

# 진화하는 사이버 침해

아시아 태평양 지역 연구 결과 개요

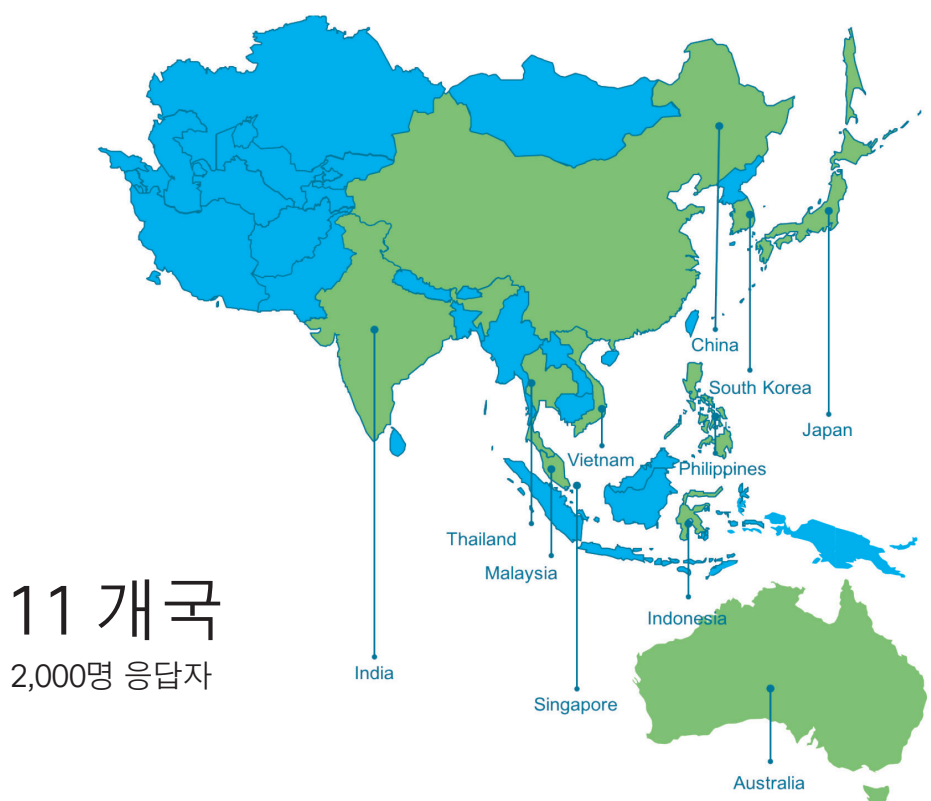
# 아태지역 분석 개요

보안은 아주 간단히 말하자면 숫자 게임입니다. 자금도 넉넉하고, 끈질기고, 가용 자원도 많은 공격자들은 네트워크에 침입할 수 있는 무한의 기회를 가지고 있으며, 그 중에 한 번만 성공하면 됩니다. 하지만 방어하는 입장에서는 모든 공격을 제대로 막아야만 침입을 막을 수 있습니다. 사이버 위협과 최신 공격 사례에 대한 이야기는 많습니다. 그래서 시스코의 보고서는 방어에 초점을 맞추려고 합니다. 사이버 공격이 있을 때 아태지역의 기업들은 과연 대비가 되어 있을까요? 사이버 공격의 영향은 무엇이며, 중요한 비즈니스 서비스를 얼마나 신속하게 복구할 수 있을까요?

## 진화하는 사이버 침해

아태지역 11개국의 2,000여 명의 응답자를 대상으로 한 보안 관행에 관한 조사 연구의 결과와 통찰을 제공하는 <시스코 2018 아태지역 보안 역량 벤치마크 보고서>에 의하면 기업이 극복해야 할 과제는 아직 많습니다. 조사 연구는 중국, 한국 및 일본, 싱가포르, 태국, 필리핀, 말레이시아, 베트남, 인도네시아, 인도, 호주로 진행되었습니다.\* 또한 이 데이터를 26개국 3,600여 명의 응답자를 대상으로 진행된 글로벌 벤치마크 연구 결과와 비교해 보았습니다.

다음은 아태지역의 기업이 직면하고 있는, 보안 공격 대비 상태, 원인, 도전 과제, 사이버 침해의 영향 그리고 다음 단계로 나아가기 위한 조건 등에 관한 핵심 요약입니다.



조직의 보안 상태에 대한 방어자의 인식을 알아보기 위해, 여러 국가에서 다양한 규모의 기업의 최고정보보안책임자(Chief Information Security Officer)와 보안운영(Security Operation) 관리자를 대상으로 보안 리소스 및 절차에 관해 질문했습니다.

<시스코 2018 아시아 태평양 보안 역량 벤치마크 보고서>를 통해 시스코는, 방어자가 해결해야 할 문제가 많다는 것을 확인했습니다. 아태지역 연구 결과는 글로벌 연구 결과와 비교했을 때 근소한 차이만 존재했습니다. 시장의 다양성을 고려할 때 이는 놀라운 결과는 아닙니다. 반면, 지역이 아닌 국가 단위의 데이터는 글로벌 연구 결과와 큰 차이를 보였습니다.

## ‘만약’이 아니라 ‘언제’의 문제: 사이버 공격의 영향

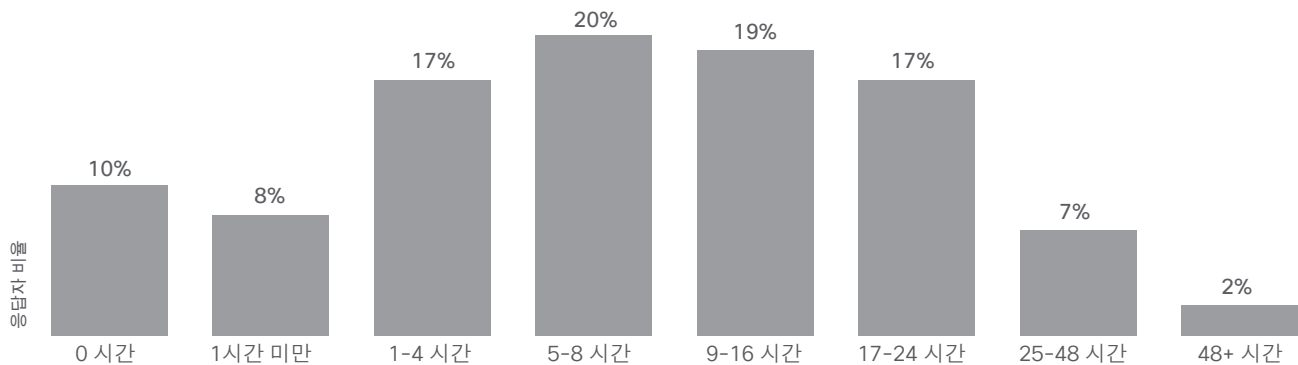
모든 사이버 공격의 1/3은 제3자에 의해 공개된다는 사실은 아태지역이나 글로벌 조사 결과 결과 사이에 큰 차이가 없습니다. 이 결과는 모든 기업에서 의식하고 대비해야 하는 부분입니다. 호주는 이 부문에서는 24%를 기록하여 가장 낮은 수치를 보였습니다.

아태지역 응답자의 41%는 사이버 침해가 발생하면, 운영 부문이 제일 큰 먼저 영향을 받는다고 답변했으며, 이는 글로벌 조사 수치와 비슷했습니다. 하지만 아태지역 연구에서 브랜드 평판에 대한 우려가 36%로 굳건히 2위를 차지한 반면, 글로벌 연구에서는 4위를 차지했습니다. 여

기에서 아태지역 기업들은 전반적으로 평판 하락을 다른 지역보다 중요시 여긴다는 사실을 알 수 있습니다.

운영 부문에 사이버 침해가 발생하면, 대다수의 아태지역의 방어자들은 최대 24시간 동안 시스템이 가동 중지되었다고 보고했으며, 이는 글로벌 조사 결과인 91%와 유사한 수치입니다. 그러나 아태지역 응답자의 절반만이 8시간 이내에 시스템이 복구되었다고 답했으나, 글로벌 조사에서는 8시간 이내에 55%가 서비스를 복구하는 것으로 나타났습니다.

그림 1 아태지역 지역에서 사이버 공격으로 인한 시스템 다운타임

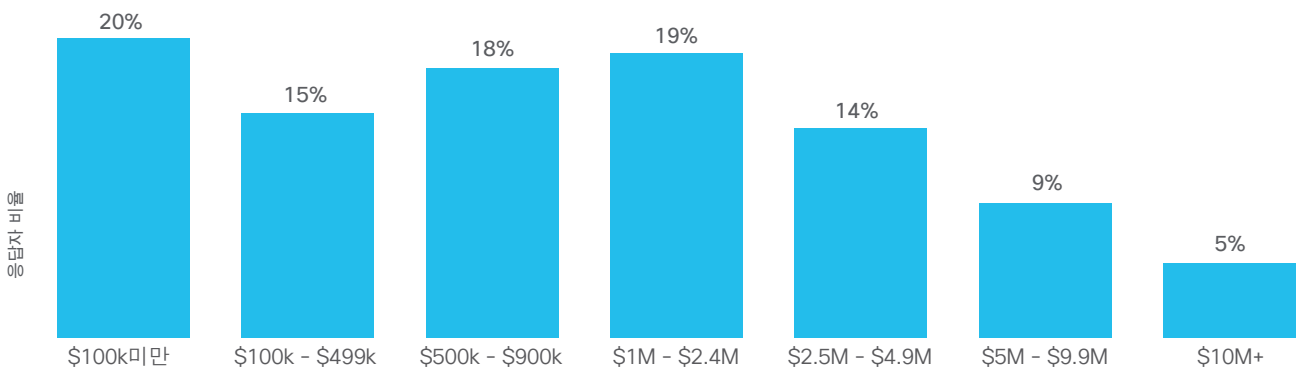


Q: 지난 1년 동안 가장 심각한 보안 공격을 떠올려 보십시오. 이로 인한 시스템 다운타임은 얼마입니까?

사이버 공격에 대한 두려움은 가상의 숫자가 아닌 실질적인 재무 비용에서 나타납니다. 사이버 침해는 조직에 실질적인 경제적 손실을 가져오며, 이를 해결하기 위해서는 몇 달 또는 몇 년이 걸릴 수 있습니다. 아태지역에서 사이버 공격으로 인해 발생하는 비용은 글로벌 조사 수치와 유사하거나, 높더라도 근소한 차이만 보입니다.

사이버 공격으로 인해 100만~500만 달러의 비용 손실이 발생한다고 응답한 비율은 아태지역이 33%, 글로벌이 30%였습니다. 1,000만 달러 이상의 재무적 손실이 발생한 경우는 호주에서는 9%인 반면 한국에서는 0%로 나타났습니다.

그림 2 아태지역에서 사이버 침해로 발생한 비용



Q: 작년에 발생한 모든 사이버 공격에서, 매출 손실, 고객 손실, 기회 손실, 비용 손실 등 모든 것을 고려한 경우, 사이버 침해의 영향은 얼마나 추산하십니까?

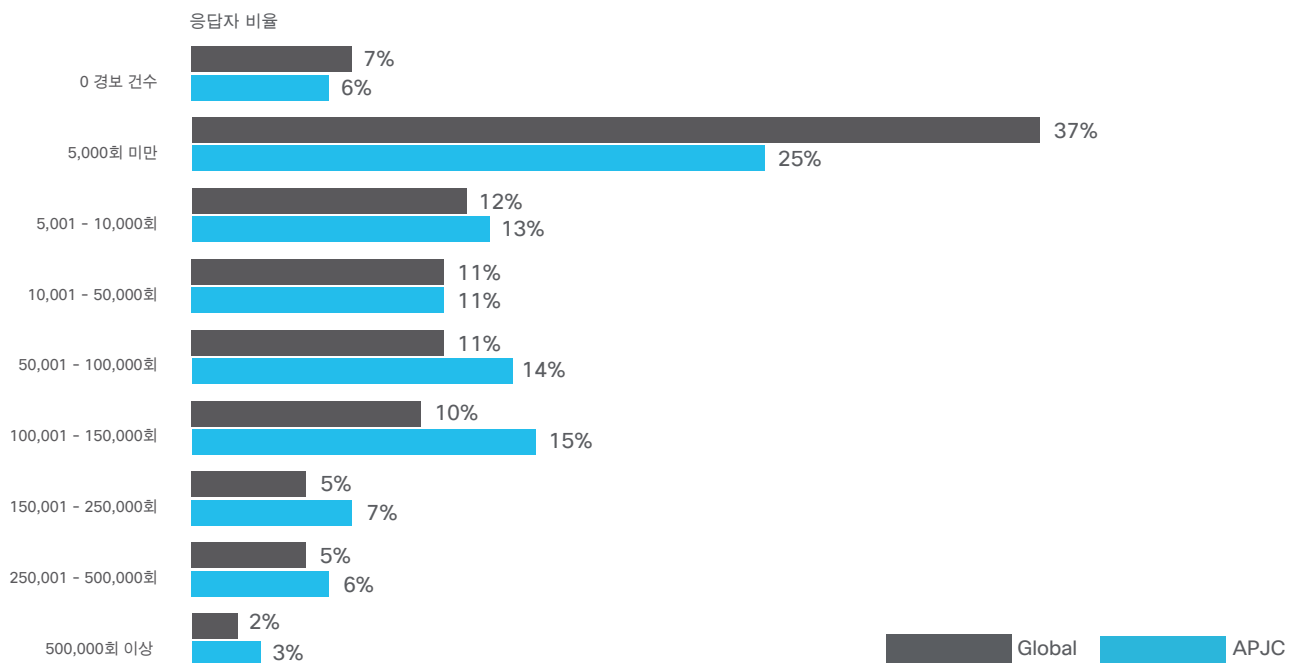
## 보안 경보 및 사이버 침해 대응

아태지역 보안 실무자들은 글로벌 실무자들보다 바쁩니다. 글로벌 벤치마크 연구의 응답자 중 37%는 하루에 5천건 미만의 경보를 받는 반면, 아태지역에서는 이 수치가 25%에 불과합니다. 언제나 그렇듯이 진짜 힘든 것은 경보를 수신한 이후입니다.

얼마나 많은 건수가 실제로 조사되었을까요? 아태지역은 56%로 글로벌 수치와 비슷하지만 여전히 낮은 수치입니다. 어떤 방식으로든 절반은 조사되고 있다는 것을 의미합니다. 한국은 가장 낮은 수치인 30%로 이 부문에서는 최하위 수치를 보이고 있으며, 호주가 72%로 가장 좋은 수치를 보입니다.

조사된 경보 중 실제 공격으로 판명된 경우에도 수치는 비슷합니다. 아태지역 전체에서는 조사된 경보 중 44%가 실제 공격인 것으로 파악되었으나, 호주에서는 65%로 경보 시스템의 정확도가 더 높은 것을 알 수 있습니다. 한국은 16%로 나타났는데, 이는 보안 전문가들이 자신의 보안 환경과 공격에 대해 정확한 정보를 얻기 위해 추가 작업이 필요하다는 것을 의미합니다.

그림 3 일일 보안 경보 건수



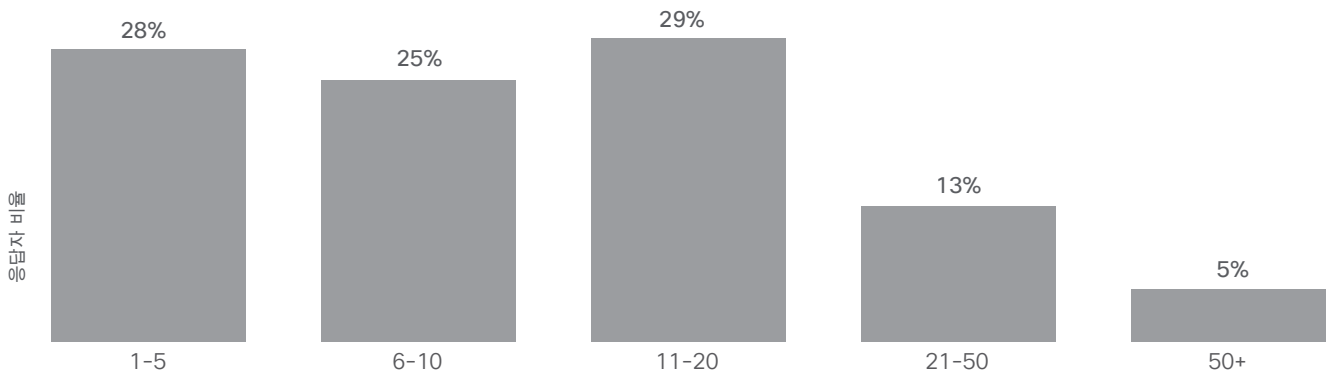
Q: 일 평균 몇 건의 보안 경보 메시지를 받으니까?

## 공급업체 파편화로 인한 복잡성

방어자들은 여러 공급 업체의 제품을 복잡하게 조합하여 사용하고 있습니다. 이렇듯 많은 도구를 사용하는 것은 보안 역량을 증가시키기 보다는 복잡하게만 만들 수 있습니다. 이러한 복잡성은 손실 위험이 증가하는 등 공격을 방어하는 기업에게 부정적 영향을 끼칠 수 있습니다.

아태지역 응답자의 47%는 보안 환경에 10곳 이상의 공급업체를 활용하고 있으며, 5%는 50곳 이상의 업체를 활용한다고 답했습니다. 호주와 인도는 평균 이상으로 복잡한 보안 환경을 보였는데, 호주는 12%가, 인도는 8%가 50곳 이상의 업체를 활용한다고 밝혔습니다.

그림 4 아태지역에서 기업과 조직들이 협업 중인 보안 업체의 수



Q: 당신의 조직에서 보안 업무로 협력 중인 업체(브랜드, 제조사 등)는 얼마나 됩니까?

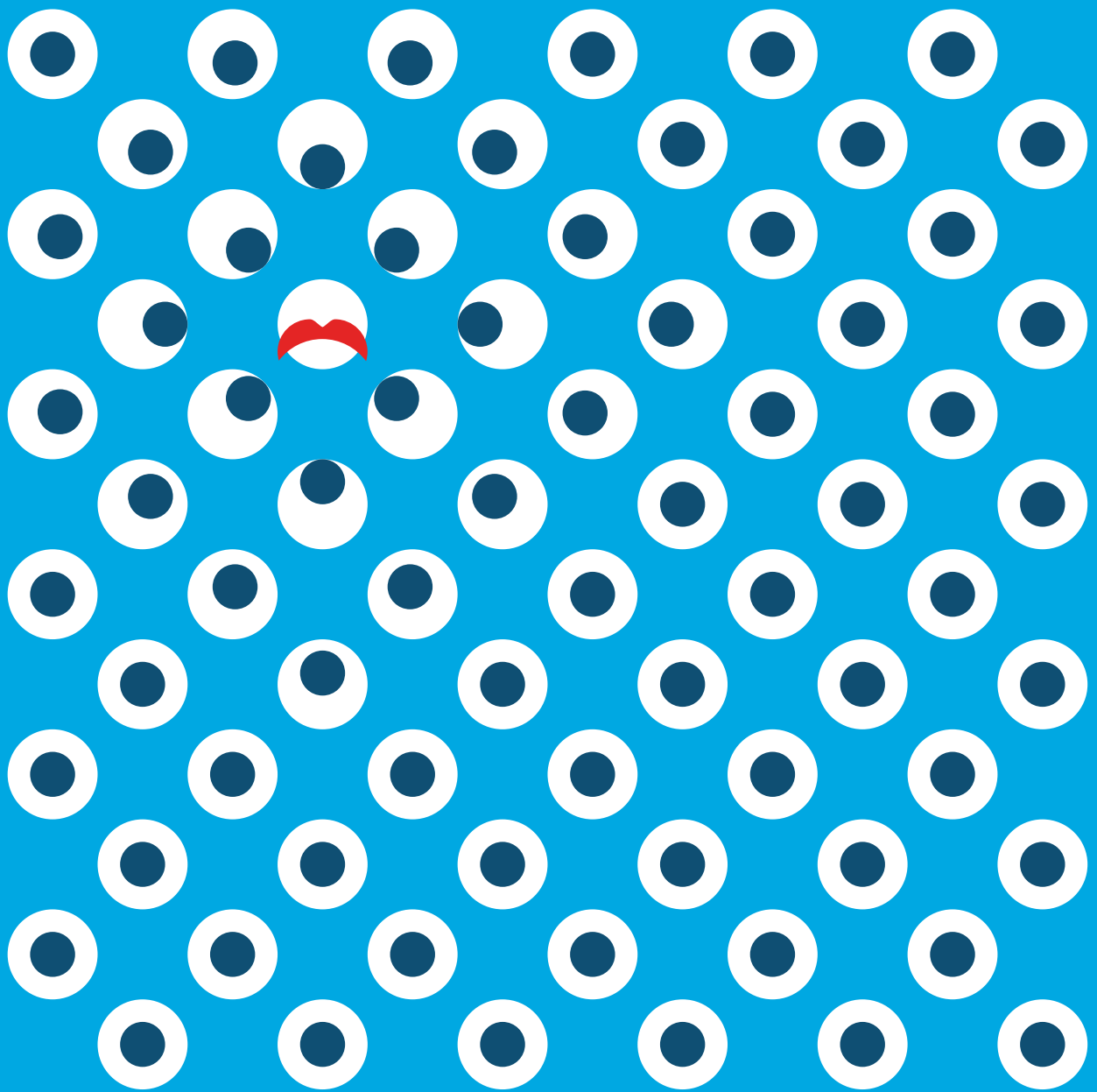
복잡성이 방어자들이 가진 유일한 과제는 아닙니다. 아태지역 보안 전문가들은 예산(32%), 기존 시스템과의 상호운용성(30%), 숙련된 인력부족(27%)을 핵심 제약 사항으로 꼽았습니다. 응답자 중 거의 2/3(59%)가 사이버 피로를 경험했고 선제적인 대응을 포기했다고 응답했습니다. 이는

글로벌 수치인 46%과 대조적이며, 아태지역의 방어자들이 적절한 장비를 갖출 수 있도록 더 많은 지원이 필요하다는 것을 의미합니다. 일본은 76%가 사이버 피로를 호소해 국가 차원에서는 가장 높은 수치를 기록한 반면 중국은 29%에 불과했습니다.

### 철저한 보안 공격 대비를 위한 제안

기업들은 보안 시스템을 전략적으로 개선하고, 우수 사례들을 잘 벤치마킹하면, 새로운 사이버 위협의 노출을 줄이고, 사이버 공격을 둔화시키며, 보안 위협에 관한 가시성을 높일 수 있다는 것을 알게 될 것입니다. 철저한 보안 공격 대비를 위해서는 다음의 5가지 사항이 고려되어야 합니다.

1. 클라우드 보안 플랫폼처럼 확장 가능한 최전방 방어 도구 구축
2. 침해 발생 노출을 줄이기 위한 네트워크를 세그멘테이션 실행
3. 차세대 엔드포인트 프로세스 모니터링 도구 채택
4. 적시에 정확한 보안 위협 정보에 관한 데이터와 프로세스에 접근하여, 이 데이터를 보안 모니터링 및 이벤틱스에 통합
5. 보안 대응 절차의 검토 및 실행



# 한국 조사 결과

국가별 요약

## 조사 결과 (한국):

# 사이버 공격 대응을 위한 훈련 필요

시스코의 조사 연구 결과 한국은 심각한 사이버 보안 도전 과제에 직면해 있습니다. 기업의 61%가 매일 5,000회 이상의 경보를 받고 있습니다. 한국의 보안 담당자 중 39%만 5,000번 미만의 경보를 받고 있으며, 이는 글로벌 표준인 44%보다 낮지만, 아태지역 벤치마크인 31%보다는 상당히 높은 수치입니다.

이 결과는 한국이 아시아 태평양 지역에서 일일 경보 건수를 낮추는 데 앞장 서고 있다는 것을 의미합니다. 경보 건수가 줄어들면, 처리해야 할 업무도 감소하여 이미 과중한 업무에 치진 보안 팀은 중요한 업무에 집중 할 수 있습니다.

또한 한국 응답자(14%)는 매일 100,000~150,000회 경보를 받고 있다고 답했습니다. 이는 글로벌 평균(10%)보다 높고, 아태지역 평균(15%) 보다 낮은 수준으로, 조사 결과 중 가장 낮은 수준에 위치하고 있다는 것으로 긍정적인 조사 결과입니다.

긍정적인 결과는 여기까지입니다. 경보의 70%는 조사되지 않습니다. 물론 보안 경보에 효율적으로 잘 조율된 대응을 한다는 것은 매우 어려운 일입니다. 하지만, 매일 경보의 30%만 조사되고 있으며, 이는 글로벌 및 지역 벤치마크 수치인 56%보다 현저히 낮은 수치입니다. 이는 경보의 70%에 대해 조치를 취하지 않는다는 뜻이며, 보안 역량 또는 보안 관련 자원이 부족하다는 뜻입니다. 최대 일일 15만회까지 경보를 받고 있는 소수의 회사의 경우, 이는 수만 건의 사고에 대해 아무런 조치가 이루어 지지 않는다고 볼 수 있습니다. 어떤 경보에 악성 코드가 있을지 누구도 알 수 없습니다.

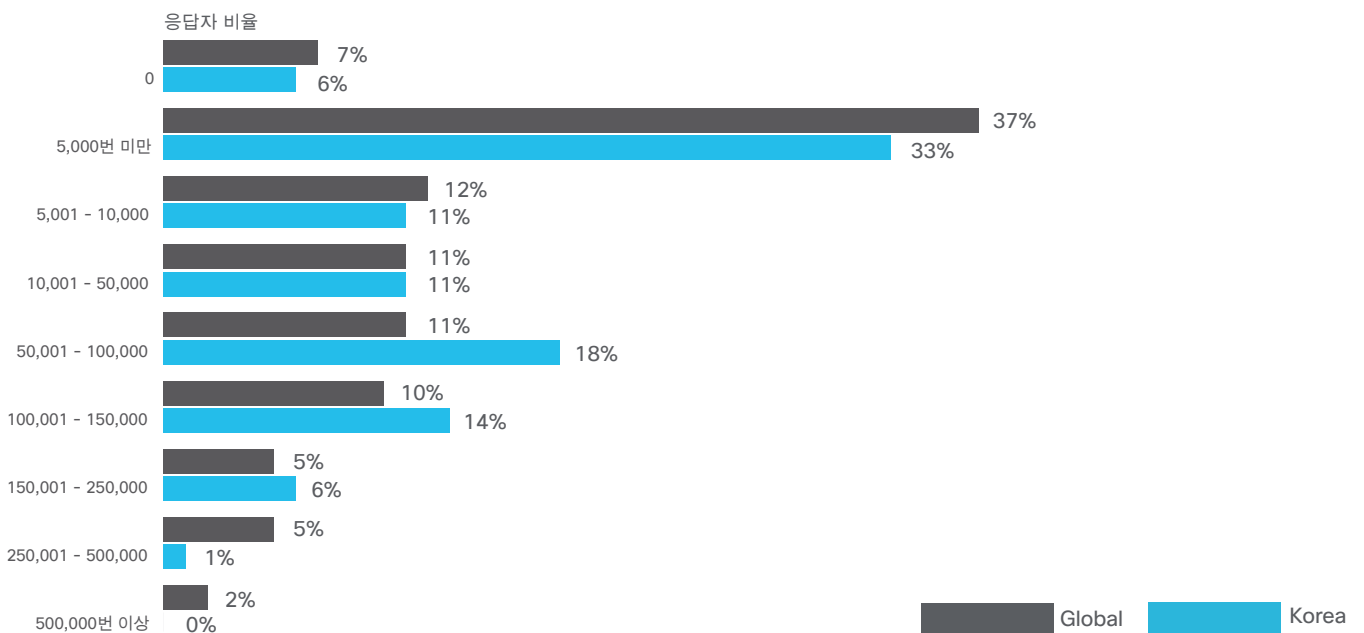
한국 방어자들은 보안 운영을 확장하고 더 많은 경보를 확인할 수 있는 새로운 방법을 모색할 필요가 있습니다.

경보를 조사하는 일은 첫 단계에 불과합니다. 즉, 방어자는 유효한 경보를 처리하고 있다는 확신이 있어야 합니다. 특히, 수많은 경보를 해결해야 할 때 그렇습니다. 조사된 경보의 16% 만 유효한 경보로 밝혀졌는데, 이는 해당 지역의 가장 낮은 수치입니다. 중국(23%)보다 낮으며 글로벌 벤치마크(34%)보다도 낮습니다. 해당 지역 표준(44%)에 비해 한참 뒤쳐져 있으며 호주(69%)와 같은 우수 국가와는 비교조차 할 수 없는 정도입니다.

이 결과는 조사한 경보의 84%가 무효 경보이며, 악성 프로그램이 처리되지 않은 로그 더미를 통해 침투할 뿐 아니라, 귀중한 작업 시간의 상당 부분이 필요 없는 작업에 투입되고 있음을 의미합니다.

유효 경보 중 궁극적으로 해결되는 비율은 40%로서, 이는 글로벌 표준(50%)과 아시아 태평양 표준(53%)에 미치지 못하며, 사실상 이 지역에서 태국(37%)과 베트남(39%)을 제외하면 가장 낮은 수치입니다.

그림 1: 매일 발생하는 보안 경보 횟수



질문: 일일 평균 귀하의 조직에서 발생하는 보안 경보의 횟수는 얼마입니까?

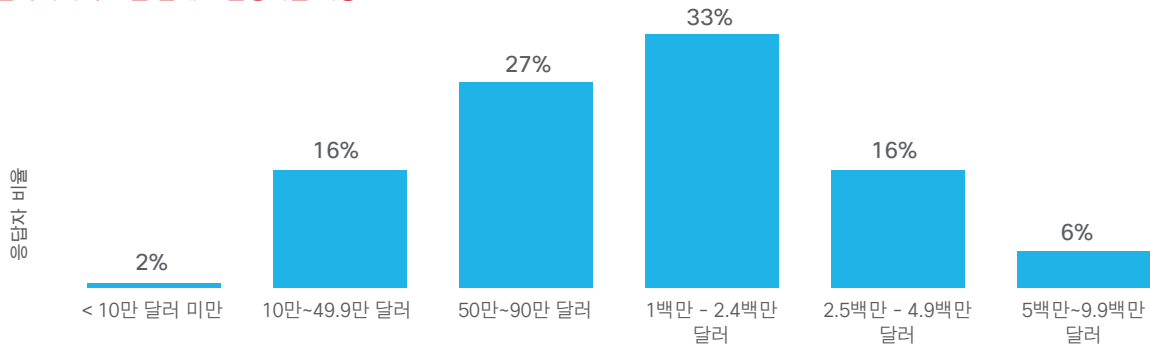
이는 한국의 보안 담당자들이 보안 전반을 살펴봐야 한다는 것을 의미합니다. 수많은 경보를 관리하고, 조사할 작업을 선별하고, 다수의 경보를 해결하기 위한 작업까지 말아야 합니다.

한국의 경우 보안 침해로 인해 발생하는 비용이 다른 지역에 비해 크기 때문에 매우 심각하게 받아들여야 합니다. 한국은 1~5백만 달러의 비용이 발생하는 보안 침해의 비율이 49%에 달해, 이는 아태지역(33%)이나 글로벌(30%) 보다 높은 수준입니다.

한국에서 사이버 침해로 발생한 비용 조사에 관한 결과는 최하위권에 머무르고 있습니다. 한국에서는 10만 달러 이하의 비용이 발생하는 침해 사례는 2%이며, 아태지역은 20%, 글로벌은 30%입니다.

또 하나 주목할만한 결과는 1천만 달러 이상의 비용이 발생한 보안 사고는 0%로 이는 지역(5%)이나 글로벌(3%) 표준에 비해 낮으며 이 지역 최고 수준인 호주(9%)보다 크게 못 미치는 수치입니다. 침해 비용이 아직도 통제 가능한 수준이라는 의미입니다.

그림 2: 한국에서의 보안 침해로 발생하는 비용



질문: 작년에 발생한 모든 사이버 공격에서 매출 손실, 고객 손실, 기회 비용, 비용 손실 등 모든 것을 고려한 경우, 사이버 침해의 영향을 얼마나 추산하십니까?

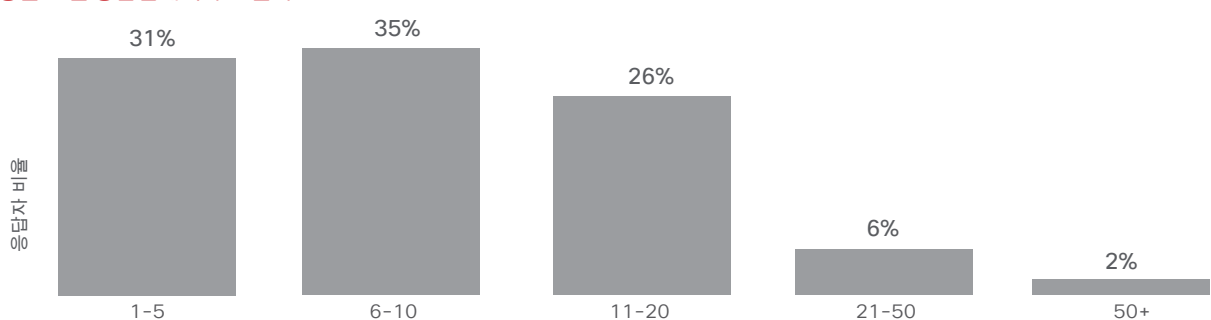
위 분석에서 중요한 부분은 한국이 보안 침해에 어떻게 대응하고 있는지입니다. 한국은 아태지역의 모범 사례에 미치지 못합니다.

응답자의 54%는 직원을 교육에 참가시켰다고 답변했으며, 이는 대응 목록의 제일 위에 있었습니다. 한국에서 고급 보안 프로세스 채택이 부족한 세 가지 원인 중 하나로 "지식 부족"이 언급된다는 것을 보면, 교육 참여는 좋은 대처 방법입니다. 세 가지 이유 중 또 다른 하나는 "레거시 시스템과의 호환성"이 포함되며, 다른 여러 국가와 마찬가지로 첫 번째 이유는 "예산 부족"이었습니다.

실질적으로 보안 분야가 개선되려면 이해관계자와 경영진의 관심과 참여가 필요합니다.

사이버 보안 관리자는 인적 자원을 잘 관리할 과제도 안고 있습니다. 응답자의 39%만 사이버 피로로 고통 받고 있다고 답변했는데, 이는 지역(59%) 평균에 비해 낮은 수치이지만, 방어자의 1/3은 여전히 조사되지 않은 다수의 경보에 압도당하기 이전에, 많은 양의 경보를 보다 정확하게 처리할 수 있는 개선된 방법을 익힐 필요가 있습니다.

그림 3: 다양한 보안 공급업체의 수 - 한국



질문: 당신의 조직에서 보안 업무로 협력 중인 업체(브랜드, 제조사 등)는 얼마나 됩니까?

위 조사 결과는 한국이 끊임없이 변화하는 사이버 위협 환경에 대처하기 위해 투자하지 않고 있다는 말은 아닙니다. 응답자는 34%는 10곳 이상의 공급자와 협업 중이며, 응답자의 50%는 10종 이상의 제품을 활용합니다.

제품의 수가 적을수록 공격자가 침투할 수 있는 틈새가 좁아진다는 금언을 생각해 보면, 이 결과는 공급업체 10곳 이상이 73%, 제품 10종 이상이 76%라고 보고된 호주보다 잘 통제되고 있음을 의미합니다.

사이버 피로의 원인은 수치에서 나타납니다. 한국 방어자의 92%는 여러 업체로부터 받는 경보를 조정하기가 다소 어렵거나 매우 어렵다고 답했으며, 이는 아태지역(82%)이나 글로벌(74%) 표준보다 높은 수치입니다. 응답자들이 모두 피로를 시인한 것은 아닐 수 있으며, 다른 국가들의 사례처럼 증가하는 사이버 위협과의 싸움에서 압도당할 것일 수도 있습니다. 보안 교육, 보안 제품 간 조율, 자동화는 한국에서 사이버 보안 과제를 해결하는데 도움이 될 것입니다.

\*일본, 중국, 인도, 호주 응답자는 2017년에 인터뷰를 마쳤습니다. 싱가포르, 인도네시아, 태국은 2018년 6월, 이 연구의 마지막 단계에 인터뷰를 진행했습니다.