2019년 사이버 위협 방어 보고서

전체 요약

CyberEdge Group 보고서

플래티넘 스폰서:

Gigamon®

설문 조사 통계

- 1,200명의 적격한 IT 보안 의사 결정자 및 실무자의 응답
- 500명 이상의 직원을 보유한 조직
- 북미, 유럽, 아시아 태평양, 중동, 라틴 아메리카 및 아프리카의 17개 국가 내 조직
- 19개 산업 내 조직

"2019년에 가장 큰 호응을 얻은 기술 (예: 도입률이 가장 높은 기술)은 SSL/TLS 암호 해독 플랫폼, 고급 맬웨어 분석/ 샌드박스, 기만 기술/ 분배 허니팟입니다."

– 2019 CDR

CyberEdge Group의 6번째 연례 사이버 위협 방어 보고서는 IT 보안 전문가가 사이버 위협을 인식하고 이에 대한 방어 계획을 수립하는 방법에 대해 자세히 살펴봅니다. 2018년 11월에 1,200명의 IT 보안 의사 결정자 및 실무자를 대상으로 실시된 설문 조사 기반의 이 보고서는 IT 보안 팀이 동료 직원과 비교하여 각자의 인식, 우선순위 및 보안 상태를 더 효과적으로 파악하는 데 사용할 수 있는 수많은 통찰력을 제공합니다.

주목할 만한 결과

- **3가지 사이버 위협.** 응답 조직은 사이버 위협의 11가지 범주 중 맬웨어에 가장 큰 우려를 보이고 있으며 랜섬웨어 및 피싱이 그 뒤를 잇고 있습니다(표 1 참조).
- **건전한 보안 예산.** 평균 보안 예산은 2019년에 4.9% 증가할 예정이며, 평균적으로 조직의 전체 IT 예산에서 12.5%를 차지하고 있습니다.
- **위협 사냥을 방해하는 장애물.** 효과적인 위협 사냥에 가장 큰 장애물은 조직이 관련 도구 도입 및 통합에 어려움을 겪는다는 것입니다.
- **가장 많이 요구되는 보안.** 2019년에 제일 먼저 확보할 계획이 있는 기술은 고급 보안 분석입니다.
- **기술 부족 악화.** 5개 중 4개 이상의 조직(84.2%)은 숙련된 IT 보안 전문가 부족 문제를 경험하고 있으며, 특히 교육(91.3%), 금융(87.5%) 분야가 가장 큰 타격을 입고 있습니다.

피할 수 없는 문제 해결

결론적으로 사이버 위협으로부터 자유로운 조직은 없습니다. 지난 한 해 동안 사이버 공격에 의해 조직의 네트워크가 손상된 횟수를 추산해 달라고 요청했을 때 응답자의 약 4/5(78%)는 최소 1번 손상을 입은 적이 있다고 대답했으며 약 1/3(32%) 이상은 6번 이상 손상을 입은 적이 있다고 대답했습니다. 내년에도 이처럼 우울한 전망이 예상됩니다. 2019년에 사이버 위협의 침입을 "받지 않을 것 같다"고 응답한 조직은 12%에 불과합니다. 최근 공격이 성공하는 일은 피할 수 없기 때문에 필수가 아니라 하더라도 조직이 위협 감지 및 사고 대응 활동을 서두르기 위해 의미 있는 단계를 취하는 것이 합리적입니다.

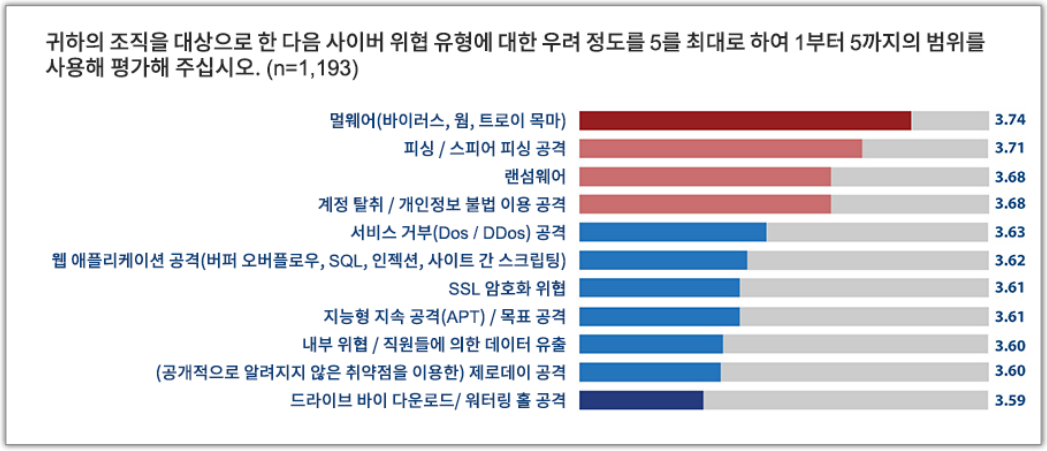

그림 1: 가장 큰 우려가 되는 사이버 위협

보이지 않는 곳 제거

감지 및 응답 속도를 높이는 것은 대부분 전반적인 가시성을 높이는 것부터 시작합니다. 위협이 활동하고 이들 "소프트웨어"가 숨어 있는 곳, 즉 조직 네트워크의 구석구석에서 무슨 일이 일어나는지 자세히 파악하지 못한다면 (예방은 말할 것도 없고) 이들을 감지할 수 있다는 보장은 거의 없습니다. 조직의 물리, 가상, 클라우드 인프라 전체에 걸친 깊이 있고 한결같은 가시성은 네트워크 데이터를 다루는 보안 팀이 차이를 만들 수 있는 핵심입니다. 물론 이 문제를 해결하는 데 보이지 않는 곳을 제거하는 것이 중요합니다. 대부분의 조직에서 주로 암호화된 네트워크 트래픽이 이에 해당합니다. 해당 주제에 관한 질문에서 무려 응답자 73.9%가 효과적인 SSL/TLS 트래픽 해독이 조직의 남아 있는 사이버 위협 검사에 도움이 될 것이라고 동의했습니다. 따라서 효율적인 암호 해독의 필요성(및 중앙화)은 오늘날의 현대화된 컴퓨팅 환경에서 암호화 트래픽이 증가함에 따라 그 비율에서도 순수한 양에서도 증가 추세를 보이고 있습니다.

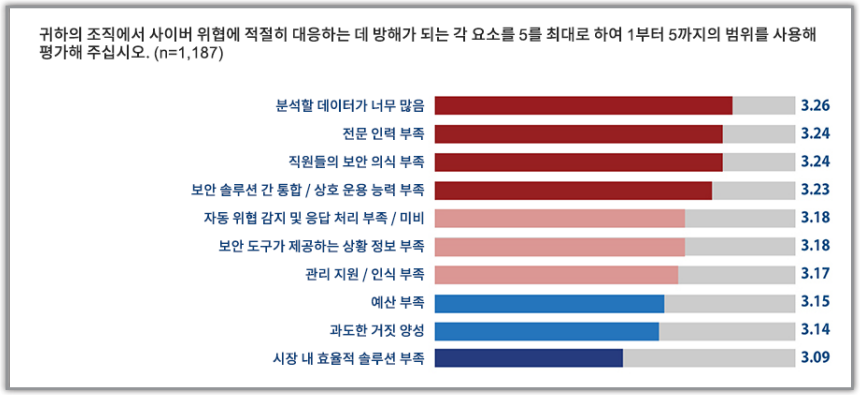

그림 2: 효과적인 사이버 위협 방어 체계 수립을 저해하는 요인

신호 대 잡음비 증가

폭넓은 가시성 확보는 빠른 감지 및 응답 능력의 핵심이지만 조직에는 피해 없이 이 문제를 해결해야 합니다. 특히 오늘날 보안 팀으로서는 무분별하게 엄청난 양의 보안 데이터를 분류하는 일은 피해야 합니다. 설문 조사 응답자들은 "분석할 데이터가 너무 많은" 것을 효과적인 사이버 위협을 방해하는 가장 큰 장애물이라고 지적했습니다(그림 2 참조). 따라서 과도한 보안 데이터는 보안 운영 관리자에게 큰 부담을 줄 수 있습니다. 성능 및 능력 향상의 필요성이 증가함에 따라 조직 내 보안 도구 및 인프라 비용과 복잡성도 늘어나고 있습니다. 이 어려운 문제들을 성공적으로 해결하기 위해서는 차세대 네트워크 패킷 중개인 등 보안 문제를 완벽하게 다루면서도 쓸데없는 분배 및 데이터 처리, 보안 이벤트를 최소화하는 솔루션이 필요합니다. 즉 도구나 팀에 부담을 주지 않고 필요한 정보 및 통찰력을 제공하는 것이 중요합니다.

무료 보고서

전체 2019 사이버 위협 방어 보고서의 무료 사본을 확인하려면 www.gigamon.com/cdr2019로 이동하십시오.

기가몬 소개

기가몬은 네트워크 가시성 솔루션의 선두 주자로서, 꼭 필요한 강력한 통찰력을 제공하며 기업 네트워크를 보호하고 강화합니다. 기가몬의 솔루션은 위협 감지 및 사고 응답 속도를 높여 물리, 가상, 클라우드 네트워크 전반에 걸친 고객 인프라 성능을 최대화하여 고객 역량을 강화합니다. 기가몬은 2004년부터 선두적인 서비스 제공자, 정부, 기관은 물론 포춘 100대 기업 중 80퍼센트의 기업, 네트워크 운영, 보안 운영 팀 등을 고객으로 확보해 왔습니다. 자세한 내용은 www.gigamon.com을 참조하십시오.

CyberEdge Group 소개

CyberEdge Group은 수상 경력에 빛나는 설문 조사, 마케팅 및 출판 전문 회사로서 정보 보안업체 및 서비스 제공업체의 요구사항에 부합하는 서비스를 제공하고 있습니다. CyberEdge Group의 전문 컨설턴트는 고객에게 수익을 높이고 경쟁 우위를 선점하며 판매 주기를 줄이는 데 필요한 이점을 제공합니다. 자세한 내용은 www.cyber-edge.com을 참조하십시오.

CYBEREDGE GROUP