COHESITY

사이버 레질리언스 보고서

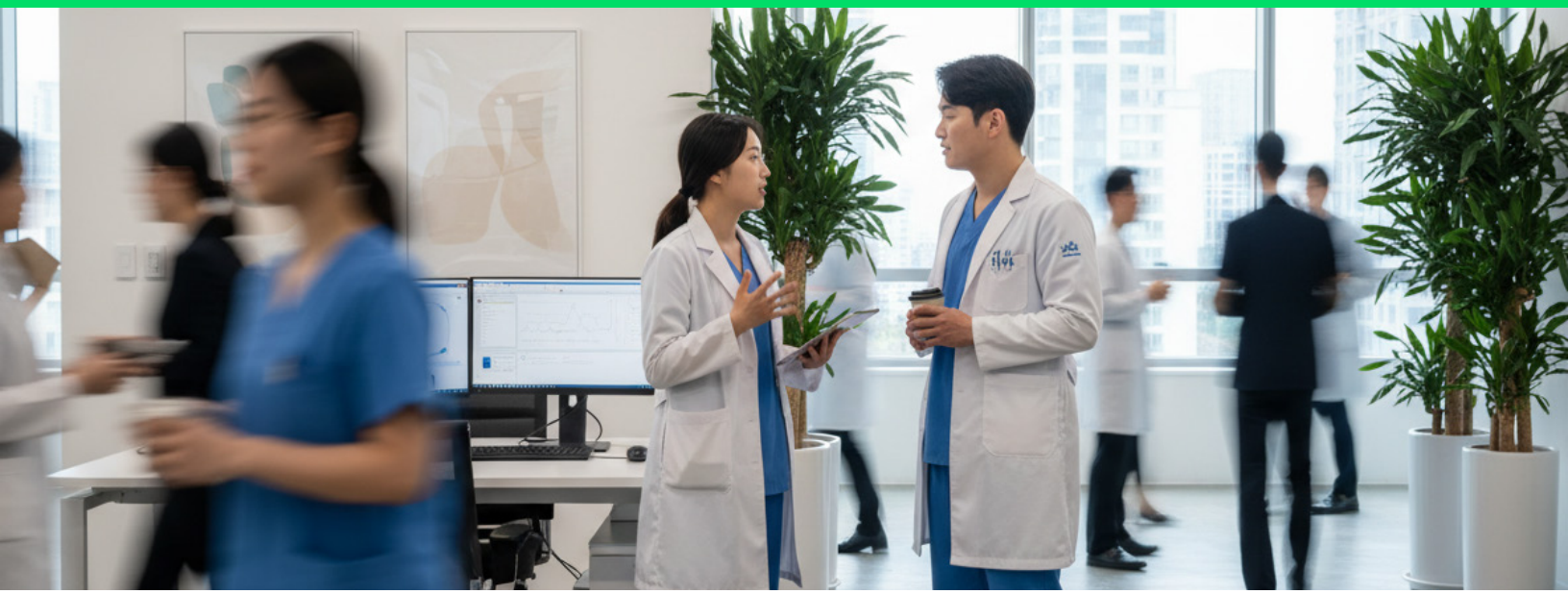
위험 대비 또는 위험 노출: 헬스케어 사이버 레질리언스 격차

2026년 4월

모두가 사이버 공격을 탐지하고 예방하는 것에 대해 이야기하지만, 언론이 전하는 내용은 다릅니다. 더 이상 예방과 탐지만으로는 충분하지 않습니다. 최첨단 기업들도 IT 운영에서 이사회 및 그 이상으로 파급되는 심각한 혼란을 겪고 있습니다.

탄력적인 조직과 여전히 어려움을 겪고 있는 조직을 구분하는 요인을 이해하기 위해 Cohesity는 전 세계 11개국의 IT 및 보안 운영 의사 결정권자 3,200명을 대상으로 설문조사를 실시했습니다.이 가운데 371명은 의료 기관 소속 참가자였습니다. 이들의 응답은 신속하고 자신 있게 복구할 수 있는 위험 대비가 된 의료 조직과, 장기간에 걸친 혼란 및 연쇄적인 재정적 피해에 취약한 상태로 남아 있는 위험 노출 조직 간의 레질리언스 격차가 확대되고 있음을 보여줍니다.

이 연구에서는 중대한 사이버 공격의 실제 영향, 한국의 조직이 모범 사례에 대해 사이버 레질리언스를 자체 평가한 방법, 이러한 사고를 탐지, 대응 및 복구하기 위해 취한 단계를 조사합니다. 또한 이들이 학습한 내용과 AI 및 자동화를 활용해 레질리언스를 가속화하고 그 격차를 해소하는 방식을 강조합니다.



중대한 사이버 공격:
현대 비즈니스의 새로운 현실

사이버 사고라고 해서 모두 같은 것은 아닙니다. 많은 의료 조직에서 일상적인 피싱 시도, 맬웨어 탐지 또는 시스템 중단을 거의 매일 관리합니다. 하지만 중대한 사이버 공격은 다릅니다.이번 설문조사에서는 중대한 사이버 공격이 재무, 평판, 운영 또는 고객 이탈에 영향을 미치는 사고로 정의되었습니다.

영향력이 높은 이러한 공격은 의료 조직의 경우 한국에서는 더 이상 단발성 사건이 아닙니다.

85%

응답자의 85%가 최소한 한 건의 사이버 공격을 경험했습니다

66%

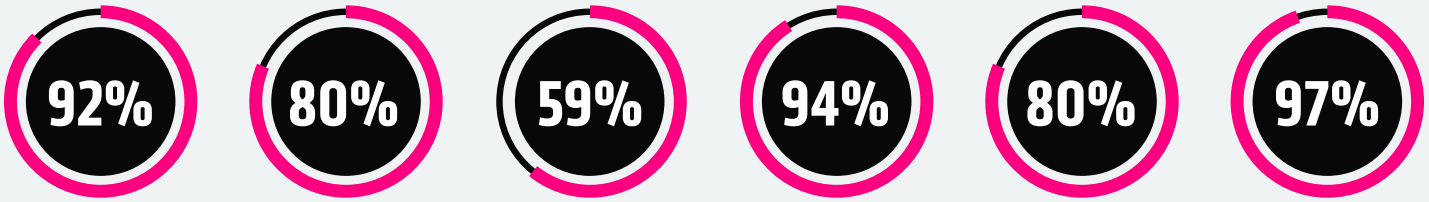
가 지난 12개월 이내에 이를 경험했습니다

35%

는 지난 12개월 동안 여러 차례의 사고를 겪었습니다

중대한 사이버 공격에 대한 실제 비용

조사 대상 조직 전반에 걸쳐 재정 및 규제 압박이 반복적으로 발생:



가 매출 감소를 격었다고 답했습니다

상장된 의료 조직의 80%가 재무 전망[1]을 수정했다고 응답했습니다

가 고객이 이탈했습니다.

가 랜섬을 지불했으며, 이는 사고당 평균 130만 달러입니다

비상장 의료 조직의 80%가 성장 이니셔티브에서 예산을 재할당했습니다

는 규제 벌금(54%) 및 소송 또는 집단 소송(39%)을 포함한 법률 및 규제상 제재를 받았습니다

[1]사이버 사고 이후 공식적으로 실적 전망치 수정안을 공개한 상장 기업은 비교적 적지만, 이러한 결과는 재무 및 운영상의 영향이 공개된 서류에 드러난 것보다 훨씬 더 크다는 점을 시사합니다.

제재에 직면한 상황에서의 자신감

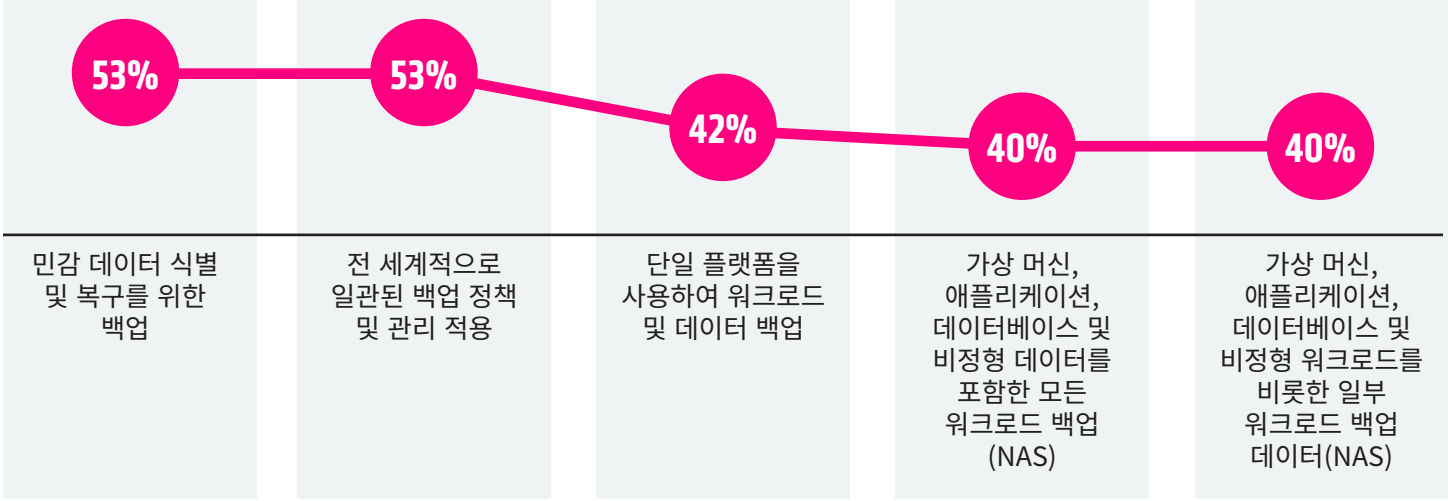
연구에서 밝혀진 재무 및 운영상 부진의 규모를 감안할 때, 조직의 레질리언스에 대한 광범위한 우려를 예상할 수 있습니다. 그러나 응답자의 거의 절반(49%)은 사이버 레질리언스 전략이 오늘날의 위협을 견딜 수 있다고 전적으로 확신했습니다. 이러한 신뢰도는 많은 동일한 조직이 지탱해 온 중요한 실질적인 영향과는 뚜렷한 대조를 이룹니다.

조직들의 대응 및 미대응 현황

우리는 겉으로 드러난 것 이상을 들여다보고 레질리언스 격차가 어디에 있는지 확인하고 싶었습니다. 이를 위해 응답자들에게 데이터 보호, 데이터 복구, 위협 탐지 및 조사, 애플리케이션 레질리언스, 데이터 위험 태세 최적화 등 사이버 레질리언스의 5가지 핵심 측면과 관련된 몇 가지주요 관행 및 기능에 대한 접근 방식을 설명하도록 요청했습니다.

하이브리드 및 멀티 클라우드 환경 전반에 걸쳐 분산되어 있는 데이터 보호

다음 중 하이브리드 및/또는 멀티 클라우드 환경에서 모든 데이터를 보호하기 위해 귀하의 조직에서 수행하는 작업은 무엇입니까?



절반이 조금 넘는 의료 기관만 복구를 위해 민감한 데이터를 식별하고 백업하고 있는 것으로 나타났습니다. 또한 같은 비율의 의료 기관이 전 세계적으로 일관된 백업 정책을 적용하고 있었습니다. 하지만 절반이 채 되지 않는 의료 기관만이 모든 워크로드를 백업하거나 단일 플랫폼에 의존하고 있습니다. 약 3분의 1을 조금 넘는 기관만 일부 워크로드만 백업하고 있습니다. 이러한 파편화는 환경 전반에 걸쳐 가시성과 정합성을 제한합니다. 안정적인 사이버 레질리언스는 Zero Trust 원칙으로 보호되는 단일 지능형 플랫폼 내에서 백업 및 복구를 통합하는 데 달려 있습니다.

데이터 복구 가능성 조치는 널리 적용되고 있지만, 성숙도에는 차이가 있습니다.

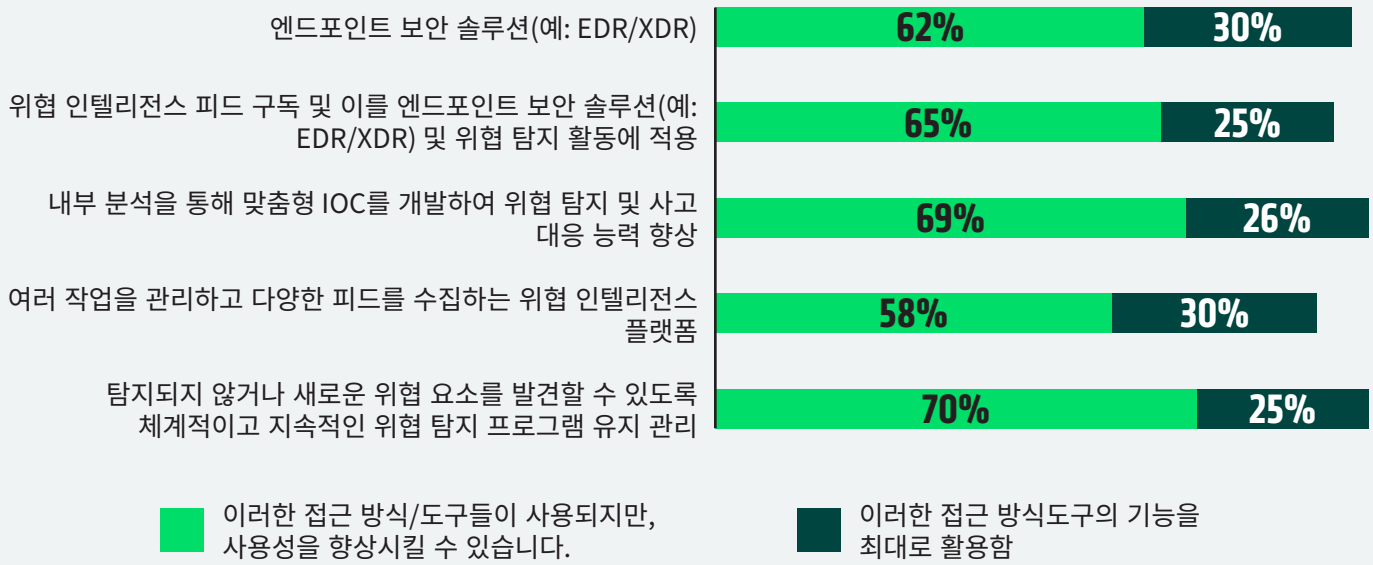
귀하의 조직은 데이터를 항상 복구할 수 있도록 무엇을 합니까?

60%	백업 및 복구 솔루션과 관련된 위험이 높은 관리 작업에 대해 추가 인증 필요
48%	백업된 워크로드에 대한 최소 권한 액세스 원칙
44%	“3-2-1 백업 규칙”을 준수(3개의 데이터 복사본, 2개의 서로 다른 매체 유형에 저장, 1개의 사본은 외부에 보관)
42%	불변성을 통해 중요한 데이터 보호
35%	백업된 워크로드에 대한 최소 권한 액세스 원칙

많은 의료 조직이 백업 환경 전반에 걸쳐 접근 제어를 강화했습니다, 또한 10곳 중 6곳은 고위험 작업을 수행하기 위해 추가 관리자 승인이 필요합니다. 절반이 채 되지 않는 의료 기관만 다중 인증을 시행하고, 3-2-1 백업 원칙을 준수하며, 중요 데이터를 불변성으로 보호하고 있는 것으로 나타났습니다. 약 3분의 1 정도만이 최소 권한 접근 원칙을 적용하고 있습니다. 이러한 격차는 완전한 복구를 더욱 불확실하게 만듭니다. 성숙한 사이버 레질리언스는 검증되고 격리되며 변조가 불가능한 복구 데이터 확보에 달려 있습니다.

활용도가 낮은 위협 탐지 및 조사 도구

귀하는 위협을 탐지하고 조사하기 위해 다음 방법 또는 도구를 어느 정도 사용하고 있습니까?



위협 탐지 및 조사 도구는 광범위하게 배포되어 있지만 활용도가 낮은 경우가 많습니다. 대부분의 헬스케어 조직에서 엔드포인트 보안, 위협 인텔리전스 피드, 구조화된 위협 헌팅 프로그램을 사용하지만, 소수 조직만이 이러한 도구를 최대한 활용하고 있습니다. 맞춤형 침해 지표(IOC)나 위협 인텔리전스 플랫폼과 같은 고급 기능의 활용은 여전히 매우 제한적인 수준에 머물러 있습니다. 안정적인 사이버 복원력은 이러한 도구를 지속적인 인텔리전스 루프에 통합하여 가시성, 탐지 및 대응을 개선하는 데 달려 있습니다.

재감염에 취약한 조직

사이버 공격에 대한 애플리케이션 레질리언스를 보장하기 위해 귀하의 조직은 어떤 조치를 취하고 있습니까?

56% 기술, 법무, 전략, 경영진 및 커뮤니케이션 이해 관계자로 구성된 다기능 팀 등과 연간 엔드투엔드 시뮬레이션 시행

54% 시스템을 운영 환경으로 복원하기 전에 보안 제어 격차 파악 및 해결

53% 중요 시스템 및 정보의 온라인 볼트 저장소로 사고 대응 및 복구

36% 사고 조사, 문제 해결 및 보안 복구를 위해 격리된 환경 사용

36% 모든 백업 데이터에 대한 불변성

헬스케어 조직들은 애플리케이션 레질리언스에 대한 접근 방식을 발전시키고 있지만, 격차는 여전히 남아 있습니다.절반이 넘는 의료 기관이 시스템을 복구하기 전에 보안 통제의 공백을 식별하고, 연간 복구 훈련을 실시하고 있습니다. 비슷한 비율의 의료 기관이 대응과 복구를 지원하기 위해 온라인 금고형 저장소를 유지하고 있습니다. 반면, 안전한 조사와 복구를 위해 격리된 환경을 활용하거나 모든 백업 데이터에 불변성을 적용하는 곳은 더 적은 것으로 나타났습니다. 이러한 격차로 인해 복구 프로세스가 재감염이나 데이터 손실에 취약해질 수 있습니다. 성숙한 사이버 레질리언스는 대비와 함께 안전하고 검증 가능한 복구 영역을 모두 갖추는 것입니다

데이터 분류가 주목받고 있지만, 여전히 발전 중인 위험 중심 활용

귀하의 조직은 데이터 검색 및 분류 접근 방식/도구를 사용하여 어떻게 전체 데이터 자산에 대한 데이터 위험 노출을 최소화합니까?

60%

사이번 공격 발생 시 백업 데이터 분류를 활용해 영향을 받은 데이터에 대한 규정 준수 의무 결정

59%

규정 준수를 위한 백업 개인 정보 보호 및 보안 위반 식별 및 해결

53%

사고가 발생하기 전에 사이버 공격의 중요성 정의 및 파악

52%

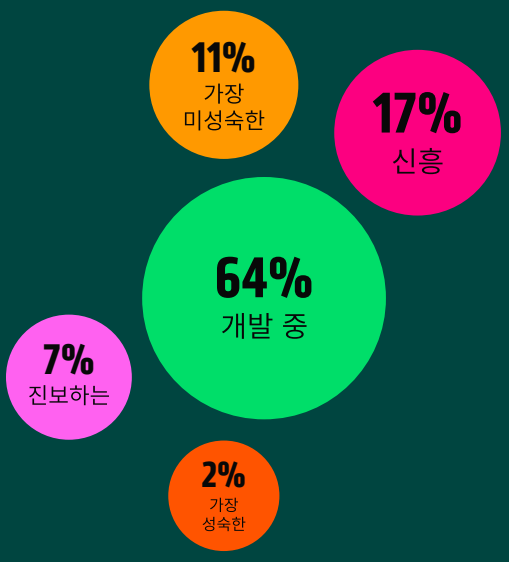
백업 시스템 식별 및 우선 순위 지정

한국의 조직에서는 규정 준수, 대응 및 복구 전반에 걸쳐 데이터 검색 및 분류 체계를 보다 전략적으로 사용하고 있습니다. 또한 10곳 중 6곳은 공격 발생 시 규정 준수를 위해 데이터 분류 체계를 활용하고 있으며, 거의 비슷한 수의 기관이 개인정보 및 보안 침해 문제에 대응하고 있는 것으로 나타났습니다. 사고 발생 전에 중대성을 정의하거나 위험 기반으로 백업 우선순위를 설정하는 기관은 그보다 더 적은 것으로 나타났습니다. 이러한 격차는 위험 중심의 분류 사용이 여전히 발전하고 있음을 시사합니다성숙한 사이버 레질리언스는 데이터 위험 상태를 최적화하고 보호, 대응 및 복구를 알리는 체계적인 접근 방식으로 분류 체계를 변화시킵니다.

레질리언스 성숙도에 대한 보다 명확한 실태

전체 점수를 매겼을 때 응답자의 답변은 사이버 레질리언스 성숙도에 대한 높은 수준의 지표로 작용하여 한국의 조직이 실제로 레질리언스를 구축하고 있거나 구축하기 위해 고군분투하고 있는 방식에 대한 명확한 패턴을 드러냈습니다. 대다수가 개발 단계에 속하는 반면, 2%만이 위험 대비 조직을 정의하는 가장 성숙하고 통합된 역량을 보여줍니다.

사이버 레질리언스 성숙도 곡선(한국)



가장 미성숙(11%): 백업, 정책 및 보안 안전장치가 주로 부재하거나 일관되지 않습니다. MFA 및 관리 제어 기능이 거의 적용되지 않고 복구에 격리 및 규정 준수가 부족한 경우가 많거나 중요성 평가는 일반적으로 간과됩니다.

도입기(17%): 일부 탄력성 관행이 마련되어 있지만 일관적이지 않습니다. 조직이 민감한 데이터를 백업하거나 글로벌 정책을 적용하거나 MFA를 사용할 수 있지만 결합하여 사용하는 경우가 드뭅니다. 위협 인텔리전스 및 규정 준수 노력은 아직 미성숙하고 분열되어 있습니다.

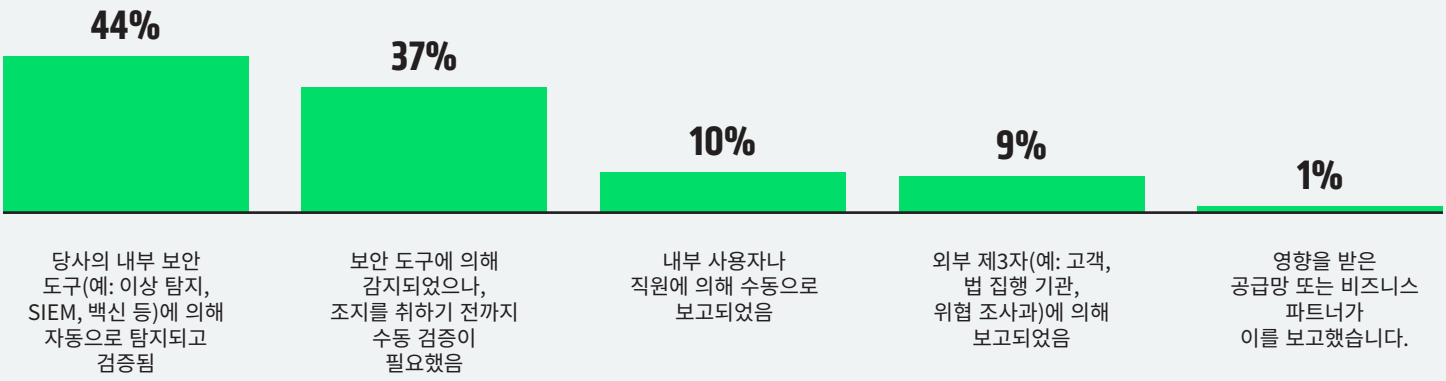
발전기(64%): 백업, 관리 권한 제어, 위협 인텔리전스와 같은 중요한 실천은 더 보편화되어 있지만 여전히 불균형합니다. 복구 환경, 규정 준수 점검, 보안 격차 수정이 불규칙적으로 적용되어, 레질리언스 노력의 효과가 부분적으로만 나타납니다. 레질리언스 노력의 효과가 부분적으로만 나타납니다.

고도화 단계(7%): 글로벌 백업 정책, 관리자 승인, 그리고 복구 전 단계의 수정 조치를을 포함한 대부분의 핵심 관행들이 일관되게 시행되고 있습니다. 위협 인텔리전스가 활용되고는 있지만 아직 완전히 최적화되지 않았으며, 격리 복구 및 완전한 규정 준수 적용 범위 측면에서는 일부 공백이 남아 있습니다.

가장 성숙(2%): 레질리언스가 체계적이고 포괄적입니다. 민감 데이터는 전 세계적으로 백업되며, MFA과 관리자 제어는 표준입니다. 위협 인텔리전스는 최대로 활용되고, 복구는 수정을 통해 안전하게 시행되며, 규정 준수 보호 조치들이 일관되게 충족되고 있습니다.

공격 상황에서의 레질리언스

팀이 공격을 식별하는 방법

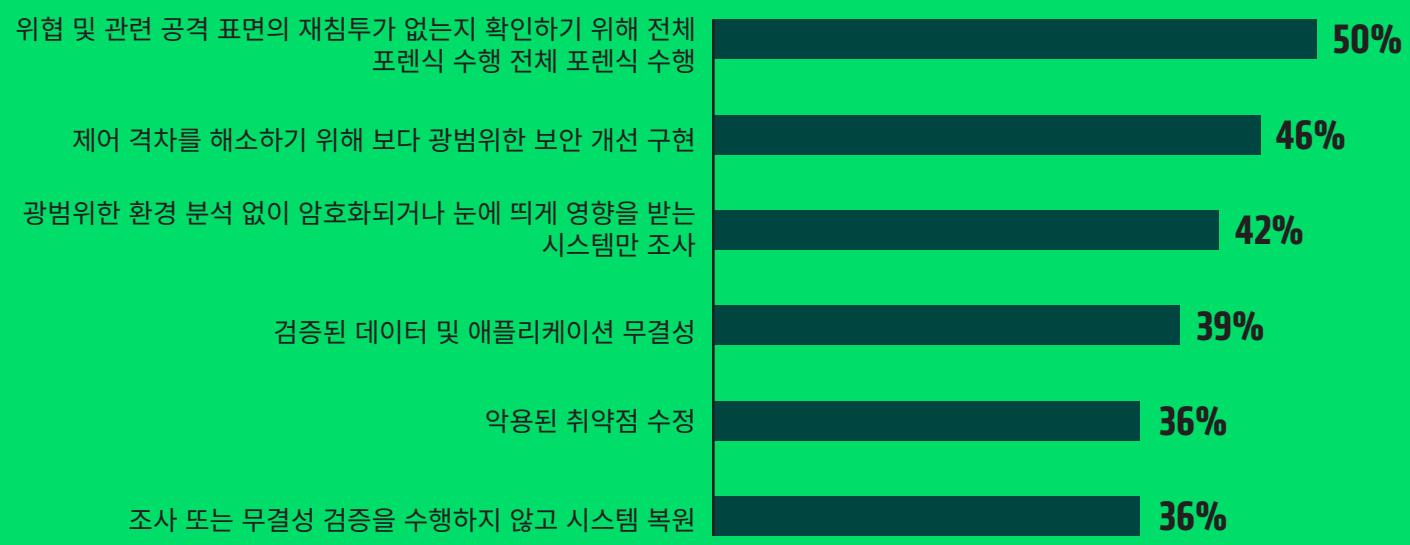


사이버 공격이 발생했을 때, 의료 기관의 거의 절반은 자사의 보안 도구가 공격을 자동으로 식별하고 확인했다고 답했습니다. 반면 3분의 1이 넘는 기관은 보안 도구에서 공격이 탐지되지만 대응 조치를 취하기 전에 수동 확인이 필요했다고 밝혔습니다. 제3자로부터의 경고는 훨씬 드물었습니다. 전반적으로 탐지는 주로 내부에서 이루어지지만, 여전히 사람의 확인에 크게 의존하는 것으로 나타났습니다.

공격 확인 후 팀이 취한 조치

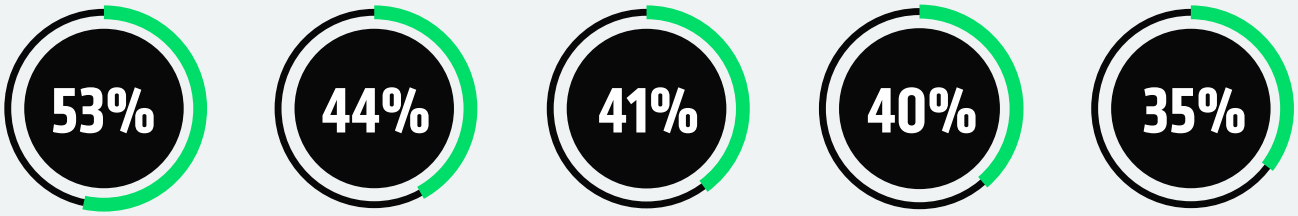
공격이 확인된 이후, 의료 기관들은 복구를 지원하기 위해 다양한 조치를 취했습니다. 절반에 약간 못 미치는 의료 기관이 클린 인프라를 복구하거나 백업 데이터를 준비 단계에 올려 복구를 시작했습니다. 절반이 넘는 기관은 안전한 조사와 복구를 위해 격리된 클린룸 환경을 구축했으며, 또한 약 10곳 중 4곳은 주요 이해관계자에게 통보하고, 감염된 시스템을 격리했으며, 공식 대응 플레이북을 가동하거나 외부 사고 대응 또는 포렌식 전문가를 참여시킨 것으로 나타났습니다. 이러한 변화는 대응 조치가 중요 단계 전반에 걸쳐 아직 완전히 표준화되지 않았음을 나타냅니다.

시스템과 데이터를 다시 온라인 상태로 전화하기 전에 취해진 조치



시스템을 다시 온라인 상태로 전환하기 전에 의료 기관은 포렌식과 개선 조치를 병행하여 수행했습니다. 의료 기관 절반이 전체 포렌식 조사를 수행했으며, 절반에 약간 못 미치는 기관은 보다 광범위한 보안 개선 조치를 시행했습니다. 하지만 데이터와 애플리케이션의 무결성을 검증하거나, 악용된 취약점을 패치하고, 눈에 보이는 영향을 받은 시스템을 넘어서는 추가 조사를 수행한 기관은 더 적었습니다. 3분의 1이 넘는 기관은 충분한 조사나 무결성 검증 없이 시스템을 복구했으며, 이는 재침해와 잔존 위험이 발생할 여지를 남기는 결과로 이어졌습니다.

공격 발생 시 팀이 직면한 어려움



팀들은 프로세스 내내 상당한 어려움을 겪었다고 답했습니다. 많은 팀이 중요한 시스템이 오프라인 상태일 때 소통하거나 협력하는 데에 어려움을 겪었습니다. 절반에 가까운 의료 기관이 복구 조치가 완료되기 전에 운영을 재개해야 한다는 압박을 받은 것으로 나타났습니다. 보안 도구 회피, 재침해, 그리고 신뢰할 수 있는 복구 지점의 부족이 이러한 어려움을 더욱 가중시켰으며, 이는 보다 강력한 레질리언스 조치의 필요성을 보여줍니다.

레질리언스 투자가 여전히 부족한 영역

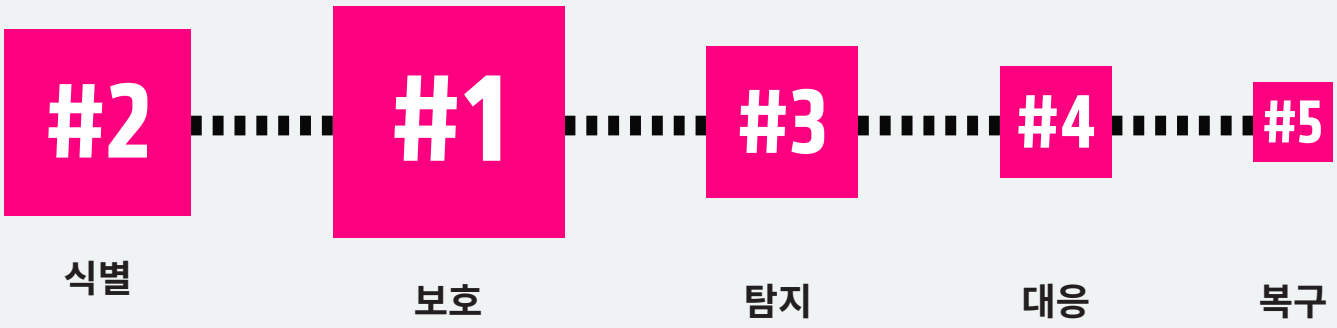
잘 준비된 헬스케어 조직도 공격이 시작되면 레질리언스를 유지하기 위해 고군분투합니다. 운영 압력이 높아지고 조정 공백, 불완전한 개선, 재감염 위험이 겹치면서 통합된 프로세스와 지속적인 보증 없이는 복구가 얼마나 취약한지 드러납니다.

이러한 패턴은 오늘날 의료 기관들이 사이버 레질리언스 예산을 어떻게 배분하고 있는지를 그대로 보여줍니다. 응답자들에게 NIST 사이버보안 프레임워크의 다섯 가지 핵심 기능인 식별, 보호, 탐지, 대응, 복구에 대해 지출을 어떻게 배분하고 있는지 질문했습니다. 대부분 여전히 예방, 보호, 탐지에 많은 투자를 하고 있는 반면, 대응과 검증된 복구에는 상대적으로 적은 예산이 투입되고 있었습니다. 그 결과 성숙도는 여전히 복구보다 방어에 치우쳐 있으며, 이는 공격 이후 단계에서 레질리언스를 강화할 수 있는 중요한 기회가 충분히 활용되지 않고 있음을 보여줍니다.

전 세계 의료 기관의 IT 및 보안 운영 의사결정자 약 400명을 대상으로 실시한 설문조사에서 이러한 현실이 드러납니다.

NIST 사이버 보안 프레임워크에 기반한 순서.

박스 크기는 사이버 레질리언스 투자 비율이 높은 순서부터 낮은 순서로 표시됩니다.



AI와 자동화가 레질리언스 승수로 부상

이 결과는 또한 한국의 조직들이 특히 탐지 속도와 응답 정밀도를 향상시키는 데 있어 AI를 사이버 레질리언스의 강력한 조력자로 보고 있다는 점을 보여줍니다. 거의 모든 응답자가 이상 징후 탐지, 사용자 행동 분석, AI 기반 위협 조사 및 대응과 같은 도구가 보안 태세를 강화하는 데 효과적이라고 평가했습니다.

자연어 위협 쿼리와 콘텍스트 분석을 수행할 수 있는 더욱 새로운 GenAI 기반 어시스턴트도 의사 결정을 단순화하고 가속화하는 방법으로 주목을 받고 있습니다. 헬스케어 조직의 61%는 사이버 공격 이후 얻은 가장 큰 교훈으로 탐지, 대응 및 복구 전반에서 더 높은 수준의 자동화가 필요하다는 점을 꼽았습니다. 이는 AI가 증폭 승수 역할을 수행하여 이러한 프로세스 전반에서 효율성, 일관성 및 효과성을 향상시키는 통합 자동화 및 오케스트레이션 플랫폼에 대한 수요 증가를 반영합니다.

앞을 내다볼 때, 대부분의 사람들은 AI가 2026년 말까지 사이버 방어에서 점점 더 전략적인 역할을 할 것으로 예상합니다. 54%는 AI가 인간의 의사 결정을 지원하고 분석 및 권장 사항을 강화하며 인간은 최종 조치를 통제할 수 있을 것으로 예측합니다. 또 다른 37%는 AI가 탐지 및 대응의 중심이 되며, 심지어 자율적인 결정을 내릴 수도 있다고 예상합니다. 이는 명확한 방향성을 시사합니다. AI는 도우미에서 사이버 레질리언스의 운영 초석으로 진화하고 있으며 탐지, 대응 및 복구 전반에 걸쳐 속도, 정확성 및 신뢰성을 향상시킬 준비가 되어 있습니다.

지금 레질리언스의 미래가 시작됩니다

한국의 조직들은 사이버 레질리언스에 상당한 진전을 보이고 있지만, 많은 조직들은 공격 후 대응, 복구 및 준비 태세 검증을 개선할 여지가 여전히 있습니다. 사이버 레질리언스는 엄청난 경쟁 우위에 해당합니다. 미래는 사람, 제품 및 프로세스에 투자하여 더 빨리 복구하고, 고객의 신뢰를 유지하며, 다른 조직이 할 수 없는 상황에서 비즈니스를 계속 진행하는 조직이 누릴 수 있는 것입니다. 사실상 중단이 불가피한 경우, 레질리언스는 단순한 보호가 아니라 성능입니다.

위기가 발생하기 전에 레질리언스를 구축하십시오.

- 랜섬웨어 레질리언스 워크숍 예약하기.
- 5단계 사이버 레질리언스 실행 계획으로 수준 높이기.
- Cohesity의 사이버 레질리언스 솔루션에 대해 알아보기

조사 방법론

COHESITY

Cohesity는 Vanson Bourne에게 2025년 9월 3,200명의 IT 및 보안 의사 결정권자에게 설문조사를 의뢰하여 이러한 조사 결과의 기초를 형성했습니다. 응답자는 미국(500개), 브라질(200개), 영국(400개), 독일(400개), 프랑스(400개), UAE/사우디아라비아(100개), 오스트레일리아(200개), 대한민국(200개), 일본(400개), 인도(200개), 싱가포르(200개)의 조직을 대표합니다. 해당 조직에는 1,000명 이상의 직원이 근무하고 있으며 직원들은 금융 서비스, 공공 부문 및 의료 분야에 중점을 둔 다양한 공공 및 민간 부문 출신입니다.

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000077-001-KO 4-2026