CONCERT FORECAST 2019

기업 정보보호 이슈 전망

(사)한국침해사고대응팀협의회

CONCERT의 한 해 사업은 '기업 정보보호 이슈 전망 보고서'와 함께 시작된다. CONCERT 정회원사를 대상으로 하는 몇 안되는 질문 –올해는 4개다- 이 설문조사의 전부다. 정보보호 부서의 올해 사업계획, 정보보호 담당자로서 가지고 있는 고민, 신규인력에게 기대하는 바, 올해 유행할 것으로 예상하는 솔루션 등 4개의 질문에 대한 응답만으로 또 한 권의 보고서가 만들어졌다. 각각의 질문에 내포된 의미가 다르기 때문에 보고서 역시 해당 질문에 따라 섹션을 구분해 작성했다.

'계획' 파트에서는 사업계획에서 드러난 큰 움직임에 대한 그림을 담았고, '고민' 파트에서는 아직 해법을 찾지 못하고 고민하고 있는 내용에 대한 파악을, '결핍' 파트에서는 현재 조직 내에서 가장 시급하게 강화되어야 하는 부분에 대한 인식을, '전망' 파트에서는 정보보호 수요자 입장에서 바라보는 정보보호 솔루션 전망을 각각 다뤘다.

주관식 응답을 정리하는 것 만으로도 어느 정도 흐름이 보이기도 하지만, 상세 내용 파악을 위해 응답한 담당자와 추가 인터뷰를 하는 와중에 설문응답만으로는 보이지 않았던 맥락이 보이는 경우도 있다. 올해 응답에서는 모든 응답을 관통하는 하나의 키워드가 있었으니, 자동화로 대표되는 "효율화"가 그것이다. 위협은 고도화되고, 관리해야 할 통제범위는 넓어지고, 인력은 여전히 부족한데다 주52시간 근무제 시행으로 인력운용의 심리적 탄력성까지 떨어진 이 상황에서 취할 수 있는 액션은 뭘까. 자동화시킬 수 있는 부분은 최대한 자동화 시키고, 모든 것을 다 통제하겠다는 욕심을 버리고 전체적인 관점에서 할 수 있는 것을 제대로 하겠다는 움직임이다.

CONCERT 정회원사의 업종이 다양하고 처한 상황이 다르기 때문에 각 회사의 답변이 상당히 넓게 분포되었지만, 그 중에서 두드러지게 나타난 것들을 화두로 삼아 현황과 전망을 제시했다. 보고서를 읽는 와중에 고민에 대한 해결의 실마리가 떠오른다거나 특정 주제에 대해 심도 깊은 토의, 또는 함께 고민할 누군가가 필요하다 싶으면 언제든지 사무국으로 연락주시라. 사무국은 그것을 위한 시간이자 공간이니까.

심상현 | 한국침해사고대응팀협의회 사무국장

Part Ⅰ. 계 획

Part Ⅰ 1 "EDR, 이제 들여놓을 준비가 되셨습니까?"

EDR(Endpoint Detection & Response)

정보보호 솔루션에도 유행이라는 것이 존재한다. 도입기-성장기-성숙기-쇠퇴기의 라이프사이클을 따르는데, 솔루션마다 그 속도가 다르기는 해도 유행하는 솔루션은 짧게는 1년, 길게는 3~4년의 간격으로 달라지는 것이 보통이다. 지난해에 이어 올해도 CONCERT 정회원사에서 도입계획이 가장 많은 솔루션으로 EDR(Endpoint Detection & Response)이 꼽혔다. EDR은 엔드포인트에서 일어나는 여러 위협을 지속적으로 탐지하고 빠르게 대응할 수 있는 '보안위협 탐지-분석-대응' 솔루션이다. ICBM으로 대표되는 IoT, Cloud, Mobile 등 여러 플랫폼에서 등장하는 알려지지 않은 보안 위협과 고도화된 APT 공격을 효과적으로 막기 위해서는 엔드포인트단에서의 빠른 탐지와 대응이 중요하다는 공감대가 낳은 솔루션인 것이다.

대부분의 공격은 엔드포인트에서 악성코드를 통해 시작되기 때문에 엔드포인트를 모니터링하는 것은 분명 유효한 전략이다. 엔드포인트 영역에서 백신(AV), 패치 관리(PMS), 매체 제어(Device Control), 네트워크접근제어(NAC) 등의 보안 제품이 동작하고 있지만, 이들의 탐지를 회피하는 기술은 계속 진화를 거듭해왔다. 네트워크 영역에도 방화벽(Firewall), 침입방지시스템(IPS), DDoS 방어시스템, 웹 방화벽(WAF) 등이 있지만 이들 네트워크 보안 장비는 접속이 허용된 IP, 프로토콜, 앱으로부터의 악성코드 차단에 어려움을 안고 있다.

EDR이라고 해서 다 같은 솔루션이 아니다. EDR 단독으로 적용되기 보다는 타 솔루션과 연계해서 적용되는 경우가 많으며, 그 출발점에 따라 EPP(Endpoint Protection Platform)기반 EDR, AV기반 EDR 등으로 구분할 수 있다. 대부분의 EDR 솔루션은 위협 점수와 보고서를 통해 정보를 제공해주지만, 그렇기 때문에 EDR 솔루션 운영에는 수많은 데이터를 보고 판단할 수 있는 시간과 인적자원이 필수적이다.

AV는 알려진 공격이나 이미 등록된 시그니처와 유사한 공격 패턴을 차단할 수 있지만, 파일리스 공격을 탐지하는데는 한계가 있는 반면, EDR은 엔드포인트에 설치된 에이전트에서 관찰하고 정리된 데이터를 서버로 보내 서버에서 자신의 DB와 비교하여 탐지를 수행하며 DB에 없는 경우 AI 기반의 인텔리전스 플랫폼을 통해 위협 여부를 판단하도록 하는 방식으로 알려지지 않은 은밀한 공격을 탐지하는데 탁월한 것으로 기대를 모으고 있다.

허나, 어느 솔루션이나 그렇겠지만 그것의 도입만으로 문제가 해결되는 경우는 거의 없다. 오히려 충분한 준비없이 도입해서 더 문제가 되는 경우도 자주 발생한다. "엔드포인트에 대한 가시성만 확보되면 어떤 위협이 있는지 한 눈에 볼 수 있으니 우선순위를 정해서 대응하기 편해질 줄

알았어요. 그런데 과유불급이라고 하나요. TMI(Too Much Information)라 할까요. 엔드포인트에 대한 이벤트가 너무 많이 쏟아져서 감당이 안되더라고요. 우선순위가 낮은 이벤트는 예외처리로 돌려서 겨우 숨을 돌릴 수 있었는데, 몰랐다면 모를까, 알고도 무시하는게 너무 찜찜했습니다"라는 한 보안담당자의 토로를 듣는데 왜 뜬금없이 쇼펜하우어가 생각났을까. "좋은 책을 사는 것은 그것을 읽기 위한 시간도 같이 사는 것이다."

Part I 2 "어차피 이 싸움은 기술 아닌 인식의 싸움이었다" 클라우드

클라우드가 고민의 영역에서 계획의 영역으로 넘어왔다. 그만큼 저변이 확산됐고, 환경이 갖추어졌다는 뜻이다. 재작년 조사 때까지만 해도, 클라우드 서비스 제공자(CSP)를 무작정 믿어야 한다는 것에 부담을 표시한 곳이 많았는데, 그 동안 클라우드 보안인증제도도 시행되었고, AWS 서울 리전이 ISMS 인증을 받으면서 클라우드로의 전환 여건과 레퍼런스가 많이 축적되어 더 이상 First Mover의 이미지가 아니게 된 것도 중요한 한 계단이 된 것 같다. 이런 분위기 속에서 공공기관에도 클라우드 사용이 허용됐고, 올해부터는 금융사의 정보시스템도 클라우드 서비스를 이용할 수 있게 됐다.

예전에는 클라우드 인프라에 대한 정보가 부족하다보니 클라우드 데이터 보호와 컴플라이언스 관리를 클라우드 서비스 제공자들이 해줄 것이라고 기대하는 목소리가 있기도 했지만, 이제 클라우드 서비스의 보안 책임에 관한 부분은 '책임 공유'라는 형태로 상당부분 정리가 됐다. 물리적인 클라우드 환경과 서비스형 인프라(IaaS)를 위해 제공하는 기반에 대한 부분은 클라우드 서비스 제공자가 책임지지만 가상머신 및 운영체제(OS)부터는 고객사의 책임으로 분담이 된 것이다. 따라서 클라우드 자체에 대한 보안은 클라우드 서비스 제공자가, 클라우드에 올라간 서버와 데이터에 대한 보안은 고객사가 책임을 지는 것이다. 여기에 클라우드 보안인증을 통해 클라우드 서비스 제공자가 고객사의 동의 없이 고객사의 가상환경, 서버, 데이터에 임의로 접근하지 않도록 강제한 것도 고객사의 불안감을 지우는데 큰 부분을 차지했다. 또한 클라우드 인프라에 대해 고객사가 가시성을 가지기 어려운 부분도 클라우드로의 전환을 주저하게 만드는 걸림돌이었는데 클라우드접근보안중개(CASB) 솔루션이 등장하면서 클라우드 사용 가시성 확보와 데이터 보호를 수행할 수 있는 환경을 제공하게 됐다.

작년에 있었던 AWS 한국리전 장애의 여파인지, 인터뷰 과정에서 멀티 클라우드 사용을 검토하고 있다는 곳이 여럿 있었다. 서비스 가용성을 하나의 클라우드 사업자에만 맡기기에는 불안하기도 하고, 특정 클라우드에 종속되기 싫어하는 부분도 있어 멀티 클라우드를 사용할 예정이라는 한 회원사의 담당자는 "각 CSP가 제공하는 클라우드 서비스가 엇비슷해 보여도 가시성 부분이나 제공하는 보안 서비스 부분에서 차이가 있어 온프레미스 환경처럼 각 클라우드에 보안정책을 동

일하게 가져갈 수 없는 부분이 걱정이다. 하지만 서비스 장애가 나면 손실은 직접적인데 반해, 보상은 장애시간만큼의 클라우드 서비스 이용요금 보상수준에 그치기 때문에 서비스의 가용성을 생각하면 멀티 클라우드를 생각하지 않을 수 없다."며 "보장하는 서비스 가용성 SLA 수준이 IDC 이용 시보다 올라가긴 했지만, 장애에 대한 대비를 고객사에게 전가하는 것이 맞는 것인지 모르겠다."라고 볼멘소리를 했다.

어쨌거나, 우리나라에서의 클라우드 전환은 기술의 싸움이라기 보다는 인식의 싸움이었다. 클라우드로 전환했을 때의 세세한 기술적 이슈보다 더 큰 장벽은 "써도 되나?" 또는 "다른 회사들 쓰고 있대?"와 같은 다소 막연한 인식의 장벽이었다. 이와 같은 장벽들이 서서히 허물어져 가고 있는 지금을 바라보면, 보안업계에 몸담고 있는 한 사람으로서 다음의 고민은 클라우드를 기반으로 한 다양한 보안 솔루션, 서비스들이 확대될 크나큰 시장에서 국내 전문업체들의 경쟁력에 관한 것이 되지 않을까. 지금까지와는 궤를 달리 하는 싸움. 건투를 빌 수밖에.

Part I 3 "보이지 않는 것을 보이게 하기" 통합로그관리/모니터링

각종 정보보호 시스템에서 생성된 로그는 시스템 또는 애플리케이션의 장애/침해 징후를 파악하는 데 유용한 정보를 포함하고 있다. 매일 수많은 보안 이벤트가 발생하기 때문에 분석해야 할 정보 또한 늘어나고 있는 만큼, 보안 데이터에 대한 통합 분석, 빅데이터 분석은 지능화되고 급증하고 있는 보안 위협에 맞서 기업의 보안성을 높이기 위한 필수 요건이 되고 있다.

이미 UTM, SIEM을 필두로 통합 로그/위협관리를 도와주는 솔루션이 나온지 오래 됐지만, 기술이 발달하고 스토리지 가격이 내려가면서 보다 더 많은 정보를 한 곳에 부어 넣고 빅데이터 분석기술을 이용해 위험 예측과 고급 분석 기법과 고급 통계 기법을 통해 지금까지는 보이지 않던 특이사항을 보고 싶어 하는 움직임이다.

조직 경계 내·외부를 막론하고 인증받기 전까지는 누구도 믿으면 안된다는 제로 트러스트 정책의 출현과 데이터를 정형·비정형을 가리지 않고 무작정 가두어 놓는 데이터레이크(Data Lake) 개념의 도입으로 지금까지의 데이터 분석과는 한 단계 달라진 모습을 사용자들은 원하고 있다. 빅데이터 분석의 목표가 가능한 한 긴 시간 동안 취합한 많은 소스로부터 데이터를 취합해 유의미한 통계를 도출해 내는 것이지만, 분석 비용이 데이터량에 비례해 또는 그 이상의 비율로 증가한다면 분석의 효용성이 떨어지게 된다. 스토리지 비용 자체는 예전에 비해 많이 내려갔지만, 상용 빅데이터 분석 솔루션의 스토리지에 대한 라이센스 비용은 무시할 수 없는 수준이다. 따라서 상용 솔루션에 비해 성능 면에서는 조금 부족하지만 오픈소스로 활용할 수 있는 빅데이터 로그분석 솔루션에 대한 관심도 커지고 있다.

ELK(ElasticSearch<분석,저장> + Logstash<수집> + Kibana<시각화>) 또는 ELK Stack으로 대표되는 오픈소스 로그 및 데이터 분석 엔진을 사용하여 구축하는 케이스도 늘어나고 있다. 이미 SIEM을 가지고 있는 경우에도, SIEM의 데이터를 ElasticSearch 엔진에서 가져와 분석하기도 하고, SIEM은 SIEM대로 분석을 하게 하고 Beats와 Logstash를 활용해 보안장비로부터 직접 로그를 가져와서 ElasticSearch 엔진에서 새로 분석하기도 한다. 벤더의 손을 빌리지 않고 SIEM의 대시보드를 직접 수정하는 것은 굉장히 어렵지만, ELK에서는 Kibana를 통해 대시보드를 쉽게 만들 수 있기 때문에 원하는 통계를 정확하고 빠르게 확인하는 것이 가능하게 됐다.

"모니터링 대상이 되는 시스템과 구조를 파악하고 있어야 각 시스템에서 생성된 로그간의 상관관계를 뽑아낼 수 있습니다. 솔루션 벤더들이 다양한 사례에 대한 구축경험은 많을지 모르지만 우리 환경에 딱 들어맞는 경험은 없지 않을까요? 누가 봐도 알 수 있는 보안위협은 물론이고, 숨어있는 보안위협까지 식별하기 위해서는 우리 환경을 잘 알아야 적합한 시나리오를 만들 수 있다고 생각합니다."고 말하던 담당자는 "예전에는 하고 싶어도 할 수가 없던 일인데, 이제 할 수 있는 환경은 갖춰졌네요. 어찌어찌 올해 사업계획에 반영도 했구요. 그런데 실제로 어떤 효과가 있고, 어떤 평가를 받게 될지 기대 반, 걱정 반 입니다." 목소리가 살짝 흔들린다고 느낀 건 기분 탓일까.

ESM과 보안관제가 막 꽃을 피우던 시절. ESM은 보안담당자 옆을 지나가던 사장님이 "보안팀은 하는 일이 뭔가?"라고 물었을 때 자신이 하고 있는 일을 시각화해 손가락으로 가리킬 수 있게 만드는 혁혁한 성과를 이루어낸 바 있다. 아주 먼 옛날의 일처럼 생각될 수도 있겠다. 하지만 예나 지금이나 모든 보안담당자들의 화두는 보이지 않는 것을 보이게 하는 것에 있다는 사실에는 변함이 없다. 단지 지금은 손가락으로 화면을 가리키는 것보다 훨씬 더 많은 일을 해야할 뿐.

Part Ⅱ. 고 민

Part Ⅱ 1 "조령모개(朝令暮改), 어찌하오리까" 컴플라이언스

기업 입장에서 컴플라이언스는 선택의 문제가 아니라 무조건 준수해야 하는 법적 의무에 해당한다. 처벌조항의 유무, 처벌수위의 높고 낮음과 상관없이 법을 어겼다는 사실 하나만으로 기업 이미지에 미치는 영향이 크기 때문이다. 따라서 기업들은 법령 개정내용에 많은 관심을 가질 수밖에 없다.

2018년 한 해 동안 국회에 제출된 정보통신망법 개정안은 62건이나 되고, 개인정보보호법 개

정안은 17건에 달한다. 정보통신망법은 일주일에 하나, 개인정보보호법은 한달에 하나 꼴로 적지 않은 숫자의 법률개정안이다. 물론 제출된 법안이 모두 통과되는 것은 아니고 상임위원회, 법제사법위원회, 본회의 등을 거치면서 여러 법안이 하나로 병합되어 처리되거나 국회의원 임기까지 처리되지 않은 법안은 자동 폐기된다. 법안이 통과되면 그 내용에 따라 공포되는 즉시 시행되는 법안도 있고, 구체적인 기준을 시행령에 위임하거나, 기업에서 법안의 내용을 준수하기 위해 시간이 필요한 경우에는 일정 기간의 유예기간을 부칙에 명시하기도 한다.

그런데 법이 정해지고(입법) 시행되는(행정)과정에서 기업이 준비할 충분한 시간이 보장되지 않는 경우가 많다. 2018년 6월에 개정된 정보통신망법의 경우에도 개정법률의 시행시점은 공포시점으로부터 6개월 이후인 2018년 12월이었지만, 손해배상책임의 이행을 위한 보험가입 등 피해구제방법 의무 확보 조항과 CISO 임원급 의무지정 및 타 직무와 겸직을 금지하는 조항은 시행일자를 법률 공포 후 1년이 되는 2019년 6월에 시행하는 것으로 결정된 바 있다. 그런데, 1년 동안의 유예기간 동안 기업이 준비할 시간은 충분할까? 안타깝게도 그 대답은 전혀 그렇지 않다. 법이 공포된지 6개월이 지났지만, 보고서를 작성중인 지금 시점까지도 구체적인 기준을 담은 시행령이 아직 발표되지 않았다. 행정부처의 어려움도 짐작이 간다. 해당 조항은 모든 기업에 일률적으로 적용되는 조항이 아니라, 시행령에서 지정하는 특정 조건에 해당하는 기업에 한해 적용되는 법 조항이기 때문에 시행령의 해당 조건이 어떻게 정해지느냐에 따라 적용대상에 포함되는 기업의 숫자가 크게 달라진다. 정책의 효과와 기업의 부담을 잘 살펴서 최적의 기준점을 도출하는 것은 정말 중요한 일이지만, 너무 심사숙고하면 기업이 준비할 시간이 부족해 진다는 점을 잊어서는 안된다. 물론 잊지 않고 있겠지만 말이다.

인터뷰 중 "임원급 CISO가 하늘에서 떨어지는 것도 아니고, 기업에서는 미리 준비해야 하는데, 우리 회사가 CISO 겸직금지 대상에 들어가는지 여부도 모르겠고, CPO 업무와 겸직하는 것이 허용되는지도 모르겠다"면서 "기업에서 임원의 숫자는 민감한 사항인데, 시행시기가 다 되어가도록 아무런 지침이 없는 것을 보면 정부가 정보보호의 중요성을 강조한다기 보다는 오히려 그 반대인 것 같은 기분이다."고 말한 응답자도 있었다.

정보보호 컴플라이언스가 갈수록 강화되어 가는 것도 기업 입장에서는 반갑지 않지만, 가장 무서운 것은 정책의 불확실성이다. 믿고 따를 수 있는 정책을 기대해본다. 언제나 기대는 무료니까.

Part Ⅱ 2 "효율과 보안 그 지루한 줄다리기" 인력부족

300인 이상 사업장의 주 52시간 근무가 지난해 7월부터 시행됐고, 올해 1월부터는 50인 이

상 사업장까지 확대됐다. 기존에도 정보보호 조직은 항상 인력부족에 시달리고 있었는데, 이제는 연장근로로도 어찌할 수 없는 상황이 벌어진 것이다. 언제고 보안인력이 충분한 적은 없었지만, 적은 인원으로 어떻게든 끌고가야만 한다. 내부정보 유출에 대한 우려로 이전보다 정보보호 통제가 강화되어 위험 요소에 대한 전사 정책을 차단으로 설정하고 보안담당자가 선별적으로 허용하는 경우 수작업 처리 업무량이 증가한다. 강력한 보안조치와 기업의 업무 생산성 간의 간극을 어떻게 메울것인가 하는 질문은 해묵은 것임에도 아직 명쾌한 해법이 나오지 못하고 있다.

정보보호가 중요하다는 전제에 대해서는 대부분의 구성원이 동의하고 있고, 정보보호 예산도 이전과 비교하면 많이 늘어난 상황이지만, 정보보호 부서에 대한 반감은 그리 많이 줄어든 것 같지 않다. 아무래도 '안돼요', '하지마세요' 등 부정적인 메시지가 많고 요구하는 사항들이 일을 하는데 불편하게 하기 때문으로 보이는데, 내부의 적을 줄일 수 있는 방법은 없는 것일까. 여기 하나의 사례가 있다.

보통 클린데스크로 대표되는 사무실 보안은 어느 기업에서나 정보보호 활동의 기본으로 여겨지는데, 인터뷰 중 더 이상 클린데스크를 시행하지 않는다는 회원사는 "매번 남들 다 퇴근한 시간에 책상 위 서류방치, 서랍 시건 점검하는데 들어가는 자원이 너무 아까웠어요. 습관을 들이는 효과는 있겠지만, 실제 정보유출을 막는 데 얼마나 효과가 있을지 의문이 들었죠. 그래서 사무실 출입통제와 외부로의 트래픽에 대한 모니터링을 더 강화하고 클린데스크는 더 이상 시행하지 않아요."라고 이유를 밝히며 "막는다고 다 막아지는게 아닌데 언제까지 막기만 할 것인지에 대한 근본적인 질문을 했어요. 가용자원에 한계가 있는 상황에서 사전통제를 고집하기 보다는 사후 모니터링으로 전환하기로 한거죠. 물론 임직원은 어떤 정보를 어떻게 들여다보고 있는지를 모른다는 정보의 비대칭성 때문에 스스로 조심하고 있구요. 모니터링 적발 사례가 나오기 시작하면서 효과는 더 커졌다고 봅니다."고 의견을 피력했다.

Part Ⅲ. 결 핍

Part Ⅲ "잘안다. 잘한다. 자란다~!!" 개발능력

지금 정보보호조직에 신규인원이 충원된다면 해당 인력이 보유하기를 바라는 능력에 대한 설문도 진행했다. 현재 상태에서 조직 내부에서 가장 필요로 하는 능력을 조사할 수 있는 질문으로 설계했는데, 올해 응답에서는 개발능력이 압도적으로 많이 나왔다. 예년의 조사결과를 보면 정보보호 분야에 대한 전문지식을 최우선적으로 꼽았는데, 올해는 그 양상이 다르게 나타난 것이다. 개발능력이라고 해서 대단한 깊이를 요구하는 것은 아니고 DB에 대한 기본적인 지식과 웹 개발

능력, 매크로 등을 활용한 약간의 업무자동화 능력 정도로 나타났다. 딱 대시보드를 직접 만들어서 보고 싶은 것만 볼 수 있도록 구현하는 정도라고 할까... 현재의 솔루션 만으로 채워지지 않는 부분을 직접적인 화면 개발을 통해 해결하려는 모습이 보였다.

그 밖에 하둡, ElasticSearch 같은 빅데이터 처리·분석능력, 클라우드 환경과 보안 아키텍쳐에 대한 이해 능력, 로그분석 능력 등의 전문지식을 원하는 응답도 많았다.

기업에서 지출하는 보이지 않는 비용 중 커뮤니케이션 비용은 큰 편에 속한다. 한 사람만 건너가도 전달되는 메시지가 얼마나 달라지는지 구체적인 수치를 제시하지 않아도 다들 이미 몸으로 체감하고 있으리라. 커뮤니케이션 비용을 줄이는 방법에는 여러 가지가 있을 수 있지만, 가장 확실한 방법은 커뮤니케이션 단계를 줄이는 것이다. 내부 개발부서의 손을 빌리지 않고 직접 개발한다던지, 타 부서의 협조를 얻거나 외주로 진행할 때에 담당자가 해당 분야 내용에 대해 충분한 지식을 가진 상태로 서로 간의 커뮤니케이션 비용을 줄이는 것이 그러한 방법 중 하나인 것이다.

개발이라는 것 역시 컴퓨팅 머신과 함께 하는 커뮤니케이션에 속한다. 단지 컴퓨팅 머신이 인간의 언어를 몰라 머신의 언어로 소통할 뿐. 상호간에 소통이 될 수 있는 언어를 공부해야 하는 것은 인간과 컴퓨팅 머신 사이에서만 있어야 할 일은 아니다. 보안부서와 그 외의 부서들 사이, 그리고 특히 보안부서와 경영진 사이에서는 더욱 공을 들여야 할 일이다. 그래서 보안부서의 장, 또는 CISO가 반드시 갖춰야 할 능력 중의 하나가 Translation 능력이라고, 필자는 믿는다.

Part IV. 올해 HOT 할 솔루션

Part IV "이거 하나면 다 된다면서?" AI/머신러닝을 적용한 솔루션

자동화의 끝은 어디인가? 데이터만 충분히 제공되고 빅데이터를 처리·분석할 수 있는 기반만 갖추어지면 AI를 통해 모든 위협을 파악하고 통제할 수 있다고 생각하는 경향이 있다. 영화 '마이너리티 리포트'가 현실화 되는 시기라면 몰라도 아직은 그럴 단계가 아니다. 현재 AI/머신러닝을 탑재한 보안 솔루션의 역할은 오탐률/정탐률 개선, 알려지지 않은 위협에 대한 대응력 향상, 보안 위협 데이터 분석 제공 정도로 사람의 역할을 부분적으로 지원하면서, **자동화를 통해 생산성을 높이는 정도의 수준이다.**

끝없이 등장하는 신종·변종 악성코드에 대해 대응하기 위해 이미 많은 개별 솔루션들이 가동되고 있지만 종합적인 가시성을 보여주고 있지는 못하고 있다. AI와 머신러닝에 바라는 바는 단위

솔루션에서는 보이지 않던 공격의 흐름을, 방대한 데이터를 분석해 나온 인사이트를 통해 위협을 탐지하고 대응할 수 있도록 하는 것이다. 따라서 공격을 막는 것뿐 아니라 실제 침입이 발생한 경우 침해지점을 빨리 파악하고 신속히 대응해 피해를 줄일 수 있도록 하는 것이다.

하지만 AI와 머신러닝은 모든 문제를 해결해주는 전가의 보도가 아니며, 다른 정보보호 기술처럼 사용자의 관리가 필요한 하나의 정보보호 기술일 뿐이다(사실은 정보보호 기술도 아니지만). 새롭게 생성되는 수많은 변종 악성코드와 신종 위협을 걸러내고, 제한된 보안인력과 운영환경에서 쏟아지는 로그·이벤트 처리 작업같이 반복되는 일들을 AI 및 머신러닝 기술이 대체하는 것이다. 이를 통해 보안담당자는 보다 중요한 업무에 집중할 수 있게 되는 것이지, 해당 기술과 솔루션이 인력을 대체하는 것은 아니다.

또 한가지, AI와 머신러닝 기술을 채용한 보안 솔루션들에 대한 CONCERT 정회원사들의 기대를 보면서 다시 한번 생각해보게 되는 것은 국산 보안전문업체들의 미래다. AI와 머신러닝 기술은 보안을 위해 탄생한 기술이 아니다. 단지 보안에 접목했을 때 효용을 매우 높일 수 있는 기술일 뿐. AI와 머신러닝 기술을 가진 업체들 또한 보안시장에 대해 별로 아쉬울 게 없다. 해당 기술을 적용했을 때 훨씬 더 큰 부가가치를 만들어낼 수 있는, 보안보다 훨씬 더 큰 시장이 많기 때문. 반면, 보안업체들은 AI와 머신러닝이 아쉬운 입장이다. 그렇다면 우린 AI와 머신러닝이 그토록 절실한, 그 기술을 아쉬워하는 입장에서, 그렇게 적극적인 입장에서 접근하고 있을까. 잘 모르겠다.

<편집후기>

매년 첫 사업으로 진행하는 보고서지만, 매번 참 어려운 작업이다. 그런데 사무국이 실감하는 어려움보다 훨씬 더 큰 어려움을 CONCERT 정회원사들은 매일매일 겪는다. 한 해 사업계획이라는 어찌 보면 대외비에 해당한다고 볼 수도 있는 내용을 보내주는 CONCERT 정회원사에 큰 감사를 드린다. 간단하게 적은 답변의 배경을 알기 위한 추가 인터뷰는 덤이다. 쉽지 않은 내용을 공유해 주는 것은 CONCERT를 신뢰하기 때문에, 그리고 그 답변의 내용이 한 권의 보고서로 정리되어 CONCERT 정회원사를 비롯해 타 기업에도 도움이 된다는 믿음이 있기에 가능한 것이라고 생각한다. 업종에 따라, 환경에 따라 와닿는 화두도 있을 것이고, 그렇지 않는 주제들도 있을 것이다. 하지만 이 보고서를 통해 공동의 인식, 공동의 대응을 이끄는 작은 움직임이 되길 희망한다.

한 사람의 열 걸음보다, 열 사람의 한 걸음이 더 중요하다. 그것이 CONCERT가 존재하는 이유며 가치다.