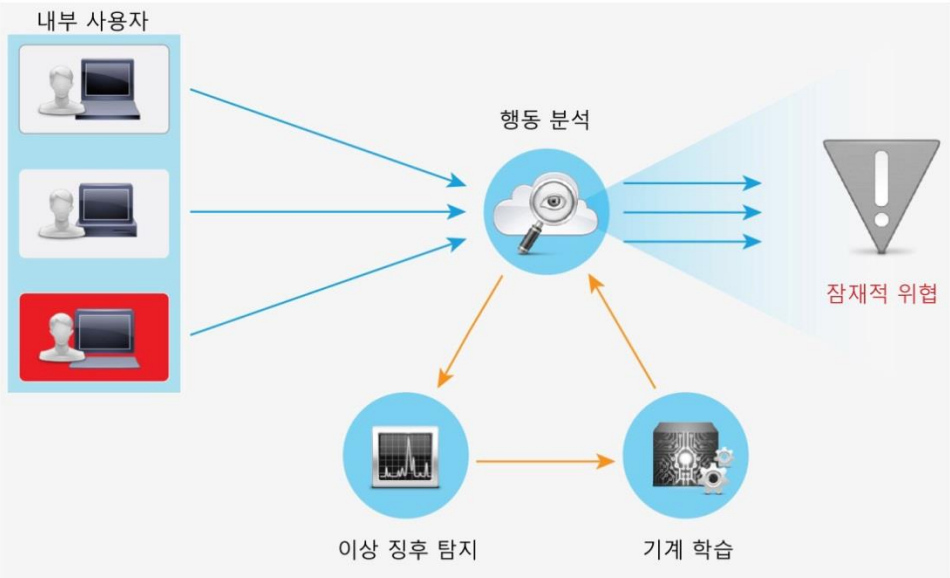
Cisco Cognitive Threat Analytics

CTA(Cognitive Threat Analytics), 보안 침해 탐지 및 분석으로 네트워크의 위협을 차단하여 웹 보안 강화

온라인 위협은 갈수록 정교해지고 있으며 표적 공격은 증가하고 있습니다. 사이버 범죄자는 다양한 벡터를 통해 조직적인 활동을 시작합니다. 이들은 멀버타이징(malvertising)을 제공하고 루트킷을 설치하는 익스플로잇 킷을 배포할 수 있습니다. 또한, 인프라 내에 봇넷을 설치할 수 있습니다. 일단 사이버 범죄자가 거점을 마련하게 되면 90% 이상의 위협이 웹을 통해 발생하며, 이 곳에서 사이버 범죄자는 C&C(command-and-control) 커뮤니케이션을 위한 채널을 구축하고 민감한 정보를 유출할 수 있습니다.

Cisco® Cognitive Threat Analytics는 매일 100억 개 이상의 웹 요청을 분석하여 보안 제어 장치를 우회하거나, 모니터링되지 않은 채널(이동식 미디어 포함)을 통해 유입되거나, 조직의 환경 내부에서 작동 중인 악의적인 활동을 찾아냅니다. Cognitive Threat Analytics는 머신 러닝 및 네트워크의 통계적 모델링을 사용하는 클라우드 기반 제품입니다. 이 솔루션은 네트워크에서 트래픽의 기준점을 만들고 이상 징후를 식별합니다. 또한, 사용자와 디바이스 행동, 웹 트래픽을 분석하여 C&C 커뮤니케이션, 데이터 유출 및 인프라 내에서 운영되는 잠재적으로 불필요한 애플리케이션을 찾아냅니다(그림 1).

그림 1. Cognitive Threat Analytics의 작동 방식



기능 및 장점

기능	장점
사용자 및 디바이스 행동	Cognitive Threat Analytics는 각 사용자와 디바이스에서 생성된 트래픽을 분석합니다. 이 솔루션은 데이터와 해당 기업의 전반적인 상황의 상관관계를 분석하여 C&C 커뮤니케이션과 관련된 비이상적인 트래픽을 찾아냅니다. 이러한 자동화 분석은 웹 기반 커뮤니케이션을 사용하여 기업을 공격하는 위협을 성공적으로 식별하는 데 매우 중요합니다.
확인된 침입	대부분의 보안 기술은 경고를 통해 조사의 필요성을 알립니다. Cognitive Threat Analytics는 기업 내에서 작동 중인 확인된 위협에 대한 알림을 제공하여 추가 조사 없이 즉각적인 조치를 취할 수 있도록 합니다.
머신 러닝(Machine Learning)	Cognitive Threat Analytics는 머신 러닝 및 통계적 모델링을 사용하여 새로운 위협을 독립적으로 파악하고, 본 것을 통해 배우고, 시간을 두고 적응함으로써 지속적인 보안 침해 식별 기능을 제공합니다.
익명 트래픽 모니터링	Cognitive Threat Analytics는 HTTPS 및 Tor를 비롯한 모든 유형의 웹 트래픽을 분석합니다. 이 솔루션은 채널 공격자가 사용하고 기타 보안 기술이 인식하지 못하는 익명 및 암호화된 커뮤니케이션에 대한 뛰어난 보기를 제공합니다.
엔드포인트 통합	CTA는 Cisco AMP for Endpoints와 통합됩니다. 이러한 통합으로 인해 사용자는 커넥터를 설치할 수 없는 디바이스(예: 개인 디바이스 또는 중요한 서버)에 대한 가시성을 확보할 수 있으며, 두 시스템의 결과를 한 곳에서 확인하고 AMP for Endpoints 콘솔에서 이에 대한 조치를 취하여 새로운 위협을 탐지하는 데 소요되는 시간을 절감할 수 있습니다.

감염된 디바이스 식별

클라우드 기반 SaaS(Software as a Service)인 Cognitive Threat Analytics는 추가 하드웨어 또는 소프트웨어를 구축할 필요가 없습니다. 이 솔루션은 웹 로그를 분석하고 즉시 위협 탐색을 시작합니다. 또한 주의를 요하는 의심스러운 행동을 개별적으로 식별합니다. 따라서 사람의 개입이 필요 없습니다. Cognitive Threat Analytics는 평균적으로 2~3시간 이내에 새로운 위협을 탐지하며, 5,000명 규모의 회사에서 매주 45개에 달하는 보안 침해가 발생한 디바이스를 찾아냅니다.

고급 분석

Cognitive Threat Analytics의 특허 출원 중인 알고리즘은 네트워크 커뮤니케이션을 면밀히 조사하여 정상적인 활동의 기준선을 만드는 데 필요한 행동을 평가합니다. 또한 정상 범주에서 벗어난 행동이나 의심스러운 행동이 탐지되면 이를 조사하며, 이상 징후 및 악의적인 활동이 발생할 경우 알림을 전달합니다. 이러한 자동화된 분석 기능은 웹 기반 커뮤니케이션을 사용하여 기업을 공격하려는 위협을 성공적으로 식별하는 데 매우 중요합니다.

통합 위협 인텔리전스

위협에 대한 종합적인 보기를 제공하기 위해 CTA는 Cisco AMP Threat Grid와 통합되었습니다. CTA가 웹 채널의 커맨드 앤 컨트롤 커뮤니케이션을 개별적으로 탐지할 경우, 이는 AMP Threat Grid 데이터베이스를 쿼리하며, AMP Threat Grid에서 발견한 수백만 개의 악성코드 아티팩트와 보안 침해 지표(IoC)의 상관관계를 분석하여 이상 징후를 초래한 악성코드를 식별합니다.

자동화된 대응

Cognitive Threat Analytics는 STIX(Structured Threat Information eXpression) 및 TAXII(Trusted Automated Exchange of Indicator Information)를 사용하여 SIEM(Security Information and Event Management) 플랫폼을 비롯한 기존 보안 모니터링 기술과 통합됩니다. 기업에서는 설정된 워크플로를 통해 대응 방법을 통합하고 자동화할 수 있습니다.

신속한 보안 침해 탐지

Cognitive Threat Analytics는 공격 요소가 커맨드 앤 컨트롤 서버에 접근할 경우 네트워크에서 점유율을 확보하려고 시도하는 이러한 공격을 찾아낼 수 있습니다. 확인된 보안 침해를 식별하므로 조사를 수행할 필요가 없으며 위협을 즉시 치료할 수 있는 실행 가능한 인텔리전스를 제공합니다.

표 1. 탐지 및 분석 엔진

엔진	기능
데이터 유출	Cognitive Threat Analytics에서는 매일 100억 개 이상의 웹 트래픽을 분석하여 웹 기업의 네트워크에 대한 통계적 모델링을 통해 비정상적인 웹 트래픽을 찾아내고 민감한 데이터의 유출을 밝혀냅니다. CTA는 HTTPS 인코딩 트래픽에서도 데이터 유출을 감지하며, 전송된 트래픽을 해독할 필요가 없습니다.
DGA(Domain Generation Algorithm)	공격자는 악성코드를 제공하는 호스트가 탐지되어 블랙리스트에 포함되는 것을 피하고자 임의 개수의 도메인 이름을 생성합니다. CTA는 각 HTTP/HTTPS 요청에서 관찰되는 여러 단어로 생성된 악성 및 난독화된 도메인 이름을 인식하고 커뮤니케이션 빈도, 헤더의 정보 내용, 기타 수백 가지의 요소를 분석합니다.
익스플로잇 킷	CTA는 웹 요청 분석을 통해 1) 감염된 웹 페이지 방문, 2) 도메인 호스팅 익스플로잇 킷으로 리디렉션, 3) 사용자의 부지불식간의 다운로드, 4) 성공적인 익스플로잇, 5) 악성 페이로드 다운로드로부터 익스플로잇 킷 감염을 밝혀냅니다.
HTTP/S 요청 터널링	대개의 경우 공격자는 직접 HTTP/HTTPS 요청을 사용하여 자격 증명과 같은 민감한 데이터를 유출하려 시도합니다. CTA는 전역 통계 및 로컬 이상 점수 등 여러 IOC를 사용하여 악성 터널링과 정상적인 기술 사용을 명확하게 구분합니다.
커맨드 앤 컨트롤(C2) 커뮤니케이션	CTA는 인터넷 전반에서 수집된 통계를 포함하여 호스트별 로컬 이상 점수까지 다양한 데이터를 통합합니다. 이러한 지표를 통계 탐지 알고리즘 내에서 통합함으로써 C2 커뮤니케이션을 정상적인 트래픽으로부터 또한 기타 악성 활동으로부터도 구별할 수 있습니다. CTA는 전송된 콘텐츠를 해독하지 않고도 Tor를 비롯한 HTTPS 인코딩 트래픽 또는 익명(TOR) 트래픽에서도 C2를 인식하여 다양한 위협을 탐지할 수 있습니다.

라이센싱

라이센스는 1년, 3년, 5년 기간으로 제공됩니다. 라이센스의 형식은 다음과 같습니다.

- Cisco Cloud Web Security의 간단한 애드온 라이센스
- Cisco Web Security Appliance의 간단한 애드온 라이센스
- 서드파티 웹 프록시(예: Blue Coat ProxySG)를 위한 독립형 Cognitive Threat Analytics 서비스

Cognitive Threat Analytics를 활용하면 복잡성을 낮추면서도 계속 변화하는 위협 환경과 함께 진화하는 탁월한 보호 기능을 확보할 수 있습니다.

Cisco Capital

목표 달성을 지원하는 파이낸싱

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. 자세히 보기.

Cisco를 선택해야 하는 이유

Cisco의 경우 전 세계의 최대 네트워크 인프라 및 서비스 공급자로서 검색 시간을 단축하고 네트워크 내의 공격 범위를 축소하는 첨단 보안 솔루션을 제공할 수 있는 위치에 있습니다. Cisco의 글로벌 점유율과 Cisco 인프라에서 실행되는 네트워크 트래픽 가시성을 활용하는 Cognitive Threat Analytics는 공격 방법이 아닌 감염 증상에 초점을 맞추므로 변화하는 위협 환경과 함께 진화하는 수준 높은 보호 기능을 제공합니다. Cognitive Threat Analytics는 Cisco Cloud Web Security, Web Security Appliance의 간단한 애드온 라이센스로 제공되며, 기존 보안 솔루션과 통합할 수 있는 독립형 솔루션으로도 제공됩니다.

세부 정보

자세한 내용은 http://www.cisco.com/go/cognitive를 참조하십시오.

Cisco 제품이 여러분 회사에 얼마나 효과적으로 적용될 수 있을지 Cisco 영업 담당자, 채널 파트너, 시스템 엔지니어와 함께 평가해 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, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-736557-01 12/16