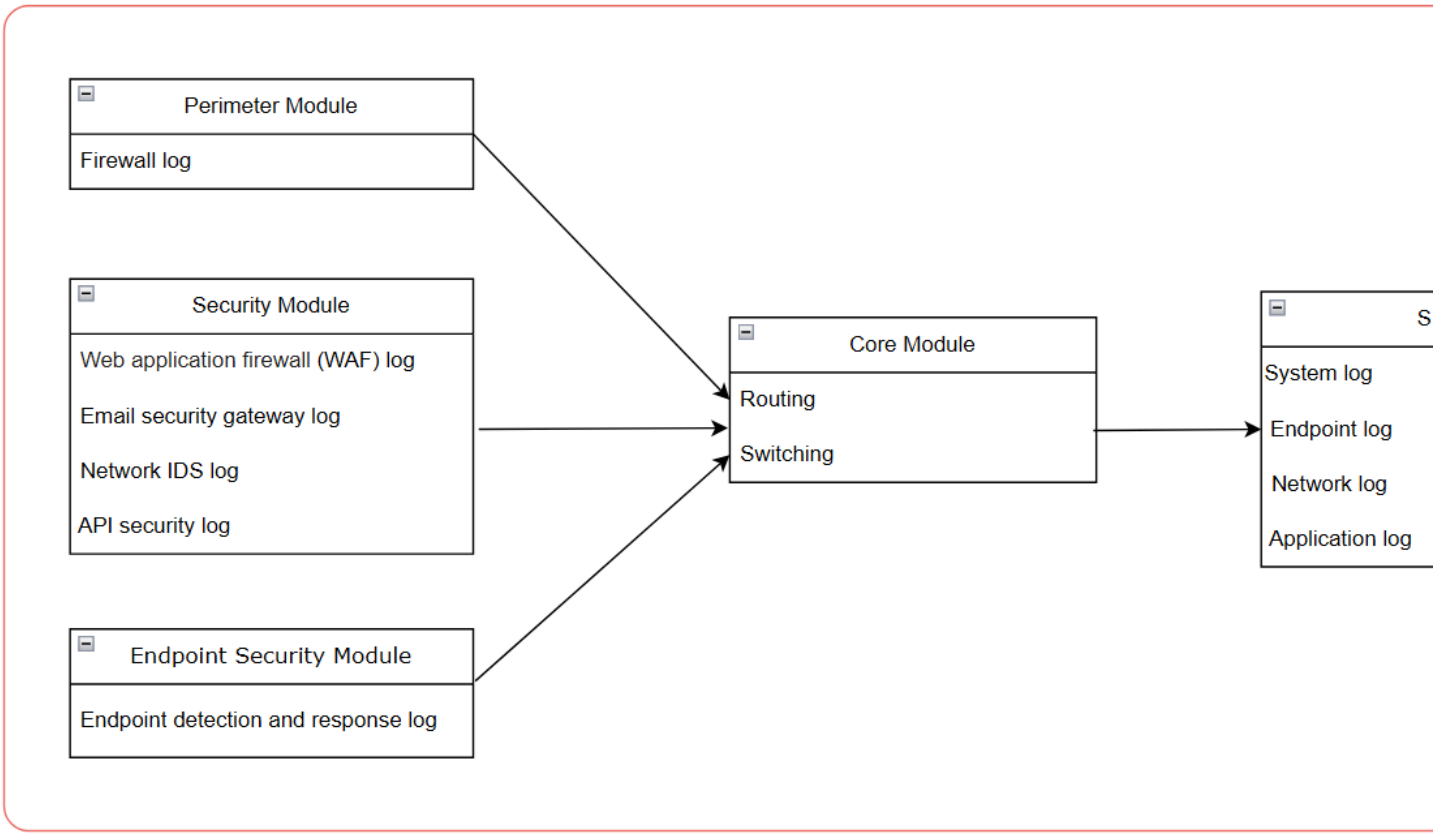
☐ **Bảng Risk Score của hệ thống hiện tại.**

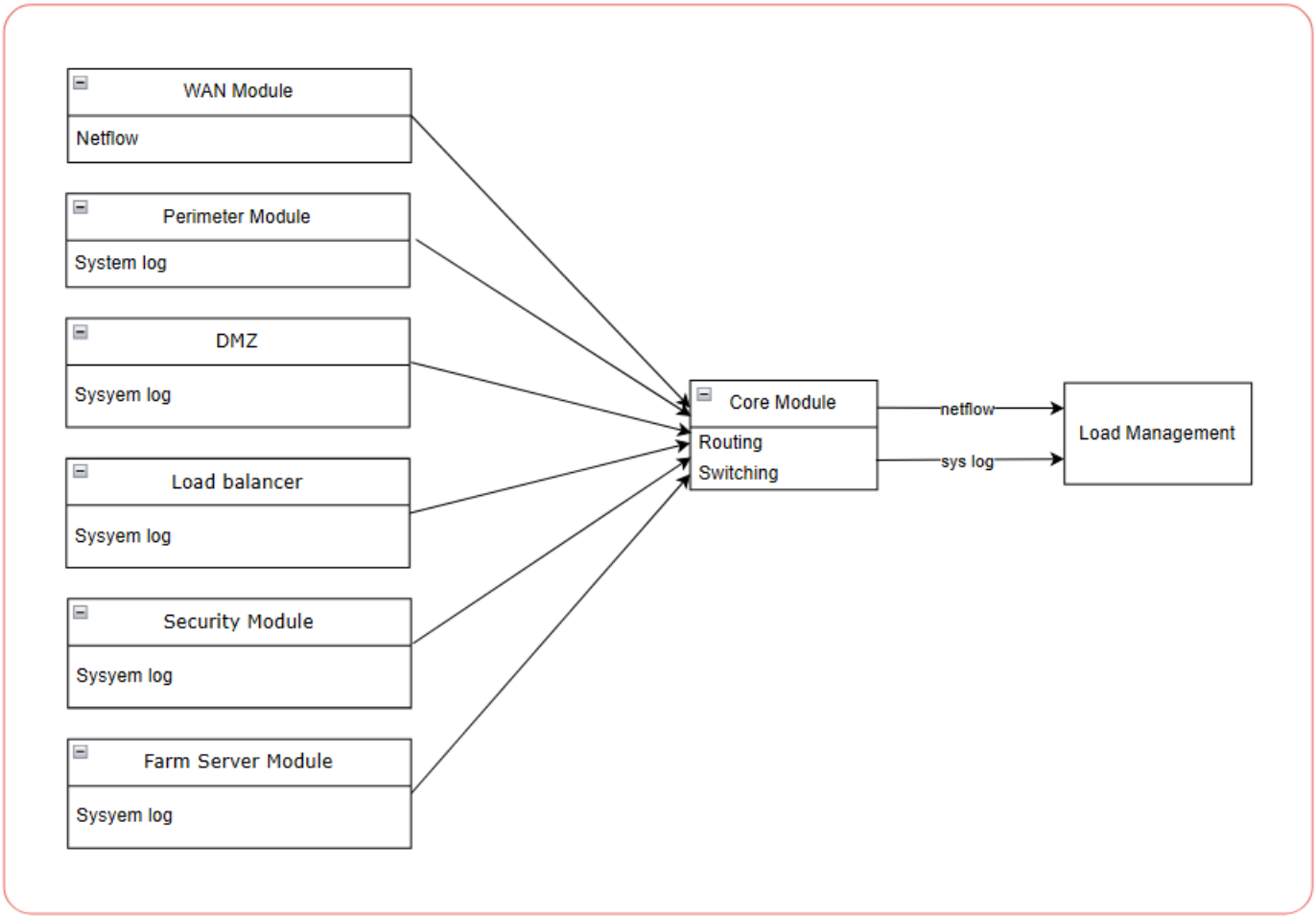
3. **Thiết kế lại hệ thống – mạng với tính bảo mật tốt nhất có thể (hướng tới giải pháp chống thất thoát dữ liệu)**

a. Vẽ mô hình tổng thể



* Log Management

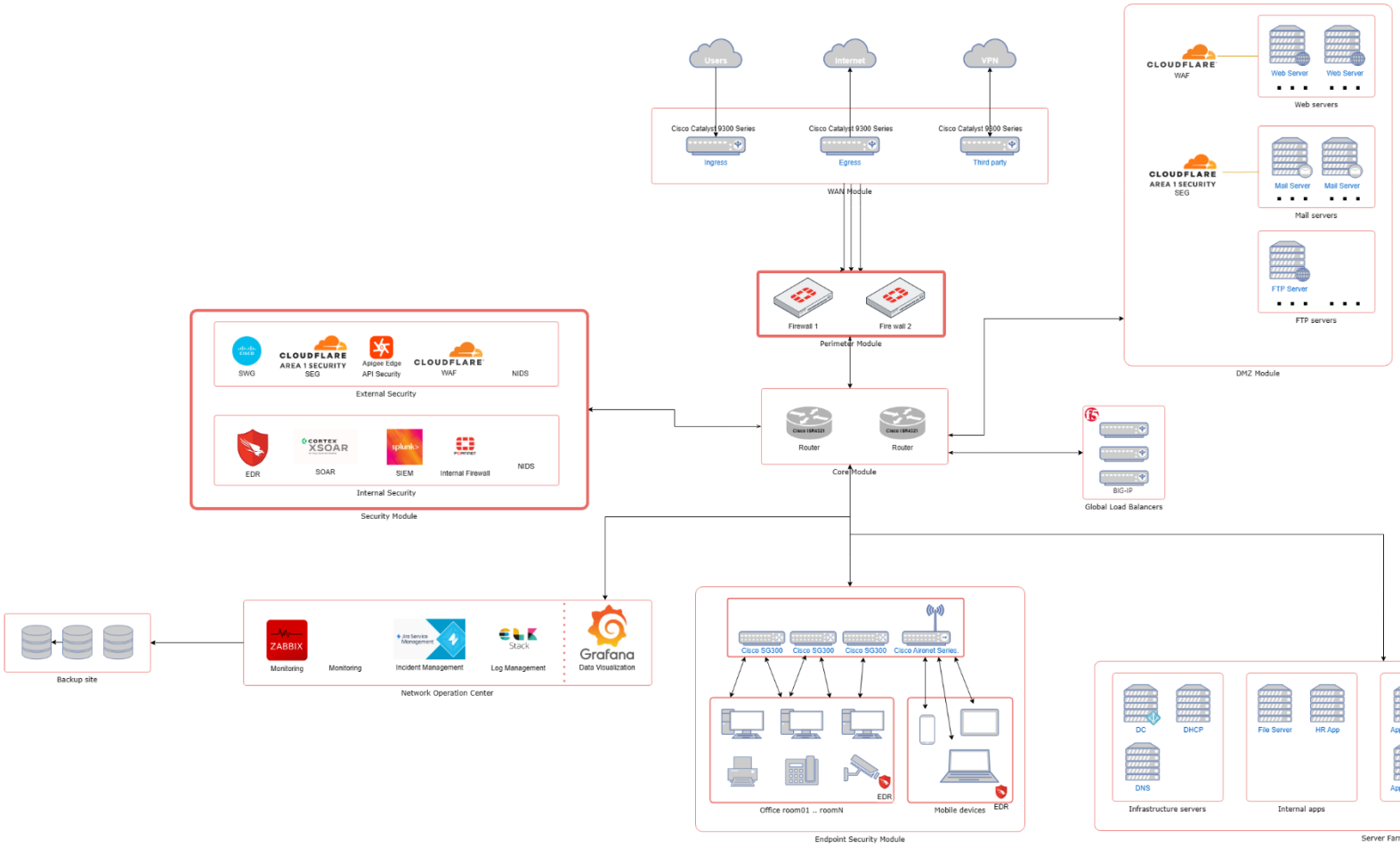




Log

b. Vẽ mô hình chi tiết cho từng phần (Web Security, Email Security, IDS/IPS Security,…)

+



c. Thuyết minh giải pháp cho từng phần (mỗi giải pháp thuyết minh 2 trang)

Security Module:

1. Firewall: fortinet

FortiGate NGFW là tường lửa mạng được triển khai nhiều nhất, chiếm hơn 50% thị phần trên toàn thế giới với khả năng cung cấp nhiều tùy chọn triển khai khác nhau (như thiết bị vật lý hoặc ảo hoá, public cloud và private cloud, hay môi trường kết hợp) và các dịch vụ được quản lý phù hợp với nhiều nhu cầu kinh doanh và ngân sách khác nhau.

Ngoài ra chính hiệu suất, khả năng mở rộng và giá cả phải chăng đã khiến FortiGate NGFW trở thành lựa chọn hàng đầu của các tổ chức, doanh nghiệp ở mọi quy mô.

Các điểm nổi bật của FortiGate NGFW:

+ Robust performance:

Được hỗ trợ bởi bộ xử lý bảo mật được cấp bằng sáng chế, FortiGate cung cấp thông lượng cao và độ trễ thấp, đảm bảo bảo mật không làm giảm hiệu suất mạng, ngay cả trong môi trường có nhu cầu cao.

+ AI/ML threat intelligence

FortiGate NGFW được tích hợp với FortiGuard AI-Powered (một dịch vụ bảo vệ) cung cấp thông tin về mối đe dọa đã cập nhật nhằm ngăn chặn, phát hiện và ứng phó các cuộc tấn công trong thời gian thực.

+ Seamless integration

Là một phần của Fortinet Security Fabric, FortiGate NGFW hoạt động trơn tru với các sản phẩm Fortinet khác, tối ưu hóa việc triển khai với tính năng zero-touch, auto-discovery

+ Unified management

Các công cụ quản lý trực quan giúp đơn giản hóa việc quản lý, hợp lý hóa việc cung cấp hàng loạt cũng như quản lý chính sách cho tường lửa FortiGate và các thiết bị được kết nối khác một cách hiệu quả

+ Cost effectiveness

Với SD-WAN, ZTNA và các tính năng mạnh mẽ, FortiGate NGFW mang lại nhiều lợi ích nhưng chi ph cao so với việc quản lý nhiều giải pháp bảo mật khác nhau.

FortiGate NGFW rất linh hoạt và hỗ trợ nhiều tình huống khác nhau để tăng cường bảo mật và hiệu suất mạng.

Sau đây là một số trường hợp sử dụng phổ biến:

+ Bảo mật chu vi: Hoạt động như tuyến phòng thủ đầu tiên của mạng để lọc lưu lượng truy cập vào và ra nhằm ngăn chặn truy cập trái phép và giảm thiểu các mối đe dọa.

+ SD-WAN an toàn: Cung cấp kết nối an toàn và tối ưu cho các chi nhánh trong khi vẫn đảm bảo hiệu suất ứng dụng.

+ Truy cập từ xa: Cho phép truy cập từ xa an toàn vào các tài nguyên của công ty bất kể vị trí của nhân viên.

+ Phân đoạn nội bộ: Phân đoạn các phần khác nhau của mạng để giảm bề mặt tấn công, cô lập dữ liệu nhạy cảm hoặc các hệ thống quan trọng để ngăn chặn vi phạm.

+ Bảo mật đám mây: Bảo vệ khối lượng công việc đám mây, bảo mật dữ liệu và ứng dụng trong khi vẫn đảm bảo tuân thủ các chính sách bảo mật.

+ Kiểm soát ứng dụng: Kiểm soát và giám sát việc sử dụng ứng dụng trong mạng, ngăn chặn các truy cập được ủy quyền và giảm các mối đe dọa từ các ứng dụng rủi ro.

+ Bảo mật IoT: Bảo mật các thiết bị được kết nối với mạng, đảm bảo các thiết bị này được giám sát và quản lý hiệu quả để ngăn ngừa lỗ hổng.

2. Security Module

2.1 NIDS: Suricata

Suricata là giải pháp bảo mật mã nguồn mở do Open Information Security Foundation (OISF) phát triển. Suricata không chỉ giúp phát hiện xâm nhập mà còn đóng vai trò quan trọng trong việc bảo vệ hệ thống mạng khỏi các mối đe dọa bằng cách kết hợp nhiều tính năng tiên tiến.

Dựa trên các quy tắc và chữ ký định nghĩa sẵn, Suricata có thể nhanh chóng phát hiện các cuộc tấn công mạng. Nhờ khả năng phân tích sâu các gói (DPI – Deep Packet Inspection) và xử lý chúng theo thời gian thực, Suricata có thể phát hiện các mẫu tấn công phức tạp ngay khi chúng xảy ra. Không chỉ giúp phát hiện hoạt động đáng ngờ, Suricata còn tạo cảnh báo và chặn các gói tin độc hại, bảo vệ mạng trước các mối đe dọa tiềm ẩn.

Với việc sử dụng Suricata, người dùng có thể chủ động phát hiện, ngăn chặn các cuộc tấn công mạng, đồng thời tăng cường an ninh mà lại tiết kiệm chi phí so với việc mua và sử dụng các phần mềm bảo mật khác.

Suricata tương thích với nhiều hệ điều hành khác nhau, từ các bản phân phối Linux phổ biến như Ubuntu, CentOS, đến các hệ thống mạng chuyên dụng.

Một số điểm nổi bật của Suricata:

+High Performance:

+Automatic Protocol Detection: Suricata sẽ tự động phát hiện các giao thức như HTTP trên bất kỳ cổng nào và áp dụng logic phát hiện và ghi nhật ký phù hợp. Điều này giúp ích rất nhiều trong việc tìm phần mềm độc hại và kênh CnC.

+Lua Scripting: Sử dụng các chức năng và phân tích nâng cao để phát hiện những điều không thể phát hiện được bằng cú pháp trong bộ quy tắc.

+Tích hợp tốt với các hệ thống khác: Suricata có thể làm việc cùng với các công cụ khác như ELK stack (Elasticsearch, Logstash, Kibana) để phân tích log, giúp cung cấp các báo cáo chi tiết hơn về tình trạng an ninh mạng.

+Mỗi thành phần tích hợp suricata có thể kiểm tra lưu lượng hàng Gigabit

2.2 Cloudflare Web Application Firewall

Cloud WAF (Web Application Firewall) là một công cụ bảo mật mạng được triển khai trên môi trường đám mây (cloud) nhằm bảo vệ ứng dụng web khỏi các cuộc tấn công mạng và các loại tấn công web phổ biến. Điều này đặc biệt quan trọng đối với các doanh nghiệp và tổ chức có các ứng dụng web quan trọng, vì chúng thường là mục tiêu của các hacker và tấn công trực tuyến.

Cloud WAF hoạt động bằng cách giám sát và kiểm tra các yêu cầu và lưu lượng mạng đến các ứng dụng web. Nó sử dụng một loạt các quy tắc và chữ ký để phát hiện và ngăn chặn các hành vi đáng ngờ hoặc tấn công, bao gồm SQL injection, cross-site scripting (XSS), và nhiều loại tấn công khác.

Mục tiêu chính của Cloud WAF là bảo vệ dữ liệu của ứng dụng, ngăn chặn tiền thất thoát, và đảm bảo tính khả dụng của ứng dụng web. Nó cũng giúp nâng cao tuân thủ các quy tắc bảo mật và đáp ứng yêu cầu bảo mật và tuân thủ.

Cloud WAF (Web Application Firewall) hoạt động bằng cách giám sát và kiểm soát lưu lượng mạng đến ứng dụng web. Quá trình hoạt động của Cloud WAF bao gồm các bước sau:

+ Giám sát lưu lượng

+ Phân tích lưu lượng

+ So sánh với quy tắc và chữ ký

+ Ngăn chặn tấn công

2.3 API sec: apigee

Apigee là một nền tảng quản lý API (API Management Platform) được phát triển bởi Google, hỗ trợ các tổ chức thiết kế, bảo mật, triển khai, phân tích và mở rộng các API. Apigee được sử dụng để kết nối các hệ thống backend, dịch vụ và ứng dụng, đồng thời cung cấp các công cụ giúp quản lý API hiệu quả hơn.

Các tính năng của apigee:

- Quản lý vòng đời API
- Bảo mật API
- Tích hợp
- Quản lý lưu lượng và hiệu suất
- Phân tích và giám sát API
- Công cụ dành cho nhà phát triển

Apigee hoạt động như một **API Gateway** và một nền tảng quản lý API. Nó đứng giữa hệ thống backend (nơi chứa dữ liệu và logic) và các ứng dụng hoặc dịch vụ sử dụng API (client), giúp đảm bảo kết nối an toàn, hiệu quả và được kiểm soát.

- **Client gửi yêu cầu** đến một API thông qua URL proxy của Apigee.
- Apigee nhận yêu cầu và thực hiện:
- Xác thực quyền truy cập (nếu được cấu hình).
- Áp dụng các chính sách bảo mật và chuyển đổi dữ liệu.
- Apigee chuyển yêu cầu đến hệ thống backend.
- Backend xử lý yêu cầu và gửi phản hồi ngược lại qua Apigee.
- Apigee áp dụng các chính sách xử lý (nếu cần) trước khi gửi phản hồi cuối cùng về client.

2.4 Secure email gateway (SEG): Cloudflare Email Security

Cloudflare Email Security là một giải pháp bảo mật email dựa trên đám mây, được thiết kế để bảo vệ doanh nghiệp khỏi các mối đe dọa qua email ngày càng tinh vi. Giống như một lớp áo giáp bảo vệ, Cloudflare Email Security giúp lọc và chặn các email độc hại, spam, phishing và các cuộc tấn công khác trước khi chúng đến được hộp thư đến của người dùng.

Các đặc điểm chính của Cloudflare Email Security:

+ Cloudflare Email Security cung cấp khả năng bảo vệ chủ động chống lại các mối đe dọa qua email.

+ Bằng cách quét Internet để tìm các trang web lừa đảo đang được xây dựng, Area 1 xác định các chiến dịch lừa đảo mới trước khi chúng xảy ra.

+ Nó cũng sử dụng máy học để phân tích tài khoản email và nội dung nhằm xác định BEC và các mối đe dọa kỹ thuật xã hội khác.

+ Bảo vệ chống lại các cuộc tấn công lừa đảo có chủ đích và sử dụng kết hợp email với các ứng dụng khác để tấn công công người dùng nhằm đạt được sự truy cập trái phép.

2.5 Secure Web Gateway (SWG) : Cisco Umbrella's Secure Web Gateway

Cisco Umbrella Secure Web Gateway (SWG) là một giải pháp bảo mật mạng thế hệ mới, hoạt động như một lớp bảo vệ trước khi các mối đe dọa có thể xâm nhập vào mạng nội bộ của doanh nghiệp. Không giống như các giải pháp truyền thống, Umbrella SWG hoạt động trên tầng DNS, cho phép chặn các mối đe dọa ngay từ khi chúng được truy cập, trước khi các gói dữ liệu có cơ hội đi sâu vào mạng. Nó còn là một full proxy ghi lại và kiểm tra lưu lượng truy cập web của tổ chức để cung cấp khả năng hiển thị đầy đủ, kiểm soát URL và cấp ứng dụng cũng như khả năng bảo vệ trước mối đe dọa tiên tiến.

Umbrella SWG linh hoạt trong việc kiểm soát và định tuyến lưu lượng truy cập web, có thể giải mã và kiểm tra lưu lượng truy cập cho các đích đến web, bao gồm các ứng dụng mà người dùng và thiết bị trong tổ chức của bạn truy cập.

Ngoài ra, SWG còn:

- Làm proxy cho lưu lượng HTTP và HTTPS trên các cổng web tiêu chuẩn và không tiêu chuẩn.
- Nhận lưu lượng đã được lọc bởi Umbrella CDFW trên các cổng, giao thức và địa chỉ IP cụ thể.
- Kiểm soát quyền truy cập đến các loại tệp và quản lý các điều khiển thuê bao.

Cấu hình SWG với kiểm tra HTTPS trong một quy tắc chính sách Web. Trong chính sách Web, chúng ta có thể cấu hình SWG và quản lý cách tổ chức truy cập tệp và ứng dụng.

2.6 SIEM: Splunk

Splunk là một phần mềm giám sát mạng dựa trên sức mạnh của việc phân tích Log. Splunk thực hiện các công việc tìm kiếm, giám sát và phân tích các dữ liệu lớn được sinh ra từ các ứng dụng, các hệ thống và các thiết bị hạ tầng mạng. Nó có thể thao tác tốt với nhiều loại dịnh dạng dữ liệu khác nhau (Syslog, csv, apache-log, access_combined…). Splunk được xây dựng dựa trên nền tảng Lucene and MongoDB.

Các tính năng:

- **Định dạng Log:** Hỗ trợ hầu như tất cả các loại log của hệ thống, thiết bị hạ tầng mạng, phần mềm, Firewall, IDS/IPS, Log Event, Register của các máy trạm ….
- **Các hình thức thu thập dữ liệu:** Splunk có thể thực hiện việc thu thập log từ rất nhiều nguồn khác nhau. Từ một file hoặc thư mục (kể cả file nén) trên server, qua các kết nối UDP, TCP từ các Splunk Server khác trong mô hình Splunk phân tán, từ các Event Logs, Registry của Windows …Splunk kết hợp rất tốt với các công cụ thu thập log khác.
- **Cập nhật dữ liệu:** Splunk cập nhật dữ liệu liên tục khi có thay đổi trong thời gian thực. Giúp cho việc phát hiện và cảnh báo trong thời gian thực.
- **Đánh chỉ mục dữ liệu:** Splunk có thể đánh chỉ mục dữ liệu với một khối lượng dữ liệu rất lớn trong một khoảng thời gian ngắn. Giúp việc tìm kiếm diễn ra nhanh chóng và thuận tiện.
- **Tìm kiếm thông tin:** Splunk làm việc rất tốt với dữ liệu lớn và cập nhật liên tục. Nó cung cấp cơ chế tìm kiếm với một "Splunk Language" cực kỳ thông minh bao gồm các từ khóa, các hàm và cấu trúc tìm kiếm giúp người sử dụng có thể truy xuất mọi thứ, theo rất nhiều tiêu chí từ tập dữ liệu rất lớn. Những nhà quản trị mạng cao cấp và chuyên nghiệp thường gọi Splunk với cái tên "Splunk toàn năng" hay "Splunk as Google for Log files" để nói lên sức mạnh của Splunk.
- **Giám sát và cảnh báo:** Splunk cung cấp cho người dùng một cơ chế cảnh báo dựa trên việc tìm kiếm các thông tin do chính người sử dụng đặt ra. Khi có vấn đề liên quan tới hệ thống phù hợp với các tiêu chí mà người dùng đã đặt ra thì hệ thống sẽ cảnh báo ngay tới người dùng (cảnh bảo trực tiếp qua giao diện, giử Email).
- Khắc phục sự cố: Splunk còn cung câp một cơ chế tự động khắc phục với các vấn đề xảy ra bằng việc tự động chạy các file Script mà người dùng tự tạo (Ví dụ như: Chặn IP, đòng Port …) khi có các cảnh báo xảy ra.
- **Hiển thị thông tin:** Splunk cung cấp một cơ chế hiển thị rất trực quan giúp người sử dụng có thể dễ dàng hình dung về tình trạng của hệ thống, đưa ra các đánh giá về hệ thống. Splunk còn từ động kết xuất ra các báo cáo với nhiều loại định dạng một cách rất chuyên nghiệp.
- **Phát triển:** Cung cấp các API hỗ trợ việc tạo các ứng dụng trên Splunk của người dùng. Một số bộ API điển hình như Splunk SDK (cung cấp các SDK trên nền tảng Python,

Java, JS, PHP), Shep (Splunk Hadoop Intergration - đây là sự kết hợp giữa Splunk và Hadoop), Shuttl (là một sản phẩm hỗ trợ việc sao lưu dữ liệu trong Splunk), Splunkgit (Giúp bạn hình dung dữ liệu tốt hơn), Splunk power shell resource Kit (Bộ công cụ hỗ trợ việc mở rộng và quản lý hệ thống).

2.7 SOAR: Cortex XSOAR

Cortex XSOAR kết hợp điều phối bảo mật, quản lý sự cố và điều tra tương tác thành một trải nghiệm liền mạch. Công cụ điều phối được thiết kế để tự động hóa các tác vụ của sản phẩm bảo mật và kết hợp các tác vụ và quy trình công việc của nhà phân tích con người. Cortex XSOAR được cung cấp bởi DBot, tính năng này học hỏi từ các tương tác thực tế của nhà phân tích và các cuộc điều tra trong quá khứ để giúp các nhóm SOC đưa ra các đề xuất về nhiệm vụ của nhà phân tích, cải tiến cẩm nang và các bước điều tra tiếp theo tốt nhất. Với Cortex XSOAR, các nhóm bảo mật có thể xây dựng các hoạt động bảo mật phù hợp với tương lai để giảm MTTR, tạo quy trình quản lý sự cố nhất quán và đã được kiểm tra, đồng thời tăng năng suất của nhà phân tích.

Các đặc điểm:

Hợp nhất chức năng bảo mật
Sử dụng không gian làm việc cộng tác, tích hợp AI và tương quan chéo

Thống nhất việc tổng hợp, chấm điểm và chia sẻ thông tin tình báo về mối đe dọa bằng cơ chế tự động hóa dựa trên quy trình playbook-driven automation với khả năng quản lý thông tin tình báo về mối đe dọa tích hợp sẵn.

Thông tin tình báo về mối đe dọa có độ tin cậy cao được tích hợp sẵn có thể được tăng cường bằng cách kết hợp thêm thông tin tình báo về mối đe dọa từ bên thứ ba để **tốt hơn trong việc phát hiện và ưu tiên các mối đe dọa nghiêm trọng.**

Tự động hóa các hành động để chuẩn hóa và quy mô ứng phó sự cố
Thu thập thông tin tình báo từ nhiều sản phẩm trên một bảng điều khiển duy nhất

Cải thiện Chất lượng Điều tra bằng cách Làm việc Cùng nhau

Khuyến nghị lựa chọn chuyên viên tiếp nhận xử lý sự cố

Sử dụng năng lực "Học Máy", Cortex XSOAR sẽ so sánh chéo các thông tin này với khối lượng công việc hiện tại của các chuyên viên và đề xuất 3 chuyên viên phù hợp nhất để tiếp nhận xử lý sự cố.

Đề xuất chuyên gia hỗ trợ xử lý sự cố

Tính năng War Room trên XSOAR cho phép các chuyên viên hợp tác trong quá trình điều tra xử lý sự cố và các chuyên viên cũng có thể mời các đồng nghiệp khác tham gia ngay lập tức vào quá trình xử lý sự cố với cú pháp thân thiện như các chương trình chat phổ biến

Tự động đề xuất các câu lệnh thường được sử dụng

Khi các chuyên viên nhập "!" để bắt đầu lựa chọn các câu lệnh, Cortex XSOAR sẽ nghiên cứu lịch sử các lệnh thủ công đã được thực thi với các loại sự cố tương ứng trước đó và đưa ra đề xuất các lệnh nên được thực thi trước. Ngay cả khi các chuyên viên đã đang thử một số lệnh và chưa tìm ra các thông tin phù hợp, tính năng này cũng có thể hỗ trợ họ đi đúng hướng với các lệnh mà họ đã có thể bỏ qua hoặc quên.

Hiển thị trực quan các sự cố tương đồng

Với mỗi sự cố, Cortex XSOAR sẽ tự động phân tích và tìm các sự cố có đặc điểm tương đồng diễn ra trên hệ thống. Một biểu đồ trực quan, dễ dàng tương tác cho phép chuyên viên phân tích, tìm kiếm, điều chỉnh các mức độ tương đồng khác nhau hay theo mốc thời gian.

Đơn giản hóa quá trình xây dựng các kịch bản xử lý sự cố (Playbook)

Cortex XSOAR áp dụng công nghệ học máy để phân tích và tự động đề xuất các giá trị đầu vào (input) phù hợp cho các Task trong playbook. Tính năng này sẽ hỗ trợ rất nhiều cho các chuyên viên trong quá trình xây dựng playbook, tăng độ chính xác và rút ngắn thời gian đưa playbook vào hoạt động trong thực tế.

Trích xuất các sự cố trùng lặp

Cortex XSOAR sử dụng công nghệ máy học để phân tích các dữ liệu trong quá trình tiếp nhận và xử lý các sự cố, tìm kiếm các thông tin tương đương (như các email labels trong việc xác định các email phishing), thời gian xảy ra sự cố và các dấu hiệu phổ biến để xác định sự trùng lặp.

Tự động xử lý các tấn công phishing

Năng lực học máy của Cortex XSOAR có thể giải quyết các công đoạn đánh giá thủ công này với độ chính xác rất cao bằng cách sử dụng bộ phân loại tấn công phishing. Bộ phân loại phishing là một mô hình học máy chuyên sâu cho phép Cortex XSOAR phân tích và dựa đoán hành vi thông qua loại sự cố và các trường thông tin có trong các sự cố (như domain, IP, URL…). Mô hình học máy này có thể được sử dụng để tự động phát hiện các loại email phishing, địa chỉ URL hợp pháp hay chứa các nội dung spam, lừa đảo.

2.8 EDR: CrowdStrike Falcon® Insight XDR

CrowdStrike Falcon® Insight XDR là một nền tảng bảo mật tiên tiến, được thiết kế để phát hiện và phản ứng trước các mối đe dọa mạng một cách hiệu quả và toàn diện. Nó kết hợp các công nghệ tiên tiến như trí tuệ nhân tạo (AI), học máy (machine learning) và thông tin tình báo về mối đe dọa để bảo vệ doanh nghiệp khỏi các cuộc tấn công mạng ngày càng tinh vi.

Nâng cao hiệu quả bảo mật

- **Tận dụng khả năng cả EDR và XDR trên cùng một nền tảng, giúp quản lý và bảo vệ toàn bộ hệ thống một cách dễ dàng**
- **Sử dụng quy trình tự động hóa được hỗ trợ bởi AI với sự cộng tác trong thời gian thực:**
    - Cách mạng hóa tốc độ và hiệu quả của các cuộc điều tra với sự trợ giúp của CrowdStrike® Charlotte AI™.
    - Tập trung vào các sự cố thay vì cảnh báo và tận dụng AI để đẩy nhanh quá trình phân loại và điều tra.*

    - Tăng tốc thời gian phản ứng với Bảng làm việc sự cố cực nhanh được thiết kế xung quanh các sự cố, không phải các cảnh báo độc lập.
    - Các nhà phân tích có thể tối ưu hóa quy trình làm việc làm việc cùng nhau, chia sẻ thông tin và phối hợp để xử lý các sự cố một cách nhanh chóng., bổ sung ngữ cảnh cross-doamin, chú thích, theo dõi lịch sử sự cố và hơn thế nữa.
- **Thu thập, tổng hợp và chuẩn hóa dễ dàng:**

CrowdStrike giúp thu thập dữ liệu từ nhiều nguồn khác nhau, sau đó tổng hợp và chuẩn hóa dữ liệu đó để tạo ra một cái nhìn tổng quan về tình hình bảo mật của hệ thống. Nhờ đó, chúng ta có thể dễ dàng phát hiện và xử lý các mối đe dọa.

Tối ưu hóa hoạt động bảo mật

Phát hiện các cuộc tấn công bị bỏ lỡ bởi các phương pháp tiếp cận độc lập:

- **Phát hiện các cuộc tấn công tàng hình xuyên miền:** Phát hiện các cuộc tấn công tinh vi lan rộng qua nhiều hệ thống (ví dụ: từ máy tính đến mạng, từ mạng đến đám mây) bằng cách kết hợp thông tin tình báo về mối đe dọa hàng đầu và trí tuệ nhân tạo tiên tiến.
- **Hỗ trợ từ các chuyên gia:** Nhận được phản hồi từ các chuyên gia săn tìm mối đe dọa của CrowdStrike, các chuyên gia phát hiện và phản ứng quản lý (MDR) và các chuyên gia phản ứng sự cố (IR).
- **Khả năng phát hiện linh hoạt:** Khả năng phát hiện sẵn có và tùy chỉnh cung cấp cho bạn sức mạnh và sự linh hoạt cần thiết để vượt qua đối thủ.

Tối ưu hóa quá trình phân loại và điều tra:

- **Cảnh báo được ưu tiên:** Các cảnh báo quan trọng được ưu tiên xử lý, giúp nhân viên an ninh tập trung vào những mối đe dọa thực sự nghiêm trọng.
- **Thông tin chi tiết và ngữ cảnh phong phú:** Thông tin chi tiết về các mối đe dọa được trình bày rõ ràng, giúp nhân viên an ninh nhanh chóng hiểu và phản ứng.
- **Giao diện trực quan:** Giao diện Falcon dễ sử dụng giúp bạn dễ dàng tìm kiếm, lọc và phân tích dữ liệu.

- **Hiểu rõ mối đe dọa:** Khả năng phân tích sâu và hồ sơ chi tiết về kẻ tấn công giúp bạn hiểu rõ hơn về mối đe dọa và kẻ tấn công.

Triển khai toàn bộ doanh nghiệp nhanh chóng:

- **Triển khai dễ dàng:** Agent của Falcon nhẹ và dễ triển khai trên toàn bộ hệ thống của bạn chỉ trong vài phút.
- **Bảo vệ toàn diện từ ngày đầu tiên:** Với khả năng phát hiện và hiển thị toàn diện ngay từ ngày đầu tiên, giao diện Falcon Insight XDR cung cấp trải nghiệm người dùng vượt trội với quy trình làm việc liền mạch giữa bảo vệ điểm cuối (EPP), EDR, XDR và thông tin tình báo về mối đe dọa.

Lợi ích từ các chuyên gia sẵn sàng hỗ trợ:

- **Tận dụng sự kết hợp của công nghệ và chuyên môn:** Tìm được sự cân bằng phù hợp giữa công nghệ và chuyên môn với dịch vụ săn tìm mối đe dọa chủ động 24/7 hàng đầu thế giới và dịch vụ MDR hàng đầu thế giới với khả năng khắc phục toàn diện thông qua nâng cấp tùy chọn liền mạch.
- **Hỗ trợ từ các chuyên gia hàng đầu:** Người dùng Falcon Insight XDR được hưởng lợi từ vòng phản hồi chặt chẽ giữa các sản phẩm của CrowdStrike và các chuyên gia hàng đầu trong ngành, cho dù bạn tự quản lý nền tảng Falcon hay nâng cấp lên Falcon Complete Next-Gen MDR để trải nghiệm được quản lý đầy đủ.

3. Global Load Balancer

3.1 Load balancer: F5 BIG-IP Local Traffic Manager

F5 BIG-IP Local Traffic Manager (LTM) là một phần của dòng sản phẩm BIG-IP. BIG-IP LMT tối ưu hóa tốc độ và độ tin cậy của các ứng dụng thông qua cả lớp mạng và lớp ứng dụng, lần lượt là lớp 3 và 7. Nó cải thiện khả năng đáp ứng của ứng dụng và cơ sở hạ tầng bằng cách sử dụng giao thức thời gian thực và các quyết định quản lý lưu lượng dựa trên điều kiện ứng dụng và máy chủ, kết nối rộng rãi quản lý, TCP và giảm tải nội dung.

Kiến trúc proxy đầy đủ của LTM cung cấp cho người dùng nhận thức về giao thức để kiểm soát lưu lượng cho các ứng dụng quan trọng nhất. Nó cũng theo dõi mức hiệu suất động của các máy

chủ, đảm bảo rằng các ứng dụng không chỉ luôn hoạt động mà còn dễ mở rộng và quản lý hơn. BIG-IP LTM mang lại hiệu suất và khả năng hiển thị SSL cho lưu lượng đến và đi, để bảo vệ trải nghiệm người dùng bằng cách mã hóa mọi thứ từ máy khách đến máy chủ.

Được coi là chuẩn mực cho thiết bị cân bằng tải load balancer, nhiều bộ phận CNTT lớn nhất thế giới sử dụng F5. Dòng sản phẩm BIG-IP có giải pháp thiết bị cân bằng tải load balancer cho hầu hết mọi ngân sách và ứng dụng, có thể giúp so sánh chi phí giữa các bộ thiết bị cân bằng tải load balancer trên dòng sản phẩm của nó cũng như so với các nhà cung cấp thiết bị cân bằng tải load balancer khác

Đặc điểm:

+ Quàn lý lưu lượng: Duy trì tính khả dụng của ứng dụng bằng cách Điều chỉnh lưu lượng truy cập đến ứng dụng (tại các lớp 4 và 7) một cách tức thời để đảm bảo ứng dụng luôn hoạt động tốt.

+ Tự động hóa khai báo:

- **Tối ưu hóa tự động hóa dịch vụ:** Sử dụng các API khai báo (API mô tả cấu hình mong muốn) để đơn giản hóa quá trình tự động hóa các dịch vụ.

+ Khả năng mở rộng nhanh chóng và đáng tin cậy:

- **Tối ưu hóa phản ứng với nhu cầu lưu lượng:** Điều chỉnh nhanh chóng để đáp ứng sự thay đổi đột ngột trong lượng người dùng truy cập, đảm bảo ứng dụng luôn hoạt động ổn định.

+ Quản lý phiên bản cho các mục cấu hình:

- **Lưu trữ và sắp xếp các công cụ như iRules và mẫu ứng dụng:** Cho phép triển khai nhanh chóng và lặp lại các cấu hình.

+ Cập nhật bảo mật nhanh chóng:

- **Theo kịp cảnh báo an ninh luôn thay đổi:** Cập nhật liên tục để đối phó với các mối đe dọa an ninh mạng mới.

Phân tích dữ liệu thời gian thực:

- **Nâng cao quản lý lưu lượng:** Cung cấp thông tin chi tiết và phân tích dữ liệu lưu lượng truy cập để cải thiện hiệu suất quản lý.

Giải thích đơn giản:

- **Quản lý lưu lượng:** Giống như điều khiển giao thông, đảm bảo lưu lượng truy cập đến ứng dụng của bạn luôn ổn định và không bị tắc nghẽn.
- **Tự động hóa:** Tạo các quy tắc tự động để đơn giản hóa việc quản lý và điều chỉnh hệ thống.
- **Mở rộng linh hoạt:** Có thể nhanh chóng tăng hoặc giảm công suất của hệ thống để đáp ứng nhu cầu thay đổi của người dùng.
- **Quản lý phiên bản:** Giữ lại các bản sao lưu của cấu hình để dễ dàng khôi phục hoặc thay đổi.
- **Cập nhật bảo mật:** Luôn đảm bảo hệ thống của bạn được bảo vệ khỏi các mối đe dọa mới nhất.
- **Phân tích dữ liệu:** Theo dõi và phân tích cách người dùng sử dụng ứng dụng để cải thiện hiệu suất và trải nghiệm người dùng.

4. Network Operator Center

4.1 Data visualization: Grafana

Grafana là công cụ được sử dụng với nhiệm vụ chính là trực quan hóa và phần tích dữ liệu thời gian thực – tức là nó không phải đi thu thập metric từ hệ thống cần giám sát mà chỉ công cụ để hiển thị và phân tích dữ liệu.

Tính năng:

Visualize (trực quan hóa) : Vẽ biểu đồ từ metric được cung cấp. Grafana có rất nhiều tùy chọn visualize giúp người dùng vẽ biểu đồ một cách nhanh chóng và linh hoạt. Các panel plugin với nhiều cách khác nhau để trực quan hóa các metric và log hệ thống.

Alerting - Cảnh báo : Giúp người dùng xác định các ngưỡng metric, hiển thị ngưỡng metric cảnh báo và định nghĩa các quy tắc cảnh báo. Grafana liên tục đánh giá metric và gửi cảnh báo khi metric vượt quá ngưỡng cho phép. Cảnh báo có thể được gửi qua Slack, Mail, PagerDuty, Telegram, ...

Unify – Hợp nhất : Kết hợp dữ liệu để có cái nhìn toàn cảnh tốt hơn. Grafana hỗ trợ hàng chục loại database một cách tự nhiên, kết hợp chúng với nhau trong cùng một giao diện dashboard.

Open - Mở: Grafana đưa bạn nhiều tùy chọn. Nó hoàn toàn là nguồn mở, được hỗ trợ bởi cộng đồng sôi động. Có thể dễ dàng cài đặt Grafana hoặc sử dụng Hosted Grafana trên bất kì nền tảng nào.

Extend: Khám phá hàng trăm daaashboard và plugin trong thư viện chính thức. Nhờ đam mê và động lực của cộng đồng, một dashboard hoặc plugin mới được thêm vào mỗi tuần.

- ***Collaborate - Cộng tác***: mang mọi người lại với nhau, chia sẻ dữ liệu và các dashboard với các nhóm. Grafana trao quyền cho người dùng và giúp nuôi dưỡng một nền văn hóa hướng dữ liệu.

- ***Dynamic Dashboards***: Tạo và sử dụng lại các dashboards với các biến template xuất hiện ở phần đầu của dashboard

- ***Annotations - Chú thích*** : Biểu đồ chú thích có sự kiện phong phú từ các nguồn dữ liệu khác nhau. Di chuột qua các sự kiện cho bạn thấy siêu dữ liệu sự kiện đầy đủ và các thẻ tag.

4.2 Log Management: Grafana Loki

Grafana Loki là một hệ thống thu thập và lưu trữ logs phân tán mã nguồn mở, được phát triển bởi Grafana Labs để tích hợp chặt chẽ với Grafana. Loki lưu trữ logs bằng cách sử dụng nhãn (labels), giống như cách Prometheus xử lý metrics.

Đặc điểm:

+ Loki được xây dựng với mục tiêu tối giản và hiệu quả về tài nguyên. Thay vì lập chỉ mục từng dòng log, Loki chỉ sử dụng nhãn (labels) để tổ chức và truy xuất dữ liệu. Cách tiếp cận này không chỉ giúp giảm đáng kể chi phí lưu trữ mà còn tối ưu hóa việc sử dụng tài nguyên hệ thống, khiến Loki phù hợp với các môi trường có khối lượng nhật ký lớn.

+ Hỗ trợ tìm kiếm logs dựa trên các nhãn (labels) mà bạn định nghĩa trước. Ví dụ, bạn có thể truy vấn logs từ một ứng dụng hoặc một máy chủ cụ thể. Loki vẫn có khả năm tìm kiếm trên nội dung logs, nhưng nó sẽ chậm hơn nhiều so với Elasticsearch vì Loki không lập chỉ mục cho từng từ hoặc từng trường trong logs.

+ Sử dụng ít tài nguyên hơn do không lập chỉ mục chi tiết cho từng dòng log.

+ Hỗ trợ kiến trúc phân tán, nhưng cách thức hoạt động nhẹ hơn. Logs được chia thành các chunk và có thể được lưu trữ trên các hệ thống lưu trữ như S3, Loki dễ mở rộng và tiêu tốn ít tài nguyên hơn.

4.3 Jire Service Management: Incident Management

Jira Service Management là một phần mềm giúp các doanh nghiệp quản lý dịch vụ IT một cách hiệu quả. Nó cung cấp một nền tảng tập trung để khách hàng có thể báo cáo các vấn đề, yêu cầu hỗ trợ, và các đội ngũ IT có thể theo dõi, giải quyết và quản lý các yêu cầu đó.

Các tính năng:

+ Quản lý yêu cầu – Request Management

Xử lý yêu cầu của khách hàng không phải là việc nhỏ. Với Request Management của JSM, mọi truy vấn và nhu cầu đều được lập danh mục và giải quyết một cách tỉ mỉ, đảm bảo tính nhất quán và hiệu quả.

+ Quản lý sự cố – Incident Management

Các sự cố không lường trước được trong lĩnh vực CNTT có thể làm gián đoạn workflow. Incident Management của JSM đảm bảo rằng các vấn đề như vậy được xác định, giải quyết và giải quyết nhanh chóng, duy trì tính liên tục của dịch vụ.

+ Quản lý thay đổi – Change Management

Việc thực hiện các thay đổi trong môi trường CNTT đòi hỏi sự chính xác. Change Management của JSM hướng dẫn đánh giá, phê duyệt và cung cấp thông tin một cách suôn sẻ về các thay đổi đối với quy trình hoặc hệ thống của bạn.

+ Quản lý tài sản – Asset Management

Việc theo dõi cả tài sản hữu hình hay vô hình đều là điều tối quan trọng. Configuration Management của JSM cung cấp một hệ thống theo dõi toàn diện, đảm bảo sử dụng và bảo trì tối ưu.

+ Quản lý cấu hình – Configuration Management

Việc hài hòa các thành phần CNTT để hoạt động đồng bộ là điều cần thiết. Knowledge Management trong JSM cung cấp một cách tiếp cận có phương pháp để tổ chức và tích hợp các thành phần CNTT đa dạng.

+ Quản lý tri thức – Knowledge Management

Không thể đánh giá thấp sức mạnh của thông tin. Problem Management của JSM tập trung những kiến thức sâu sắc của nhóm, sắp xếp chúng một cách gọn gàng và dễ truy cập, thúc đẩy việc học tập liên tục.

+ Quản lý vấn đề – Problem Management:

Giải quyết các thách thức CNTT đòi hỏi một cách tiếp cận có hệ thống. Problem Management của JSM đi sâu vào việc xác định, phân tích và giải quyết hiệu quả các vấn đề cơ bản.

Mỗi tính năng của JSM đều được thiết kế tỉ mỉ, đảm bảo các nhóm được trang bị những công cụ tốt nhất để hợp lý hóa hoạt động của họ và đạt được sự xuất sắc.

4.4 Mornitoring: Prometheus

Prometheus là một hệ thống giám sát nguồn mở với mô hình dữ liệu đa chiều, ngôn ngữ truy vấn linh hoạt, cơ sở dữ liệu chuỗi thời gian hiệu quả và phương pháp cảnh báo hiện đại.

Các đăc điểm:

- Dữ liệu đa chiều

  Prometheus triển khai mô hình dữ liệu đa chiều. Chuỗi thời gian được xác định bằng tên số liệu và một tập hợp các cặp khóa-giá trị.

- Truy vấn mạnh mẽ

  PromQL cho phép cắt và phân tích dữ liệu chuỗi thời gian đã thu thập để tạo biểu đồ, bảng và cảnh báo tùy ý.

- Hình ảnh hóa tuyệt vời

  Prometheus có nhiều chế độ để hình ảnh hóa dữ liệu: trình duyệt biểu thức tích hợp, tích hợp Grafana và ngôn ngữ mẫu bảng điều khiển.

- Lưu trữ hiệu quả

  Prometheus lưu trữ chuỗi thời gian trong bộ nhớ và trên đĩa cục bộ theo định dạng tùy chỉnh hiệu quả. Khả năng mở rộng được thực hiện bằng cách phân mảnh và liên kết chức năng.

· Hoạt động đơn giản

Mỗi máy chủ đều độc lập về độ tin cậy, chỉ dựa vào bộ nhớ cục bộ. Được viết bằng Go, tất cả các tệp nhị phân đều được liên kết tĩnh và dễ triển khai.

· Cảnh báo chính xác

Cảnh báo được xác định dựa trên PromQL linh hoạt của Prometheus và duy trì thông tin đa chiều. Một trình quản lý cảnh báo xử lý thông báo và tắt tiếng.

· Nhiều thư viện máy khách

Thư viện máy khách cho phép dễ dàng đo lường các dịch vụ. Hơn mười ngôn ngữ đã được hỗ trợ và các thư viện tùy chỉnh dễ triển khai.

· Nhiều tích hợp

Các trình xuất hiện có cho phép kết nối dữ liệu của bên thứ ba vào Prometheus. Ví dụ: số liệu thống kê hệ thống, cũng như số liệu Docker, HAProxy, StatsD và JMX.

□ **Bảng Risk Score của hệ thống mới.**

4. Xây dựng chính sách để phối hợp với các công nghệ được sử dụng trong hệ thống để giảm thiểu tối đa khả năng mất mất dữ liệu trong hệ thống

4.1. Quản lí nhân viên

- Tất cả nhân viên phải được đào tạo kiến thức về an toàn thông tin trước khi bắt đầu làm việc tại công ty.
- Nhân viên bộ phận IT phải có kiến thức về bảo mật thông tin, kỹ thuật an ninh mạng, có thể triển khai và duy trì các biện pháp bảo mật thông tin.
- Thiết lập các chính sách bảo mật trong công ty tránh thất thoát dữ liệu:
    + Chính sách về bảo mật thông tin: Nhân viên không được phép tiết lộ thông tin, dữ liệu của công ty. Kể cả nhân viên đã nghỉ việc.
    + Chính sách về việc sử dụng Email, Internet: Nhân viên phải hạn chế sử dụng email, internet cho mục đích cá nhân; Giới hạn tải các file từ nguồn không an toàn; Thường xuyên thực hiện cảnh báo nhân viên về mối đe dọa qua email (phishing) và cách nhận diện chúng.
    + Chính sách về mật khẩu: Thiết lập chính sách mật khẩu một cách rõ ràng và nhân viên phải tuân thủ; Nhắc nhở nhân viên thay đổi mật khẩu định kì để tránh nguy cơ bị tấn công do sử dụng mật khẩu cũ quá lâu.
    + Chính sách xác thực đa yếu tố: Yêu cầu nhân viên phải thực hiện xác thực đa yếu tố cho các tài khoản sử dụng trong hệ thống để tăng cường bảo mật khi đăng nhập.

4.2. Quản lí tài sản vật lí

- Các thiết bị quan trọng cần được giám sát an ninh nghiêm ngặt, chỉ những người có quyền hạn thì mới được tiếp cận và sử dụng
- Các thiết bị trong hệ thống cần được bảo trì, sửa chữa định kì
- Thiết bị nên đặt trong khu vực được trang bị phòng chống cháy nổ.
- Thực hiện cài đặt mật khẩu cho ổ cứng của máy tính cá nhân được cấp cho nhân viên, phòng trường hợp bị đánh cắp vẫn có thể khóa ổ cứng từ xa tránh gây thất thoát dữ liệu công ty.
- Yêu cầu các thiết bị di động phải được cài đặt phần mềm bảo mật để có thể truy cập vào dữ liệu công ty.

4.3. Quản lí truy cập Internet

- Kiểm soát việc sử dụng ứng dụng trong mạng để ngăn chặn việc truy cập, truyền tải các dữ liệu độc hại
- Ngăn chặn hoặc hạn chế truy cập vào các trang web có thể tạo ra rủi ro bảo mật.
- Nhân viên IT phải luôn giám sát lưu lượng mạng trong hệ thống để kịp thời xử lí các hoạt động bất thường.
- Thực hiện kiểm thử các file, ứng dụng được cài đặt từ Internet vào máy tính công ty.

4.4. Vận hành hệ thống

- Thiết lập chính sách sao lưu hồi phục dữ liệu mỗi ngày, thực hiện kiểm tra database định kì để đảm bảo tính khả dụng và độ tin cậy của quy trình sao lưu hồi phục.

- Xác định quy trình xóa dữ liệu và các điều kiện cần thiết nếu muốn xóa dữ liệu
- Áp dụng chính sách nguyên tắc least privilege, chỉ cung cấp những quyền truy cập cần thiết để đảm bảo công việc không bị trì hoãn.
- Mã hóa các dữ liệu quan trọng và dữ liệu được chuyển qua mạng hoặc lưu trữ trên thiết bị di động.
- Cho phép ghi nhật kí chi tiết các hoạt động mạng để firewall theo dõi và phân tích lưu lượng mạng. Thường xuyên kiểm tra nhật kí để có thể tìm điểm bất thường, hoạt động đáng ngờ có thể gây thất thoát dữ liệu.
- Triển khai các chính sách bảo mật cho Firewall, IDS/IPS để có thể tự động ngăn chặn các cuộc tấn công.