sumo logic

사례 연구

암호화폐(가상화폐) 거래에 대한 모니터링 환경 조성과 보안 및 재무 감사를 위한 IT 통제 대폭 강화

bitbank

과제

bitbank는 AWS에서 암호화폐(가상화폐) 거래 시스템을 운영합니다. bitbank는 로그 모니터링을 위해 OSS 분산 검색 및 분석 엔진을 이용했지만, 애플리케이션에 대한 정확한 오류 감지 및 분석과 같은 작업은 수행할 수 없었기 때문에 보안 및 재무 감사의 유지 관리를 위한 IT 통제라는 과제를 안고 있었습니다.

솔루션

Sumo Logic은 AWS와의 호환성이 뛰어나고 리소스 확장이 유연하다는 장점을 고려하여 도입되었습니다. 그 결과, 대량의 데이터에서도 빠르고 정확한 검색을 할 수 있게 되었습니다. Sumo Logic을 도입한 이유는 비정형 데이터를 자동으로 구조화하는 소프트웨어 기능을 제공할 뿐만 아니라 ISMS, SOC2 및 PCI DSS 컴플라이언스 인증을 취득하여 중요한 정보 처리 시 안전성을 보장했기 때문입니다. Sumo Logic 솔루션은 테스트 환경에서 약 한 달간의 검증을 거친 후 본격적으로 가동되었습니다.

성과

Sumo Logic에서는 모든 로그를 애플리케이션 측의 사전 로그 수집 및 로그 변환 없이 수집할 수 있습니다. 필요한 대로 로그를 검색하고 추출할 수 있으며, 보안이 한층 강화되었고 재무 감사에 대한 IT 통제 대응 체계가 구현되었습니다. 또한 Sumo Logic의 권한 관리 기능을 통해 개발 부서, 마케팅 부서 등 전사적으로 로그를 최대한 활용할 수 있도록 허용하는 방안도 마련 중입니다.

보안 기능 부족으로 인한 로그 모니터링 문제

암호화폐(가상화폐) 거래소 bitbank.cc를 운영하는 bitbank는 비트코인을 비롯한 가상화폐 거래량이 일본 내 최상위 수준이며*1, 인기를 끌고 있는 XRP와 Monacoin 통화 거래량 또한 전 세계에서 최상위 수준입니다. 또한 타사 리서치 결과*2에 따르면 이 회사는 일본 시장의 보안 부문에서 최고의 평가를 받았습니다.

bitbank의 시스템은 모두 AWS(Amazon Web Services)에서 구성 및 운영되고 있지만 로그 모니터링 작업은 항상 문제였습니다.

bitbank의 보안 전문가 Hashimoto는 이 문제에 대해 “이전에는 IT 통제를 위한 모니터링이 재무 감사 대응에 있어 필수적인 작업이었습니다. 우리는 최소한으로 필요한 수준의 모니터링을 위해 주로 OSS 분산 검색/분석 엔진을 이용했지만, 서비스 보안을 대폭 강화하기 위해서는 로그 모니터링 범위를 확대하고 다중 사용자 모니터링 시스템을 구축할 필요가 있었습니다. 그러나 기존 OSS 분산 검색/분석 엔진으로는 성능과 보안 면에서 모두 부족하다는 점이 우려되었고 모니터링 환경도 재검토해야 했습니다.”라고 말했습니다.

bitbank의 AWS 전문가 Yatsu는 “로그를 완전히 분석하고 활용할 수 없었을 뿐만 아니라, 검색/분석 엔진 시스템이 복잡해 AWS 이용료 부담이 커지고 있었습니다.”라고 덧붙였습니다.

업종
금융

본사
KDX Nishigotanda Building, 7th Floor, 7-20-9 Nishigotanda, Shinagawa Ward, Tokyo

규모
70명

사용 사례
보안 인텔리전스

bitbank, inc.
리스크 관리 부서
Kenji Hashimoto

bitbank, inc.
시스템 부서
데이터 팀장
Yuuma Wakimoto

bitbank, inc.
시스템 인프라 팀
Kaori Yatsu

애플리케이션 로그에서 오류를 감지하는 데도 문제가 있었습니다. bitbank의 데이터 분석 전문가 Wakimoto는 “애플리케이션 오류 감지의 경우, 미리 정해진 패턴의 간단한 오류만 탐지할 수 있었습니다. 오류 감지 시 알림 기능이 있긴 하지만 세부 사항은 직원들이 직접 판단해야 하기 때문에 별로 효율적이지 않았습니다.”라고 설명했습니다.

AWS 호환성이 뛰어난 Sumo Logic 도입

2019년 6월, bitbank는 모니터링 환경을 조성하기 위한 첫 걸음을 떼며 그 시작점으로 Sumo Logic의 SaaS형 SIEM(보안 정보 및 이벤트 관리) 솔루션인 ‘Sumo Logic’을 도입했습니다.

이 솔루션을 선택한 주요 이유는 클라우드를 기반으로 하며 구성 및 운영상의 부담을 줄일 수 있다는 점이었습니다. Hashimoto는 “Sumo Logic의 많은 장점 중에서도 가장 큰 장점은 회사의 시스템과 동일하게 AWS에서 제공되기 때문에 로그 연동이 쉽고, 필요에 따라 신속하게 리소스를 늘리거나 줄일 수 있다는 점입니다.”라고 평가했습니다.

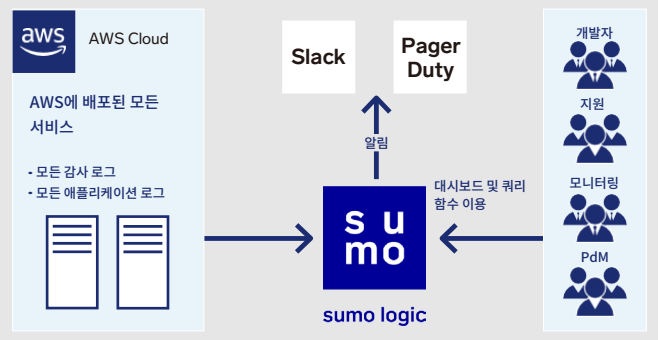
Wakimoto는 로그 데이터에 대해 “대량의 데이터를 검색할 때도 속도가 빠르다는 점이 아주 마음에 듭니다. 또한 비정형 데이터는 자동으로 정형 데이터로 변환됩니다.”라고 설명했습니다. 지불해야 할 이용료는 저장된 데이터의 양에 따라서만 결정되며 ISMS, SOC2, PCI DDS 등 Sumo Logic이 획득한 많은 국제 인증을 통해 검증된 보안 신뢰도 또한 Sumo Logic 솔루션을 도입한 이유가 되었습니다.

이 솔루션은 도입 결정 후 약 1개월의 테스트 기간을 거쳐 2019년 10월부터 본격 가동되었습니다. 실제 데이터를 이용해 테스트 환경을 검증했으며, 이는 큰 변화 없이 프로덕션 환경으로 전환되었습니다.

“검증에 쓸 수 있는 계정을 여러 개 발급받은 덕분에 다양한 시도를 해보고 매우 효율적으로 검증을 수행할 수 있었습니다.” (Yatsu)

로그 수집 및 검색 효율성 대폭 향상, 추후 전사적 로그 활용 허용 방안 검토 중

Sumo Logic을 도입한 결과, bitbank는 견고한 모니터링 시스템을 구축할 수 있었습니다. “Sumo Logic 덕분에 재무 감사 및 IT 통제 시스템 대응 능력을 향상시킬 수 있었을 뿐만 아니라, 보안 조치도 대폭 개선할 수 있었습니다. 상세 로그 감사에서도 빠르고 정확한 검색이 가능하며 직관적인 대시보드 덕분에 필요한 로그를 신속하게 찾을 수 있습니다.” (Hashimoto)



Yatsu는 운영 측면에서 “이제 높은 수준의 로그 분석도 수행할 수 있게 되었습니다. 기존 검색 및 분석 엔진을 더 이상 이용하지 않기 때문에 시스템 복잡성 문제가 해소되었으며, 관련 비용도 절감할 수 있었습니다.”라고 평가했습니다.

Wakimoto는 애플리케이션 오류 감지에 대해 “이제 복잡한 패턴을 이용해 감지할 수 있게 되었고, 그에 따라 서비스 품질도 향상되었습니다.”라고 설명했습니다. 오류뿐만 아니라 작업 실행 시간도 로그를 이용하여 측정되므로 AWS 비용도 최적화할 수 있게 되었습니다.

Wakimoto는 “일반적으로 수집하고 싶은 로그가 있으면 애플리케이션 개발 중에 수집 방법을 통합해야 합니다. 하지만 Sumo Logic에서는 이런 작업이 전혀 필요하지 않습니다. 모든 로그가 저장되며 필요한 로그를 나중에 검색할 수 있습니다. 덕분에 로그 활용 범위가 확대되어 개발 및 운영 부담이 크게 줄었습니다.”라고 설명했습니다.

향후 bitbank는 새로운 모니터링 환경 활용을 가속화하고, 비정상적으로 빈번한 로그인 활동 감지 또는 신원 도용 방지와 같은 사전 예방적인 보안 조치를 구현하고자 합니다.

또한 개발자와 고객 지원 및 마케팅 담당 직원이 업무에 정보를 활용할 수 있도록, 시스템 운영 관리자가 아닌 경우에도 로그 조회 및 분석을 허용하는 방안도 고려하고 있습니다. “Sumo Logic은 사용자나 로그 유형에 따라 매우 세부적인 설정을 적용할 수 있기 때문에, 보안 및 컴플라이언스 요건을 유지하면서 전사적인 로그 활용을 지원할 수 있을 것입니다.” (Hashimoto)

bitbank는 로그 활용 범위를 확대하는 방안을 적극적으로 추진하여 서비스 수준과 경쟁력을 한층 더 높이기 위해 노력하고 있습니다.

*1 2020년 2월 20일 CoinMarketCap 조사 결과
*2 2018년 10월 3일 ICORating 조사 결과

bitbank 소개

2014년에 설립된 bitbank는 암호화폐(가상화폐) 거래소 bitbank.cc 운영에 주력하고 있습니다. bitbank는 비트코인 등 6종의 가상화폐를 취급하고 있으며 업계 최저 스프레드(매수가와 판매가의 차이)를 제공합니다. bitbank에서 서비스하는 앱은 일본 앱스토어에서 1위를 차지한 바 있으며, bitbank는 많은 사용자로부터 지속적인 지원을 받고 있습니다.

Sumo Logic 소개

Sumo Logic Inc.(NSDQ: SUMO)는 새로운 소프트웨어 분야인 컨티뉴어스 인텔리전스를 선도하여 모든 규모의 고객사가 디지털 전환, 첨단 애플리케이션과 클라우드 컴퓨팅으로 인해 대두되는 데이터 관련 문제와 기회에 대응할 수 있도록 지원합니다. Sumo Logic Continuous Intelligence Platform™은 애플리케이션, 인프라, 보안 및 IoT 데이터의 수집, 처리 및 분석을 자동화하여 단 몇 초만에 실용적인 인사이트를 도출합니다. 전 세계 2,100개 이상의 고객사가 Sumo Logic을 사용하여 최신 애플리케이션 및 클라우드 인프라를 구축, 실행 및 보호하고 있습니다. 오직 Sumo Logic만이 다양한 사례에서 진정한 멀티 테넌트 SaaS 아키텍처로서의 플랫폼을 제공하여 인텔리전스 이코노미 부문에서 기업이 성장할 수 있도록 지원합니다. 더 자세한 내용은 www.sumologic.com에서 확인해 보세요.

sumo logic

Sumo Logic Japan KK
이메일: info-jp@sumologic.com

sumologic.jp