한눈에 보기

이점

- **기존 보안 솔루션과의 투명한 통합으로** 탐지 향상
- **보안 및 대응 팀의** 효율성 개선
- **보안 사고에 대한** 빠른 조사 및 대응
- **기존** Cisco 보안 툴에서 원활하게 악성코드 분석 수행

Cisco Threat Grid

통합 악성코드 분석 및 위협 인텔리전스

기업들은 다수의 일반 악성코드 및 지능형 악성코드 공격에 시달리고 있습니다. 보안 전문가 또는 IT 관리자는 가장 먼저 처리해야 할 최고 위험도의 공격에 우선순위를 부여하는 것은 고사하고 모든 공격을 조사할 시간을 내기도 부족한 상황입니다.

이제 걱정하지 마십시오. Cisco® Threat Grid를 활용하면 클라우드 기반 서브스크립션을 통해 또는 기존 Cisco 보안 기술의 일부로 통합하여 악성코드 분석을 수행하고, 독립형 어플라이언스로 사이트에서 상황 기반 위협 인텔리전스를 수집할 수 있습니다. 또는 이 솔루션을 메일 게이트웨이, SIEM(Security Information and Event Management), GRC(Governance, Risk Management, Compliance) 플랫폼을 비롯한 기존 네트워크 및 보안 인프라와 통합할 수 있습니다. 이러한 대규모의 정적 및 동적 악성코드 분석 솔루션을 활용하여 시기적절하고 실행 가능한 상황 기반의 인텔리전스를 확보하여 악성코드를 식별하고 피해를 완화할 수 있습니다.

Threat Grid는 세계 각처에 구축되어 보안 운영 센터 및 사고 대응팀이 더 효과적이고 일관성 있는 조치를 취하는 데 기여하고 있습니다(그림 1).

악성코드와의 전쟁에서 꼭 필요한 두 가지 무기: 분석 및 위협 인텔리전스

Threat Grid는 상황 중심의 분석을 통해 거의 실시간으로 공격을 정확히 식별할 수 있습니다. 이 솔루션은 수백만 개의 파일을 분석하고 그 결과를 이미 분석된 수억 개의 다른 악성코드 아티팩트와 비교하여 연관성을 찾아냅니다. 고객은 악성코드 공격, 캠페인, 그 분포를 이전 내역을 포함하여 종합적으로 파악할 수 있습니다.

Threat Grid로 다음과 같은 혜택을 누릴 수 있습니다.

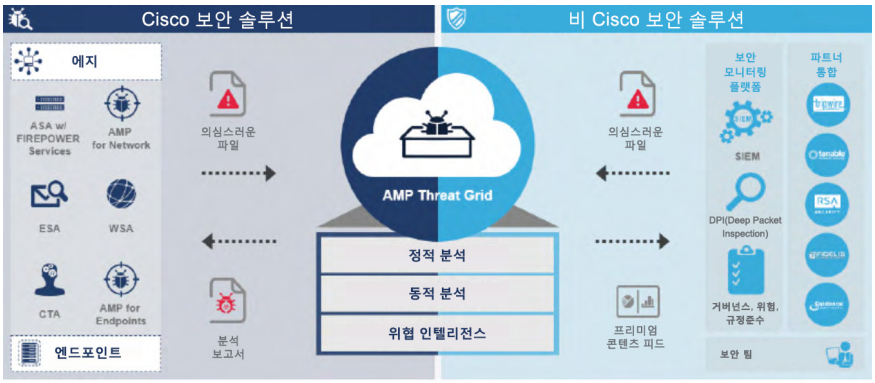
- 위협 점수와 행동 지표를 사용하여 지능형 악성코드를 빠르게 식별하고 우선순위를 지정해서 복구
- 악성코드 차단 기능을 자동화하여 더 신속하게 탐지하고 대응
- 프리미엄 피드를 SIEM, 침입 탐지 시스템, 게이트웨이, 프록시 등의 기존 보안 기술과 손쉽게 통합하여 더 빠르게 악성코드 탐지 및 차단

Threat Grid를 사용하면 지능형 공격을 정확하게 탐지하고 방어할 수 있습니다. 강력한 검색, 상관관계 분석, 보고 기능은 현재와 과거의 악성코드 아티팩트, 지표, 샘플에 대한 자세한 정보를 제공합니다. 자세한 분석 보고서에는 네트워크 트래픽 및 아티팩트를 비롯하여 모든 악성코드 샘플 활동이 포함됩니다.

"Threat Grid는 조직이 정확한 상황 기반 악성코드 분석과 위협 인텔리전스를 활용하여 지능형 사이버 공격에 대처하는 방식에 혁신적인 변화를 일으키고 있습니다."

Jon Olstik,
ESG Group

그림 1. 에지에서 엔드포인트까지 통합



Threat Grid를 에지에서 엔드포인트까지 Cisco 포트폴리오 전반에 걸쳐 통합했으며 여기에는 다음 제품이 포함됩니다.

- Adaptive Security Appliances(ASA) with FirePOWER™ Services
- Next Generation Firewalls
- Next Generation Intrusion Prevention Systems
- AMP for Networks
- Email Security Appliance(ESA)
- Web Security Appliance(WSA)
- AMP for Endpoints
- Cognitive Threat Analytics(CTA)
- Cisco Umbrella and Investigate

Threat Grid Premium 서브스크립션은 사용자에게 강력한 REST(Representational State Transfer) API 액세스를 제공합니다. Threat Grid에 의심스러운 파일 제출을 자동화하여 거의 모든 기존 보안 플랫폼에서 분석을 지원하도록 할 수 있습니다.

다음 단계

Cisco Threat Grid Premium에 대해 자세히 알아보려면 다음을 방문하십시오. http://www.cisco.com/content/en/us/products/security/amp-threat-grid-cloud/index.html.

Cisco Threat Grid - Appliances에 대해 자세히 알아보려면 다음을 방문하십시오. http://www.cisco.com/content/en/us/products/security/amp-threat-grid-appliances/index.html.

C45-733452-02 03/17