Gigamon

2018 사이버 위협 방어 보고서

CyberEdge Group의 5번째 연례 사이버 위협 방어 보고서는 IT 보안 전문가가 조직의 보안 상태, 효과적인 사이버 위협 방어 체제를 수립할 때 직면하는 문제점 및 이러한 문제를 해결하기 위해 필요한 계획을 인식하는 방법에 대해 다룹니다. 올해 보고서를 읽고 주요 결과에 대해 알아보십시오.

불가피한 손상

조직은 급속도로 사이버 공격의 피해를 입고 있습니다... 앞으로도 비슷한 현상이 벌어질 것으로 예상됩니다.

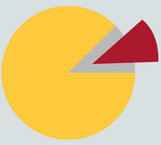
2017년에 최소 1번의 손상을 입음 — 77.2%

2017년에 6번 이상 손상을 입음 — 27.4%

EXPECT TO BE HIT IN 2018 — 62.3%

보안 예산의 증가

응답에 따르면 2018년에 기업은 보안 제품, 서비스 및 인력에 대한 비용 지출을 평균 4.7% 이상 확장하고 있습니다.



12%
보안에 대해 할당된 IT 예산의 평균적인 비율

여전히 남아 있는 수많은 문제

문제 #1: 수행할 일이 너무 많음

오늘날 기업의 기술 공간이 확장될수록, 방어해야 할 공격의 범위도 확장됩니다.

가장 취약한 보안 상태로 평가된 인프라

1. 컨테이너
2. 모바일 장치
3. 클라우드 인프라

가장 심각한 결함이 있는 프로세스/기능

1. 애플리케이션 개발 및 테스트(SDLC)
2. 공격 범위 축소
3. 악의를 가진 내부자/내부자 공격 탐지

가장 큰 장애물

분석할 데이터가 너무 많음

문제2: 숙련된 인력 부족

전 세계적으로 사이버 보안 전문가가 부족한 상황에서 보안에 추가적인 비용을 지출하는 것은 작은 위안이 됩니다.

숙련된 인력의 부족은 사이버 위협을 방어하는 데 가장 큰 장애물으로 평가되었습니다.

81% 숙련된 IT 보안 전문가 부족을 경험하고 있는 조직

IT 보안 기술 부족으로 인한 수직 산업의 타격

교육	87%
기술	85%
제조	82%
금융	81%

문제 #3: 올바른 솔루션에 대한 지속적인 검색

모든 적절한 장소에 충분한 기술투자를 하고 이를 최대한 활용할 수 있도록 관리하는 일은 거의 모든 조직이 해결해야 할 과제입니다.

32%
1/3 이하의 조직만이 사이버 위협 방지 작업에 적절한 투자를 했습니다.

91%
10개 중 9개 이상의 조직은 클라우드 보안과 관련된 중대한 문제를 경험하고 있습니다.

83%
5개 중 4개 이상의 조직은 잘 알려져 있는 취약점을 적시에 패치하는 데 어려움을 겪고 있습니다.

발전을 위한 경로 준비

오늘날 기업을 괴롭히는 IT 보안 문제를 해결하기 위해서는 "작업을 무사히 끝내는" 사이버 위협 방어 체계가 필요합니다. 이를 위해 다음과 같은 작업을 수행할 수 있습니다.

1. 전체적인 가시성 전달
2. 보안 인프라 오프로딩 및 단순화
3. 새로운 보안 도구 개발 및 통합 가속화
4. 오케스트레이션 및 자동화 활성화

전체 보고서 다운로드:
www.gigamon.com/cdr2018

CYBEREDGE GROUP