CyStack

DATA SHEET

# Red Teaming

Tầm soát năng lực bảo mật của doanh nghiệp trước những mối đe dọa thực tế

## Tổng quan

Red Teaming là giải pháp bảo mật mô phỏng các cuộc tấn công trên thực tế để đánh giá năng lực ứng phó của doanh nghiệp trước các mối đe dọa tiềm ẩn trên không gian mạng. Red Teaming không tập trung tìm kiếm lỗ hổng trên đối tượng ứng dụng hoặc dịch vụ cụ thể được chỉ định trước (như ứng dụng mạng, ứng dụng di động, API, v.v.) như giải pháp Kiểm thử xâm nhập (Penetration Testing). Thay vào đó, chuỗi hoạt động trong Red Teaming áp dụng các chiến thuật (tactic), kỹ thuật (technique) và quy trình (procedure) phát triển bởi tội phạm công nghệ cao để tìm yếu các điểm yếu trong hàng rào phòng thủ bảo mật, từ đó tiến hành các khai thác không giới hạn theo thỏa thuận vào hạ tầng mạng của doanh nghiệp.

Với cách tiếp cận này, Red Teaming sẽ đi xa hơn hình thức Penetration Testing thông thường về chiều sâu và phạm vi tấn công. Red Teaming là sự sắp xếp và tối ưu diễn tiến các phương pháp tấn công, từ việc thu thập thông tin về toàn bộ tài nguyên của doanh nghiệp bằng công cụ OSINT và hình thức tấn công phi kỹ thuật, đến khai thác lỗ hổng, duy trì kết nối tới máy chủ nội bộ và tấn công lan rộng trong toàn mạng doanh nghiệp, thậm chí đánh cắp các dữ liệu đã thỏa thuận từ trước. Do đó, quá trình triển khai Red Teaming thường đòi hỏi thời gian tiến hành dài hơn so với Penetration Testing thông thường, có thể lên tới vài tháng, tùy theo quy mô hạ tầng CNTT của doanh nghiệp. Đây là khoảng thời gian phù hợp để đồng thời đánh giá kiến thức, năng lực bảo mật và tính hiệu quả của quy trình phát hiện - ứng phó sự cố an ninh mạng của toàn bộ nhân sự trong doanh nghiệp.

### Lợi ích của khách hàng

- Mô phỏng các mối đe dọa thực tế mà không gây bất kỳ tổn hại nào cho tổ chức
- Phát hiện các lỗ hổng tiềm ẩn và kiểm tra khả năng chống chịu của tổ chức trước các cuộc tấn công APT
- Đánh giá và cải thiện quy trình phát hiện - ứng cứu sự cố
- Nâng cao các cơ chế phòng thủ cả về mặt kỹ thuật và phi kỹ thuật
- Tăng cường nhận thức bảo mật và tính sẵn sàng trước các sự kiện an ninh mạng

## Hướng tiếp cận của CyStack

Thành viên Red Team của CyStack bao gồm những chuyên gia tài năng và giàu kinh nghiệm, thường xuyên tham gia các hội nghị an ninh mạng lớn hàng năm trên thế giới với vai trò diễn giả, đồng thời họ cũng là những chuyên gia săn lỗ hổng với bề dày thành tích phát hiện các lỗi bảo mật nghiêm trọng và được ghi danh trên Hall of Fame của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Nokia, Alibaba, Sea Group, v.v.

Dịch vụ Red Teaming của CyStack là một giải pháp toàn vẹn cho các doanh nghiệp vừa thực hiện các thay đổi lớn về hạ tầng CNTT, cần đánh giá quy trình phản ứng sự cố, hoặc đang tìm kiếm những điểm yếu bảo mật còn tồn đọng ở cả các yếu tố phi kỹ thuật như chính sách, quy trình và con người. Một trong những điều làm nên sự khác biệt ở dịch vụ Red Teaming của CyStack đó là tính linh hoạt cao đối với các nhóm đối tượng khách hàng khác nhau, trải rộng trên mọi quy mô, cũng như mọi lĩnh vực ngành nghề. Chiến thuật Red Teaming tại CyStack luôn cập nhật mới và bám sát với các xu hướng tấn công trên không gian mạng thực tế.

Ngoài ra, dịch vụ Red Teaming tại CyStack cũng đi kèm với một nền tảng phát hiện lộ lọt dữ liệu được phát triển bởi chính đội ngũ kỹ sư nội bộ. Nền tảng này được trang bị các công cụ và tính năng mạnh mẽ giúp phát hiện, theo dõi, phân loại và đánh giá mức độ nghiêm trọng của các dữ liệu lộ lọt. Hệ thống này cũng bao gồm khả năng giám sát lộ lọt dữ liệu theo thời gian thực, được đội ngũ Red Team của CyStack tận dụng cho các bước đầu tiên trong quá trình triển khai dịch vụ.

# Giải pháp của CyStack

Dịch vụ Red Teaming của CyStack có thể hiểu như là sự kết hợp và quy trình hóa các giải pháp dưới đây một cách hợp lý và hiệu quả:

- **Threat Intelligence (TI)**: Đây là quá trình thu thập, phân tích và sử dụng thông tin về các tác nhân nguy hại (threat actor) để có góc nhìn chính xác về xu hướng các TTP trên thực tế. Thông tin lưu trữ bao gồm tổng hợp các sự kiện an ninh mạng đã và đang diễn ra, hồ sơ threat actor, các dấu vết chứng minh xâm nhập thành công (Indicator of Compromise, IoC), thông tin chi tiết các 0-day và CVE, dữ liệu lộ lọt, v.v. Tham khảo thông tin chi tiết về công cụ phát hiện lộ lọt dữ liệu tại đây.
- **Social Engineering (SE)**: Giải pháp này bao gồm các cuộc tấn công sử dụng yếu tố con người như phishing qua email hoặc ứng dụng web, pretexting, hoặc vishing để khai thác thông tin nhạy cảm của người dùng hoặc đánh lừa người dùng cài đặt phần mềm khai thác hệ thống nội bộ.
- **Physical Security Assessment (PSA)**: Là giải pháp đánh giá mức độ chặt chẽ và an toàn của các hình thức giám sát và kiểm soát truy cập vật lý, như việc vào ra các tòa nhà, văn phòng, trung tâm dữ liệu và các khu vực bị giới hạn khác. PSA sẽ chỉ được sử dụng trong chiến dịch Red Teaming khi có sự yêu cầu từ phía khách hàng, cũng như sau khi hai bên thực hiện đánh giá rủi ro bảo mật kỹ lưỡng và cam kết tuân thủ bộ Nguyên tắc Tham gia (Rules of Engagement, hay RoE) đã ký kết.
- **Vulnerability Assessment (VA)**: VA tập trung vào việc tầm soát liên tục các lỗ hổng và điểm yếu bảo mật trên một đối tượng cụ thể, có thể là ứng dụng web, máy chủ, hoặc mạng lưới hệ thống nhất định. Để đơn giản hóa và tự động thực hiện VA, CyStack phát triển CyStack Web Security (CWS), là công cụ rà quét và giám sát lỗ hổng cho các ứng dụng web. CWS tận dụng các kỹ thuật fuzzing và cơ sở dữ liệu về lỗ hổng bảo mật tổng hợp từ nhiều nguồn mở, cũng như sở hữu riêng của CyStack. Với CWS, các lỗ hổng bảo mật mới được giám sát liên tục và cảnh bảo tự động ngay khi phát hiện. CWS cũng cung cấp một nền tảng để quản lý, theo dõi, sắp xếp mức độ ưu tiên và đề xuất cách xử lý cho các phát hiện. Tham khảo thông tin chi tiết tại đây.
- **Penetration Testing (PT)**: PT là sự mô phỏng lại cuộc tấn công an ninh mạng vào một đối tượng cụ thể như ứng dụng web, ứng dụng mobile, máy chủ, v.v. PT được thực hiện thủ công bởi các chuyên gia bảo mật, sử dụng đa dạng các loại công cụ và kỹ thuật tấn công. Mục tiêu của giải pháp này là phát hiện tối đa các lỗ hổng và điểm yếu bảo mật có thể bị khai thác. Tham khảo thông tin chi tiết tại đây.
- **Advanced Persistent Threat (APT)**: Giải pháp giúp mô phỏng cuộc tấn công có chủ đích trên thực tế, toàn diện với nhiều pha, từ thu thập thông tin, xâm nhập vào hệ thống, duy trì quyền kiểm soát, đến đánh cắp dữ liệu hoặc gây ra thiệt hại. Các cuộc tấn công này được thực hiện như một kẻ tấn công thật sự, sử dụng các TTP tinh vi.

Giải pháp Red Teaming của CyStack được xây dựng tuân theo những phương pháp và tiêu chuẩn ngành tốt nhất khi tiến hành Red Teaming. Một trong những tài nguyên chính đội ngũ chuyên gia dựa vào là MITRE ATT&CK. Đây là bộ khung mô tả các chiến thuật, kỹ thật và quy trình (TTP) được kẻ tấn công sử dụng trong các cuộc tấn công trên thực tế. Ngoài ra, phương pháp luận Red Teaming của CyStack được xây dựng bám sát theo khung CBEST và TIBER-EU, là hai bộ khung quy trình Red Teaming hàng đầu, được công nhận rộng rãi trong lĩnh vực tài chính - ngân hàng.

## Tính năng chính

- Thiết lập chiến dịch linh hoạt theo quy mô, đặc thù và yêu cầu cụ thể từ từng khách hàng
- Mô phỏng các cuộc tấn công mạng trên thực tế
- Thực hiện bởi đội ngũ chuyên gia sở hữu chứng chỉ bảo mật uy tín hàng đầu trên thế giới
- Đánh giá toàn diện năng lực bảo mật từ hạ tầng IT đến các yếu tố con người và chính sách
- Thông báo theo thời gian thực đối với các lỗ hổng đặc biệt nghiêm trọng
- Cảnh báo sớm các dữ liệu bị rò rỉ trên không gian mạng
- Báo cáo phân tích chi tiết quá trình tấn công theo khung MITRE ATT&CK kèm theo các IoA và IoC cụ thể
- Hướng dẫn khắc phục cụ thể, ưu tiên theo mức độ nghiêm trọng của lỗ hổng và điểm yếu bảo mật
- Kiểm tra mức độ tuân thủ các tiêu chuẩn bảo mật và bảo vệ dữ liệu đang được áp dụng trong tổ chức
- Đảm bảo quá trình tiến hành chiến dịch không gây ảnh hưởng tới vận hành hệ thống của doanh nghiệp

# Phương pháp luận

Các bước cụ thể trong từng giai đoạn của một dự án Red Teaming có thể khác nhau, tùy vào mục đích, phạm vi và đặc thù doanh nghiệp triển khai. Nhưng nhìn chung, quy trình Red Teaming của CyStack tuân thủ nghiêm ngặt các bước sau:

1. **Chuẩn bị**: Giai đoạn này liên quan đến việc xác định các loại rủi ro bảo mật quan trọng nhất với tổ chức và hiểu mục tiêu của chiến dịch Red Teaming. Ngoài ra, các đầu mối liên hệ, kênh trao đổi, RoE, phạm vi, đánh giá rủi ro và cũng như các yêu cầu đặc biệt khác cũng được thống nhất trong giai đoạn này. CyStack lựa chọn nhân sự phù hợp và xây dựng một Red Team bao gồm đầy đủ các vai trò: Governance/QA, Project Manager, Red Team Lead và các Red Team Operator.
2. **Thu thập thông tin và Mô hình hóa mối đe dọa**: Đây là giai đoạn phân tích các dấu vết kỹ thuật số với công cụ OSINT cũng như biện pháp tấn công phi kỹ thuật, nhằm xác định bề mặt tấn công và tìm kiếm các dịch vụ dễ bị khai thác nhất của tổ chức. Bên cạnh đó, CyStack cũng kết hợp tham chiếu các cuộc tấn công đã từng xảy ra trên chính tổ chức hoặc các doanh nghiệp tương đồng, từ đó xây dựng mô hình mối đe dọa riêng biệt cho chiến dịch Red Teaming.
3. **Phát hiện lỗ hổng**: Sử dụng dữ liệu từ giai đoạn kề trước, CyStack xác định các hướng tấn công khả thi và tiến hành thử nghiệm tấn công liên tục bằng những công cụ chuyên biệt và tự phát triển bởi CyStack đã được thỏa thuận từ trước, đảm bảo không gây ảnh hưởng tới việc vận hành hệ thống kinh doanh của tổ chức.
4. **Khai thác và Truy cập ban đầu**: Tận dụng nguồn thông tin rò rỉ tìm thấy bởi Nền tảng phát hiện lộ lọt dữ liệu của CyStack, kết hợp mọi thủ đoạn tấn công phi kỹ thuật và xâm nhập vật lý để khai thác thành công tập lỗ hổng đã được phát hiện ở giai đoạn trước. Sau khi đã có quyền truy cập thành phần bất kỳ trong hạ tầng CNTT của tổ chức, đội ngũ Red Team của CyStack sẽ tìm cách duy trì truy cập và tiến hành nâng quyền để phục vụ cho các giai đoạn tiếp theo.
5. **Tìm kiếm thêm thông tin xác thực và Khai thác sâu**: Ở giai đoạn này, đội ngũ Red Team tập trung rà quét các dịch vụ nội bộ, cũng như vét cạn toàn bộ các thông tin xác thực liên quan, để tiếp tục khai thác các lỗ hổng ẩn sâu bên trong, cũng như tấn công lan sang và chiếm quyền truy cập các thành phần khác trong hạ tầng CNTT của tổ chức.
6. **Lấy dữ liệu**: CyStack tiến hành thu thập và trích xuất những dữ liệu đã được thỏa thuận từ trước làm bằng chứng chiếm hữu thành công máy chủ bất kỳ. Quá trình này được thực hiện một cách kín đáo và thận trọng, đảm bảo không bị phát hiện bởi các cơ chế phòng vệ mặc định cũng như các công cụ nâng cao bảo vệ thiết bị đầu cuối.
7. **Báo cáo**: Đây là giai đoạn cuối của chiến dịch Red Teaming. Sau khoảng thời gian cam kết thực hiện dịch vụ, CyStack tổng hợp lại các kết quả thu được trong chiến dịch, trình bày tổng quan các vấn đề tồn đọng trong hệ thống, đưa ra các khuyến nghị khắc phục, và mô tả chi tiết quá trình tấn công vào hạ tầng CNTT của tổ chức bám sát theo khung MITRE ATT&CK. Ngoài ra, CyStack cũng đưa ra danh sách các dấu vết chỉ điểm tấn công (Indicator of Attack, IoA) và dấu vết chứng minh xâm nhập thành công (Indicator of Compromise, IoC), giúp đội ngũ nhân sự nội bộ của tổ chức rà soát hệ thống và củng cố năng lực bảo mật để ứng phó kịp thời trước các cuộc tấn công tương tự.

# Các mô hình chiến dịch Red Teaming phổ biến

## Định hướng theo kết quả

- **Tình huống**: Thỏa thuận đạt được tiêu chí nhất định, ví dụ lấy được thông tin nhạy cảm, khai thác thành công máy chủ nội bộ cụ thể, gây sập dịch vụ, v.v.
- **Mục đích**: Kiểm tra tính phù hợp và an toàn của các giải pháp bảo mật áp dụng trên đối tượng xác định

## Định hướng theo kịch bản

- **Tình huống**: Giả lập một hoặc một vài kịch bản cụ thể, có thể là tấn công ransomware, tấn công chuỗi cung ứng, mối đe dọa từ bên trong, v.v.
- **Mục đích**: Kiểm tra tính sẵn sàng của tổ chức trước kịch bản tương ứng

## Giả lập APT thuần túy

- **Tình huống**: Mô phỏng chính xác các TTP đã ghi nhận của một hoặc một vài threat actor xác định
- **Mục đích**: Đánh giá năng lực phát hiện và ứng phó sự cố của đội ngũ bảo mật nội bộ, cũng như khả năng chống chịu của tổ chức trước hình thức tấn công APT

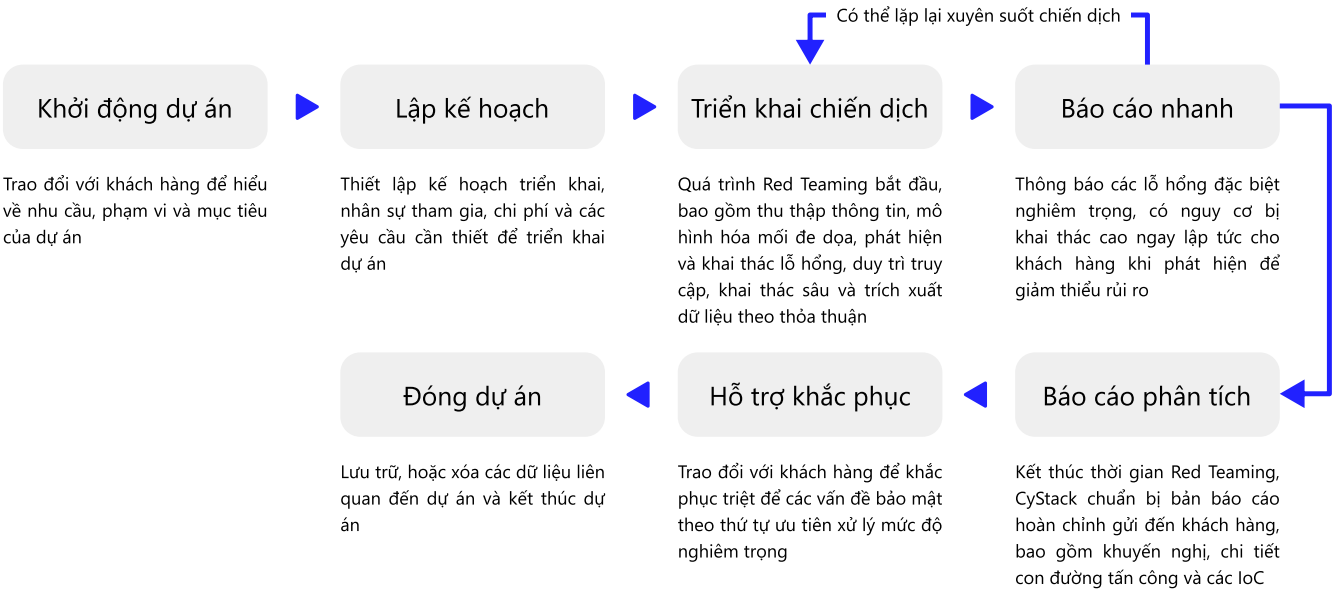
## Kết hợp với Blue Team

- **Tình huống**: Thực hiện tấn công như các threat actor nhưng đồng thời bám sát và chia sẻ ý tưởng cho các hoạt động của đội ngũ Blue Team.
- **Mục đích**: Nâng cao năng lực phát hiện và ứng phó sự cố của đội ngũ bảo mật nội bộ qua tương tác thực tế.

# So sánh Red Teaming với Penetration Testing

| | Red Teaming | Penetration Testing |
|---|---|---|
| **Mục tiêu** | Mô phỏng các cuộc tấn công trên thực tế để kiểm tra khả năng phát hiện, ứng phó sự cố và mức độ chống chịu về mặt bảo mật | Xác định các lỗ hổng tồn tại trong ứng dụng, hệ thống hoặc mạng nội bộ |
| **Phạm vi** | • Toàn diện, không chỉ bao gồm yếu tố kỹ thuật, mà cả yếu tố con người, quy trình và an ninh tầng vật lý<br>• Đánh giá bảo mật cả bề mặt bên ngoài và nội bộ của tổ chức | • Chỉ định trên một hoặc một vài đối tượng cụ thể, tập trung vào các yếu tố kỹ thuật và logic vận hành trong ứng dụng<br>• Đánh giá bảo mật trên đối tượng cụ thể như ứng dụng, máy chủ, hay dải mạng |
| **Thời gian triển khai** | • Dài, thường từ vài tuần đến vài tháng<br>• Trung bình kéo dài trong 3 tháng<br>• Phụ thuộc quy mô hạ tầng CNTT của tổ chức | • Ngắn, thường từ vài ngày đến vài tuần<br>• Trung bình kéo dài trong 12 ngày<br>• Phụ thuộc mức độ phức tạp của đối tượng |
| **Cách tiếp cận** | • Thường kín đáo và bất ngờ, chỉ có đại diện hai bên và đội ngũ Red Team biết<br>• Giả lập các cuộc tấn công APT, áp dụng tất cả các TTP phù hợp với đối tượng (chiến thuật, kỹ thuật và quy trình) | • Được thông báo cụ thể cho đội ngũ kỹ thuật hai bên<br>• Sử dụng công cụ quét và kiểm thử thủ công theo các checklist tiêu chuẩn hoặc định nghĩa trước từ hai phía |
| **Kết quả đem lại** | Báo cáo tổng quan về các điểm yếu, khuyến nghị khắc phục toàn diện đối với cả bề mặt bên ngoài và bên trong tổ chức, chi tiết con đường tấn công đối chiếu theo từng TTP | Báo cáo tổng quan về số lượng và phân loại lỗ hổng, khuyến nghị khắc phục, chi tiết và bằng chứng khai thác từng lỗ hổng |
| **Các tiêu chuẩn liên quan** | MITRE ATT&CK, CBEST, hoặc TIBER-EU | NIST SP 800-115 hoặc OWASP (Testing Guide, Top Ten) |
| **Use case** | • Đánh giá năng lực bảo mật của tổ chức về mọi mặt<br>• Kiểm tra và cải thiện quy trình phát hiện và ứng phó sự cố<br>• Xác định tính sẵn sàng và khả năng chống chịu của tổ chức trước các cuộc tấn công APT trên thực tế | • Đánh giá mức độ bảo mật của đối tượng cụ thể như ứng dụng, hệ thống hoặc dải mạng<br>• Tầm soát lỗ hổng trong ứng dụng trước khi đưa vào môi trường production |
| **Phù hợp với** | • Doanh nghiệp đã xây dựng và áp dụng các chương trình và khung bảo mật<br>• Doanh nghiệp vừa thực hiện thay đổi lớn về hạ tầng CNTT | • Doanh nghiệp phát triển phần mềm có sự giới hạn về nhân sự bảo mật<br>• Doanh nghiệp sử dụng phần mềm phát triển bởi bên thứ ba |

# Quy trình làm việc với khách hàng




**Về CyStack**

CyStack là một công ty đổi mới sáng tạo trong lĩnh vực an ninh mạng tại Việt Nam, chúng tôi tiên phong xây dựng các sản phẩm bảo mật thế hệ mới cho cả doanh nghiệp và cá nhân. Các giải pháp của CyStack tập trung vào bảo vệ dữ liệu, phòng chống tấn công mạng và quản lý lỗ hổng bảo mật.

Để biết thêm chi tiết, liên lạc tới hotline **(+84) 247 109 9656** hoặc gửi mail tới **contact@cystack.net** để trao đổi cùng các chuyên gia bảo mật tại CyStack.
**cystack.net**