사례 연구

Barclays: 미래를 위한 플랫폼

Tanium 아키텍처로 IT 운영 및 보안을 강화한 사례

40개국에 300,000개 이상의 엔드포인트를 보유한 Barclays는 과다한 포인트 솔루션, 패치 관리 문제 및 침해 사고 대응 팀의 불만 문제에 대처하고 있었습니다. Tanium 플랫폼을 통해 조직은 모든 포인트 도구를 통합하고, 패치 적용을 관리하는 효과적인 방법을 찾을 수 있었으며, 사고 대응 시간을 몇 분으로 단축할 수 있었습니다.

2008년 금융 위기 이후 글로벌 은행은 늘어 나고 있는 사업 규제 압력에 직면하고 있었습니다. 전 세계 4,800만 명의 고객과 2조 4,200억 달러 이상의 자산을 보유한 세계 7대 은행인 Barclays도 예외는 아니었습니다. Barclays는 영국 중앙은행의 취약성 테스트인 CBEST와 기타 규제 요건으로 인하여 보안 대응의 속도, 민첩성 및 확장성을 향상시키기 위해 새로운 툴에 투자하기로 결정했습니다.

그리고 2016년에 Tanium을 도입했습니다. Barclays의 IT 리더들은 40개국 300,000개 이상의 엔드포인트를 명료하게 관리 할 수 있다는 Tanium의 약속에 깊은 인상을 받았습니다. 또한 기존 보안 툴의 성능을 향상 시키는 것뿐만이 아니라 호환성을 보장 할 수 있는 솔루션이 필요했습니다. 7월 Tanium을 도입한 이후 다른 솔루션 검토는 더이상 필요하지 않았습니다. Barclays의 그룹 최고 보안 책임자 Troels Oerting은 “전 세계에 분산된 엔드포인트 환경을 파악하고 이를 운영하는 것에 많은 어려움을 겪고 있었습니다. 하지만 우리는 처음으로 Tanium을 통해 우리의 IT 환경을 빠르고 정확하게 파악할 수 있었습니다.”

Tanium Use Case

- 시큐리티 하이진 (Security Hygiene)
- 엔드포인트 탐지 및 대응 (EDR)

해결 과제

- 전 세계적 엔드포인트 가시성 확보 및 컨트롤
- 보안 사고 탐지, 방지 및 문제 해결 시간
- 완벽한 패치 배포
- 다양한 엔드포인트 툴 통합

혜택

- 보안 사고 문제 해결 시간 몇 분 내로 단축
- 실시간 확인 가능한 성공적인 패치
- 전 세계적으로 분산된 300,000개 이상의 엔드포인트 가시성 확보 및 컨트롤
- 비즈니스 신뢰도 향상 및 비용 절감

싱글 플랫폼에서 엔드포인트 통합

Barclays 역시 대기업이 공통으로 갖고 있는 문제점 중 하나인 상호운영이 제한된 전문 툴을 많이 갖고 있었습니다. 툴 사용의 어려움 외에도, 이러한 툴이 필요한 데이터 생성에 최소 몇시간 혹은 며칠, 몇 주가 필요하였습니다.

Tanium의 플랫폼은 Barclays가 운영하는 모든 엔드포인트의 위협을 탐지하고 이들이 정상 작동할 수 있도록 합니다. 이는, 필요한 상황에 적합한 데이터를 제공함으로써 다른 보안 툴을 더 스마트하게 만들 수 있습니다.

Tanium 플랫폼의 또 다른 특징은 엔드포인트 관리 및 보안에 필요한 기능을 쉽게 추가할 수 있습니다. Barclays는 과거 새로운 기능을 추가할 때 커스트마이징 개발이 필요했다면, 이제는 Tanium 플랫폼을 활용하여 클릭 한번으로 필요한 기능을 손쉽게 추가 할 수 있습니다.

패치 작업의 어려움

Barclays의 IT 팀은 윈도우 서버 패치 작업에 많은 노력을 하였지만, 늘 많은 어려움이 있었습니다. 호환성 문제가 발생하면 서버 성능이 저하되거나 심각 시 서버 장애를 일으킬 수도 있습니다. 패치는 기업의 IT 환경을 보호하고 공격자가 소프트웨어 취약성을 활용하는 것을 방지하기 위한 중요한 활동입니다.

과거 IT팀은 패치 배포의 성공 및 실패 확인을 위해 패치 실행 종료 시까지 기다려야 했습니다. Tanium은 패치 배포 상황을 실시간으로 확인 할 수 있어, 서버 호환 문제 발생시 바로 조치 및 해결이 가능합니다.

신속한 보안 사고 대응

Barclays 사이버 침해 사고 대응팀은 잠재적 보안 위협에 대비한 기업 전체의 엔드포인트 가시성을 확보하고, 사고 범위를 정하여 문제 발생 시 이를 실시간 해결 및 대응 해야하는 어려움을 갖고 있었습니다. Tanium을 도입하기 전 팀은 문제 해결에 필요한 로그 수집에만 많은 시간을 사용하였습니다. 하지만, Barclays는 Tanium 도입 후 엔드포인트에 직접 접속하여 로그 확인을 신속히 할 수 있게 되었습니다.

이러한 빠른 속도로 인해 IR 팀은 위협을 처리하기 위한 새로운 프로세스를 개발하게 되었습니다. Barclays는 Tanium으로 실시간 문제를 확인하고 이를 해결할 수 있으며, 단 몇 분 만에 프로세스를 개선하여 위험을 크게 줄일 수 있습니다.

Tanium과 함께 미래 준비

Barclays는 현재 다양한 모듈을 사용중이나, 컴플라이언스를 준수하기 위해 Tanium Comply 모듈을 추가하고자 합니다. Tanium Comply의 엔드포인트 취약성 스캔 기능은 소프트웨어 인벤토리 및 위험 분석에 도움이 됩니다.

Tanium 모듈을 추가하는 것은 매우 간단하면서도 배포에 필요한 비용이 들지 않습니다. 이를 통해 Barclays는 효율적으로 플랫폼을 확장하고 개발하여 필요한 구체적인 요건를 충족할 수 있습니다. Tanium 플랫폼의 운영은 모듈 전반에 걸쳐 일관성을 유지하기 때문에 Barclays는 필요시 Tanium 모듈을 언제든지 계속 추가하여 사용 할 수 있으며, 이에 따른 사용자 재교육에 필요한 시간과 비용을 절감할 것으로 기대하고 있습니다.

Barclays는 IT 보안 팀이 얻은 혜택뿐만 아니라 비즈니스에도 엄청난 이점이 있음을 단시간에 확인했습니다. 또한, 비용 절감 및 철저한 데이터 보호로 고객 신뢰도까지 높일 수 있었습니다.

회사 정보

Tanium은 세계에서 가장 높은 보안 수준의 IT 환경을 위한 통합 엔드포인트 관리 및 보안 플랫폼을 제공합니다. 매우 빠른 속도, 가시성 및 규모를 제공하는 당사는 Fortune 100대 기업의 절반, 상위 소매업체 및 금융기관 그리고 미정보기관/육/해/공/해병대를 지원하고 있으며, 이들 조직은 Tanium을 활용하여 신속한 비즈니스 결정을 내리고 효율적으로 운영하며 보안위험을 줄이고 있습니다. Tanium은 최근 Forbes 선정 “2019년 최고의 100대 클라우드 컴퓨팅 민간 기업”에서 7위, FORTUNE 선정 미국 “최고의 100대 중소기업 직장” 10위, 영국 최고 직장 18위를 차지했습니다. www.tanium.com을 방문하거나 LinkedIn과 Twitter에서 팔로우하세요.

TANIUM