사례 연구: AKAMAI IT 부서

AKAMAI가 **ENTERPRISE THREAT PROTECTOR**를 사용하는 이유

목차

EXECUTIVE SUMMARY

Akamai의 IT 부서는 2017년 3월에 Akamai 사내 유무선 네트워크에 Enterprise Threat Protector를 구축했습니다.

3월부터 5월까지의 기간 동안 Enterprise Threat Protector로 유의미하고 수치화된 성과를 얻을 수 있었습니다.

구체적인 내용은 다음과 같습니다.

- 기존 엔드포인트 보호 솔루션으로 탐지된 멀웨어의 개수가 3월~4월에는 **54%**, 3월~5월에는 **37%** 감소했습니다.
- 기존 고급 탐지 솔루션에서 발생한 이벤트의 개수가 3월~4월에는 **30%**, 3월~5월에는 **15%** 감소했습니다.
- 기존 엔드포인트 보호 솔루션과 고급 탐지 솔루션에서 발생한 알림과 이벤트 건수가 줄어든 결과 **상근직(FTE) 직원 1인의 0.75**에 해당하는 시간이 절약되었습니다.

엔드포인트 보호

Akamai는 멀웨어 탐지 기능과 침입 방지 기능이 포함된 엔드포인트 보호 솔루션을 구축했습니다.

멀웨어 감염 사고

멀웨어 감염 현황에 주력하기 위해 멀웨어 지표에서 "애드웨어"와 "필요하지 않은 소프트웨어" 알림이 제외되도록 필터링했습니다. Enterprise Threat Protector를 구축한 결과 3월(199)~4월(92)에 탐지된 멀웨어 감염 사고 건수가 54%, 3월~5월(125)에 탐지된 멀웨어 감염 사고 건수가 37% 줄어들었습니다.

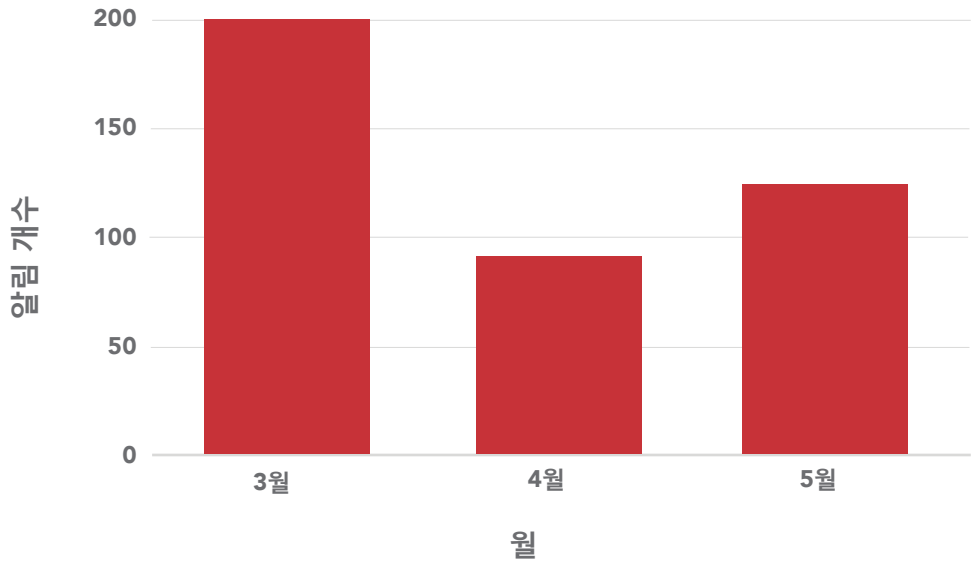

그림 1 – Enterprise Threat Protector를 구축한 결과 감소한 멀웨어 사고 건수

침입 방지 시스템(IPS) 알림

엔드포인트 IPS에 의해 생성된 알림도 비슷한 정도로 줄어들었습니다. 알림 중 대부분을 토렌트가 차지했으나, 3월~4월에, 그리고 3월~5월에 발생한 알림 수가 큰 폭으로 감소했습니다.

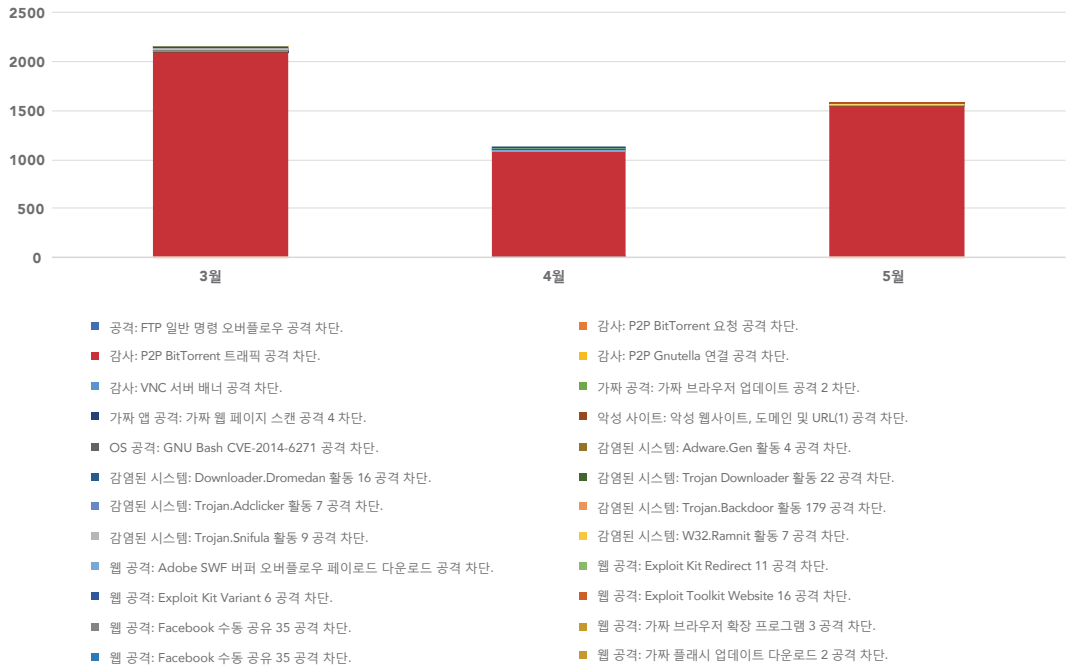

그림 2 – Enterprise Threat Protector를 구축한 결과 감소한 IPS 알림(토렌트 포함)

토렌트를 모두 제외해 보아도 3월~4월에 27%, 3월~5월에 35%가 감소한 것을 알 수 있습니다.

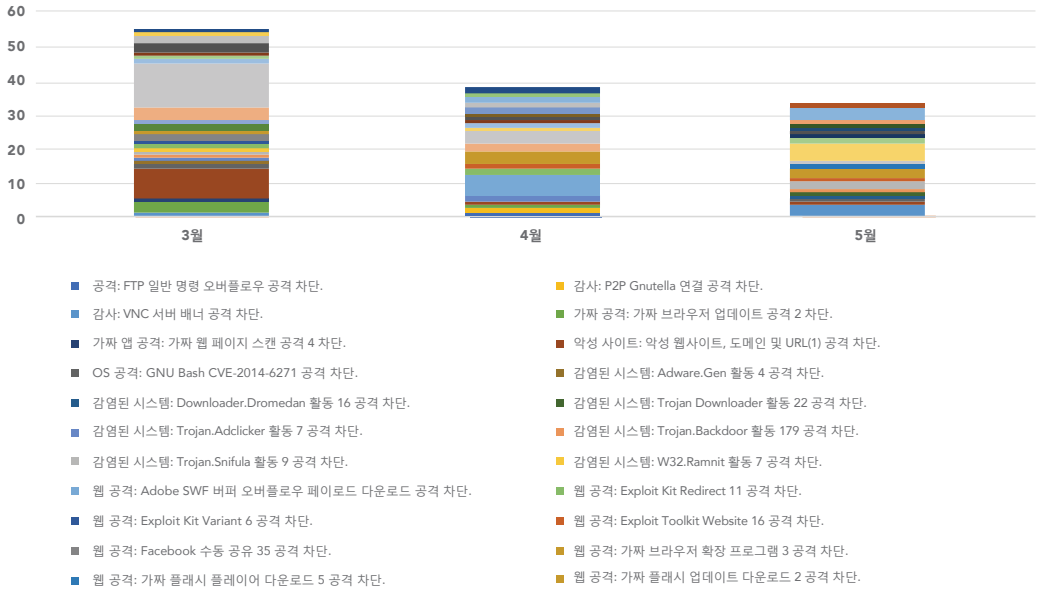

그림 3 – Enterprise Threat Protector를 구축한 결과 감소한 IPS 알림(토렌트 제외)

토렌트를 제외하면 IPS에서 두 번째로 많이 생성된 알림은 악성 웹사이트, 도메인 및 URL이었으며, 웹 공격과 가짜 웹 페이지 스캔 공격이 그 뒤를 이었습니다.

알림	3월 알림	4월 알림	5월 알림
악성 웹사이트, 도메인 및 URL	13	1	1
웹 공격과 가짜 웹 페이지 스캔 공격	12	4	1

표 1 – Enterprise Threat Protector를 구축한 결과 감소한 IPS 알림 건수

고급 탐지

Akamai는 추가적인 보안 레이어를 제공하는 보조 방어 메커니즘으로 기능하는 고급 탐지 솔루션을 구축했습니다. 이 솔루션은 개수는 비교적 적으나 중요도는 훨씬 높은 알림을 생성합니다.

그림 4에서 Enterprise Threat Protector를 구축한 결과 이 솔루션에서 생성된 알림의 건수도 줄어든 것을 볼 수 있습니다.

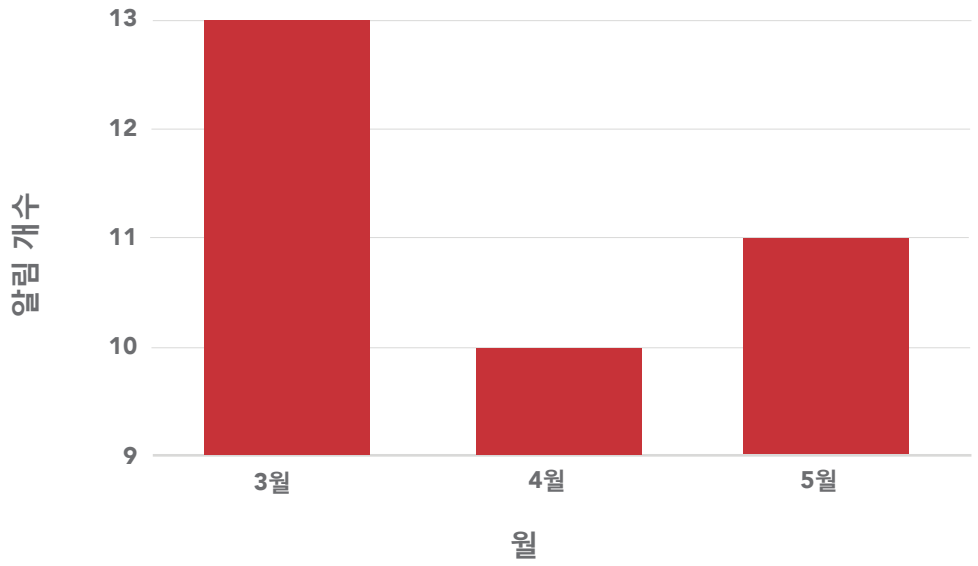

그림 4 – Enterprise Threat Protector를 구축한 결과 감소한 고급 탐지 알림

ROI

Enterprise Threat Protector를 구축한 뒤 사고 및 알림 건수가 줄어든 결과 귀중한 시간을 절약할 수 있었습니다.

"감축된 시간"은 평균 대응 시간 추산치, 멀웨어 사고 대응에 걸린 시간 및 토렌트 소프트웨어를 제거하는 데 걸린 시간을 사용하여 산출했습니다. 이는 매달 기본적으로 수행되는 운영 작업입니다. 토렌트의 개수도 줄어든 것을 볼 수 있었습니다.

월	사용자 수	차단된 토렌트 IP 개수
3월	56	2,089
4월	48	1,100
5월	40	1,546

표 2 – IPS 모듈 알림

멀웨어 조사에는 사고 1건당 조사, 대응 및 조치에 소요된 시간이 사용되었습니다.

이와 같은 지표를 사용하여 감축된 시간을 계산한 결과 Enterprise Threat Protector를 구축함으로써 매월 평균 **상근직(FTE) 직원 1인의 0.75**에 해당하는 시간이 절약되었음을 알 수 있었습니다.

엔드포인트 보호 솔루션의 멀웨어 모듈과 IPS 모듈을 함께 사용하여 Enterprise Threat Protector를 구축한 결과 4월~6월의 평균 대응 시간을 계산하고 Enterprise Threat Protector를 구축하기 전인 3월의 평균 대응 시간과 비교했습니다.

결과는 다음과 같습니다.

- **멀웨어 탐지 모듈**: **27시간** 감축
- **IPS 모듈**: 사고 대응 시간 **8시간** 감축

감축된 대응 시간(단위: 시간)	
멀웨어 모듈	27
IPS 모듈	8
합계	**35**

표 3 – 멀웨어 및 IPS 모듈 알림(Enterprise Threat Protector를 구축한 결과 감축된 대응 시간)

사고 1건당 초기 대응부터 조치가 이루어지기까지 걸린 평균 시간까지 감안하면 매월 엔드포인트 멀웨어 모듈의 경우 **51시간**, IPS 모듈의 경우 **24시간**이 감축되었습니다.

감축된 조치 시간(단위: 시간)	
멀웨어 모듈	51
IPS 모듈	24
합계	**75**

표 4 – 멀웨어 및 IPS 모듈 알림(Enterprise Threat Protector를 구축한 결과 감축된 조치 시간)

따라서 Enterprise Threat Protector를 구축한 결과 약 **110시간**이 감축되었다는 결론을 확인할 수 있었습니다.