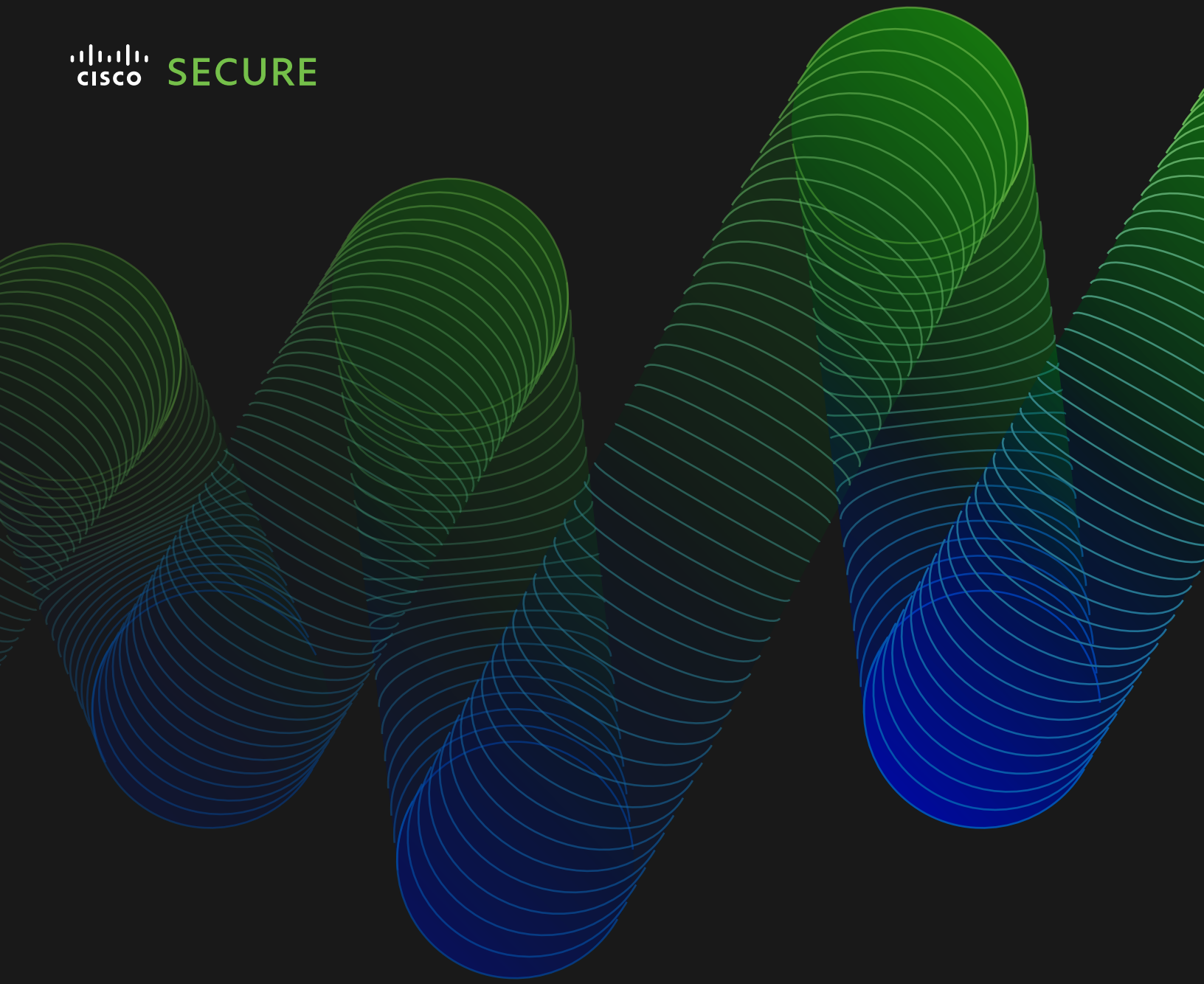
cisco SECURE



APJC 지역의 보안 탄력성 현황

보안 성과 보고서 제3권 주요 내용

cisco The bridge to possible

보안 탄력성 평가

보안 탄력성이란 무엇이며, 왜 중요하고, 성공적으로 강화하려면 어떻게 해야 할까요? 이것이 바로 시스코에서 최근 발표한 보안 성과 보고서 제3권에서 답하고자 했던 질문들입니다. 이 보고서에서는 전 세계 보안 리더 및 전문가 4,700명으로부터 수집한 데이터를 분석합니다. 본 스냅샷에서는 APJC (Asia-Pacific, Japan, China) 지역에서 일하는 참여자 1,400명의 답변을 중점적으로 살펴봅니다.

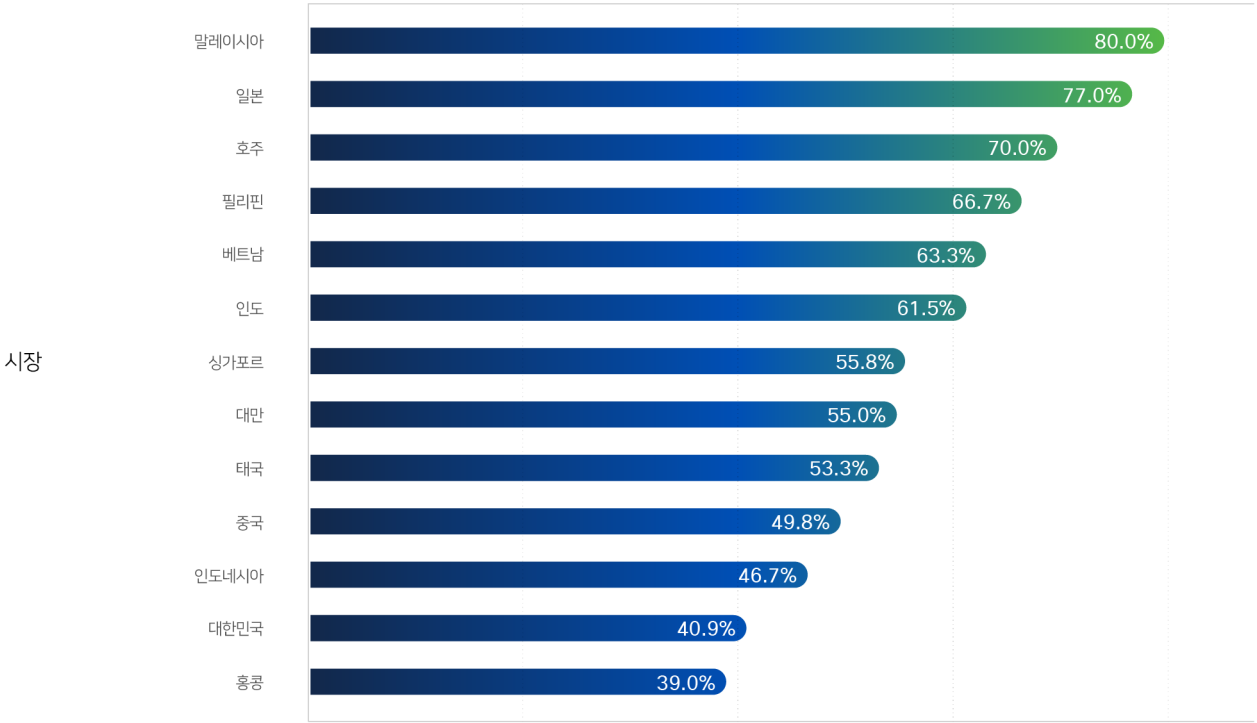
임원진이 탄력성의 중요성을 인식하고 있을까요?

네, 그렇습니다! 시스코에서는 응답자들에게 최고위 임원진이 보안 탄력성에 대해 얼마나 관심이 있고 중요하게 생각하는지 물었습니다. 그 메시지는 아주 분명했습니다. APJC 임원진의 97%가 보안 탄력성을 매우 중요하게 여기고 있으며 해당 통계는 APJC 지역 전체에서 비슷하게 나타납니다.

사이버 이벤트는 탄력성에 영향을 미칠까요?

전 세계 조직의 62% (APJC 조직의 58%) 에서 대규모 보안 사고로 인해 비즈니스 운영에 타격을 입었으며, 그중 대부분이 지난 몇 년 동안 발생한 사고라고 답했습니다. 탄력성에 영향을 미치는 이벤트의 비율은 APJC 전체에 걸쳐 상당히 다르게 나타납니다. 보안 사고 빈도가 가장 낮은 곳은 홍콩 (조직의 39%) , 가장 높은 곳은 말레이시아 (조직의 80%) 인 것으로 나타났으며, 다른 시장들은 두 국가 사이에 고르게 분포되어 있습니다.

그림 1: 탄력성에 영향을 미친 것으로 보고된 보안 사고의 비율



출처: 시스코 보안 성과 보고서

APJC 지역의 탄력성 현황

보안 성과 보고서 제3권 전문 보기

어떤 유형의 사이버 이벤트가 탄력성에 영향을 미칠까요?

시스코에서는 응답자들에게 그들이 경험했던 탄력성에 영향을 미치는 사고의 유형을 자세히 설명해 달라고 요청했습니다. 아래 차트는 각 시장에서 조직이 보고한 보안 사고의 백분율을 기준으로 매긴 보안 사고 유형의 순위입니다. 예를 들어 싱가포르 (60%) 와 한국 (59%) 에서는 DDoS 공격이 기업에서 가장 흔히 발생하지만 인도에서는 마지막에서 두 번째 순위를 차지합니다 (37%). 모든 시장에서 물리적 파괴와 관련된 보안 사고의 빈도가 가장 낮은 것으로 나타났습니다.

그림 2: 탄력성에 영향을 미치는 보안 사고 유형

출처: 시스코 보안 성과 보고서

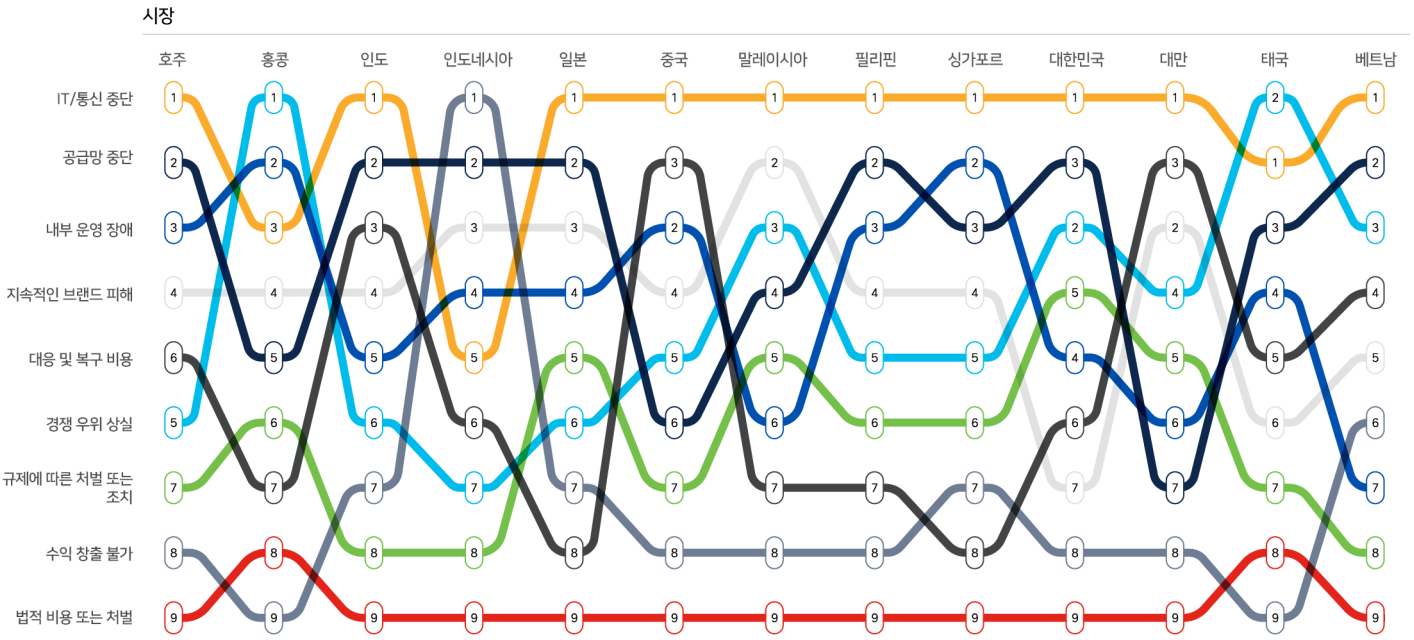
APJC 지역의 탄력성 현황

보안 성과 보고서 제3권 전문 보기

보안 사고는 비즈니스에 어떤 영향을 미칠까요?

시스코에서는 응답자에게 대규모 보안 사고가 조직에 미친 영향에 대해 질문했습니다. 다음 차트는 영향이 발생했다고 답한 각 APJC 시장 내 조직의 백분율을 기준으로 영향 유형의 순위를 비교한 것입니다. 예를 들어 대부분의 시장에서 IT 중단이 가장 많이 발생했고, 법무 비용 또는 벌금이 일반적으로 가장 낮은 순위를 차지했습니다. 보안 사고 발생 후 수익 창출에 문제가 발생한 경우는 인도네시아가 1위, 홍콩과 태국이 9위로 나타났습니다.

그림 3: 보안 사고로 인한 탄력성 영향의 유형



출처: 시스코 보안 성과 보고서

시장마다 보안 사고 발생률, 유형, 영향이 다른 이유로는 규정 및 컴플라이언스 강도, 지정학적 요인, 주요 비즈니스 모델, 보안 사고 탐지 역량, 보안 프로그램 성숙도의 차이 등이 있습니다.

"수많은 조직이 초기 정책을 수립하고 에셋 보호를 인스턴스화하는 데 어려움을 겪습니다. 적합한 보안 조치가 구축되어 있지 않으면, 조직 네트워크 전체에 악성코드 또는 기타 위협이 탐지되지 않은 채로 확산되어 횡적 이동을 통해 광범위한 감염이 발생할 수 있습니다.

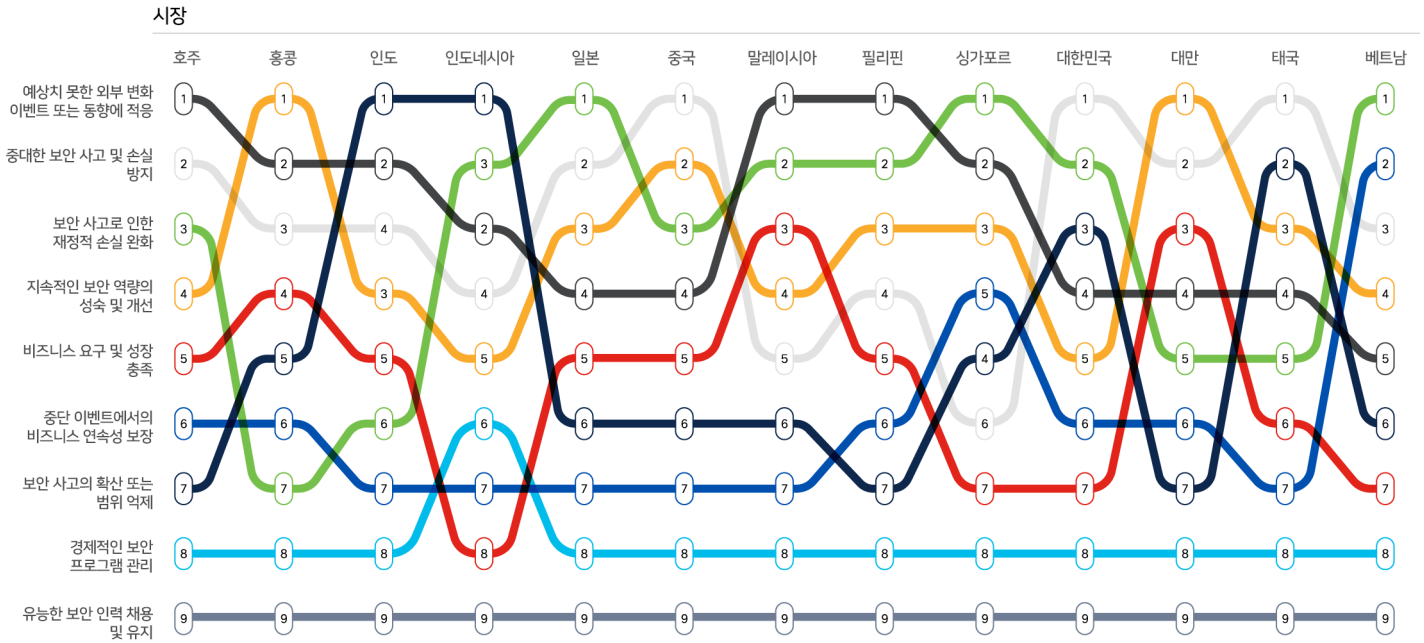
보안 조치가 부족하면 감염을 식별하고 소스를 분리하기가 어려워 문제 해결에 더 많은 시간이 소요되므로 문서에서 "IT/통신 중단" 및 "내부 운영 장애"로 언급된 전체적인 서버 중단이 조직 전체에 발생할 수 있습니다.

— Timothy Snow,
시스코 APJC 지역 CISO 자문 겸 아키텍트

어떤 탄력성 성과가 가장 중요할까요?

주 보고서에서는 보안 탄력성과 관련된 9가지 핵심 목표 또는 성과를 제시합니다. 시스코에서 참여자들의 소속 조직이 9가지 성과 중 무엇을 가장 중요하게 여기는지 질문한 결과, APJC 시장에서의 순위는 아래와 같습니다. 대부분의 시장에서 비용 효율적인 프로그램 운영과 보안 인력 유치/유지가 가장 낮은 순위로 나타났습니다. 하지만 다른 성과들에서는 차이가 있습니다. 예를 들어 일본과 싱가포르에서는 보안 사고로 인한 재정적 손실 완화가 최우선순위인 반면 홍콩과 인도에서는 각각 7위와 6위를 차지했습니다.

그림 4: 보안 탄력성 성과의 중요도 순위

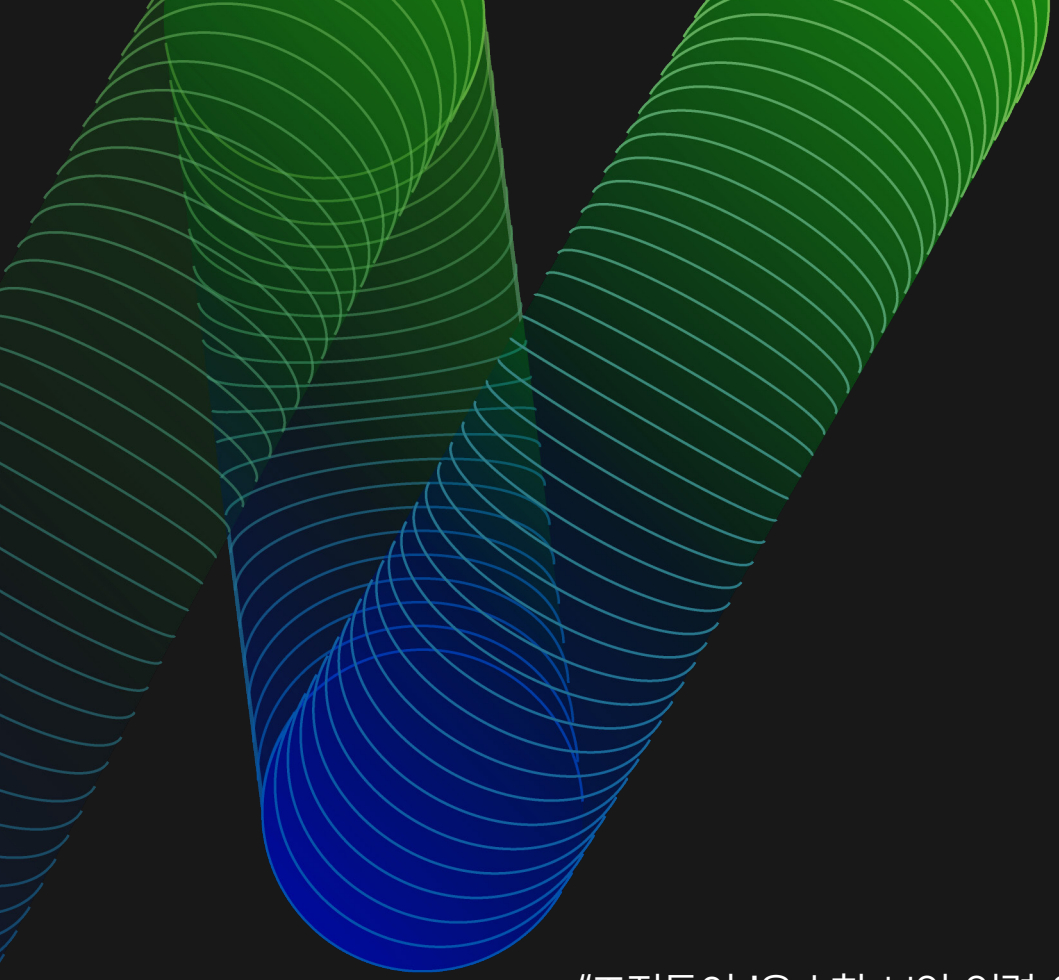


출처: 시스코 보안 성과 보고서

고객 스포트라이트

금융 서비스 기업인 **Kasikorn Bank and Business-Technology Group (KBTG)**의 CISO인 Chatchawat Asawarakwong의 이야기를 통해 Cisco CX로 디지털 혁신 여정에서 조직의 보안을 유지한 방법을 알아보세요. 비디오 보기

호주 최대의 국내선 및 국제선 항공사 **Quantas**에서는 25,000명의 사용자를 보호하기 위해 Cisco SASE를 구축하여 원활한 하이브리드 업무를 지원하고 직원 만족도를 높이고 있습니다. 사례 연구 읽기



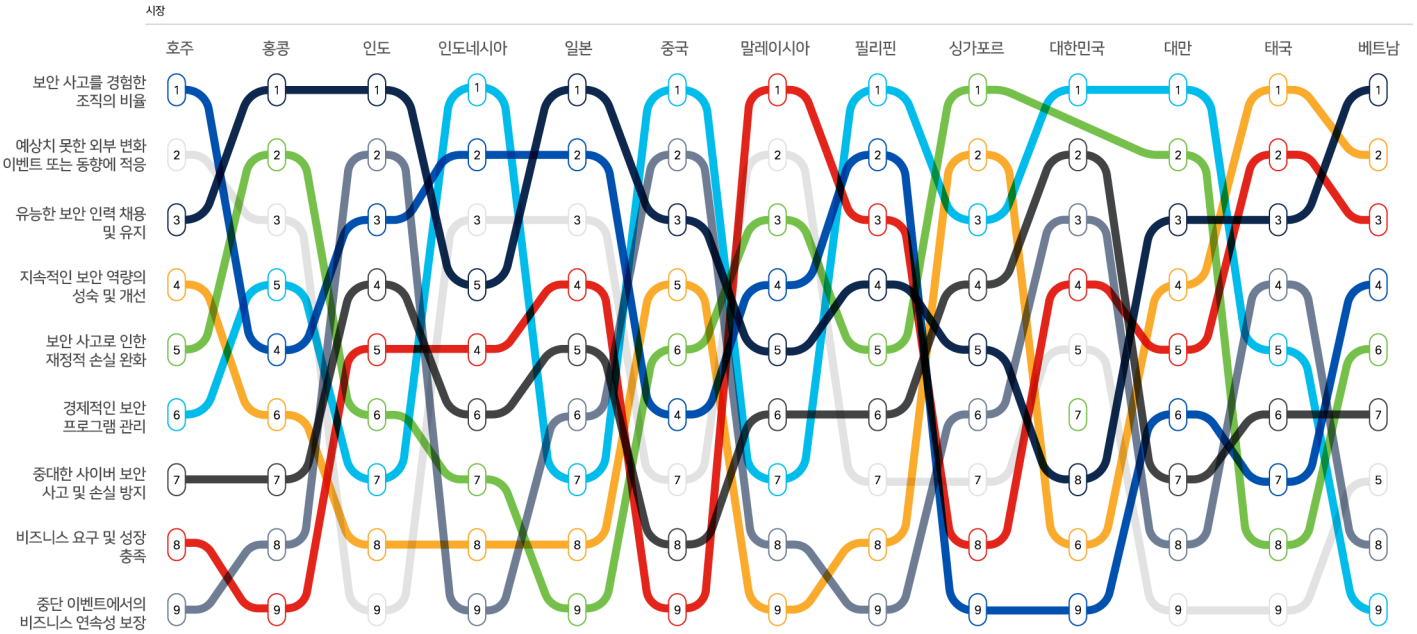
"조직들이 '우수한 보안 인력 유치 및 유지'에 낮은 순위를 주었다는 사실이 놀랍습니다. 조직에 전문 인력이 부족하고 기존 팀이 이미 과중한 업무에 시달리고 있어 새로운 기술의 도입이 어려운 경우가 많기 때문이죠. 이러한 현상은 중견·중소기업에서 두드러지지만, 대기업에도 유지 문제가 발생합니다. 이는 비즈니스 확장 및 보호를 위한 새로운 기술의 소비에 직접적인 영향을 줍니다."

— Timothy Snow,
시스코 APJC 지역 CISO 자문 겸 아키텍트

가장 달성하기 어려운 탄력성 성과는 무엇일까요?

시스코에서는 응답자들에게 소속 조직이 각 탄력성 성과를 실제로 얼마나 잘 달성하고 있는지 순위를 매기도록 했습니다. 아래 차트는 각 성과와 관련한 당면과제의 순위와 APJC 지역 전체에서 순위 변화를 보여줍니다. 시장마다 당면과제가 다르다는 점이 흥미롭습니다. 예를 들어 호주에서는 보안 사고의 범위와 확산을 제한하는 것이 가장 큰 당면과제이지만 싱가포르와 한국에서는 가장 작은 당면과제입니다. 말레이시아 기업들의 가장 큰 어려움은 보안 프로그램을 비즈니스 성장 속도에 따라 업그레이드하는 것이지만, 홍콩과 중국 본토 기업들은 탄력성 당면과제 중 이를 가장 낮은 순위로 꼽았습니다.

그림 5: 보안 탄력성 성과 달성의 어려움 순위



출처: 시스코 보안 성과 보고서

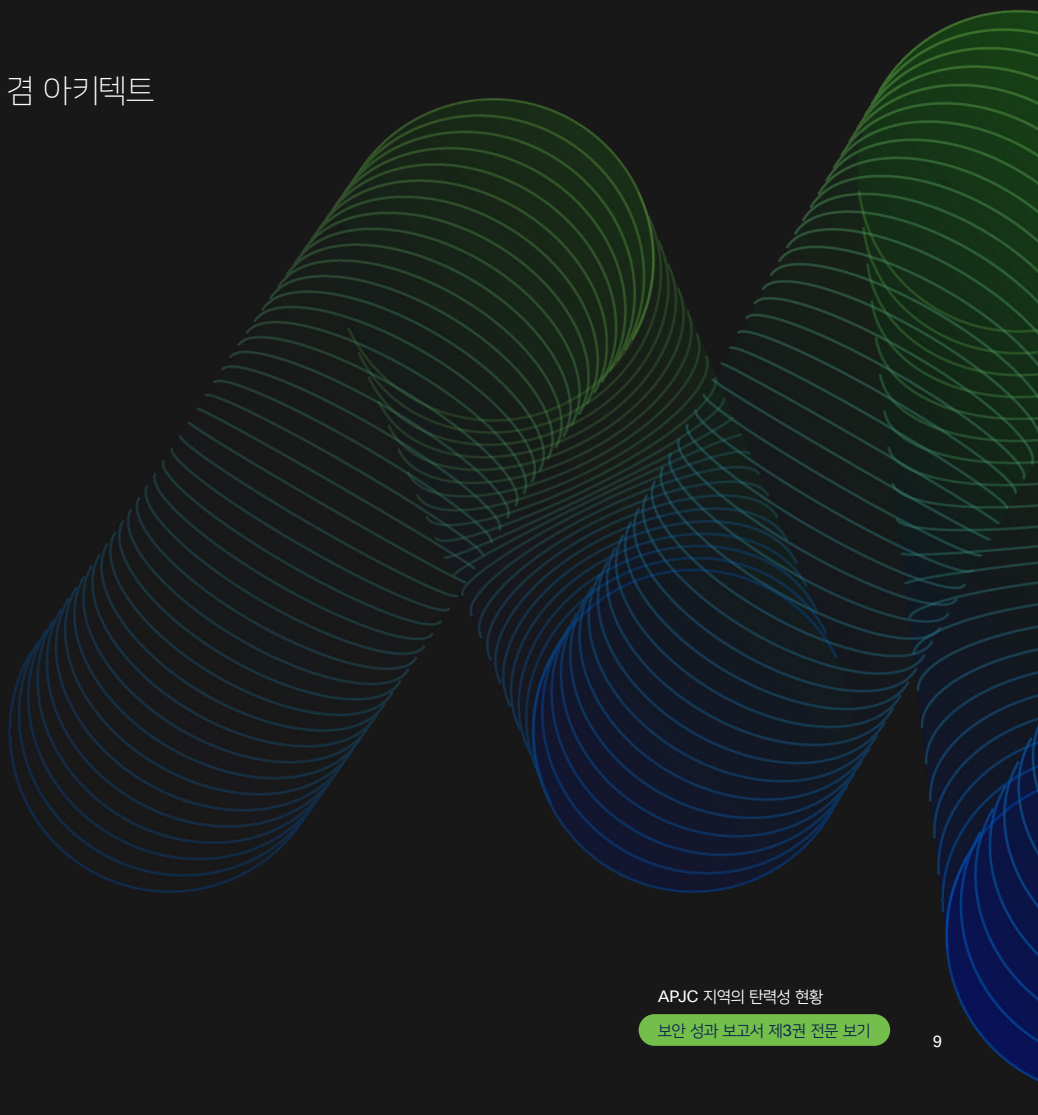
보안 탄력성을 통한 적응 및 극복

원활하게 통합된 보안 스택을 통해 실제 제품 비용을 절감하고 구축, 관리, 유지보수에 소요되는 리소스를 줄일 수 있습니다. 클라우드 우선 솔루션부터 관리형 서비스까지, Cisco Secure를 통해 보안 팀이 더 많은 비즈니스 크리티컬 이니셔티브에 집중할 수 있습니다. 보안 탄력성을 구축하면서도 위험과 비용을 줄이는 방법에 대해 알아보세요.

eBook 읽기

"APJC 지역에서는 비용을 매우 중요하게 생각하기 때문에 여러 시장에서 '비용 효율적인 보안 프로그램 운영'을 최우선으로 꼽았습니다. 비용에는 제품 또는 서비스의 도입뿐 아니라 해당 기술의 설치, 라이선싱, 교육, 유지도 포함됩니다. 이는 APJC 지역에서 포괄적인 보안 아키텍처를 구축하는 데 어려움을 겪고 있다는 것을 보여주기도 합니다." 보안 성과 보고서 (제2권) 이전판에서 다루었듯이, 보안 인력의 비율이 높은 조직이 그렇지 않은 조직보다 강한 역량을 보이는 것으로 나타나 보안 인력 비율과 효과적인 위협 대응 간에는 직접적인 상관관계가 있는 것으로 나타났습니다.

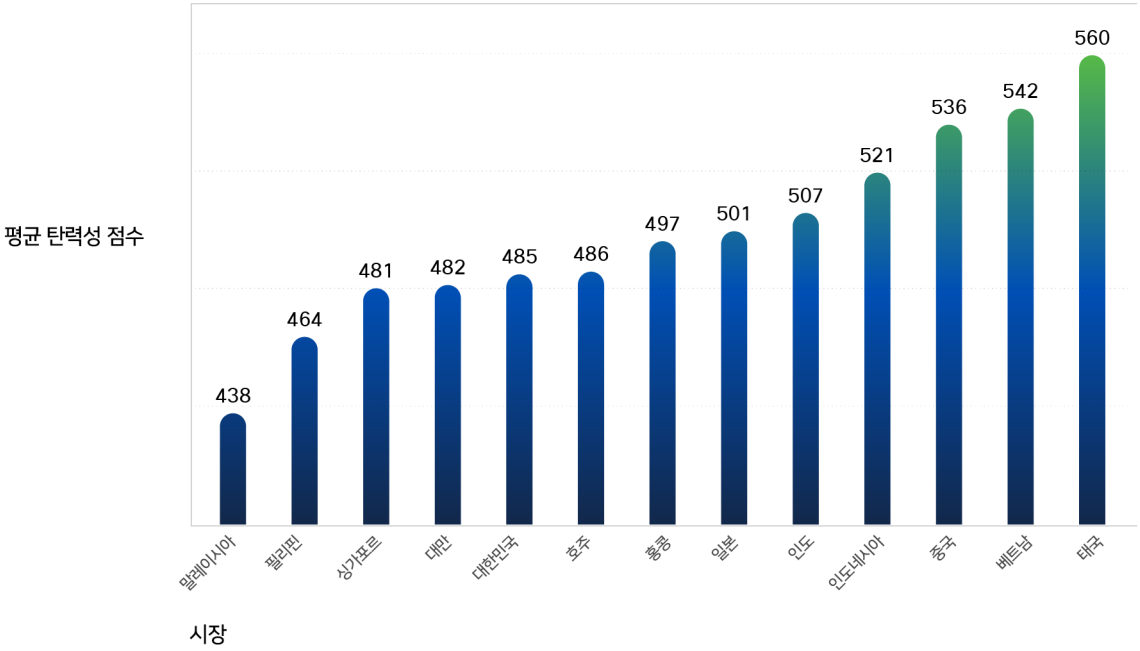
— Timothy Snow,
시스코 APJC 지역 CISO 자문 겸 아키텍트



전체적인 보안 탄력성을 어떻게 측정할 수 있을까요?

9가지 성과의 순위에 따라, 시스코에서는 각 조직의 종합적인 보안 탄력성 점수를 매기고 이러한 점수를 세계 평균을 500으로 하여 정규화했습니다. 전체적으로 APJC 시장 13곳 중 6곳이 시장 평균을 웃돌았습니다. 말레이시아 조직들의 평균 보안 탄력성 점수가 가장 낮았고 (438) , 태국의 점수가 가장 높았습니다 (560) .

그림 6: 각 시장 조직의 평균 보안 탄력성 점수



출처: 시스코 보안 성과 보고서

보안 탄력성 강화

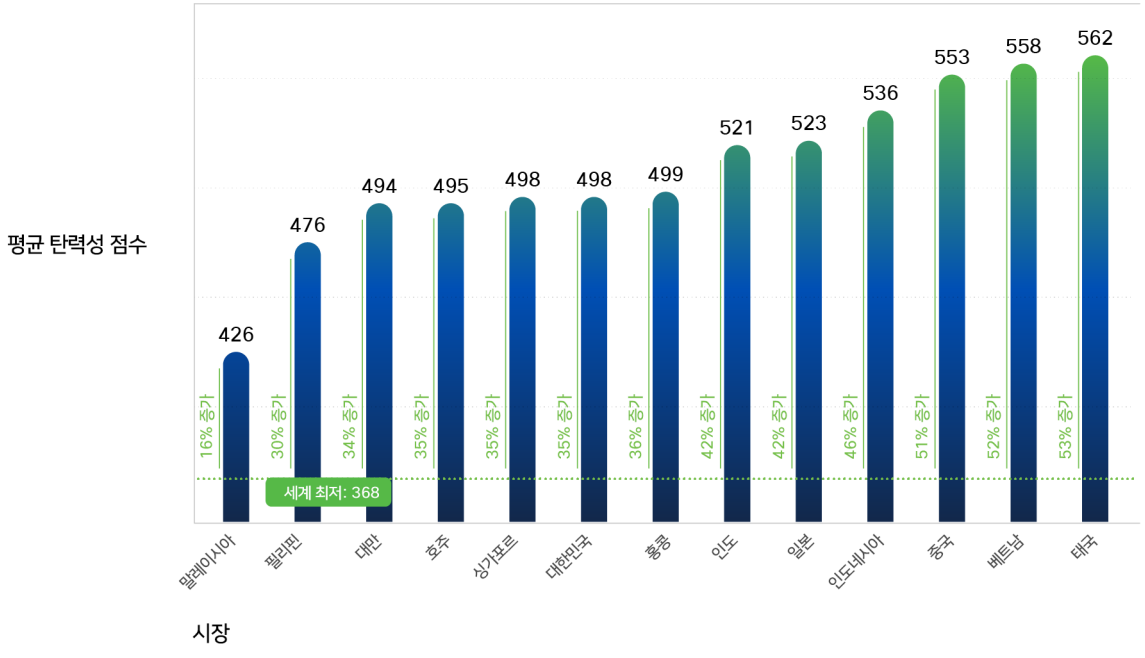
APJC 지역 각 조직의 9가지 성과에 걸친 전체적인 보안 탄력성을 나타내는 점수를 통해, 시스코에서는 다양한 요인을 테스트하여 효과적으로 성과를 향상하는 7가지 요인을 파악했습니다. 이제 APJC 지역에 해당하는 이러한 몇 가지 요인과 관련하여 전체적인 보안 탄력성 점수를 향상할 수 있는 방법을 알아보겠습니다.

임원진 지원 구축

전 세계적으로, 최고위 임원진의 지원이 부실하다고 답하는 조직은 강력한 C 레벨 임원진의 지원을 받는 조직보다 보안 탄력성 점수가 39% 낮습니다. 주 보고서의 데이터에서 얻은 몇 가지 단서를 바탕으로, 이러한 지원을 확보하는 방법을 알아보겠습니다. 여기에서는 APJC 시장에서 유사한 효과가 있는지 확인합니다.

다음 차트는 각 시장에서 보안 프로그램에 대해 강력한 임원진 지원이 이루어지는 조직들의 평균 보안 탄력성 점수 (파란색 막대) 를 보여줍니다. 막대 옆의 백분율 증가는 임원진 지원이 부족한 조직들의 잠재적인 개선 범위를 나타냅니다. 이를 통해, 예를 들어 말레이시아 조직들은 강력한 임원진 지원으로부터 혜택을 받는다는 것을 알 수 있지만 (평균 보안 탄력성 점수에서 16% 상승) , 세계 평균은 +39%이므로 그다지 큰 상승은 아닙니다. 하지만 태국의 경우, 강력한 임원진 지원이 이루어지는 경우 +53%라는 상대적으로 더 큰 상승이 이루어집니다.

그림 7: 임원진 지원이 보안 탄력성에 미치는 잠재적 영향



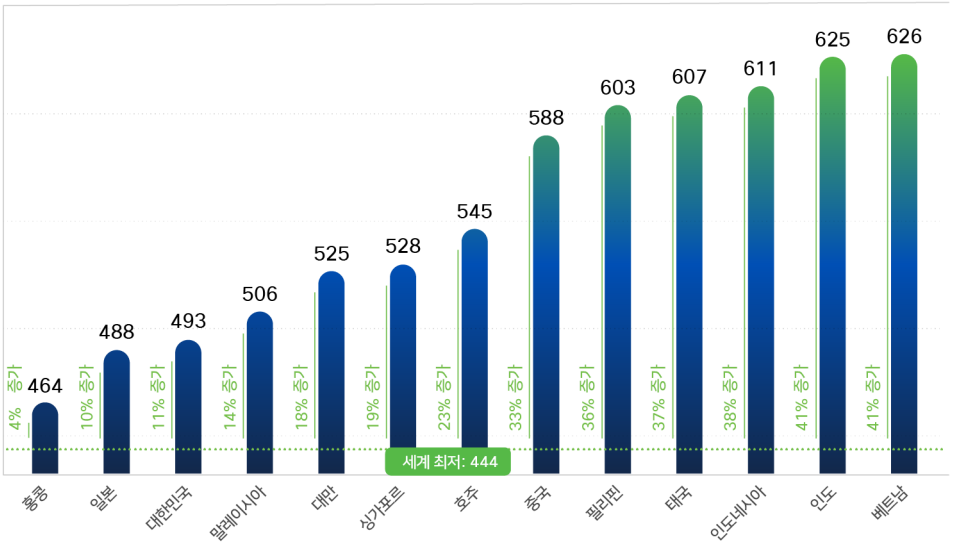
출처: 시스코 보안 성과 보고서

제로 트러스트 채택 극대화

주 보고서에 따르면, 제로 트러스트 원칙 실행에 있어 진전이 없는 조직과 실행의 성숙도가 높은 조직 (적응형 정책을 통한 MFA, 지속적인 검증, 마이크로 세그멘테이션, 포괄적인 모니터링, 사용자 워크플로우 오케스트레이션) 의 평균 탄력성 점수가 30%의 차이를 보이는 것으로 나타났습니다.

대부분의 APJC 시장에서 제로 트러스트와 관련하여 유사한 탄력성 향상을 보이고 있습니다. 홍콩 기업들은 세계 평균에 비해 훨씬 낮은 증가율을 보이고 있지만 (+4%), 베트남 기업들은 제로 트러스트 구현의 성숙도가 높은 경우 보안 탄력성이 훨씬 커집니다 (+41%).

그림 8: 제로 트러스트 도입이 보안 탄력성에 미치는 잠재적 영향



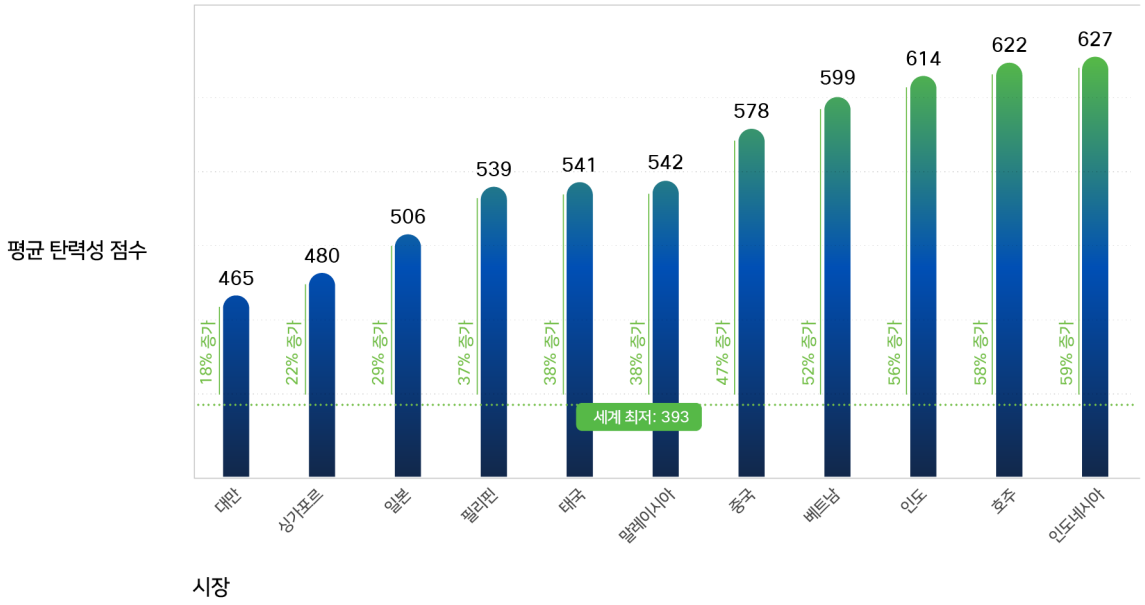
출처: 시스코 보안 성과 보고서

XDR (Extended Detection and Response) 역량

첨단 사이버 위협은 여러 방향으로부터 이루어집니다. 따라서 이러한 다양한 방향에 걸쳐 여러 밴티지 포인트를 확보하면 사이버 보안에 도움이 됩니다. 네트워크, 클라우드, 엔드포인트, 애플리케이션에 대한 가시성을 제공함과 동시에 애널리틱스 및 자동화를 적용하여 위협을 탐지, 분석, 추적, 해결하는 것이 XDR (Extended Detection and Response) 솔루션 가치 제안의 핵심입니다.

시스코 데이터에 따르면, XDR은 이러한 가치를 실현하는 것으로 나타났습니다. 성숙도가 높은 XDR을 구현하는 조직은 XDR 역량을 갖추지 않은 조직보다 전체적인 탄력성 점수가 45% 높았습니다. 아래 그림과 같이, 주요 APJC 시장의 평균 상승폭은 이 수치 위 (중국, 베트남, 인도, 호주, 인도네시아) 와 아래 (대만, 싱가포르, 일본, 필리핀, 태국) 에 골고루 분포해 있습니다.

그림 9: XDR 도입이 보안 탄력성에 미치는 잠재적 영향



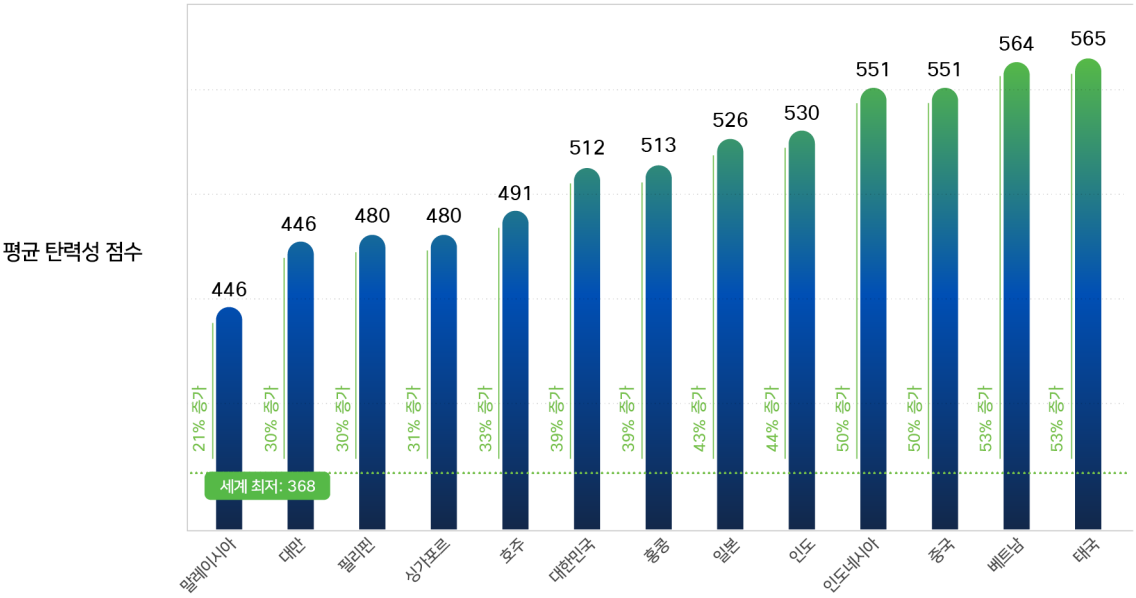
출처: 시스코 보안 성과 보고서

보안을 엣지에 배치

모바일 인력, 디바이스 확산, 여러 클라우드 공급업체를 통한 애플리케이션 하이퍼 분산을 비롯한 하이브리드 작업의 가속화로 인해 광범위하고 파편화된 상호 연결성 보안에 대한 당면과제가 증가하고 있습니다. 보안 액세스 서비스 엣지 (SASE) 는 네트워킹 및 보안을 클라우드 제공 서비스에 통합하고, 운영을 간소화하며, 끊임없이 변화하는 비즈니스 요구에도 탄력성을 유지하는 전략을 제공합니다. 또한 최근 보안 성과 보고서에서는 SASE의 효과를 뒷받침하는 강력한 증거를 제시합니다.

전 세계적으로, 성숙한 SASE를 구현하지 않은 조직과 구현한 조직 간의 평균 탄력성 점수는 27%의 차이를 보였습니다 (자세한 내용은 여기를 참조) . APJC 시장 중 한 곳 (말레이시아) 을 제외하면 SASE 롤아웃을 시작하지 않은 기업들에 비해 평균 탄력성 점수가 최대 53% (태국) 높아졌습니다.

그림 10: SASE 도입이 보안 탄력성에 미치는 잠재적 영향



출처: 시스코 보안 성과 보고서

결론

APJC 지역 내 여러 국가 및 시장마다 차이는 있지만, 살펴볼 만한 일관성도 찾을 수 있었습니다. 이 지역의 임원진은 보안 탄력성을 매우 중요하게 생각합니다. 그렇다면 보안 탄력성과 관련한 우려 사항을 해결하려면 조직 내에서 무엇을 해야 할까요? 데이터에 따르면, 보안 탄력성을 강화하기 위한 필수 조건은 XDR 역량 강화, 제로 트러스트 도입 확대, 성숙한 SASE 구현입니다. 물론 이러한 각 영역을 최적화하는 것은 긴 여정이며 IT 팀과 보안 운영 팀의 계획과 협업이 필요합니다.

추가 정보:

보안 탄력성 목표를 달성하기 위해 팀이 협업하는 방법에 대한 자세한 내용을 알아보려면, Security Outcomes Report, Volume 3: Achieving Security Resilience (보안 성과 보고서 제3권: 보안 탄력성 확보) 전문을 다운로드하세요.

APJC 지역의 탄력성 현황

보안 성과 보고서 제3권 전문 보기

CISCO
SECURE

미주 본사
Cisco Systems, Inc.
캘리포니아 주 새너제이

아시아 태평양 본사
Cisco Systems (USA) , Pte. Ltd.
싱가포르

유럽 본사
Cisco Systems International BV
네덜란드 암스테르담

Published March 2023