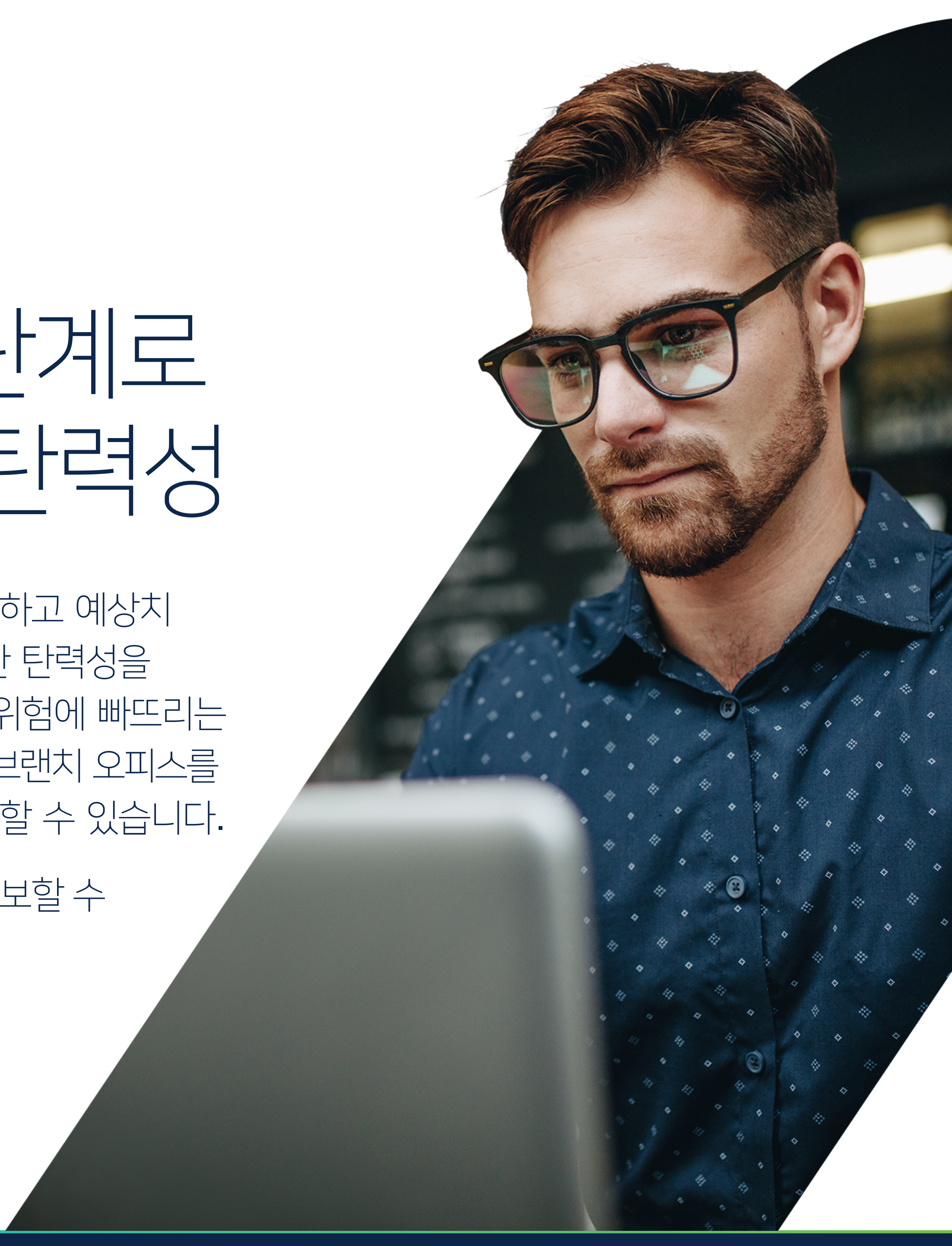
CISCO SECURE



5가지 핵심 단계로 확보하는 보안 탄력성

보안 탄력성이란 두려움 없이 변화를 시도하고 예상치 못한 사태에 대비하게 하는 힘입니다. 보안 탄력성을 갖추면 클릭 실수 한 번으로 회사 전체를 위험에 빠뜨리는 일을 방지하는 것은 물론이고, 갑작스럽게 브랜치 오피스를 설립하게 되더라도 그 즉시 안전성을 보장할 수 있습니다.

어떤 핵심 단계를 거쳐야 보안 탄력성을 확보할 수 있습니까?

1

보안 문화 조성

보안 문화가 강력한 곳에서는 직원을 문제가 아닌 해결책의 일부로 여깁니다. 직원들이 담당하는 역할을 인지하는 것이 중요합니다. 이는 피싱 시도, 잠재적 악성코드 및 기타 사고를 정기적으로 보고함으로써 확인할 수 있습니다. 반대로 빈번한 보안정책 위반과 회피책은 보안 문화가 빈약하다는 증거입니다.

46% | 보안 문화를 조성한 조직은 탄력성이 46% 향상되었습니다.

출처: 시스코 보안 성과 보고서 3권

2

경영진 차원의 지지 확대

최고 경영진의 지원이 부족하다고 응답한 조직은 충분한 지원을 받는 조직보다 보안 탄력성 점수가 39% 낮습니다.

보안 탄력성은 보안 팀만의 책임이 아닙니다. 최고 경영진의 지지는 필수입니다.

경영진 차원의 지지를 확대하는 방법

- 경영진의 관심사 파악
- 비즈니스 중심 성과가 탄력성 계획의 일부임을 설명
- 아무런 행동을 하지 않을 때 위험성을 명확히 전달
- 감수할 수 있는 위험과 그럴 수 없는 위험에 대해 논의

3

필요한 리소스 확보

예상치 못한 사이버 사고에 더 철저히 대응하기 위해 내부 인력과 리소스를 초과 유지할 경우와 그러지 않을 때의 차이는 매우 큽니다.

조직에서 예상치 못한 이벤트에 대처할 추가적인 인력을 유지하기 어려울 수 있습니다. 외부의 사고 대응(IR) 서비스를 이용하는 기업은 보안 탄력성이 평균 11% 높은 것으로 나타났습니다. 전화 한 통이면 도움을 받을 수 있도록 신뢰할 수 있는 IR 서비스 제공업체와 유지 계약을 체결하는 것을 고려해 보십시오.

15% | 초과 자원을 유지할 수 있는 조직은 필요할 때 활용할 수 있는 "유연한" 자원이 없는 조직보다 보안 탄력성 점수가 평균 15% 더 높습니다.

출처: 시스코 보안 성과 보고서 3권

4

위협 정보를 탐지 및 대응 능력으로 활용

탐지 및 응답 기능은 찾아야 할 대상과 찾을 방법을 알고 있을 때 가장 효율적으로 작동합니다. 이를 위해 양질의 사이버 위협 정보를 기대하는 사람들이 많습니다.

우리는 어떤 보호 조치도 완전무결할 수 없으며, 위협이 어떤 방식으로 변화하고 진화하는지 완전히 예측할 수도 없다는 점을 인정해야 합니다. 대비가 핵심입니다. 조직의 시스템에 단일 장애 지점이 없도록 하면, 위협으로 인해 구성 요소 하나가 작업이 중단되어도 작업을 계속 진행할 수 있습니다.

통합적인 확장 탐지 및 대응(XDR) 솔루션의 두 가지 핵심 요소

- 사이버 위협 정보
- 자동화/조정

이러한 기능을 갖춘 조직은 XDR 솔루션을 갖추지 않은 조직보다 전체적인 탄력성 점수가 45% 높았습니다.

5

관리가 간편하고 유연한 기술에 집중

다행히도 온프레미스를 많이 사용하는 환경과 클라우드를 많이 사용하는 환경 간에는 보안 탄력성 성과에 차이가 없었습니다. 두 환경 모두 보안 탄력성은 동일합니다.

그러나 단순하고 마찰이 없는 상태를 유지하는 것이 두 인프라 유형의 핵심 성공 요인입니다.

다단계 인증(MFA)은 조직의 탄력성을 높일 수 있는 최적의 방법에 속하며, 롤아웃과 관리도 쉽습니다.

11% | MFA를 구축한 경우 보안 탄력성 점수가 11% 향상되었습니다.

출처: 시스코 보안 성과 보고서 3권

자세한 내용은 다음 eBook을 참조하십시오.
Cisco Secure를 통한 보안 탄력성 구축 가이드

Cisco Secure는 전 세계의 조직이 예상치 못한 상황에 대비할 수 있도록 지원하합니다. 조직이 이러한 상황을 피하는 것이 아니라 직면하고, 빠르게 적응하여 대처하게 하는 것을 목표로 합니다.

1043249609 | 03/23

CISCO The bridge to possible