

CyStack

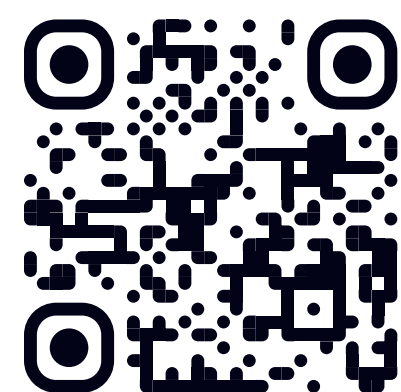
Bảo vệ dữ liệu

Kiểm thử & Đánh giá bảo mật

Vận hành an toàn

Ngăn chặn các mối đe dọa số, bảo vệ doanh nghiệp 24/7

CyStack giúp phát hiện sớm lỗ hổng, bảo vệ dữ liệu, và đảm bảo vận hành an toàn - để bạn yên tâm tập trung vào tăng trưởng



Đặt lịch tư vấn miễn phí
với CyStack ngay hôm nay



Giới thiệu về CyStack

CyStack là công ty an ninh mạng nổi bật tại Đông Nam Á, được biết đến với năng lực nghiên cứu, đổi mới sáng tạo, và các giải pháp được tin dùng bởi các tổ chức, doanh nghiệp hàng đầu.

Chúng tôi cung cấp các sản phẩm - dịch vụ chuyên sâu về 3 nhóm:

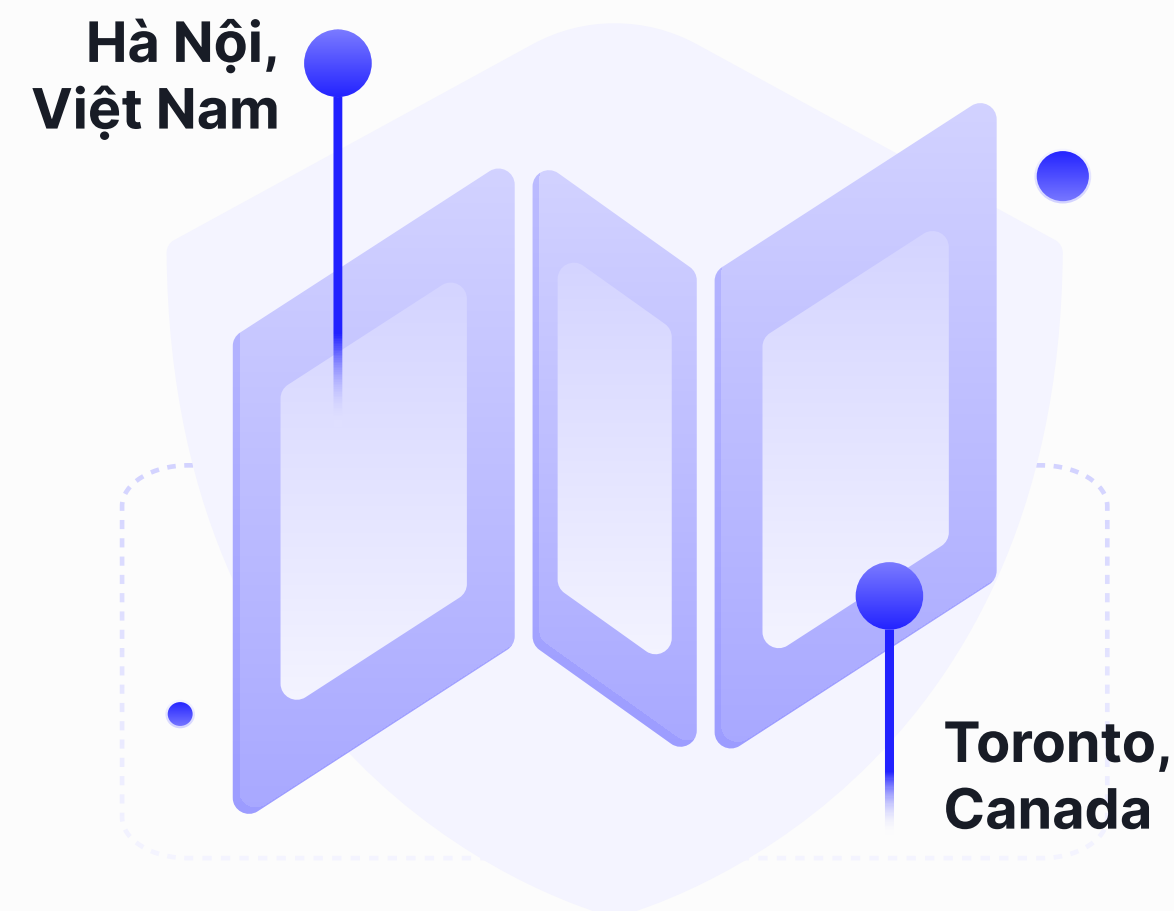
Bảo vệ dữ liệu

Kiểm thử & Đánh giá bảo mật

Vận hành an toàn

Cột mốc phát triển

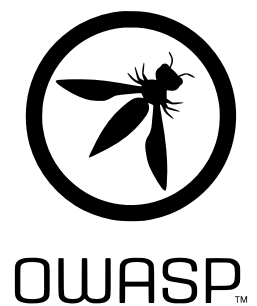
CyStack được thành lập năm 2017 tại Hà Nội và hiện đã mở rộng với chi nhánh tại Toronto, Canada



Thành viên của



Chứng nhận quốc tế



40+ Đội ngũ chuyên gia

15+ Giải pháp dịch vụ và sản phẩm về bảo mật

600+ khách hàng Doanh nghiệp

50.000+ khách hàng người dùng cá nhân

Đa dạng khách hàng từ doanh nghiệp quy mô vừa đến tập đoàn lớn nhất Việt Nam

Tìm hiểu thêm về các dự án của CyStack tại <https://cystack.net/vi/projects>

Chính phủ



Fintech



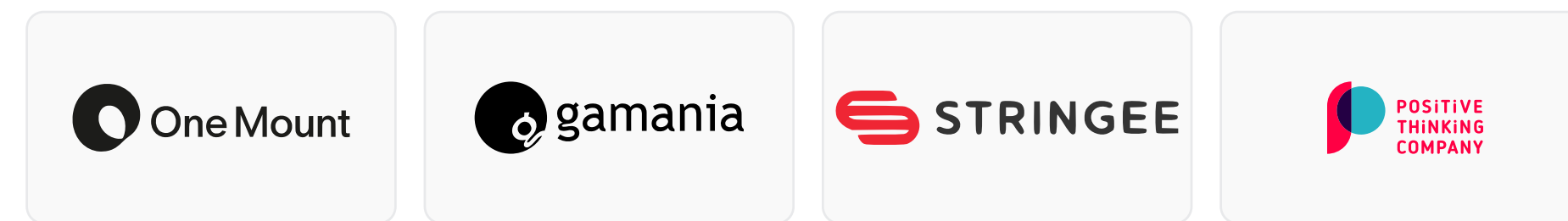
Công nghiệp



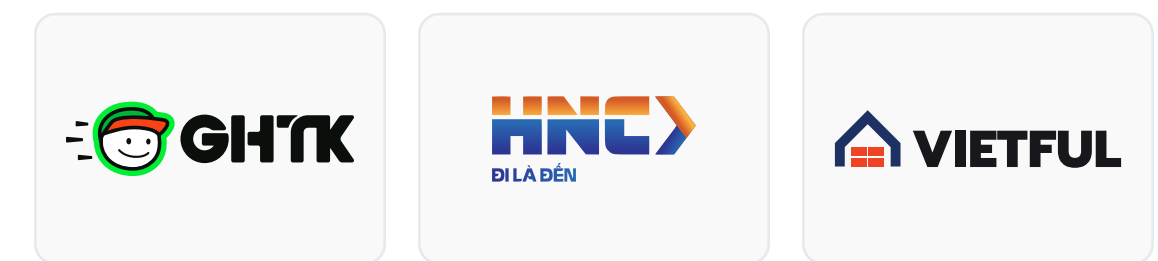
Ngân hàng



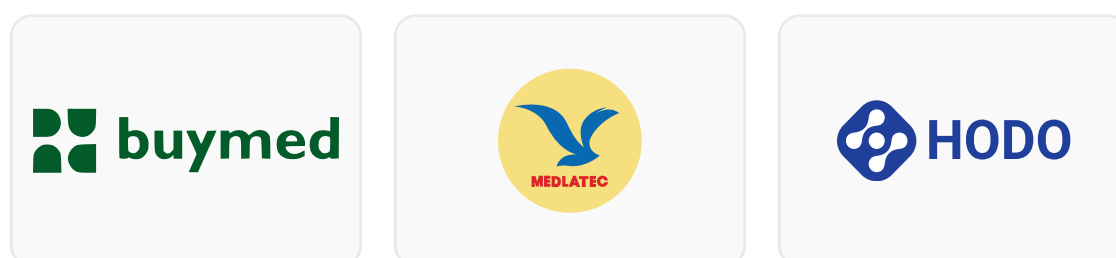
Công nghệ



Vận tải



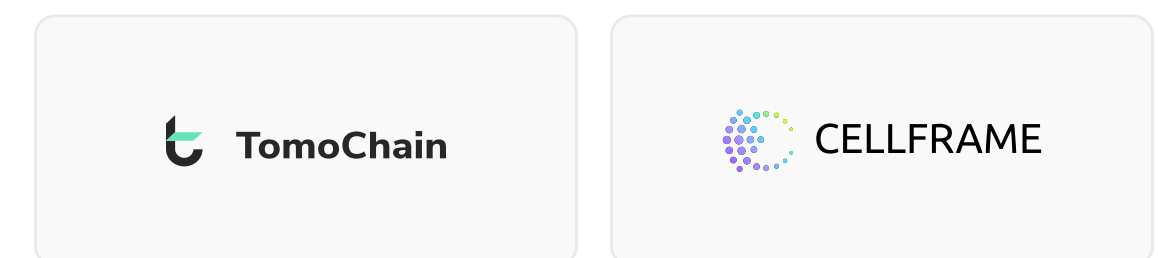
Y tế



TMĐT



Blockchain



Giải thưởng

 **Hiệp hội Phần mềm và Dịch vụ Công nghệ thông tin Việt Nam (VINASA)**
2025

- Sản phẩm công nghệ xuất sắc, xếp hạng 5 sao (Giải thưởng Sao Khuê)

 **(Make in Vietnam)**
Bộ Thông tin & Truyền thông Việt Nam
2024

- Sản phẩm công nghệ số xuất sắc trong lĩnh vực tài chính, ngân hàng, thương mại, dịch vụ.
- Sản phẩm số xuất sắc cho thị trường nước ngoài

 **(Make in Vietnam)**
Bộ Thông tin & Truyền thông Việt Nam
2023

- Sản phẩm công nghệ số xuất sắc cho thị trường nước ngoài
- Sản phẩm số xuất sắc cho xã hội số
- Sản phẩm số tiềm năng

 **Hiệp Hội Truyền thông số Việt Nam (VDCA)**
2021

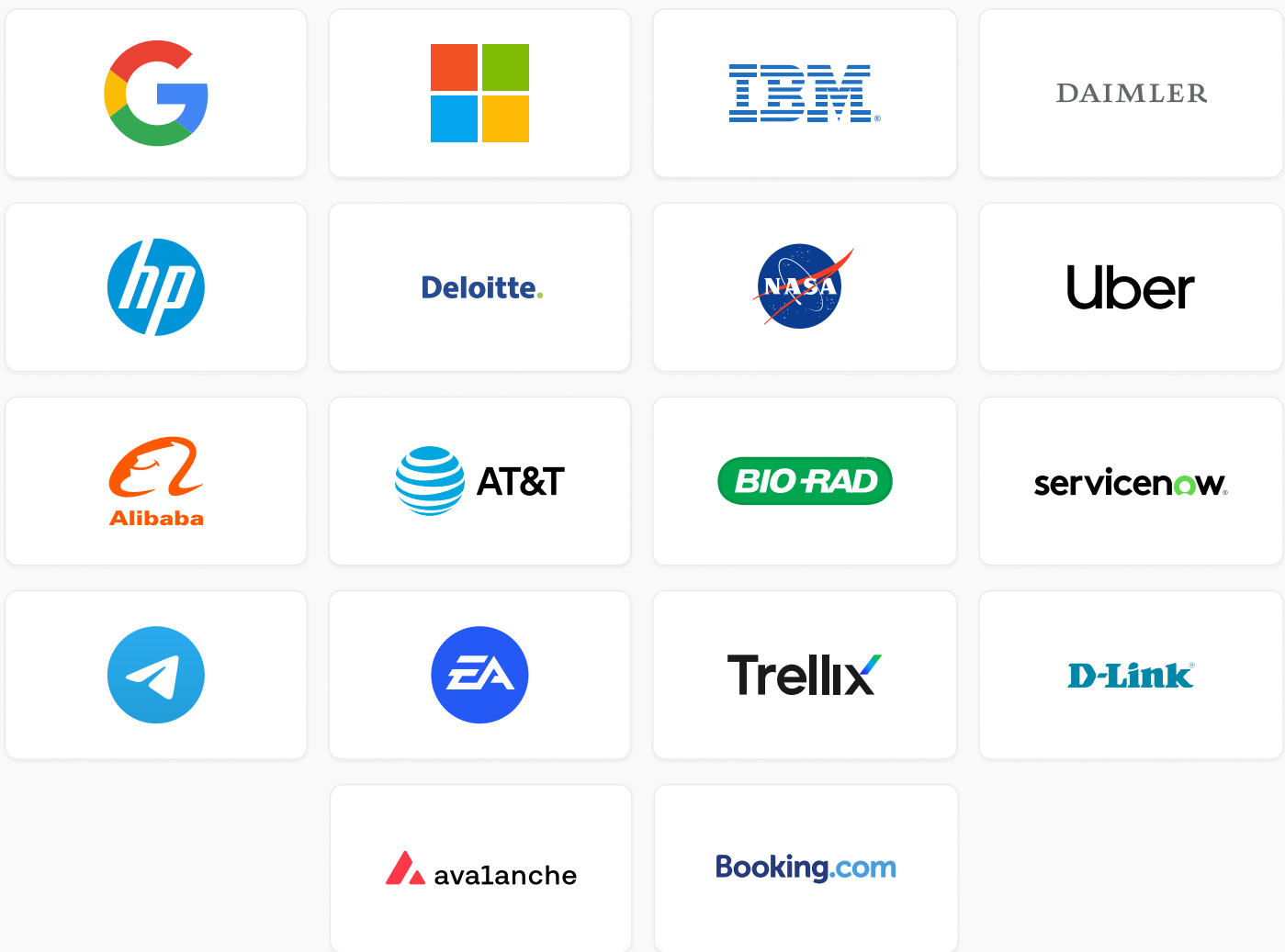
- Sản phẩm chuyển đổi số xuất sắc

 **Hiệp hội An toàn thông tin Việt Nam (VNISA)**
2021

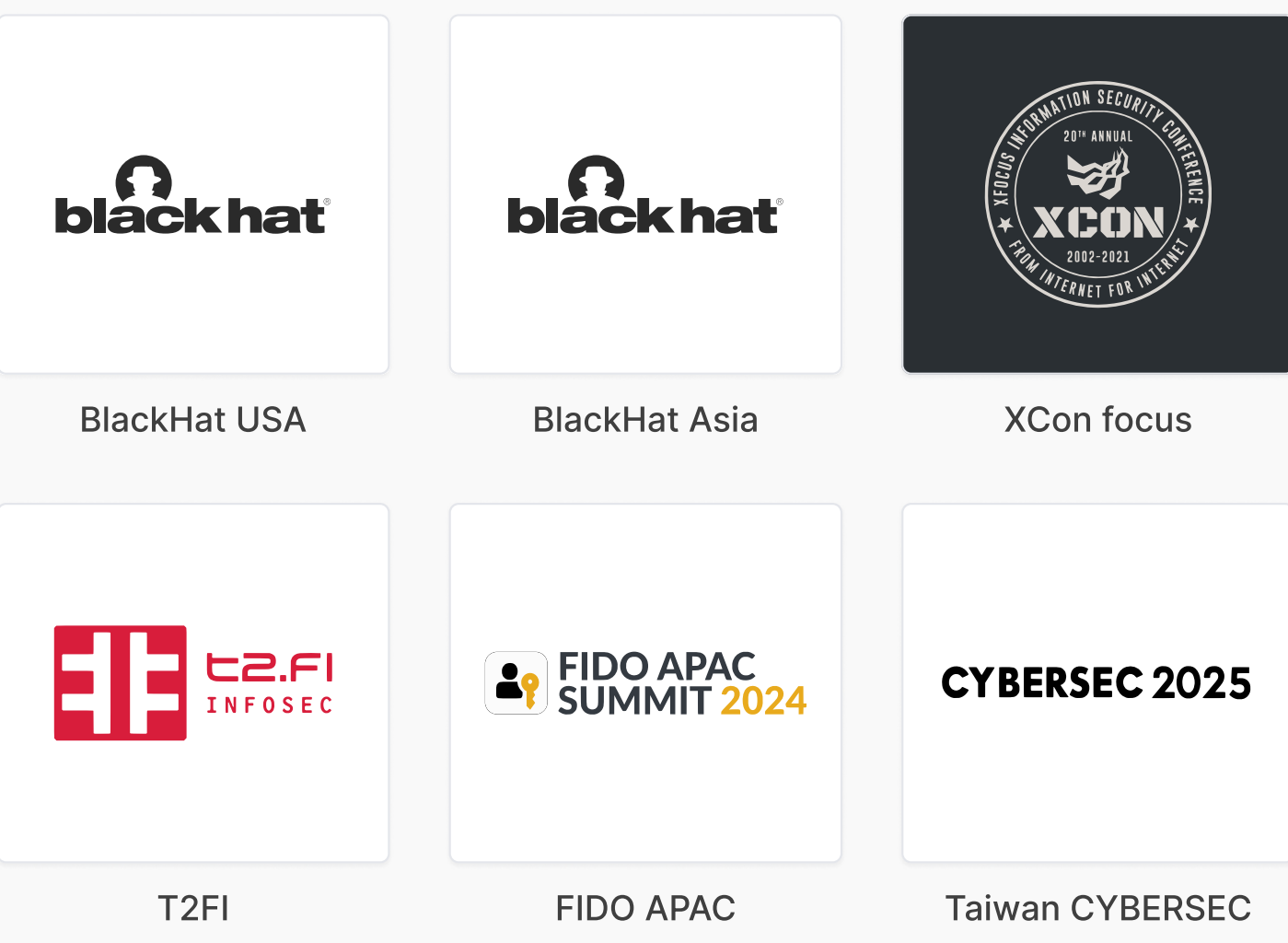
- Sản phẩm an toàn thông tin triển vọng xuất sắc
- Nền tảng ATTT tiêu biểu cho Chuyển đổi số
- Dịch vụ ATTT tiêu biểu

Được công nhận toàn cầu

nhờ đóng góp trong việc phát hiện và công bố có trách nhiệm các lỗ hổng bảo mật nghiêm trọng trong các sản phẩm và dịch vụ quan trọng



Tham luận tại các sự kiện quốc tế



Rủi ro mạng đang âm thầm đe dọa doanh nghiệp mỗi ngày!

Dữ liệu là huyết mạch, hệ thống là xương sống của doanh nghiệp, bất kể quy mô. Nhưng mỗi đe dọa thì xuất hiện ở khắp nơi, từ cả bên trong và bên ngoài.



Các giải pháp từ CyStack

CyStack không chỉ mang đến công nghệ, mà còn là người đồng hành đáng tin cậy của doanh nghiệp. Chúng tôi tư vấn giải pháp tối ưu và triển khai trọn gói: từ phòng ngừa, phát hiện, đến ứng phó - giúp bạn làm bảo mật đúng cách và hiệu quả.

Đánh giá & Kiểm thử bảo mật



Pentest

Kiểm thử xâm nhập



Red Teaming

Mô phỏng tấn công



CyStack VulnScan

Quét lỗ hổng tự động



WhiteHub Bug Bounty

Nền tảng săn lỗi nhận thưởng



Đánh giá hạ tầng

Đánh giá hạ tầng CNTT



Đánh giá Blockchain

Đánh giá smart contract và protocol

Bảo vệ dữ liệu



CyStack Endpoint

Phần mềm quản lý thiết bị nội bộ



Locker

Phần mềm quản lý mật khẩu và dữ liệu bí mật



Data Leak Detection

Phần mềm phát hiện rò rỉ dữ liệu

Vận hành hệ thống an toàn



SOC

Trung tâm điều hành bảo mật



Quản lý lỗ hổng bảo mật

Săn lỗ hổng liên tục



Đào tạo

Nâng cao nhận thức & quy trình



Điều tra số

Xử lý các sự cố an ninh

Các giải pháp từ CyStack

Kiểm thử & Đánh giá bảo mật

Phát hiện lỗ hổng, đánh giá rủi ro, và kiểm thử hệ thống từ hạ tầng đến mã nguồn - giúp doanh nghiệp chủ động bảo vệ trước khi bị tấn công



Kiểm thử xâm nhập (Pentest)

Mô phỏng các cuộc tấn công mạng thực tế vào ứng dụng, API, hạ tầng cloud, hoặc hệ thống nội bộ để phát hiện lỗ hổng trước khi hacker kịp khai thác



Red Teaming

Mô phỏng các cuộc tấn công tinh vi như hacker APT thực thụ, nhằm kiểm tra khả năng phát hiện, phản ứng, và phòng thủ đa lớp của hệ thống



Nền tảng săn lỗi nhận thưởng (bug bounty) WhiteHub

Kết nối doanh nghiệp với cộng đồng 4.000+ hacker mũ trắng uy tín để nhanh chóng phát hiện lỗ hổng bảo mật, đảm bảo kết quả tối ưu với chi phí hợp lý



Phần mềm quét lỗ hổng CyStack VulnScan

Tự động phát hiện và cảnh báo lỗ hổng trên IP, website, máy chủ, và tài nguyên đám mây, tích hợp vào CI/CD và báo cáo theo thời gian thực



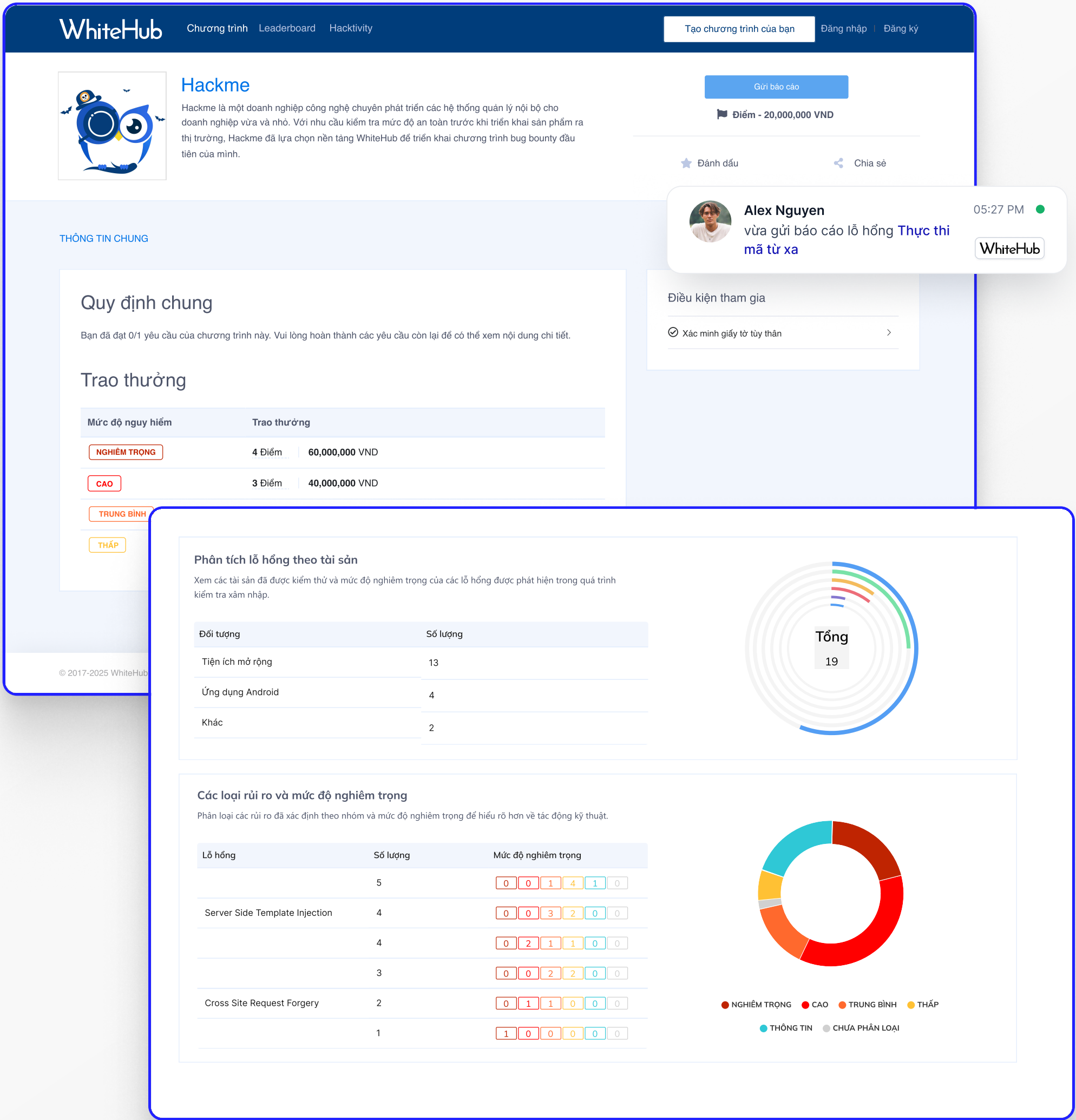
Đánh giá blockchain

Đánh giá và rà soát mã nguồn toàn diện cho smart contract và giao thức blockchain, phát hiện lỗi logic, vấn đề phân quyền, và lỗ hổng bảo mật



Đánh giá hạ tầng

Rà soát chuyên sâu thiết kế mạng, cấu hình hệ thống, firewall, cloud, và các điểm dễ bị tấn công trong hạ tầng CNTT để phát hiện rủi ro



Các giải pháp từ CyStack

Bảo vệ dữ liệu

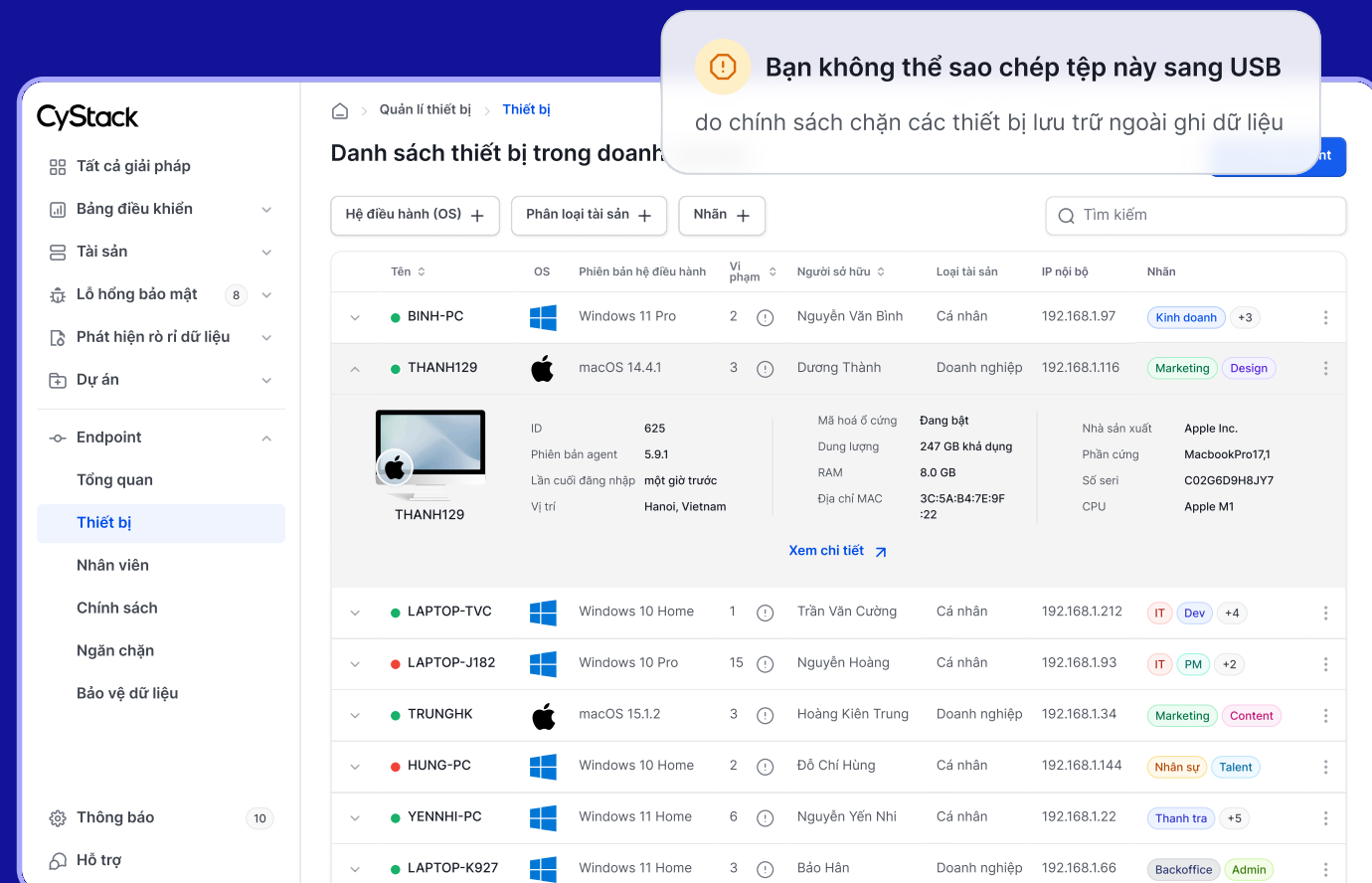
Bảo vệ thiết bị đầu cuối, kiểm soát truy cập, quản lý mật khẩu, giám sát và phát hiện rò rỉ dữ liệu



Endpoint

Phần mềm quản lý thiết bị nội bộ

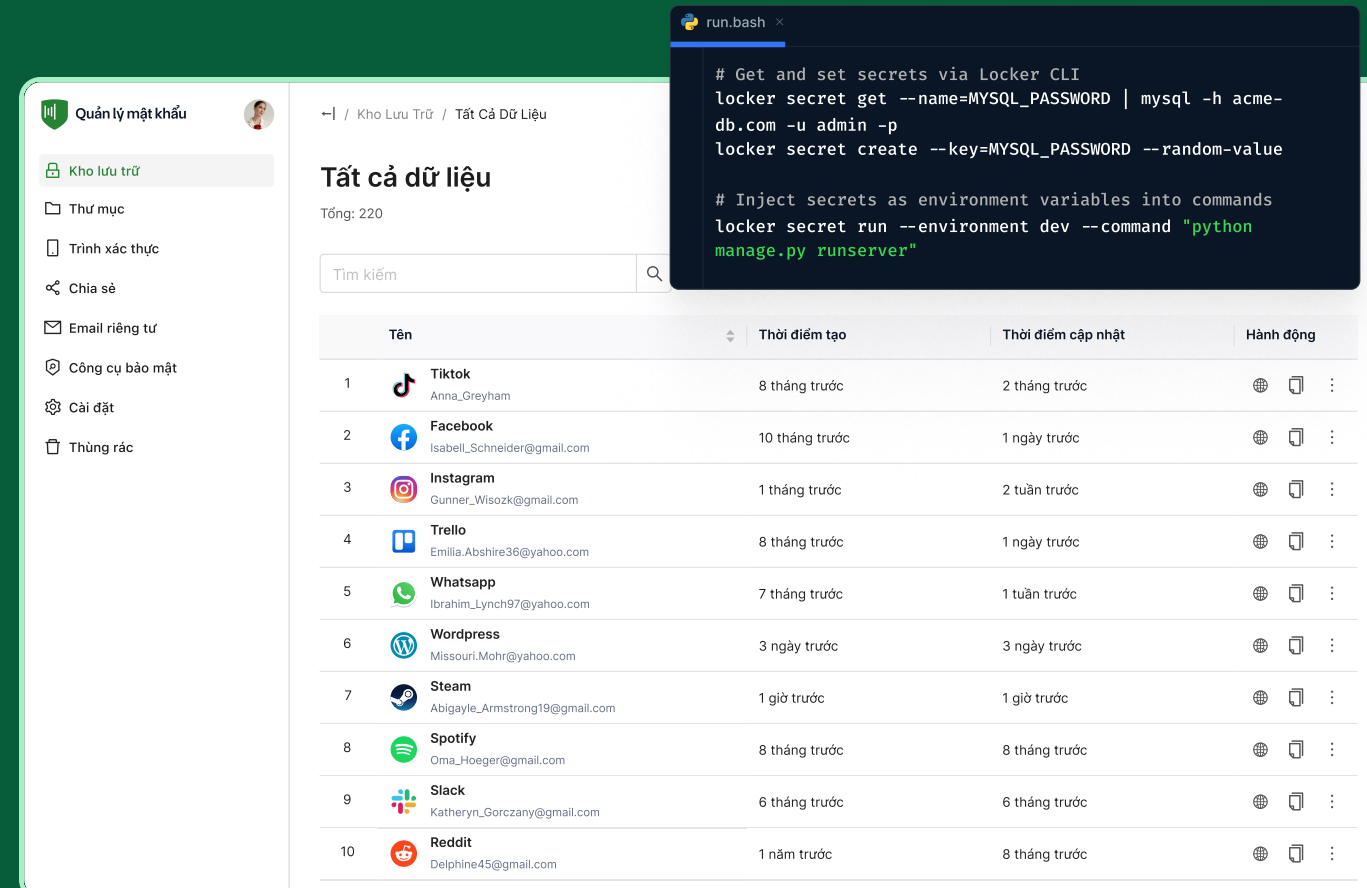
Quản lý tập trung thiết bị, giám sát hoạt động người dùng, kiểm soát truy cập, và bảo vệ dữ liệu trên máy tính, laptop, và các thiết bị di động



Locker

Phần mềm quản lý mật khẩu và dữ liệu bí mật

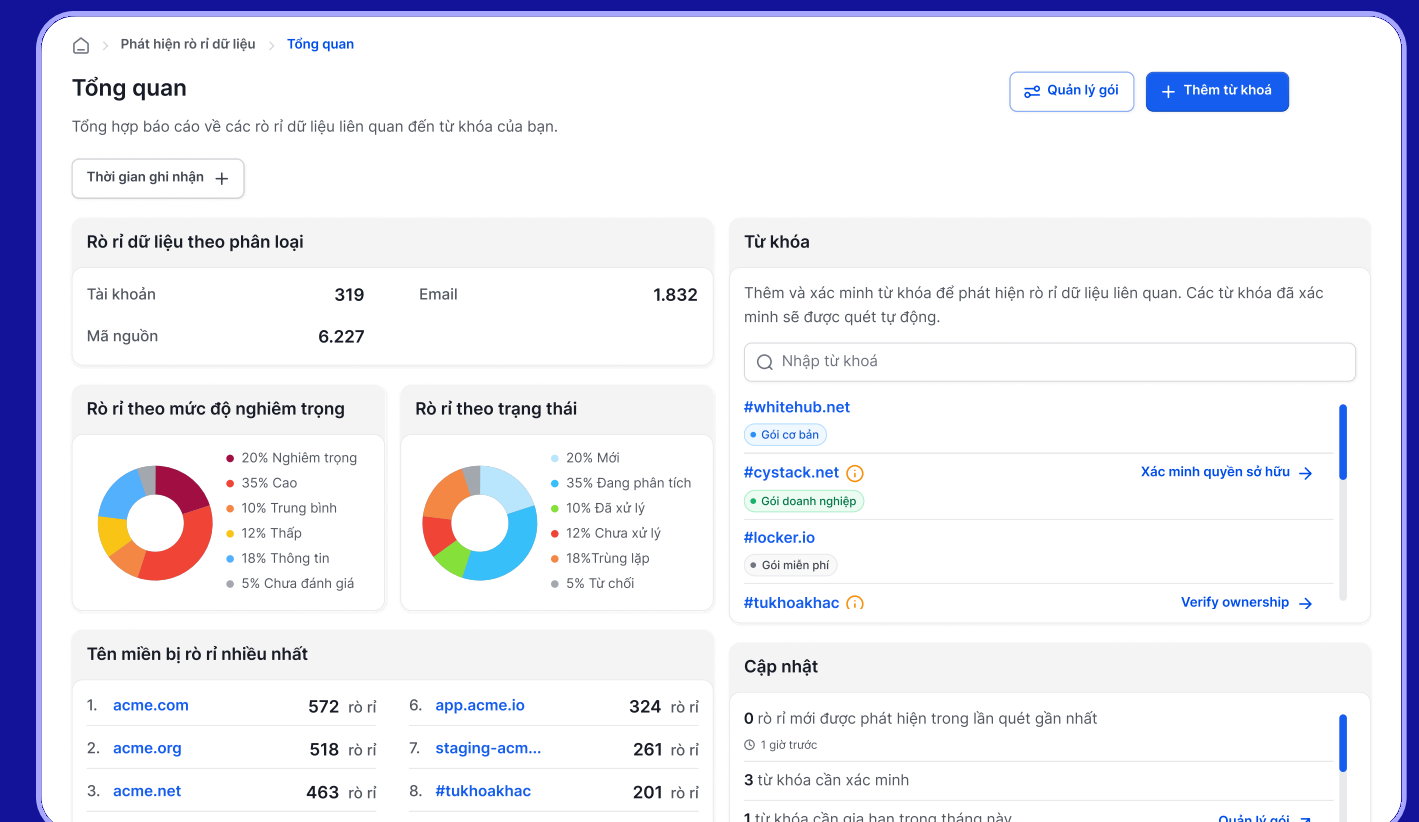
Quản lý mật khẩu, API key, token, và secrets cho cá nhân, doanh nghiệp, và lập trình viên với kho lưu trữ mã hóa, chia sẻ an toàn, và kiểm soát truy cập chi tiết



Data Leak Detection

Phần mềm phát hiện rò rỉ dữ liệu

Giám sát theo thời gian thực để phát hiện dữ liệu nhạy cảm bị rò rỉ trên dark web, diễn đàn hacker, và các nguồn công khai; hỗ trợ xử lý dữ liệu rò rỉ



Các giải pháp từ CyStack

Vận hành an toàn

Cung cấp dịch vụ giám sát 24/7, quản lý lỗ hổng, ứng phó sự cố, và đào tạo - giúp doanh nghiệp duy trì trạng thái an toàn liên tục

Quản lý lỗ hổng

Phát hiện, phân loại, ưu tiên, và theo dõi xử lý lỗ hổng bảo mật liên tục, kết hợp báo cáo tiến độ theo thời gian thực, giúp giảm rủi ro và tăng tốc độ xử lý

Trung tâm điều hành bảo mật (SOC)

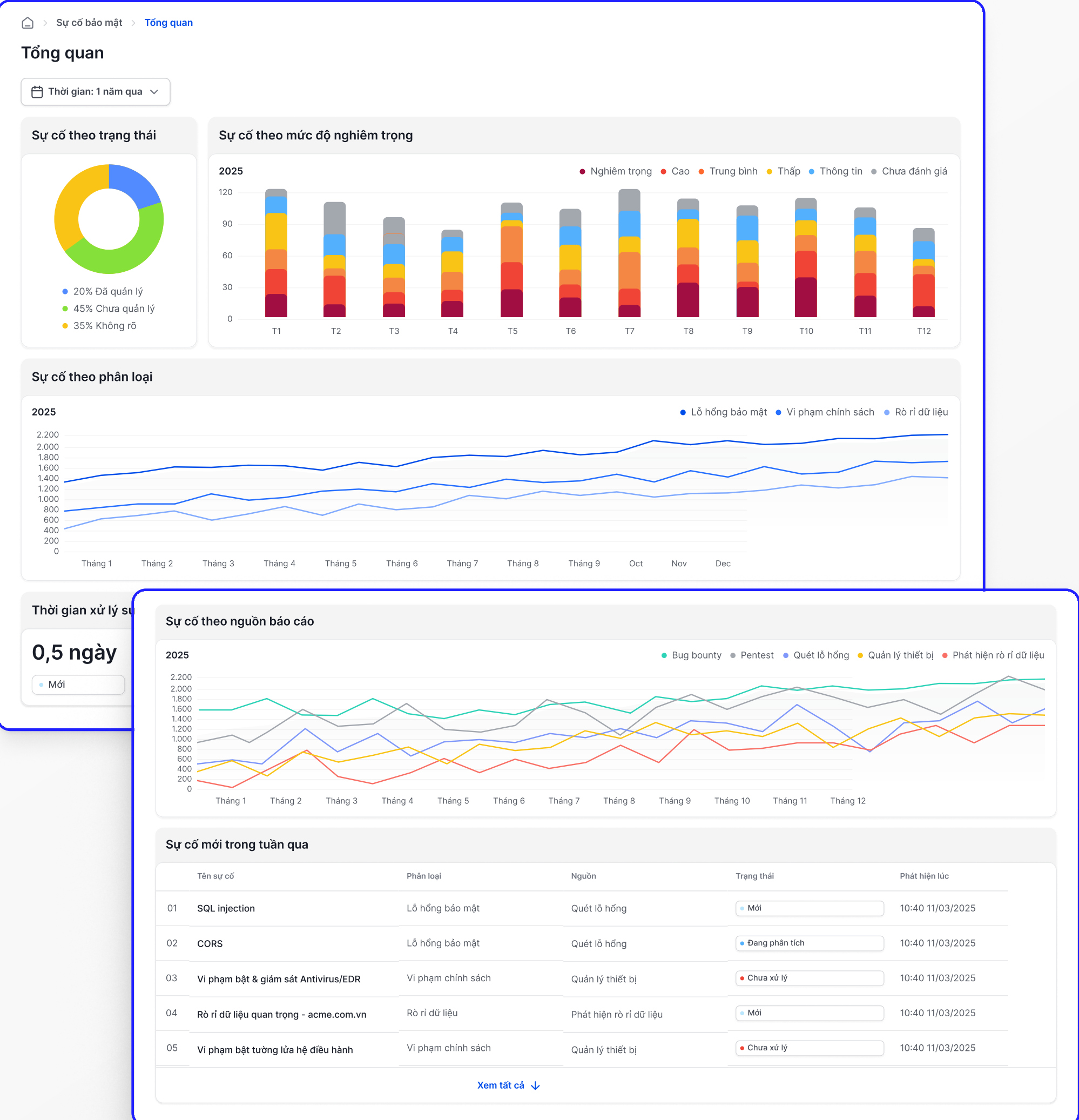
Giám sát 24/7, phát hiện mỗi đe dọa, và phản ứng sự cố theo thời gian thực với quy trình phân tích log, xử lý cảnh báo, và điều tra chuyên sâu

Điều tra số

Phản ứng nhanh khi có sự cố an ninh mạng và điều tra chuyên sâu để truy vết nguyên nhân, điểm xâm nhập, và hệ thống bị ảnh hưởng

Đào tạo

Đào tạo bảo mật thực tiễn cho nhân sự kỹ thuật và phi kỹ thuật: lập trình an toàn, nhận diện phishing, xử lý sự cố, và các kiến thức nền tảng khác



Điều gì làm CyStack khác biệt?

Vừa là chuyên gia bảo mật, vừa là nhà phát triển phần mềm, chúng tôi hiểu cách hệ thống được thiết kế, xây dựng, và triển khai cũng như cách chúng bị khai thác, từ đó nhận diện chính xác các rủi ro



Quản lý bảo mật bằng công nghệ

Nền tảng tập trung giúp:

- Quản lý lỗ hổng, theo dõi tiến độ dự án kiểm thử
- Giám sát theo thời gian thực, tích hợp AI
- Minh bạch, liền mạch, kiểm soát rủi ro tối đa

→ Giúp lãnh đạo có cái nhìn toàn cảnh và quyết định nhanh



Kết hợp Hack & Dev

Chúng tôi kết hợp tư duy hacker và kinh nghiệm phát triển phần mềm:

- Hiểu hệ thống sâu như lập trình viên, phát hiện rủi ro thực tế
- Đưa ra giải pháp khả thi, tối ưu cho vận hành
- Không chỉ báo lỗi mà còn giúp doanh nghiệp vá và chạy an toàn

→ Biến bảo mật thành giá trị thực tiễn, giảm gián đoạn và chi phí



Bảo mật cộng đồng

WhiteHub - nền tảng săn lỗi nhận thưởng (bug bounty) tiên phong và lớn nhất tại Việt Nam hiện nay với 4.000+ chuyên gia:

- Kết nối doanh nghiệp tới các chuyên gia bảo mật chất lượng cao
- Phát hiện & xử lý lỗ hổng hiệu quả gấp 3,5 lần thông thường
- Tùy chỉnh chương trình phù hợp từng doanh nghiệp

→ Tận dụng sức mạnh cộng đồng chuyên gia đa dạng góc nhìn



Đội ngũ chuyên gia được kiểm chứng

Chúng tôi sở hữu đội ngũ kỹ sư bảo mật được công nhận toàn cầu:

- Diễn giả tại các hội thảo hàng đầu: BlackHat USA, CYBERSEC,...
- Được vinh danh trong bảng vàng (Hall of Fame) của IBM, Microsoft, NASA, D-Link... nhờ phát hiện lỗ hổng nghiêm trọng
- Kinh nghiệm bảo mật cho các doanh nghiệp và tổ chức đa ngành

→ Tư vấn và thực hiện bởi đội ngũ thực chiến, chuẩn quốc tế

Hiệu quả thực tế từ giải pháp của CyStack



Agribank là ngân hàng thương mại nhà nước lớn nhất cả nước, thuộc **Top 200 ngân hàng toàn cầu** và là thành viên chủ chốt của **Big 4** ngành ngân hàng Việt Nam.

Với hơn 2.300 chi nhánh, 40.000+ nhân sự và 20+ triệu khách hàng, Agribank đóng vai trò then chốt trong tài chính nông thôn và tiên phong chuyển đổi số trong lĩnh vực.

01 / Thách thức

Là ngân hàng có hệ thống phân tán quy mô lớn, Agribank đối mặt với nhiều thách thức trong việc đảm bảo an toàn cho cả ứng dụng nghiệp vụ lẫn hạ tầng vận hành

- ⚠ Bảo vệ ứng dụng tùy biến cao, tích hợp bên thứ ba
- ⚠ Đánh giá hạ tầng phân tán quy mô lớn
- ⚠ Giảm rủi ro mạng từ dịch vụ mở cổng và phân vùng mạng
- ⚠ Tự động hóa kiểm tra lỗi hỏng định kỳ
- ⚠ Phát hiện lỗi hỏng tiềm ẩn, đặc biệt là lỗi logic, sai phân quyền và cấu hình sai trong hệ thống phức tạp

02 / Phạm vi triển khai

📖 Ứng dụng Web & API

- Hệ thống quản lý & cổng nội bộ
- Hệ thống thanh toán song phương
- Hệ thống IPCAS liên ngân hàng

📖 Hạ tầng hệ thống

- Máy chủ & hệ điều hành (Linux/Windows)
- Thiết bị mạng & phân vùng hệ thống
- Máy chủ cơ sở dữ liệu (DB Server)

03 / Giải pháp từ CyStack

CyStack đồng hành cùng Agribank kiểm thử thực chiến và củng cố bảo mật, đáp ứng tiêu chuẩn an ninh thông tin ngành ngân hàng

- 🔍 Kiểm thử xâm nhập (Penetration Testing)
- 🔍 Củng cố hạ tầng (Infrastructure Hardening)
- 🔍 Quét lỗi hỏng tự động (Vulnerability Scanning)

04 / Kết quả

- ✅ Phát hiện và xử lý nhiều lỗi nghiêm trọng trước khi bị khai thác
- ✅ **Giảm 70%** nguy cơ bị tấn công mạng nhờ mô phỏng kịch bản tấn công thực tế từ hacker
- ✅ **Tiết kiệm 50%** chi phí và thời gian xử lý sự cố hạ tầng nhờ tối ưu cấu hình mạng, phân vùng và truy cập
- ✅ **Đảm bảo 100%** hệ thống đạt chứng nhận kiểm thử bảo mật từ CyStack, phục vụ kiểm toán và chứng minh tuân thủ

Hiệu quả thực tế từ giải pháp của CyStack



dzcard thuộc Top 10 nhà cung cấp thẻ thanh toán thông minh hàng đầu thế giới, với hơn 50 năm kinh nghiệm, sản xuất hơn 65 triệu thẻ mỗi năm, và hiện diện tại 40+ quốc gia.

Công ty cung cấp đa dạng sản phẩm như thẻ ngân hàng, thẻ chip EMV, thẻ sinh trắc học, thẻ không tiếp xúc cho các ngân hàng, tổ chức tài chính, chính phủ, và nhà mạng viễn thông.

01 / Thách thức

dzcard phải duy trì mức độ bảo mật cực kỳ nghiêm ngặt trên toàn chuỗi sản xuất và vận hành.

- ❗ Bảo vệ hệ thống kết nối khỏi các cuộc tấn công nâng cao như chuỗi cung ứng và phần mềm nhúng
- ❗ Phát hiện và xử lý sớm lỗ hổng bảo mật
- ❗ Ngăn chặn gian lận, sao chép thẻ, và tấn công vật lý
- ❗ Tuân thủ các tiêu chuẩn bảo mật quốc tế
- ❗ Duy trì khả năng kiểm soát và truy vết

02 / Phạm vi triển khai

Lỗi hệ thống phát hành thẻ tại dzcard để xử lý dữ liệu nhạy cảm và kết nối trực tiếp với chuỗi thanh toán toàn cầu

- 📖 Thiết kế kiến trúc hệ thống
- 📖 Hệ thống quản lý khóa
- 📖 Hệ thống quản lý thẻ
- 📖 Ứng dụng desktop tích hợp thiết bị phần cứng

03 / Giải pháp từ CyStack

Kiểm thử xâm nhập (Penetration Testing) với 2 cách thức:

- 💡 **Whitebox Pentest:** Để phát hiện sớm lỗi logic, cấu hình sai, và thuật toán mã hóa yếu, hỗ trợ đánh giá PCI DSS cũng như tăng cường bảo mật từ giai đoạn phát triển
- 💡 **Graybox Pentest:** Để kiểm tra luồng nghiệp vụ, quyền truy cập và mô phỏng tấn công thực tế

04 / Kết quả

- ✅ **100%** kiến trúc hệ thống được rà soát từ đầu, phát hiện sớm điểm yếu và tối ưu phương án triển khai bảo mật trước khi đưa vào vận hành
- ✅ **Hệ thống DCDR (Data Center Disaster Recovery)** được thiết kế đạt chuẩn, đảm bảo khả năng sao lưu và khôi phục trung tâm dữ liệu khi xảy ra sự cố
- ✅ **Phát hiện & khắc phục điểm yếu** trong mã hóa, ưu tiên thành phần mật mã học, giúp tăng cường an toàn và hiệu quả hệ thống
- ✅ **100% kiểm thử đáp ứng PCI DSS** với báo cáo đầy đủ theo từng hệ thống, có log, phân loại rủi ro và hướng xử lý rõ ràng

Hiệu quả thực tế từ giải pháp của CyStack



Thành lập năm 2019 bởi Masan Group, Techcombank và Vingroup, **One Mount** là hệ sinh thái công nghệ hàng đầu Việt Nam, kết nối hàng triệu người dùng và doanh nghiệp nhỏ trong các lĩnh vực bán lẻ, tài chính và bất động sản.

Sản phẩm chiến lược:

- **VinShop**: Nền tảng B2B cho tạp hoá
- **VinID**: Ứng dụng tích điểm & ví điện tử
- **OneHousing**: Nền tảng bất động sản tích hợp

01 / Thách thức

- ! Theo kịp tốc độ phát triển và độ phức tạp hệ sinh thái
- ! Phát hiện lỗ hổng từ nhiều góc nhìn hacker, vượt qua giới hạn kiểm thử nội bộ
- ! Kiểm thử trực tiếp trên production, phản ánh rủi ro thực tế
- ! Giám sát và xử lý liên tục các lỗ hổng mới
- ! Đáp ứng chuẩn bảo mật quốc tế với dữ liệu người dùng và dịch vụ tài chính

03 / Giải pháp từ CyStack

- 💡 **Quản lý chương trình săn lỗi nhận thưởng (Managed Bug Bounty)**, với đội ngũ kiểm thử 4.000+ chuyên gia bảo mật độc lập.
- 💡 Giải pháp giúp phát hiện nhanh các lỗ hổng nghiêm trọng trong môi trường thực tế, giảm thời gian phân tích code, tăng góc nhìn tấn công và đảm bảo xác minh, phân loại lỗ hổng minh bạch, hiệu quả

02 / Phạm vi triển khai

Các nền tảng chủ chốt của One Mount cần giải quyết các rủi ro bảo mật nghiêm trọng ở quy mô lớn:

- 📖 **VinID**: Ứng dụng tích điểm, thanh toán không tiền mặt thông qua VinID Pay, hỗ trợ thanh toán hóa đơn, nạp điện thoại và ưu đãi tại WinMart/WinMart+
- 📖 **VinShop**: Nền tảng B2B giúp tạp hoá tiếp cận nguồn hàng đa dạng, đặt hàng linh hoạt, thanh toán thuận tiện và tham gia chương trình khuyến mãi

04 / Kết quả

- ✅ **3,5x** số lỗ hổng nghiêm trọng được phát hiện so với pentest truyền thống
- ✅ **< 48 giờ** Phát hiện và xử lý lỗ hổng nghiêm trọng đầu tiên - rút ngắn đáng kể so với thời gian trung bình 2-3 tuần trước đây
- ✅ **100%** lỗ hổng đều được khắc phục nhanh chóng với hướng dẫn chi tiết
- ✅ **10 triệu VNĐ** là chi phí trung bình để tìm một lỗ hổng nghiêm trọng (Critical), thấp hơn nhiều so với tổn thất trung bình do một vụ tấn công gây ra (trung bình \$4.45 triệu USD, theo IBM 2023)

Hiệu quả thực tế từ giải pháp của CyStack



Cellframe là nền tảng **blockchain** thế hệ mới của **Châu Âu**, với khả năng **bảo mật hậu lượng tử**, hỗ trợ ứng dụng phi tập trung nhanh và an toàn, được tin dùng bởi chính phủ và doanh nghiệp trong viễn thông, tài chính và IoT.

01 / Thách thức

Cellframe đối mặt với nhiều thách thức bảo mật quan trọng trước khi ra mắt:

- ⚠ Kiểm thử bảo mật bắt buộc trong 2 tuần
- ⚠ Xác minh giao thức hậu lượng tử và tương tác đa chuỗi
- ⚠ Phát hiện lỗ hổng ẩn trong mã nguồn mở tùy chỉnh
- ⚠ Mô phỏng tấn công tài khoản đặc quyền để đánh giá rủi ro hệ thống
- ⚠ Đảm bảo mở rộng, hiệu năng và tương thích đa chuỗi mà không giảm tính bảo mật

02 / Phạm vi triển khai

Bảo vệ toàn diện cho các lớp quan trọng của nền tảng Cellframe:

- 📖 Khung blockchain mã nguồn mở
- 📖 Các module AI và thuật toán hành vi
- 📖 Smart contract và cấu hình giao thức blockchain
- 📖 Ứng dụng frontend và tích hợp blockchain hướng người dùng
- 📖 Hạ tầng hệ điều hành, firmware và phần cứng IoT

03 / Giải pháp từ CyStack

CyStack đã cung cấp giải pháp bảo mật toàn diện, kết hợp giữa kiểm thử chuyên sâu do chuyên gia thực hiện và chương trình kiểm thử cộng đồng:

- 🔍 **Đánh giá hợp đồng thông minh** (Smart Contract Audit)
- 🔍 **Quản lý chương trình săn lỗi nhận thưởng** (Bug Bounty) qua WhiteHub với 4.000+ chuyên gia kiểm duyệt
- 🔍 **Đánh giá giao thức Blockchain**

04 / Kết quả

- ✅ **94%** báo cáo được chấp nhận
- ✅ **24%** lỗ hổng được phân loại Critical/High
- ✅ **<48** giờ để phát hiện và khắc phục các lỗi nghiêm trọng đầu tiên
- ✅ **100%** lỗ hổng hợp lệ được xử lý triệt để
- ✅ **\$78,500** tiền thưởng được chi trong 2 tuần - thúc đẩy sự tham gia của các chuyên gia hàng đầu

Đóng góp không ngừng cho cộng đồng bảo mật doanh nghiệp

viettel

Viettel là tập đoàn viễn thông - công nghệ lớn nhất Việt Nam, dẫn đầu thị phần di động (~60%).

Doanh nghiệp hiện diện tại **11 quốc gia** trên 3 châu lục; khối quốc tế phục vụ **90+ triệu** khách hàng và giữ vị trí số **1** ở 7/10 thị trường.

Trong nước, Viettel nhiều năm liên tục được Ookla ghi nhận đứng đầu về tốc độ mạng di động và băng rộng cố định, khẳng định vị thế **#1** ở các mảng hạ tầng số.

01 / Thách thức

Viettel sở hữu nhiều giải pháp phần mềm và công nghệ khác nhau

- ⚠ Bề mặt tấn công rộng, nhiều lớp hạ tầng và dịch vụ khác nhau như viễn thông, IoT, các ứng dụng số, giao thông,...
- ⚠ Nguy cơ từ tấn công chuỗi cung ứng và phụ thuộc bên thứ ba
- ⚠ Các giải pháp nội bộ hoạt động liên tục, với lượng người dùng hàng ngày (DAU) không ngừng tăng
- ⚠ Áp lực tuân thủ liên tục các yêu cầu về an toàn thông tin

02 / Phạm vi triển khai

Phát hiện các lỗ hổng trên các nền tảng của Viettel

- 📖 Ứng dụng và nền tảng trên thiết bị di động
- 📖 Dịch vụ, nền tảng số của Viettel và doanh nghiệp thành viên
- 📖 Hệ sinh thái điện toán đám mây hay tiếp cận với internet
- 📖 Các lỗ hổng liên quan đến chuỗi cung ứng phần mềm của Viettel
- 📖 Hạ tầng firmware và phần cứng IoT

03 / Đóng góp của CyStack

Các chuyên gia bảo mật của CyStack đã đóng góp vào quá trình phát hiện và hỗ trợ vá lỗ hổng cho Viettel

- 💡 **Trực tiếp tìm kiếm và kiểm thử** nhiều nền tảng, sản phẩm và dịch vụ của Viettel (ePass, Viettel Cloud, Viettel Money,...)
- 💡 **Báo cáo lỗ hổng mới** qua nền tảng Săn lỗi nhận thưởng (Bug Bounty) của Viettel
- 💡 **Hỗ trợ cung cấp PoC, thử nghiệm và tái kiểm thử** cho các nhóm phát triển phần mềm của Tập đoàn Viettel

04 / Kết quả

#1 nhóm chuyên gia bảo mật trên nền tảng

- ✅ **~90** lỗ hổng được chấp nhận bởi Viettel và tiếp tục phát hiện thêm các lỗ hổng mới
- ✅ **1800+** điểm đóng góp trên nền tảng Bug Bounty của đơn vị
- ✅ **100%** lỗ hổng hợp lệ được xử lý triệt để sau khi báo cáo đầu tiên từ các chuyên gia bảo mật của CyStack



Đối tác bảo mật tin cậy của bạn

CyStack không chỉ cung cấp sản phẩm, dịch vụ theo dự án. Chúng tôi đồng hành lâu dài cùng doanh nghiệp như một đối tác bảo mật: từ **tư vấn**, **thiết kế lộ trình**, đến **triển khai** giải pháp **bảo vệ dữ liệu và hệ thống tối ưu** - để bạn yên tâm tập trung vào tăng trưởng.

Đặt lịch tư vấn miễn phí với CyStack ngay hôm nay

CyStack

Văn phòng Việt Nam

📍 Tòa nhà Tân Hồng Hà, 317 Trường Chinh,
Hà Nội, Việt Nam

☎ (+84) 247 109 9656

Văn phòng Canada

📍 2376 Dundas St W, Toronto, Ontario
M6P 0C1, Canada.

☎ (+1) 437 361 5461

