위협 인텔리전스를 통해 보안을 향상한 최고의 인적 자원 관리 기업 사례

ADP는 지능형 악성코드 분석 및 글로벌 위협 인텔리전스를 보안 플랫폼과 통합하여 클라이언트 지원을 향상합니다.

핵심 요약

ADP

- 인적 자원 관리
- 뉴저지, 로즈랜드
- 직원 수 52,000명

과제

- 악성코드 공격 수 감소
- 악성코드 방어 프로세스 자동화
- 악성코드 분석을 보안 플랫폼과 통합

솔루션

- 단일 솔루션으로 악성코드 분석 기술, 서비스, 인텔리전스 제공
- 회사에서 제공하는 모든 업계에 대한 글로벌 위협 인텔리전스
- 지원 팀의 전문 지식으로 탁월한 보안 보호 지원

비즈니스 성과

- 단일 모니터링 플랫폼에 악성코드 분석 및 위협 인텔리전스 통합
- 일일 악성코드 분석 및 자가 검사량 20배 증가
- 예방 조치에 대한 더욱 빠르고 정확한 의사 결정

당면 과제

클라우드 기반 인적 자원 관리 솔루션을 제공하는 종합적인 글로벌 기업인 ADP는 전 세계 100여 개국에서 625,000개 이상의 회사에 인사, 급여, 인재, 세금, 성과급 관리 솔루션을 제공하고 있습니다. ADP는 Fortune 500대 기업에 속할 뿐만 아니라, 다른 Fortune대 500대 기업 중 80%에 서비스를 제공하고 있으며 Fortune 100대 조직 가운데 90%가 넘는 조직에도 서비스를 제공하고 있습니다. 2014년 ADP는 전 세계 3,600만 명 이상의 사람들에게 급여를 지불하고, 미국 내에서 1조 5천억 달러에 달하는 고객 세금, 계좌 입금, 관련 자금의 이동을 단독으로 처리했습니다.

보안 및 개인정보 보호는 두말할 필요 없이 ADP의 가장 중요한 사안이며, 이는 고객의 신뢰를 유지하고 위험을 줄이기 위한 토대입니다. ADP의 CSO(Chief Security Officer)인 Roland Cloutier는 보안, 위험, 개인정보 보호가 곧 자사가 일컫는 비즈니스 운영 보호와 같은 의미라고 말합니다. 최고 보안 책임자인 Cloutier는 "이는 우리가 비즈니스를 설계하는 방식의 일부라고 할 수 있습니다. 우리는 업계에서 검증된 최신 툴, 전략, 기법, 절차를 사용하여 비즈니스 프로세스에 영향을 미칠 수 있는 모든 위험 및 취약점을 식별합니다"라고 설명하며, "우리가 고객에게 제공하는 서비스의 연속성을 보장할 수 없다면, 이는 해당 고객의 비즈니스 및 관련 경제에 큰 피해를 입힐 것입니다"라고 덧붙여 말합니다.

ADP 비즈니스를 둘러싼 현재의 사이버 보안 환경은 광범위하고 복잡합니다. 이어 그는 "각 비즈니스 부문별로 서로 다른 위협 및 위협 벡터가 존재합니다. 소비자의 신원 정보를 비롯하여 보호된 정보에 액세스하기 위해 다양한 플랫폼을 표적으로 하는 공격을 볼 수 있습니다"라고 했으며,

"우리가 중점을 두는 점은 우리 회사의 플랫폼에 누가 어떤 목적으로 액세스하는지 파악하는 것입니다. 우리는 위조된 액세스 유형 또는 사이버 공격을 근절하고 회사 플랫폼의 지속 가능성과 업타임을 보장하고자 합니다"라고 덧붙여 설명했습니다. "이러한 이유로 Cisco® AMP Threat Grid를 눈여겨보게 되었습니다."

> “이는 ADP를 24시간 방어할 수 있도록 지원하는 통합 방어 시스템입니다.”
>
> **— ADP CSO(Chief Security Officer), Roland Cloutier**

솔루션

ADP의 보안 플랫폼에는 12개 이상의 기술이 조합되어 있으며 회사에서는 이를 함께 사용하여 운영 모델을 만듭니다. 그리고 보안 팀은 이러한 운영 모델을 사용하여 해당 환경의 방어 상태를 검토할 수 있습니다. 이는 ADP가 악성 트래픽을 신속하게 식별하고 전체 위협을 파악한 후, 회사 내에서 이러한 위협이 실행되는 것을 방지하는 데 도움이 됩니다. "우리 회사는 뛰어난 시스템을 갖추었으나, 더 많은 공격을 경험하고 있으며 이를 해결할 시간은 더욱 부족한 실정입니다. 우리는 에코시스템의 구성 요소 중 자동화할 수 있는 구성 요소를 검토하기 시작했으며, Threat Grid가 즉시 눈에 들어왔습니다. 우리 회사는 악성코드 방어 프로세스에 점점 더 많은 비중을 두고 있기 때문입니다"라고 Cloutier는 설명했습니다.

철저한 평가 프로세스 후, ADP는 몇 가지 주요 조건에 따라 Cisco AMP Threat Grid를 사용하기로 결정했습니다. 이어 그는 "Threat Grid를 선택한 첫 번째 이유는 이 솔루션의 효과 때문입니다. Threat Grid에서 하나의 패키지로 제공되는 기술, 서비스, 인텔리전스 기능은 이전의 그 어떤 솔루션과도 차원이 달랐습니다”라고 전했습니다. 다른 결정 요인으로는 Cisco AMP Threat Grid 팀의 솔루션 및 전문 지식을 통해 제공되는 심층적인 기술 인텔리전스가 포함되었습니다. Cloutier는 "평가 프로세스 동안 Threat Grid 팀에 어떤 내용을 문의해도 문제가 되지 않았습니다. 또한, 어떤 업계에 위협이 발생했는지 또는 어떤 위협 프로세스가 관련되었는지 여부도 문제가 되지 않았습니다. Threat Grid 팀은 당사가 전반적인 보호 운영을 지속적으로 향상하는 데 도움이 되는 심층적인 지식을 보유하고 있었습니다"라고 설명했습니다.

오늘날, ADP에서는 Cisco AMP Threat Grid를 두 가지 방법으로 사용하고 있습니다. 첫째, 네트워크 트래픽의 특정 부분을 자동으로 추출하고 해당 트래픽이 위협적인지 아닌지 여부를 평가합니다. 둘째, 이 솔루션의 광범위한 심층 인텔리전스 플랫폼을 Cisco AMP Threat Grid API를 사용하는 보안 인텔리전스 플랫폼에 있는 자사의 분석 시스템과 통합했습니다. Cloutier는 "우리 회사는 인텔리전스 중심의 보안 방식을 채택하게 되었습니다. 따라서 위협 인텔리전스는 당사의 의사 결정 지원 인프라를 구성하는 한 부분이며, 이는 당사가 매일 의사 결정을 수행하는 방식의 핵심 구성 요소입니다. 이러한 인텔리전스는 더욱 빠른 알림을 생성하고 신속한 결정을 내리는 데 도움이 됩니다”라고 전했습니다.

ADP에서는 이제 Cisco AMP Threat Grid의 상황 기반 위협 인텔리전스를 사용하여 미래에 어떤 요소가 무슨 이유로 회사를 공격할 가능성이 있는지 파악할 수 있습니다. 또한, 이는 가장 비용 효율적인 방식으로 최상의 방어를 형성하는 데 필요한 요소가 무엇인지 파악하는 데도 도움이 됩니다.

이어 그는, "Threat Grid는 단일 제품을 통해 우리가 악성코드 방어 프로그램을 자동화하고 인텔리전스 프로그램을 확장할 수 있도록 지원했습니다. Threat Grid는 이제 우리 회사의 신뢰할 수 있는 보안 플랫폼의 핵심 구성 요소로서 구현된 상태입니다. 이는 주요 네트워크 트래픽 요소를 확인하고 해당 트래픽의 악성 여부를 결정하는 자동화된 악성코드 방어 및 방지 메커니즘입니다"라고 덧붙여 말했습니다.

결과

Cisco는 보안, 위험 관리, 개인정보 보호 측면에서 ADP의 종합적인 보안 에코시스템을 구성하는 장기적이고 신뢰할 수 있는 파트너이자 필수적인 요소로서의 역할을 해왔습니다. 이제 Cisco AMP Threat Grid도 이러한 역할을 수행합니다.

Cloutier는 "Threat Grid로 인해 수작업 프로세스가 없어졌으며 향상된 의사 결정 기능을 갖춘 클라우드 기반 서비스를 사용할 수 있게 되었습니다. 따라서 사람이 직접 작업을 수행하던 때보다 하루에 10배 또는 20배 이상의 악성코드 검사를 수행할 수 있습니다. 또한, 이러한 자동화된 방어 솔루션 덕분에 악성코드 리버스 엔지니어링 및 악성코드 해독 같은 작업을 수행하는 역량이 대폭 강화되었습니다"라고 설명했습니다.

제품 목록

- Cisco AMP Threat Grid
- Cisco AMP(Advanced Malware Protection) for Networks
- Cisco NGIPS(Next-Generation Intrusion Prevention System)
- Cisco Cyber Threat Defense
- Cisco AnyConnect® Secure Mobility Solution
- Cisco Incident Response Services

Cloutier는 보안 기술, IT 기술, 클라우드 비즈니스 플랫폼 내의 트랜잭션을 포함한 ADP의 방대한 인프라 및 보안 인텔리전스 공급자가 하루에 확인하는 이벤트의 수는 약 80억 개에 달한다고 밝히며, "침입 탐지 플랫폼, DPI(Deep Packet Inspection) 기술 또는 비정형 데이터 보호 환경을 막론하고, 이러한 모든 요소는 이제 단일한 모니터링 플랫폼으로 함께 통합되어 당사의 글로벌 위협 모니터링에 대한 정보를 제공합니다"라고 말했습니다. 그는 또한 Cisco AMP Threat Grid는 API를 통해 준비 및 연결되므로, 방어 시스템 중 하나에서 잠재적인 위협을 탐지한 경우 ADP에 알림이 전송된다고 설명하며, "위협이 탐지되면 어떤 악성코드에 주의해야 하는지 정의하는 데 도움이 될 수 있도록 몇 가지 중요한 분석을 실행합니다. 이는 ADP를 24시간 방어할 수 있도록 지원하는 통합 방어 시스템입니다"라고 전했습니다.

Cloutier가 생각하는 Cisco AMP Threat Grid의 가장 큰 이점은 속도와 정확성입니다. "속도 관점에서 보았을 때, 우리는 위협적인 트래픽을 확인할 수 있는 기능을 대폭 강화하고 매우 빠른 속도로 결정을 내릴 수 있게 되었습니다. 또한, Threat Grid의 위협 인텔리전스를 사용하여 ADP의 벽을 넘어 우리가 지원하는 시장 및 업계의 정황도 살펴볼 수 있습니다. 이를 통해 특정 유형의 데이터에 대한 구체적인 위협 인텔리전스를 확인하고, 사전 예방적인 조치를 취할 수 있습니다."

Cisco 및 Cisco AMP Threat Grid 팀은 글로벌 전문 지식, 심층적인 기술, 지식을 활용하여 ADP가 보안 플랫폼을 최적화하고 회사 보안을 하루하루 꾸준히 실현할 수 있도록 지원합니다. Cloutier는 끝으로 다음과 같이 덧붙였습니다. "Cisco와 Threat Grid와의 관계를 통해 얻고자 한 심층적인 기술 파트너십이 바로 이것입니다. Cisco에 대한 투자는 매우 현명했습니다. Cisco의 기술 및 전문 지식을 당사의 기존 플랫폼 및 전략과 함께 활용하여 당사에 다시 제공되는 서비스의 제공 속도를 단축할 수 있게 되었습니다."

추가 정보

Cisco AMP Threat Grid에 대한 자세한 내용을 보려면 www.cisco.com/go/amptg를 참조하거나 여기에서 ADP 비디오 사례 연구를 시청하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C36-735041-00 06/15