지속적 엔드포인트 위협 탐지 및 대응

개요

오늘날의 보안 위협을 차단하는 유일한 방법은 공격 전, 중, 후 전 단계에서 전방위적으로 위협에 대응하하는 것입니다. 빅 데이터 아키텍처와 결합한 Cisco 의 지속적 엔드포인트 분석 접근 방식은 이 모델의 기반이 됩니다. 지능형 악성코드 차단과 관련한 Cisco 의 혁신은 다음과 같습니다.

- 지속적 분석
- 회귀 분석
- 동작 표적 지표
- 디바이스 및 파일 전파 흔적 분석
- 보안 침해 통제
- 낮은 방생률

이러한 기능이 통합 워크플로우에 결합되면 악성코드 탐지, 모니터링, 분석, 조사 및 억제에 있어 실질적인 효과를 분명히 확인할 수 있습니다.

엔드포인트를 보호하는 새로운 모델

Cisco 는 오래전부터 보안 혁신을 위해 노력해 왔으며, 공격자가 발전을 거듭해 오는 동안 가만히 지켜보고만 있지 않았습니다. 실제로, 2003 년에 이미 Cisco(이전의 Sourcefire)는 지능형 위협을 차단하는 데 필요한 비전을 수립하고 NGIPS(Next-Generation Intrusion Prevention System)의 기반이 된 지속적 네트워크 검색의 개념을 개척했습니다. 오늘날, 특정 대상을 목표로 하는 지능형 악성코드 및 정교한 공격은 끈질기게 이어지고 있으며, 새롭고 은밀한 기법을 사용하여 기업 IT 환경을 감염시키고 있습니다. 다시 한 번, Cisco 는 보안에 대한 사고 방식을 혁신하고 있습니다. Cisco 는 지속적 기능을 발전시키고 있으며 공격을 차단하기 위한 새로운 모델을 도입하고 있습니다.

지속적으로 변화하는 세계에서의 지속적 보호

(Cisco 의 일부가 된) Sourcefire 가 10 여 년 전에 실시간 네트워크 감시를 소개할 당시, 네트워크 가시성에 대한 표준은 침해 네트워크의 특정 시점 스캔 툴을 사용하는 것이었습니다. 이 툴은 전체 스캔을 마치는 데 상당한 시간이 걸렸으며, 스캔 대상 네트워크 및 시스템에 지장을 주었습니다. 더 큰 문제가 되었던 것은 네트워크의 동적 특성으로 인해 데이터가 금세 오래되어 쓸모없는 상태가 되었기 때문에 전체 프로세스를 반복적으로 다시 실행해야 한다는 것이었습니다. 마지막으로, 데이터에 사각지대가 많이 포함되었으며 라이브 위협 데이터에 대한 상관 관계를 찾기가 힘들었습니다.

Cisco 는 많은 방어자가 직면하고 있는 근본적인 보안 문제는 환경을 보호하는 것이 아니라, 환경이 발전함에 따라 해당 환경을 보호하는 지속적 프로세스를 시작할 수 있도록 보호 대상과 보호가 이루어지는 방식에 대한 충분한 이해를 확보하는 것임을 인식했습니다. 지속적인 실시간 네트워크 감시를 통해 최초로 가시성이 위협 탐지와 긴밀하게 통합될 수 있었으며, 이를 통해 네트워크 위협 방어 논의가 영구적으로 바뀌게 되었습니다. Gartner 가 정의한 대로, 실시간 네트워크 감시는 NGIPS 의 핵심 필요 조건이 되었으며 이는 곧 Cisco FireSIGHT™ 기술입니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

2013 년에 Cisco 는 지능형 위협의 문제를 해결하기 위해 또 다시 패러다임을 전환하는 보안 모델을 도입했습니다. 오늘날의 위협 환경 및 IT 환경은 동적이며 끊임없이 확장되고 있다는 개념을 토대로 이 새로운 보안 모델은 공격 전, 중, 후 전 단계에서 전방위적으로 대응합니다.

실시간 네트워크 감시를 기반으로 Cisco 는 전통적인 특정 시점 방법론을 지속적 접근 방식으로 전환하고 있습니다. 이 모델의 특징은 다음과 같습니다.

- 오늘날의 지능형 위협을 차단하기 위해 고유한 혁신을 거듭합니다.
- 감염 및 공격 지속성에 대해 전례없이 탁월한 가시성을 제공합니다.
- 엔드 유저와 보안 인력에게 지장을 주지 않고 보안 팀이 신속하고 정확하게 감염을 억제 및 치료합니다.
- 보안 팀이 사냥감이 아니라 사냥꾼이 될 수 있도록 역량을 강화합니다.

다른 결과 기대

엔드포인트 위협 탐지 및 대응 분야에는 모두 똑같이 들리는 고급 브랜딩 및 메시징이 만연해 있습니다. 모두가 악성코드 탐지 분야에서 차기 혁신을 주도하고 있다고 주장합니다. 예전의 네트워크 스캔 프로그램과 매우 유사하게, 각 제품은 실제로 똑같은 근본적인 한계를 가지고 있는 동일한 툴에 약간의 기능 향상을 더했을 뿐이지만 타 제품보다 더 실시간이며 지속적인 보호 기능을 제공한다고 주장합니다.

> 광기: 동일한 행동을 계속 반복하면서 다른 결과를 기대하는 것
>
> – 알버트 아인슈타인

위협 탐지 분야의 최신 기능 향상은 탐지 및 분석을 위해 샌드박스(sandbox)에서 파일을 실행하고, 사용자 및 운영 체제로부터 악성코드를 교란하기 위해 가상 에뮬레이션 레이어를 사용하며, 허용 가능한 애플리케이션으로부터 악성 애플리케이션의 기준을 설정할 수 있도록 평판 기반 애플리케이션 화이트리스팅을 사용하는 것입니다. 더욱 최근에는 공격 체인 시뮬레이션 및 분석 탐지가 등장했습니다. 하지만 공격자는 이러한 보안 기술의 정적 특성을 이해하며, 예상대로, 네트워크 및 엔드포인트 방어를 뚫고 침입하기 위해 자신과 관련한 한계를 혁신하고 있습니다.

안타깝게도, 지난해의 "최첨단" 탐지 기술의 혁신적이지 못한 기능 향상을 떠안게 된 것은 엔드 유저이며, 근본적인 한계를 해결하지 못한 채 같은 사이클이 계속 반복되고 있습니다. 오늘날의 탐지 기술은 시간, 정확히 말해 특정 시점에 갇혀 있습니다.

악성코드는 동적이며 3 차원적입니다. 악성코드는 X 는 시간, Y 는 탐지 메커니즘인 2 차원적인특정 시점 'X-Y' 틀 안에서 탐지되기를 기다리며 존재하지 않습니다. 악성코드는 끊임없이 움직이는 상호 연결된 에코시스템으로서 존재합니다. 조금이라도 효과를 발휘하려면, 악성코드 간의 관계도 고려하여 악성코드 방어는 다차원적이면서 악성코드만큼 동적이어야 합니다. 슈퍼 탐지 기술이 문제를 완전히 해결해 줄 것이라는 희망을 버려야 합니다.

지능형 위협 및 보안 침해 활동 탐지에 대한 접근 방식을 진정으로 혁신할 수 있는 변화가 필요합니다. 지속적 보호 기능과 전파 동향과 감염 후 치료를 통한 진입 지점의 가시성이 필요합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

가장 중요한 질문에 답하는 진정한 지속적 모델

- 어떤 방법과 진입 지점이 사용되었습니까?
- 어떤 시스템이 감염되었습니까?
- 위협 요소가 무엇을 했습니까?
- 위협과 침입 전파 흔적 분석를 차단할 수 있습니까?
- 어떻게 복구합니까?
- 어떻게 재발을 방지합니까?
- 조직에 영향을 미치기 전에 표적지표를 신속하게 추적 제거할 수 있습니까?

특정 시점 패러다임 전환

오늘날의 지능형 악성코드는 다양한 공격 벡터로 환경을 감염시키고, 무한한 폼 팩터를 사용하며, 긴 시간에 걸쳐 공격을 실행할 뿐만 아니라, 데이터 유출을 숨길 수 있습니다. 공격을 진행하면서 막대한 양의 데이터를 흔적으로 남기고 있으며, 이를 캡처, 저장, 조작, 분석 그리고 관리하여 이러한 공격을 이해하고 해결하는 방법을 파악할 수 있습니다. 공격 전, 중, 후 전 단계에 보호 기능을 제공하는 모델에 기반한 Cisco® AMP(Advanced Malware Protection) for Endpoints 솔루션은 빅 데이터 아키텍처와 지속적 접근 방식을 결합하여 전통적인 특정 시점 탐지 및 대응 기술의 한계를 극복합니다.

이 모델에서는 모든 소스에서 발생과 동시에 프로세스 수준 텔레메트리 데이터가 지속적으로 수집되며, 필요할 때 항상 최신 상태로 유지됩니다. 제어 지점에 미치는 영향을 없애고 오랜 기간에 걸쳐 높은 수준의 탐지 기능을 제공하기 위해 분석을 레이어로 만들어 함께 구현할 수 있습니다. 분석은 이벤트 나열과 상관관계에 머무르지 않습니다. 또한, 텔레메트리 데이터를 엮어서 전체 환경에서 무엇이 일어나고 있는지 더 큰 통찰을 제공하는 것도 의미합니다. 더 광범위한 사용자 커뮤니티와의 교류를 통해 Cisco Collective Security Intelligence 는 지속적으로 글로벌 업데이트 되고 즉시 공유됩니다. 더 많은 정보를 토대로 의사 결정을 할 수 있도록 글로벌 인텔리전스는 로컬 데이터와 상관 관계를 파악합니다.

이 모델에서 탐지와 대응은 더 이상 별개의 분야 또는 프로세스가 아니며, 지능형 위협이 침입하기 전에 해당 위협을 차단한다는 동일한 목표를 확장한 것입니다. 탐지 및 대응 기능은 지속적이고, 통합되어 있으며, 전통적인 특정 시점 방법론보다 성능이 뛰어납니다.

지속적 분석의 혜택

- 데이터 탐지에 대한 집중 완화
- 고급 분석의 자동화
- 더 나은 위협 우선순위 지정
- 치료 시간 단축

탐지

공격자들이 최초의 방어를 우회하기 위해 계속 발전을 거듭하고 있기 때문에 100% 효과적인 탐지 방법은 없습니다. 하지만 특정 시점 탐지는 여러 가지 한계에도 불구하고 대부분의 잠재적 위협을 없애는 데 여전히 중요한 역할을 합니다. 그뿐만 아니라 전통적인 탐지에 지속적 접근 방식을 적용함으로써 방어자들은 특정 시점 기술을 더 개선하여 더 효과적이고, 효율적이며, 보편적으로 만들 수 있습니다.

하지만 이것은 Cisco 의 지속적인 접근 방식이 지능형 악성코드 차단을 혁신하는 시작에 불과합니다. 더 중요한 것은 이 접근 방식을 통해 탐지에서 대응에 이르는 전체 지능형 악성코드 차단 프로세스를 향상하는 다양한 기타 혁신을 제공할 수 있다는 것입니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

혁신을 지원하는 지속적 기능

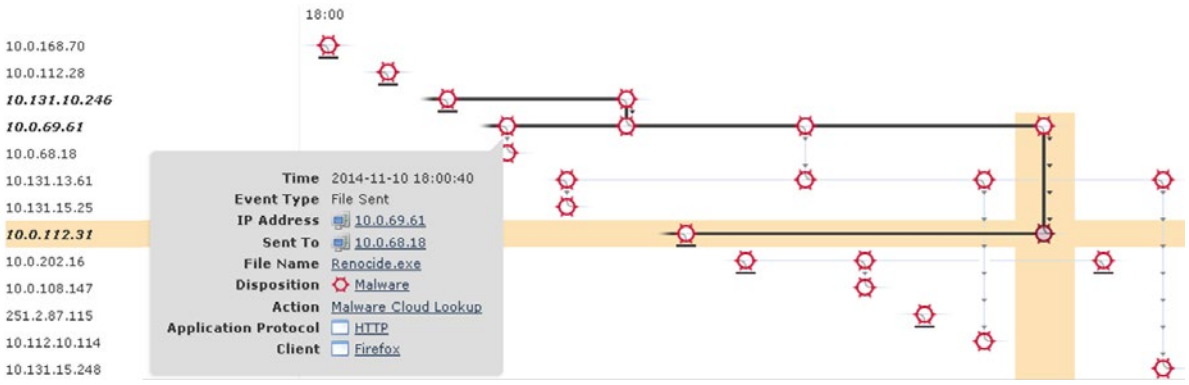
지능형 위협을 차단하는 유일한 방법은 공격 전, 중, 후 전 단계에서 전방위적으로 위협에 대응하여 문제를 해결하는 것입니다. 빅 데이터 아키텍처와 결합된 Cisco 의 지속적 접근 방식은 이 모델의 근간을 이루며 다음을 포함한 지능형 악성코드 차단의 다양한 추가 혁신을 가능하게 합니다.

- **회귀 분석**: 초기 특정 시점뿐만 아니라 오랜 기간에 걸쳐 분석을 실행할 수 있는 기능으로 파일에만 국한되지 않습니다. 여기에는 전통적인 특정 시점 모델로는 처리할 수 없는 프로세스, 커뮤니케이션 및 기타 텔레메트리 데이터도 포함됩니다.
- **공격 체인 위빙**: 긴 시간에 걸쳐 파일, 프로세스 및 커뮤니케이션 회귀 분석 스트림을 엮는 방법으로 관계적 차원을 캡처하며 2 차원적인 특정 시점 기술에는 포함되어 있지 않습니다.
- **동작 표적 지표**: 이러한 지표는 정적 아티팩트 이상의 의미를 갖습니다. 이는 공격 체인 위빙이 실시간으로 캡처하는 복잡한 동작 단서이며, 동작 표적 지표는 이러한 단서가 발생할 때 실시간으로 이를 탐지합니다.
- **전파 흔적 분석**: 전파 흔적 분석은 마케팅 용어로 트래킹(tracking, 추적)을 그럴듯하게 포장한 것이 아닙니다. 트래킹은 특정 이벤트가 어디에서 발생했는지 표시할 수 있도록 특정 시점 이벤트의 열거된 목록을 생성합니다. 반면에 "전파 흔적 분석"은 시간의 함수로서 이동하는 사물, 즉 이경우에는 악성 코드의 연속 경로를 의미합니다. 전파 흔적 분석은 악성코드가 어디에 있었는지 무엇을 실행했는지와 관련하여 악성코드의 범위와 감염 경로를 표시하는 데 훨씬 더 효과적입니다.
- **위협 헌팅:** 긴 시간에 걸쳐 잡아낸 악성코드의 동적 특성과 해당 데이터의 범위가 항상 최신 상태로 유지되므로 포착하기 어려운 악성코드 표적 지표를 찾아 내는 것은 Google 에서 맛집을 찾는 것만큼 간단합니다.

각각의 혁신만큼 중요한 것은 각각의 악성코드와 이에 해당하는 지능형 위협을 개별적으로 퇴치하는 것입니다. 악성코드 탐지, 모니터링, 분석, 조사 및 억제 전체에서 실질적인 효과를 분명히 확인할 수 있는 것은 이들이 하나의 통합 워크플로우로 결합되었을 때입니다.

그림 1 은 진입 지점, 악성코드 활동, 영향을 받는 엔드포인트에 대한 정보와 함께 악성코드 전파를 보여 줍니다.

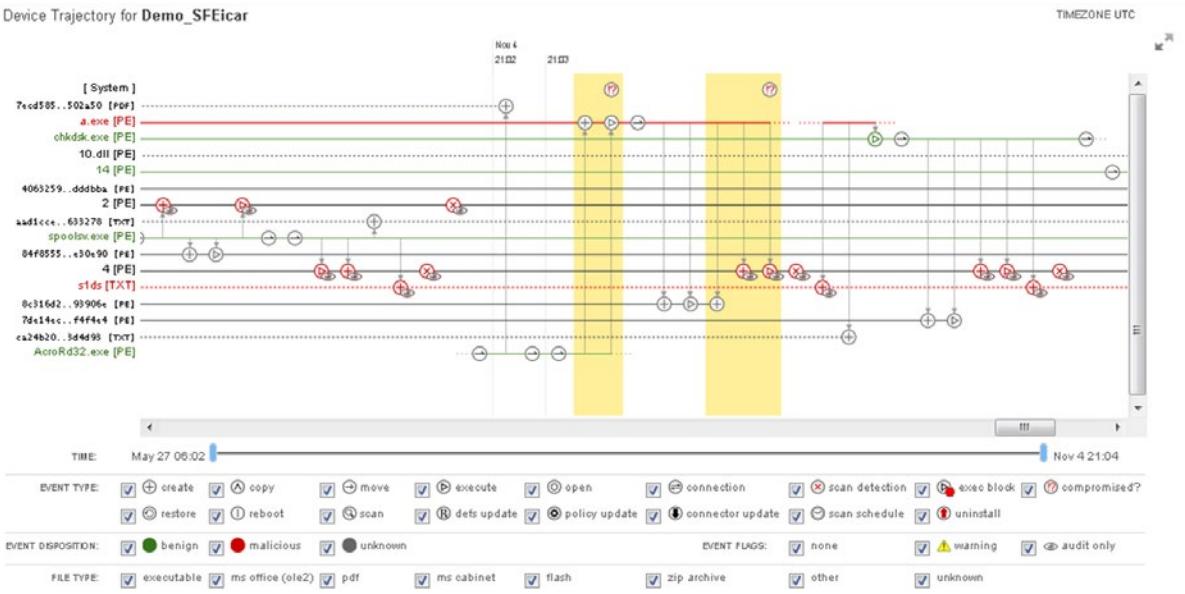
그림 1. Cisco AMP 네트워크 파일 전파 흔적 분석 화면



© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

그림 2 는 진입 지점, 악성코드 활동, 특정 엔드포인트에 영향을 주는 바이너리 및 실행 파일에 대한 정보와 함께 디바이스 전파 흔적 분석 화면 악성코드 전파를 보여 줍니다. 이 정보는 확장된 네트워크 전체의 엔드포인트 간에 상관 관계가 파악되고 공유되며, 그림 1 의 네트워크 보기와 통합됩니다.

그림 2. Cisco AMP for Endpoints 디바이스 전파 흔적 분석 화면



모니터링

엔드포인트에서 텔레메트리 데이터를 수집하고 해당 데이터를 발생 했을 때는 물론 긴 기간에 걸쳐 위협 활동에 대해 분석하는 기능을 회귀 분석이라고 부릅니다. 이러한 혁신적인 기술을 최초로 제공한 기업이 바로 Cisco 입니다. 이는 이벤트 중심의 데이터 수집 또는 새로운 데이터에 대한 예약된 스캔에서 큰 발전을 이룬 것으로, 비디오 감시 시스템과 유사하게 발생 즉시 공격을 잡아냅니다.

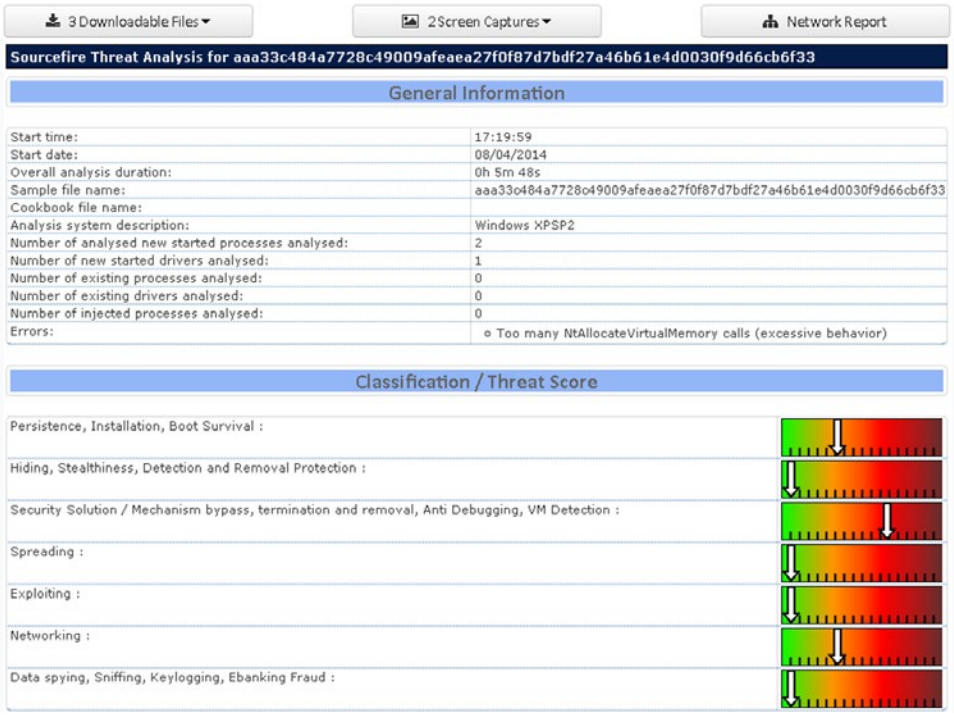
자동화된 고급 분석

네트워크를 통해 엔드포인트 간에 측면 이동하는 지능형 공격을 탐지하기 위해 방어자에게는 악성코드 및 공격용 악성코드가 남긴 표적 지표뿐만 아니라 긴 시간에 걸쳐 발생하는 더욱 지능적인 감염 동작을 자동으로 검색하는 기술이 필요합니다. Cisco 의 지속적 접근 방식은 조사해야 하는 또 다른 알림 목록을 제공하기 위해서가 아니라, 주요 감염 및 보안 침해 활동 영역에 대한 우선순위가 지정되고 수집 및 분석된 보기를 제공하기 위해 지능형 동작 탐지 기능을 통해 이러한 수준의 자동화를 제공합니다. 빅 데이터 분석 및 지속적 기능의 사용을 통해 패턴 및 표적 지표가 발생 즉시 식별될 수 있으므로 보안 팀은 잠재적인 손상 가능성이 가장 큰 위협을 해결하는 데 주력할 수 있습니다.

그림 3 은 동작의 심각도, 원래 파일 이름, 악성코드 실행의 스크린샷, 샘플 패킷 캡처 등 파일 동작에 대한 자세한 정보를 보여 줍니다. 이 정보를 통해 보안 침해를 억제하고 이후 공격을 차단하기 위해 필요한 사항을 더욱 명확하게 파악할 수 있습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

그림 3. Cisco AMP for Endpoints 파일 분석 화면



위협 헌팅 vs. 조사

지속적 접근 방식의 상황과 기능이 없을 경우 "조사"라는 말은 아무런 상황적 증거 없이 보안 침해를 추적했던 힘든 경험이 있는 보안 팀에게 약간의 거부감을 유발할 수 있습니다. 많은 경우 대답하기 가장 어려운 질문은 "어디서부터 시작할까?"입니다. 지속적 접근 방식에서 조사는 더 빠르고, 목표가 더 뚜렷하며, 더 생산적입니다.

지속적 접근 방식은 교묘한 사실과 단서를 찾는 것에서 악성코드 탐지와 정적 및 동작 표적 지표 같은 실제 이벤트에 기반한 보안 침해에 초점을 맞춘 추적으로 전환합니다. 빅 데이터 아키텍처가 지원하는 지속적 기능을 통해 언제든지 모든 데이터를 쉽게 검색할 수 있습니다. 앞에서 설명한 기능(동작 및 특정 시점 탐지와 회귀 분석 포함)을 사용하는 지속적 모델에서는 악성코드를 신속하고 효과적으로 추적할 수 있습니다. 조사 또는 위협 헌팅에는 감염의 진입 지점, 범위 및 근본 원인을 시각적으로 파악하는 것이 포함됩니다. 또한 추적 제거의 시간대를 식별하고, 해당 시간대를 확장 또는 축소하며, 필터를 사용하여 추적 제거를 정확히 지정하는 기능도 포함됩니다. 보안 팀이 알림 및 보안 사고에 아무 정보 없이 대응하는 것에서 벗어나 공격이 확대되기 전에 악성코드를 신속하게 추적하는 것으로 전환할 수 있기 때문에 이 기능은 중요한 툴이자 효율성 증대의 수단이 됩니다.

보안 침해 제어 vs. 억제

조사가 특정 시점 탐지 및 포렌식 기술로 제한될 경우 감당하기 어려운 작업처럼 보일 수 있습니다. 시각적으로 파악되는 모든 것의 이미지를 다시 작성할 필요 없이 악성코드 또는 의심되는 악성코드를 억제한다는 개념도 마찬가지입니다. 특정 시점 기술로는 이벤트 체인이나 이에 수반되는 상황 정보를 파악할 수 없기 때문에 악성코드를 철저히 억제하는 능력은 불가능합니다.

특정 감염 경로를 목표로 하는 기능이 지속적 접근 방식의 가시성과 결합되었을 때, 공격 체인을 신속하고 간편하게 해체할 수 있습니다. 그뿐만 아니라, 표준 운영 절차에서 중대한 감염이 발생한 디바이스의 이미지를 다시 작성하는 것이더라도 모든 탐지 및 텔레메트리 데이터는 계속 보존되며 이후 공격자가 동일한 감염 게이트웨이를 사용하여 감염시키는 것을 방지하고 억제합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

마지막으로, 전통적인 특정 시점 기술은 공격을 탐지하는 것조차도 실패할 때가 있어 조직이 적극적인 보안 침해를 겪을 수 있습니다. 일반적으로 많은 엔드포인트는 오랜 기간에 걸쳐 감염되어 왔고 보안 사고 대응 팀이 해당 상황을 조사하고 치료하는 작업을 수행해 왔습니다. 탐지 및 검색의 경우와 마찬가지로, 시간은 이 시나리오에서 매우 중요하며 "어디서부터 시작할까? 그리고 상황은 얼마나 나쁜가?"라는 동일한 근본적인 질문이 적용됩니다. 하지만 이 보안 침해 시나리오에서 공격에 대응하고 공격을 억제하는 것은 공격자에게 손을 대지 않고 매우 신속하게 범위 및 근본 원인을 파악하는 것을 포함하는 경우가 많습니다. 감염된 모든 지점과 감염 게이트웨이를 동시에 신속하게 차단하는 것은 공격자의 측면 이동을 방지하기 위해 매우 중요합니다.

구축하는 순간부터 지속적 접근 방식은 대응 담당자가 보안 침해의 정도와 핫스팟 위치를 파악하고 가장 중요한 작업인 쉽게 즉시 사용할 수 있는 억제 프로파일 구축을 수행할 수 있도록 지원하는 필수적인 탐지 및 텔레메트리 정보의 수집을 즉시 시작합니다. 지능형 동작 탐지, 추적, 및 시각화가 즉시 시작되지만, 탐지 및 보호 시나리오의 프로세스와 달리 모두 감사 모드로 수행됩니다. 이러한 프로세스는 계속 탐지하고 알림을 생성하지만 악성코드를 능동적으로 차단하는 대신에 마치 SWAT 팀이 급습하여 작전을 종료할 수 있도록 정보를 수집하는 잠복 근무 탐정처럼 증거를 캡처합니다.

지속적 대응과 특정 시점 대응 간의 근본적인 차이점은 지속적 대응은 철저한 억제를 포함하는 강력한 보안 침해 제어 기능을 제공하는 반면, 특정 시점 대응은 사실 및 증거의 열거된 목록만 제공한다는 것입니다. 이러한 목록은 보안 팀에서 사용할 수 있지만, 억제를 위해 실행 가능한 목록이 되기에는 너무 단순합니다.

통합 및 보고

Cisco AMP for Endpoints 는 처음부터 지속적 접근 방식 및 빅 데이터 아키텍처를 지원하도록 설계되었습니다. 클라우드 모델을 사용하여 엔드포인트에서 무거운 에이전트 아키텍처 대신에 경량형 커넥터를 구현합니다. 커넥터는 계산과 엔드포인트 및 사용자에 대한 메모리 영향으로 인해 범위 및 유효성이 제한되는 무거운 탐지 에이전트보다는 파일 및 텔레메트리 데이터의 수집기와 유사합니다. 이 모델은 커넥터가 텔레메트리 데이터를 지속적으로 모니터링 및 수집하고 빅 데이터 분석을 위해 클라우드에 효율적으로 전송할 수 있도록 리소스를 확보합니다.

또한 경량형 커넥터 모델은 플랫폼 간의 높은 패리티 수준으로 Windows, Mac, Android 및 가상 환경 등 다양한 엔드포인트 플랫폼에서 커넥터가 지원될 수 있도록 합니다. 이 연결은 이메일 및 웹 게이트웨이 어플라이언스, NGIPS 및 방화벽, 파일 트랜잭션이 많은 클라우드 서비스와 같은 기타 제어 지점 전체에 악성코드 탐지 및 차단 기능을 확장합니다.

제어 지점 전체에 대한 파일 및 텔레메트리 데이터의 보편적인 수집과 고급 분석을 통해 한 환경 내에서 로컬로 그리고 더 광범위한 Cisco Collective Intelligence Cloud 를 통해 고객 간에 글로벌하게 공유될 수 있는 종합 인텔리전스 수준이 향상됩니다. 실시간으로 인텔리전스를 공유하면 보안 팀이 동일한 초기 페이로드를 통해 많은 사용자가 감염된 후 이후 다른 다운로드 및 명령을 수신할 수 있는 피싱과 같은 기법을 사용하는 광범위한 공격에 대한 정보를 미리 파악할 수 있습니다. 파일 데이터 분석에 그치지 않고 제어 지점 전체에서 기타 텔레메트리 데이터를 분석하여 보안 침해의 범위를 더 정확히 파악할 수 있습니다.

일단 클라우드에 포함되면 제어 지점 전체에서 수집된 심층적인 텔레메트리 정보가 모든 제어 지점과 공유되어 해당 수준의 정보를 수집할 수 없는 제어 지점에서도 상황 정보를 동등하게 제공할 수 있습니다. 예를 들어, 한 엔드포인트에서 수집된 텔레메트리 데이터 및 동작 탐지를 네트워크 보안 팀에서 사용하여 특정 악성코드에 노출된 범위를 파악할 수 있습니다. 해당 엔드포인트에서 파일이 다운로드되었거나, 열렸거나, 이동했는지를 나타내는 정보는 일반적인 알림 데이터로 제공할 수 있는 것보다 더 완전한 상황 정보를 보안 팀에 제공할 수 있습니다. 악성코드를 활성화한 엔드포인트에는 악성코드를 다운로드하기만 한 엔드포인트보다 높은 우선순위가 지정됩니다. 더 나은 위협 파악 및 의사 결정을 위해 다른 제어 지점과 실시간으로 공유되는 엔드포인트의 풍부한 상황 정보는 실제 위협일지도 아닐 지도 모르는 일반적인이벤트의 단순한 목록과 크게 대조됩니다.

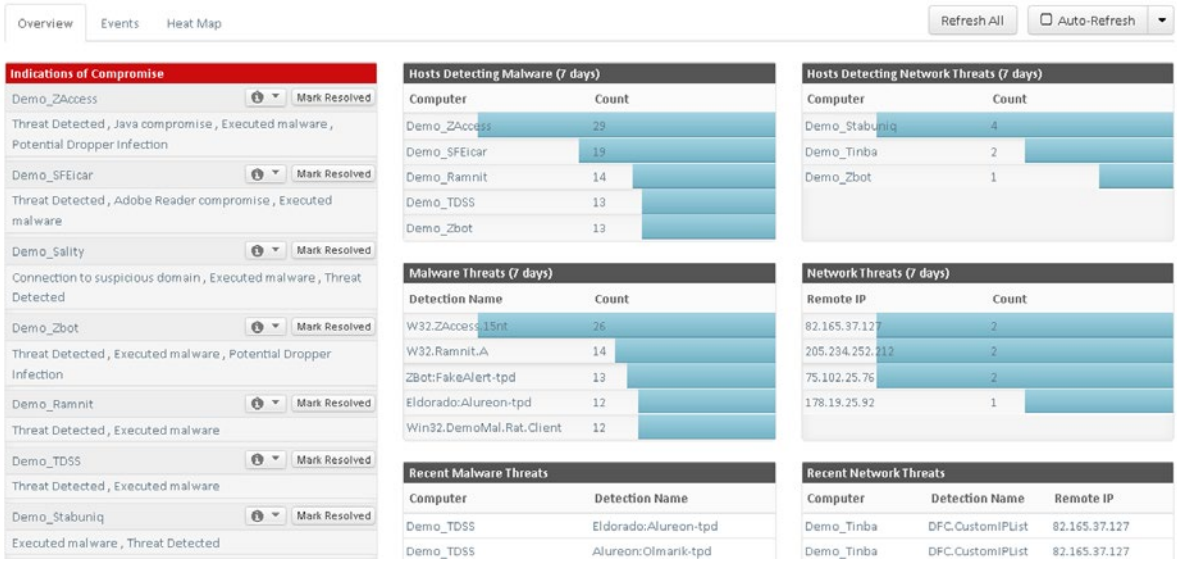
© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

지속적 접근 방식은 보고 기능에도 확장됩니다. 보고서는 더 이상 이벤트 열거 및 집계에 국한되지 않습니다. 보고서에는 실행 가능한 대시보드와 비즈니스 관련성 및 가능한 위험을 강조하는 트렌드가 포함될 수 있습니다. 특정 시점 기술로 대시보드와 위험 관련성도 제공할 수 있지만, 이를 위해서는 일반적으로 많은 양의 이벤트 데이터를 면밀히 확인하고 상관 관계를 파악하기 위해 SIEM(Security Intelligence and Event Management) 통합 방식으로 복잡한 레이어가 하나 더 추가되어야 합니다.

빅 데이터 아키텍처는 효과적인 악성코드 탐지 및 분석에 필수적인 끊임없이 증가하는 데이터를 처리하는 반면, 지속적 접근 방식은 이 데이터를 사용하여 필요할 때 필요한 곳에 상황과, 가장 중요하게는, 우선순위를 제공합니다.

그림 4 는 Cisco AMP for Endpoints 의 실행 가능한 대시보드와 비즈니스 관련성 및 위험 관점에서의 영향을 강조하는 경향을 보여 줍니다. 보고서는 이벤트 열거 및 집계에 국한되지 않습니다. 이 보기에는 우선순위가 지정된 표적 지표, 악성코드 탐지 호스트, 네트워크 위협 등 다양한 데이터가 표시됩니다.

그림 4. Cisco AMP for Endpoints 대시보드



결론: 실제로 1 + 1 은 3 이 아니라 6 이 될 수도 있습니다.

빅 데이터 아키텍처와 결합된 지속적 접근 방식은 엔드포인트를 목표로 하는 지능형 위협을 차단하기 위한 6 가지 주요 혁신 영역을 구현합니다.

1. **특정 시점 이상의 범위를 포괄하는 탐지.** 지속적 접근 방식으로 더 효과적이고, 효율적이며, 보편적으로 탐지할 수 있습니다. 샌드박싱과 같은 동작 탐지 방법이 최적화되고, 활동하는 즉시 잡아내며, 탐지 엔진 및 제어 지점 전체에서 인텔리전스가 공유됩니다.
2. **공격 체인 위빙을 지원하는 모니터링.** 파일, 프로세스 및 커뮤니케이션을 지속적으로 모니터링한 후 해당 정보를 취합하여 활동의 계보를 생성하는 회귀 분석으로 공격 발생 즉시 해당 공격에 대해 전례 없던 통찰을 제공합니다.
3. **긴 시간에 걸쳐 동작을 파악하는 자동화된 고급 분석.** 빅 데이터 분석과 지속적 기능을 결합하여 패턴 및 표적 지표가 발생하는 즉시 해당 항목을 식별함으로써 보안 팀이 가장 중요한 위협을 해결하는 데 주력할 수 있도록 지원합니다.
4. **사냥감을 사냥꾼으로 전환하는 조사.** 조사를 실제 이벤트 및 표적 지표에 기반한 집중적인 위협 헌팅으로 전환하여 보안 팀이 신속하고 효과적으로 공격을 이해하고 공격의 범위를 파악할 수 있도록 합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

5. **매우 간편한 억제.** 지속적 접근 방식이 제공하는 높은 수준의 가시성과 특정 근본 원인을 목표로 하는 기능을 사용하여 공격 체인을 신속하고 효과적으로 해체할 수 있습니다.
6. **실행 가능하며 상황 정보를 포함하는 대시보드.** 제어 지점 전체에 대한 파일 및 텔레메트리 데이터의 보편적인 수집 및 고급 분석을 기반으로 하며 상황 정보가 더해진 보고서는 트렌드, 비즈니스 관련성 및 위험으로 인한 영향을 요약해 줍니다.

Cisco 는 지속적 기능에 대한 선구적인 노력을 토대로 이를 빅 데이터 아키텍처와 결합하여 오늘날의 지능형 공격을 해결하는 새로운 모델을 제공합니다. 이 모델에서 탐지와 대응은 더 이상 별개의 분야 또는 프로세스가 아니라, 지능형 위협이 운영을 중단시키기 전에 해당 위협을 중단시킨다는 동일한 목표의 확장입니다. 전통적인 특정 시점 방법론을 넘어서서 지속적이고 통합된 탐지 및 대응 기능을 구현합니다. 실제 환경에서 엔드포인트 위협 탐지 및 대응에 필요한 것은 바로 이러한 솔루션입니다.

지속적 접근 방식과 특정 시점 모델의 비교

아래에는 특정 시점 모델로부터 지속적 접근 방식을 차별화하는 기능이 자세하게 비교 정리되어 있습니다. 향상된 탐지 기능과 지능형 악성코드 차단 분야의 혁신 사항도 설명되어 있습니다.

표 1. 탐지

지속적 접근 방식	특정 시점 모델
• 통합된 격자 모양의 엔진이 함께 협력하여 상황을 공유함으로써 향상된 탐지 기능을 제공합니다. • 워크로드와 레이턴시를 줄이고 모든 새 파일을 샌드박싱할 필요성을 없애 샌드박싱과 같은 동작 방법의 탐지가 최적화 되었습니다. • 오랜 기간에 걸쳐 탐지하며, 이는 실제로 긴 시간에 걸쳐 이루어지는 공격의 방식과 정확히 일치하는 것입니다. • 감사 모드는 오탐(false positive)을 줄이는 데 사용하던 간단한 조정 파라미터가 변한 것으로 공격자에게 알리지 않고 실시간 활동을 포착하기 위한 보안 사고 대응 수집 툴입니다. • 탐지 인텔리전스는 여러 제어 지점에서 전체적으로 즉시 공유됩니다.	• 둘 이상의 엔진이 있는 경우 엔진이 연속으로 및 독립적으로 작동하여 하나의 스택으로 운영되므로 엔드포인트에서 효과가 줄어들고 성능이 저하됩니다. • 벤더 업데이트가 필요하며, 여기에는 시간이 소요되고 보안 면에서 추가 공백이 발생합니다.

표 2. 모니터링

지속적 접근 방식	특정 시점 모델
• 파일 회귀 분석: 초기 탐지 분석 후 최신 탐지 기능 및 종합 위협 인텔리전스를 사용하여 오랜 기간에 걸쳐 파일에 대한 조사를 지속적으로 수행합니다. 따라서 업데이트된 처리를 렌더링할 수 있으며, 해당 파일이 처음 발견된 시점 이상으로 더 자세한 분석을 수행할 수 있습니다. • 프로세스 회귀 분석: 파일 회귀 분석과 유사하게, 프로세스 회귀 분석은 공격 체인 분석 및 동작 표적 지표 탐지에 오랜 기간 동안 시스템 프로세스 I/O 를 지속적으로 캡처 및 분석하는 기능입니다. • 커뮤니케이션 회귀 분석: 엔트포인트에서 보내고 받은 커뮤니케이션을 지속적으로 캡처하며 커뮤니케이션을 시작하거나 수신한 관련 애플리케이션과 프로세스도 지속적으로 캡처합니다. 이 정보는 공격 체인 분석 및 동작 표적 지표 탐지의 일부로 추가 상황 데이터를 제공합니다. • 공격 체인 위빙: Cisco AMP for Endpoints 는 회귀 분석 이상의 작업을 수행합니다. 다양한 형태의 회귀 분석을 언제든지 필요할 때 실시간으로 분석할 수 있는 하나의 활동 계보로 취합하여 새로운 수준의 인텔리전스를 제공합니다. 특히, 서로 다른 형태의 회귀 분석은 분석을 통해 엮여 개별 엔드포인트 또는 엔드포인트 커뮤니티 전체에서 동작의 패턴을 검색할 수 있습니다.	• 회귀 분석 없음: 이 모델은 탐지 활동을 넘어서는 엔드포인트에서의 관계적 활동에 대한 정보를 파악하지 못합니다. • 또한 이 모델은 악성코드가 제어 지점을 거친 후 네트워크 내에서 발생하는 어떠한 활동에 대해서도 전혀 정보를 제공하지 못합니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

표 3. 자동화된 고급 분석

지속적 접근 방식	특정 시점 모델
• 실시간 대응: 엔드포인트 텔레메트리 데이터가 지속적으로 수집되어 데이터 저장소에 추가되므로 정적 및 동작 표적 지표와 자동으로 비교할 수 있습니다. 따라서 정적 또는 동작 표적 지표의 탐지 시간이 크게 단축될 수 있습니다. • 동작 표적 지표: 공격 체인 위빙을 사용하여 동작 표적 지표는 탐지 이벤트, 정적 표적 지표 및 텔레메트리 데이터 전체에서 잠재적인 감염을 나타내는 정교한 활동 패턴을 검색합니다. 대표적인 예는 초기 탐지를 빠져나간 드로퍼(dropper)입니다. • 공격 체인 위빙: 공격 체인 위빙은 트리거된 동작 표적 지표 전후에 발생한 활동도 기록합니다. 보안 팀은 보안 침해의 범위를 완전히 파악하고 문제를 철저히 억제하는 기능에 의미가 있는 알림을 기반으로 신속하게 대응할 수 있습니다. • 개방형 표적 지표(Open IoC): 개방형 표적 지표를 통해 고객은 맞춤형 정적 표적 지표 탐지 목록을 사용할 수 있습니다. • 인텔리전스 기반 표적 지표: 정적 인텔리전스, 블랙리스트 또는 탐지 스크립트 이상으로 이러한 표적 지표는 긴 시간에 걸쳐 악의적인 특정 작업 및 관련 작업을 검색하는 동작 알고리즘에 기반합니다. 인텔리전스 기반 표적 지표는 Cisco Talos Security Intelligence and Research Group 에서 개발하고 전체 지원합니다. • 발생률: 고급 분석 엔진이 해당 조직 및 더 광범위한 글로벌 커뮤니티와 관련하여 탐지된 악성코드의 발생률을 파악합니다. 발생률이 낮은 악성 파일은 대부분 표적형 악성코드 및 표적형 감염 시도를 나타냅니다. 이러한 정보는 일반적으로 보안 팀에서 놓치기 쉽습니다. 발생률 분석은 특히 해당 시스템을 포함하는 다른 정적 또는 동작 표적 지표와 상관 관계가 파악되는 경우 이러한 종류의 공격을 강조합니다.	• 일부 특정 시점 기술은 정적 표적 지표 아티팩트를 검색할 수 있지만 실시간으로 검색하지는 못하며 표적 지표가 실행되기 전에 오랜 시간이 소요되는 데이터 수집이 필요한 경우가 많습니다. • 이 모델은 악성코드가 몇 번 또는 어디서 발견되었는지를 표시할 수는 있을지 모르지만, 근본 원인에 관한 관계적 정보는 제공하지 못합니다. • 위협의 중대성 또는 발생률은 표시되지 않습니다. • 발생률 기능이 있는 경우, 해당 기능은 실시간으로 구현되거나 특정 파일, 프로세스 또는 커뮤니케이션을 계속 추적할 수 없습니다. • 동작 표적 지표를 식별할 수 없습니다.

표 4. 위협 헌팅 vs. 조사

지속적 접근 방식	특정 시점 모델
• 파일 전파 흔적 분석: 엔드포인트를 스캔하거나 스냅샷을 생성할 필요 없이 악성 파일 또는 의심되는 파일에 노출된 범위를 시간, 방법 및 진입 지점, 영향을 받은 시스템, 발생률과 함께 신속하게 파악합니다. • 디바이스 전파 흔적 분석: 파일 전파 흔적 분석에서 제공하는 범위의 수준에 기반하여 디바이스 전파 흔적 분석는 시스템 프로세스에 대한 강력한 시간대 분석을 제공하여 근본 원인 기록 및 계보를 파악합니다. 또한 시간대를 확장 또는 축소하거나 필터링을 통해 감염의 정확한 원인을 신속하고 정확하게 찾아낼 수 있습니다. • 엘라스틱 검색(Elastic Search) : 엘라스틱 검색은 관계형 데이터베이스 쿼리의 일반적인 경계 없이 "다른 어떤 곳에서 이 지표가 발견되었는가?"를 묻는 신속하고 간편한 방법을 제공합니다. 전체 데이터 세트 및 글로벌 종합 인텔리전스에서 호스트 이름, 파일 이름, URL 및 IP 주소에서 텍스트 문자열에 이르는 모든 항목을 검색할 수 있습니다. 정기적으로 수백만 개의 파일을 분석하는 이 기능은 너무 늦기 전에 지능형 위협을 신속하게 추적 제거하기 위한 강력한 툴이 됩니다. • 파일 분석: 첫째, 이 모델은 동작을 완전히 분석하고 해당 동작의 위협 수준에 대한 점수를 매기기 위해 샌드박스에서 파일을 실행하는 보안 메커니즘을 제공합니다. 둘째, 해당 분석의 결과가 세부 보고서로 제공됩니다. 셋째, 모든 분석 결과는 종합 인텔리전스에 추가됩니다. 넷째, 모든 분석 결과는 엘라스틱 검색을 통해 검색할 수 있습니다. 다시 한 번, 보안 팀은 신속하게 파일 분석 보고서의 지표를 기반으로 전체 기업에서 이 지표가 발견되었을 수 있는 다른 위치를 확인할 수 있습니다. 이는 공격이 표적형 공격이지만 일반적인 감염 방법을 사용하는 경우 매우 중요합니다.	• 전통적인 특정 시점 탐지 기술로는 부족합니다. 전통적인 특정 시점 탐지 기술은 탐지 후 모니터링 또는 상황 정보를 제공하지 못합니다. ◦ 이벤트 열거 목록에 추가되는 캡처된 독립 이벤트를 탐비하는 경우가 많습니다. 이 목록이 지속적으로 업데이트 되지만 어떠한 상황 회귀 분석도 포함되어 있지 않습니다. ◦ 탐지 전후의 이벤트를 확인할 수 있는 기능이 없습니다. ◦ 파일에서 동작을 완전히 분석한 후 모든 엔드포인트에서 특정 표적 지표를 신속하게 검색할 수 있는 기능이 없습니다. • 일부 기술은 제한된 기능(예: 이벤트 열거 데이터를 기반으로 악성코드가 탐지된 시간 및 위치 파악)을 제공할 수도 있지만, 감염 전후의 시간대 이벤트를 확인할 수 있는 기능은 제공하지 못합니다. • 전통적인 특정 시점 포렌식 및 조사 툴은 지속적 기능을 제공한다고 주장하는 경우에도 탐지 기능에 비해 훨씬 더 나은 성능을 제공하지 못합니다. ◦ 이러한 툴에는 지능형 위협 탐지 수단이 없습니다. 탐지 기능은 지속적 상황 정보와 결합되는 경우 중요한 시작 지점이 될 수 있지만, 포렌식 툴은 관계가 아니라 아티팩트 및 단서를 찾도록 설계되었습니다. ◦ 감염 전후의 이벤트에 대한 시간대 시각화를 제공할 수 있는 기능이 없습니다. ◦ 모든 데이터를 업데이트할 필요 없이 특정 표적 지표를 신속하게 검색할 수 있는 기능이 없습니다.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

표 5. 보안 침해 제어 vs. 억제

지속적 접근 방식	특정 시점 모델
• 간편한 억제: 파일이 악성으로 의심됩니까? 문제가 될 것도 없고 기다릴 필요도 없습니다. 파일의 SHA256(보안 해시 알고리즘)을 사용하여 마우스 클릭 몇 번으로 모든 엔드포인트, 엔드포인트 그룹 또는 단 하나의 엔드포인트에서 해당 파일을 즉시 차단할 수 있습니다. • 지능형 억제: Snort® 스크립트와 유사하게, 지능형 맞춤 탐지는 서명 업데이트를 기다리지 않고 악성코드를 처리할 수 있는 기능을 제공합니다. • 애플리케이션 화이트리스트 및 블랙리스트: 풍부한 상황 정보를 통해 안전한 애플리케이션이 악의적인 활동에 게이트웨이로 사용되고 있는지를 더 효과적으로 파악하고 의심되는 위험한 애플리케이션을 중지하는 데 제어 목록을 사용할 수 있습니다. 이러한 목록은 지속적 분석 및 텔레메트리 데이터를 확장합니다. 보안 팀은 대응을 위한 표준 절차를 사용하면서 상황을 신속하게 제어할 수 있습니다. • IP 블랙리스트: 애플리케이션 제어 목록과 유사하게, IP 블랙리스트는 실제 이벤트 또는 기업 정책의 상황에서 더 효과적으로 사용되어 보안 침해를 제어하고 엔드포인트에서 발생하는 의심스러운 커뮤니케이션을 전체 엔드포인트에서 모니터링할 수 있습니다. 이 기능은 억제 계획이 구현될 때 공격자가 사용하던 모든 교차 커뮤니케이션을 제거해야 하는 보안 침해 시나리오에서 매우 중요합니다.	• 특정 시점 기술은 공격 전, 중, 후를 아우르는 전 단계에서 이후 시점이 아니라 억제가 중요한 요건인 탐지의 시점에 초점을 맞추도록 설계되기 때문에 악성코드 또는 의심되는 악성코드를 억제할 수 있는 기능이 상당히 제한됩니다. • 일부 특정 시점 탐지 기술은 애플리케이션의 블랙리스트 작성을 지원합니다. 이는 조직에 위험을 야기하는 애플리케이션이나 아직 안전한지 아니면 위험한지는 파악되지 않았지만 예방 조치로서 차단해야 하는 의심스러운 애플리케이션을 억제하기 위한 좋은 방법입니다. 하지만 블랙리스트 작성은 강력한 파일 세트와 탐지, 분석 및 억제의 주요 역할을 수행하는 동작 탐지 기능이 정보를 제공하는 경우 가장 효과적입니다. 주된 단점은 이러한 기술을 보호의 기본 레이어으로 관리하는 데 매우 많은 인력이 필요하게 되며, 공격을 놓치고 공격 체인 활동에 대한 정보를 전혀 파악하지 못할 가능성이 높다는 것입니다. • 마지막으로, 특정 시점 포렌식 및 대응 툴은 오늘날 확인되는 지능형 위협 유형에 필요한 신속한 보안 침해 제어를 위해 설계되지 않았습니다. 이러한 툴은 조사에는 유용하지만, 데이터 열거를 기반으로 억제를 수행할 수는 없습니다. 이 단계에는 종종 많은 인력이 필요한 활동이 수반되며, 일반적으로 이 방법 대신에 더 간편한 이미지 리이미지(reimage) 접근 방식이 사용됩니다.

자세한 정보

보안에 대한 Cisco 의 접근 방식에 대해 자세히 알아보려면 이메일(ciscosecurityinfo@cisco.com) 또는 전화(800 553-6387)로 문의하시기 바랍니다.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-733649-00 02/15

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.