CyStack

DATA SHEET

Kiểm thử giao thức blockchain

Đánh giá tính toàn vẹn của giao thức blockchain

Thách thức bảo mật

Công nghệ blockchain được thiết kế vô cùng an toàn, tuy nhiên vẫn còn một số thách thức để đảm bảo tính bảo mật của blockchain, có thể kể đến:

- **Tấn công 51% (51% attack)**: Trong cuộc tấn công 51%, nhóm kẻ tấn công giành quyền kiểm soát hơn 50% năng lực tính toán của blockchain, cho phép chúng thao túng mạng và có khả năng đảo ngược hoặc chặn các giao dịch hợp lệ.
- **Tấn công mạo nhận (Sybil attack)**: Tấn công mạo nhận là khi một kẻ tấn công tạo ra nhiều danh tính hoặc node trong mạng để giành quyền kiểm soát một phần đáng kể năng lực tính toán của mạng.
- **Gian lận lặp chi (Double-spending)**: Trong một cuộc tấn công gian lận lặp chi, kẻ tấn công có thể chi tiêu cùng một loại tiền kỹ thuật số hoặc token nhiều lần bằng cách tạo bản sao tài sản kỹ thuật số.
- **Rò rỉ dữ liệu và quyền riêng tư**: Tấn công rò rỉ dữ liệu và quyền riêng tư là khi kẻ tấn công truy cập dữ liệu nhạy cảm lưu trữ trên blockchain như thông tin cá nhân hoặc dữ liệu tài chính.
- **Tấn công kênh bên (Side-channel attack)**: Tấn công kênh bên là cuộc tấn công nhằm khai thác một số thông tin bên lề không thuộc kênh giao tiếp chính như mức tiêu thụ năng lượng hoặc bức xạ điện từ.

Trên đây chỉ là một vài ví dụ về những thách thức bảo mật mà công nghệ blockchain phải đối mặt. Lĩnh vực này vẫn đang phát triển, các chuyên gia bảo mật cũng như nhà phát triển vẫn đang không ngừng nghiên cứu để xác định và giảm thiểu các mối đe dọa mới.

Lợi ích của khách hàng

- Xác định và khắc phục các lỗ hổng hay rủi ro bảo mật tiềm ẩn trước khi khởi chạy chính thức
- Đảm bảo rằng giao thức tương tác an toàn với các hệ thống khác
- Tạo dựng niềm tin với khách hàng và các bên liên quan
- Tránh các vi phạm bảo mật gây thiệt hại nghiêm trọng và downtime
- Cải thiện hiệu năng và hiệu quả tổng thể của mạng

Tổng quan

Kiểm thử bảo mật giao thức blockchain là quy trình đánh giá và phân tích thiết kế, cách triển khai và tính bảo mật của giao thức blockchain, từ đó xác định các lỗ hổng hay điểm yếu có thể bị kẻ tấn công khai thác, được thực hiện bởi các chuyên gia bảo mật có trình độ cao về công nghệ blockchain. Quy trình kiểm thử này thường bao gồm việc đánh giá, kiểm tra và phân tích mã nguồn cũng như tài liệu kỹ thuật để chỉ ra các lỗ hổng bảo mật, đồng thời trao đổi trực tiếp với nhà phát triển và các bên liên quan để đảm bảo giao thức blockchain được triển khai khớp với mô tả trong tài liệu kỹ thuật.

Kiểm thử bảo mật giao thức blockchain giúp nhà phát triển:

- Đánh giá tổng thể tình trạng bảo mật và độ tin cậy của giao thức blockchain để xác định hổng hay điểm yếu nào có thể bị khai thác.
- Đánh giá thiết kế và cách triển khai giao thức blockchain để đảm bảo đạt các tiêu chí đề ra cũng như các khuyến nghị bảo mật cập nhật mới nhất.
- Xác định các mối đe dọa và vector tấn công tiềm ẩn có thể sử dụng để phá vỡ tính bảo mật của giao thức blockchain.
- Nhận được các khuyến nghị để cải thiện tình trạng bảo mật và độ tin cậy của giao thức blockchain.

Nhìn chung, kiểm thử giao thức blockchain rất quan trọng đối với việc đảm bảo tính bảo mật và độ tin cậy của giao thức blockchain, đồng thời rất cần thiết để duy trì sự tin tưởng và tín nhiệm của người dùng và các bên liên quan.

Giải pháp của CyStack

Đội ngũ kiểm thử bảo mật của CyStack bao gồm những chuyên gia tài năng, giàu kinh nghiệm, thành thạo các phương pháp kiểm thử bám sát mục tiêu và tối ưu nhất. Họ là những chuyên gia có nền tảng vững chắc về phát triển phần mềm và nghiên cứu an ninh mạng, giúp đội ngũ CyStack đánh giá toàn diện nhất các rủi ro bảo mật trong sản phẩm số của doanh nghiệp. Các chuyên gia tại CyStack cũng thường xuyên tham gia các hội nghị an ninh mạng lớn trên thế giới với vai trò diễn giả hàng năm, đồng thời họ là những chuyên gia săn lỗi phần mềm với nhiều thành tích phát hiện ra các lỗ hổng bảo mật nghiêm trọng và được ghi danh trên Hall of Fame của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Sea Group, Alibaba, v.v.

Hiểu được sự phức tạp của các giao thức blockchain và những rủi ro tiềm ẩn liên quan, CyStack cung cấp giải pháp bao gồm đánh giá mã, đánh giá tự động, kiểm thử bảo mật, kiểm thử tuân thủ, kiểm thử hiệu suất và kiểm thử khả năng tương tác. Cách tiếp cận này giúp xác định và khắc phục mọi lỗ hổng hoặc sự cố trong giao thức blockchain để đảm bảo tính an toàn, hiệu quả và độ tin cậy. Đánh giá hiệu suất của giao thức blockchain bao gồm việc kiểm thử khả năng mở rộng, mức tiêu thụ gas và khả năng sử dụng. Từ đó giúp các doanh nghiệp xác định và giải quyết mọi vấn đề có thể ảnh hưởng đến hiệu suất của giao thức blockchain.

Tính năng chính

- Đánh giá toàn diện
- Đánh giá mã nguồn kỹ càng
- Kiểm thử tự động với công cụ SafeChain.org
- Kiểm thử xâm nhập
- Kiểm thử hệ quản trị
- Kiểm thử hiệu năng
- Kiểm thử khả năng tương tác
- Mở chương trình săn lỗi nhận thưởng với WhiteHub.net

Phương pháp luận

Kiểm thử bảo mật giao thức blockchain là một quy trình có hệ thống nhằm xác định các lỗ hổng và các mối đe dọa tiềm ẩn. Đội ngũ CyStack thực hiện tuân thủ nghiêm ngặt các bước sau đây:

1. **Phân tích tài liệu kỹ thuật**: Nghiên cứu tài liệu để hiểu thiết kế và chức năng của giao thức blockchain. Các tài liệu bao gồm whitepaper, mã nguồn và các tài liệu có sẵn khác.
2. **Xác định cơ chế đồng thuận**: Hiểu cơ chế đồng thuận được sử dụng trong giao thức blockchain, giúp xác định các điểm yếu tiềm ẩn có thể bị khai thác.
3. **Đánh giá mã nguồn**: Đánh giá toàn diện mã nguồn của giao thức blockchain, tìm kiếm các lỗ hổng tiềm ẩn như lỗi buffer overflow, SQL injection và các lỗ hổng phần mềm phổ biến khác.
4. **Quét mã nguồn**: Sử dụng các công cụ kiểm thử tự động để kiểm thử mã nguồn và tìm các lỗ hổng tiềm ẩn, bao gồm kiểm thử đơn vị, kiểm thử tích hợp và kiểm thử hồi quy.
5. **Kiểm thử xâm nhập**: Mô phỏng cuộc tấn công trong thực tế vào giao thức blockchain, bao gồm khai thác các lỗ hổng được xác định trong quá trình đánh giá và kiểm tra tự động mã nguồn.
6. **Đánh giá mức độ tuân thủ**: Đánh giá giao thức blockchain để đảm bảo tính tuân thủ tiêu chuẩn ngành hay các quy định liên quan.
7. **Kiểm thử khả năng tương tác**: Đánh giá khả năng tương thích của giao thức blockchain với các mạng và hệ thống blockchain khác, đảm bảo giao thức này có thể tương tác với các hệ thống liên quan trong hệ sinh thái.
8. **Kiểm thử hiệu năng**: Đánh giá hiệu năng của giao thức blockchain, bao gồm khả năng mở rộng, mức tiêu thụ gas và khả năng sử dụng.
9. **Xuất báo cáo**: Tạo báo cáo chi tiết về kết quả kiểm thử gồm bất kỳ lỗ hổng hoặc vấn đề nào được xác định và các đề xuất khắc phục.
10. **Hỗ trợ khắc phục**: Hỗ trợ giải quyết mọi vấn đề hoặc lỗ hổng được xác định trong quá trình kiểm thử với các hướng dẫn về cách khắc phục sự cố.

Danh sách lỗ hổng

Trong quá trình kiểm thử, các lỗ hổng trong bảng sau được kiểm thử:

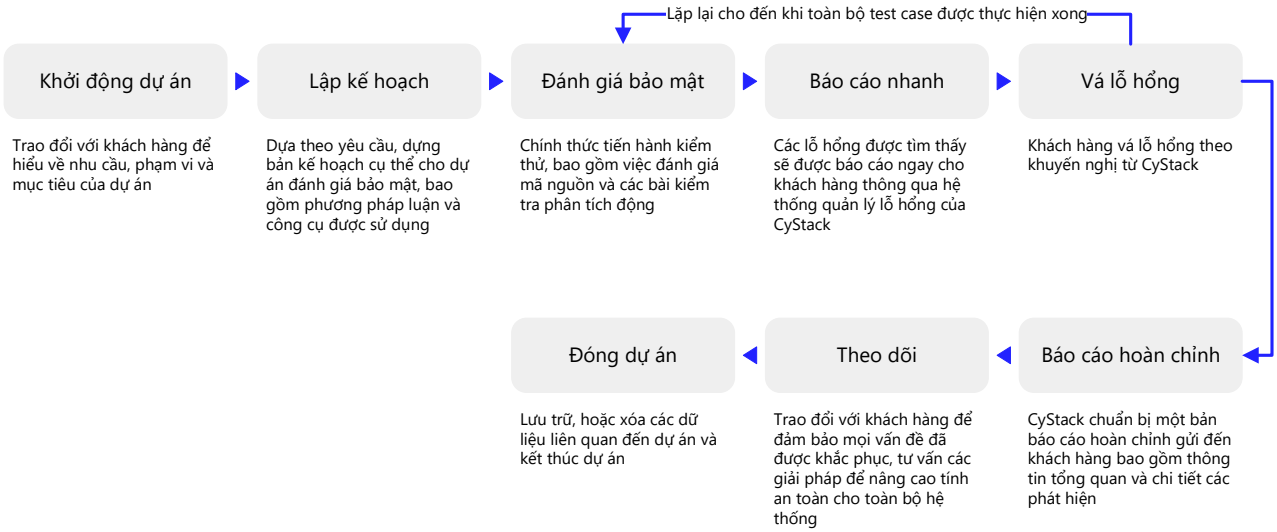
Tầng	Thành phần	Lỗ hổng	Mức độ nghiêm trọng	Mô tả
Tầng mạng (Network Layer)	**P2P**	**Sybil Attack**	High	Kẻ tấn công tạo nhiều danh tính, sau đó sử dụng chúng để kiểm soát mạng hoặc làm gián đoạn hoạt động bình thường của mạng. Ví dụ, kẻ tấn công có thể tạo nhiều danh tính để kiểm soát phần lớn quyền biểu quyết trong mạng phi tập trung, cho phép kiểm soát quá trình ra quyết định của mạng.
		Eclipse Attack	High	Kẻ tấn công cô lập một node hoặc nhóm node khỏi phần còn lại của mạng bằng cách điều hướng các kết nối in-bound và outbound trong mạng lưới mục tiêu tới các node của kẻ tấn công, thay vì tới một node hoặc một nhóm các node nhất định.
		Eavesdropping Attack	Low	Kẻ tấn công xen giữa và giám sát quá trình truyền tải thông tin giữa hai hoặc nhiều bên mà không có sự thông báo hoặc sự đồng ý, nhờ đó có quyền truy cập vào thông tin nhạy cảm như thông tin đăng nhập, dữ liệu tài chính hoặc thông tin cá nhân.
		Denial of Service Attack	Medium	Tấn công Denial of Service (DoS) làm gián đoạn hoạt động bình thường của mạng bằng cách chiếm tài nguyên của một hoặc nhiều node. Ví dụ, kẻ tấn công có thể sử dụng mạng botnet để gửi số lượng lớn request tới một node, khiến node đó quá tải và không thể phản hồi, dẫn đến giảm hiệu năng tổng thể cũng như tính sẵn sàng của mạng, đồng thời có thể khiến người dùng không thể thực hiện các chức năng trên mạng.
		BGP Hijack Attack	Low	Kẻ tấn công chặn và chuyển hướng các gói tin gửi qua đường truyền Internet bằng cách thao túng thông tin định tuyến trao đổi giữa các bộ định tuyến. Ví dụ, kẻ tấn công gửi đi thông báo giả về chủ quyền đối với các địa chỉ IP mà chúng không thực sự sở hữu, điều khiển hoặc được định tuyến đến, khiến toàn bộ các gói tin bị điều hướng khỏi đích đến ban đầu.
		Alien Attack	Low	Kiểu tấn công nhắm vào các mạng phi tập trung, thực hiện tạo một chuỗi khối mới có cùng giao thức giao tiếp với một chuỗi có sẵn hoặc là một nhánh của chuỗi có sẵn. Sau đó, kẻ tấn công sử dụng chuỗi mới này để tấn công chuỗi hiện có, làm các chuỗi này xung đột lẫn nhau, giảm hiệu năng giao tiếp giữa các node, và thậm chí gây ra hiện tượng tắc nghẽn node.
		Timejacking	High	Kiểu tấn công vào mạng blockchain nhằm thao túng thời gian trong hệ thống. Kẻ tấn công gửi đi thông tin thời gian không chính xác tới toàn mạng, khiến các node trong mạng không nắm được chính xác thời gian hiện tại, dẫn đến sai lệch và làm gián đoạn hoạt động bình thường của mạng, cũng như có khả năng khiến người dùng không thể thực hiện được các chức năng trên mạng.

Tầng mạng (Network Layer)	**RPC**	**Eavesdropping Attack**	Low	Kẻ tấn công xen giữa và giám sát quá trình truyền tải thông tin giữa hai hoặc nhiều bên mà không có sự thông báo hoặc sự đồng ý, nhờ đó có quyền truy cập vào thông tin nhạy cảm như thông tin đăng nhập, dữ liệu tài chính hoặc thông tin cá nhân.
		Denial of Service Attack	Medium	Tấn công DoS làm gián đoạn hoạt động bình thường của mạng bằng cách chiếm tài nguyên của một hoặc nhiều node. Ví dụ, kẻ tấn công có thể sử dụng mạng botnet để gửi số lượng lớn request tới một node, khiến node đó quá tải và không thể phản hồi, dẫn đến giảm hiệu năng tổng thể cũng như tính sẵn sàng của mạng, đồng thời có thể khiến người dùng không thể thực hiện các chức năng trên mạng.
		The Ethereum Black Valentine's Day Vulnerability	Low	Lỗ hổng này được khai thác bằng cách lợi dụng lỗi xác thực ở RPC API của Geth/Parity tại các node Ethereum thông qua hàm eth_sendTransaction.
		HTTP Input Attack	Low	Các lỗ hổng như: Cross-Site Scripting (XSS) / Template injection / Third-party component vulnerability / HTTP parameter pollution / SQL injection / XXE entity injection / Deserialization vulnerability / SSRF vulnerability / Code injection / Local file contains / Remote file contains / Command execution injection / Buffer overflow / Formatted string
		Cross-Domain Phishing Attack	Low	Cuộc tấn công nhằm đánh cắp thông tin nhạy cảm như private key, các cụm từ khôi phục (seed phrase) hoặc thông tin đăng nhập, thực hiện bằng cách lừa người dùng truy cập vào trang web giả mạo trông giống như RPC hợp lệ.
Tầng sổ cái (Ledger Layer)	**Cơ chế đồng thuận**	**Long Range Attack**	High	Long Range Attack chỉ có thể xảy ra trên giao thức Proof of Stake (PoS). Kẻ tấn công tạo ra một chuỗi khối mới là một nhánh của chuỗi hiện tại nhưng có lịch sử chuỗi dài hơn, mà lịch sử này có sự khác biệt một phần hoặc hoàn toàn so với của chuỗi chính. Sau đó, kẻ tấn công sử dụng chuỗi mới này để thay thế vai trò của chuỗi chính, khiến người dùng không thể thực hiện các chức năng trên mạng, cũng như cho phép chúng thao túng mạng lưới tùy ý.
		Bribery Attack	High	Kẻ tấn công mua chuộc người điều khiển máy đào hoặc máy xác thực để khai thác hay xác thực các giao dịch độc hại bằng cách chi trả khoản tiền lớn để khai thác hoặc xác thực một giao dịch cụ thể hoặc bằng cách đe dọa rút tài trợ.
		Race Attack	High	Kẻ tấn công tạo hai giao dịch xung đột, một giao dịch gửi tài sản kỹ thuật số đến địa chỉ của kẻ tấn công và giao dịch kia gửi tài sản kỹ thuật số đến người nhận hợp lệ. Sau đó, kẻ tấn công cố gắng gửi toàn mạng tin về giao dịch đến địa chỉ của mình trước khi giao dịch tới địa chỉ hợp lệ được xác nhận.

Tầng sổ cái (Ledger Layer)	**Cơ chế đồng thuận**	**Liveness Denial**	High	Liveness Denial là hình thức tấn công Denial of Service đối với các giao thức PoS. Ở kiểu tấn công này, một vài hoặc tất cả các validator cố tình chặn các giao dịch bằng cách không công khai các khối. Khi các validator không hoàn thành nhiệm vụ của chúng, chuỗi khối sẽ bị ngưng trệ, do các khối mới không được xác nhận tính hợp lệ và công khai nối vào chuỗi khối.
		Censorship	High	Kẻ tấn công ngăn chặn không cho một số giao dịch nhất định được xử lý hoặc ghi lại trên blockchain bằng cách chặn quyền truy cập vào các node nhất định, thao túng cơ chế đồng thuận hoặc can thiệp vào các kênh truyền tin của mạng, từ đólàm gián đoạn hoạt động bình thường của mạng.
		Finney Attack	High	Finney Attack là một dạng tấn công lặp chi (Double Spend Attack). Dạng tấn công này được thực hiện bằng cách tạo ra hai giao dịch tương đồng, trong đó có một giao dịch đã được xác nhận trong một khối được đào sẵn. Khi giao dịch còn lại được thực hiện, kẻ tấn công lập tức thông báo về khối đã đào được đó lên toàn mạng, và vô hiệu hóa giao dịch này. Lợi dụng điều này, kẻ tấn công có thể thực hiện chuyển tiền về chính ví của mình, thay vì chuyển tiền cho bên bán sản phẩm hay dịch vụ.
		Vector76 Attack	High	Vector76 là sự kết hợp của Race Attack và Finney Attack. Kiểu tấn công này cho phép một máy đào độc hại thực hiện gian lập lặp chi bằng cách nhắm mục tiêu vào một tập số lượng nhỏ các node, gây hại cho mạng lưới.
		Alternative Historical Attack	High	Kẻ tấn công tạo ra một phiên bản thay thế lịch sử blockchain và tìm cách khiến mạng chuyển sang phiên bản đó bằng cách tạo một nhánh từ blockchain hiện tại, sau đó sử dụng sức mạnh tính toán để đào các khối trên nhánh này, dẫn tới sự phân chia mạng.
		51% Attack	High	Kẻ tấn công kiểm soát hơn 50% sức mạnh đào khối của mạng (hash rate), cho phép kiểm soát và thao túng mạng.
		Grinding Attack	High	Grinding Attack là vấn đề xảy ra do cách thức triển khai và ảnh hưởng đế các hệ thống PoS. Bằng cách khai thác tính thiếu ngẫu nhiên trong quá trình biểu quyết chọn slot leader, có thể thao túng tần suất được bầu làm slot leader cho các khối tiếp theo.
		Coin Age Accumulation Attack	High	Coin age là một khái niệm trọng tâm trong các thuật toán PoS, được định tính bằng khoảng thời gian bất hoạt của một số lượng xu. Kẻ tấn công có thể tích lũy lượng lớn coin age bằng cách không sử dụng lượng lớn xu trong thời gian dài, có thể dẫn tới việc nhận được phần thưởng nhanh chóng trong vài phút, hoặc chiếm quyền điều khiển mạng lưới.
		Selfing Mining	High	Kẻ tấn công kiểm soát hơn 50% hash rate của mạng, cho phép chúng đào các khối nhanh hơn các node còn lại. Sau đó, kẻ tấn công lợi dụng quyền kiểm soát này để thực hiện selfish mining, là quá trình đào các khối trên blockchain riêng mà không truyền tin đến các node còn lại trong mạng cho đến khi chuỗi đạt độ dài nhất định.

Tầng sổ cái (Ledger Layer)	**Cơ chế đồng thuận**	**Block Double Production**	High	Kẻ tấn công tạo và công bố hai khối khác nhau ở cùng cao độ của blockchain. Điều này xảy ra khi kẻ tấn công kiểm soát hơn 50% hash rate của mạng, cho phép chúng khai thác các khối nhanh hơn các node còn lại trong mạng.
	Cơ chế mã hóa	**Cryptographic Attack**	High	Các kỹ thuật tấn công phổ biến: Analytic Attack / Implementation Attack / Statistical Attack / Brute Force / Frequency Analysis and the Ciphertext Only Attack / Known Plaintext / Chosen Ciphertext / Chosen Plaintext / Meet in the Middle / Man in the Middle / Birthday attack / Replay attack / Collision attack
		Private Key Prediction	High	Kẻ tấn công sử dụng nhiều phương pháp khác nhau để dự đoán private key tương ứng với địa chỉ công khai. Nếu thành công, kẻ tấn công có thể sử dụng các khoản tiền được liên kết với địa chỉ công khai mà chủ sở hữu không biết hoặc không đồng ý.
		Length Extension Attack	Low	Kiểu tấn công vào hàm băm mật mã cho phép kẻ tấn công kéo dài độ dài của tin gửi đi và tìm giá trị băm tương ứng mà không cần biết tin gốc hoặc giá trị băm của nó, được thực hiện bằng cách điều khiển trạng thái trong của hàm băm, thường dựa trên cấu trúc Merkle-Damgard.
		Hash Collision attack	High	Kiểu tấn công vào hàm băm mật mã cho phép kẻ tấn công tìm thấy hai đoạn tin khác nhau có cùng giá trị băm, còn được gọi là "va chạm" (collision), thực hiện bằng cách điều khiển trạng thái trong của hàm băm hoặc sử dụng các thuật toán toán học để tìm hai đoạn tin có cùng giá trị băm.
	Cơ chế giao dịch	**Double Spend Attack**	High	Kẻ tấn công tìm cách thực hiện giao dịch nhiều lần với một tài sản kỹ thuật số, có thể bằng cách tạo nhiều bản sao cho tài sản kỹ thuật số hoặc tạo các giao dịch xung đột sử dụng chung tài sản kỹ thuật số theo nhiều cách khác nhau.
		Transaction Malleability Attack	High	Kiểu tấn công mạng blockchain cho phép kẻ tấn công thay đổi ID giao dịch mà không thay đổi nội dung của giao dịch, được thực hiện bằng cách thao túng chữ ký số của giao dịch hoặc sửa đổi dữ liệu giao dịch một cách phù hợp.
	Cơ chế giao dịch	**Time-Locked Transaction Attack**	Low	Kẻ tấn công thao túng tính năng time-lock của một giao dịch để ngăn không cho giao dịch được thực hiện hoặc thực hiện sớm hơn dự định bằng cách điều chỉnh giá trị time-lock trong giao dịch hoặc thao túng thời gian hệ thống của các node liên quan đến giao dịch.
		False Top-Up Attack	High	Kẻ tấn công thao túng mạng để khiến tài khoản của người dùng được ghi nhận là nạp nhiều tiền hơn so với thực tế, có thể bằng cách tạo một bản ghi giao dịch giả hoặc thao túng các bản ghi.
		Rug Pull Attack	High	Kiểu tấn công vào giao thức tài chính phi tập trung (DeFi), trong đó một hoặc nhóm các tác nhân độc hại kiểm soát một lượng đáng kể thanh khoản trong thị trường hoặc bể thanh khoản cụ thể, rồi đột ngột rút thanh khoản đó, khiến giá trị của tài sản trong bể giảm đáng kể. Điều này dẫn đến tổn thất tài chính đáng kể cho những người tham gia thị trường.

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