



코그니티브 시대의 사이버 보안

디지털 면역 시스템(Immune System) 가동

IBM 기업가치연구소

위협 환경에서 요구되는 새로운 전문성

보안 분야의 리더들은 인텔리전스, 속도, 정확성의 세 가지 측면에서 드러나는 기존 역량의 한계를 극복하고자 애쓰고 있습니다. 일부 기업에서는 이러한 전문성의 빈틈을 보완하고 위험 및 위협에 대비하는 방법으로 코그너티브 보안 솔루션에 주목하고 그 가능성을 타진하기 시작했습니다. IBM 설문 조사에 참여한 보안 리더의 57%가 코그너티브 보안 기술로 사이버 범죄자의 활동을 크게 둔화시킬 수 있다고 생각합니다. IBM이 “준비된 그룹(Primed)”으로 분류한 22%의 응답자는 코그너티브 시대의 사이버 보안을 향한 여정을 이미 시작했습니다. 이들은 코그너티브 보안 기술이 더 이상 생소하지 않고 충분히 성숙했으며 필요한 리소스도 확보했다고 확신합니다. 귀사도 이들과 같이 코그너티브 사이버 보안의 여정을 시작하려면 귀사의 약점을 조명하고 코그너티브 솔루션으로 귀사의 보안 역량을 보완할 방법을 결정하고 귀사의 이해 관계자를 위한 교육 및 투자 계획 수립에 나서야 합니다.

요약

사이버 보안이 전환점을 맞이하고 있습니다. 보안 위협이 수적으로 급격히 증가하는 가운데 보안 운영 팀은 고전하고 있습니다. 보안 위협 환경이 빠르게 변화하고 위협의 변종이 더욱 정교해지고 많아지면서 기존의 방식으로는 감당하기 어려운 수준이 되었습니다. 각종 보안 사고 및 데이터 유출의 파급 효과가 갈수록 확산되면서 경제적 비용 및 위험 또한 빠르게 증가합니다. 게다가 다수의 기업은 적합한 기술력을 가진 보안 전문가가 부족한 상태입니다. 이와 같은 여러 스트레스 요인 때문에 기업이 스스로를 지킬 튼튼한 디지털 면역 시스템을 유지하기가 힘들어집니다.

최근 IBM은 35개국, 18개 산업의 최고 정보보안책임자(CISO) 및 보안 리더 700명을 대상으로 설문 조사를 실시했습니다. 이 리더들의 당면 과제, 미비한 점, 해결을 위한 노력을 알아보는 데 목적을 두었습니다. 또한 코그너티브 보안 솔루션에 대한 그들의 관점, 즉 이 솔루션이 어떻게 도움이 될 수 있는지, 각자 이 솔루션을 구현할 준비가 얼마나 되었는지, 무엇이 걸림돌로 작용할 수 있는지에 대한 생각을 듣고자 했습니다.

보안 리더들은 위협의 복잡성 및 그에 대응하는 속도를 당면 과제로 꼽았습니다. 이들은 보안 사고가 현재의 기업 운영 및 미래의 기업 평판에 미칠 영향을 우려합니다. 네트워크/데이터 보호 및 신속하고 현명한 위협 대응 측면에서 부족함을 느끼고 있습니다. 앞으로 몇 년 내에 이와 같은 미비한 점을 해결할 계획이지만, 이를 위한 적합한 리소스 확보는 쉽지 않을 것입니다. 보안 리더는 비용이 치솟고 고급 보안 리소스가 부족한 현실에서 비즈니스 리더에게 투자의 타당성을 더 설득력 있게 전달할 방법을 모색하고 있습니다.



현재 및 미래의 **일차적인 사이버 보안 과제**는 **사고 대응 및 해결의 평균 시간을 단축하는 것**입니다.



보안 리더의 **57%**는 **코그너티브 보안 솔루션으로 사이버 범죄자의 활동을 크게 둔화할 수 있다**고 생각합니다.



앞으로 2년 ~ 3년간 **코그너티브 보안 솔루션을 구현**하는 전문가의 수가 **3배 정도 늘어날 것**으로 예상됩니다.

기업에서 더 많은 보안 데이터를 수집하고 더 많은 분석 기능을 적용함에 따라 워크로드가 증가하면서 이제 더 이상 수작업으로 이루어지는 방식은 한계에 이르렀습니다. 이러한 상황을 타개하고 인텔리전스, 속도, 정확성의 한계를 극복하고자 코그너티브 보안 솔루션에 주목하는 기업도 있습니다. 보안을 위한 코그너티브 기술은 초기 단계이지만 그 잠재력에 대한 기대와 낙관이 큼니다. 이번 설문 조사에서 응답자들은 코그너티브 기반 보안 솔루션에 가장 기대하는 점으로 탐지 및 대응을 위한 의사결정 기술 향상, 사고 대응 시간 대폭 단축, 일상적 이벤트와 실제 보안 사고의 구별 능력 향상을 꼽았습니다. 이와 같이 큰 가능성을 가진 기술이지만 앞으로 보편적으로 사용되기 위해서는 더 많은 교육과 준비가 필요합니다.

IBM은 “코그너티브 시대에 준비된” 보안 솔루션을 갖춘 기업들을 발견했습니다. 보안 실효성, 코그너티브 준비성, 이해와 인식의 측면에서 코그너티브 시대를 맞이할 만반의 준비를 갖췄다고 확인하는 보안 리더들을 만났습니다. 대체로 이들은 상대적으로 코그너티브 솔루션에 친숙하고 전반적으로 보안 기능에 대해 강한 자신감을 갖고 있으며 리소스 확보에도 별 어려움이 없는 편입니다.

코그너티브 보안 솔루션이 확고히 자리잡고 널리 보급되면 모든 기업이 그 혜택을 누릴 수 있게 됩니다. 귀사에서 이 여정을 시작할 경우 가장 먼저 할 일은 코그너티브 보안 솔루션으로 귀사의 어떤 취약점을 해결할지 결정하는 것입니다. 그 다음에는 가능한 활용 사례(use cases)를 알아보고 이를 귀사의 취약점과 연결해야 합니다. 투자의 타당성을 입증해야 한다면 비즈니스 이해 관계자에게 코그너티브 보안 솔루션으로 누릴 수 있는 혜택을 알리고 인식을 제고하는 데 집중해야 합니다. 코그너티브 보안 솔루션을 통해 귀사의 전반적인 보안 수준을 끌어올릴 수 있음을 경영진이 이해할 수 있는 비즈니스 언어로 강하게 피력하십시오. 이 초기 단계를 거치면서 코그너티브 시대의 사이버 보안을 준비하게 됩니다.

현재 당면 과제

이번 조사에 참여한 보안 리더들은 각자의 기술 및 조직 역량에 대한 확신을 갖고 있습니다. 사이버 보안 준비 상태에 관한 질문을 받자 대다수(77%)는 업계의 다른 기업과 동등한 수준이라고 밝혔습니다. 또한 향후 2년 ~ 3년의 사이버 보안에 대해서도 매우 낙관적이었는데, 86%가 업계의 다른 기업보다 더 유리한 상황이라고 말했습니다.

보안 리더들은 다른 누구 못지않게 잘하고 있으며 앞으로 더욱 발전할 것으로 확신합니다. 3/4 가까이는 기업 보안의 기초적 문제를 잘 다루고 있다 생각하며 72%는 IT 안전성에서, 71%는 전사적 범위의 위험 인식 제고에서 성과를 거두고 있다고 밝혔습니다. 이제 더 깊숙이 들어가서 보안 투자의 과제, 영향, 전문성, 자원, ROI와 관련된 현황을 살펴보겠습니다.

필요한 것은 대응 속도

응답자의 45%가 최우선 사이버 보안 과제로 꼽은 것은 사고 대응 및 해결 시간 단축입니다. 2년 ~ 3년 새에 이 문제가 해결되지는 않을 것으로 예상하고 있으며, 대응 속도 관련 과제는 앞으로도 최우선 사이버 보안 과제로 남으리라 예상합니다(그림 1 참조).

“해적 황금기에 살았던 무역상과 같은 처지입니다. 군대나 공권력의 보호 없이 자력으로 해결해야 합니다. 이 상인들 대다수는 배를 조종할 줄도 모르고 공격자에 맞서 싸우는 것도 (법에 저촉되므로) 불가능합니다. 마치 양팔이 등 뒤에 묶인 채 사투를 벌이는 것 같습니다. 하지만 나를 둘러싼 온갖 위협에 대한 모든 것을 알아낼 수 있는 기막히게 훌륭하고 정교한 방법이 나타났습니다.”

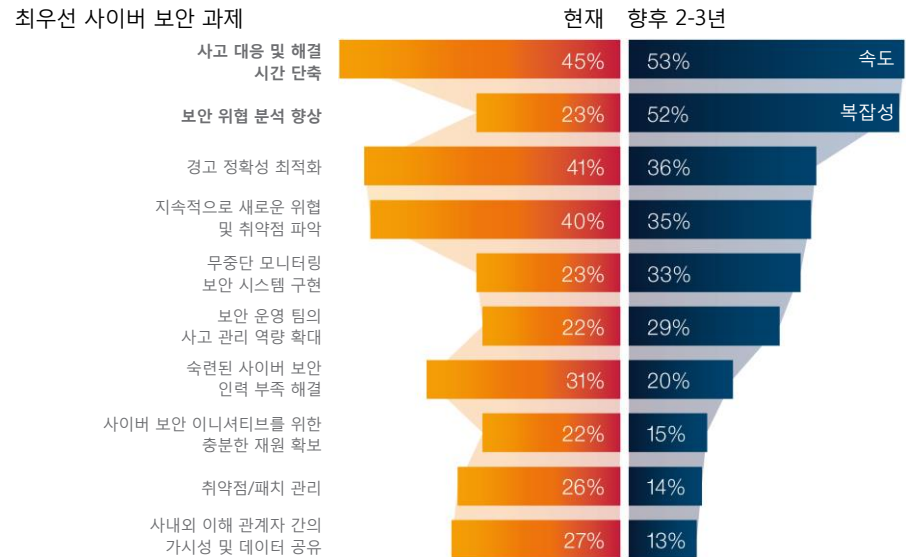
David Shipley, New Brunswick 대학교 정보 기술 서비스 전략 이니셔티브 책임자

시간이 길어질수록 가중되는 위험

Ponemon Institute의 2016년 조사에 따르면 보안 사고를 발견하기까지 평균 201일, 이를 억제하는 데에는 평균 70일이 소요됩니다. 또한 데이터 유출 사고의 비용을 줄일 가장 효과적인 방법으로 사고 대응팀 가동을 꼽고 있습니다.¹

그림 1

현재 가장 중대한 사이버 보안 과제를 선정하고, 이 과제가 가까운 장래에 어떤 양상을 보일 것인지 내다봤습니다.



80%의 기업에서 사고 대응 속도가 2년 전보다 훨씬 빨라졌다고 평가했지만(평균적으로 16% 향상) 여전히 우려되는 상황입니다. 86%는 향후 2년 ~ 3년간 대응 속도를 한층 더 높이려 합니다(평균적으로 24% 향상이 목표).

이 속도는 기업에게 특히 중요한 문제입니다. 사고 대응 시간이 길어질수록 피해의 규모가 커지고 위기 해결 비용도 눈덩이처럼 불어납니다. 시간은 손실 위험을 가중시키는 가장 결정적인 요소입니다.

보안 리더들은 더 효과적인 보안 위협 분석의 필요성도 느끼고 있습니다. 23%가 현재의 최우선 과제로 꼽았으며 52%는 더 효과적인 보안 위협 분석이 향후 2년 ~ 3년간 가장 중대한 사이버 보안 과제가 될 것으로 예상합니다. 보안 분석가가 가장 시급히 해결해야 할 위협을 판별하고 행동의 패턴 및 이상을 신속하게 포착하려면 다양한 도움이 필요합니다. 따라서 기업의 보안 리더는 속도를 높이고 위협의 복잡성을 해결하는 데 모든 수단을 강구할 것입니다.

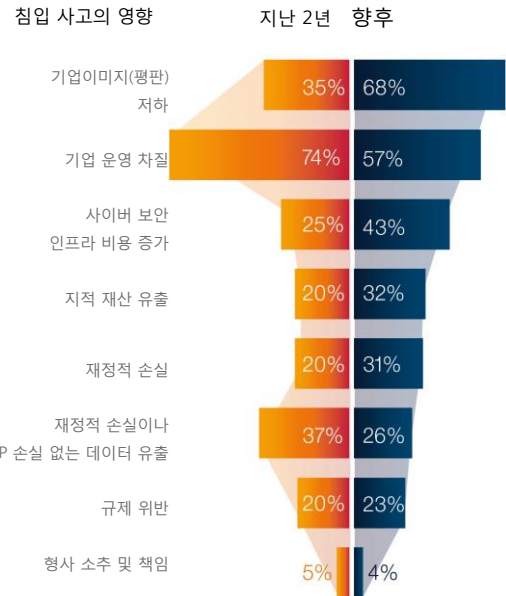
운영 차질과 이미지 실추 우려

설문 응답자의 3/4 가까이는 지난 2년간 각종 침입 사고로 인해 기업 운영에 큰 차질을 겪었다고 말했습니다. 그러나 향후 몇 년간 지금까지와는 매우 다른 상황이 전개될 것으로 예상합니다.

기업들은 향후, 침입 사고로 인한 기업 운영 차질보다는 기업 이미지 실추, 즉 브랜드 평판 저하를 점점 더 우려하는 것으로 나타났습니다. 지난 2년간 발생한 침입 사고의 영향으로 평판 저하를 선택한 응답자는 35%였지만, 앞으로 이 문제가 걱정된다고 밝힌 응답자는 68%, 2배에 달합니다(그림 2 참조). 즉 다수의 보안 리더들은 침입의 여파가 확대되는 것을 경계합니다. 보안 사고는 갈수록 기업의 운영뿐 아니라 평판도 좌우할 것이고, 고객의 신뢰를 잃고 외면 받으면서 매출이 하락하게 될 것입니다.

그림 2

기업들은 지난 2년간 침입 사고로 다양한 여파가 있었지만 앞으로 다른 양상을 보일 것으로 내다봤습니다.



치솟는 사이버 보안 인프라 비용도 앞으로 더 우려되는 문제입니다. 공격의 위험이 계속되면 그 해결에 더 많이 지출할 수 밖에 없습니다. 보안 리더는 공격을 당하면 그 책임 소재나 원인을 찾아 해결해야 한다고 생각하고 인력, 포인트 솔루션, 인프라 업그레이드에 나섭니다.

중요 보안 영역과 대응 능력의 격차

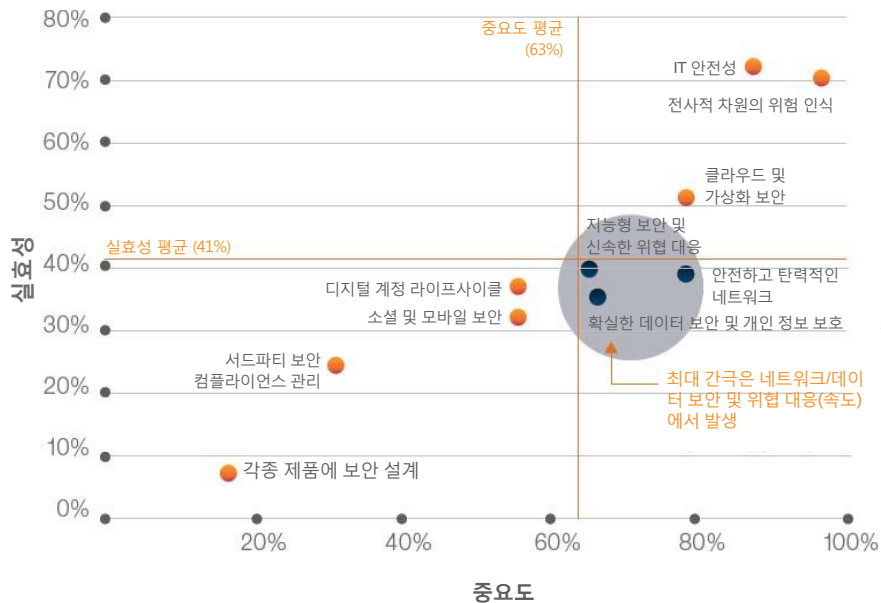
다양한 보안 기능 중에서 자사 보안에 중요한 것과 현재 잘하고 있는 것이 무엇인지 물었습니다. 일반적으로 보안 리더는 소홀한 점이 단 하나라도 있어서는 안 된다는 생각에 거의 모든 것을 중요하게 다루려고 합니다. 그러나 한정된 리소스로 모든 영역에서 최고 수준을 유지할 수는 없습니다. 새로운 기술, 접근법, 과제가 끊임없이 등장하는 경우에는 더욱 그렇습니다.

IBM은 응답자들이 중요하다고 생각하지만 현재 효과적으로 대응하지 못하는 분야에 주목하려 합니다(그림 3 참조). 이를테면 위협 대응과 연계하는 네트워크 및 데이터 보호입니다.

응답자들은 위협 대응 속도, 보안 정보 이벤트 관리(SIEM), 네트워크 활동 탐지, 필터링, 데이터 분류 및 데이터 유출 방지에서 필요한 만큼의 효과를 거두지 못한다고 밝혔습니다. 대응 속도에 초점을 맞추고 더 뛰어난 위협 분석을 통해 복잡성을 관리함으로써 획기적으로 방어 체계를 강화할 수 있어야 합니다.

그림 3

다양한 보안 전문성의 중요성 및 실효성



“전사 차원에서 보안 모니터링 및 분석을 통해 다방면에서 비용 절감 효과를 거뒀고, 스팸을 대폭 줄여 밴드위스(bandwidth) 비용을 절감하고 사용률이 저조한 리소스 가동을 중단하여 직원들의 업무 생산성을 높였습니다.”

캐나다 자산 관리 기업의 금융 보호 책임자

보안 투자 타당성 확보 문제

효과적인 사이버 보안 구축에 드는 비용이 크게 늘어나고 당분간은 이 증가세가 이어질 것으로 보입니다. 사이버 보안 비용이 지난 2년간 증가했다는 응답이 78%, 앞으로 2년 ~ 3년간 계속 증가할 것이라는 의견이 84%였습니다. 실제로 응답자의 70% 이상은 전체 IT 예산의 10%가 넘는 비용을 사이버 보안에 지출합니다(10% ~ 15%인 곳이 가장 많음). 대개 예방 및 탐지에 쓰이는 비용입니다. 금융 기관의 경우 매년 많게는 5억 달러 이상을 사이버 보안에 사용합니다.² 더 많이 지출하더라도 더 확실한 안전이 보장되는 건 아니기 때문에, 투자의 타당성을 입증하라는 압박이 더욱 거세질 것입니다.

92%의 응답자가 사이버 보안을 위한 경제적 지원을 요청할 때 ROI 또는 기타 재무 분석을 통해 그 타당성을 입증해야 한다고 밝혔습니다. 이와 같이 투자의 타당성을 입증하는 데 가장 많이 활용되는 2가지 수단은 조직의 현재 위험 수준에 대한 명확한 커뮤니케이션(61%)과 재무 팀, 위험 관리 팀, 운영 팀, 기타 주요 경영진의 지지 확보(51%)입니다. 보안 리더는 비즈니스 언어로 자신의 니즈를 설명하면서 다른 경영진을 설득해야 하기 때문에,³ 앞으로는 새로운 방법으로 사이버 보안 투자 비용의 근거를 제시하고 그 가치를 보여주어야 합니다. 보안이 단순히 보험 상품과 같거나 비즈니스 활동을 위해 치러야 하는 비용이라는 인식에서 벗어나야 합니다.

사이버 보안 위협에 대한 대비

반가운 소식은 설문 조사에 참여한 보안 리더들이 각자 부족한 점을 인식하고 서둘러 해결할 계획이라는 것입니다. 기업들은 사이버 보안 위협에 대한 대비 태세를 강화하고자 다양한 이니셔티브를 추진하는 중입니다(그림 4 참조). 당장은 교육 및 훈련을 통한 직원의 행동 개선에 역점을 두고 있는데 67%가 여기에 주력하고 있습니다. 응답자의 40%는 계정 모니터링 소프트웨어도 구현하고 있습니다. 이는 일반적으로 기초 요건으로 분류되는 옵션들입니다.

그림 4

보안 리더들이 사이버 보안 위협에 대한 대비를 강화하기 위해 추진하고 있는 이니셔티브

현재 순위	2-3년 후 순위	이니셔티브
1 ▼ -30%	5	교육 및 훈련으로 직원의 행동 개선
2 ▼ -25%	7	계정 모니터링(사용자 활동) 소프트웨어 구현
3 ▲ +8%	4	새로운 분석 톨로 운영/전략 보안 지표 보고
4 ▲ +28%	1	네트워크, 애플리케이션, 데이터 레벨 보안 모니터링 개선
5 ▲ +17%	3	사고 대응 방법론, 프로세스, 대응 속도 개선
6 ▼ -9%	8	보안 분석가 추가 고용 및 훈련
7 ▼ -16%	10	애플리케이션 보안 테스트(모바일, API 포함)
8 ▲ +36%	2	SOC 기능 구현 또는 업그레이드
9 ▲ +14%	6	코그니티브 기술 기반 보안 솔루션 구현
10 ▲ +1%	9	보안 운영에 포렌직 기능 통합

“보안 리더는 더 적극적으로 투자의 타당성을 입증해야 합니다. 왜냐하면 보안에 막대한 비용을 사용하면서도 훨씬 더 안전해졌다는 피드백을 경영진들로부터 얻지 못하기 때문입니다.”

Chad Holmes, Ernst & Young LLP 책임자(Principal) 겸 사이버 보안 기술 리더(CTO)

이러한 개선 이니셔티브는 앞으로 2년 ~ 3년간 거대한 변화를 겪을 것으로 예상됩니다. 실제로 응답자들은 최상위 3개 이니셔티브가 지금과는 전혀 다를 것이라고 밝혔습니다. 1위는 네트워크, 애플리케이션, 데이터 레벨의 보안 강화가 될 것입니다(57%). 그 다음은 SOC 기능 구현 또는 업그레이드입니다. 마지막으로, 사고 대응 속도 향상이 3위에 새롭게 진입할 것입니다. 이 영역 모두 앞서 언급했던 대응 능력 부족과 관련 있습니다.

보안 리더가 각자의 미흡한 점 해결에 나선 것은 반가운 일이지만, 우선 순위가 크게 달라지면서 새로운 간극이 생기거나 기존 간극이 커질 수도 있습니다. 어떤 경우에서든 보안 리더는 비즈니스에 가장 중요한 문제를 해결해야 합니다. 관건은 이러한 미흡한 것들을 보완하는 작업이 실행에 옮겨질 수 있는가입니다..

3대 간극

이 모든 과제, 취약점, 노력, 압박 요인은 인텔리전스, 속도, 정확성의 3대 간극을 중심으로 합니다. 보안 리더는 이러한 한계를 극복하는 한편 비용 및 ROI 문제도 다뤄야 합니다.

인텔리전스 간극

- 65%가 불충분한 리소스 때문에 위협 탐지의 어려움이 가장 크다고 답했습니다.
- 40%는 지속적으로 새로운 위협 및 취약점을 파악하고 대비하는 것이 중대한 사이버 보안 과제라고 말했습니다.

속도 간극

- 80%가 2년 전에 비해 사고 대응 속도가 훨씬 빨라졌다고 평가하지만, 현재와 미래의 최대 사이버 보안 과제는 사고 대응 및 해결의 평균 시간을 단축하는 것입니다.
- 사고 대응 개선을 위한 과제가 진행 중이라는 응답은 27%에 불과했지만 2년~3년 후에는 43%까지 증가할 것입니다.

정확성 간극

- 응답자들은 경고의 정확성 이슈를 두 번째 까다로운 과제로 꼽았습니다. 즉 현재는 오탐이 너무 많다는 것입니다.
- 61%는 리소스 부족 때문에 위협 식별에서도 큰 어려움을 겪는다고 밝혔습니다. 이는 위협을 평가하고 그로부터 발생할 수 있는 잠재적 사고를 알아내는 것입니다.

코그니티브 보안 솔루션에 대한 기대로 가장 많이 언급된 혜택



1. 인텔리전스

탐지 및 사고 대응 의사결정 가능 향상



2. 속도

획기적으로 사고 대응 시간 단축



3. 정확성

일상적 이벤트와 실제 보안 사고의 구별법에 대한 신뢰도 향상

3배 증가

향후 2-3년간 도입될 코그니티브 보안 솔루션

코그니티브 보안 솔루션의 시대

코그니티브 보안의 활용 분야는?

보안 동향을 분석하고 방대한 정형 및 비정형 데이터를 정제하여 실행 가능한 지식을 얻는 데 코그니티브 시스템이 활용될 것입니다. 보안 리더 및 분석가가 각종 연구 문서, 업계 간행물, 분석 보고서, 블로그 등 생성된 보안 지식을 모두 흡수할 수는 없습니다. 코그니티브 시스템은 그러한 정보와 더 전통적인 보안 데이터의 융합을 모색합니다. 코그니티브 보안 솔루션과 자동화된 데이터 중심의 보안 기술, 기법, 프로세스가 만나 최고 수준의 상황 정보 및 정확성이 보장될 것입니다.

코그니티브 보안 솔루션으로 SOC 분석가의 전문성을 보완할 수 있습니다. 즉 응답 속도를 높이고 더 효과적으로 위협을 식별하고 애플리케이션 보안을 강화하고 기업의 전반적인 위험 수준을 낮추는 데 활용합니다. 분석가들이 일상적이고 반복적인 보안 작업에 매달리지 않고 까다로운 임무에 전념하게 하는 데 목적이 있습니다.

이와 같은 간극을 해소하려면 다양한 기술 및 접근법이 필요합니다. 무작정 자금을 투입하거나 인력을 고용하는 것만으로 목표를 이룰 수는 없습니다.

바야흐로 코그니티브 보안의 시대가 시작되고 있습니다. 보안 기술이 발전하면서 고정된 방어 체계 등에 의존하는 단순한 경계 제어 기능보다는 실시간 정보, 패턴 불일치 등에 주목하는 지능적인 보안 인텔리전스 기능이 각광받고 있습니다. 따라서 정형 및 비정형 보안 데이터를 모두 분석하여 상황, 행동, 의미를 이해할 수 있는 솔루션이 본격화될 것입니다. 코그니티브 보안은 보안 분석가와 이들이 구사하는 기술 간의 새로운 관계를 지향합니다. 코그니티브 보안 솔루션은 정보를 해석하고 체계화하며 그 의미를 설명할 뿐 아니라 결론에 대한 근거도 제시할 수 있습니다. 또한 데이터가 축적되고 상호 작용을 통해 인사이트가 개발되면서 지속적인 학습이 이루어집니다.

코그니티브 보안 솔루션의 혜택

코그니티브 기술 기반의 솔루션으로 다음과 같은 혜택을 누릴 수 있습니다.

- 초보 SOC 분석가가 예전에 오랜 경험을 통해서만 얻을 수 있었던 베스트 프랙티스 및 인사이트를 접하면서 전문 역량이 향상됩니다.
- 블로그 및 기타 외부 소스에 인텔리전스를 적용하면서 더 발 빠르게 대응하고 시그니처가 나오기 전에도 조치를 취할 수 있습니다.
- 첨단 분석 기법을 통해 신속하게 위협을 식별하고 위험한 사용자 행동, 데이터 유출, 악성코드 감염 사례를 탐지합니다.
- 로컬/외부 데이터 수집 및 추론을 자동화하면서, 보안 사고에 대한 상황 인식을 확대합니다.

전망 및 과제

응답자 다수는 코그너티브 보안 솔루션으로 현재의 간극들을 해결할 것으로 믿고 있습니다. 이는 새로운 기술 분야이지만, 응답자의 57%가 사이버 범죄자의 활동을 크게 둔화시킬 수 있다고 기대하고 있습니다. 즉 코그너티브 보안의 가능성 및 잠재적 혜택을 인정하고 있습니다.

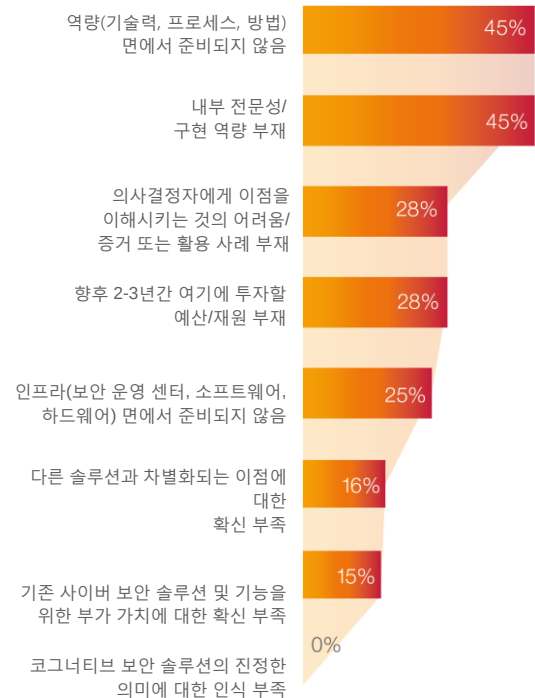
코그너티브 기반 보안 솔루션으로 누릴 혜택을 묻는 질문에서 40%는 탐지 및 사고 대응 의사결정 기능의 향상이라고 답했고, 37%는 사고 대응 시간 대폭 단축, 36%는 이벤트와 실제 사고의 구별법에 대한 신뢰도 향상이라고 밝혔습니다. 이들은 코그너티브 보안 솔루션으로 간극 해소를 원합니다.

지금까지 사이버 보안 위협에 더 철저히 대비하고자 코그너티브 기반 보안 솔루션을 구현하는 중이라는 응답은 7%에 불과했습니다. 새로운 기술이므로 뜻밖의 결과는 아닙니다. 그러나 조만간 이 솔루션 구현을 검토하겠다는 응답자는 그 3배인 21%에 달합니다. 보안 리더들이 디지털 면역 시스템 강화를 위해 코그너티브 보안 기능을 추가 하면서 머지않아 도입 속도가 빨라질 것입니다.

응답자들은 코그너티브 보안 솔루션 도입 시 극복해야 할 과제에 주목했습니다. 즉 기술력, 프로세스, 방법론입니다. 45%는 부족한 인적 역량과 사내 기술력 부족을 최대 장애물로 꼽았습니다(그림 5 참조). 이러한 우려를 해소하려면 추가적인 교육 및 준비가 이루어져야 합니다

그림 5

보안 리더들이 코그너티브 보안 솔루션 구현과 관련하여 극복해야 할 주요 과제를 꼽았습니다.



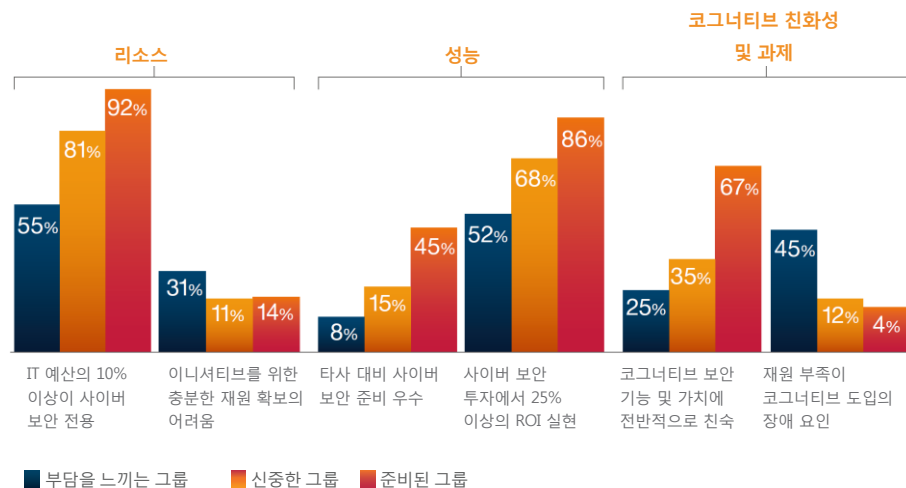
“현재 많은 시간과 리소스가 투입되고 있는 방대한 보안 정보 및 지식을 효율적으로 수집, 체계화하고 상황 정보와 연계하는 지능형 코그너티브 솔루션과 함께 다음 단계를 시작할 준비가 되었습니다.”

캐나다 자산 관리 기업의 금융 보호 책임자

코그너티브 시대에 준비된 기업들

IBM은 현재 어떤 기업이 코그너티브 보안 시대에 진입할 준비가 되었는지 알아보고자 응답자가 스스로 평가한 보안 실효성 및 코그너티브에 대한 인식/준비 수준에 따라 응답자들을 프로파일링했습니다. 이들의 응답을 분석하여 뚜렷이 구별되는 세 그룹으로 분류했습니다(그림 6 참조).

그림 6 각자 평가한 준비 수준 : 부담을 느끼는 그룹, 신중한 그룹, 준비된 그룹.



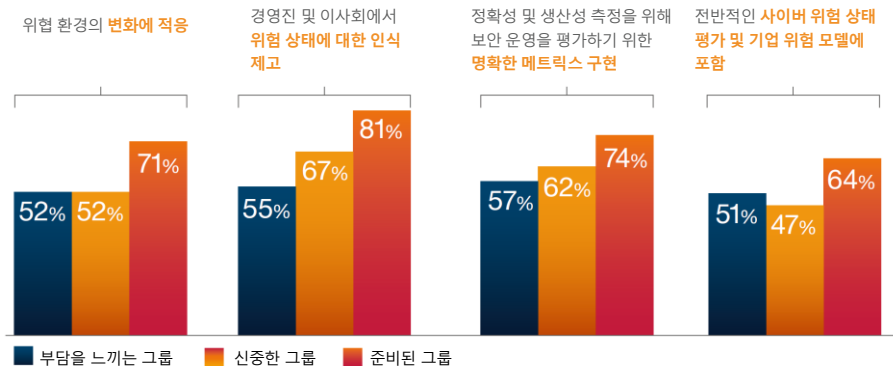
표본의 52%에 해당하는 '부담을 느끼는 그룹(The Pressured)'은 자금 및 인력 확보에 어려움이 있으며 코그너티브 보안 기능 및 가치에 대한 전반적인 인식이 낮은 편입니다. 대개 IT 예산 중 사이버 보안의 비중이 더 낮으며 충분한 자원 및 인력 확보와 관련된 어려움을 토로하는 경우가 많았습니다. 또한 코그너티브 도입의 장애물로 자원 부족을 지적했습니다(이 그룹을 분류하고 정의한 방법에 대해서는 20페이지의 “통계 및 방법론” 참조).

표본의 27%에 해당되는 '신중한 그룹(The Prudent)'은 부담을 느끼는 그룹과 같은 리소스 문제는 없지만, 아직 차세대 코그너티브 보안을 구현할 준비가 되지 않은 상태입니다.

표본의 22%에 해당하는 '준비된 그룹(The Primed)'은 코그너티브 보안 솔루션에 가장 정통하고 열정적인 그룹으로, 다른 그룹보다 코그너티브 보안에 익숙하고 자신 있으며 예산 및 ROI도 높습니다. 더 효과적으로 경영진 및 이사회에 보안 위험을 알리며 전사적 위험 모델에 사이버 위험 지수를 포함시킵니다(그림 7 참조).

그림 7

부담을 느끼는 그룹, 신중한 그룹, 준비된 그룹의 각기 다른 보안 프랙티스 접근 방식



“인간의 두뇌로는 매일 모든 것을 처리할 수 없을만큼 불필요한 데이터도 많습니다. AI 또는 코그너티브 기술의 도움이 필요합니다.”

Chad Holmes, Ernst & Young LLP 책임자(Principal) 겸 사이버 전략 기술 리더(CTO)

“대개는 보안 업무의 24/7 특성 때문에 인력 확보에서 재정적 어려움을 겪습니다. 여기서 코그네티브 기반 보안이 진가를 발휘합니다. 결코 잠들거나 지치지 않으니까요.”

Michael Pinch, 로체스터 대학교 최고 정보 보안 책임자

보안 리더는 코그네티브 보안 솔루션에 무엇을 기대하고 바랄까요? 준비된 그룹과의 대화를 통해 이들이 다음 사항을 원한다는 것을 알 수 있었습니다.

- 중단 없이 실행되면서 지속적인 지원 제공
- 오탐 감소, 행동의 이상 요소 파악
- 더 정확하게 위협 환경 이해, 사고에 대한 상황 정보 제공
- 업종, 지역, 규제 관련 요건에 따라 거버넌스, 위험 관리, 컴플라이언스 지원
- 보안 업무의 속성을 변화시켜, 분석가가 더 지능적으로 일하고 더 많은 가치를 제공할 수 있도록 지원

IBM 제언

IBM은 현재의 보안 환경을 면밀히 살펴보면서 보안 리더들을 압박하는 요인과 해결 과제, 주요 목표를 살펴보았습니다. 이번 조사 결과를 바탕으로 사이버 보안 시대에 대비하기 위한 방법을 제안합니다.

취약점 이해

보안 리더는 대응 능력을 강화하고 복잡성을 줄이길 원하며 보안 사고에 따른 기업의 이미지 실추를 점점 더 우려하고 있습니다. 가장 미흡하고 취약한 영역에 주목하고, 무엇이 우선 순위에 있는지 파악해야 합니다.

- 필요한 인텔리전스 및 위협 탐지 기능이 있는지
- 보안 사고 대응 및 해결 속도가 충분히 빠르는지
- 이벤트와 실제 사고를 구별하거나 정확한 상황 정보를 얻는 데 어려움이 있는지 등

보안 전문성 습득

코그니티브 보안 솔루션의 기능, 비용, 구현과 관련하여 잘못된 인식이 자리잡고 있을 수도 있기 때문에, 공식적인 학습 경로를 마련해야 합니다.

- 코그니티브 보안 솔루션의 잠재적 활용 사례를 알아보고 자사의 취약한 분야와 연결하여 의사결정 향상을 위한 더 유용한 증거가 필요한지 확인해야 합니다.
- 기업 내 이해 관계자들에게 코그니티브 보안 솔루션의 혜택과 설득 방법을 마련하고, 실무 팀과 경영진을 위한 교육 계획을 마련해야 합니다.

“코그니티브 보안은 엄청난 잠재력을 지니고 있습니다. 인력 부족으로 인한 공백을 해결하고 위험 요소를 줄이고 대응의 효율성을 높일 수 있습니다. 또한 코그니티브 기술로 사이버 보안 기술력의 문턱을 낮출 수 있습니다. IT 배경 지식이 없는 사람의 새로운 시각을 통해 문제 해결의 실마리를 찾는 것이 가능해집니다.”

David Shipley, New Brunswick 대학교 정보 기술 서비스 전략 이니셔티브 책임자

- 기업 내부에서 기술 도입에 걸림돌이 될 수 있는 기술력 간극을 파악하고 해결해 합니다.

투자 계획 수립

아직 시장에서 검증되지 않은 새로운 기술에 대한 투자의 타당성을 입증하기란 어렵습니다. 제시할 사례가 많지 않고 신뢰를 얻는 데 어려움이 생길 수 있습니다. 응답자의 대다수가 예산 확보 시 ROI 및 기타 재무 분석이 필요하다고 밝힌 만큼, 보안 리더는 코그네티브 보안 솔루션과 관련하여 기존과 다른 접근법을 구사해야 합니다.

- 코그네티브 보안 솔루션을 차별화된 영역으로 다루십시오. 기존의 보안 투자 타당성 조사 방식(예: 해결 비용)에만 의존해서는 안 됩니다. 그보다는 코그네티브 보안이 보안 운영의 전반적인 대응 능력을 높일 수 있는 기술이라는 사실에 초점을 맞춰야 합니다.
- 교육 계획을 개발하여 다른 경영진의 지지를 확보하고 투자 타당성 입증에 도움을 받는 데 활용해야 합니다.
- 코그네티브 보안에 투자함으로써, ROI 외에도 다른 비즈니스 가치를 얻을 수 있는지 구상해야 합니다.

현 준비 수준에서도 전문성 강화 모색

준비된 그룹(The Primed)은 넉넉한 리소스를 확보했고 자신의 역량에 대한 자신감이 높으며 당장 코그너티브 보안 솔루션을 구현할 준비가 되어 있지만, 그렇다고 해서 코그너티브 보안이 선택된 자들의 전유물은 아닙니다. 코그너티브 보안 솔루션은 새로운 기술 영역이며 그 고유성은 어떤 규모의 기업에서도 진가를 발휘할 수 있습니다.

- 부담을 느끼는 그룹: 코그너티브 보안 솔루션으로 개선할 수 있는 구체적인 비즈니스 지표 및 기술력 부족 문제를 정의하고 투자의 타당성을 입증해야 합니다.
- 신중한 그룹: 기술력 간극에 대한 우려를 해소하기 위해 양질의 정보 수집에 중점을 둬야 합니다.
- 준비된 그룹: 코그너티브 파일럿 구현을 위한 매우 구체적인 활용 사례를 선정해야 합니다.

추가 정보

이번 IBM 기업가치 연구소의 연구 조사에 대한 자세한 내용은 iibv@us.ibm.com에 문의하십시오. 트위터에서 @IBMIBV를 팔로우하실 수 있습니다. IBM 기업가치 연구소의 전체 연구 카탈로그가 필요하거나 월간 뉴스레터를 구독하려면 ibm.com/iibv를 방문하십시오.

앱스토어에서 무료 "IBM IBV" 스마트폰 또는 태블릿 앱을 다운로드하여 모바일 기기에서 IBM 기업가치 연구소 Executive Report를 이용하십시오.

변화하는 세상에서 최고의 파트너

IBM은 고객과 긴밀하게 협업하면서 비즈니스 인사이트, 전문 연구와 기술을 접목시켜 시시각각 변화하는 오늘날의 환경에서 고객이 차별화된 이점을 확보할 수 있도록 지원합니다.

IBM 기업가치 연구소

IBM 글로벌 비즈니스 서비스는 IBM 기업가치 연구소를 통해 공공 및 민간 분야의 주요 쟁점에 대해 사실 기반의 전략적 인사이트를 개발하여 기업의 최고경영진에게 제공하고 있습니다.

연구 참여자

Lisa van Deth, IBM Security 캠페인 및 Thought Leadership 전략 프로그램 마케팅 매니저
 Christophe Veltsos, 맨카토 미네소타주립대 컴퓨터 정보 과학부 부교수

도움 주신 분들

Caleb Barlow, IBM Security WW 포트폴리오 마케팅 부사장
 Maria Battaglia, IBM Security 레질리언스 CMO
 Wangui McKelvey, IBM Security 보안 서비스 및 웹 사기 대응 포트폴리오 마케팅 책임자
 Kevin Skapinetz, IBM Security 전략 책임자
 Oxford Economics – 설문 조사 데이터 수집 관리 지원

참고 및 출처

- 1 "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute. 2016년 6월. <http://www-03.ibm.com/security/data-breach/>
- 2 Friedman, Gabe. "JPMorgan Chase Atty: Bank Will Spend \$500M on Cyber Security." 2016년 1월 29일. <https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/>. 2016년 9월 21일 액세스
- 3 Kelley, Diana, Carl Nordman. "Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite." IBM 기업가치 연구소 2016년 ibm.biz/csuitesecurity

통계 및 방법론

IBM 기업가치 연구소(IBV)와 Oxford Economics는 기업이 어떤 보안 과제에 어떻게 대응하고 코그니티브 보안 솔루션과 그 잠재력을 어떻게 평가하고 있는지 자세히 알아보기 위해 2016년 5월 ~ 7월에 35개국, 18개 업종을 대표하는 CISO 및 기타 보안 전문가 700명으로 이루어진 균형 분포 그룹을 대상으로 설문 조사를 실시했습니다.

준비된 그룹(The Primed), 신중한 그룹(The Prudent), 부담을 느끼는 그룹(The Pressured)의 분류에는 k-means 클러스터링 알고리즘을 적용하여 뚜렷이 구별되는 3가지 행동 패턴을 밝혀냈습니다. 이 행동 패턴은 보안 실효성, 코그니티브 이해, 코그니티브 대비와 관련된 문항을 토대로 했습니다.

저자 소개

Diana Kelley는 IBM Security의 총괄 보안 자문(Executive Security Advisor, ESA)이자 IBM Security Newsroom 관리자입니다. 그녀는 25년 넘게 IT 보안 분야에서 쌓은 경험을 바탕으로 CISO 및 보안 전문가에게 조언하고 방향을 제시하면서 ESA의 직책을 수행하고 있습니다. 그녀는 IBM X-Force 보고서에 기고해 왔으며 Security Intelligence 블로그에서도 사고의 리더십 기사를 자주 게재하고 있습니다. IANS Research 교수진의 일원으로 활동 중이며 InfoSec World 자문 위원회 및 Executive Women's Forum 컨텐츠 위원회에서도 일하고 있습니다. Diana는 각종 보안 컨퍼런스에 자주 연사로 참여하며 The New York Times, TIME, MSNBC.com, Information Security 매거진, The Wall Street Journal에서도 보안 전문가로 인용되고 있습니다. 그녀는 Cryptographic Libraries for Developers의 공동 저자입니다. 연락처는 drkelley@us.ibm.com입니다.

Vijay Dheap은 IBM Security 사업부의 프로그램 책임자로서 새로운 기술의 상용화를 전문적으로 다루고 있습니다. 현재는 첨단 분석, 코그너티브 및 SaaS를 포괄하는 보안 인텔리전스 솔루션 포트폴리오를 이끌고 있습니다. 이전에는 사이버 포렌직 및 모바일 보안 비즈니스의 리더로 활동했습니다. Vijay는 진정한 테크놀로지스트로서 IBM Master Inventor 직책을 갖고 있습니다. 그가 취득한 특허 포트폴리오는 모바일, 엔터프라이즈 협업, 보안 혁신을 망라합니다. Duke Fuqua 경영대학원에서 국제 MBA를, 캐나다 워털루 대학교에서 컴퓨터 공학 석사 학위를 취득했습니다. 연락처는 vdheap@us.ibm.com입니다.

David Jarvis는 IBM 기업가치 연구소의 보안 및 CIO 리더입니다. 이 분야에서 새로운 비즈니스 및 기술 주제를 탐구하는 의제 개발 및 이행을 맡고 있습니다. 그는 마켓 인사이트, 사고의 리더십, 전략적 예측 프로젝트의 개발 및 관리에 열정을 갖고 있는 전문가로서 IBM에서 이와 관련된 여러 보직을 맡고 있습니다. 그는 2012- 2014 IBM CISO Assessments를 포함한 수많은 사이버 보안 사고의 리더십 보고서에 저자로 참여했습니다. David는 연구 활동 외에도 비즈니스 인사이트 및 창의적 문제 해결에 대한 교육도 맡고 있습니다. 연락처는 djarvis@us.ibm.com입니다.

Carl Nordman은 IBM 기업가치 연구소 최고경영진 연구 프로그램의 글로벌 책임자이자 CFO 리서치 리더입니다. 그는 두 분야의 1차 연구를 책임지고 있습니다. 최신 전략적 이슈에 대한 동향 및 관점을 규명하는 연구를 지휘합니다. Carl은 금융 위험 및 사기 전문가로 25년 넘게 일했습니다. 이전에는 IBM Consulting Services에 몸담고 있으면서 Fortune 1000 대 기업의 CFO를 위한 프로젝트를 수행했고 여러 고객을 위해 Finance and Accounting BPO 서비스의 거래처 담당 임원으로 일한 바 있습니다. 연락처는 carl.nordman@us.ibm.com입니다.

© Copyright IBM Corporation 2016

Route 100
Somers, NY 10589
Produced in the United States of America
2016 12월

IBM, IBM 로고 및 ibm.com은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보" (www.ibm.com/legal/copytrade.shtml)에 있습니다.

이 문서는 최초 발행일을 기준으로 하며, 통지 없이 언제든지 변경될 수 있습니다. IBM이 영업하는 모든 국가에서 모든 오퍼링이 제공되는 것은 아닙니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증 및 타인의 권리 침해에 대한 보증이나 조건을 포함하여(단, 이에 한하지 않음) 명시적이든 묵시적이든 일체의 보증 없이 "현상대로" 제공됩니다. IBM 제품에 대한 보증은 제품의 준거 계약 조항에 의거하여 제공됩니다.

이 보고서는 일반 지침으로만 제공됩니다. 세부적인 연구나 전문가 의견의 예제를 대체할 수 없습니다. IBM은 본 문서에 의존한 개인 또는 조직에 발생한 어떠한 손해에 대하여도 책임을 지지 않습니다.

이 보고서의 데이터는 제3자가 출처일 수 있으며, IBM은 별도로 이러한 데이터를 확인, 검증 또는 감사하지 않습니다. 이러한 데이터의 사용으로 인한 결과는 "현상대로" 제공되며 IBM은 명시적이거나 묵시적인 일체의 진술이나 보증을 제공하지 않습니다.



재활용하십시오.

