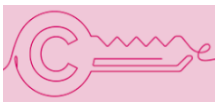
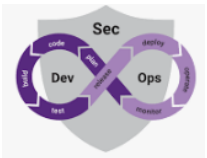
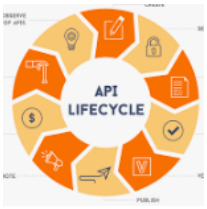
CÁC CÔNG NGHỆ TRONG LĨNH VỰC AN TOÀN THÔNG TIN

Công nghệ	Biểu tượng	Thông tin
Secure Web Gateways (SWG)		**SWG** là các hệ thống an toàn thông tin mạng giúp kiểm soát và bảo vệ truy cập vào các trang web và ứng dụng từ mạng nội bộ của tổ chức, nhằm ngăn chặn mối đe dọa và phòng ngừa tấn công trực tuyến. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Bình minh công nghệ
Endpoint Protection Platforms		**Endpoint Protection Platforms** là một tập hợp các công cụ bảo mật được triển khai tại các thiết bị đầu cuối như máy tính cá nhân và thiết bị di động. Nhiệm vụ của chúng là ngăn chặn, phát hiện và xử lý các mối đe dọa đối với các thiết bị này. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
Cloud Access Security Brokers (CASBs):		**Cloud Access Security Brokers (CASBs)** là các nền tảng bảo mật được triển khai giữa người dùng và các dịch vụ đám mây để kiểm soát và bảo vệ dữ liệu khi được chia sẻ và truy cập từ các ứng dụng đám mây. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đáy của sự vỡ mộng
UEM (Unified Endpoint Management		**UEM** là một hệ thống quản lý đa nhiệm được sử dụng để quản lý các thiết bị đầu cuối, bao gồm cả máy tính cá nhân, điện thoại di động và thiết bị IoT, thông qua một giao diện duy nhất. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
Endpoint Detection and Response (EDR)		**Endpoint Detection and Response (EDR)** là một công nghệ an toàn thông tin được sử dụng để phát hiện, phản ứng và phân tích các mối đe dọa trên các thiết bị đầu cuối. Nó giúp tổ chức xác định các hoạt động đáng ngờ và ngăn chặn các cuộc tấn công trên các thiết bị này. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đáy của sự vỡ mộng
Network Firewalls		**Firewalls** là các thiết bị hoặc phần mềm được triển khai để kiểm soát và giám sát luồng thông tin vào và ra khỏi mạng. Chúng giúp ngăn chặn các mối đe dọa từ bên ngoài và duy trì an toàn cho mạng nội bộ. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Hardware-Based Security		**Hardware-Based Security** là các biện pháp bảo mật được tích hợp trực tiếp vào phần cứng của các thiết bị. Chúng giúp bảo vệ thông tin quan trọng và ngăn chặn các tấn công liên quan đến phần cứng. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng .

Cloud Workload Protection Platforms		**Cloud Workload Protection Platforms** là các giải pháp bảo mật dành riêng cho việc bảo vệ các khối công việc (workload) đang chạy trên môi trường đám mây. Chúng cung cấp các biện pháp bảo mật như phát hiện xâm nhập, quản lý danh tính và kiểm soát truy cập để đảm bảo tính bảo mật cho các ứng dụng và dịch vụ đang hoạt động trên nền đám mây. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
Cloud Application Discovery		**Cloud Application Discovery** là một công nghệ cho phép tổ chức xác định và theo dõi các ứng dụng đang hoạt động trên môi trường đám mây. Chúng giúp tổ chức có cái nhìn chi tiết về việc sử dụng các ứng dụng đám mây và đảm bảo tính bảo mật cho các hoạt động này.. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
EDRM (Enterprise Digital Rights Management)		**EDRM** là một công nghệ cho phép tổ chức kiểm soát và quản lý quyền truy cập và sử dụng các tài liệu và thông tin trong môi trường kỹ thuật số. EDRM đảm bảo rằng dữ liệu quan trọng được bảo vệ, không bị rò rỉ hoặc truy cập trái phép. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
DevSecOps (Development, Security, Operations)		**DevSecOps** là một phương pháp tiếp cận tích hợp an toàn thông tin vào quy trình phát triển và vận hành ứng dụng. Công nghệ này tập trung vào việc đảm bảo tích hợp bảo mật từ giai đoạn phát triển đến triển khai và vận hành. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ được sử dụng rộng rãi, ổn định
Web Application Firewall Appliance		**Web Application Firewall (WAF) Appliance** là một thiết bị bảo mật dành riêng cho việc bảo vệ các ứng dụng web khỏi các cuộc tấn công và lỗ hổng bảo mật. Thiết bị này hoạt động như một bức tường bảo vệ giữa ứng dụng và internet, kiểm soát và giám sát lưu lượng truy cập. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Sofware Composition Analysis (SCA)		**Sofware Composition Analysis (SCA)** là một phương pháp kiểm tra và phân tích các thành phần phần mềm và thư viện bên ngoài được sử dụng trong ứng dụng. Mục tiêu của SCA là xác định và giảm thiểu rủi ro bảo mật do việc sử dụng các thành phần có lỗ hổng bảo mật. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận

Full Life Cycle API Management		**Full Life Cycle API Management** là một phương pháp quản lý toàn bộ chu kỳ cuộc sống của các giao diện lập trình ứng dụng (API), bao gồm thiết kế, triển khai, vận hành, và theo dõi. Công nghệ này giúp tổ chức quản lý và kiểm soát việc sử dụng các API trong môi trường phát triển và vận hành. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Enterprise Key Management (EKM)		**Enterprise Key Management (EKM)** là một phương pháp quản lý và bảo vệ các khóa mã hóa trong một tổ chức. EKM giúp tổ chức quản lý việc tạo, lưu trữ, quản lý và hủy các khóa mã hóa một cách an toàn và hiệu quả. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Cloud Data Protection Gateways		**Cloud Data Protection Gateways (CDPG)** là các thiết bị hoặc dịch vụ trung gian được triển khai trong môi trường đám mây để bảo vệ dữ liệu trong quá trình truyền tải và lưu trữ. CDPG cung cấp các chức năng bảo mật như mã hóa, kiểm soát truy cập và theo dõi dữ liệu trong môi trường đám mây. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Vulnerability Assessment		**Vulnerability Assessment** là quá trình xác định và đánh giá các lỗ hổng bảo mật trong hệ thống, ứng dụng hoặc mạng. Quá trình này nhằm mục đích phát hiện các điểm yếu trong hệ thống để từ đó triển khai các biện pháp bảo mật hợp lý. ■ Thời gian: 2 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Data Sanitization		**Data Sanitization** là quá trình loại bỏ hoặc xóa các dữ liệu nhạy cảm hoặc thông tin cá nhân từ thiết bị lưu trữ mà không gây tổn hại đến tính toàn vẹn của thiết bị. Quá trình này đảm bảo rằng dữ liệu không thể khôi phục lại sau khi đã được xóa. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: đoạn Bình minh công nghệ
ZTNA (Zero Trust Network Access)		**ZTNA** là một phương pháp an toàn thông tin mạng dựa trên triết lý "Zero Trust", trong đó mọi kết nối mạng được xem xét một cách cẩn trọng, ngay cả từ bên trong mạng nội bộ. ZTNA thực hiện việc cấp quyền truy cập dựa trên danh tính, trạng thái thiết bị, vị trí và ngữ cảnh. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận

Secure Service Edge (SASE)		**Secure Service Edge (SASE)** là một khái niệm an toàn thông tin mạng kết hợp với việc cung cấp dịch vụ mạng qua mô hình đám mây. SASE kết hợp tính bảo mật và dịch vụ mạng, cho phép tổ chức cung cấp truy cập an toàn và hiệu quả từ bất kỳ đâu. ■ Thời gian: 3- 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
BYOPC Security (Bring Your Own PC Security)		**BYOPC Security** là việc đảm bảo tính bảo mật cho các thiết bị máy tính cá nhân mà nhân viên mang đến làm việc trong môi trường công việc. Điều này đòi hỏi các biện pháp bảo mật như mã hóa dữ liệu, cài đặt phần mềm bảo mật và kiểm soát truy cập. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đáy của sự vỡ mộng

DDoS Mitigation (Distributed Denial of Service Mitigation)		**DDoS Mitigation** là việc triển khai các biện pháp và giải pháp để ngăn chặn tấn công từ chối dịch vụ (DDoS). DDoS là loại tấn công mạng nhằm làm cho một dịch vụ mạng trở nên không hoạt động bằng cách làm cho máy chủ quá tải. ■ Thời gian: 3- 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
CSPM (Cloud Security Posture Management)		**CSPM** là việc quản lý và đảm bảo tính bảo mật cho cấu hình của các tài nguyên đám mây. Điều này bao gồm việc kiểm tra và cải thiện cấu hình của các tài nguyên đám mây để đảm bảo tuân thủ các tiêu chuẩn bảo mật. ■ Thời gian: 3- 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Security Service Edge (SSE)		**Security Service Edge (SSE)** là một kiến trúc an toàn thông tin mạng tiên tiến, tập trung vào việc cung cấp các dịch vụ an toàn thông tin trực tiếp tại điểm kết nối của người dùng với ứng dụng và dịch vụ trên mạng. ■ Thời gian: 3- 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Firewall as a Service (FWaaS)		**Firewall** as a Service (FWaaS) là một mô hình cung cấp dịch vụ tường lửa qua mạng, cho phép người dùng thuê và quản lý tường lửa thông qua môi trường đám mây hoặc dịch vụ. ■ Thời gian: 3- 5 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng

Hardware-Based Security		**Hardware-Based Security** là một phương pháp an toàn thông tin và dữ liệu bằng cách sử dụng phần cứng thay vì phần mềm. Điều này có thể bao gồm việc sử dụng chip bảo mật, mô-đun bảo mật phần cứng, hoặc các giải pháp khác tích hợp trực tiếp vào phần cứng của hệ thống. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
Cloud Workload Protection Platforms (CWPP)		**Cloud Workload Protection Platforms (CWPP)** là các giải pháp an toàn thông tin được thiết kế đặc biệt để bảo vệ các ứng dụng và dịch vụ đang chạy trên môi trường đám mây, bao gồm việc kiểm soát quyền truy cập, phát hiện và ngăn chặn các mối đe dọa, và bảo vệ tính toàn vẹn của dữ liệu. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận

Mobile Application Security Testing		**Mobile Application Security Testing** là quá trình kiểm tra và đánh giá tính bảo mật của ứng dụng di động, nhằm xác định và khắc phục các lỗ hổng bảo mật có thể bị khai thác. ■ Thời gian: 3- 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
Container and Kubernetes Security		**Container and Kubernetes Security** là việc bảo vệ tính bảo mật cho các môi trường chứa (container) và quản lý (Kubernetes) để đảm bảo rằng các ứng dụng chạy trong các môi trường này được bảo vệ khỏi các mối đe dọa. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
API Security Testing		**API Security Testing là quá trình kiểm tra và đánh giá tính bảo mật của các giao diện lập trình ứng dụng (API) để đảm bảo rằng các API này không có lỗ hổng bảo mật có thể bị khai thác.** ■ Thời gian: trên 2- 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
Data Access Governmance		**Data Access Governance** là việc quản lý và kiểm soát quyền truy cập đối với dữ liệu nhằm đảm bảo rằng chỉ những người có quyền truy cập thích hợp mới có thể truy cập vào dữ liệu đó. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận

Secure Instant Communications		**Secure Instant Communications** là việc cung cấp các phương tiện truyền thông tức thì an toàn như tin nhắn và cuộc gọi, đảm bảo tính bảo mật và mã hóa trong quá trình truyền tải. ■ Thời gian: 3 -5 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Đáy của sự vỡ mộng
Privacy Management Tools		**Privacy Management Tools** là các công cụ hỗ trợ quản lý và thực hiện các chính sách về quyền riêng tư và bảo vệ dữ liệu cá nhân, đảm bảo rằng các hoạt động xử lý dữ liệu tuân thủ các quy định về quyền riêng tư. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Data Classification.		**Data Classification** là quá trình phân loại dữ liệu theo mức độ bảo mật và quyền riêng tư. Việc phân loại dữ liệu giúp tổ chức xác định và xử lý dữ liệu theo các chính sách bảo mật và quyền riêng tư tương ứng. ■ Thời gian: 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Đỉnh điểm của sự thổi phồng kỳ vọng
SIEM		**SIEM** là một hệ thống tự động tập hợp và phân tích dữ liệu từ nhiều nguồn để giám sát và phát hiện các sự kiện bất thường và xâm nhập trong môi trường an toàn thông tin. ■ Thời gian: 5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Digital Risk Protection Services		**Digital Risk Protection Services** là các dịch vụ giúp tổ chức theo dõi và bảo vệ khỏi các rủi ro liên quan đến an toàn thông tin thông tin trên môi trường kỹ thuật số, bao gồm việc giám sát trên internet sâu, mạng xã hội và các nguồn thông tin trực tuyến khác. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Breach and Attack Simulation		**Breach and Attack Simulation** là quá trình mô phỏng các cuộc tấn công và việc xâm nhập vào hệ thống để kiểm tra khả năng phát hiện và ứng phó của hệ thống bảo mật. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: : Đỉnh điểm của sự thổi phồng kỳ vọng

Digital forensics And Incident Response		**Digital Forensics and Incident Response** là quá trình thu thập, phân tích và giải quyết các sự cố bảo mật và tấn công mạng trong môi trường số hóa. Quá trình này bao gồm khảo sát, phân tích bằng chứng số hóa và thực hiện các biện pháp ứng phó. ■ Thời gian: 3-5 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 4 ■ Sự kỳ vọng: : Công nghệ dần được chấp nhận
XDR		**XDR (Extended Detection and Response)** là một khái niệm mới trong lĩnh vực an toàn thông tin, tập hợp các công nghệ phát hiện và phản ứng mở rộng để giám sát và ứng phó với các cuộc tấn công mạng, bao gồm cả sự cố trên các thiết bị mạng, máy tính và thiết bị di động. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: : Công nghệ dần được chấp nhận
Business Email Compromise Protection		**Business Email Compromise (BEC) Protection** là các công nghệ và biện pháp được triển khai để phát hiện và ngăn chặn các cuộc tấn công thông qua việc xâm nhập vào hòm thư điện tử của tổ chức và lừa đảo nhân viên để thực hiện các giao dịch bất hợp pháp. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: : Đỉnh điểm của sự thổi phồng kỳ vọng
Cloud-Native Application Protection Platforms		**Cloud-Native Application Protection Platforms** là các giải pháp bảo mật được thiết kế đặc biệt để bảo vệ ứng dụng được triển khai trên môi trường điện toán đám mây. Chúng cung cấp các tính năng bảo mật như phát hiện xâm nhập, bảo vệ dữ liệu, quản lý danh tính và kiểm tra an toàn cho các ứng dụng cloud-native.. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: : Đỉnh điểm của sự thổi phồng kỳ vọng
CIEM		**CIEM (Cloud Infrastructure Entitlement Management)** là một loại giải pháp quản lý và bảo vệ quyền truy cập vào các tài nguyên điện toán đám mây. Nó giúp tổ chức kiểm soát và giám sát quyền truy cập của người dùng và ứng dụng vào các tài nguyên trong môi trường đám mây. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: : Công nghệ dần được chấp nhận
CSP-Native DLP		**CSP-Native DLP** là một dạng của giải pháp DLP được tích hợp trực tiếp vào các dịch vụ đám mây như nền tảng cung cấp của Gartner và nền tảng điện toán đám mây. Nó giúp phát hiện và ngăn chặn việc rò rỉ dữ liệu trong các tài khoản đám mây bằng cách theo dõi và kiểm soát quyền truy cập và hoạt động của người dùng. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: : Đỉnh điểm của sự thổi phồng kỳ vọng

EAM		**EAM** là các giải pháp quản lý tài sản cuối điểm, bao gồm các thiết bị đầu cuối như máy tính, điện thoại di động và máy tính bảng. EAM giúp tổ chức theo dõi, quản lý và bảo mật các thiết bị đầu cuối trong môi trường làm việc.. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: : Công nghệ dần được chấp nhận
Blockchain for Data Security		**Blockchain for Data Security** là việc sử dụng công nghệ blockchain để bảo vệ dữ liệu bằng cách tạo ra các giao dịch dữ liệu có tính bất biến và xác thực. Các giao dịch này được ghi vào chuỗi khối và không thể thay đổi hoặc xóa bỏ. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 2 ■ Sự kỳ vọng: : Đỉnh điểm của sự thổi phồng kỳ vọng
Zero-Knowledge Proofs		**Zero-Knowledge Proofs** là một phương pháp trong mật mã học cho phép một bên chứng minh rằng họ có thông tin đúng mà không cần tiết lộ thông tin này cho bên thứ ba. Điều này giúp bảo vệ tính riêng tư trong các giao dịch và chứng minh. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Cao ■ Độ trưởng thành: 3 ■ Sự kỳ vọng: Công nghệ dần được chấp nhận
Threat Intelligence Products and Services.		**Threat Intelligence Products and Services (TIPS)** là các giải pháp và dịch vụ cung cấp thông tin chi tiết và phân tích về các mối đe dọa an ninh mạng và tấn công tiềm năng. Chúng thu thập, xử lý và phân tích dữ liệu từ các nguồn khác nhau để cung cấp thông tin hữu ích giúp các tổ chức định vị, phòng ngừa và ứng phó với các mối đe dọa an ninh mạng. ■ Thời gian: 5 -10 năm ■ Mức độ ảnh hưởng: Trung bình ■ Độ trưởng thành: 1 ■ Sự kỳ vọng: : Đỉnh điểm của sự thổi phồng kỳ vọng