CÁC CÔNG NGHỆ TRONG LĨNH VỰC AN TOÀN THÔNG TIN

STT	Tên công nghệ	Biểu tượng	Định nghĩa công nghệ
I.	**CÔNG NGHỆ AN TOÀN LỚP DỮ LIỆU**		
1.	Data Security Posture Management		Công nghệ quản lý tình trạng an toàn thông tin dữ liệu của tổ chức. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
2.	Data Security as a Service		Cung cấp dịch vụ an toàn thông tin dữ liệu dưới dạng đám mây, giúp tổ chức đảm bảo tính an toàn thông tin. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
3.	Data Security Platforms		Nền tảng cung cấp các giải pháp an toàn thông tin dữ liệu tổng thể. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
4.	Multicloud DAM		Giải pháp quản lý và bảo vệ an toàn thông tin dữ liệu đa đám mây. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
5.	Data Risk Assessment		Đánh giá rủi ro an toàn thông tin dữ liệu trong tổ chức và xác định biện pháp phòng ngừa. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Bình minh công nghệ
6.	FinDRA		Một hệ thống tự động hóa để phát hiện và đánh giá rủi ro an toàn thông tin dựa trên dữ liệu tài chính. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
7.	Confidential Computing		Mô hình tính toán an toàn thông tin, cho phép xử lý dữ liệu mà không cần tiết lộ thông tin. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
8.	Data Security Governance		Quản lý và giám sát tuân thủ chính sách an toàn thông tin dữ liệu trong tổ chức. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
9.	Homomorphic Encryption		Loại mã hóa cho phép tính toán trực tiếp trên dữ liệu đã mã hóa, đảm bảo tính an toàn thông tin. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ

10.	Differential Privacy		Kỹ thuật an toàn thông tin thông tin cá nhân trong các tập dữ liệu, bảo vệ sự riêng tư khi phân tích. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
11.	Zero-Knowledge Proofs		Phương pháp chứng minh một thông tin là đúng mà không cần tiết lộ thông tin gốc. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
12.	Blockchain for Data Security		Sử dụng công nghệ blockchain để cải thiện tính an toàn thông tin và truy xuất dữ liệu. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đỉnh điểm của sự thôi phồng kỳ vọng
13.	DevOps Test Data Management		Quản lý dữ liệu thử nghiệm trong môi trường DevOps để đảm bảo tính an toàn. - Thời gian: 2 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 1 - Mức độ kỳ vọng: Đỉnh điểm của sự thôi phồng kỳ vọng
14.	Synthetic Data		Tạo dữ liệu giả lập để bảo vệ dữ liệu thật và đảm bảo tính riêng tư. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đỉnh điểm của sự thôi phồng kỳ vọng
15.	Machine Identity Management		Quản lý và bảo vệ thông tin xác thực của các thực thể và ứng dụng trong mạng. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành:1 - Mức độ kỳ vọng: Đỉnh điểm của sự thôi phồng kỳ vọng
16.	Data Breach Response		Công nghệ ứng phó với việc xâm nhập dữ liệu, bao gồm cả quá trình phát hiện và ứng phó. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
17.	Data Discovery and Management		Công cụ và phương pháp để phát hiện, quản lý, và đảm bảo tính toàn vẹn của dữ liệu trong tổ chức. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
18.	Multicloud KMaaS		Quản lý an toàn thông tin và khóa mã trong môi trường đa đám mây. - Thời gian: 3- 5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
19.	Secure Multiparty Computation		Cho phép nhiều bên tính toán chung trên dữ liệu mà không cần tiết lộ thông tin riêng tư cho nhau. - Thời gian: 5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng

20.	CSP-Native DLP		Giải pháp an toàn thông tin dữ liệu dựa trên chính sách tích hợp sâu với nhà cung cấp dịch vụ đám mây. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
21.	Format-Preserving Encryption		Mã hóa dữ liệu sao cho định dạng và cấu trúc ban đầu của dữ liệu được bảo vệ. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
22.	Privacy by Design		Thiết kế sản phẩm và dịch vụ với sự quan tâm đến an toàn thông tin thông tin cá nhân từ giai đoạn đầu. - Thời gian: 5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
23.	Privacy Impact Assessments		Đánh giá tác động tiềm năng đến quyền riêng tư khi triển khai các dự án hoặc công nghệ mới. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
24.	Augmented Data Cataloging and MMS		Sử dụng trí tuệ nhân tạo để cải thiện việc phân loại, quản lý dữ liệu và quản lý metadata. - Thời gian:3- 5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
25.	TLS Decryption Platform		Giải pháp giám sát và phân tích giao thức TLS để phát hiện và ngăn chặn các mối đe dọa. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
26.	Data Classification		Phân loại dữ liệu dựa trên mức độ nhạy cảm để quản lý và an toàn thông tin hiệu quả hơn. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
27.	Privacy Management Tools		Công cụ quản lý quyền riêng tư để giúp tổ chức tuân thủ các quy định về bảo vệ dữ liệu cá nhân. - Thời gian: 5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
28.	Secure Instant Communications		Giải pháp an toàn thông tin cho việc truyền tải thông tin nhạy cảm qua các kênh trực tiếp. - Thời gian: 5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận

29.	Data Access Governance		Quản lý quyền truy cập dữ liệu để đảm bảo tính toàn vẹn và an toàn thông tin. - Thời gian: 2 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
30.	Cloud Data Protection Gateways		Cổng bảo vệ dữ liệu trong môi trường đám mây để đảm bảo an toàn thông tin. - Thời gian: 5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
31.	CASBs		Giải pháp an toàn thông tin cho việc sử dụng dịch vụ đám mây bằng cách kiểm soát truy cập và bảo vệ dữ liệu. - Thời gian: 2 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
32.	Enterprise Key Management		Quản lý và bảo vệ các khóa mật mã hóa trong tổ chức. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
II.	**CÔNG NGHỆ AN TOÀN LỚP ỨNG DỤNG**		
33.	Policy as Code		Viết và triển khai các chính sách an toàn thông tin dưới dạng mã để tự động hóa việc áp dụng chính sách. - Thời gian: 5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
34.	SaaS Security Posture Management		Quản lý và đánh giá tình trạng an toàn thông tin của các dịch vụ đám mây để đảm bảo tuân thủ chính sách an toàn thông tin. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
35.	SBOM		Danh sách thành phần của phần mềm cùng với nguồn gốc và các thông tin liên quan. - Thời gian: 10 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 1 - Mức độ kỳ vọng: Bình minh công nghệ
36.	Chaos Engineering		Áp dụng sự cố tình và kiểm tra sự Công nghệ được sử dụng rộng rãi, ổn định của hệ thống để tìm ra các lỗ hổng và vấn đề tiềm ẩn. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
37.	Securing Development Environments		Đảm bảo an toàn thông tin môi trường phát triển bằng cách áp dụng các biện pháp bảo vệ cho quá trình phát triển. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3

			▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
38.	DevOps Test Data Management		Quản lý và an toàn thông tin dữ liệu kiểm thử trong quá trình phát triển phần mềm. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Thấp ▪ Mức độ trưởng thành: 2 ▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
39.	Cloud-Native Application Protection Platforms		Giải pháp an toàn thông tin cho các ứng dụng cloud-native, bao gồm bảo vệ mức ứng dụng và quản lý rủi ro. ▪ Thời gian: 10 năm ▪ Mức độ ảnh hưởng: Cao ▪ Mức độ trưởng thành: 3 ▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
40.	API Security Testing		Kiểm tra an toàn thông tin các giao diện lập trình ứng dụng (API) để đảm bảo tính toàn vẹn và an toàn. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Trung bình ▪ Mức độ trưởng thành: 3 ▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
41.	Security Service Edge		Kết hợp mạng và an toàn thông tin ứng dụng để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Trung bình ▪ Mức độ trưởng thành: 3 ▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
42.	Web App Client-Side Protection		Bảo vệ các ứng dụng web khỏi các tấn công từ phía máy khách bằng cách kiểm soát và giám sát mã JS. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Thấp ▪ Mức độ trưởng thành: 2 ▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
43.	Product Analysis		Phân tích sản phẩm phần mềm để tìm ra các lỗ hổng và vấn đề an toàn thông tin, đảm bảo tính an toàn. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Thấp ▪ Mức độ trưởng thành: 2 ▪ Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
44.	Application Security Orchestration and Correlation		Tự động hóa việc triển khai chính sách và phát hiện các sự cố an toàn thông tin trong ứng dụng. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Cao ▪ Mức độ trưởng thành: 3 ▪ Mức độ kỳ vọng: Đáy của sự vỡ mộng
45.	API Threat Protection		Bảo vệ các API khỏi các mối đe dọa an toàn thông tin như tấn công DoS, SQL injection, XSS, v.v. ▪ Thời gian: 3-5 năm ▪ Mức độ ảnh hưởng: Cao ▪ Mức độ trưởng thành: 3 ▪ Mức độ kỳ vọng: Đáy của sự vỡ mộng

46.	ASRTM		Quản lý rủi ro an toàn thông tin cho ứng dụng bằng cách áp dụng chính sách an toàn thông tin cho dữ liệu và truy cập. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
47.	Application Monitoring and Protection		Theo dõi và bảo vệ các ứng dụng khỏi các mối đe dọa và tấn công an toàn thông tin bằng cách phát hiện sự cố. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
48.	CSSTPs		Bảo vệ các ứng dụng web khỏi các cuộc tấn công bằng cách giám sát và kiểm soát các hoạt động. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
49.	Serverless Function Security		Bảo vệ các hàm serverless khỏi các mối đe dọa và tấn công bằng cách áp dụng biện pháp an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
50.	Cloud WAAP		Bảo vệ ứng dụng web và API trên nền tảng đám mây khỏi các cuộc tấn công và mối đe dọa. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
51.	Privacy by Design		Thiết kế sản phẩm với tính riêng tư tích hợp từ đầu để đảm bảo tuân thủ các quy định về an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trugn bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
52.	Service Mesh		Mạng dịch vụ cung cấp tích hợp mạng và an toàn thông tin cho các ứng dụng chạy trên nền tảng đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
53.	Application Shielding		Bảo vệ ứng dụng bằng cách thêm lớp bảo vệ vào mã nguồn hoặc tại thời điểm thực thi. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
54.	Bot Management		Phát hiện và ngăn chặn các hoạt động độc hại từ các bot và các hoạt động tự động. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng

55.	Container and Kubernetes Security		Bảo vệ môi trường container và Kubernetes khỏi các mối đe dọa bằng cách áp dụng biện pháp an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
56.	Mobile Application Security Testing		Kiểm tra an toàn thông tin các ứng dụng di động để đảm bảo tính toàn vẹn và an toàn trước các mối đe dọa. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
57.	EAM		Quản lý tài sản doanh nghiệp (EAM) bao gồm việc an toàn thông tin và duy trì các tài sản IT của doanh nghiệp. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
58.	Enterprise App Stores		Nền tảng cung cấp và quản lý ứng dụng doanh nghiệp cho người dùng nội bộ của tổ chức. - Thời gian: 2 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
59.	Full Life Cycle API Management		Quản lý toàn bộ vòng đời của các giao diện lập trình ứng dụng (API) từ phát triển đến triển khai. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
60.	Software Composition Analysis		Phân tích thành phần phần mềm để xác định các thành phần có thể bị tổn thương và cần cập nhật. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
61.	Web Application Firewall Appliance		Thiết bị tường lửa ứng dụng web dùng để bảo vệ ứng dụng khỏi các cuộc tấn công mạng. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
62.	DevSecOps		Kết hợp an toàn thông tin vào quá trình phát triển và vận hành để đảm bảo tích hợp liên tục của an toàn thông tin. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
III.	**CÔNG NGHỆ AN TOÀN LỚP MẠNG**		

63.	CAASM		Quản lý và an toàn thông tin quy trình và tài sản của ứng dụng sử dụng các biện pháp tự động và an toàn. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
64.	Hybrid Mesh Firewall Platform		Nền tảng tường lửa mạng kết hợp giữa các mô hình tường lửa truyền thống và SD-WAN. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
65.	SaaS Security Posture Management		Quản lý và đánh giá tình trạng an toàn thông tin của các dịch vụ đám mây để đảm bảo tuân thủ chính sách. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
66.	Identity-First Security		Tiếp cận an toàn thông tin thông qua quản lý danh tính, đảm bảo quyền truy cập dựa trên danh tính người dùng. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
67.	CIEM		Quản lý toàn diện danh tính và quyền truy cập của người dùng đối với các tài sản và dịch vụ. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
68.	Cloud-Native Application Protection Platforms		Giải pháp an toàn thông tin cho các ứng dụng cloud-native, bao gồm bảo vệ mức ứng dụng và quản lý rủi ro. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
69.	Security Service Edge		Kết hợp mạng và an toàn thông tin ứng dụng để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
70.	Firewall as a Service		Cung cấp tường lửa dưới dạng dịch vụ để bảo vệ các ứng dụng và dữ liệu trong môi trường đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
71.	Cloud Firewalls		Tường lửa được triển khai trong môi trường đám mây để kiểm soát và bảo vệ lưu lượng mạng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng

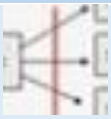
72.	Serverless Function Security		Bảo vệ các hàm serverless khỏi các mối đe dọa và tấn công bằng cách áp dụng biện pháp an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
73.	Cloud WAAP		Bảo vệ ứng dụng web và API trên nền tảng đám mây khỏi các cuộc tấn công và mối đe dọa. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
74.	SASE		Kết hợp mạng và an toàn thông tin để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây và xa hội. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
75.	Immutable Infrastructure		Triển khai hạ tầng và ứng dụng không thể thay đổi để ngăn chặn các thay đổi không được ủy quyền. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
76.	NDR		Phát hiện và phản ứng trên mạng (NDR) là quá trình phát hiện và ứng phó với các mối đe dọa mạng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
77.	ZTNA		Kiến trúc mạng Zero Trust (ZTNA) chỉ cho phép truy cập dựa trên danh tính và quyền truy cập. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
78.	NSPM		Quản lý hiệu suất mạng và an toàn thông tin (NSPM) cung cấp giám sát và quản lý các khía cạnh mạng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
79.	Container and Kubernetes Security		Bảo vệ môi trường container và Kubernetes khỏi các mối đe dọa bằng cách áp dụng biện pháp an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
80.	Microsegmentation		Chia nhỏ mạng thành các phân đoạn nhỏ hơn để kiểm soát chính xác việc truy cập và lưu lượng. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận

81.	CSPM		Quản lý an toàn thông tin và tuân thủ chính sách cho các dịch vụ đám mây bằng cách kiểm tra cấu hình. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
82.	DDoS Mitigation		Ngăn chặn hoặc giảm thiểu tác động của cuộc tấn công từ chối dịch vụ (DDoS) lên hạ tầng mạng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
83.	Cloud Workload Protection Platforms		Bảo vệ các tải công việc và ứng dụng đang chạy trên đám mây khỏi các mối đe dọa và rủi ro. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
84.	Hardware-Based Security		Sử dụng phần cứng để cung cấp lớp an toàn thông tin bổ sung cho hệ thống và ứng dụng. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
85.	CASBs		Các dịch vụ an toàn thông tin cơ sở dữ liệu đám mây (CASBs) giúp quản lý và bảo vệ dữ liệu trong đám mây. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
86.	Network Access Control		Kiểm soát truy cập mạng dựa trên chính sách để đảm bảo rằng chỉ người dùng hợp lệ mới có thể truy cập. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
87.	Secure Web Gateway		Cổng web an toàn kiểm soát và bảo vệ lưu lượng web của tổ chức khỏi các mối đe dọa mạng. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
88.	Network Firewall		Tường lửa mạng kiểm soát và theo dõi lưu lượng mạng giữa các phần mạng khác nhau. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
IV.	**LỚP AN TOÀN THIẾT BỊ ĐẦU CUỐI**		

89.	Exposure Management		Quản lý và giảm thiểu các nguy cơ an toàn thông tin liên quan đến việc công bố thông tin và dữ liệu. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Bình minh công nghệ
90.	VDI/DaaS Endpoint Security		Bảo vệ an toàn thông tin cho các thiết bị cuối trong môi trường VDI và DaaS. Điều này bao gồm việc áp dụng chính sách an toàn thông tin, phát hiện và ngăn chặn các mối đe dọa, và quản lý tích hợp cho các thiết bị này. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
91.	Unified Endpoint Security		Tích hợp các giải pháp an toàn thông tin đa dạng vào một nền tảng duy nhất để bảo vệ các thiết bị đầu cuối. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
92.	External Attack Surface Management		Quản lý và giảm thiểu các điểm tiếp xúc với bên ngoài có thể bị tấn công trong môi trường mạng. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
93.	ITDR		Phát hiện và phản ứng trước các mối đe dọa liên quan đến danh tính người dùng trong môi trường. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
94.	BYOPC Security		an toàn thông tin các thiết bị đầu cuối cá nhân được mang đến nơi làm việc (Bring Your Own PC). - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
95.	Security Service Edge		Kết hợp mạng và an toàn thông tin thiết bị đầu cuối để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
96.	Breach and Attack Simulation		Mô phỏng các cuộc tấn công và xâm nhập để đánh giá khả năng phản ứng và phòng thủ của hệ thống. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
97.	Business Email Compromise Protection		Bảo vệ chống lại các cuộc tấn công và lừa đảo liên quan đến email nhằm chiếm quyền truy cập. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng

98.	Device Endpoint Security for Frontline Workers		An toàn thông tin thiết bị đầu cuối cho người làm việc tại hiện trường, không cố định văn phòng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
99.	Content Disarm and Reconstruction		Gỡ bỏ các phần nguy hiểm khỏi tài liệu và nội dung để ngăn chặn các cuộc tấn công thông qua email. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
100.	SASE		Kết hợp mạng và an toàn thông tin thiết bị đầu cuối để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
101.	Remote Browser Isolation		Cách ly trình duyệt từ hạ tầng đám mây để ngăn chặn các mối đe dọa trực tiếp tới máy người dùng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
102.	Desktop as a Service		Cung cấp môi trường máy tính dưới dạng dịch vụ để truy cập từ xa thông qua internet. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
103.	Mobile Threat Defense		Bảo vệ thiết bị di động khỏi các mối đe dọa bằng cách phát hiện và ngăn chặn các cuộc tấn công. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
104.	ZTNA		Kiến trúc mạng Zero Trust (ZTNA) chỉ cho phép truy cập dựa trên danh tính và quyền truy cập. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
105.	Data Sanitization		Loại bỏ thông tin nhạy cảm từ dữ liệu để đảm bảo rằng nó không thể Công nghệ dần được chấp nhận được. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
106.	Endpoint Detection and Response		Phát hiện và phản ứng trước các mối đe dọa đối với các thiết bị đầu cuối trong hệ thống. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận

107.	UEM		Quản lý và an toàn thông tin các thiết bị đầu cuối trong toàn bộ mạng nội bộ từ một nền tảng duy nhất. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
108.	CASBs		Các dịch vụ an toàn thông tin cơ sở dữ liệu đám mây (CASBs) giúp quản lý và bảo vệ dữ liệu trong đám mây. - Thời gian: 2 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được chấp nhận
109.	Endpoint Protection Platform		Cung cấp bảo vệ toàn diện cho các thiết bị đầu cuối khỏi các mối đe dọa và phần mềm độc hại. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
110.	Secure Web Gateways		Cổng web an toàn kiểm soát và bảo vệ lưu lượng web của tổ chức khỏi các mối đe dọa mạng. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
V.	**LỚP AN TOÀN DỊCH VỤ**		
111.	CIEM		Quản lý sự nhạy cảm về thông tin và quyền truy cập đối với các dịch vụ và ứng dụng đám mây. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
112.	Confidential Computing		Một phương pháp mã hóa dữ liệu trong các môi trường đám mây để an toàn thông tin ngay cả khi đang xử lý. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
113.	SaaS Security Posture Management		Quản lý và đảm bảo tính an toàn của các ứng dụng và dịch vụ đám mây được triển khai. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
114.	Chaos Engineering		Áp dụng các cuộc tấn công kiểm tra hệ thống để xác định sự Công nghệ được sử dụng rộng rãi, ổn định và độ tin cậy của nó. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành:2 - Mức độ kỳ vọng: Bình minh công nghệ

115.	PTaaS		Dịch vụ kiểm tra thâm nhập được cung cấp như một dịch vụ để kiểm tra độ an toàn thông tin của hệ thống. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành:2 - Mức độ kỳ vọng: Bình minh công nghệ
116.	ITDR		Phát hiện và phản ứng trước các mối đe dọa liên quan đến danh tính người dùng trong môi trường. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
117.	CPS Security		an toàn thông tin các dịch vụ đám mây thông qua các biện pháp an toàn thông tin kiểu dáng vật lý và logic. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
118.	External Attack Surface Management		Quản lý và giảm thiểu các điểm tiếp xúc với bên ngoài có thể bị tấn công trong môi trường mạng. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
119.	CAASM		Quản lý và bảo vệ các dịch vụ đám mây thông qua việc kiểm soát và phân quyền truy cập. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
120.	Automated Penetration Test and Red Teaming Tool		Công cụ tự động thử nghiệm xâm nhập và tấn công mô phỏng để đánh giá an toàn thông tin của hệ thống. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
121.	Exposure Mangement		Quản lý và giảm thiểu các nguy cơ an toàn thông tin liên quan đến việc công bố thông tin và dữ liệu. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Bình minh công nghệ
122.	Cloud-native Application Protection Platforms		Cung cấp bảo vệ toàn diện cho các ứng dụng đám mây thông qua việc tích hợp an toàn thông tin vào mã nguồn. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
123.	Security Service Edge		Kết hợp mạng và an toàn thông tin thiết bị đầu cuối để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng

124.	Saas Management Platforms		Cung cấp quản lý toàn diện và kiểm soát các ứng dụng đám mây và dịch vụ sử dụng các gói giải pháp. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
125.	SASE		Kết hợp mạng và an toàn thông tin thiết bị đầu cuối để cung cấp bảo vệ toàn diện cho các dịch vụ đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
126.	Security Rating Services		Cung cấp xếp hạng và đánh giá mức độ an toàn của các dịch vụ và ứng dụng sử dụng trong môi trường. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
127.	CSP-Native DLP		Giải pháp DLP tích hợp trực tiếp vào nhà cung cấp dịch vụ đám mây để kiểm soát dữ liệu. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
128.	Breach and Attack Simulation		Mô phỏng các cuộc tấn công và xâm nhập để đánh giá khả năng phản ứng và phòng thủ của hệ thống. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trugn bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
129.	XDR		Phát hiện và phản ứng trước các mối đe dọa chéo nhiều lớp trong môi trường mạng và đám mây. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
130.	Digital Risk Protection Services		Cung cấp giám sát và phản ứng đối với các mối đe dọa về dữ liệu và danh tính trực tuyến. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
131.	Digital Forensics and Incident Response		Tìm hiểu và phản ứng sau các sự cố an toàn thông tin để khắc phục hậu quả và củng cố an toàn. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
132.	Cloud Data Backup		Sao lưu và bảo vệ dữ liệu trong đám mây để đảm bảo khả năng Công nghệ dần được chấp nhận sau sự cố. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đáy của sự vỡ mộng

133.	Multicloud KMaas		Quản lý và bảo vệ khóa trong đám mây để đảm bảo tính toàn vẹn và an toàn của dữ liệu. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
134.	Serverless Function Security		Bảo vệ các hàm chạy không máy chủ trên đám mây khỏi các mối đe dọa và lỗ hổng an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
135.	Immutable Infrastructure		Triển khai hạ tầng và cơ sở hạ tầng không thể thay đổi để an toàn thông tin và Công nghệ được sử dụng rộng rãi, ổn định hệ thống. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
136.	SaaS-Delivered IAM		Cung cấp giải pháp quản lý danh tính và truy cập dưới dạng dịch vụ sử dụng đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
137.	OT Security		Bảo vệ các hệ thống và thiết bị quản lý công nghiệp (OT) khỏi các mối đe dọa mạng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
138.	SOAR		Tự động hóa quy trình phản ứng sau sự cố an toàn thông tin để tăng cường hiệu suất và hiệu quả. - Thời gian: 10 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
139.	MDR Services		Dịch vụ phát hiện, phản ứng và phục hồi dựa trên máy móc cho các sự cố an toàn thông tin. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
140.	Vulnerability Prioritization Technology		Xác định và ưu tiên các lỗ hổng an toàn thông tin dựa trên tiêu chí quan trọng của tổ chức. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Đáy của sự vỡ mộng
141.	Data Discovery and Management		Phát hiện và quản lý dữ liệu trong đám mây để tuân thủ quy định về quản lý dữ liệu. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Đáy của sự vỡ mộng

142.	Cloud Data Protection Gateways		Bảo vệ dữ liệu trong đám mây bằng cách kiểm soát và mã hóa dữ liệu khi nó đi qua cổng. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định
143.	ZTNA		Cung cấp truy cập an toàn dựa trên danh tính và tình trạng thiết bị từ bất kỳ vị trí nào. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định
144.	Container and Kurnernetes Security		Bảo vệ các ứng dụng và dịch vụ đang chạy trên nền tảng container và Kubernetes. - Thời gian: 5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định
145.	CSPM		Quản lý và an toàn thông tin cài đặt và cấu hình đám mây để đảm bảo tuân thủ các tiêu chuẩn an toàn. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định
146.	Enterprise Key Management		Quản lý và an toàn thông tin khóa mã hóa dữ liệu trong môi trường đám mây và hệ thống nội bộ. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định
147.	Identity-Based Segmentation		Phân đoạn mạng dựa trên danh tính để kiểm soát truy cập mạng từ các người dùng cụ thể. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
148.	Cloud Workload Protection Platforms		Bảo vệ các ứng dụng và dịch vụ đám mây bằng cách giám sát và bảo vệ khỏi các mối đe dọa. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định
149.	Hardware-Based Security		Sử dụng phần cứng để bảo vệ an toàn thông tin, đặc biệt là trong môi trường đám mây. - Thời gian: 3-5 năm - Mức độ ảnh hưởng: Trung bình - Mức độ trưởng thành: 3 - Mức độ kỳ vọng: Công nghệ dần được ổn định

150.	Multicloud Managed Services		Quản lý và duy trì các dịch vụ đám mây từ nhiều nhà cung cấp để đảm bảo tính Công nghệ được sử dụng rộng rãi, ổn định. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
151.	Private Cloud Computing		Xây dựng và duy trì các hạ tầng đám mây riêng tư để kiểm soát hoàn toàn quyền kiểm soát. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
152.	CASBs		Cung cấp kiểm soát và an toàn thông tin cho dữ liệu và hoạt động trong đám mây của các tổ chức. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
153.	Cloud Management Platforms		Cung cấp quản lý tổng thể và kiểm soát cho các dịch vụ và tài nguyên đám mây. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
154.	SIEM		Cung cấp giải pháp quản lý sự kiện và thông báo an toàn thông tin để giám sát và phản ứng đối với sự cố. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
155.	Endpoint Detection and Response		Phát hiện và phản ứng trước các mối đe dọa đối với các thiết bị đầu cuối trong môi trường. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ dần được ổn định
156.	Threat Intelligence Products and Services		Cung cấp thông tin và dịch vụ về thông tin mối đe dọa để cung cấp thông tin cho tổ chức. - Thời gian: 10 năm - Mức độ ảnh hưởng: Thấp - Mức độ trưởng thành: 2 - Mức độ kỳ vọng: Công nghệ dần được ổn định
157.	EDRM		Quản lý và an toàn thông tin dữ liệu hợp pháp trong hệ thống để tuân thủ các quy định pháp luật. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4 - Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
158.	Cloud Application Discovery		Phát hiện và theo dõi các ứng dụng đám mây được sử dụng trong tổ chức để duy trì tính an toàn. - Thời gian: 2 năm - Mức độ ảnh hưởng: Cao - Mức độ trưởng thành: 4

			▪ Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
159.	Vulnerability Assessment		Đánh giá và ưu tiên các lỗ hổng an toàn thông tin dựa trên mức độ nghiêm trọng và tiềm năng tổn thất. ▪ Thời gian: 2 năm ▪ Mức độ ảnh hưởng: Cao ▪ Mức độ trưởng thành: 4 ▪ Mức độ kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định