네트워크 보안 모니터링: 가시성 격차 없애기

ESG의 네트워크 보안 모니터링 추세 보고서 하이라이트

2016년 Cisco는 ESG(Enterprise Strategy Group)와 함께 200명의 IT 및 사이버 보안 의사 결정권자를 대상으로 설문 조사를 시행했습니다. 목표: 현재의 네트워크 보안 모니터링 방식 평가 네트워크 보안 모니터링 추세 보고서를 읽으면 네트워크 모니터링이 왜 중요한 보안 방식이고, 당면 과제는 무엇이며, 최고 정보 보안 책임자가 왜 대규모 투자를 하는지에 대한 인사이트를 얻을 수 있습니다.

네트워크 보안 모니터링 노력에 장애가 되는 가시성 격차

보안 전문가는 네트워크 보안 모니터링에 높은 가치를 두고 있습니다. 80%는 네트워크 보안 모니터링이 조직의 전반적인 사이버 보안 전략에 중요하다고 생각합니다.

그러나 네트워크 보안 모니터링은 어렵습니다. 대부분의 보안 전문가도 2년 전보다 지금이 더 어렵다고 말합니다. 그 이유에는 악성코드의 양, 네트워크 트래픽, 기존 보안 툴을 우회하는 공격의 수가 증가하는 등의 외부 요인이 포함됩니다.

그러나 네트워크 보안 모니터링을 더욱 어렵게 만드는 조직 내부의 요소도 존재합니다. 주요 요소로 네트워크 사각지대 및 가시성 부족을 들 수 있습니다.

네트워크 보안 모니터링의 당면 과제

Q 12: 네트워크 보안 모니터링과 관련하여 귀사의 가장 큰 문제는 다음 중 무엇이라고 생각하십니까?

데이터에 대해 좀 더 자세히 살펴보면 보안 조직에서 경험하는 다음과 같은 가장 큰 가시성 격차가 있습니다.

네트워크 보안 모니터링 가시성 격차

Q 13: 네트워크 보안 모니터링 측면에서, 귀사에서는 어디에 가장 큰 가시성 격차가 존재한다고 생각하십니까(즉, 조직에서 적절한 양의 네트워크 데이터를 캡처, 처리 또는 분석하지 못하는 영역)?

네트워크 사각지대 제거는 네트워크 보안 모니터링을 성공적으로 수행하고 지능형 위협으로부터 조직을 보호하기 위한 핵심 사항입니다. 그러나 대부분의 보안 툴은 이러한 가시성을 제공할 수 없습니다. 가시성 격차 해소 방법을 알아보려면 Eliminate Network Blind Spots 백서를 읽어보고, 네트워크 가시성 및 보안에 대한 Cisco Stealthwatch™ System 및 Cisco© ISE(Identity Services Engine)에 대해 알아보십시오.

ESG 전체 보고서 읽기:
네트워크 보안 모니터링 추세.

(11/16/16-r02)