고객 사례 연구

19,000개 회원사의 악성코드 분석 자동화를 지원한 비영리 보안 기업의 사례

Center for Internet Security에서는 미국 정부기관에 대한 악성 공격 대응 시간을 단축하기 위해 Cisco® 지능형 악성코드 보안을 구축했습니다.

핵심 요약

CENTER FOR INTERNET SECURITY
- 보안
- 뉴욕, 올버니

과제
- 회원 조직의 악성코드 사고 해결
- 신속하고 정확한 대응을 위한 악성코드 분석 자동화
- 사고 증가 시 손쉽게 확장

솔루션
- 수천 개의 악성코드 샘플을 분석할 수 있는 확장 가능한 인프라
- 자동화된 악성코드 제출 및 해결을 지원하는 사용하기 쉬운 API
- 잠재적 위협을 실시간으로 분석할 수 있는 위협 인텔리전스 피드

비즈니스 성과
- 비용 효율적이고 자동화된 악성코드 분석
- 적시에 정확한 조치를 지원하는 상황 기반의 위협 콘텐츠
- 더욱 심층적인 통찰력으로 사전 예방적 악성코드 방어 지원

당면 과제

CIS(Center for Internet Security)는 공공 및 민간 부문 기관의 사이버 보안을 향상하도록 지원하는 비영리 조직입니다. CIS는 MS-ISAC(Multi-State Information Sharing and Analysis Center)의 출범 기관이기도 하며, 이는 미국 국토안보부에서 주, 지역, 민족, 영토(SLTT) 정부기관의 핵심 사이버 보안 리소스로서 지정한 프로그램입니다. MS-ISAC에는 모든 미국 주 정부기관은 물론 미국 영토 및 민족 기관, 그리고 수백 개에 달하는 지역 정부기관이 회원으로 포함되어 있습니다.

회원 여부에 상관없이, SLTT 정부기관은 매니지드 보안, 사고 대응, 악성코드 분석, 컴퓨터 포렌식 등의 서비스를 제공하는 24/7 운영 센터를 통해 MS-ISAC 사이버 보안 서비스를 이용할 수 있습니다.

계속해서 증가하는 악성코드 공격으로 인해, CIS에서는 MS-ISAC 서비스를 지원하려면 대규모 인프라 및 자동화된 악성코드 분석 기능을 갖춘 더욱 확장 가능한 솔루션이 필요하다는 사실을 깨닫게 되었습니다. CIS의 보안 서비스 부사장 Adnan Baykal은 다음과 같이 말합니다. "매일 수백만 개의 악성코드 샘플이 퍼블릭 도메인에 릴리스되고 있으며, 그 수는 점점 증가하고 있습니다. 그와 더불어, 국가 첩보원의 공격이 점점 증가함에 따라 신뢰할 수 있는 환경에서 자동화된 악성코드 분석이 더욱더 필요하게 되었습니다."

CIS에서 처음에는 사내 인프라 구축을 고려했으나, 추가적인 조사 결과 리소스가 제한된 비영리 조직으로서는 비용에 제약이 있는 방식이라는 결론을 내렸습니다. CIS에서는 처음에는 적은 양을 관리하다가, 필요에 따라 수천 개의 악성코드 제출 작업을 처리하도록 확장할 수 있는 솔루션을 찾기 시작했습니다. Baykal은 또한, "처음에는 많은 오픈 소스 솔루션을 살펴보았으나, 우리가 원하는 확장성을 제공하지 못했습니다. 또한, 오픈 소스 솔루션은 공격자들이 숨어 있는 퍼블릭 도메인에 있습니다. 공격자가 우리의 조사 내용을 발견할 경우 자신들의 TTP나 툴, 전략, 절차를 변경할 수 있으며 이렇게 되면 문제를 해결하기가 더욱 어려워집니다"라고 설명했습니다.

솔루션

시장에 출시된 수많은 악성코드 분석 플랫폼 중에서 CIS가 선택한 제품은 동적 악성코드 분석과 위협 인텔리전스를 하나의 솔루션에 통합한 Cisco AMP Threat Grid였습니다. 이 솔루션은 실시간 행동 분석 및 최신 위협 인텔리전스 피드도 제공하므로 CIS가 회원들의 문제에 신속하게 대응할 수 있습니다.

> "우리는 매일 수많은 악성코드 샘플을 처리할 수 있는 확장 가능한 인프라를 갖춘 신뢰할 수 있는 파트너를 원했습니다. 이 솔루션은 바로 이러한 기능을 제공합니다."
>
> **— Adnan Baykal, Center for Internet Security 보안 서비스 부사장**

Baykal은 이 솔루션이 수많은 다양한 방식을 통해 서로 다른 악성코드 샘플을 전환할 수 있는 기능 및 편의성을 갖추었다고 설명합니다. "Threat Grid를 통해 악성코드 샘플을 분석할 수 있으며 마우스 버튼 하나만 클릭하면 특정 지표에서 전환하고 동일한 지표를 가진 다른 모든 악성코드 샘플을 가져올 수 있습니다." 이에 따라 CIS는 불과 몇 분이면 악성코드의 활동 또는 목적, 위협의 범위, 이를 막을 수 있는 방법을 파악하는 데 필요한 기능을 확보합니다.

CIS는 Threat Grid를 사용하여 정적 및 동적 분석을 포함한 독자적인 기술을 통해 분석을 우회하도록 설계된 악성코드를 식별하고 샘플을 실시간으로 분석합니다. 또한, 이 솔루션은 전 세계에서 도출한 행동 분석 지표 및 악성코드 기술 자료를 사용하여 샘플이 악의적인지, 의심스러운지, 무해한지 여부와 그 이유를 식별합니다.

이 솔루션은 이러한 상황 기반 위협 콘텐츠를 사용하여 Threat Grid를 통한 심층 분석이 필요할 수 있는 특정 위협을 CIS가 파악할 수 있도록 지원합니다. 특정 도메인, URL 또는 IP 주소에 대한 지표가 있을 경우 Threat Grid는 수천 개의 지표 및 악성코드 샘플을 제공할 수 있으므로 CIS는 이것이 일반적인 위협인지 아닌지 식별할 수 있습니다. Baykal은 "Threat Grid는 이 공격의 배후자가 누구인지, 그리고 이러한 특정 위협이 일반적인 것인지 아니면 특정 기관을 노리는 것인지 파악하는 데 필요한 상황 정보를 제공합니다. 이 솔루션은 위협 인텔리전스를 클러스터링하여 이를 유의미한 데이터로 전환할 수 있도록 지원합니다. 또한, 이 솔루션은 서로 다른 악성코드 샘플의 상관관계를 고유한 방식으로 분석하여 악성코드 및 우리가 다루고 있는 위협에 대해 더 많은 정보를 제공할 수 있습니다"라고 설명합니다.

Baykal과 해당 팀이 찬사를 보낸 Threat Grid의 또 다른 기능은 기능 중심 API입니다. Baykal은 "차원이 다른 프론트엔드 및 맞춤형 인프라를 구축하여 역할 기반 액세스 제어를 통해 우리 팀과 회원들의 특정 요구 사항을 더욱 향상된 방식으로 지원할 수 있게 되었습니다"라고 전했습니다. 이 프론트엔드를 MCAP라고 하며, 이는 악성 코드 분석 플랫폼(Malicious Code Analysis Platform)의 약어입니다. "회원들은 MCAP를 사용하여 커뮤니티를 구축할 수 있으므로 사고 대응 팀에서는 악성코드 샘플을 제출하고 태그를 추가할 수 있으며, 샘플의 구체적인 특징을 다른 커뮤니티 회원과 공유하지 않고도 다른 샘플을 확인할 수 있습니다."

"우리는 매일 수많은 악성코드 샘플을 처리할 수 있는 확장 가능한 인프라를 갖춘 신뢰할 수 있는 파트너를 원했습니다. 이 솔루션은 바로 이러한 기능을 제공합니다"라고 Baykal은 말합니다. "우리에게 꼭 필요했던 심층 분석 기능을 제공하며, 회원을 위한 솔루션을 맞춤화할 수 있는 기능 또한 마찬가지입니다."

결과

인프라 관점에서 보았을 때, Cisco AMP Threat Grid의 확장성은 물론 지능형 악성코드 분석 기능 및 위협 인텔리전스 피드 역시 CIS에 적합한 기능입니다. Baykal은 "악성코드를 제출하면 적시에 정확한 결과를 얻을 수 있습니다. 또한, 위협 인텔리전스 피드를 통해 수백만 개의 악성코드 샘플 및 지표에 액세스할 수 있으며 이는 전 세계의 악성코드 샘플 간의 상관관계를 밝히고 분석하며, 완전한 위협 그림을 구축하는 데 도움이 됩니다"라고 언급했습니다.

MCAP 프론트엔드는 회원들에게도 유용합니다. Baykal은 또한, "사용자가 MCAP를 사용할 경우, 일련의 풀다운 메뉴를 통해 필요한 지원 유형이 현장 지원인지 또는 전화 통화인지 등의 악성코드에 대한 정보를 제출할 수 있습니다. 정보를 제출한 지 몇 분 내에 악성코드 행동에 대한 분석 결과를 받을 수 있습니다. 사용자는 문제의 범위에 대한 방안, 그리고 신뢰할 수 있고 정확한 치료 권장 사항을 개발하는 데 필요한 모든 지표를 얻게 됩니다"라고 덧붙였습니다. 예를 들어, 네트워크 지표는 기관의 네트워크 그룹과 공유할 가능성이 가장 높습니다. 이를 통해 경계 방화벽 또는 코어 라우터에서 예방 조치를 취하여 특정 IP 주소 또는 도메인을 차단하기 위해서입니다.

Threat Grid의 폭넓고 심층적인 기능을 통해 CIS는 더욱 광범위한 글로벌 위협 그림을 볼 수 있습니다. 이 단계에서 CIS는 모든 회원에게 악성코드 지표와 함께 주의보를 발령하는 등의 적절한 조치를 결정하여 해당 기관이 더욱 사전 예방적인 방어 체계를 갖출 수 있도록 합니다. 그리고 정부기관에서 추가적인 안내를 필요로 할 경우, CIS는 특정 위협 행위자가 어떤 행동을 하는지, 어떤 방식으로 이동하는지, 필요한 대응은 무엇인지 등을 비롯하여 어떤 작업을 처리해야 하는지 해당 기관이 파악할 수 있도록 지원을 제공합니다. 필요한 경우, CIS는 현장에 팀을 구축하여 사고 대응 프로세스를 지원하도록 할 수 있습니다.

Baykal은 끝으로 다음과 같이 덧붙였습니다. "솔루션 운영의 투명성, 커뮤니케이션, 그리고 가장 중요한 요소인 업타임. 이 모든 점을 고려했을 때 신뢰할 수 있는 파트너와 함께하고 있다고 확신할 수 있습니다. 우리는 Cisco를 신뢰할 수 있으며, 회원들은 우리를 신뢰할 수 있습니다."

추가 정보

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

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