

Nhóm 13

NT207.P11.ANTT

BÁO CÁO CUỐI KỲ

GVHD: ThS. Nguyễn Duy

Thành viên nhóm 13


21521581	Nguyễn Phương Trinh
21520155	Nguyễn Triệu Thiên Bảo
21521195	Trần Lê Minh Ngọc
21522240	Huỳnh Minh Khuê
20520823	Mai Ngọc Phương Trinh



Nội dung báo cáo

01 Tổng quan đề tài

02 Hiện trạng hệ thống mạng của doanh nghiệp





03 Phân tích những điểm yếu, rủi ro mất mát dữ liệu của mô hình mạng hiện tại
Risk score của mô hình hiện tại

$P = P_1 \cdot P_2$

04 Security Assessments trên các tiêu chuẩn bảo mật nổi bật

05 Đề xuất mô hình mạng mới + chính sách vận hành mới
Risk score của mô hình mới

$P = P_1 \cdot P_2$

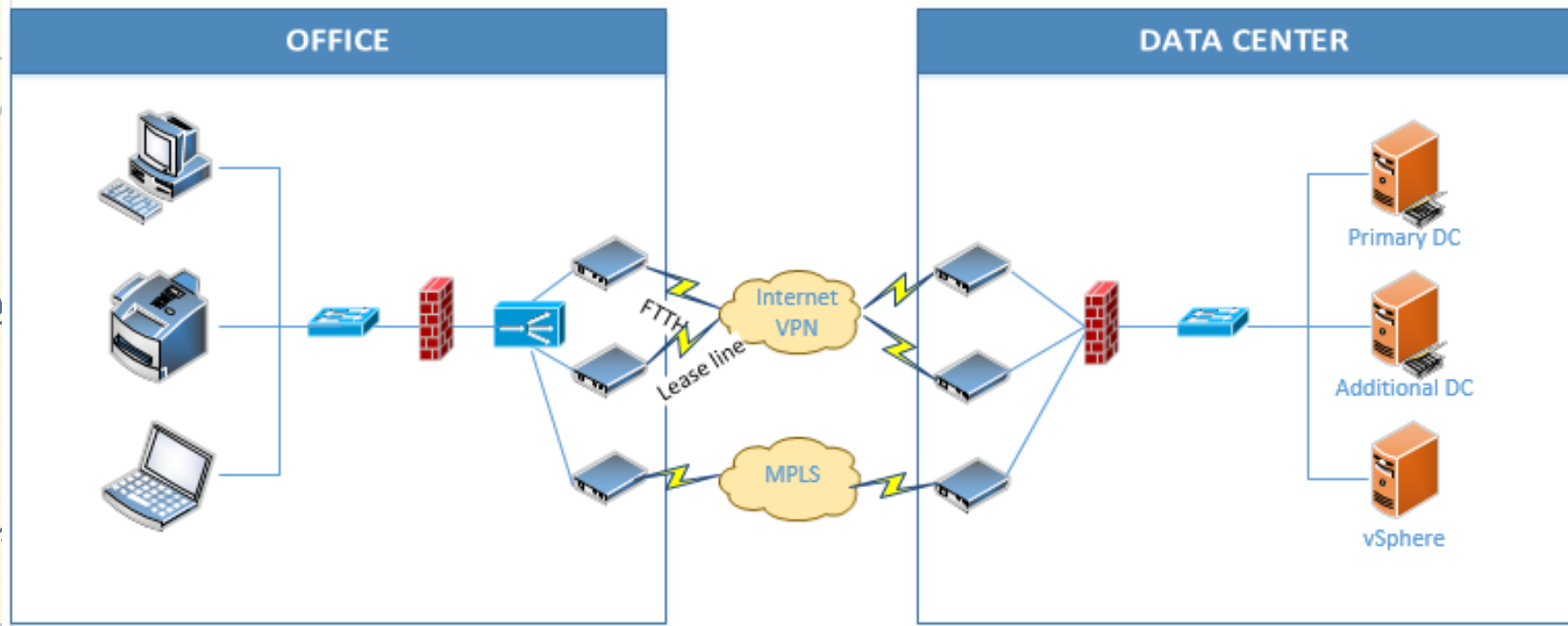


$P = P_1 \cdot P_2$

01. Tổng quan đề tài

- Bối cảnh: Trước sự gia tăng phức tạp của các mối đe dọa an ninh mạng và nguy cơ mất mát dữ liệu, việc xây dựng hệ thống bảo mật toàn diện trở nên cấp thiết hơn bao giờ hết. Chúng ta cần tập luyện thực hiện các đánh giá thực trạng hệ thống mạng doanh nghiệp và các rủi ro tiềm tàng về ATTT
- Mục tiêu:
 - + Đánh giá hệ thống hiện tại để xác định các điểm yếu và rủi ro về an toàn thông tin (ATTT)
 - + Đưa ra các phương pháp bảo vệ dữ liệu hiệu quả, hướng đến triển khai giải pháp ngăn ngừa mất mát dữ liệu (Data Loss Prevention – DLP) toàn diện

02. Hiện trạng hệ thống mạng



02. Hiện trạng hệ thống mạng

Mô hình ban đầu là một kiến trúc mạng đơn giản, bao gồm office kết nối với Data center thông qua mạng internet. Đặc điểm của mô hình trên:

- Kết nối: FTTH (truyền tải dữ liệu nhanh chóng), lease line (đảm bảo tính ổn định, độ tin cậy cao, tốc độ truyền tải lớn), MPLS (phù hợp kết nối nhiều địa điểm), internet VPN (tận dụng internet công cộng và được bảo mật).
- Bảo mật: Firewall và VPN.
- Quản lý và hiệu suất: Vsphere và Load balancer.
- Ứng dụng: Phù hợp với yêu cầu doanh nghiệp có nhiều văn phòng; các kết nối từ xa được đảm bảo an toàn nhưng cũng ổn định về hiệu suất.

02. Hiện trạng hệ thống mạng

- Quản trị theo mô hình Domain
- Không có phần mềm Antivirus, Firewall chuyên dụng
- Không có các chính sách an toàn thông tin trong hệ thống
- Chính sách vận hành chưa được tổng hợp, chuẩn hóa
- Không có chính sách sao lưu và phục hồi dữ liệu
- Thiết bị cân bằng tải kết nối internet, router không được bảo mật tối ưu
- Toàn bộ máy chủ đặt tại Data Center
- Không có giám sát và phát hiện xâm nhập

03. Điểm yếu của mô hình hiện tại

Threat Agent	Threat Action	Vulnerability
Employee	Lộ cấu hình server	File cấu hình công khai hoặc dễ dàng truy cập, chỉnh sửa
Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	Không có phần mềm chống mã độc trên thiết bị đầu cuối, FW, AV
Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	Không có biện pháp backup và khôi phục dữ liệu kịp thời
Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	Không áp dụng chính sách mật khẩu mạnh
Employee	Sử dụng phần mềm không rõ nguồn gốc	Cho phép cài đặt phần mềm từ nguồn không đáng tin cậy

03. Điểm yếu trong mô hình hiện tại

Threat Agent	Threat Action	Vulnerability
Employee	Dữ liệu không được mã hóa	Làm lộ dữ liệu trong quá trình truyền tin
Employee	Sử dụng quyền hạn vượt mức để truy cập tài nguyên	Làm lộ dữ liệu, xóa hoặc chỉnh sửa tài nguyên
Attacker	Tấn công vào cơ sở dữ liệu	Lợi dụng lỗ hổng SQL, không có cơ chế SQL
Attacker	Tấn công DDoS	Không có biện pháp phòng chống DDoS (solution chống DDoS, FW chống DDoS, cân bằng tải, ...)
Other	Thiên tai, sự cố bất ngờ tại vùng lưu trữ	Dữ liệu bị mất, không thể khôi phục

03. Risk Score (mô hình hiện tại)

Threat			Vulnerability
Agent	Action		
Employee	Lộ thông tin cấu hình server		Cấu hình server công khai hoặc dễ dàng truy cập, chỉnh sửa
Employee	Sử dụng mật khẩu yếu hoặc trùng lặp		Không áp dụng chính sách mật khẩu mạnh
Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân		Lưu trữ dữ liệu nhạy cảm mà không mã hóa
Employee	Sử dụng phần mềm không rõ nguồn gốc		Cho phép cài đặt phần mềm từ nguồn không đáng tin cậy
Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống		Không có phần mềm chống mã độc trên thiết bị đầu cuối, AVE, FW + AV
Employee	Bị khai thác thông tin thông qua phương thức Social Engineering		Không có chính sách training cho nhân viên về các hình thức lừa đảo qua mạng
Employee	Không khóa máy tính khi rời khỏi vị trí làm việc		Không có khóa màn hình tự động
Employee	Làm lộ bản ghi nhật ký (log)		Không bảo vệ nhật ký hệ thống
Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy file ra ngoài thiết bị cá nhân và ngược lại, ...)		Không giới hạn số lượng thiết bị ngoại vi được sử dụng, không có chính sách bảo mật
Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)		Không có chính sách phân quyền hợp lý
Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố		Không có biện pháp backup và khôi phục dữ liệu kịp thời
Attacker	Tấn công thông qua email giả mạo (Spear Phishing)		Không đào tạo kiến thức bảo mật nghiêm ngặt, không kiểm tra email kỹ lưỡng
Attacker	Khai thác lỗ hổng phần mềm chưa vá		Không cập nhật hoặc vá lỗi phần mềm thường xuyên
Attacker	Sniffing		Không mã hóa thông tin nhạy cảm qua mạng
Attacker	Tấn công DDoS		Không có biện pháp phòng chống DDoS (solution chống DDoS, FW chống DDoS, cân bằng tải, ...)
Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp		Không có phần mềm chống mã độc trên thiết bị đầu cuối, AVE, FW + AV
Attacker	Phá hủy thiết bị		Không có biện pháp bảo vệ phần cứng và giám sát truy cập vật lý
Attacker	Khai thác thông tin thông qua Social Engineering		Thiếu đào tạo bảo mật cho nhân viên về nhận diện và đối phó với các hình thức lừa đảo như phishing (giả mạo email, cuộc gọi, hoặc tin nhắn)
Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)		Thiếu cơ chế xác thực danh tính đa yếu tố (MFA) cho các yêu cầu từ bên ngoài hoặc các truy cập từ xa
Attacker	Tấn công Brute Force để phá mật khẩu		Thiếu biện pháp mã hóa và kiểm tra các đầu vào (input validation and sanitization) trên các trường đầu vào trong trang web, như hộp tìm kiếm, bình luận, ...
Attacker	Tấn công Cơ sở dữ liệu		Không sử dụng Content Security Policy (CSP) để giới hạn nguồn tài nguyên hoặc ngăn chặn thực thi mã không mong muốn, không dùng X-XSS-Protection, X-Content-Type-Options, ...
			Không có chính sách khóa tài khoản sau nhiều lần đăng nhập thất bại hoặc không giới hạn số lần thử mật khẩu, chính sách mật khẩu thiếu sót, ...
			Bị lỗi SQL Injection, không có cơ chế kiểm tra input (này thầy bảo ok nè)

$$C_y = C_1^{\alpha} (\alpha - \alpha)$$

03. Risk Score (mô hình hiện tại)

Threat		Impact
Agent	Action	
Employee	Lộ thông tin cấu hình server	Thông tin cấu hình server bị lộ có thể cung cấp cho kẻ tấn công các điểm yếu để khai thác
Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	Mật khẩu yếu dễ bị phá vỡ, và sử dụng mật khẩu trùng lặp có thể dẫn đến lộ tài khoản truy cập hệ thống
Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân	Dữ liệu nhạy cảm được lưu trữ trên thiết bị cá nhân có thể bị xâm nhập
Employee	Sử dụng phần mềm không rõ nguồn gốc	Phần mềm không rõ nguồn gốc có thể chứa mã độc hoặc mở ra lỗ hổng bảo mật cho hệ thống
Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	Malware có thể thay đổi tính toàn vẹn của hệ thống và lộ dữ liệu nhạy cảm
Employee	Bị khai thác thông tin thông qua phương thức Social Engineering	Nhân viên bị lừa cung cấp quyền truy cập hoặc thông tin nhạy cảm
Employee	Không khóa máy tính khi rời khỏi vị trí làm việc	Ai đó có thể truy cập trái phép vào hệ thống từ máy tính của nhân viên nếu không được khóa
Employee	Làm lộ bản ghi nhật ký (log)	Nhật ký hệ thống (log) không được bảo vệ có thể bị kẻ tấn công chỉnh sửa hoặc xóa bỏ
Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy file ra ngoài thiết bị cá nhân)	USB chứa mã độc hoặc thiết bị cá nhân không được bảo vệ đầy đủ có thể làm lây lan mã độc vào hệ thống nội bộ của công ty
Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)	Nếu nhân viên có quyền truy cập nhiều hơn mức cần thiết, họ có thể vô tình hoặc cố ý gây thiệt hại cho hệ thống
Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	Lỗi phần cứng hoặc phần mềm có thể gây mất mát dữ liệu vĩnh viễn, làm gián đoạn hoạt động và tăng nguy cơ thất thoát tài sản số.
Attacker	Tấn công thông qua email giả mạo (Spear Phishing)	Email giả mạo có thể lừa người nhận cung cấp thông tin đăng nhập hoặc tải xuống mã độc
Attacker	Khai thác lỗ hổng phần mềm chưa vá	Khai thác lỗ hổng trong phần mềm chưa được cập nhật hoặc vá lỗi để chiếm quyền điều khiển hệ thống
Attacker	Sniffing	Kẻ tấn công chặn bắt thông tin không được mã hóa qua mạng
Attacker	Tấn công DDoS	Tấn công từ chối dịch vụ phân tán (DDoS) làm gián đoạn hệ thống
Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp	Malware có thể làm hỏng dữ liệu hoặc lộ thông tin nhạy cảm
Attacker	Phá hủy thiết bị	Kẻ tấn công phá hủy thiết bị phần cứng hoặc gây lỗi logic
Attacker	Khai thác thông tin thông qua Social Engineering	Kẻ tấn công lừa nhân viên cung cấp thông tin hoặc quyền truy cập
Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)	Kẻ tấn công có thể chèn mã độc vào ứng dụng web, gây lộ dữ liệu hoặc chiếm quyền điều khiển phiên người dùng
Attacker	Tấn công Brute Force để phá mật khẩu	Kẻ tấn công thử hàng loạt mật khẩu để truy cập vào hệ thống
Attacker	Tấn công Cơ sở dữ liệu	Kẻ tấn công khai thác lỗ hổng SQL để truy cập vào hệ thống

$$C_y = C_y^{\alpha}(\alpha - \alpha)$$

03. Risk Score (mô hình hiện tại)

1	Threat		Risk mitigate
2	Agent	Action	
3	Employee	Lộ thông tin cấu hình server	Thiết lập quyền truy cập nghiêm ngặt và mã hóa các file cấu hình quan trọng.
4	Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	Thực thi chính sách mật khẩu mạnh và kích hoạt xác thực hai yếu tố (2FA), passwordless, ...
5	Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân	Mã hóa dữ liệu và cung cấp các phương thức an toàn để truyền tải thông tin nhạy cảm.
6	Employee	Sử dụng phần mềm không rõ nguồn gốc	Thực thi chính sách cài đặt phần mềm và chỉ cho phép sử dụng phần mềm đã được kiểm tra an toàn.
7	Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	Áp dụng chính sách sử dụng phần mềm nghiêm ngặt, cài đặt các công cụ bảo vệ điểm cuối (AVE, FW + AV filter, ...)
8	Employee	Bị khai thác thông tin thông qua phương thức Social Engineering	Đào tạo về nhận thức bảo mật và quản lý quyền truy cập của người dùng.
9	Employee	Không khóa máy tính khi rời khỏi vị trí làm việc	Cài đặt tự động khóa màn hình sau một thời gian không hoạt động và có chính sách, quy trình đào tạo nhân viên.
10	Employee	Làm lộ bản ghi nhật ký (log)	Bảo mật nhật ký bằng cách mã hóa và lưu trữ chúng trong một hệ thống riêng biệt, chỉ cấp quyền truy cập hạn chế cho nhân viên có nhiệm vụ giám sát.
11	Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy)	Thiết lập chính sách rõ ràng về sử dụng thiết bị di động, chỉ cho phép các thiết bị đã được mã hóa và cài đặt phần mềm bảo mật, quét virus tự động khi cắm vào hệ thống.
12	Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)	Áp dụng nguyên tắc "quyền truy cập tối thiểu" cho mỗi nhân viên và kiểm tra định kỳ để điều chỉnh quyền truy cập nếu cần.
13	Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	Thiết lập các giải pháp khôi phục dự phòng bằng cách lưu dữ liệu trên các đám mây hoặc hệ thống sao lưu ngoại vi và xây dựng chính sách bảo trì định kỳ.
14	Attacker	Tấn công thông qua email giả mạo (Spear Phishing)	Sử dụng các giải pháp bảo mật email và đào tạo nhân viên về cách phát hiện phishing.
15	Attacker	Khai thác lỗ hổng phần mềm chưa vá	Liên tục kiểm tra và cập nhật các bản vá và bảo mật.
16	Attacker	Sniffing	Mã hóa dữ liệu khi truyền và bảo mật kết nối mạng.
17	Attacker	Tấn công DDoS	Sử dụng tường lửa ứng dụng web (WAF) và các giải pháp chống DDoS.
18	Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp	Cài đặt phần mềm chống virus và tường lửa mạng.
19	Attacker	Phá hủy thiết bị	Theo dõi thiết bị vật lý và có kế hoạch khôi phục từ sao lưu.
20	Attacker	Khai thác thông tin thông qua Social Engineering	Đào tạo nhận thức bảo mật cho nhân viên và cập nhật thường xuyên chính sách bảo mật.
21			
22	Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)	Kiểm tra và xử lý các đầu vào của người dùng để ngăn chặn XSS.
23			
24	Attacker	Tấn công Brute Force để phá mật khẩu	Giới hạn số lần thử đăng nhập và kích hoạt CAPTCHA hoặc 2FA.
25	Attacker	Tấn công Cơ sở dữ liệu	Thiết lập cơ chế kiểm tra đầu vào.

$$C_y = C_y^{\alpha} (\alpha - \alpha)$$

03. Risk Score (mô hình hiện tại)

1	Threat		STRIDE category		Impact Score			Likelihood			Risk Score
2	Agent	Action			C	I	A	E	F	S	
3	Employee	Lộ thông tin cấu hình server	I	endpoint	5	5	1	5	3	1	20
4	Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	S, I	endpoint	5	1	1	3	4	1	17.5
5	Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân	T	endpoint	3	2	0	3	3	1	9
6	Employee	Sử dụng phần mềm không rõ nguồn gốc	I, T	network	3	5	3	3	3	1	15
7	Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	T, I	endpoint	5	5	3	3	3	1	15
8	Employee	Bị khai thác thông tin thông qua phương thức Social Engineering	E	network	3	1	0	1	3	1	6
9	Employee	Không khóa máy tính khi rời khỏi vị trí làm việc	S, I	endpoint	5	5	1	1	2	1	7.5
10	Employee	Làm lộ bản ghi nhật ký (log)	I	endpoint	5	3	1	5	5	1	25
11	Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy)	I, D	endpoint	3	5	1	2	4	1	15
12	Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)	E	other	5	5	3	5	3	1	20
13	Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	D	endpoint	3	5	5	4	2	1	15
14	Attacker	Tấn công thông qua email giả mạo (Spear Phishing)		email	5	3	1	5	5	1	25
15	Attacker	Khai thác lỗ hổng phần mềm chưa vá	T, I, E	endpoint	5	5	4	5	3	1	20
16	Attacker	Sniffing	I	network	5	5	2	5	3	1	20
17	Attacker	Tấn công DDoS	D	network	1	1	5	1	5	1	15
18	Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp	T, I	endpoint	5	5	3	5	3	1	20
19	Attacker	Phá hủy thiết bị	T, D	endpoint	3	3	1	2	2	1	6
20	Attacker	Khai thác thông tin thông qua Social Engineering	E, S	other	5	2	2	5	5	1	25
21				endpoint	5	4	2	4	3	1	17.5
22	Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)	T, I	endpoint	4	5	5	5	4	1	22.5
23				endpoint	4	5	3	4	5	1	22.5
24	Attacker	Tấn công Brute Force để phá mật khẩu	S, E	endpoint	5	0	0	5	5	1	25
25	Attacker	Tấn công Cơ sở dữ liệu	I	endpoint	3	3	0	2	3	1	7.5

STRIDE framework
 Spoofing identity (S)
 Tampering with data (T)
 Repudiation (R)
 Information disclosure (I)
 Denial of service (D)
 Elevation of privilege (E)

xem xét lại điểm S
 Thêm cột nguồn gốc

$$C_y = C_1^{\alpha} (\alpha - \alpha)$$

04. Rủi ro mất mát dữ liệu (tiêu chuẩn NIST CSF 2.0)

Rủi ro từ việc truy cập trái phép

- **Mô tả:** Dữ liệu bị truy cập trái phép do không có cơ chế quản lý quyền truy cập chặt chẽ làm lộ thông tin nhạy cảm hoặc thất thoát dữ liệu.
- **Tiêu chuẩn:** thuộc chức năng **Protect (PR)** về **Identity Management, Authentication, and Access Control (PR.AA)**.
 - **PR.AA-03:** Người dùng, dịch vụ, và thiết bị được xác thực trước khi truy cập tài sản.
 - **PR.AA-05:** Quyền truy cập, quyền lợi, và các ủy quyền được quản lý, thực thi, và xem xét định kỳ, đồng thời tuân thủ nguyên tắc quyền tối thiểu (Least Privilege) và phân tách nhiệm vụ (Separation of Duties).

04. Rủi ro mất mát dữ liệu (tiêu chuẩn NIST CSF 2.0)

Rủi ro mất mát dữ liệu do không backup

- **Mô tả:** Không có cơ chế sao lưu dữ liệu, dữ liệu không được sao lưu định kỳ có thể dẫn đến mất mát dữ liệu khi sự cố xảy ra.
- **Tiêu chuẩn:** thuộc chức năng **Protect (PR)** về **Data Security (PR.DS)**.
 - **PR.DS-01:** Tính bảo mật, toàn vẹn, và sẵn sàng của dữ liệu khi lưu trữ được bảo vệ.
 - **PR.DS-02:** Tính bảo mật, toàn vẹn, và sẵn sàng của dữ liệu khi truyền tải được bảo vệ.
 - **PR.DS-11:** Các bản sao lưu dữ liệu được tạo, bảo vệ, duy trì và kiểm tra định kỳ.

04. Rủi ro mất mát dữ liệu (tiêu chuẩn NIST CSF 2.0)

Rủi ro từ việc không ghi log

- **Mô tả:** Thiếu công cụ ghi log và quản lý log, không phát hiện sớm các sự kiện tiềm ẩn có thể gây hại, gây khó khăn trong việc điều tra và phục hồi sau sự cố.
- **Tiêu chuẩn:** thuộc chức năng **Detect (DE)** về **Continuous Monitoring (DE.CM)**.
 - **DE.CM-03:** Hoạt động của nhân sự và việc sử dụng công nghệ được giám sát để phát hiện các sự kiện tiềm ẩn có thể gây hại.
 - **DE.CM-06:** Hoạt động và dịch vụ của các nhà cung cấp dịch vụ bên ngoài được giám sát để phát hiện các sự kiện tiềm ẩn có thể gây hại.
 - **DE.CM-09:** Phần cứng và phần mềm máy tính, môi trường chạy và dữ liệu của chúng được giám sát để phát hiện các sự kiện tiềm ẩn có thể gây hại.

04. Rủi ro mất mát dữ liệu (tiêu chuẩn NIST CSF 2.0)

Rủi ro giám sát sự cố không đầy đủ

Mô tả: Không có các công cụ giám sát tự động và phản ứng khi bị tấn công, sự cố bảo mật có thể bị bỏ sót hoặc phát hiện muộn, không ngăn cản kịp thời.

- **Tiêu chuẩn:** thuộc chức năng **Respond (RS)** về **Incident Management (RS.MA)**.
 - **RS.MA-01:** Kế hoạch phản ứng sự cố được thực hiện phối hợp với các bên thứ ba liên quan khi một sự cố được công nhận.
 - **RS.MA-02:** Báo cáo sự cố được phân loại và xác thực.
 - **RS.MA-03:** Các sự cố được phân loại và ưu tiên.

04. Rủi ro mất mát dữ liệu (tiêu chuẩn NIST CSF 2.0)

Rủi ro về tính sẵn sàng và hiệu suất truyền tải dữ liệu

Mô tả: Thiếu load balancing có thể gây mất cân bằng trong việc phân phối tải và dẫn đến sự gián đoạn trong việc kiểm soát và bảo mật các luồng dữ liệu.

- **Tiêu chuẩn:** thuộc chức năng **Identify (ID)** về **Asset Management (ID.AM)**.
 - o **ID.AM-03:** Các giao tiếp mạng được ủy quyền của tổ chức và luồng dữ liệu mạng nội bộ và bên ngoài được duy trì.

04. Rủi ro mất mát dữ liệu (tiêu chuẩn PCI DSS)

Yếu tố	Điểm hiện tại	Phân tích	Điểm đề xuất	Biện pháp cải thiện
Bảo vệ đầu cuối (endpoints)	1	Nguy cơ khai thác các endpoint không bảo mật để thực hiện tấn công như phishing hoặc ransomware.	4	Cài đặt phần mềm antivirus, kiểm tra thiết bị định kỳ và yêu cầu sử dụng MFA khi đăng nhập vào các thiết bị đầu cuối
Theo dõi và giám sát truy cập	2	Thiếu nhật ký có thể gây khó khăn trong việc phát hiện sự cố.	4	Triển khai hệ thống SIEM và log management
Chính sách bảo mật	2	Thiếu chính sách có nguy cơ không tuân thủ PCI DSS.	4	Tổ chức đào tạo nhân viên và cập nhật chính sách bảo mật
Xác thực và quản lý danh tính	1	Các kết nối từ xa không an toàn có thể bị tấn công	4	Triển khai MFA, Single Sign-On và chính sách mật khẩu.
Tường lửa	3	Tường lửa cơ bản không đủ mạnh để phát hiện và ngăn chặn các mối đe dọa tinh vi.	5	Triển khai Next-Generation Firewall tại Perimeter Module và các giải pháp bảo vệ WAF, ACL ở External Security Module.

$$C_4 = C_1^{\alpha} (\alpha - \dots)$$

04. Rủi ro mất mát dữ liệu (tiêu chuẩn ISO/IEC 27001)

A. Về mặt tổ chức

1. Không có các chính sách an ninh thông tin, không có các chính sách cụ thể cho từng chủ đề
2. Không có dịch vụ hay bộ phận thu thập các mẫu thông tin từ các cuộc tấn công cũng như không có quy trình cập nhật cơ sở dữ liệu về các cuộc tấn công
3. Không có quy tắc sử dụng thông tin, không có các quy trình xử lý thông tin cùng các tài sản liên quan khác đối với các bên có liên quan
4. Không có quy định, quy trình hoàn trả tài sản cho nhân viên và các bên liên quan trong trường hợp kết thúc hợp đồng hoặc mối quan hệ làm việc
5. Không có các quy tắc, quy trình hoặc thỏa thuận về việc truyền thông tin cho các hình thức truyền trong nội bộ tổ chức và giữa tổ chức với các bên khác.
6. Không kiểm soát truy cập vật lý và logic vào dữ liệu và các tài sản liên quan
7. Không có dịch vụ hay hệ thống quản lý danh tính
8. Không có quy trình quản lý xác thực thông tin, không có hướng dẫn nhân sự về cách xử lý thông tin xác thực

04. Rủi ro mất mát dữ liệu (tiêu chuẩn ISO/IEC 27001)

A. Về mặt tổ chức

9. Không có phân quyền rõ về quyền truy cập vào thông tin và các tài sản liên quan khác
10. Các quy trình và thủ tục liên quan đến việc sử dụng sản phẩm hoặc dịch vụ của nhà cung cấp chưa được xác định và thực hiện
11. Không có phân công giám sát thường xuyên các thay đổi về dịch vụ của các nhà cung cấp bên thứ ba
12. Chưa có kế hoạch để quản lý các sự cố an ninh, chưa có quy trình để đánh giá các sự kiện an ninh và phân loại thành sự cố, chưa có văn bản quy định quy trình, thủ tục ứng phó các sự cố an ninh thông tin
13. Không có quy trình bảo vệ hồ sơ khởi vấn đề mất cắp, bị phá hủy, làm giả, truy cập hoặc công khai khi chưa được cấp phép
14. Chưa đáp ứng được các yêu cầu liên quan đến việc bảo vệ quyền riêng tư và bảo vệ thông tin nhận dạng cá nhân (PII) theo các luật, quy định hiện hành

04. Rủi ro mất mát dữ liệu (tiêu chuẩn ISO/IEC 27001)

B. Về mặt quản lý con người

1. Không có quá trình xác minh lý lịch đối với tất cả các ứng viên trước khi trở thành nhân sự
2. Nhân sự của tổ chức và các bên liên quan chưa được đào tạo, giáo dục về an ninh thông tin
3. Các thỏa thuận bảo mật và không tiết lộ thông tin chưa được xác định, lập văn bản, xem xét định kỳ và ký kết bởi nhân sự và các bên liên quan

04. Rủi ro mất mát dữ liệu (tiêu chuẩn ISO/IEC 27001)

C. Về mặt quản lý tài sản vật lý

1. An ninh vật lý cho văn phòng, phòng và các cơ sở vật chất chưa được thiết kế và triển khai.
2. Các khu vực an ninh chưa được bảo vệ bằng các biện pháp kiểm soát truy cập
3. Các khu vực an ninh chưa được bảo vệ bằng các biện pháp kiểm soát truy cập
4. Các biện pháp bảo vệ chống lại mối đe dọa vật lý và môi trường, như thiên tai hoặc các mối đe dọa vật lý cố ý hay vô ý đối với cơ sở hạ tầng, chưa được thiết kế và triển khai.
5. Các biện pháp cho việc làm việc trong khu vực an ninh chưa được thiết kế và triển khai
6. Thiết bị cần được đặt ở vị trí an toàn và được bảo vệ.
7. Phương tiện lưu trữ chưa có quy trình quản lý
8. A.7.14 Xử lý hoặc tái sử dụng thiết bị an toàn
9. Chưa có quy trình xóa hoặc ghi đè an toàn mọi dữ liệu nhạy cảm và phần mềm có bản quyền trước khi tiến hành hủy bỏ hoặc tái sử dụng thiết bị.

04. Rủi ro mất mát dữ liệu (tiêu chuẩn ISO/IEC 27001)

D. Về mặt kĩ thuật

1. Chưa có biện pháp bảo vệ trên thiết bị đầu cuối của người dùng
2. Cấp phát và sử dụng quyền truy cập đặc quyền chưa được quản lý chặt chẽ
3. Không có hạn chế truy cập vào thông tin và các tài sản liên quan
4. Không có phân rõ quyền đọc và sửa đổi mã nguồn, công cụ phát triển và thư viện
5. Không có triển khai công nghệ và quy trình xác thực an toàn dựa trên các hạn chế truy cập thông tin và chính sách cụ thể về kiểm soát truy cập
6. Không có các biện pháp bảo vệ chống phần mềm độc hại, không có hướng dẫn, đào tạo để nâng cao nhận thức người dùng
7. Không có quy trình quản lí, thu thập thông tin về các lỗ hổng kĩ thuật của hệ thống thông tin đang sử dụng và mức độ phơi nhiễm của chúng
8. Các cấu hình, bao gồm cấu hình bảo mật, của phần cứng, phần mềm, dịch vụ và mạng chưa được thiết lập, lập thành văn bản, triển khai, giám sát và xem xét định kỳ.

04. Rủi ro mất mát dữ liệu (tiêu chuẩn ISO/IEC 27001)

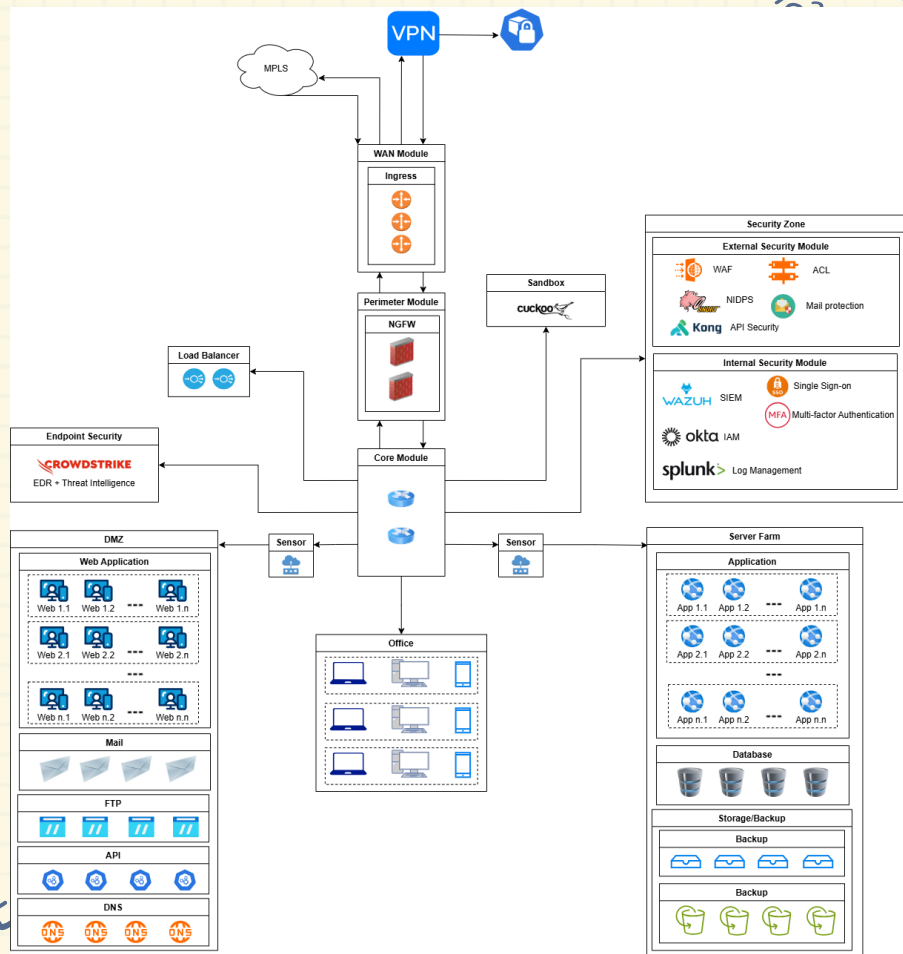
D. Về mặt kĩ thuật

9. Thông tin được lưu trữ trong hệ thống thông tin, thiết bị hoặc bất kỳ phương tiện lưu trữ nào khác cần được xóa khi không còn cần thiết.
10. Không có biện pháp che dấu dữ liệu
11. Không có quy định về hạn chế và kiểm soát việc sử dụng các chương trình tiện ích có khả năng ghi đè lên các kiểm soát hệ thống và ứng dụng
12. Các quy trình và biện pháp cần được triển khai để quản lý an toàn việc cài đặt phần mềm trên các hệ thống hoạt động.
13. Mạng và các thiết bị mạng cần được bảo mật, quản lý và kiểm soát để bảo vệ thông tin trong hệ thống và ứng dụng.
14. Cơ chế bảo mật, mức độ dịch vụ và các yêu cầu dịch vụ của dịch vụ mạng cần được xác định, triển khai và giám sát.
15. Truy cập vào các trang web bên ngoài cần được quản lý để giảm thiểu rủi ro tiếp xúc với nội dung độc hại.
16. Các quy tắc sử dụng mật mã hiệu quả, bao gồm quản lý khóa mật mã, cần được xác định và triển khai.
17. Tổ chức cần hướng dẫn, giám sát và xem xét các hoạt động liên quan đến các dịch vụ đang được thuê, sử dụng từ nguồn ngoài

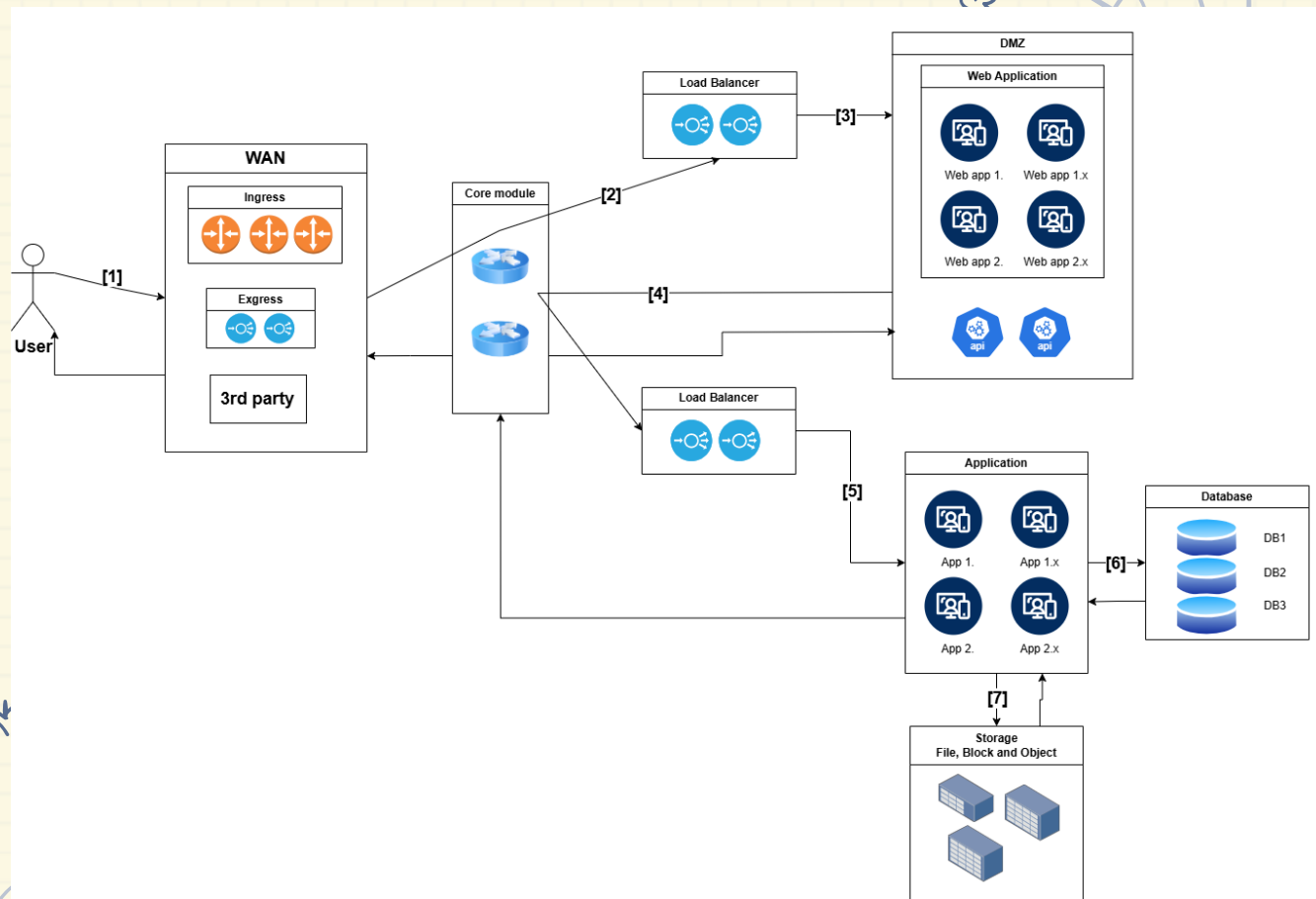
05

**Đề xuất mô hình mạng mới
+ chính sách vận hành mới
Bảng Risk score mới**

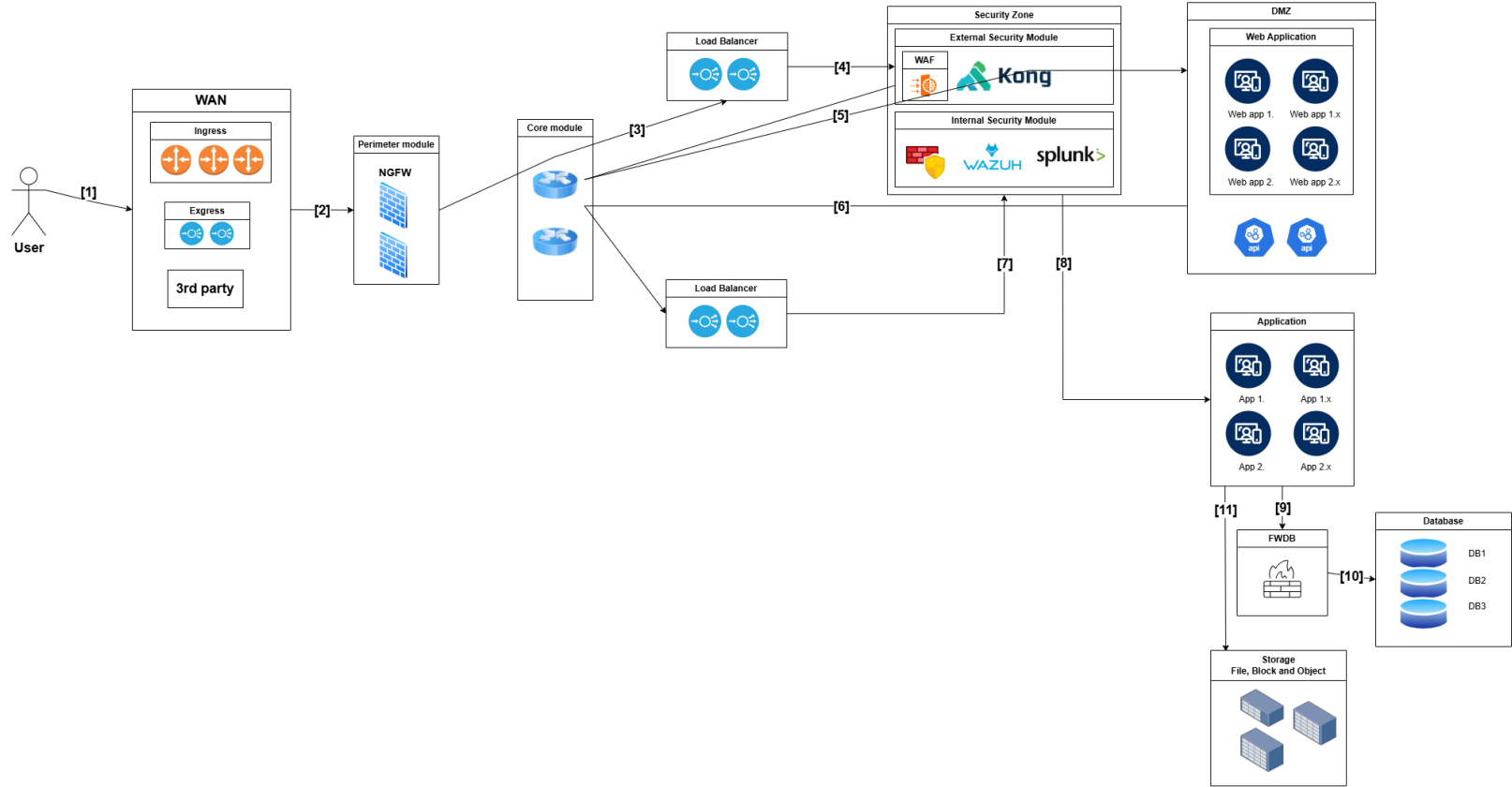
Overall architect



Application architect



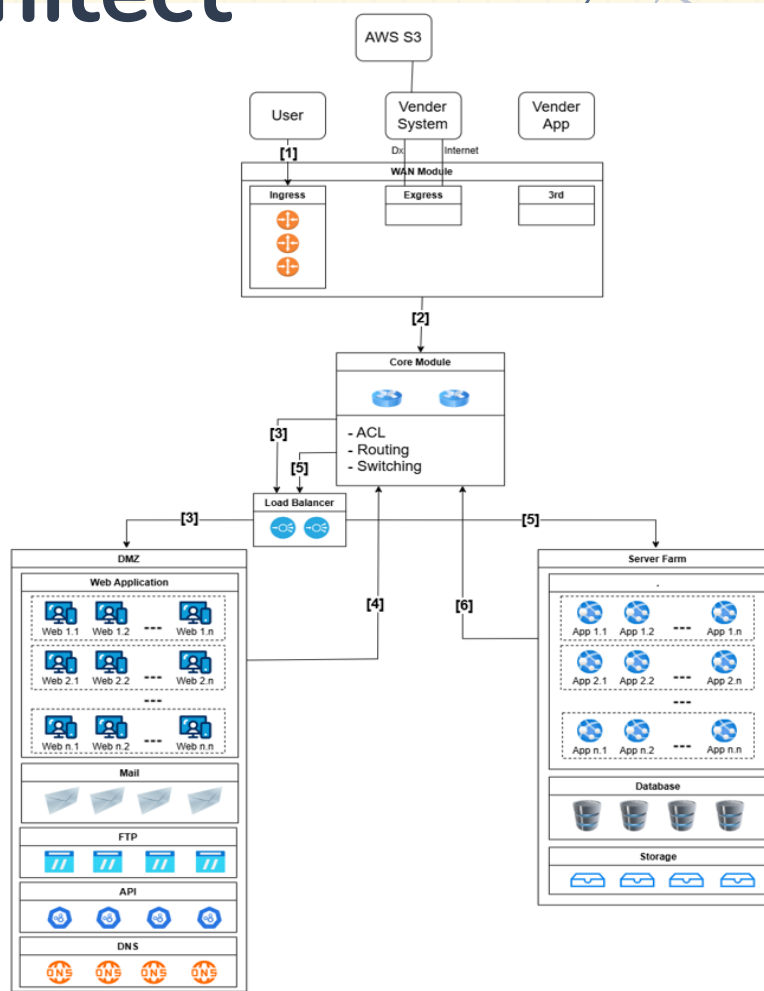
Application Security architect



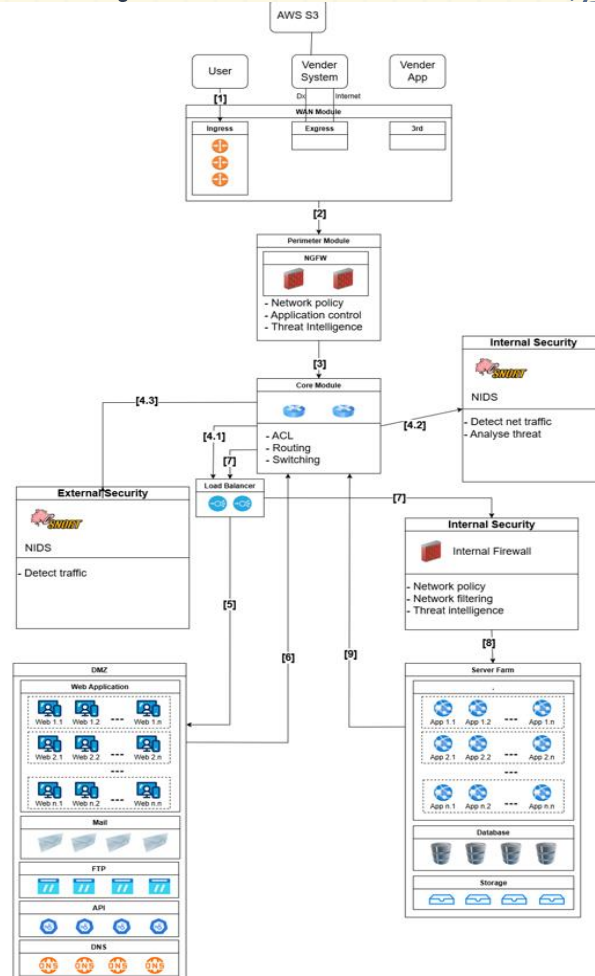
Application Security policy

1. Bảo vệ API: Rate Limiting và sử dụng API Gateway với xác thực bắt buộc (OAuth2, JWT)
2. Sử dụng mã hóa mạnh mẽ (AES-256) cho tất cả dữ liệu lưu trữ và truyền tải dữ liệu qua mạng phải được bảo mật qua giao thức HTTPS (tối thiểu TLS v1.2)
3. Cấu hình Secure Cookie: Bật thuộc tính HttpOnly, Secure, và SameSite cho tất cả cookie phiên làm việc, mã hóa Cookie
4. Tích hợp CSP (Content Security Policy): CSP phải được cấu hình để chỉ cho phép tải tài nguyên từ các nguồn đáng tin cậy. Chặn tất cả các script, style, và hình ảnh không được liệt kê rõ ràng trong chính sách CSP
5. Kiểm tra và khắc phục lỗ hổng ứng dụng bằng DAST trước khi triển khai vì giúp phát hiện các lỗ hổng bảo mật trong ứng dụng, sử dụng trước khi triển khai để giảm thiểu nguy cơ bị khai thác lỗ hổng
6. Thực hiện Code Review thường xuyên với các công cụ SAST kiểm tra mã nguồn để phát hiện lỗ hổng bảo mật, giảm nguy cơ khai thác từ lỗi lập trình
7. Áp dụng chuẩn bảo mật OWASP Top 10 cho phát triển ứng dụng, bảo vệ khỏi các lỗ hổng phổ biến, tăng cường độ an toàn của ứng dụng
8. Áp dụng chính sách Least Privilege cho tài khoản ứng dụng, giới hạn quyền truy cập của người dùng, áp dụng cho tài khoản ứng dụng để giảm thiểu rủi ro khi bị xâm phạm
9. Sử dụng SIEM: Tích hợp hệ thống SIEM để ghi nhận và phân tích hoạt động người dùng trong thời gian thực để phát hiện hành vi bất thường và tự động gửi cảnh báo
10. Thực hiện kiểm tra bảo mật định kỳ với các chuyên gia; các kết quả kiểm tra phải được lập báo cáo và đưa vào kế hoạch cải thiện.

Network Architect



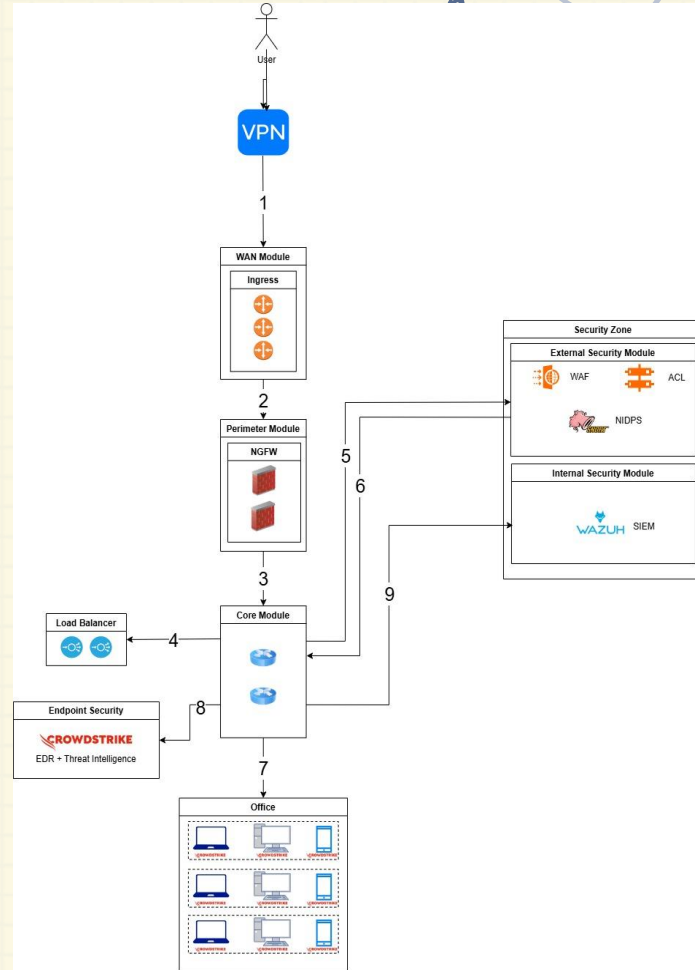
Network Security Architect



Network Security policy

1. Thiết lập các quy tắc ACL trên core module để cho phép hoặc từ chối lưu lượng dựa trên địa chỉ IP, giao thức và cổng mạng
2. Hạn chế hoặc chặn các cổng và giao thức không cần thiết để giảm nguy cơ khai thác lỗ hổng
3. Cấu hình NIDS để giám sát toàn bộ lưu lượng nội bộ và phát hiện hành vi bất thường
4. Sử dụng internal firewall để kiểm soát lưu lượng giữa các thành phần trong hệ thống
5. Triển khai DNSSEC để ngăn chặn các cuộc tấn công giả mạo DNS (DNS Spoofing) và đảm bảo tính toàn vẹn của truy vấn DNS
6. Triển khai Email Security Gateway: Lọc và giám sát tất cả email ra/vào để ngăn chặn thư rác, phishing, và các tệp đính kèm độc hại
7. Thực hiện kiểm tra bảo mật mạng định kỳ với penetration testing để phát hiện các lỗ hổng có nguy cơ, đảm bảo các thiết lập luôn hoạt động đúng chức năng
8. Tích hợp các nguồn dữ liệu threat intelligence để cập nhật về các mối đe dọa mới nhất
9. Sử dụng mã hóa cho tất cả lưu lượng truyền qua mạng để không bị nghe lén, sửa, xóa trong quá trình truyền tải dữ liệu.
10. Phân đoạn mạng sâu hơn bằng cách kiểm soát lưu lượng giữa các workload hoặc máy chủ để hạn chế vùng bị ảnh hưởng khi xảy ra xâm nhập (các vùng như DMZ, internal security, external security, và public network để cô lập lưu lượng truy cập)

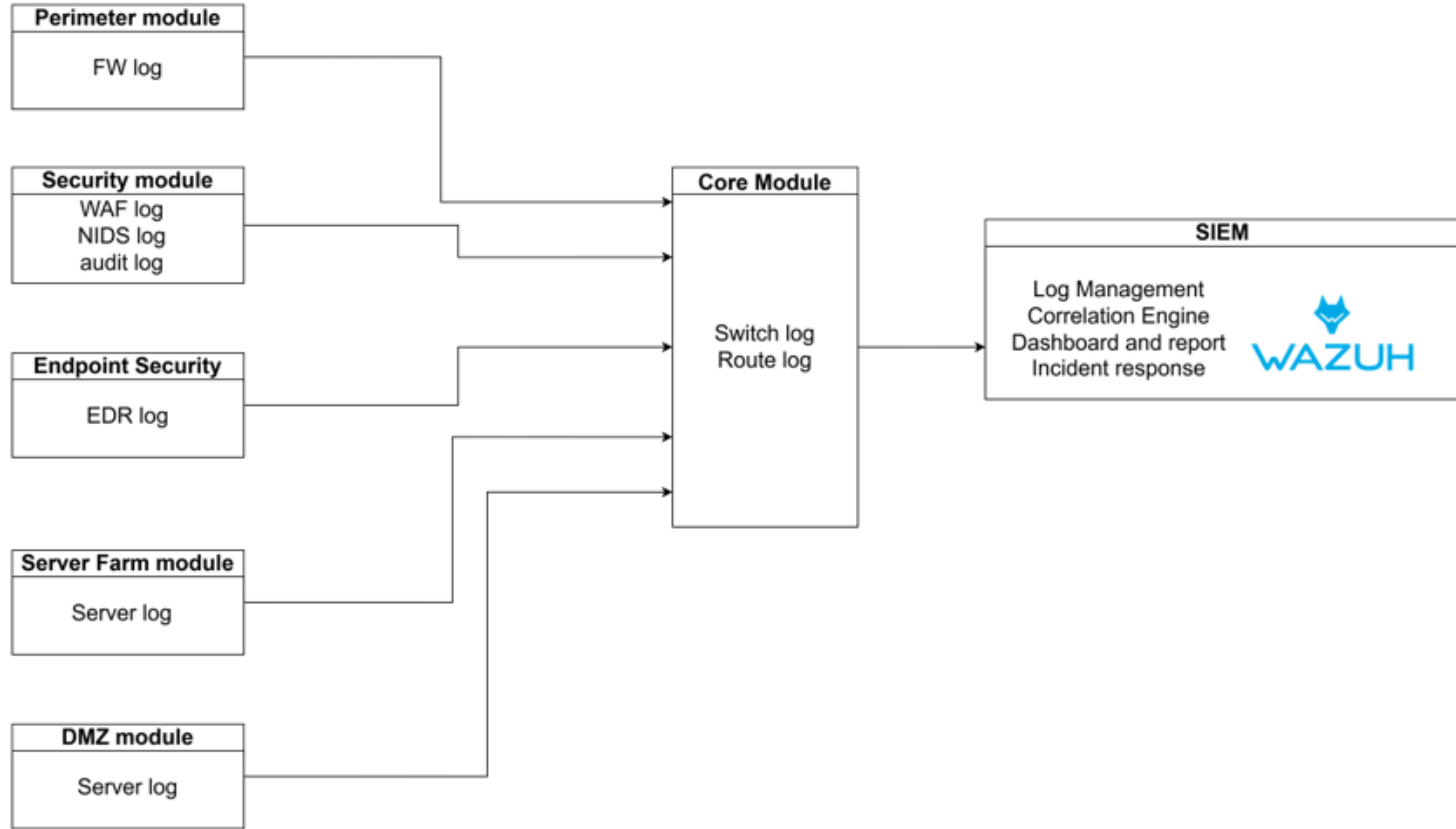
Endpoint security architect



Endpoint security policy

1. Giải pháp EDR cần có khả năng giám sát liên tục theo thời gian thực, khả năng thu thập dữ liệu, phản hồi tự động theo cơ chế rule-based và khả năng phân tích sự kiện
2. Giải pháp EDR cần phải giám sát và bảo vệ trên tất cả các thiết bị đầu cuối. Giải pháp EDR không được phụ thuộc vào hệ điều hành. Trong trường hợp thiết bị đầu cuối không thể triển khai giải pháp, cần tách thiết bị vào một nhóm riêng và được giám sát đặc biệt
3. Giải pháp EDR cần phải cung cấp thông tin về kỹ thuật, chiến thuật, quy trình mà kẻ tấn công sử dụng
4. Tất cả các bản vá, bản cập nhật của phần mềm EDR cần được cập nhật ngay khi nhà phát hành ra mắt
5. Tất cả bản cập nhật phải tuân thủ quy trình được đề ra trong tổ chức
6. Giải pháp EDR phải cung cấp được khả năng phân tích sâu và pháp chứng kỹ thuật số trong trường hợp cần phải tiến hành điều tra
7. Giải pháp EDR cần có khả năng mở rộng
8. Có quy trình sao lưu và lịch trình sao lưu các dữ liệu, cảnh báo, tệp cấu hình của giải pháp EDR
9. Giải pháp EDR phải giám sát và thu thập dữ liệu hoạt động từ các thiết bị đầu cuối để phát hiện các dấu hiệu có thể là mối đe dọa.
10. EDR phải có khả năng tương quan dữ liệu trên toàn bộ phạm vi giám sát của môi trường.

SIEM architect



SIEM policy

- Chính sách quản lý log:

Mục tiêu: Đảm bảo dữ liệu nhật ký được thu thập, và quản lý đúng cách để hỗ trợ việc giám sát và phát hiện mối đe dọa.

Quy định:

- Loại thông tin thu thập: Server log, EDR log, Syslog, WAF log, NIDS log, audit log, FW log, switch log, route log.
- Các module: Perimeter module, Security module, Endpoint Security, Server Farm module, DMZ module, Core module.
- Các sự kiện cần được thu thập: Log của traffic từ bên ngoài vào mạng nội bộ, log của traffic lưu thông trong mạng nội bộ, các log, cảnh báo từ EDR, IDS, IAM, PAM, Web Application Firewall, các log sự kiện từ Server Farm, DMZ.
- Bảo vệ và kiểm soát truy cập dữ liệu nhật ký: Chỉ có các thành viên đội ngũ an ninh được phép truy cập và xem dữ liệu nhật ký.

- Chính sách phát hiện mối đe dọa:

Mục tiêu: Trình tự xử lý khi phát hiện sự cố an ninh mạng qua SIEM

Quy định:

- Xác định các hành vi đáng ngờ, ngưỡng phát hiện
- Phân loại mối đe dọa (thấp, trung bình, cao, nghiêm trọng) dựa trên các tiêu chuẩn bảo mật như NIST, ISO/IEC27001 để đánh giá, từ đó đưa ra plan khắc phục
- Cập nhật thông tin liên tục về mối đe dọa (có thể dựa trên các mô hình hành vi, tích hợp Threat Intelligence Feeds, ...)

SIEM policy

- Chính sách ứng phó sự cố:

Mục tiêu: Trình tự xử lý khi phát hiện sự cố an ninh mạng qua SIEM

Quy định:

- Xác định và báo cáo sự cố.
- Các bước ứng phó: cô lập hệ thống, điều tra, xử lý và khôi phục.
- Xác định vai trò và trách nhiệm của các bộ phận liên quan.
- Hướng dẫn báo cáo sự cố cho quản lý hoặc cơ quan chức năng.

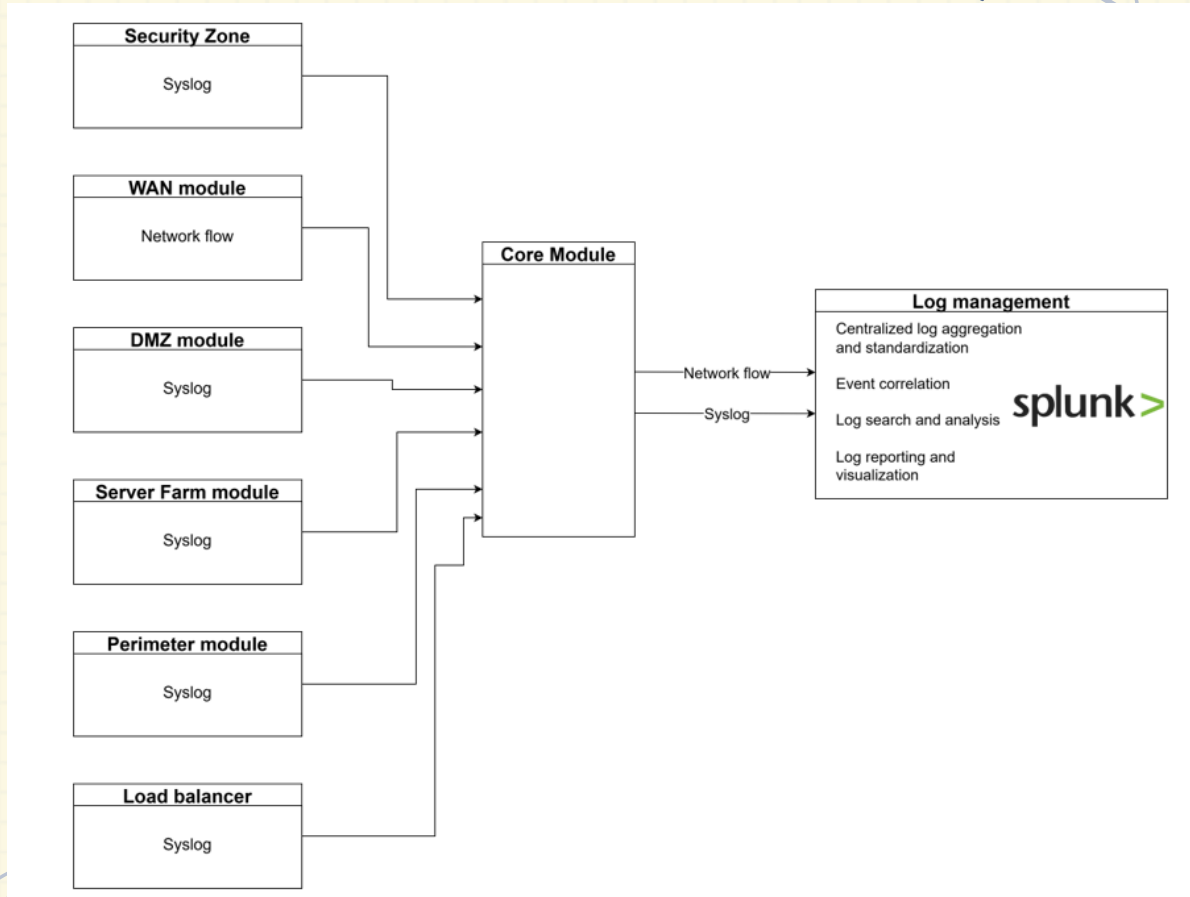
- Chính sách sao lưu log:

Mục tiêu: Đảm bảo tính toàn vẹn và khả năng phục hồi dữ liệu trong mọi tình huống

Quy định:

- Tần suất: Hằng tuần.
- Phương pháp sao lưu: Có thể sử dụng các dịch vụ đám mây để lưu trữ dữ liệu
- Thời gian lưu trữ: Tối thiểu 1 năm (theo tiêu chuẩn PCI DSS)
- Kiểm tra định kỳ tính toàn vẹn.
- Bảo mật: Mã hóa và kiểm soát quyền truy cập (chỉ có trưởng phòng an ninh có quyền chỉnh sửa, khôi phục sao lưu).

Log management architect



Log management policy



a. Tất cả các hệ thống sản xuất trong tổ chức phải ghi lại và lưu trữ thông tin nhật ký kiểm tra, bao gồm:

- i. Các hoạt động được thực hiện trên hệ thống.
- ii. Người dùng hoặc tài khoản hệ thống thực hiện hoạt động, bao gồm cả hệ thống mà hoạt động được thực hiện trên đó.
- iii. Tập, ứng dụng hoặc đối tượng khác mà hoạt động được thực hiện trên đó.
- iv. Thời gian diễn ra hoạt động.
- v. Công cụ được sử dụng để thực hiện hoạt động.
- vi. Kết quả (ví dụ: thành công hoặc thất bại) của hoạt động.

b. Các hoạt động cụ thể cần được ghi lại phải bao gồm tối thiểu:

- i. Thông tin (bao gồm thông tin xác thực như tên người dùng hoặc mật khẩu) được tạo, đọc, cập nhật hoặc xóa.
- ii. Các kết nối mạng được chấp nhận hoặc khởi tạo.
- iii. Xác thực và ủy quyền của người dùng tới các hệ thống và mạng.
- iv. Cấp, sửa đổi hoặc thu hồi quyền truy cập, bao gồm thêm người dùng hoặc nhóm mới; thay đổi quyền người dùng, quyền tập, quyền đối tượng cơ sở dữ liệu, quy tắc tường lửa và mật khẩu.
- v. Thay đổi cấu hình hệ thống, mạng hoặc dịch vụ, bao gồm cài đặt phần mềm, vá lỗi, cập nhật hoặc các thay đổi phần mềm khác.
- vi. Khởi động, tắt hoặc khởi động lại một ứng dụng.
- vii. Application process bị hủy, thất bại hoặc kết thúc bất thường, đặc biệt là do cạn kiệt tài nguyên hoặc đạt đến giới hạn hoặc ngưỡng tài nguyên (như CPU, bộ nhớ, kết nối mạng, băng thông mạng, dung lượng đĩa, hoặc các tài nguyên khác); thất bại của các dịch vụ mạng như DHCP hoặc DNS, hoặc lỗi phần cứng.
- viii. Phát hiện hoạt động đáng ngờ và/hoặc độc hại từ các hệ thống bảo mật như IDS/IPS, hệ thống chống virus hoặc chống phần mềm gián điệp.

Log management policy

$$E=mc^2$$



$$T=2\pi$$

c. Tất cả các nhật ký phải được tập hợp trong một hệ thống trung tâm, nếu khả thi về mặt kỹ thuật, để các hoạt động trên các hệ thống khác nhau có thể được liên kết, phân tích và theo dõi theo xu hướng hoặc hiệu ứng dây chuyền. Hệ thống tập hợp nhật ký phải:

- Tự động và kịp thời cập nhật nhật ký.
- Giảm thiểu sự kiện và bất thường, phát cảnh báo.
- Có khả năng kiểm tra thủ công.

d. Nhật ký phải được kiểm tra thủ công định kỳ:

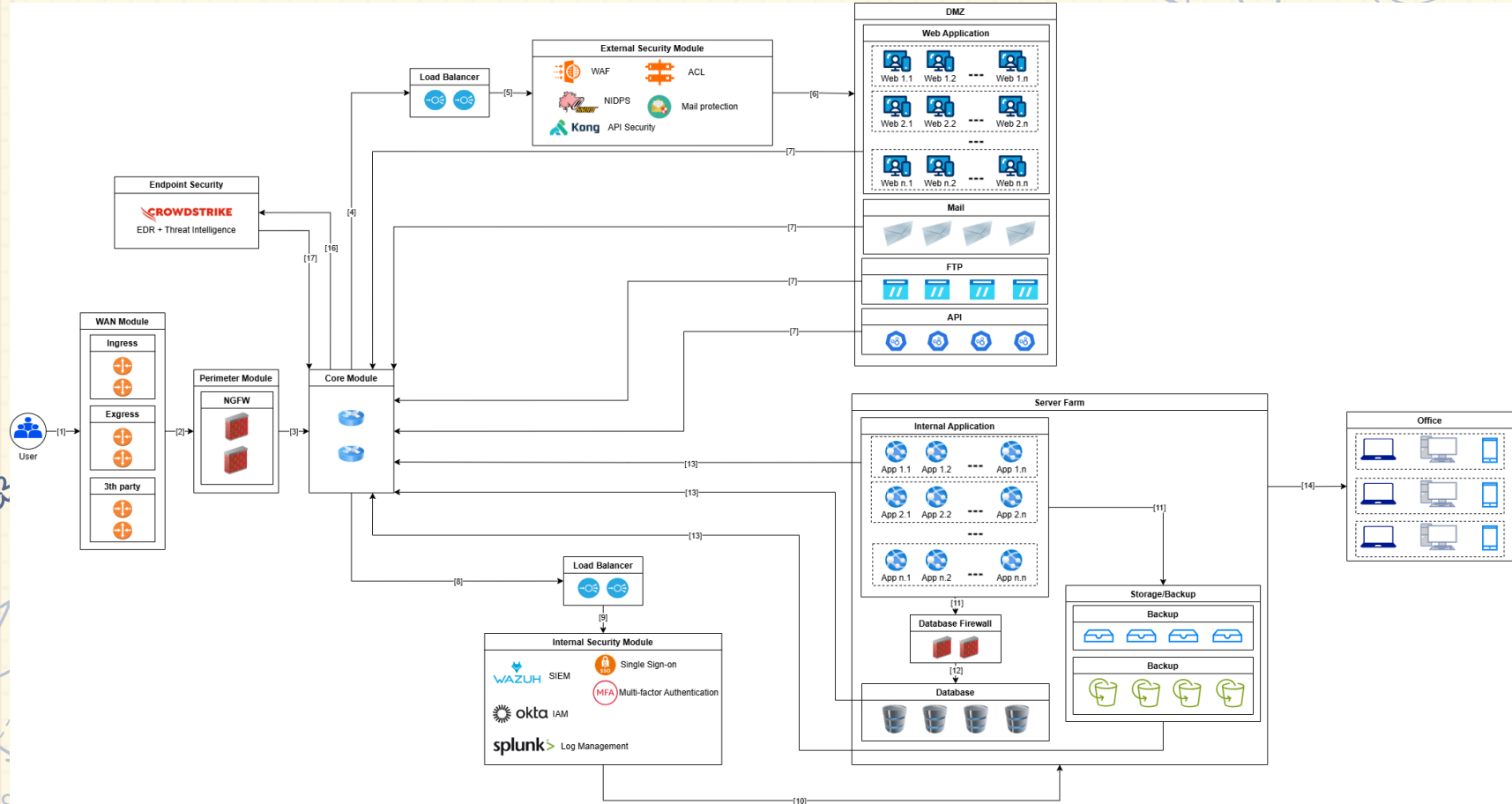
- i. Các hoạt động của người dùng, quản trị viên và người vận hành hệ thống phải được xem xét ít nhất hàng tháng.
- ii. Nhật ký liên quan đến thông tin nhận dạng cá nhân (PII) phải được kiểm tra ít nhất hàng tháng để phát hiện hành vi bất thường.

e. Khi sử dụng môi trường đám mây thuê ngoài, phải lưu giữ nhật ký về:

- Quyền truy cập và sử dụng môi trường đám mây.
- Phân bổ và sử dụng tài nguyên.
- Các thay đổi đối với thông tin nhận dạng cá nhân (PII).
- Nhật ký phải được lưu trữ cho tất cả quản trị viên và nhà vận hành thực hiện các hoạt động trong môi trường đám mây.

f. Tất cả các hệ thống thông tin trong tổ chức phải đồng bộ hóa đồng hồ của mình bằng cách triển khai Network Time Protocol (NTP) hoặc các khả năng tương tự. Tất cả các hệ thống thông tin phải đồng bộ hóa với cùng một mốc thời gian.

Incident response architect



Incident response policy

1. Policy về phản hồi sự cố (Incident Response Policy):

Mục tiêu: Đảm bảo sự cố được xử lý nhanh chóng, giảm thiểu tác động.

Quy định:

- Định nghĩa các cấp độ ưu tiên cho từng loại sự cố (Low, Medium, High, Critical).
- Thông báo sự cố đến các bên liên quan theo mức độ ưu tiên.
- Thiết lập đội phản ứng nhanh (IRT - Incident Response Team) với vai trò và trách nhiệm rõ ràng.

2. Policy về lưu trữ bằng chứng (Evidence Preservation Policy):

Mục tiêu: Lưu giữ và bảo vệ các bằng chứng phục vụ điều tra sự cố.

Quy định:

- Lưu trữ nhật ký hệ thống, nhật ký mạng (network logs), và các file bị ảnh hưởng trong ít nhất 90 ngày.
- Bảo đảm dữ liệu không bị chỉnh sửa trong quá trình lưu trữ.
- Sử dụng công cụ quản lý bằng chứng chuẩn như FTK Imager hoặc EnCase.

3. Policy về đào tạo và nhận thức (Training and Awareness Policy):

Mục tiêu: Đảm bảo nhân sự hiểu rõ quy trình phản hồi sự cố.

Quy định:

- Tổ chức diễn tập xử lý sự cố ít nhất 2 lần/năm.
- Đào tạo đội ngũ IRT về các công cụ và kỹ thuật phản ứng nhanh.
- Nâng cao nhận thức cho toàn bộ nhân viên về cách nhận diện và báo cáo sự cố.

Data security policy

1. Mã hóa dữ liệu khi lưu trữ và truyền tải (AES-256 và TLS 1.2 trở lên) bảo vệ thông tin khỏi truy cập trái phép để đảm bảo dữ liệu luôn an toàn
2. Áp dụng Role-Based Access Control (RBAC) cho quản lý quyền truy cập để giảm nguy cơ rò rỉ thông tin từ người dùng trái phép
3. Giám sát và phát hiện hành vi bất thường trên cơ sở dữ liệu với SIEM giám sát và xử lý kịp thời các vi phạm bảo mật khi xử lý dữ liệu
4. Tích hợp chính sách sao lưu dữ liệu định kỳ, đảm bảo khả năng khôi phục trong trường hợp mất dữ liệu, thực hiện định kỳ để giảm thiểu tác động từ sự cố
5. Sử dụng cơ chế Data Masking để ẩn danh dữ liệu nhạy cảm khi chia sẻ để giảm nguy cơ lộ thông tin quan trọng
6. Giới hạn quyền truy vấn cơ sở dữ liệu theo vai trò người dùng để giảm rủi ro nguy cơ xâm phạm
7. Tự động khóa tài khoản sau nhiều lần truy cập sai mật khẩu, phòng trường hợp bị tấn công Brute-force gây hậu quả nghiêm trọng
8. Thực hiện kiểm tra bảo mật cơ sở dữ liệu định kỳ giúp phát hiện và sửa lỗi kịp thời để tăng cường an toàn dữ liệu
9. Theo dõi lịch sử truy cập và thay đổi trên dữ liệu để kiểm soát và xử lý vi phạm nếu có
10. Tuân thủ các quy định bảo mật dữ liệu như GDPR, PCI DSS để tránh vi phạm luật, đảm bảo tuân thủ pháp luật

Identity security policy

1. Sử dụng MFA cho tất cả tài khoản truy cập, tăng cường lớp bảo mật để giảm nguy cơ xâm phạm
2. Thực hiện xác thực và ủy quyền người dùng thông qua IAM để đảm bảo chỉ những người được phép mới truy cập được tài nguyên
3. Kiểm tra logs đăng nhập thường xuyên để quan sát thông tin về các hoạt động trái phép, kiểm tra thường xuyên để phát hiện và xử lý sớm các hành vi đáng ngờ
4. Hạn chế quyền truy cập theo quy tắc Least Privilege chỉ cung cấp quyền hạn cần thiết để giảm thiểu thiệt hại nếu tài khoản bị xâm phạm. Phát triển chính sách Role-Based Access Control (RBAC): Quản lý quyền truy cập dựa trên vai trò cụ thể, đảm bảo chỉ những người thực sự cần thiết mới có quyền đối với tài nguyên
5. Sử dụng công cụ PAM để kiểm soát chặt chẽ tài khoản đặc quyền, giảm nguy cơ từ việc lạm dụng quyền truy cập
6. Áp dụng Conditional Access (Truy cập có điều kiện): Thiết lập các điều kiện cho phép hoặc từ chối truy cập (theo vị trí địa lý, thiết bị, hoặc thời gian) để giảm nguy cơ truy cập trái phép
7. Triển khai các chính sách mật khẩu mạnh mẽ: đặt chuẩn mật khẩu, tự động khóa tài khoản sau khi vượt số lượng lần nhập sai mật khẩu, thời gian thay đổi mật khẩu định kỳ để tránh việc bị rò rỉ thông tin
8. Sử dụng Identity Federation: Tích hợp xác thực liên kết (Identity Federation) để đồng bộ hóa danh tính trên nhiều hệ thống và giảm rủi ro từ mật khẩu yếu
9. Thu hồi quyền truy cập ngay khi nhân viên rời khỏi tổ chức tránh lạm dụng quyền không rõ ràng
10. Định danh mạnh với Hardware Tokens: Sử dụng các thiết bị vật lý (như YubiKey, RSA token) cho các tài khoản có quyền truy cập nhạy cảm để tăng cường bảo mật.

03. Risk Score (mô hình mới)

Threat			Vulnerability
Agent	Action		
Employee	Lộ thông tin cấu hình server		Cấu hình server công khai hoặc dễ dàng truy cập, chỉnh sửa
Employee	Sử dụng mật khẩu yếu hoặc trùng lặp		Không áp dụng chính sách mật khẩu mạnh
Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân		Lưu trữ dữ liệu nhạy cảm mà không mã hóa
Employee	Sử dụng phần mềm không rõ nguồn gốc		Cho phép cài đặt phần mềm từ nguồn không đáng tin cậy
Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống		Không có phần mềm chống mã độc trên thiết bị đầu cuối, AVE, FW + AV
Employee	Bị khai thác thông tin thông qua phương thức Social Engineering		Không có chính sách training cho nhân viên về các hình thức lừa đảo qua mạng
Employee	Không khóa máy tính khi rời khỏi vị trí làm việc		Không có khóa màn hình tự động
Employee	Làm lộ bản ghi nhật ký (log)		Không bảo vệ nhật ký hệ thống
Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy file ra ngoài thiết bị cá nhân và ngược lại, ...)		Không giới hạn số lượng thiết bị ngoại vi được sử dụng, không có chính sách bảo mật
Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)		Không có chính sách phân quyền hợp lý
Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố		Không có biện pháp backup và khôi phục dữ liệu kịp thời
Attacker	Tấn công thông qua email giả mạo (Spear Phishing)		Không đào tạo kiến thức bảo mật nghiêm ngặt, không kiểm tra email kỹ lưỡng
Attacker	Khai thác lỗ hổng phần mềm chưa vá		Không cập nhật hoặc vá lỗi phần mềm thường xuyên
Attacker	Sniffing		Không mã hóa thông tin nhạy cảm qua mạng
Attacker	Tấn công DDoS		Không có biện pháp phòng chống DDoS (solution chống DDoS, FW chống DDoS, cân bằng tải, ...)
Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp		Không có phần mềm chống mã độc trên thiết bị đầu cuối, AVE, FW + AV
Attacker	Phá hủy thiết bị		Không có biện pháp bảo vệ phần cứng và giám sát truy cập vật lý
Attacker	Khai thác thông tin thông qua Social Engineering		Thiếu đào tạo bảo mật cho nhân viên về nhận diện và đối phó với các hình thức lừa đảo như phishing (giả mạo email, cuộc gọi, hoặc tin nhắn)
Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)		Thiếu cơ chế xác thực danh tính đa yếu tố (MFA) cho các yêu cầu từ bên ngoài hoặc các truy cập từ xa
Attacker	Tấn công Brute Force để phá mật khẩu		Thiếu biện pháp mã hóa và kiểm tra các đầu vào (input validation and sanitization) trên các trường đầu vào trong trang web, như hộp tìm kiếm, bình luận, ...
Attacker	Tấn công Cơ sở dữ liệu		Không sử dụng Content Security Policy (CSP) để giới hạn nguồn tài nguyên hoặc ngăn chặn thực thi mã không mong muốn, không dùng X-XSS-Protection, X-Content-Type-Options, ...
			Không có chính sách khóa tài khoản sau nhiều lần đăng nhập thất bại hoặc không giới hạn số lần thử mật khẩu, chính sách mật khẩu thiếu sót, ...
			Bị lỗi SQL Injection, không có cơ chế kiểm tra input (này thầy bảo ok nè)

$$C_y = C_1^{\alpha} (\alpha - \alpha)$$

03. Risk Score (mô hình mới)

Threat		Impact
Agent	Action	
Employee	Lộ thông tin cấu hình server	Thông tin cấu hình server bị lộ có thể cung cấp cho kẻ tấn công các điểm yếu để khai thác
Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	Mật khẩu yếu dễ bị phá vỡ, và sử dụng mật khẩu trùng lặp có thể dẫn đến lộ tài khoản truy cập hệ thống
Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân	Dữ liệu nhạy cảm được lưu trữ trên thiết bị cá nhân có thể bị xâm nhập
Employee	Sử dụng phần mềm không rõ nguồn gốc	Phần mềm không rõ nguồn gốc có thể chứa mã độc hoặc mở ra lỗ hổng bảo mật cho hệ thống
Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	Malware có thể thay đổi tính toàn vẹn của hệ thống và lộ dữ liệu nhạy cảm
Employee	Bị khai thác thông tin thông qua phương thức Social Engineering	Nhân viên bị lừa cung cấp quyền truy cập hoặc thông tin nhạy cảm
Employee	Không khóa máy tính khi rời khỏi vị trí làm việc	Ai đó có thể truy cập trái phép vào hệ thống từ máy tính của nhân viên nếu không được khóa
Employee	Làm lộ bản ghi nhật ký (log)	Nhật ký hệ thống (log) không được bảo vệ có thể bị kẻ tấn công chỉnh sửa hoặc xóa bỏ
Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy file ra ngoài thiết bị cá nhân)	USB chứa mã độc hoặc thiết bị cá nhân không được bảo vệ đầy đủ có thể làm lây lan mã độc vào hệ thống nội bộ của công ty
Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)	Nếu nhân viên có quyền truy cập nhiều hơn mức cần thiết, họ có thể vô tình hoặc cố ý gây thiệt hại cho hệ thống
Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	Lỗi phần cứng hoặc phần mềm có thể gây mất mát dữ liệu vĩnh viễn, làm gián đoạn hoạt động và tăng nguy cơ thất thoát tài sản số.
Attacker	Tấn công thông qua email giả mạo (Spear Phishing)	Email giả mạo có thể lừa người nhận cung cấp thông tin đăng nhập hoặc tải xuống mã độc
Attacker	Khai thác lỗ hổng phần mềm chưa vá	Khai thác lỗ hổng trong phần mềm chưa được cập nhật hoặc vá lỗi để chiếm quyền điều khiển hệ thống
Attacker	Sniffing	Kẻ tấn công chặn bắt thông tin không được mã hóa qua mạng
Attacker	Tấn công DDoS	Tấn công từ chối dịch vụ phân tán (DDoS) làm gián đoạn hệ thống
Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp	Malware có thể làm hỏng dữ liệu hoặc lộ thông tin nhạy cảm
Attacker	Phá hủy thiết bị	Kẻ tấn công phá hủy thiết bị phần cứng hoặc gây lỗi logic
Attacker	Khai thác thông tin thông qua Social Engineering	Kẻ tấn công lừa nhân viên cung cấp thông tin hoặc quyền truy cập
Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)	Kẻ tấn công có thể chèn mã độc vào ứng dụng web, gây lộ dữ liệu hoặc chiếm quyền điều khiển phiên người dùng
Attacker	Tấn công Brute Force để phá mật khẩu	Kẻ tấn công thử hàng loạt mật khẩu để truy cập vào hệ thống
Attacker	Tấn công Cơ sở dữ liệu	Kẻ tấn công khai thác lỗ hổng SQL để truy cập vào hệ thống

$$C_y = C_y^{\alpha}(\alpha - \alpha)$$

03. Risk Score (mô hình mới)

1	Threat		Risk mitigate
2	Agent	Action	
3	Employee	Lộ thông tin cấu hình server	Thiết lập quyền truy cập nghiêm ngặt và mã hóa các file cấu hình quan trọng.
4	Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	Thực thi chính sách mật khẩu mạnh và kích hoạt xác thực hai yếu tố (2FA), passwordless, ...
5	Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân	Mã hóa dữ liệu và cung cấp các phương thức an toàn để truyền tải thông tin nhạy cảm.
6	Employee	Sử dụng phần mềm không rõ nguồn gốc	Thực thi chính sách cài đặt phần mềm và chỉ cho phép sử dụng phần mềm đã được kiểm tra an toàn.
7	Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	Áp dụng chính sách sử dụng phần mềm nghiêm ngặt, cài đặt các công cụ bảo vệ điểm cuối (AVE, FW + AV filter, ...)
8	Employee	Bị khai thác thông tin thông qua phương thức Social Engineering	Đào tạo về nhận thức bảo mật và quản lý quyền truy cập của người dùng.
9	Employee	Không khóa máy tính khi rời khỏi vị trí làm việc	Cài đặt tự động khóa màn hình sau một thời gian không hoạt động và có chính sách, quy trình đào tạo nhân viên.
10	Employee	Làm lộ bản ghi nhật ký (log)	Bảo mật nhật ký bằng cách mã hóa và lưu trữ chúng trong một hệ thống riêng biệt, chỉ cấp quyền truy cập hạn chế cho nhân viên có nhiệm vụ giám sát.
11	Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy)	Thiết lập chính sách rõ ràng về sử dụng thiết bị di động, chỉ cho phép các thiết bị đã được mã hóa và cài đặt phần mềm bảo mật, quét virus tự động khi cắm vào hệ thống.
12	Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)	Áp dụng nguyên tắc "quyền truy cập tối thiểu" cho mỗi nhân viên và kiểm tra định kỳ để điều chỉnh quyền truy cập nếu cần.
13	Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	Thiết lập các giải pháp khôi phục dự phòng bằng cách lưu dữ liệu trên các đám mây hoặc hệ thống sao lưu ngoại vi và xây dựng chính sách bảo trì định kỳ.
14	Attacker	Tấn công thông qua email giả mạo (Spear Phishing)	Sử dụng các giải pháp bảo mật email và đào tạo nhân viên về cách phát hiện phishing.
15	Attacker	Khai thác lỗ hổng phần mềm chưa vá	Liên tục kiểm tra và cập nhật các bản vá và bảo mật.
16	Attacker	Sniffing	Mã hóa dữ liệu khi truyền và bảo mật kết nối mạng.
17	Attacker	Tấn công DDoS	Sử dụng tường lửa ứng dụng web (WAF) và các giải pháp chống DDoS.
18	Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp	Cài đặt phần mềm chống virus và tường lửa mạng.
19	Attacker	Phá hủy thiết bị	Theo dõi thiết bị vật lý và có kế hoạch khôi phục từ sao lưu.
20	Attacker	Khai thác thông tin thông qua Social Engineering	Đào tạo nhận thức bảo mật cho nhân viên và cập nhật thường xuyên chính sách bảo mật.
21			
22	Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)	Kiểm tra và xử lý các đầu vào của người dùng để ngăn chặn XSS.
23			
24	Attacker	Tấn công Brute Force để phá mật khẩu	Giới hạn số lần thử đăng nhập và kích hoạt CAPTCHA hoặc 2FA.
25	Attacker	Tấn công Cơ sở dữ liệu	Thiết lập cơ chế kiểm tra đầu vào.

$$C_y = C_y^{\alpha} (\alpha - \alpha)$$

03. Risk Score (mô hình mới)

44	Threat		STRIDE category		Impact Score			Likelihood			Risk Score
45	Agent	Action			C	I	A	E	F	S	
46	Employee	Lộ thông tin cấu hình server	I	endpoint	1	1	1	1	1	0.2	0.2
47	Employee	Sử dụng mật khẩu yếu hoặc trùng lặp	S, I	endpoint	0	1	1	0	0	0.2	0
48	Employee	Lộ thông tin quan trọng qua thiết bị lưu trữ cá nhân	T	endpoint	0	2	0	0	2	0.2	0.4
49	Employee	Sử dụng phần mềm không rõ nguồn gốc	I, T	network	0	0	0	1	1	0.2	0
50	Employee	Tải xuống phần mềm chứa virus, malware, gây lây lan cho hệ thống	T, I	endpoint	0	1	0	1	1	0.2	0.2
51	Employee	Bị khai thác thông tin thông qua phương thức Social Engineering	E	network	2	1	0	1	3	0.2	0.8
52	Employee	Không khóa máy tính khi rời khỏi vị trí làm việc	S, I	endpoint	0	0	1	1	2	0.2	0.3
53	Employee	Làm lộ bản ghi nhật ký (log)	I	endpoint	1	1	1	1	1	0.2	0.2
54	Employee	Sử dụng USB hoặc thiết bị di động cá nhân không kiểm soát (copy)	I, D	endpoint	1	0	1	2	1	0.2	0.3
55	Employee	Không tuân thủ quy tắc về quyền truy cập tối thiểu (Least Privilege)	E	other	2	2	2	3	1	0.2	0.8
56	Employee	Sử dụng hệ thống không có backup, gây mất dữ liệu khi gặp sự cố	D	endpoint	1	1	2	2	1	0.2	0.6
57	Attacker	Tấn công thông qua email giả mạo (Spear Phishing)		email	1	1	0	2	2	0.2	0.4
58	Attacker	Khai thác lỗ hổng phần mềm chưa vá	T, I, E	endpoint	0	0	0	0	1	0.2	0
59	Attacker	Sniffing	I	network	2	2	2	2	3	0.2	1
60	Attacker	Tấn công DDoS	D	network	1	1	2	1	3	0.2	0.8
61	Attacker	Sử dụng Malware để thực hiện các hành động bất hợp pháp	T, I	endpoint	1	2	1	2	2	0.2	0.8
62	Attacker	Phá hủy thiết bị	T, D	endpoint	3	3	1	2	2	0.2	1.2
63	Attacker	Khai thác thông tin thông qua Social Engineering	E, S	other	3	2	2	3	5	0.2	2.4
64				endpoint	3	2	2	3	3	0.2	1.8
65	Attacker	Khai thác lỗ hổng Cross-Site Scripting (XSS)	T, I	endpoint	2	3	3	2	4	0.2	1.8
66				endpoint	2	3	3	2	5	0.2	2.1
67	Attacker	Tấn công Brute Force để phá mật khẩu	S, E	endpoint	2	0	0	3	5	0.2	1.6
68	Attacker	Tấn công Cơ sở dữ liệu	I	endpoint	1	0	0	2	2	0.2	0.4

$$C_y = C_y^{\alpha}$$

Xin cảm ơn!



$$x+y=a^2b$$



$$P=P_0-(V-100)/k$$

$$E_n = \frac{kx^2}{2}$$

