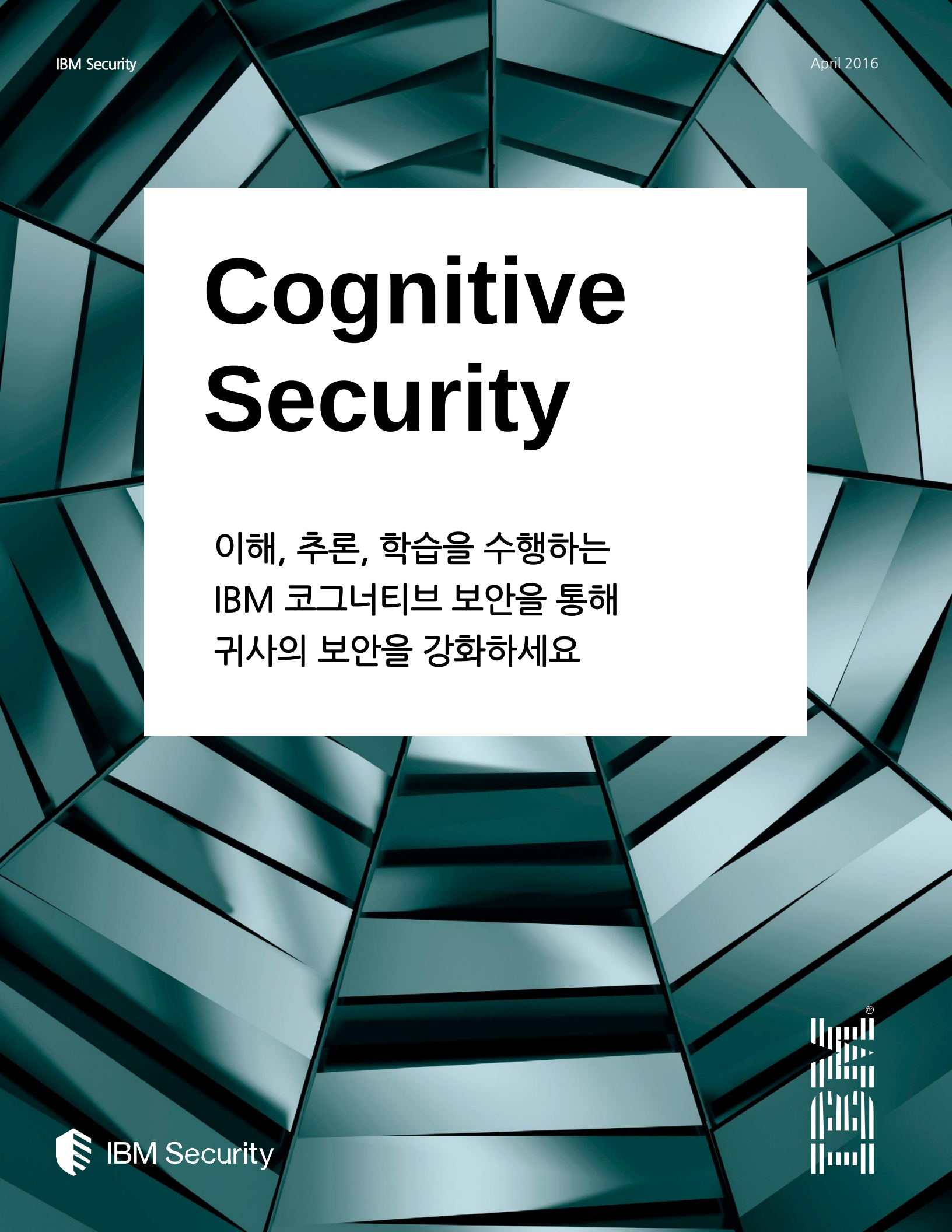
April 2016



Cognitive Security

이해, 추론, 학습을 수행하는 IBM 코그너티브 보안을 통해 귀사의 보안을 강화하세요

IBM Security

목차

새로운 과제

컴퓨터를 프로그래밍하여 복잡한 문제를 해결하는 방식이 100여 년간 주를 이뤘습니다. 이제는 날씨를 시뮬레이션하고 유전자 배열을 분석하고 즉시 전 세계에 데이터를 공유할 수 있습니다. 그러나 사람이 매일 하는 일, 즉 이미지를 인식하고 책을 읽고 어떤 시의 의미를 설명하는 행위를 컴퓨터에게 시키는 것은 전혀 다릅니다. 기존의 시스템으로는 역부족입니다.

보안도 마찬가지입니다. 우리는 수십 년간 바이러스, 악성코드, 익스플로잇을 찾아내도록 프로그래밍해 왔습니다. 지속적인 튜닝을 통해 정확성을 높였지만 그것으로는 충분하지 않습니다. 공격자는 끊임없이 공격을 변형시키고 온갖 창의적인 방법으로 방어막을 통과하려 합니다. 이제 기업은 활동의 가장 미묘한 변화도 탐지하고 이를 최대한 많은 컨텍스트와 연계하여 분석함으로써 새로운 위협을 찾아내 제거하는 능력이 필요합니다.

80%
of the world's data
has been
invisible.
Until now.

실제로 피해가 발생하기 전에 공격 및 비정상적인 동작을 찾아내기 위해서는 지속적으로 모니터링하고 데이터를 최대한 활용해야 합니다. 그러나 전 세계적으로 매일 250 경 바이트 이상의 데이터가 생성되고 있으며 그 중 80%가 비정형 데이터입니다. 즉 사람은 쉽게 이해하지만 기존 보안 시스템은 이해할 수 없는 자연어(말, 글, 신호)로 이루어져 있습니다. 사실 매일 수천 개의 보안 블로그가 게시되어 세부적인 보안 인텔리전스를 제공합니다. 그러나 보안 분석가가 그 내용을 모두 파악할 수는 없으며 기존의 보안 시스템은 분석가처럼 인사이트 있는 분석과 응용이 불가능합니다.

이런 까닭으로 여전히 보안 분야에서는 어떤 조치가 필요한지 또한 무엇이 잘못된 경보인지 제대로 판단하는 것이 가장 어려운 일입니다. 사실 최고의 보안 전문가는 매일의 경험, 동료와의 대화, 컨퍼런스 참여, 최신 연구 자료 학습을 통해 지식을 키워나갑니다.

IBM Security 에서는 차세대 시스템이 지속적인 훈련을 받으며 이해와 추론을 통해 끊임없이 진화하는 보안 위협에 대해 학습하고 있습니다. 보안에 대한 직관 및 전문성을 바탕으로 연구 보고서, 웹 텍스트, 위협 데이터, 기타 보안 관련 정형 및 비정형 데이터를 분석하는 새로운 방어 체계가 구축되기 시작했습니다. 이는 보안 전문가들이 일상적으로 수행하는 작업과 비슷하지만 전례 없는 규모로 이루어지고 있습니다. 이것이 코그너티브 보안의 핵심입니다.

그 결과 분석가가 코그너티브 시스템을 활용하여 위협에 대한 인식을 보완하고 자동화할 수 있으며 궁극적으로는 더 현명하게 최신 공격에 대응하고 귀중한 시간을 절약하여 다른 시급한 현안 해결에 주력할 수 있습니다.

코그너티브 보안이란?

코그너티브 시스템은 스스로 학습하는 시스템으로서 데이터 마이닝, 기계 학습, 자연어 처리, 사람-컴퓨터 상호 작용을 활용하여 사람의 뇌가 작동하는 방식을 모방합니다.

코그너티브 보안은 포괄적이고 상호 연관된 2 가지 기능의 구현입니다.

코그너티브 시스템을 사용하여 보안 위협을 분석하고 방대한 정형 및 비정형 데이터로부터 값진 정보를 얻고 이를 실행 가능한 지식으로 발전시켜 지속적인 보안 및 비즈니스 개선을 가능하게 합니다.

코그너티브 시스템이 최고 수준의 컨텍스트 및 정확성을 확보할 수 있도록 자동화되고 데이터 중심적인 보안 기술, 기법, 프로세스를 활용합니다.

컴플라이언스부터 코그너티브까지

처음 네트워크가 탄생하고 얼마 되지 않아 해커가 등장한 이래 공격을 막기 위한 보안 기술은 꾸준히 진화했습니다. 지금까지 사이버 보안은 뚜렷이 구별되는 시대를 거쳤습니다. 주변 통제와 보안 인텔리전스 시대입니다. 이를 바탕으로 제 3 의 시대, 즉 코그너티브 보안의 시대가 시작되고 있습니다.

주변 통제 : 제한된 보안 (2005 년 이전)

방화벽, 안티바이러스 소프트웨어, 웹 게이트웨이 등 데이터 흐름을 보호하거나 제한하는 고정 방어 체계가 출발점이었습니다. 기업의 정보 보안은 컴플라이언스 활동 중 하나로 시작했습니다. 암호 및 다양한 액세스 제어 전략을 통해 중요 정보를 잠그고 그에 대한 접근을 제어하는 것이 목표였습니다. 감사를 통과하면 성공으로 간주되었습니다. 경계 방어가 아직도 사용되고 있지만 오늘날의 환경에서 그것만으로는 충분하지 않습니다.

보안 인텔리전스 : 생각을 지원하는 보안 (2005 년 이후)

차츰 정교한 모니터링 시스템으로 발전하여 방대한 데이터를 수집하고 분석함으로써 취약점을 발견하고 우선 순위에 따라 잠재적 공격을 처리할 수 있게 되었습니다. 이러한 변화로 실시간 정보에 초점을 맞추고 의심스러운 활동을 탐지하기 시작했습니다. 오늘날 보안 인텔리전스는 사용자, 애플리케이션, 인프라에서 생성하는 정형 데이터를 실시간으로 수집, 정규화하고 분석하는 것을 의미합니다.

보안 인텔리전스에서는 분석을 통해 정상적 패턴과의 불일치를 탐지하고 네트워크 트래픽의 변화를 식별하고 지정된 수준을 넘어서는 활동을 찾아냅니다. 보안 인텔리전스 인프라 내에서 방대한 정보에 분석을 적용함으로써 컨텍스트와 연계하여 기업 데이터를 이해하고 우선 순위에 따라 일상 활동을 수행합니다. 보안 인텔리전스는 어떤 비정상이 유의미한지 판단함으로써 더 신속하게 감염을 탐지하고 오탐지를 줄여 시간과 자원을 절약할 수 있게 합니다.

코그너티브 보안 : 이해하고 추론하며 학습하는 보안 (2015 년 이후)

빅데이터 분석을 활용하는 보안 인텔리전스에 기초한 코그너티브 보안은 이해, 추론, 학습 능력을 갖춘 기술을 특징으로 합니다. 이제는 현재 데이터의 80%에 달하는 비정형 데이터(예: 문서, 말)를 처리하고 해석하는 능력을 갖춘 코그너티브 시스템으로 중요 보안 데이터를 훨씬 더 큰 규모로 액세스할 수 있습니다.

특정 주제의 전문가가 관리하는 지식 코퍼스를 수용한 코그너티브 보안 시스템은 일련의 질의-응답 세트를 수신하면서 훈련 받습니다. 이러한 기계 "지식"은 보안 전문가와 시스템의 상호 작용을 통해 시스템 응답의 정확성에 대한 피드백이 이루어지면서 더욱 향상됩니다. 중요한 차이점이 있습니다. 코그너티브 시스템은 어떤 사람보다 훨씬 빠른 속도로 새로운 정보를 이해하고 처리합니다. 이제 기술적 방어 체계가 훈련을 받아 매일 수천 건의 연구 보고서, 컨퍼런스 자료, 학술 자료, 뉴스 기사, 블로그 게시물, 업계 소식을 분석할 수 있습니다.

코그너티브 시스템이 끊임없이 사건과 동작을 관찰하면서 안전한 것과 위험한 것을 구별하는 과정에서 통합 방어 체계로 새로운 위협을 차단하는 기능이 더욱 강력해집니다. 코그너티브 보안은 보안 분석가가 더 효과적이고 신속한 방식으로 새로운 위협에 대응하게 함으로써 현재의 기술력 공백을 채우고 신뢰도를 높이며 리스크를 통제하는 데 기여합니다. 그림 1 참조

시대별 보안 중요도

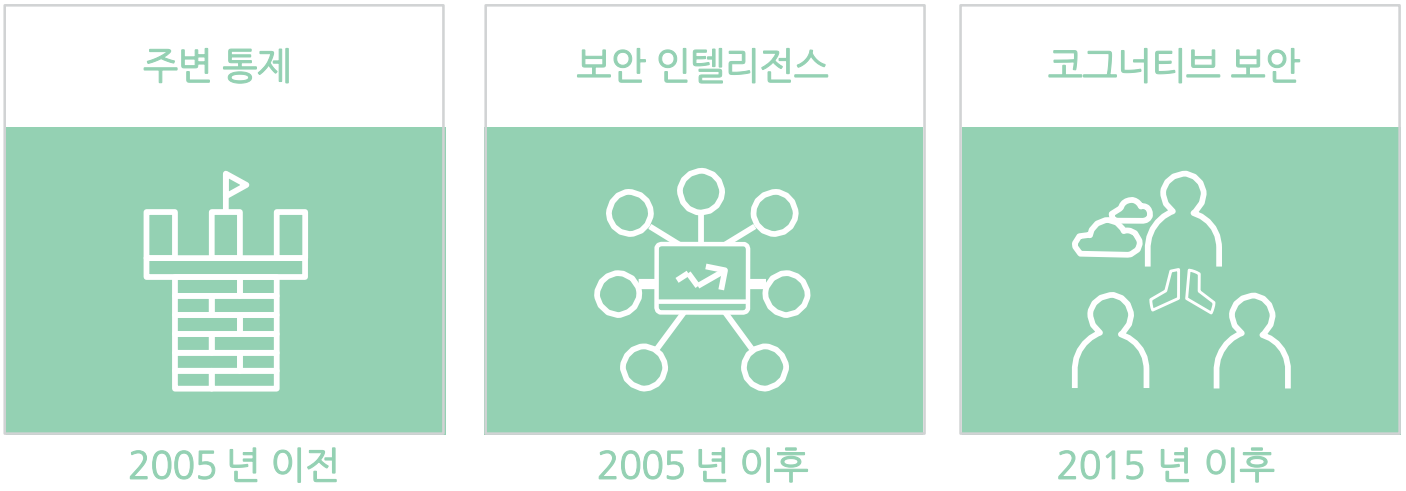


그림 1

코그너티브는 결국 기존 보안의 기초 위에 하나의 프레임워크로 자리잡을 것입니다. 보안 인텔리전스가 사라지는 건 아니고 코그너티브 보안의 핵심 구성 요소가 될 것입니다. 코그너티브는 위협 인텔리전스와 탐지 내용을 분류하고 전례 없는 속도와 규모로 실행 가능한 정보를 제공할 방법을 제시합니다.

그림 2

보안 인텔리전스와 빅데이터 분석은 대개 비정형이므로 코그너티브 요소는 현재의 상황 및 대응 방법을 이해하는 중요한 인식 단계를 추가합니다. 이와 같이 위용이 갖춰지면 해당 보안 환경에서 가능한 최고 수준의 보호를 받을 수 있습니다. 그림 2 참조

코그너티브 보안의 이점

기존의 프로그래밍 기반 보안 시스템은 미리 정의된 매개변수에 따라 요청에 응답하고 결정하고 데이터를 분석합니다. 코그너티브 시스템은 데이터를 해석하고 모든 상호 작용으로 지식 기반을 확장하고 인사이트 있는 관점에서 개연성을 평가하고 유의미한 변수를 고려한 행동을 지원합니다.

현재의 시스템은 비정상 또는 공격을 탐지하여 응답하는 사후 대응적이지만 코그너티브 보안은 사전 대응적입니다. 코그너티브 시스템은 미래에 초점을 맞추고 지속적으로 멀티태스킹을 수행하면서 취약점을 찾아내고 단편적 정보를 연결하고 변화를 탐지하고 수십억 건의 이벤트를 분석하여 실행 가능한 지식 기반을 구축합니다.

코그너티브 솔루션은 질의에 대한 답변을 생성할 뿐 아니라 가설, 증거 기반의 추론과 조언을 제공합니다. 기존 시스템에서는 접근할 수 없었던 80%의 비정형 데이터를 해석하고 이를 수많은 출처 및 위치에서 얻은 정형 데이터와 통합하는 것이 가능합니다. 점점 더 정보로부터 가치가 창출되는 글로벌 경제 환경에서 데이터는 전 세계에서 가장 풍부하고 값지며 복잡한 원자재라 할 수 있습니다. 이제는 정형 데이터와 비정형 데이터 모두 마이닝하고 지속적으로 특성과 패턴을 추출하여 실시간 컨텍스트를 확보함으로써 더 현명한 결정을 내리는 것이 가능해졌습니다.

코그너티브 보안의 다음 3 대 영역에서는 사람과 비슷한 사고 패턴이 빠른 속도로 진행됩니다.

1. 비정형 데이터와 자연어 텍스트를 **이해**하고 터득합니다. 여기에는 맥락에 따라 책, 보고서, 블로그, 관련 산업 데이터를 "읽고" 이미지를 "보고" 자연 음성을 "듣는" 활동을 통해 정보를 습득하고 이해하는 것이 포함됩니다.

2. 정보를 해석하고 체계화하는 능력을 발휘하여 **추론**하고 그 의미를 설명하고 결론을 위한 근거를 제시합니다.

3. 축적되는 데이터 및 상호 작용으로부터 얻어지는 인사이트에 기초하여 지속적으로 **학습**합니다.

더 깊이 있고 폭넓은 분석

악성코드, 악성 위협, 변칙, 비정상을 탐지하는 데만 몰두한다면 너무 많은 오탐지가 발생할 수 있습니다. 코그너티브 시스템의 다차원 분석 기능은 이와 관련하여 우위를 제공합니다.

오늘날에는 흑과 백을 구분하는 능력이 통합 보안 인프라에 필요한 전문성의 일부일 뿐입니다. 회색 지대가 점차 늘어나고 있으며 여기서 코그너티브가 진가를 발휘합니다.

더 우수한 직관, 지성, 인사이트를 지닌 코그너티브 시스템은 데이터를 통해 지속적으로 발전하면서 새로운 위협의 징후가 될 만한 미묘한 변화와 합당한 동작을 구별할 수 있습니다. 그에 따라 더 거시적 관점과 선제적 대처가 가능해집니다.

기술력 공백 해결

오늘날의 보안 환경에서 고전하는 것은 시스템뿐이 아닙니다. 실무자들도 큰 어려움을 겪고 있습니다. 전 세계적으로 충원되지 못한 정보 보안 보직 수가 208,000 개에 달하며 2020 년에는 150 만 개에 이를 것으로 예상됩니다. 코그너티브 보안으로 이 문제를 해결할 수 있습니다.

사람의 능력을 뒷받침하는 확장 가능한 리소스가 되는 코그너티브 시스템은 인력난에 시달리는 보안 팀의 특별한 보충력이 될 수 있습니다. 이 새로운 차원은 중요한 역할을 합니다. 이제는 시스템 내부 상황을 예의 주시하는 것만으로는 충분하지 않기 때문입니다. 글로벌 차원에서 위협을 모니터링하면서 잠재적 공격에 대비해야 합니다. 코그너티브 시스템은 전 세계 수천 개 고객사를 위해 초당 수십만 건의 보안 이벤트를 분석하는 글로벌 교환망을 활용할 수 있습니다

코그너티브는 고급 시각화, 대화형 취약점 분석, 리스크 평가, 조치방안, 출처 규명 등 사람 중심의 커뮤니케이션 기능을 제공하여 보안 분석가의 부담을 덜어줄 수 있습니다. 코그너티브 시스템은 비정상 요소 및 결함 있는 로직을 식별하고 증거 기반의 추론을 수행할 것입니다. 그러면 분석가는 대안의 결과를 고려하여 더 현명한 결정을 내릴 수 있습니다.

코그너티브 활용 :

SOC 분석가 지원

코그너티브 시스템에서 방대한 정형 및 비정형 데이터를 이해하여 주니어 분석가가 시니어 분석가로 고속 성장하도록 도울 수 있습니다. 코그너티브 시스템은 연구 보고서, 모범 사례와 같은 정보 수집을 자동화한 다음 실시간으로 관련 정보를 제공할 수 있습니다. 이전에는 이러한 지식과 인사이트를 갖기 위해서는 다년간 경험을 쌓아야 했습니다.

외부 인텔리전스를 활용하여 신속하게 대응

또 다시 Heartbleed 취약점이 나타나면 수많은 블로그에서 그 대응 방법을 다룰 것입니다. 이 위협에 대한 시그니처가 제공되지 않은 상황에서도 자연어 온라인 대화를 통해 해결 방법을 찾을 수 있습니다. 코그너티브 시스템은 크롤링을 수행하여 다음 제로데이 익스플로잇을 차단할 방법을 신속하게 알아낼 수 있습니다.

첨단 분석 기능으로 위협 식별

코그너티브 시스템은 기계 학습, 클러스터링, 그래프 마이닝, 엔티티 관계 모델링과 같은 분석 기법을 활용하여 잠재적 위협을 파악할 수 있습니다. 이를 통해 실제 피해가 발생하기 전에 위험한 사용자 행동, 데이터 유출, 악성코드 활동을 신속히 탐지하는 것이 가능합니다..

애플리케이션 보안 강화

코그너티브 시스템은 코드 및 코드 구조를 탐색하는 과정에서 분석 및 데이터의 의미론적 맥락을 파악할 수 있습니다. 수천 건의 취약점 조사 결과로부터 소수의 실행 가능 항목을 추출하고 코드에서 수정 가능한 위치로 연결하는 것이 가능해집니다.

전사적 리스트 완화

미래에는 코그너티브 시스템이 각종 상호 작용과 그 특성 및 감수성에 대한 집합체(corpus)를 분석하여 조직, 기업 활동, 훈련 및 재교육을 위한 리스크 프로필을 개발할 수 있습니다. 코그너티브 시스템에서 자연어 처리를 통해 어떤 조직에 민감한 내용의 데이터를 검색하고 수정할 수 있습니다.

미래 : 사이버 범죄 경제 환경의 반전

코그너티브 시스템은 악성코드라고 부르는 수많은 악성 소프트웨어의 기능과 특성을 분석하여 미묘한 공통점을 찾아낼 수 있습니다. 이는 매우 중요합니다. 악성 소프트웨어가 엄청나게 다양하지만 사이버 범죄 조직은 각자의 코드를 지속적으로 발전시켜 왔기 때문에 현재 활동 중인 악성코드의 상당수가 서로 관련되어 있습니다. 코그너티브 시스템으로, 의심스러운 실행 파일의 수천 개의 특성을 분석하고 분류하여 패턴을 찾아낼 수 있습니다. 사람의 능력으로는 그 특징이 무엇인지 어떻게 또는 왜 일치하는지 알지 못하더라도 시스템에서 패턴을 찾아내 새로운 악성코드 변종을 밝혀내고 분류할 수 있습니다.

코그너티브 보안 커뮤니티가 성장하고 새로운 공격의 성공률이 낮아지면 사이버 범죄 세계는 새로운 경제적 현실에 맞닥뜨리게 됩니다. 탐지를 피하는 악성코드 개발이 더욱 까다로워지고 많은 비용이 소요됩니다. Ponemon Institute 의 2015 년 데이터 유출 사고 비용 연구에 따르면 기업에서 지능적 지속 위협을 탐지하는 데 평균 256 일이 걸립니다. 또한 미국에서 발생한 데이터 유출 사고의 평균 비용이 650 만 달러에 달했습니다. 보안 분석가는 코그너티브 보안을 통해 잠재적 공격의 조기 징후를 성공적으로 찾아내고 훨씬 더 신속하게 탐지할 수 있습니다. 사이버 범죄자가 공격에 대한 보상을 누리는 것이 더욱 힘들어질 것입니다.

코그너티브 컴퓨팅은 데이터뿐 아니라 의미, 지식, 프로세스 흐름, 활동의 진도까지 매우 빠르게, 훨씬 더 광범위하게 활용하면서 거대한 변화를 일으키고 있습니다. 코그너티브 기능을 받아들이는 기업은 폭넓고 강력한 경쟁 우위를 확보할 수 있습니다.

코그너티브 에코시스템을 위한 통합과 전문성

올바른 보안을 실현하기 위해서는 통합과 전문성이 관건입니다. 통합되지 않고 신속한 대응에 필요한 가시성 및 실행 가능한 인텔리전스를 제공하지 않는 수많은 포인트 제품으로부터 너무 많은 보안 프랙티스가 생성되고 있습니다.

완벽한 통합이 이루어지려면 하이브리드 IT 환경 전반에서 각 전문 기능이 서로 연계하고 소통하면서 사외의 영역까지, 즉 에코시스템 전반으로 확장되어야 합니다. 이와 같이 올바른 통합은 보안 사고가 발생하더라도 신속하게 대응하는 데 필요한 가시성을 제공할 수 있습니다. 통합을 통해 더 적은 노력으로 더 많은 일을 해낼 수 있으며, 이는 보안 기술력의 공백을 근본적으로 해결할 처방이 됩니다.

매일 새로운 위협이 발견되고 있는 만큼 보안 전문성 및 위협 인텔리전스 공유가 필수적입니다. 최고 수준의 전문성을 솔루션 및 인지 활동에 접목할 수 없다면 곧 뒤처질 수 밖에 없습니다. IBM X-Force Exchange 에서는 현재 88,000 개 이상의 취약점에 대한 정보, 250 억 개 이상의 웹 페이지, 1 억 개의 엔드포인트에서 수집한 데이터를 카탈로그화하여 즉시 활용 가능한 글로벌 범위의 전문성을 실시간으로 제공하고 있습니다.

IBM 의 역할

코그너티브의 여정은 이제 막 시작했지만, IBM 은 보안 분야에서 코그너티브 혁명을 이끌 지적 및 경제적 능력을 갖추었습니다. 전 세계 36 개 보안 센터에서 7,500 명 이상의 IBM Security 전문가들이 매일 133 개국에서 발생하는 350 억 건의 이벤트를 모니터링하고 있습니다. IBM 은 수십 년 전부터 코그너티브 기술에 투자해 왔으며 지난 5 년간 자연어 처리, 음성 및 영상 처리, 쿼리하기 용이한 지식 그래프와 같은 툴을 위한 비정형 데이터 활용 등에서 괄목할 만한 성과를 거뒀습니다. IBM 은 코그너티브 기술을 적극 수용하여 지속적으로 보안 유스 케이스를 발전시키고 이 정보를 보안 분석가에게 제공할 것입니다.

IBM Security 는 현재 여러 솔루션에서 코그너티브 기능을 접목시키고 있습니다. 취약점 탐지 정확도를 높이고 우선 순위에 따라 이 취약점을 처리하여 더 신속하게 대응하는 데 기계 학습을 이용합니다. 네트워크에서 진행 중인 위협을 미리 예측하고 그와 관련된 비정상 요소를 발견하는 데 행동 학습을 이용합니다.

IBM Security 는 심층 분석, 신원 및 액세스, 첨단 사기, 데이터, 애플리케이션, 네트워크, 엔드포인트, 클라우드, 모바일, 리서치를 포괄하는 종합적인(end-to-end) 보호 및 면역 체계 방식을 적용합니다. 이러한 플랫폼 각각에서 IBM 코그너티브 기능을 활용할 것입니다. 코그너티브 보안의 혜택을 누리고 싶다면 코그너티브 기술을 혁신적으로 구현하고 융합하는 IBM 플랫폼 도입을 고려해 보십시오.

실행해야 할 3 가지

1. 위협에 선제적으로 대응하기 위해 코그너티브 기능 활용에 대해 연구

2. 코그너티브 기능을 활용할 준비가 되도록 보안 로드맵 개발

3. 보안 인프라 내에서 통합 촉진

자세한 정보

http://www.ibm.com/security/kr/ko/

IBM Security 소개

IBM Security 는 엔터프라이즈 보안 제품 및 서비스로 구성된 가장 발전되고 통합된 포트폴리오를 제공합니다. 세계 최고의 IBM X-Force 연구 개발 조직이 뒷받침하는 이 포트폴리오에서는 기업이 거시적 관점으로 사용자, 인프라, 데이터, 애플리케이션을 보호할 수 있도록 보안 인텔리전스를 제공하고 계정 및 접근권한 관리, 데이터베이스 보안, 애플리케이션 개발, 리스크 관리, 엔드포인트 관리, 네트워크 보안 등을 위한 솔루션을 공급합니다. 이러한 솔루션을 통해 모바일, 클라우드, 소셜 미디어, 기타 엔터프라이즈 비즈니스 아키텍처에서 효과적으로 리스크를 관리하고 통합형 보안을 구현할 수 있습니다. IBM 은 전 세계에서 가장 광범위한 보안 연구, 개발, 딜리버리 조직을 운영하면서 매일 133 개국에서 발생하는 350 억 건의 보안 이벤트를 모니터링하며 3,700 건 이상의 보안 관련 특허도 보유하고 있습니다.

또한 IBM Global Financing 과 함께 가장 경제적이고 전략적인 방식으로 귀사의 비즈니스 요구 사항에 부합하는 소프트웨어 기능을 도입할 수 있습니다. 신용 조건에 부합하는 고객과 함께 비즈니스 및 개발 목표를 뒷받침할 맞춤형 금융 지원 솔루션을 개발하고 효과적인 자금 관리 및 총소유비용 절감을 지원합니다. IBM Global Financin 을 통해 귀사에 중요한 IT 투자의 재원을 마련하고 비즈니스 성장의 동력을 확보하십시오. 자세한 내용은 ibm.com/financing 에서 확인하십시오

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

SEW03134USEN-00