cloudbric

DECENTRALIZED UNIVERSAL SECURITY PLATFORM

Whitepaper Ver. 4.9

General Release - Subject to Change

Cloudbric Executive Team

www.cloudbric.com/blockchain-security support@cloudbric.com

목차

현재 사이버 보안의 현실

세계가 점점 상호 연결된 인터넷 기반 사회로 이동함에 따라 개인 온라인 데이터를 안전하게 보호해야 할 필요성이 점차 커지고 있습니다.

사용자와 기업은 모두 다양한 온라인 채널의 공개된 정보 흐름으로 인해 사이버 해킹에 매우 취약합니다. 매년 수백만건의 개인 정보가 도난당하는 등, 중요한 온라인 데이터 유출 사건은 사상 최고치에 도달했습니다.

또한 사이버 공격은 암호화폐 자산 및 거래소와 같이 새롭게 떠오르는 시장으로 범위를 확장하고 있습니다. 작년 한해 동안 온라인 범죄자들에 의해 수천억 이상의 가치가 있는, 다양한 암호화폐 자금이 탈취당했습니다. 이는 모든 사용자들이 암호화폐 시장내에 있는 디지털 자산을 보호하는 것을 최우선 과제로 삼게 만듭니다.

사용자들은 증가하는 사이버 보안 문제에 대응하기 위해 모든 통신 채널(이메일, 웹사이트, 모바일 디바이스, 암호화폐 거래소 등)을 통과하는 개인 정보를 보호해야합니다. 그러나 시장에 존재하는 근본적인 문제들로 인해 여러 보안 솔루션을 적용하고 관리하는 것은 매우 어렵습니다. 결국 이로 인해 사용자가 광범위한 사이버 보안을 제대로 적용하지 못하게 됩니다.

사용자들이 직면하는 문제들

정보 보안 시장은 전반적으로 효율성, 투명성 및 신뢰에 중점을 둔 패러다임 전환이 필요합니다.
이는 사이버 보안 시장에서 사용자들이 직면하는 다양한 문제 때문입니다.

보안 솔루션의 과포화

사용자가 사용할 수 있는 솔루션은 수많은 온라인 채널의 정보를 보호해야 하기 때문에 과포화 되어 있습니다. 현재 전세계 사이버 보안 시장에는 1,600 개 이상의 솔루션이 제공되고 있어 각 보안 솔루션의 선택 프로세스가 지나치게 복잡합니다. 사용자는 유사한 솔루션을 제공하는 수많은 보안 업체를 테스트하고 적절히 판단 및 선택하기 위해 스스로 알아서 해결해야 합니다. 또한 서로 매우 다른 보안 플랫폼, 소프트웨어, 설정 구성, 가격 등에 적응하도록 사용자들이 강요 받기 때문에 이러한 다양한 솔루션의 관리는 매우 부담스러울 수 있습니다.

위에서 설명한 바와 같이 사이버 보안에 대해 단계적 접근 방식을 취한다는 발상은 그야말로 비효율적이고 시대에 뒤떨어진 것입니다. 연구에 따르면 일부 조직에서는 정보 보안과 관련된 많은 문제를 해결하기 위해 최대 70 개의 서로 다른 벤더가 만든 보안 솔루션을 사용하고 있습니다. 더 많은 보안 솔루션을 구축한다고 해서 반드시 보안이 더 강화되는 건 아닙니다. 실제로 솔루션을 더 많이 활용하면 사용자는 각 소프트웨어에서

발견되는 시스템 업그레이드 및 보안 버그를 더 잘 인식해야 하기 때문에 해킹에 훨씬 더 취약해 질 수 있습니다.

많은 사용자에게 사이버 보안은 매우 이질적이고 복잡한 주제입니다. 이로 인해 공급 업체는 사용자의 지식 부족을 이용하여 더 많은 개별적인 보안 솔루션을 제공하게 됩니다. 보안 업체는 더 이상 사용자 순진함을 이용하여 이익을 얻으려 하지 말고, 사용자가 진정으로 온라인에서 안전을 느낄 수 있도록 해 주는 통합 솔루션을 구축하는 데 초점을 맞추어야 합니다.

중앙화된 위협 정보 데이터

정보 보안 시장의 또 다른 이슈는 위협 정보에 대한 투명성의 결여입니다. 사이버 보안 업체는 사용자에게 솔루션을 제공하여 공격 행동 및 패턴, 악성 IP 주소, 멀웨어 감염 파일 식별 등과 같은 방대한 양의 사이버 위협 정보를 수집합니다. 그러나 이렇게 수집된 위협 정보 데이터는 사용자들은 공개적으로 접근 할 수 없습니다.

보안 업체는 일반적으로 이 정보를 사유화하여 회사의 이익을 위해 사용합니다. 예를 들어, 사이버 위협 데이터는 새로운 시장 솔루션을 개발하고, 관련 소프트웨어 업데이트를 배포하고, 업계 보고서 및 분석을 작성하는 데 사용되며, 이 모든 것이 수익의 중요한 원천이 될 수 있습니다. 반면, 보안 업체를 위해 이 데이터를 생성하는 데 도움을 주는 사용자에게는 보상이 전혀 없으며 공급 업체가 제공한 서비스에 대해서는 계속해서 비용을 지불해야 합니다. 이러한 불균형적인 위협 데이터의 중앙 집중화와 보상 체계는 이제 끝나야 합니다.

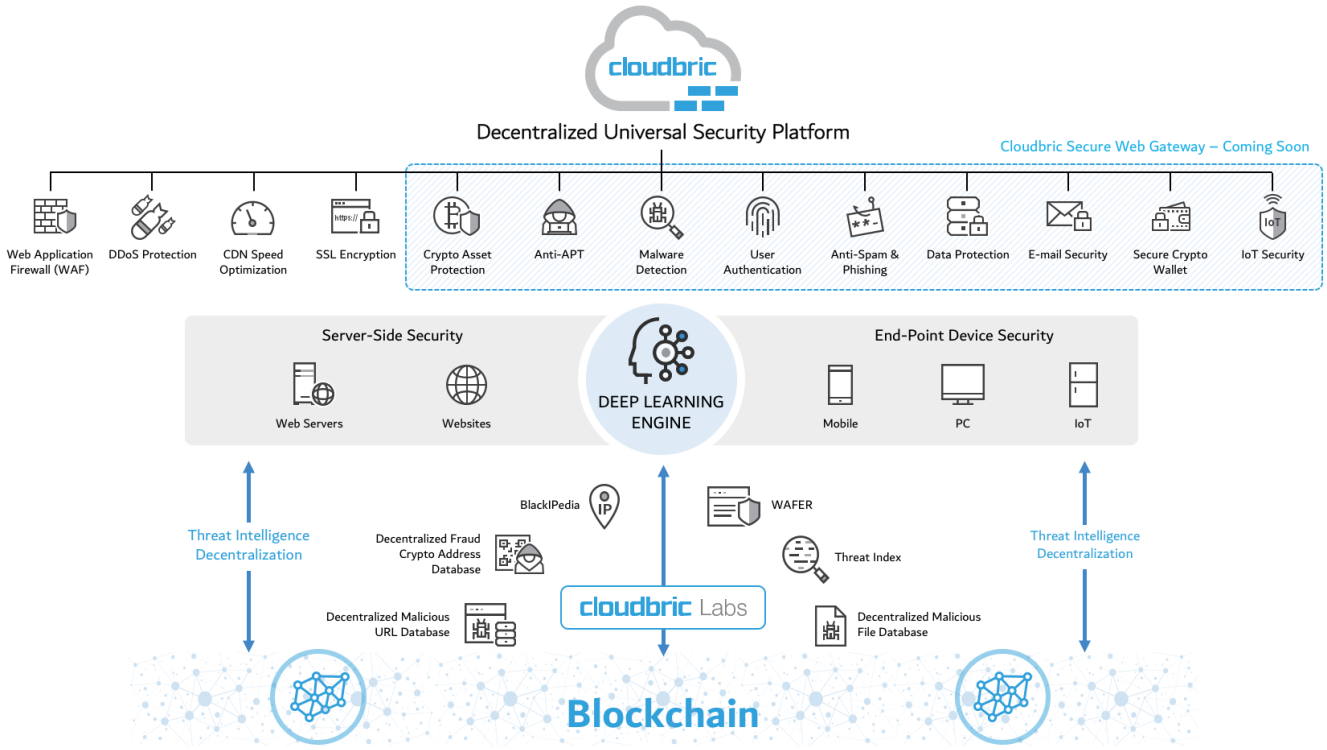
보안 성능의 불확실성

마지막으로, 현재 사이버 보안 시장에서 사용자들은 다양한 업체가 만든 솔루션의 효과를 파악하기가 매우 어렵습니다. 위에서 언급한 바와 같이, 시장은 정보 보안 업체와 솔루션의 과잉으로 인해 포화 상태에 있습니다. 사용자가 보안 업체 성능을 적절히 구별할 수 있는 유일한 방법은 이러한 솔루션을 직접 테스트하는 것뿐입니다. 하지만 이것은 매우 많은 노력 및 비용이 드는 일입니다.

사용자는 보안 솔루션에 대해 알아보고, 성능을 측정하고, 관리 및 구축이 쉬운지를 알아보기 위해 많은 시간과 비용을 투자해야 합니다. 하지만 일반 사용자나 소기업은 동시에 여러 보안 솔루션을 테스트하는데 필요한 리소스와 기능을 갖추지 못할 수 있습니다. 이로 인해 엔터프라이즈 기업만이 모든 사용자가 필요로 하는 범위의 보안에 대응 할 수 있는 유일한 고객으로 남게 되었습니다.

또한 많은 사이버 보안 업체가 자신의 보안 역량을 과도하게 홍보하지만, 신뢰할 수 있는 보안 업체가 되기에는 산업 경험이나 고성능 제품이 부족한 경우가 많습니다. 이것은 특히 보안 전문 지식이 부족한 사기 회사가 만연해 있는 ICO 분야에서 더욱 그러합니다.

해결책 제안



클라우드브릭(Cloudbric)의 주요 임무는 새로운 **분산화된 통합 보안 플랫폼**의 도입을 통해 모든 사용자에게 정보 보안을 개방하여 사이버 보안 시장에 혁명을 일으키는 것입니다. 이 AI 기반의 사이버 보안 플랫폼은 클라우드브릭의 특허 진행중인 딥러닝 모듈 비전(VISION)을 기반으로 하며, 모든 포괄적인 사이버 보안 솔루션을 제공할 뿐만 아니라, 새로운 분산화 보안 생태계를 개발할 것입니다.

나아가 사용자들은 익명의 사이버 위협 정보를 제공하여 온라인 디지털 자산을 보호하는데 도움이 되는 딥러닝 기술에 힘을 실어줄 수 있습니다. VISION 의 성장 및 고급 학습 기능에 대한 공헌으로 클라우드브릭은 무료 클라우드브릭 암호화폐(CLB)를 사용자에게 제공합니다. CLB 토큰은 클라우드브릭에서 제공하는 솔루션들 또는 클라우드브릭의 광범위한 파트너 네트워크에서 독점 제공되는 서비스들에 사용할 수 있습니다.

이 목표를 달성하기 위해 클라우드브릭은 보안 효율성, 데이터 투명성 및 사용자 신뢰를 시장에 알리는 데 주력할 것입니다.

보안 효율성

클라우드브릭은 여러 보안 솔루션을 단일 통합 플랫폼으로 통합하여 다양한 범위의 사용자를 위한 손쉬운 사이버 보안 관리를 제공합니다. 플랫폼 내에서 제공되는 솔루션은 서버측 보안(웹 사이트), 개인 보안(PC, 모바일 및 IoT 연결 장치) 및 암호화폐 자산 보호(CLB 보안 지갑 포함)의 3 가지 주요 보안 구성에 중점을 둡니다. 이를 통해 모든 사용자는 엔터프라이즈 수준의 웹사이트 보안, CDN 속도 최적화, 지능형 악성코드 방지, 스팸 / 피싱 방지, 암호화폐 사기 방지 등을 누릴 수 있습니다.

데이터 투명성

VISION 의 딥러닝 탐지 알고리즘에 의해 탐지된 모든 사이버 위협 정보(악의적인 IP, 스팸 URL 목록, 사기성 암호화폐 주소 등)는 데이터 투명성 및 보안 보상(Security Reward)에 초점을 맞춘 분산화 보안 생태계의 개발을 통해 접근이 가능하게 됩니다.

새롭게 개발되는 분산화 보안 생태계의 첫 모습은 클라우드브릭 랩스(https://labs.cloudbric.com)를 중심으로 전개될 것입니다. 클라우드브릭 랩스(베타 버전 사용 가능)는 대중에게 위협 정보를 공개하고 액세스 할 수 있는 이미 수상 경력이 있는 보안 리소스 커뮤니티입니다. 예전엔 꺼려하던 사이버 위협 정보를 분산화 시키고자 하는 클라우드브릭의 목표는 미래의 개발자, 조직 및 일반 보안 커뮤니티들을 대상으로 사이버 보안에 대한 혁신과 인식을 촉발시키는 데 도움이 될 것입니다.

다음으로, 분산화 보안 생태계의 두번째 구성 요소는 클라우드브릭의 보안 보상 프로그램(Security Rewards Program)의 출시에 중점을 둘 것입니다. 사용자는 온라인 데이터를 보호하는 보안 기술을 발전시키는 데 도움을 줄 수 있습니다. 사이버 위협 로그 및 정보를 VISION 또는 클라우드브릭 랩스 커뮤니티에 기여함으로써 클라우드브릭 사용자는 새로운 "보안을 통한 보상(Secure to Earn)" 프로그램에 참여하고 무료 CLB 토큰을 배포 받을 수 있습니다. 사용자 CLB 거래 내역 뿐만 아니라 모든 CLB 토큰의 배포 역시 공개적이고 신뢰할 수 있는 검증을 위해 블록체인에 기록됩니다.

유저 신뢰

클라우드브릭은 새로운 사용자 중심의 보안 기술 및 서비스를 개발하여 보안 커뮤니티에 권한을 부여하고 차세대 사이버 보안의 발전을 도모함으로써 보안 영역을 확장 할 것입니다. 클라우드브릭은 20 년 이상의 검증된 사이버 보안 전문 지식을 바탕으로 풍부한 지식과 보안 서비스 경험을 ICO 시장에 제공할 것입니다.

또한 클라우드브릭은 시장에 나와있는 다른 전형적인 ICO 사이버 보안 업체와도 다릅니다. 클라우드브릭은 다양한 수상 경력을 보유하고 있는 신뢰할 수 있는 싱가폴 기반의 글로벌 웹 보안 업체입니다. 좀 더

구체적으로, 클라우드브릭의 웹 보안 기술은 Gartner 및 Frost & Sullivan 과 같은 보안 분석가들에 의해 APAC 지역 1 위와 글로벌 5 위의 솔루션으로 인정 받고 있습니다.

클라우드브릭 배경

2015 년 초, 클라우드브릭은 한국 및 APAC 지역 1 위인 기업용 웹보안 및 데이터 암호화 회사 펜타시큐리티시스템의 사내 벤처로 시작했습니다. 클라우드브릭은 WAPPLES 로 알려진 펜타시큐리티의 시장 선도적인 하드웨어 웹방화벽 (Web Application Firewall, WAF)의 클라우드 기반 글로벌 보안 서비스(Security-as-a-Service)로 출시되었습니다.

클라우드브릭은 통합 WAF 서비스 사용에 관심이 있는 일반 웹사이트 소유자 뿐만 아니라 중소기업을 대상으로 신속하게 틈새 시장을 개척하기 시작했습니다. 클라우드브릭은 사용자의 요구에 제대로 부합하는 엔터프라이즈 수준의 솔루션을 제공함으로써 보안 초심자들이 사이버 보안에 대해 더욱 익숙해지게 하는데 도움을 주었습니다.

Cloudbric Pte. Ltd. 설립

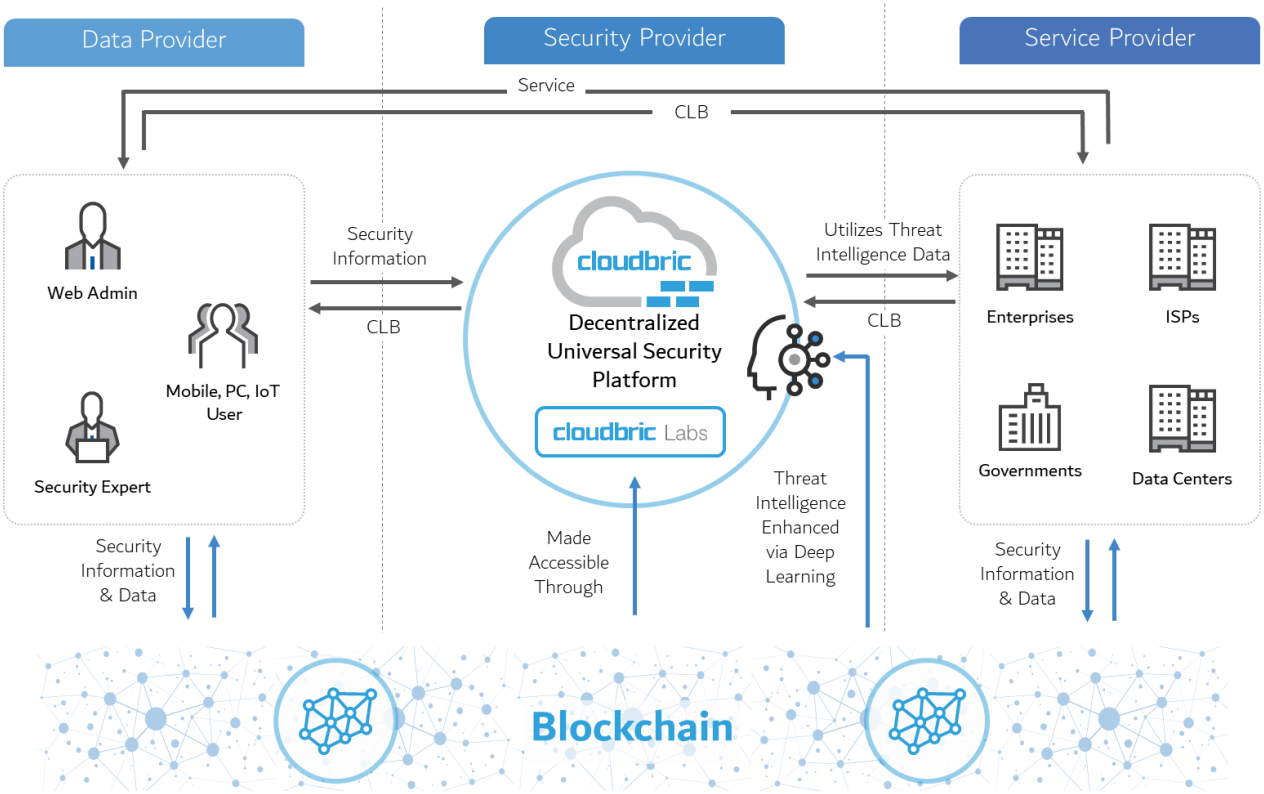
2 년간 운영하면서 클라우드브릭은 매출 및 사용자 확보를 통해 상당한 성장을 경험했습니다. 주목할 만한 성과로는 25 개 이상의 서비스 리전을 오픈하고, 10,000 명 이상의 사용자 확대, 그리고 인프라 업체, 웹호스팅 및 서비스 리셀러들과 50 곳 이상의 글로벌 파트너 관계를 구축한 것이 있습니다.

중소기업 틈새 시장에서의 클라우드브릭의 지속적인 성공은 Gartner Magic Quadrant for Web Application Firewalls 및 Frost & Sullivan 과 같은 업계를 선도하는 분석 회사로부터 인정을 이끌어냈습니다. 또한 클라우드브릭은 SC Magazine Awards Europe 및 Cyber

Defense Magazine 에서 각각 **'Best SME Security Solution'** 및 **'Hot Company in Web Application Firewall'**로 선정되었습니다.

2017 년 말, 클라우드브릭의 시장 성장에 힘입어 클라우드브릭 코어팀은 펜타시큐리티와는 별개로 Cloudbric Pte. Ltd.라는 새로운 회사를 설립하기로 결정했습니다. 이를 통해 클라우드브릭 코어팀은 사이버 보안을 위해 특별히 설계된 새로운 AI 기반의 딥러닝 기술 개발에 집중할 수 있었습니다. 클라우드브릭의 목표는 사이버 보안과 AI 사이의 간격을 메워 가장 진보된 사용자 중심의 여러 보안 솔루션을 2018 년 리버스 ICO 런칭을 통해 시장에 제공하는 것입니다.

리버스 ICO 구조



클라우드브릭이 리버스 ICO 를 시작하려는 동기는 모든 사용자가 분산화된 사이버 보안 발전의 주요 동력이 되고 AI 기반의 딥러닝 기술로 구동되는 여러 사이버 보안 솔루션을 제공하는 최초의 공급 업체가되는 것입니다.

전체 사이버 보안 시장은 2023 년까지 APAC 지역에서의 가장 빠른 보안 채택률로 1,650 억 달러 규모의 시장이 될 것으로 예상됩니다. 클라우드브릭은 APAC 보안 시장에서의 경험과 우수성으로, 통합 보안 플랫폼으로의 확장을 통해 지속적인 시장 영향력을 행사할 수 있는 강력한 입지를 구축 할 것입니다.

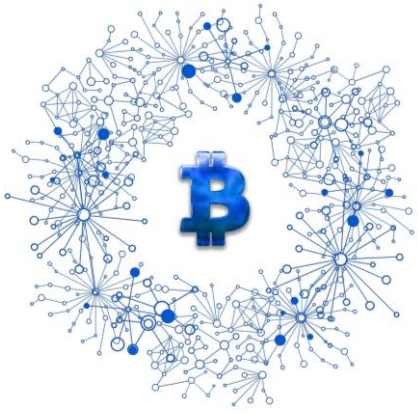
또한, 클라우드브릭은 딥러닝 기술을 핵심 보안 기술에 통합하여 업계에서 가장 혁신적인 보안 업체가 됨으로써 보안 시장을 변화시킬 수 있도록 노력할 것입니다. 이것은 또한 클라우드브릭이 오늘날 가장 빠르게 성장하는 기술 시장 중 하나인 AI 분야를 활용할 수 있게 해줄 것입니다. 세계적인 전망에 따르면, AI 시장은 2025 년까지 1,190 억 달러 규모에 이를 것으로 예상됩니다.

VISION: 딥러닝 기술

클라우드브릭은 엘리트 웹사이트 보안 벤더로서 그 뿌리를 내렸지만, 사용자에게 보다 자율적이며 고급 데이터 보호를 제공할 필요성에 따라 새로운 딥러닝을 기반으로 하는 통합 보안 플랫폼을 개발하게 되었습니다.

클라우드브릭의 딥러닝 모듈인 비전(VISION)은 곧 다양한 사용자 디바이스, 시스템 및 프로토콜을 대상으로 한 사이버 위협 공격을 보다 지능적으로 탐지하는 기능을 제공할 것입니다. 딥러닝 기술을 클라우드브릭의 통합 보안 플랫폼에 적용하면 클라우드브릭이 시장에서 가장 정확하고 낮은 오탐율 솔루션 중 하나가 될 수 있습니다. 또한 딥러닝은 분산화된 사이버 보안 생태계를 개발하려는 클라우드브릭 계획의 중추가 될 것입니다. 이 분산화된 사이버 보안 생태계는 사용자 중심의 보안 보상(Security Reward) 시스템, 개발자를 위한 사이버 보안 리소스 툴, 광범위한 파트너십 네트워크의 상호 보완적인 솔루션 및 서비스 등을 포함합니다. 클라우드브릭의 특허 진행중인 딥러닝 모듈 비전(VISION)은 다양한 공격 및 데이터 집합을 사용하여 행동 패턴을 추출하는 CNN(Convolutional Neural Network) 학습 모델을 기반으로 합니다. 클라우드브릭의 딥러닝 기술에 대한 자세한 내용은 Appendix 의 기술 요약 섹션에서 확인 가능합니다.

클라우드브릭 서비스 발전의 다음 단계는 보안 웹 게이트웨이(Secure Web Gateway)로 알려진 새로운 모바일/PC 보안 클라이언트의 개발입니다. 클라우드브릭 보안 웹 게이트웨이를 사용하면 모든 인터넷 연결 사용자가 다양한 방식으로 데이터 통신을 보호 할 수 있습니다. 예를 들어, 클라우드브릭 보안 클라이언트를 다운받은 사용자는 악의적인 스팸/피싱 URL, 멀웨어 감염 파일 다운로드, 이메일 보호 등의 보안을 24/7 실시간으로 받게 됩니다.



또한 새로운 보안 웹 게이트웨이 클라이언트의 주요 장점은 암호화폐 자산 보호에 초점을 맞추는 것입니다. 암호화폐 자산의 전송, 저장 및 액세스가 해킹 시도에 취약하다는 것은 더이상 비밀이 아닙니다. 지난 1 년 동안 해커들은 사용자 또는 거래소로부터 수백만 달러의 암호화폐 자산을 성공적으로 훔칠 수 있었습니다.

클라우드브릭이 계획중인 보안 웹 게이트웨이 클라이언트는 다양한 암호화폐 자산을 소유한 사용자에게 암호화폐 중심 해킹 시도에 대한 실시간 보호를 제공합니다. 예를 들어

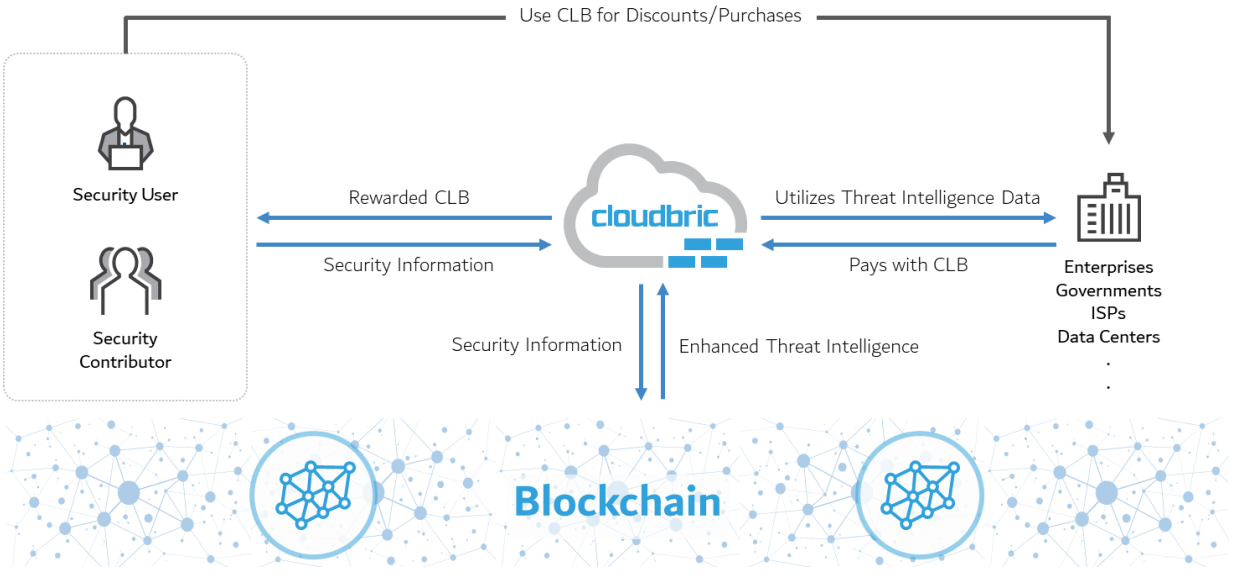
CryptoShuffler 와 같은 악성 소프트웨어에 감염된 PC 또는 모바일 디바이스는 암호화폐를 친구 및 가족에게 전송하려고 하는 사용자의 지갑 주소를 조작할 수 있습니다. 보안 웹 게이트웨이 클라이언트는 악성 암호화폐 탈취 소프트웨어를 식별하여 사용자 디바이스에 설치하는 것을 방지할 수 있습니다.

또한 암호화폐 시장을 지속적으로 괴롭히고 있는 한가지 이슈는, 진짜 암호화폐 거래소처럼 보이는 복제 웹사이트의 확대입니다. 의심이 없는 암호화폐 거래자는 사용자 이름과 암호를 사용하여 가짜 웹사이트에 로그인함으로써 이러한 해킹 전략의 희생양이 되기 쉽습니다. 이 문제를 방지하는 유일한 방법은 URL 주소에 특히 주의를 기울이거나 매우 찾기 어려운 다른 해킹 증거를 찾는 것입니다. 하지만 클라우드브릭의 보안 웹 게이트웨이는 분산된 암호화폐 사기 데이터베이스를 통해 자동으로 암호화폐 거래소 피싱 웹사이트에 대한 접근을 인식하고 차단할 것입니다.

마지막으로 클라우드브릭의 안전한 암호화폐 지갑(개발중)을 사용하는 사용자는 암호화폐 자산을 사기성 암호화폐 주소로 전송하는 것에 대한 자동화된 보호 기능을 누릴 수 있습니다. 사기성 암호 지갑 주소, 피싱 암호화폐 사이트 URL 또는 암호화폐 중심 악성코드에 감염된 파일과 관련된 모든 데이터는 클라우드브릭 보안 사용자 커뮤니티에 의해 수집되어 클라우드브릭 랩스에서 액세스 할 수 있게 됩니다.

클라우드브릭 엔드 포인트 보안을 활성화하기 위해 사용자는 공식 클라우드브릭 데스크탑 클라이언트 또는 모바일 애플리케이션을 다운로드 해야 합니다. 클라우드브릭의 보안 웹 게이트웨이 기술에 관한 기술 정보는 아래 Appendix 를 참조하십시오.

클라우드브릭 보안 보상 프로그램(Security Rewards Program)



클라우드브릭 보안 보상 프로그램(Security Rewards Program)은 클라우드브릭의 분산화된 보안 생태계의 주요 구성 요소입니다. 이 보상 프로그램은 블록체인 기반 보상 시스템으로, 사용자가 클라우드브릭의 딥러닝 보안 탐지 기능의 적극적인 성장에 참여하도록 유도하여 모든 클라우드브릭 사용자에게 보다 정확하고 향상된 보안을 제공할 수 있게 합니다. 클라우드브릭 보안 보상 프로그램에 참여하는 사용자는 클라우드브릭이 생성한 익명의 공격 로그를 딥러닝 엔진 자체에 다시 제공하여 VISION 의 딥러닝 기능을 학습시킬 수 있습니다. 이것은 글로벌 사이버 공격으로부터 사용자를 보호하는 보안 기술의 향상된 지능, 인식 및 학습에 필수적인 역할을 수행 할 것입니다.

클라우드브릭 보안 보상 프로그램 참여를 통해, 사용자는 '위협 데이터 기여' 또는 '리소스 커뮤니티 기여' 방식이라는 두가지 주요 기여 방법을 통해 무료 CLB 암호화폐 토큰을 받을 수 있습니다.

방법 1: 위협 데이터 기여 방법

클라우드브릭 범용 보안 플랫폼에서 사용 가능한 서비스를 사용하면 클라우드브릭 딥러닝 시스템 또는 보안 웹 게이트웨이 클라이언트가 탐지한 공격을 기반으로 익명 클라우드브릭 공격 탐지 로그를 자동으로 생성합니다. 사용자는 공격 탐지 능력을 향상시키기 위해 인공지능 엔진에 이러한 공격 탐지 로그를 다시 제출하여 배포 할 수 있는 옵션이 제공됩니다. 이 경우 클라우드브릭 보안 시스템의 성장에 적극적으로 기여하는 부분에 대한 보상의 형태로 사용자에게 무료 CLB 토큰이 배포됩니다.

클라우드브릭 보안 서비스를 등록하고 사용하는 모든 사용자에게는 기본 CLB 배포가 자동으로 할당됩니다. CLB 의 분배율은 다양한 요인에 따라 증가되거나, 또는 보너스로 주어질 수 있습니다. 예를 들어, 사용자는 여러 웹사이트, 이메일 계정, 모바일 및 PC 를 개인 클라우드브릭 범용 보안 대시보드에 직접 등록하여 CLB 에 대한 보상을 늘릴 수 있습니다. 보너스 CLB 배포는 사용자 추천 또는 클라우드브릭 계정 등록 기간에 따라 제공됩니다. 사용자 CLB 의 배포 주기는 일별, 주별 또는 월별로 수행되며 사용자 배포 확인을 위해 분산형 블록체인 원장에 게시됩니다.

방법 2: 위협 정보 리소스 커뮤니티 기여 방법

클라우드브릭 보안 서비스를 사용하지 않는 사용자는 클라우드브릭 랩스에 대한 기여를 통해서도 CLB 토큰 배포를 받을 수 있습니다. 클라우드브릭 랩스는 다양한 무료 보안 도구, 데이터 분석 및 공개 토론 포럼을 제공하는 분권화된 보안 리소스 커뮤니티입니다.

클라우드브릭 랩스는 보안 커뮤니티를 위한 사용하기 쉬운 툴로서 위협 정보를 투명화시키는 지속적인 노력을 통해 Cybersecurity Excellence Awards 에서 **"올해의 사이버 보안 프로젝트 - 금상"**으로 선정되었습니다. 이 툴의 베타 버전은 클라우드브릭 랩스 리소스 페이지에서 찾을 수 있습니다. 클라우드브릭 랩스 커뮤니티에서 현재 사용할 수 있는 세 가지 보안 툴은 BlackIPedia, WAFER 및 Threat Index 입니다.

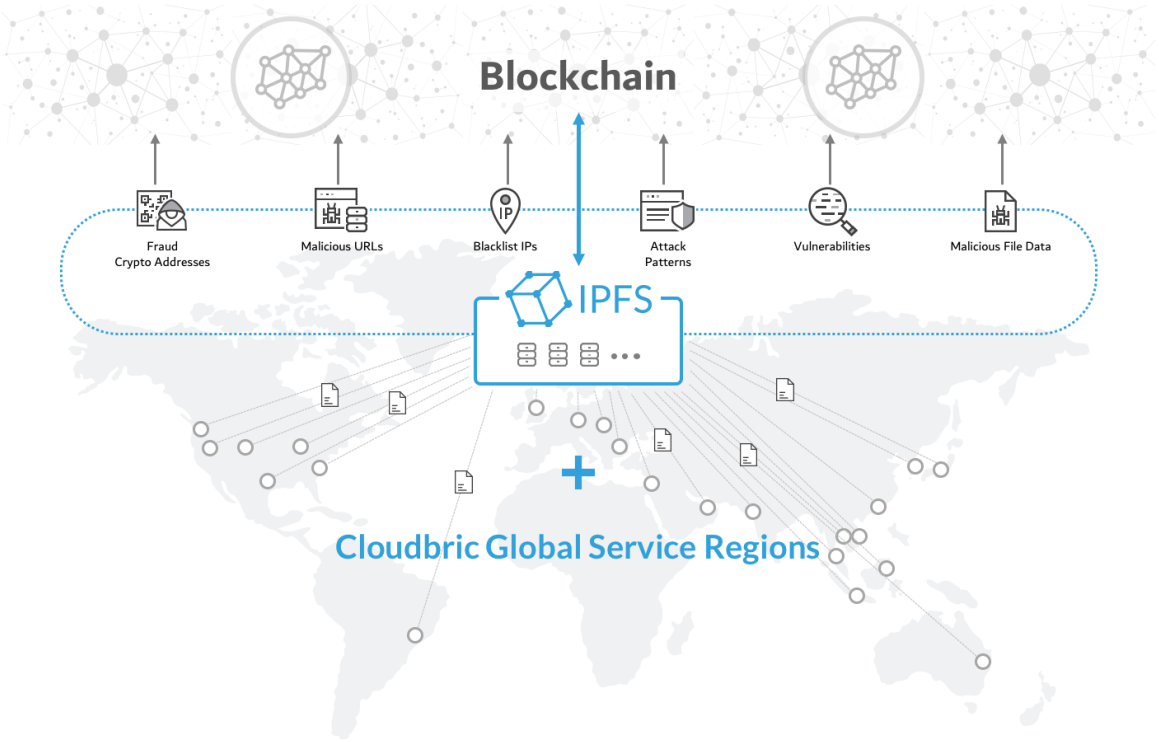
- **BlackIPedia** 는 클라우드브릭 보안 시스템에서 탐지된 전세계적의 악의적인 블랙리스트 IP 주소를 실시간으로 나열합니다.
- **WAFER** 는 WAF Evaluator 라고도 하며 웹 보안 성능을 측정하기 위해 웹사이트 "취약점 테스트"를 할 수 있는 고유한 도구입니다.
- **Threat Index** 는 새로 발견된 전세계의 웹 취약점 목록을 제공합니다.

사용자는 클라우드브릭 랩스 커뮤니티에 새로운 정보를 제공하여 무료 CLB 토큰을 배포 받을 수 있을 것입니다. 예를 들어 보안 기여자는 BlackIPedia 커뮤니티에 악의적인 IP 정보를 추가로 제공하거나 WAFER 커뮤니티에 새로운 테스트 패턴을 제안하거나 Threat Index 커뮤니티의 사용자에게 패치 해야 하는 새로 발견된 웹 취약점에 대해 경고 할 수 있습니다. 또한 암호화폐 관련하여 피싱 사이트 URL, 해커 암호화페 주소 등을 제보하여 기여할 수도 있게 할 예정입니다. 또한 위협정보 기여자는 추후 주어질 CLB 토큰 보너스를 위해, 사이버 보안 인식을 높이기 위한 커뮤니티 관련 질문에 답변하는 등 클라우드브릭 토론 게시판 및 포럼에 참여할 수 있습니다.

클라우드브릭에서 생성된 공격 탐지로그에는 개인 식별 정보(Personally Identifiable Information, PII)가 저장되거나 기록되지 않습니다. 또한 모든 사용자가 클라우드브릭 보안 보상 프로그램(Security Rewards Program)에 참여해야하는 것은 아닙니다. 딥러닝 모듈에 공격 탐지 로그를 제공하기 원치 않는 사용자는 클라우드브릭 범용 보안 서비스는 계속 누릴 수 있지만 CLB 토큰을 받을 권리는 상실됩니다.
클라우드브릭에서 생성된 공격 탐지 로그는 클라우드브릭 서버에 익명으로 보관되며 표준 보안 서비스 약관에 따라 2 년마다 영구적으로 삭제됩니다.

클라우드브릭은 또한 안전한 전용 암호화폐 지갑을 사용하거나 사용자가 선택한 지갑으로 토큰을 전송할 수 있는 옵션을 제공합니다. 클라우드브릭의 기본 암호화폐 지갑은 모든 클라우드브릭 사용자에 대해 암호화 및 보안 인증 기능을 제공하며 클라우드브릭 범용 보안 대시보드를 통해 액세스 할 수 있습니다. 사용자는 온라인상에서 또는 개발 예정인 클라우드브릭 모바일 애플리케이션을 통해 개인 대시보드에 직접 로그인 할 수 있습니다.

위협 정보의 분산화



클라우드브릭 Reverse ICO 의 주요 측면 중 하나는 모든 위협 정보를 블록체인으로 분산시키는 것입니다. 클라우드브릭의 범용 보안 플랫폼은 많은 양의 사용자 공격 탐지 로그를 수집하여 투명성과 공개 검증을 위해 블록체인에 게시합니다. 이 정보는 새로운 커뮤니티형 클라우드브릭 랩스 리소스 툴을 통해 대중이 액세스 할 수 있게 합니다.

클라우드브릭 랩스에 추가될 툴은 악성 스팸 URL 및 파일 식별, 암호화폐 사기 주소 등과 같은 다양한 사용자 생성 분산 데이터베이스를 중심으로 하며, 사용자는 인터넷에서 발견되는 새로운 악성 다운로드 파일, 사용자 계정 정보를 해킹하려는 의심스러운 피싱 URL, 사용자를 온라인에서 속이는 데 사용되는 스팸 암호화폐 지갑 주소 등을 제공하여 이 툴에 기여할 수 있습니다.

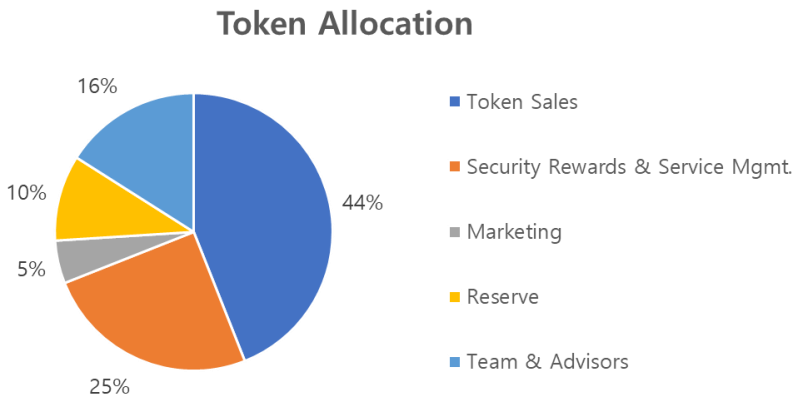
블록체인 안에는 방대한 데이터를 저장하기 어렵기 때문에 클라우드브릭은 IPFS(InterPlanetary File System)를 이용한 분산 데이터베이스를 구축할 것입니다. 클라우드브릭 서비스 리전을 IPFS 노드로 활용하여 위협 정보를 분산화 저장하고, 이 데이터들에 대한 해쉬값을 블록체인 위에 올려 위협 정보 분산화를 달성하고자 합니다. IPFS 가 원활히 동작하기 위해서는 스토리지 노드 유지가 필수이지만, 개인 노드에 의지를 하게 될 경우 보상 없이 자율적으로 노드를 유지시키기는 쉽지 않습니다. 하지만 클라우드브릭은 이미 자체

보유중인 전세계의 30 개 가까운 서비스 리전을 IPFS 노드로 활용하여 안정적이고 속도 저하 없는 분산 위협 정보 시스템을 제공하고자 하고, ICO 이후 서비스 리전도 100 개 이상까지 지속적으로 늘려 나갈 계획입니다.

클라우드브릭 랩스 툴에 대한 액세스는 개인 및 공공 용도로 항상 무료로 제공됩니다. 그러나 이미 존재하는 보안 플랫폼에 추가 통합하거나 새로운 보안 기술을 개발하기 위해 이 위협 정보를 직접 활용하고자 하는 기업은 추가 비용을 지불해야합니다.

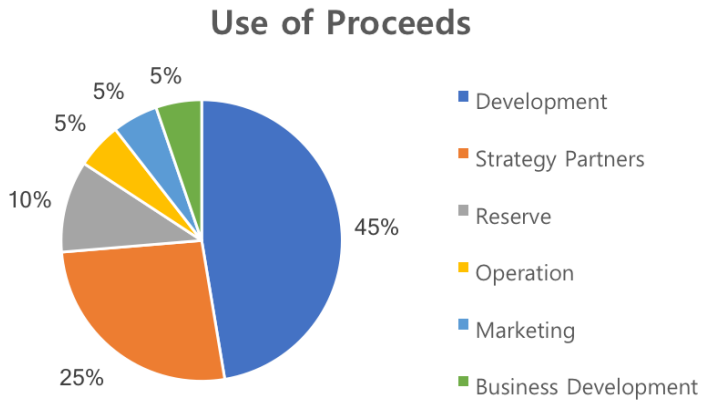
토큰 분배 계획

프리 세일 및 퍼블릭 세일을 통해 전체 발행량의 44%의 CLB 토큰을 판매 및 분배합니다. 또한 토큰은 어드바이저 및 클라우드브릭 팀원들, 그리고 마케팅이나 클라우드브릭 Security Rewards Program 을 위한 용도로도 배포될 것입니다.



CLB 배포에 대한 자세한 내용은 아래를 참고하십시오.

- 클라우드브릭은 총 10 억개의 CLB 를 발행합니다.
- 44% (4.4 억 CLB) 는 토큰 세일 이벤트에 할당됩니다.
- 25% (2.5 억 CLB) 는 클라우드브릭 Security Rewards Program 및 서비스 유지 및 관리 비용으로 할당됩니다.
- 16% (1.6 억 CLB)는 클라우드브릭 팀 멤버 및 어드바이저들에게 할당됩니다.
- 10% (1 억 CLB)는 비지니스 준비금(잠재적 거래소 상장, 전략적 파트너쉽 등)으로 할당됩니다.
- 5% (5 천만 CLB) 는 Cloudbric 을 프로모션하기 위한 마케팅에 할당됩니다.



모집금 사용

클라우드브릭 Reverse ICO 에서 모금된 기금은 클라우드브릭의 개발 및 글로벌 확장에

할당됩니다.
이 기금의 상당 부분은 제품 개발, 블록체인 통합, 딥러닝 데이터 통합, 글로벌 인프라 확장을 위해 재투자 될 것입니다.

나머지 수익금은 클라우드브릭 Reverse ICO 의 마케팅, 사업 개발 및 운영 필요 사항을 지원하는데 사용됩니다.

토큰 스테이킹(Staking) & 거버넌스(Governance)

클라우드브릭의 여러 보안 서비스를 활성화하기 위해 추후 사용자는 새로운 토큰 스테이킹(Staking) 프로그램에 참여하게 됩니다. 사용자는 통합 보안 플랫폼 (예 : 웹 사이트 보안, 모바일 디바이스 보안 및 암호화폐 자산 보호)에 완전히 액세스하려면 각 계정내 CLB 토큰의 최소 잔액을 입금하고 유지해야 합니다. 최소 CLB 활성화 보유량을 유지하지 못하면 사용자 계정이 "바이패스 모드"로 설정되어 최소 보유량이 복원될 때까지 모든 보안 조치가 일시적으로 비활성화됩니다.

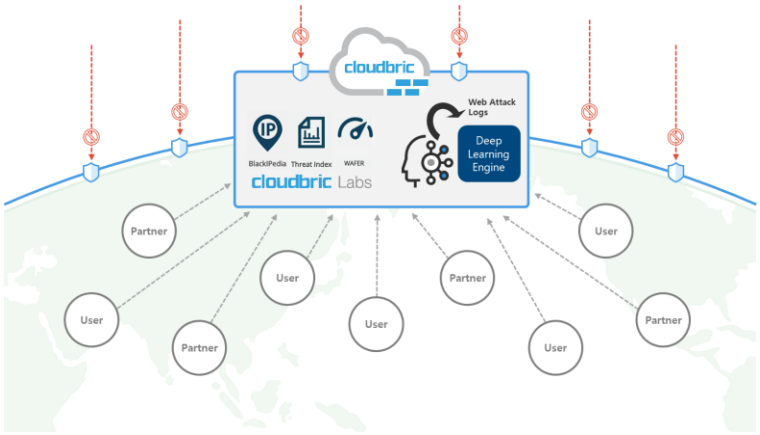
또한 클라우드브릭은 전체적인 CLB 토큰 생태계의 완전한 탈중앙화를 활성화하기 위해 새로운 사용자 거버넌스(Governance) 시스템을 구현할 것입니다. 사용자는 투표 기반 시스템을 통해 서비스 이용을 위한 CLB 최소 보유량, 보안 보상 비율 등을 완전히 제어할 권한이 부여됩니다. 클라우드브릭은 계정 활성화 및 보안 보상 프로그램 배포에 대한 초기 최소 보유량 비율을 설정합니다. 이후 클라우드브릭은 분기별로 사용자 투표 시스템을 관리 및 배포하여 사용자 거버넌스 생태계의 완전한 구현을 활성화 할 것입니다.

토큰 사용

클라우드브릭 의 보안 서비스를 활성화하려면 사용자는 자신의 계정(최소 한도는 아직 결정되지 않음)에 고정된 양의 CLB 토큰을 보관하고 유지해야 합니다. 직접 CLB 입금 또는 CLB 보상을 통해 CLB 계정 한도를 유지하면 개인 사용을 위한 클라우드브릭 통합 보안 서비스가 해제됩니다. 엔터프라이즈 고객 및 조직은 유료 보안 플랜의 적용을 받습니다. 그러나 클라우드브릭은 엔터프라이즈 사용자가 매월 서비스 요금을 지불할 때 CLB 토큰을 활용할 수 있는 인센티브를 제공합니다.

CLB 토큰을 사용하여 월별 서비스 요금제를 구매하는 기업 고객은 클라우드브릭 정가에 대해 **50 % 할인을 자동으로 받습니다.** CLB 를 사용하여 구매하지 않으려는 사용자는 유효한 신용카드 또는 PayPal 계정으로 표준 결제를 진행할 수 있습니다.

Secure Web Alliance



클라우드브릭 Secure Web Alliance 는 사용자가 CLB 토큰을 활용할 수 있는 또 다른 채널의 역할을 합니다. 이 제휴 관계는 클라우드브릭 범용 보안 서비스를 사용하여 비즈니스를 보호하고 파트너 서비스의 CLB 토큰 결재 허용을 통해 클라우드브릭 사용자에게 직접 독점적인 혜택을 제공하는 글로벌 파트너 네트워크가 될 것입니다.

사용자는 클라우드브릭 마켓플레이스나 파트너 웹사이트를 통해 새로 업데이트된 Secure Web Alliance 프로그램에 접근 할 수 있습니다. 각 파트너는 회사 웹사이트에 표시한 Secure Web Alliance 웹씰을 통해 검증됩니다. 이를 통해 파트너쉽 트랜잭션이 안전하고 파트너가 공식적으로 CLB 토큰으로 지불 받을 수 있는 라이센스가 있음을 나타냅니다. 파트너 및 사용자가 CLB 를 사용하여 이루어진 모든 거래는 블록체인에 기록되고 검증됩니다.

보안 개발 생태계

분산화된 모든 사이버 위협 정보는 클라우드브릭 랩스에서 무료로 조회할 수 있습니다. 잠재적인 보안 개발자 및 조직은 맞춤 API 를 통해 데이터를 직접 활용해서 독점적인 사이버 보안 솔루션을 개발할 수 있습니다. API 이용의 경우, CLB 토큰을 보유하고 있는 양에 따라 활용할 수 있는 데이터의 양이 결정이 됩니다.

클라우드브릭은 관련 서비스 제공 업체, 정부 기관 또는 보안 개발자가 클라우드브릭의 글로벌 위협 데이터베이스를 직접 활용하여 소프트웨어를 개발할 수 있는 새로운 보안 개발 생태계를 활성화 할 것입니다. 이를 통해 보다 폭 넓은 혁신, 보안에 대한 인식 향상 및 사이버 보안 적용 사례들을 활성화 할 것입니다.

잠재적인 서비스 제공 업체는 CLB 토큰을 통해 구입할 수 있는 커스텀 API 를 통해 클라우드브릭 랩스 데이터를 직접 활용할 수 있습니다. 엔터프라이즈 API 구매의 수익은 데이터 제공자인 사용자들을 위해 기존 Security Rewards 토큰 할당 풀을 보충하는 데 사용됩니다.

Appendix

딥러닝 기술 오버뷰

오늘날 기술 시장은 AI, 머신러닝, 딥러닝 등과 같은 업계 유행어에 점점 더 매혹되어 가고 있습니다. 특정 목적을 위한 이러한 기술의 적절한 활용과 통합은 매우 어려운 작업입니다. 그러나 AI 기술의 이점과 시장 영향력은 놀랍습니다. 클라우드브릭의 연구 개발팀은 사이버 보안에 초점을 맞춘 특허 진행중인 자체 딥러닝 엔진을 개발하는데 주력해 왔습니다.

시장에서 웹공격 탐지에 대해 가장 낮은 오탐지율을 보였음에도 불구하고 클라우드브릭은 항상 정확도를 더욱 향상시킬 수 있는 더 좋은 방법이 있는지 연구해왔습니다. 클라우드브릭은 또한 사람의 개입으로 때때로 일정한 트래픽 모니터링을 통해 육안으로 사이버 공격을 더 잘 탐지 할 수 있음을 깨달았습니다. 그러나 모든 온라인 트래픽을 지속적으로 모니터링하는데 인적 자원을 이용하는 것은 현실적으로 어렵기 때문에 클라우드브릭의 연구 개발팀은 궁극적으로 온라인 트래픽 데이터의 지능형 탐지 및 차별화를 전문으로 하는 세계 최초의 딥러닝 모듈을 구축하기로 결정했습니다.

개발 히스토리

클라우드브릭의 딥러닝 기술은 KAIST, 고려대학교 및 MIT 의 머신러닝 개발자 및 박사 학위 소지자들로 구성된 클라우드브릭의 내부팀에 의해 개발되었습니다.

새로 개발된 딥러닝 모듈을 제대로 훈련시키기 위해 팀은 먼저 웹 트래픽 데이터를 딥러닝 모듈에 넣는 방법을 극복해야 했습니다. 과거에는 딥러닝 머신이 데이터를 픽셀 단위로 받아 들일 수 있도록 설계되었습니다. 이로 인해 모든 이미지가 이미 수천 개의 픽셀로 구성되어 있으므로 이미지 데이터를 매우 편리하게 넣을 수 있습니다. 그러나 모든 온라인 요청, 통신 및 웹 주소들은 문자 및 문구를 통해 표시됩니다. 이로 인해 R & D 팀은 사전 지식을 바탕으로 데이터를 적절하게 개념화하고 올바른 판단을 내릴 수 있도록 알파벳 문자를 딥러닝 머신으로 재구성하는 어려운 과제를 안게 되었습니다.

클라우드브릭팀은 웹 트래픽을 딥러닝 머신이 파악하기 위해 보다 쉽게 소화 가능한 형태의 데이터로 변환해야한다는 결론에 도달했습니다. 변환이 어떻게 작동하는지 더 잘 설명하기 위해 온라인 트래픽을 구성하는 다양한 구성 요소의 각 문자와 기호가 먼저 이미지로 변환되었습니다. 그 다음 딥러닝 머신을 프로그램하여 해당 이미지에 포함된 특정 패턴 또는 규칙성을 발견했습니다. 그 이후부터는 합법적인 온라인 트래픽과 악의적인 온라인 트래픽에서 발견되는 패턴을 구분하도록 딥러닝 모듈을 훈련하였습니다.

트래픽 변환

이를 보다 간단하게 설명하기 위해 클라우드브릭 연구원들은 "DBFC"라고 알려진 특정 패턴을 아래 그림으로 변환할 수 있었습니다.

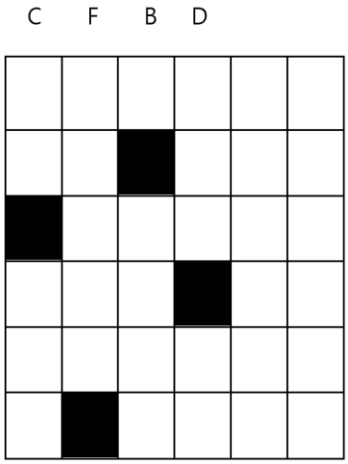


*그림 **1:** 딥러닝 이미지 변환*

딥러닝 머신은 벤치마크를 통해 다른 이미지 또는 온라인 트래픽 간의 관계를 찾기 위해 훈련됩니다. 그 결과에 따라, 머신은 "DBFC"가 합법적인 트래픽인지 또는 악의적인 트래픽인지 정확하게 판단합니다.

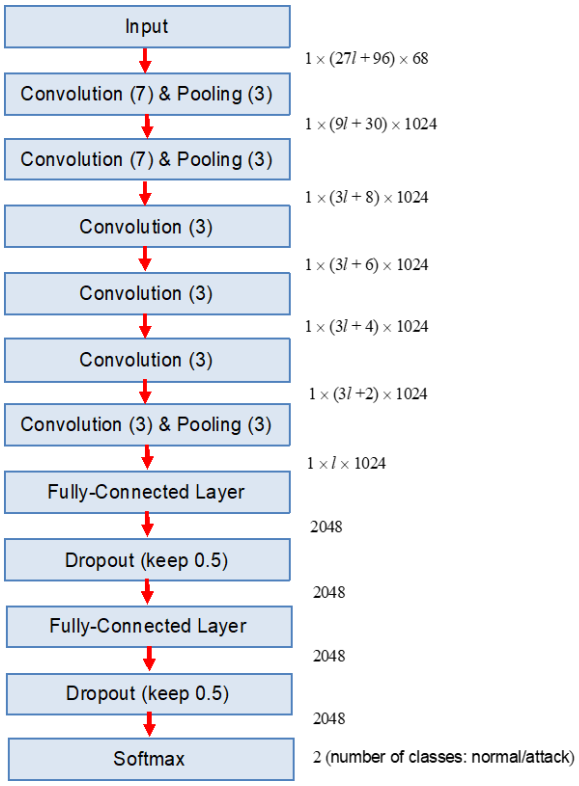


그림 2: 클라우드브릭 딥러닝의 기본 구조

클라우드브릭의 개발 초기에는 문자를 고유 이미지 세트로 적절하게 변환할 수 있는 다른 딥러닝 모듈이 부족했습니다. 클라우드브릭은 이 작업에 적합한 CNN(Convolutional Neural Network) 구조를 기반으로 하는 2 개의 오픈 소스 컴퓨터를 테스트하여 성과를 달성할 수 있었습니다.

클라우드브릭은 두 시스템을 모두 테스트하여 장점과 단점을 다 가지고 있음을 확인했습니다. 예를 들어, 한 머신은 훈련하기가 쉬우나 두 번째 머신보다 정확도가 떨어집니다. 클라우드브릭은 궁극적으로 웹 트래픽 탐지에 더 빠른 모듈을 사용하기로 결정했습니다. 왜냐하면 후자의 시스템이 지속적으로 업데이트되는 엄청난 수의 웹 트래픽 로그를 처리 할 수 없었기 때문입니다.

적절한 머신을 선택한 후, 연구 개발팀은 또 다른 문제에 봉착했습니다. 웹 공격에 특화된 이 시스템을 적용하려고 시도했을 때, 팀은 공격 URL 의 특정 문자가 기존의 68 글자(시스템에서 인식 가능한)에 포함될 수 없음을 곧 알아차렸습니다. 이는 웹 사이트가 다양한 언어로 구축 될 수 있기 때문에 클라우드브릭 팀이 제한없이 문자를 허용하는 방법을 찾아야한다는 것을 의미했습니다.

이로 인해 팀은 UTF-8 16 진수 형식으로 사이버 공격을 해석할 수 있는 특허 기술을 구현한 후 딥러닝 시스템으로 다시 적용하였습니다. 이를 통해 딥러닝 머신은 UTF-8 기반 문자를 받아 들일 수 있었으며, 결국 팀이 웹 트래픽 인식을 위해 특별히 설계된 모듈을 훈련시킬 수 있게 되었습니다.

정확한 트래픽 탐지

머신 정확도와 관련하여 클라우드브릭 팀은 증분 학습이라고하는 원시적이지만 효과적인 솔루션을 제안했습니다. 한 대의 머신이 모든 작업을 수행시키는 대신 처음에 각각 4 주간의 사이버 공격 데이터로 교육을 받은 4 대의 딥러닝 머신을 구축합니다. 그런 다음 팀은 오류 비율에 따라 각 시스템에 가중치를 할당합니다.

타입	데이터 훈련 기간	Final Result
머신 A	1 주 - 4 주	$argmax_{c\in\{0,1\}}\sum_{n} W_n \mathbb{1}\{O_n = c\}$ W 는 아래와 같이 정의됨 $\log\frac{1}{E_n}$ n = 머신 A, B, C, D W = 가중치 O = 머신 결과 E = 에러율
머신 B	2 주 - 5 주	
머신 C	3 주 - 6 주	
머신 D	4 주 - 7 주	

위 기간 및 최종 결과는 클라우드브릭 테스트 결과의 정확성에 따라 변경 될 수 있습니다. 그러나 현재의 내부 딥러닝 테스트 결과는 로직 기반 클라우드브릭 보안 엔진에 비해 85 %의 정확도 증가율을 보였습니다. 비교를 위해, 클라우드브릭의 로직 기반 웹방화벽 엔진은 업계 분석가들에 의해 시장에서 가장 낮은 오탐지율을 가진 웹방화벽 중 하나로 여겨집니다.

요약하면, 클라우드브릭은 독점적인 딥러닝 엔진을 개발하기 위해 3 가지 주요 장애물을 극복해야했습니다. 즉, 웹 트래픽 특성을 픽셀로 변환하고, 선택한 머신의 효율성을 찾고, 머신 표준 정확도를 개선해야했습니다. 클라우드브릭 팀은 특허 진행중인 딥러닝 엔진인 VISION 을 계획된 모든 클라우드브릭 보안 솔루션에 통합 할 수 있는 길을 열어 놓은 2018 년 초에 이러한 장애물을 극복 할 수 있었습니다.

개인(End-Point) 보안 기술 오버뷰

클라우드브릭은 리버스 ICO 프로젝트를 통해 보안 서비스를 확장할 계획이지만 현재 클라우드브릭 보안 서비스 (Security-as-a-Service)는 사용자를 위한 서버측 보안만 제공합니다. 여기에는 주로 웹방화벽, CDN 속도 최적화, DDoS 보호, SSL 암호화 등과 같은 보안 솔루션이 포함됩니다. 이 솔루션은 주로 특정 웹 서버를 보호하는 데 사용되며 개인 디바이스에는 적용되지 않습니다.

클라우드브릭 팀은 대부분의 일반 사용자가 웹 서버와 거의 관련이 없지만 모바일 디바이스와 PC 는 일상 생활의 일부임을 잘 알고 있습니다. 사이버 보안 시장은 현재 이러한 두 가지 세계(서버 보안 및 모바일 디바이스 보안)를 통합 솔루션으로 제공하지 않습니다. 이는 클라우드브릭이 리버스 ICO 프로젝트를 통해 이룩하고자 희망하는 것입니다.

보안 웹 게이트웨이(Secure Web Gateway)

개인 디바이스의 보안을 침해하는 방법에는 여러 가지가 있습니다. 클라우드브릭은 클라우드브릭의 광범위한 위협 정보 데이터베이스를 활용하고 기존 개인 보안 업체와 협력하여 이러한 보안 위험을 줄이고 모든 사용자 개인 디바이스를 보호하는 통합 플랫폼을 제공할 계획입니다. 또한 클라우드브릭의 딥러닝 엔진을 통합하여 새롭고 알려지지 않은 악성 프로그램 소스, 바이러스 감염 파일, 스팸 및 피싱 URL 등을 보다 효과적으로 탐지할 것 입니다. 이는 궁극적으로 클라우드브릭의 보안 웹 게이트웨이(Secure Web Gateway)로 알려진 통합된 개인 중심 클라이언트로 패키징 됩니다.

보안 웹 게이트웨이 클라이언트는 PC 및 모바일 전화 모두에 사용 및 다운로드 가능한 클라이언트입니다. 이 클라이언트는 VPN(Virtual Private Network) 터널링을 자동으로 활성화하여 전 세계에 전략적으로 위치한 클라우드브릭의 광범위한 서비스 노드 네트워크를 통해 사용자를 연결할 수 있습니다.

클라우드브릭은 이미 약 25 개의 활성화된 서비스 리전을 보유하고 있지만, 이번 리버스 ICO 의 주요 목표중 하나는 모든 사용자 지역의 속도, 안정성 및 성능을 수용할 수 있도록 서비스 노드(2020 년까지 100 개 이상의 서비스 지역을 개방)를 기하 급수적으로 확장하는 것입니다. 보안 웹 게이트웨이는 스팸 / 피싱 URL 사이트 방문 차단, 악성코드 파일 다운로드 방지, 이메일 검사 보호 등과 같은 일일 위협으로부터 개인 디바이스를 보호할 뿐만 아니라 사용자 소유의 암호화폐 자산의 보안 역시 보장합니다.

클라우드브릭(CLB) 암호화폐 지갑

보안은 언제나 암호화폐 지갑에서 문제가 되었습니다. 온라인 지갑은 빠르고 사용하기 쉽지만 모든 정보는 인터넷을 통해 전송됩니다. 이러한 유형의 지갑은 보통 사용자 인증의 한 가지 방법만을 제공하며, 일반적으로 2 팩터 인증(2FA) 사용이 가능한 지갑도 온라인으로 수행이 됩니다. 이것은 간단한 패킷 스니퍼가 쉽게 이러한 자격 증명에 대한 무단 액세스를 얻을 수 있음을 의미합니다. 콜드 또는 하드웨어 암호화 지갑은 이러한 보안 문제를 해결하고자 합니다. 그러나 지갑이 오프라인 상태가 된다는 불편함과 실제 장치 자체를 잃을 가능성은 많은 사람들에게 부담스럽습니다.

클라우드브릭은 보안 웹 게이트웨이 기술의 기반을 활용하여 보안 암호화폐 지갑(2019 년 초 초기 개발)을 개발하여 부정한 주소로의 원치 않는 전송 위험을 방지하고 예방하고자 합니다. 클라우드브릭 CLB 보안 암호화폐 지갑은 스마트폰과 PC 모두에서 사용할 수 있을 예정입니다.

또한 CLB 암호화폐 지갑의 핵심 기능은 지갑의 개인키가 절대로 공개되지 않는다는 것입니다. 대신 사용자의 지갑을 활성화하는 12 개의 사용자 인증 암호문이 있습니다. 활성화된 사용자는 보안 암호를 설정하거나 생체 인식을 사용하여 지갑에 다시 액세스 할 수 있습니다.

CLB 지갑은 암호로 보호될 뿐만 아니라 모바일 장치에서도 FIDO(Fast Identity Online) 인증 방법을 활용할 수도 있습니다. 또한 CLB 지갑은 종단간 암호화(E2EE) 통신을 사용하므로 도난당한 데이터 패킷은 잠재적인 사이버 범죄에 거의 사용되지 않습니다.

마지막으로, 암호화폐 자산 탈취의 출현은 전체 암호화폐 시장에 강한 인상을 남겼습니다. 그러나 클라우드브릭의 보안 CLB 지갑을 사용함으로써 사용자는 자신 있게 그들의 암호화폐를 입금, 보관 및 전송할 수 있습니다. 클라웅드브릭의 보안 웹 게이트웨이 클라이언트는 딥러닝 모듈과 함께 사용자 소유 디지털 자산을 사기성 암호화폐 주소로 전송하는 것을 보다 잘 탐지하고 방지할 수 있습니다. 사기성 지갑 주소 목록을 필터링하기 위한 데이터베이스는 클라우드브릭의 보안 보상 프로그램(Security Rewards Program)의 일환으로 클라우드브릭 랩스에 사기성 주소를 제공하는 전세계의 Cloudbric 사용자들에 의해 구축됩니다.

위협 데이터베이스

사용자가 중요한 정보를 사용하여 웹 사이트를 사용하는 한 스팸 및 피싱 웹 사이트는 언제나 존재합니다. 요즘같은 시대에는 스팸 및 피싱 웹 사이트를 식별하고 피하는 것이 쉬운 작업이라고 생각할 수도 있습니다. 하지만 새로운 복제 웹 사이트들의 정교함과 정확성, 특히 암호화폐 사용자를 대상으로 하는 피싱 웹 사이트들이 새로운 정점에 도달하고 있습니다.

많은 사용자들이 원본 사이트처럼 보여지는 사기성 암호화폐 웹 사이트에 희생되고 있지만, 매우 미묘하고 차이를 찾기가 어렵습니다. 예를 들어 이러한 피싱 웹 사이트는 신뢰할 수 있는 웹 사이트 페이지를 페이지별로 복제하지만 암호화되지 않은 프로토콜(SSL 을 적용하지 않음)에서 제공하거나 주소 URL 에 매우 미묘한 문자 차이가 있을 수 있습니다. 사용자가 조심하지 않으면 사기성 웹 사이트가 암호 도난 또는 거래소 계정에 액세스 할 수 없게 될 수 있습니다.

기존 솔루션은 스팸 및 피싱 웹 사이트에 대한 액세스를 차단하는데 적합합니다. 예를 들어 사용자는 사기성 웹 사이트 또는 전자 메일 주소의 신원을 보고하고 브라우저 / 이메일 클라이언트는 업데이트를 제공하여 해당 소스에 대한 액세스를 차단합니다. 그러나 이러한 스팸 / 피싱 데이터베이스의 다양성과 데이터베이스의 느린 업데이트는 특히 해커가 새로운 공격을 시작할 때 항상 문제가 되었습니다.

클라우드브릭의 분산화된 위협 정보 데이터베이스(클라우드브릭 보안 시스템 및 사용자 기여에 따라 실시간으로 수집되는)는 스팸 및 피싱 방지를 위한 자원으로 부상시킬 계획입니다. 클라우드브릭의 보안 웹 게이트웨이는 이러한 증가하는 데이터베이스를 활용하여 악성 이메일 피싱 시도 및 사기성 웹 사이트에 대한

액세스를 차단합니다. 또한 클라우드브릭은 분산화된 위협 정보 데이터베이스에 나열된 사기성 암호화폐 주소로 자금을 전송하는 것을 방지합니다.

또한 암호화폐 지갑 주소는 일련의 임의의 숫자 및 문자로 기억하기가 매우 어렵기 때문에 대부분의 사람들이 단순히 복사하여 붙여넣기를 통해 주소를 복사하거나 QR 코드를 사용하여 자금을 이체합니다. 사용자가 클라우드브릭 보안 웹게이트웨이 클라이언트를 다운로드하면 보안 클라이언트는 사용자가 받는 사람 암호화폐 지갑 주소를 복사하여 붙여 넣자 마자 위협 정보 데이터베이스에 대해 간단한 확인을 자동으로 실행합니다. 나가는 지갑 주소가 클라우드브릭 커뮤니티에 의해 악성 또는 사기로 보고된 경우 보안 웹 게이트웨이 클라이언트는 사기의 가능성을 사용자에게 즉시 통지하고 자금 이체를 방지합니다. 이를 통해 클라우드브릭 사용자는 자금이 실시간으로 보호되고 있음을 보다 확실하게 알 수 있습니다.

또한, 개인용 컴퓨터에 존재하는 파일도 동일한 과정을 따릅니다. 클라우드브릭의 보안 웹 게이트웨이는 악성코드 감염에 대한 분산화된 위협 정보 데이터베이스와 교차 검색하기 위해 시스템 파일의 이진 코드를 검사하고 올바르게 읽을 수 있습니다. 분산화된 위협 정보 데이터베이스의 바이너리와 일치하는 악의적인 파일이 특정 웹 사이트 또는 이메일 주소에서 다운로드 된 경우, 이 정보도 클라우드브릭의 데이터베이스에 추가됩니다. 클라우드브릭의 위협 정보 데이터베이스의 모든 정보는 사용자들을 위한 위협 정보 리소스 커뮤니티 클라우드브릭 랩스 를 통해 액세스 할 수 있습니다.

데이터 보호 & 사용자 인증

개인 정보는 항상 개인 디바이스에서 우려 사항이었습니다. 사람들은 개인용 컴퓨터의 모든 정보가 안전하다고 가정하기 때문에 일반적으로 컴퓨터와 휴대 전화에 중요한 정보를 저장합니다. 하지만 이것은 진실과 거리가 멉니다. 개인 연락처, 저장된 암호, 신용카드 번호 및 심지어 개인 휴가 또는 회의 일정과 같은 정보는 디바이스가 열린 인터넷에 연결되면 쉽게 노출 될 수 있습니다.

앞서 언급했듯이 클라우드브릭은 전세계 클라우드브릭 서비스 노드 (데이터 센터)의 광범위한 네트워크를 구축하는데 우선 순위를 두게 됩니다. 이러한 서비스 노드는 최종 사용자와 나머지 세계간의 프록시 역할을 합니다. 클라우드브릭 보안 웹 게이트웨이가 VPN(Virtual Private Network) 을 통해 트래픽을 터널링하는 기본 개념하에서, 최종 사용자의 디바이스로 들어오고 나가는 모든 트래픽은 이러한 글로벌 서비스 노드 중 하나를 통해 흐르게 됩니다.

각 노드는 디바이스의 모든 인터넷 연결 트래픽을 모니터링하고 사용자가 개인 디바이스로 유입 및 유출되는 트래픽 유형을 제어 할 수 있도록 합니다. 이 기능은 현재 클라우드브릭 웹방화벽 서비스와 동일하게 작동하지만 모바일 디바이스의 보안 요구 사항을 충족 할 수 있도록 보다 정교하게 조정된 표준을 사용할 예정입니다.

리소스

1. Gilchrist, Michelle. (2018, January 29). Retrieved from http://www.sandiegouniontribune.com/news/data-watch/sd-me-data-breaches-20180129-story.html
2. Kaspersky. (2017, October 31). Retrieved from https://www.kaspersky.com/blog/cryptoshuffler-bitcoin-stealer/19976/
3. McLean, Asha. (2016, November 23). Retrieved from http://www.zdnet.com/article/security-landscape-plagued-by-too-many-vendors-cisco/
4. Shane, Daniel. (2018, January 29). Retrieved from http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html
5. Smith, Sarah. (2018, January 23). Retrieved from https://www.prnewswire.com/news-releases/global-cyber-security-market-is-projected-to-reach-a-size-of-1652-billion-by-2023-300587117.html
6. Markets and Markets. (2018, February). Retrieved from https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html?gclid=EAIaIQobChMI98fK3cXD2wIVxjUrCh1v2wVlEAAYASAAEgK2S_D_BwE
7. X. Zhang and Y. LeCun. (2015). Retrieved from “Text understanding from scratch,” arXiv preprint arXiv:1502.01710.