
cybereason
DOOSAN
2023
랜섬웨어와
보안 운영 센터(SOC) 현대화
*Security Operations Center
랜섬웨어가 보안 운영 센터(SOC) 현대화를 어떻게 이끌까?

Contents

개요

모든 보안 운영 센터(SOC)는 지속적으로 전문 인력 부족, 가시성 및 자동화 취약성, 무분별한 도구 확장, 경고 알람 과부하 문제를 직면해왔습니다.

이로 인해 경쟁자보다 앞서고, 보안 투자의 수익성을 보여주고, 직원의 번아웃을 방지하기 위해 끊임없이 노력해야하는 상황이 지속되고 있습니다.

사이버리즌은 8개국 1,203명의 보안 전문가들을 대상으로 현재 보안 운영 센터(SOC)가 직면한 과제와 이들이 현대화 계획에 미치는 영향에 대해 설문 조사를 실시했습니다.

응답자의 절반 가까이(49%)가 매일 가장 많이 처리하는 사고 유형으로 랜섬웨어를 뽑았으며, 공급망 공격(46%)이 그 뒤를 차지했습니다. 응답자의 37%는 경고 알림에 매일 대부분의 시간을 소비한다고 답했으며, 31%는 타깃 공격을 가장 흔한 보안사건으로 꼽았습니다.

1,203 보안 전문가

8 개국

가장 흔한 사건

- 렌섬웨어 **49%**
- 공급망 공격 **46%**
- 일상적인 보안 문제 **37%**
- 타깃 공격 **31%**

주요 요점

57%

응답자 57%는 랜섬웨어를 해결하는 데 평균적으로 3~6시간이 소요된다고 답했습니다.

59%

응답자 59%는 2시간에서 1일이 걸린다고 답했으며, 19%는 3~7일 정도 소요된다고 응답했습니다.

88%

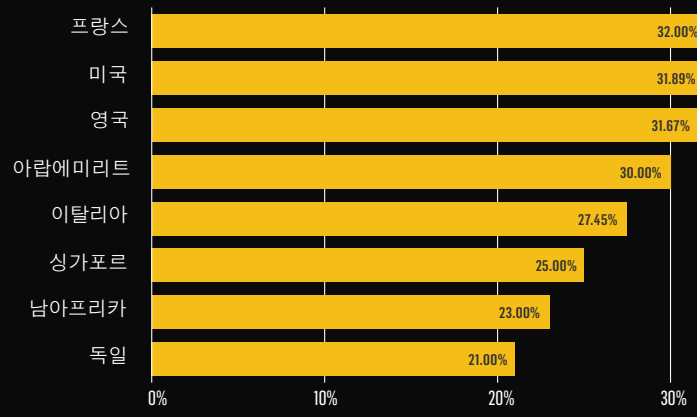
응답자 88%는 랜섬웨어 공격으로 인해 휴일 혹은 주말에 근무해왔다고 답했습니다.

기업의 3분의 1 이상은 매일

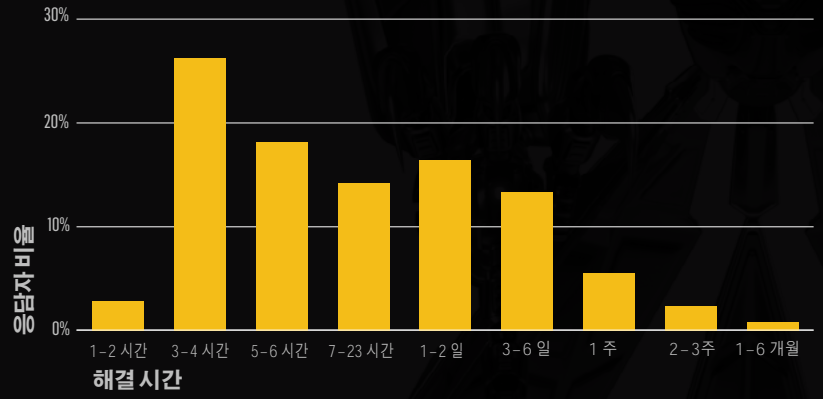
10,000 - 15,000

건의 보안 경고를 받고 있습니다.

랜섬웨어가 자동화 및 대응 속도 향상의 필요성을 증가시켰다고 응답한 비율



랜섬웨어 공격을 해결하는 데 걸리는 평균 시간



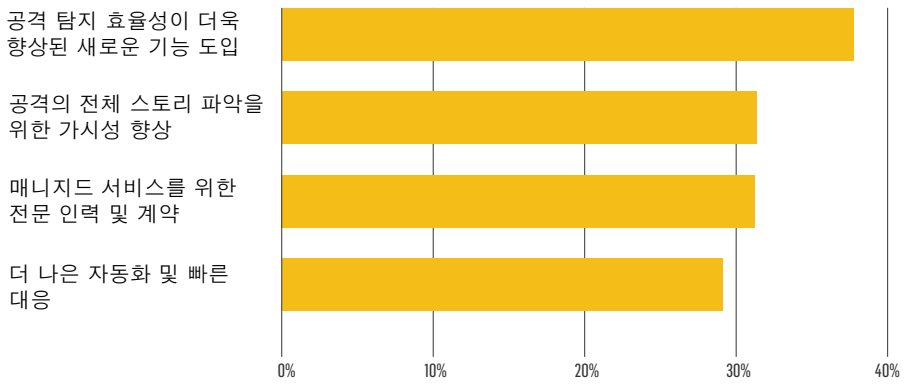
랜섬웨어와 역량 기반 보안 운영 센터

앞장에서 언급된 챌린지들은 기업이 보안 운영 센터(SOC) 현대화에 투자해야 하는 이유를 보여줍니다.

오늘날의 SOC 구축 혹은 현대화는 특정 보안 툴을 사용해 중앙 집중식으로 운영되는 것이 아니며, 각 조직에서 요구하는 특정 기능, 역량, 결과를 제공해야 합니다.

설문 조사 응답자의 58% 이상이 보안 운영 센터(SOC)가 랜섬웨어 및 공급망 공격 대응에 대부분의 시간을 소비한다고 답했습니다. 랜섬웨어가 보안 운영 센터(SOC) 현대화 계획에 어떤 영향을 미쳤는지를 묻는 질문에는 아래 네 가지 요구 사항을 구체적으로 언급했습니다:

Q1 랜섬웨어 등장으로 SOC 기술에 어떤 변화가 필요해졌나요?



38%
공격 탐지 효율성이 더욱 향상된 새로운 기능 도입

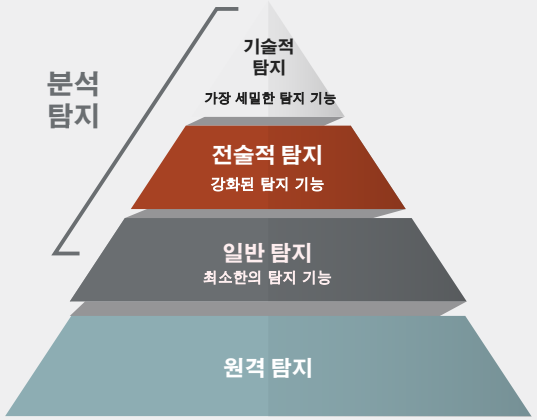
31%
공격 전체 스토리에 대한 가시성 향상

31%
매니지드 서비스를 위한 전문 인력 및 계약

29%
더 나은 자동화 및 빠른 대응

보안 운영센터(SOC) 구축, 현대화 또는 운영 프로세스는 비즈니스 및 위협 환경에 따라 변화하는데 포스트 코로나 시대 보안 운영 센터(SOC) 목적은 명확합니다:
탐지, 예방, 가시성 및 자동화 기술 등 역량를 바탕으로 업계를 선도하는 탈중앙화 조직을 구성하고, 이 모든 기술을 매니지드 서비스로 강화하는 것입니다.

새로운 탐지 기능의 필요성



분석 탐지는 더 광범위한 데이터 세트에서 구축되며 기술 + 전술 탐지의 조합을 의미합니다. 보안 운영 센터(SOC)는 탐지력 강화를 위해 발생한 일에 대해 세밀한 시각이 필요합니다.

설문 응답자 38%는 사이버 공격 탐지 효율성이 더욱 향상된 새로운 기능을 도입할 계획이 있다고 밝혔습니다.

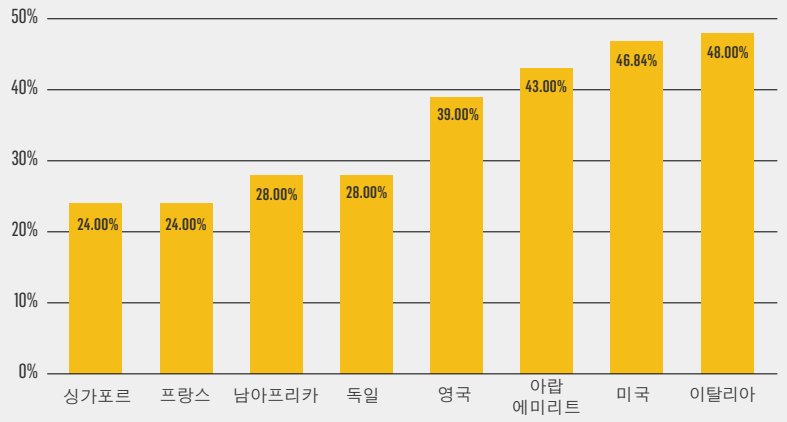
현대 보안 운영 센터(SOC)는 비즈니스 리스크와 우선순위에 따라 위협을 탐지하고 대응해야 합니다.

기존 엔드포인트 보안 솔루션은 이미 알려진 공격을 기반으로 구성된 IOC(Indicators of Promise)에 의존한 반면, 최신 탐지 기능은 IOC와 더불어 IOB(Indicators of Behavior)를 활용하여 미묘한 공격 징후까지 탐지합니다.

즉, 악의적인 인간 및 기계 활동을 표면화하여 이전에 보지 못했던 공격을 탐지하고, 중대한 침해 이벤트로 확산되기 전에 공격 초기 단계에서 종료시키는 것입니다.

랜섬웨어와 같은 오늘날의 정교한 위협들을 해결하기 위해서는 즉시 악성 활동을 탐지할 수 있어야 합니다.

Q2 랜섬웨어 때문에 새로운 탐지 기술 배포/도입 계획을 세웠습니까?



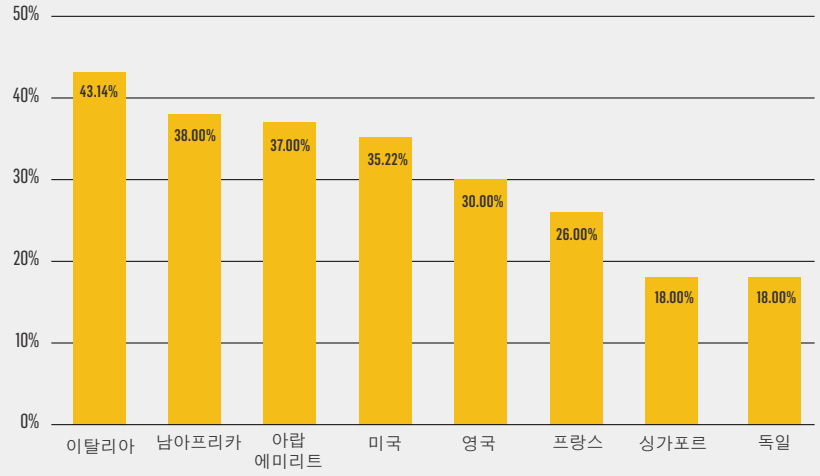
공격 전체 스토리 파악을 위한 가시성 향상

설문 응답자의 31%는 랜섬웨어의 위협으로 공격 전체 스토리 파악을 위해 더 나은 가시성이 필요하다고 답했습니다.

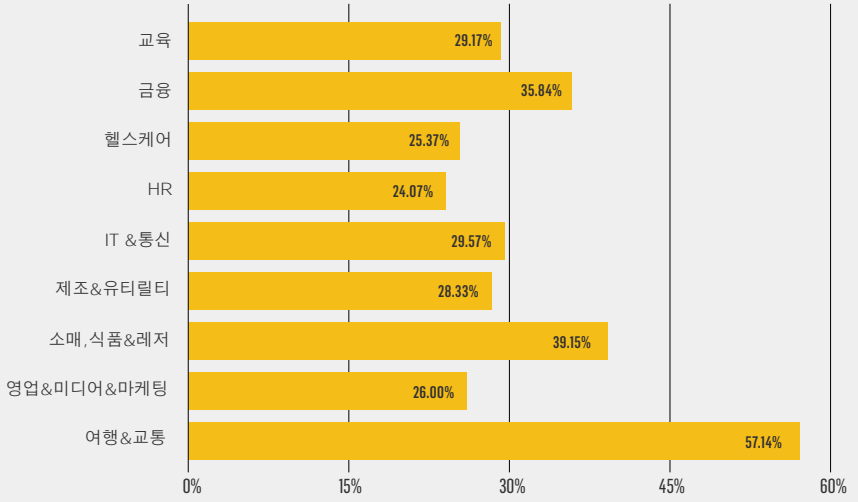
솔루션의 가시성 평가는 전체적인 공격 맥락, 공격의 시작점, 영향 받은 내용, 이벤트 타임라인, 공격 체인의 세부 정보 등에 대해 정량화하여 이루어집니다.
운영 중심 접근 방식을 활용하면 영향을 받는 모든 사용자 및 장치를 포함하여 A부터Z까지 공격 전체 스토리를 단일 화면에서 확인할 수 있습니다.

즉, 공격 전체의 맥락에서 사용자, 장치, ID 및 네트워크 연결 등 모든 곳에서 일어나는 악의적인 작업에 대해 탐지가 가능함을 의미합니다.

Q3 공격 전체 스토리 파악을 위해 더 나은 가시성이 필요하다고 답한 국가별 응답자 비율



Q4 공격 전체 스토리 파악을 위해 더 나은 가시성이 필요하다고 답한 산업별 응답자 비율



더 많은 전문 인력과 서비스 필요성

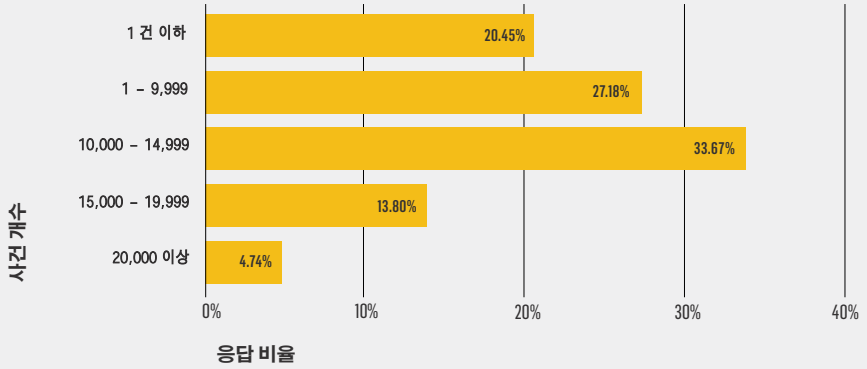
설문에 응답한 보안전문가 3분의 1 이상이 하루 평균 10,000~15,000건의 보안 경고를 받고 있습니다. 수많은 경고는 정보 과부하를 낳는데 이는 보안 담당자의 피로도를 높이는 가장 큰 원인입니다.

SIEM(Security Information and Event Management) 플랫폼은 많은 중복 경고 및 오탐지를 생성하는데, 추후 심각한 보안 사건으로 이어질 수 있는 작은 움직임라도 놓치지 않기 위함입니다. 즉, SIEM은 의심스러운 모든 움직임에 경고 알림을 보내고, 보안 분석가는 수 많은 경고 알림 속 진짜 악의적인 움직임을 찾아내야 합니다.

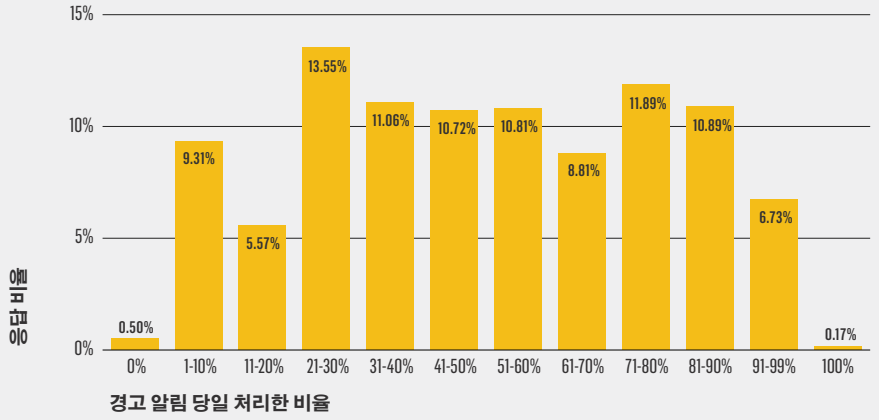
경고 과부하 문제는 사이버 보안 전문가 인력난으로 더욱 심각해지고 있습니다. 보안업계는 세계적으로 약 350만 명의 보안 전문가가 부족한 상황이며, 특히 Tier III 분석가 채용은 매우 어렵고, 이들의 근속 유지는 더욱 어렵습니다. 정보 과부하와 공격을 탐지해내야 한다는 압박감이 보안 전문 인력의 대거 이탈을 야기하기 때문입니다.

이러한 문제점은 MDR(Managed Detection and Response) 서비스에 대한 관심을 높였습니다. MDR 서비스가 경고 분류 및 우선순위 작업에 대한 부담을 덜어주기 때문입니다. 이때 보안 전문가는 우선수위가 높은 다른 보안 작업에 집중할 수 있습니다. 또한 MDR은 독립형 보안 솔루션 또는 기존 보안 운영 센터(SOC)에 대한 추가 보안 계층으로, 모든 조직의 보안 상태를 즉시 강화할 수 있습니다.

Q5 보안 사고가 하루에 몇 건 발생하나요?



Q6 경고 알림을 받은 당일에 처리되는 비율은 어떻게 되나요?



더 빠른 대응을 위한 자동화 강화

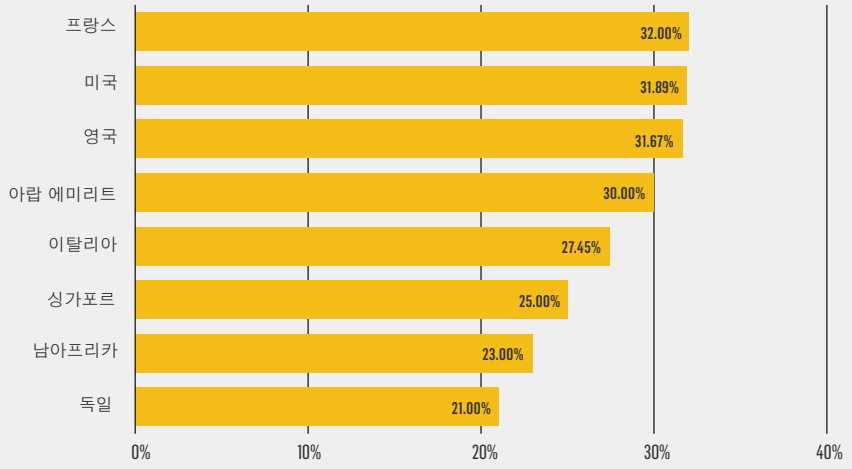
응답자의 29%는 랜섬웨어가 자동화와 더 빠른 대응에 대한 필요성을 높였다고 답했습니다.

특히 랜섬웨어와 같은 정교한 위협에 효과적으로 대응하기 위해서는 추가 처리 시간이나 보안 분석가의 개입 없이 악의적인 활동을 즉시 탐지할 수 있는 솔루션을 갖춰야합니다.

또한, 외부 SOAR(Security Orchestration, Automation, and Response) 솔루션이 아닌 기업 맞춤 플레이북을 기반으로 모든 엔드포인트와 사용자의 사고 대응이 자동화 되어야 합니다.

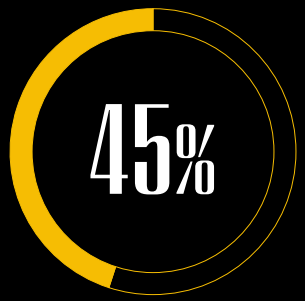
고급 자동 분석은 경고의 노이즈를 줄이고 악의적인 작업을 탐지 및 대응하는 데 필요한 모든 정보를 간결하게 제시합니다. 해당 기능을 갖추면 보안 분석가는 MTTR(Mean Time to Response)을 크게 줄이는 동시에 분석 정확도는 높일 수 있습니다.

Q7 랜섬웨어가 자동화에 대한 필요성을 높였나요?

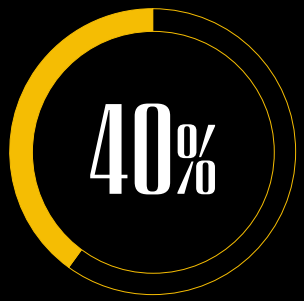


참고

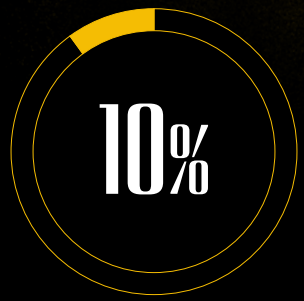
이 보고서는 임직원 700명 이상 규모 회사에서 근무하는 1,203명의 사이버 보안 전문가를 대상으로 한 글로벌 설문조사를 바탕으로 제작되었습니다.
해당 조사는 2022년 9월 27일부터 2022년 10월 4일 사이에 실시 되었으며, 응답자 구성은 다음과 같습니다.



고위 관리자/
전문가



책임자 레벨의
전문가



기업 오너

중간 관리자/전문가