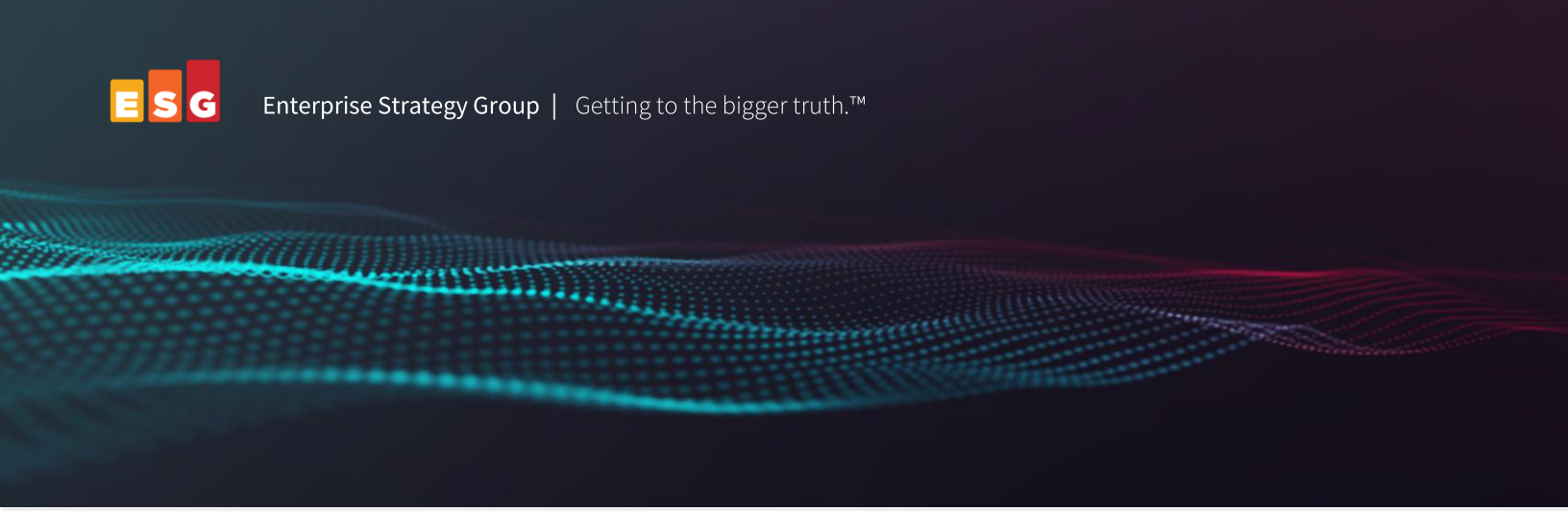


ESG RESEARCH INSIGHTS PAPER

효과적인 위협 탐지 및 대응에 대한 XDR 전망

저자: Jon Oltsik, ESG 선임 분석가 및 초빙 연구원

2020년 12월

이번 ESG Research Insights Paper는 Fortinet에서 의뢰하였으며,
ESG의 라이선스에 따라 배포됩니다.

목차

종합 요약

2020년 10월에 Enterprise Strategy Group(ESG)이 기업 내 사이버 보안 관제와 위협 탐지, 대응에 직접 관여하는 사이버 보안 전문가와 IT 전문가 388명을 대상으로 연구 조사를 실시했습니다. 응답자의 24%는 중견 기업(직원 100~999명) 소속이었고, 나머지 76%는 대기업(직원 1,000명 이상) 직원이었습니다. 조사 방법론과 인구통계학적 특성에 대한 자세한 정보는 보고서 마지막에 나와 있습니다.

이 프로젝트에 수집된 조사 내용을 바탕으로, ESG는 다음과 같은 결론에 도달했습니다.

- **위협 탐지 및 대응 노력은 한계점에 왔습니다.** 기업이 보안 관제 문제의 "퍼펙트 스톰"에 시달립니다. 많은 기업이 전 세계적인 사이버 보안 기술 부족 현상으로 인해 인력난을 경험하거나 지능적 사이버 보안 기술이 부족한 상황입니다. 또한 SOC 팀은 통합되지 않은 다수의 포인트 도구들로 위협 탐지와 대응을 해결하는 경향이 있어, 독립적인 보안 정보가 무수히 발생하며 수동 프로세스에 입력됩니다. 이런 주먹구구 방식은 확장이 불가능하기 때문에 SOC 팀들은 보안 데이터의 증가, 표적화된 위협, 늘어나는 공격 표면에 어떻게 대응해야 할지 갈피를 잡지 못합니다. 유감스럽게도 이미 일부 기업에서는 보안 관제가 빠르게 한계점에 도달하고 있는 듯합니다.

- **기업에서는 보안 관제 솔루션을 통합하기를 원합니다.** 이와 같은 한계를 인식한 기업들은 보안 분석 도구와 운영 기술을 적극적으로 통합하고 있습니다. 흩어져 있는 포인트 도구를 보안 관제와 분석 플랫폼 아키텍처(SOAPA)로 전환하고 데이터 파이프라인, 분석, 시각화, 관리를 모으기 위해서입니다. 긴밀히 통합된 SOAPA는 아키텍처 전체가 각 부분(즉, 포인트 제품)의 합보다 가치가 큽니다.

- **XDR는 기업에서 보안 효과와 운영 효율을 개선하는 데 도움을 줄 수 있습니다.** 이번 연구 조사에서는 확장된 탐지 및 대응(XDR)이라는 새로운 보안 기술 플랫폼을 어디에 활용할 수 있을지 살펴봅니다. 이 플랫폼은 컨트롤 포인트, 보안 원격 측정, 분석, 관제를 하나의 엔터프라이즈 시스템으로 가져온 통합형 보안 제품입니다. 보안 전문가가 수집된 데이터를 바탕으로 XDR 설계 특징과 잠재적 장점을 평가합니다. 많은 CISO가 보안 효과와 운영 효율 개선을 기대하고 향후 12개월 이내에 XDR을 시험해볼 계획이라고 합니다.

사이버 보안 관제 현황

위협 탐지와 대응은 모든 사이버 보안 팀의 핵심 업무이지만, 이 영역에서 어려움을 겪는 팀이 많습니다. ESG는 전 세계적인 사이버 보안 기술 부족 현상 외에도 다음과 같이 다양한 위협 탐지 및 대응 문제에 초점을 맞추었습니다.

- 수동 프로세스가 여전히 큰 장애물로 작용: 기업의 43%가 위협 탐지와 대응에 지나치게 많은 수동 프로세스를 사용한다고 답했습니다. 이는 이미 과중한 업무 부담에 시달리는 직원에게 더욱 스트레스를 줍니다.

- 보안 관제는 보안 노이즈에 시달립니다. 기업의 44%가 보안 팀에서 매일 발생하는 보안 알림을 처리하는 데 어려움을 겪는다고 답했습니다. 즉, 화이트 노이즈와 오탐지 지표를 조사하는 동안 중요한 신호를 놓친다는 것을 의미합니다.

- 기업의 2/3(67%)가 여러 개의 포인트 도구로 위협 탐지와 대응을 관리합니다. SOC 팀은 각 도구에서 개별적인 뷰를 조각조각 모아서 엔터프라이즈 보안 상태를 모니터링할 수밖에 없기 때문에 사각지대와 비효율이 발생합니다.

위협 탐지 노력에는 보안 데이터를 실시간으로 수집, 처리 및 분석하는 확장형 고성능 데이터 파이프라인이 필요합니다. 여기에는 엔드포인트 데이터, 네트워크 데이터, 클라우드 데이터, 위협 인텔리전스가 포함됩니다. 안타깝게도 확장형 보안 데이터 파이프라인을 구축하고 관리하기가 쉽지 않습니다. 조사 결과에 따르면, 응답자의 36~38%가 데이터 파이프라인 확장, 위협 인텔리전스와 내부 보안 알림의 통합, 보안 데이터를 신호와 노이즈로 구분하는 데 어려움을 겪고 있다고 답했습니다.

ESG의 조사에서 걱정스러운 현실이 드러났습니다. 많은 보안 팀에서 위협 탐지와 대응이 효과적으로 운영되고 있지 않으며, 문제가 커지고 있습니다. 생각을 바꾸어 위협 탐지와 대응을 위한 도구와 프로세스에 새로운 방식을 도입하지 않으면 앞으로 사이버 보안 위험이 커지고 수시로 보안 인시던트가 발생하는 미래에 직면하게 됩니다.

XDR의 잠재력

다행히 CISO들은 미션 크리티컬 자산과 비즈니스 프로세스를 보호하려면 위협 탐지 및 대응을 개선하는 것이 중요하다는 점을 알고 있습니다. 많은 CISO가 이미 공급업체를 통합하고 보안 도구를 보안 관제 및 분석 플랫폼 아키텍처(SOAPA)에 통합하는 등의 노력을 기울이고 있습니다. 공급 측면에서는 보안 기술 공급업체들이 확장형 탐지 및 대응(XDR)이라는 새로운 SOAPA형 통합 보안 플랫폼을 출시했습니다. ESG에서는 XDR을 다음과 같이 정의합니다.

> 하이브리드 IT 아키텍처에서 위협 방지, 탐지 및 대응을 상호 운용 및 조정하도록 설계된 통합형 제품군. XDR은 컨트롤 포인트, 보안 원격 측정, 보안 관제를 하나의 엔터프라이즈 시스템으로 통합합니다.

XDR은 SOAPA와 마찬가지로 개별 포인트 도구를 공통 아키텍처에 통합합니다. 또한, XDR은 고급 분석 도구와 프로세스 자동화 기능도 추가됩니다. 이러한 방식으로 앞서 설명한 여러 가지 문제를 해결합니다. 고급 분석은 노이즈를 필터링하고 신호를 알림으로 집계하여 과중한 업무 부담에 시달리는 SOC 분석가의 생산성을 높일 수 있습니다. 이와 동시에 프로세스 자동화는 수동 프로세스의 비중을 낮춥니다.

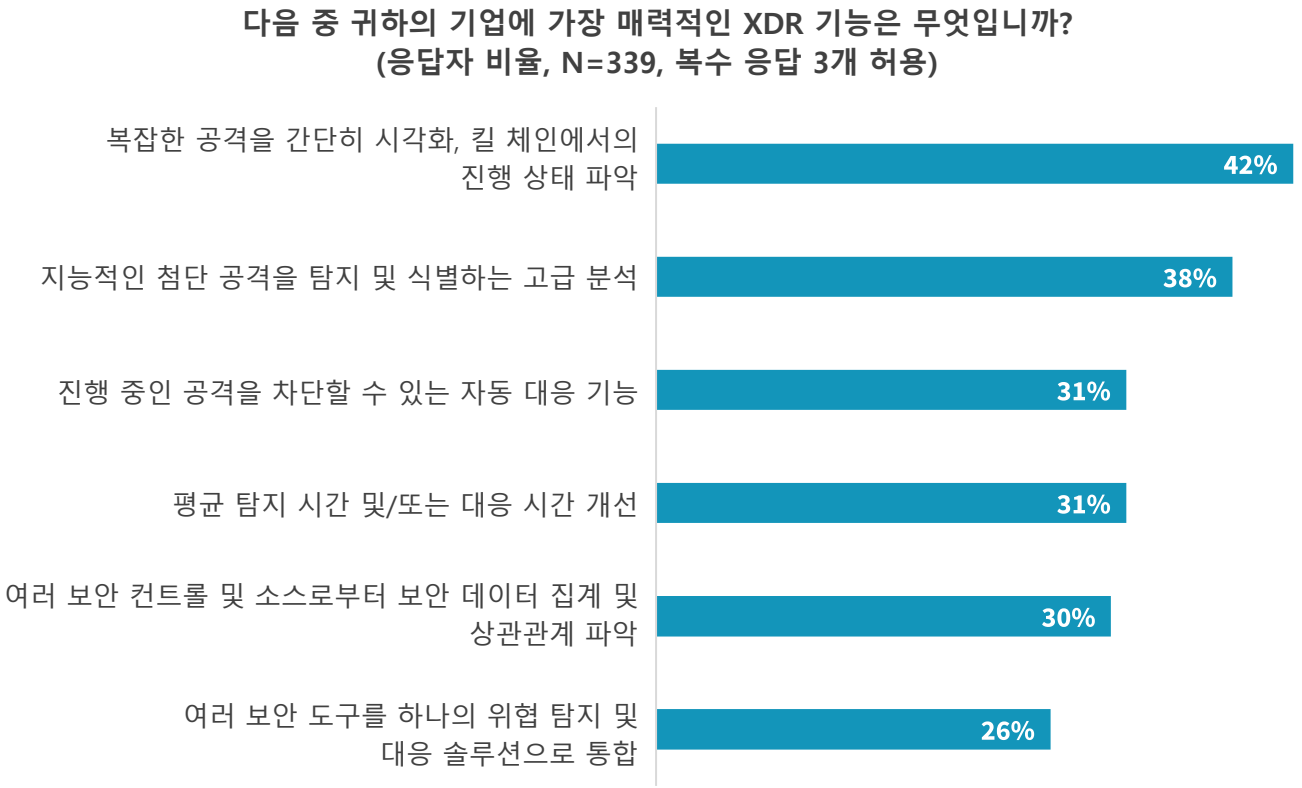
ESG 조사에 따르면, 보안 전문가들은 XDR의 잠재적 가치를 인정합니다. 사실 XDR은 다음과 같은 보안 관제 영역에 특히 매력적일 수 있습니다(그림 1 참조).

- **모든 공격 표면에서 복잡한 공격을 간단하게 시각화.** SOC 분석가는 위협을 조사할 때 여러 보안 대시보드, 로그, 보고서를 오가야 하는 현실을 빗대 "회전 의자식" 관리라며 불만을 표하는 경우가 많습니다. 설문조사 응답자들(42%)은 XDR이 공격 표면에서 복잡한 공격을 간단하게 시각화할 수 있다면 특히 유용할 것이라고 답했습니다. 다시 말해, 킬 체인을 구축하는 동안 사이버 공격 수명 주기를 모니터링하고 조사할 수 있는 XDR 인터페이스를 원합니다.

- **지능적인 첨단 공격을 탐지하기 위한 고급 분석.** 사이버 보안 전문가의 38%는 모든 보안 영역(예: 엔드포인트, 네트워크)에서 이벤트 상관 관계, 이산적 머신 러닝 알고리즘 등의 기술을 활용하기보다는 지능적인 첨단 공격을 탐지할 수 있는 고급 분석을 제공하는 XDR 솔루션을 원합니다. 이렇게 하면 모든 컨트롤 포인트에서 방대한 데이터를 처리하고, 현재 진행 중인 실제 사이버 공격을 탐지하여 분석가에게 공격 수명 주기와 관련된 자세한 이벤트 타임라인을 제시할 수 있습니다. 이러한 정보로 무장한 보안 팀은 조사와 인시던트 대응을 가속화할 수 있습니다.

- **자동화된 대응 기능.** 보안 팀의 31%는 위협 탐지의 신뢰도가 높으면 XDR이 자동 대응을 통해 현재 진행 중인 공격을 차단하기를 원합니다. 이런 자동 대응 조치에는 엔드포인트 보안 서명 업데이트, DNS 도메인 차단, 새로운 방화벽 규칙 추가 등이 포함됩니다. 그렇다면 목표는 무엇일까요? 각 보안 영역뿐만 아니라 모든 사이버 보안 인프라를 지속적으로 자동 강화하는 것입니다.

그림 1. XDR에서 가장 매력적인 기능



출처: Enterprise Strategy Group

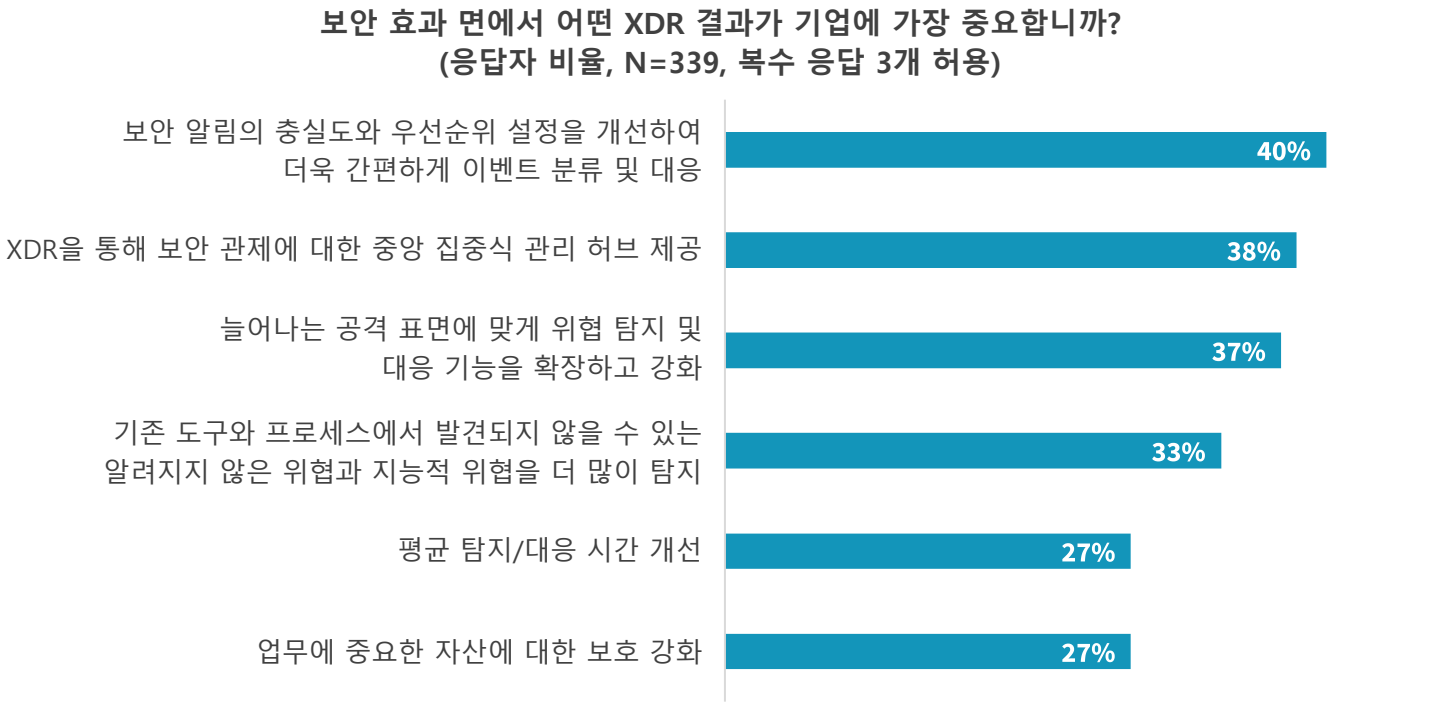
CISO는 XDR로부터 기능 외에도, 현재의 위협 탐지 및 대응 문제를 해결하고 실질적 사업 이익이 되는 결과를 얻기를 바랍니다. ESG 조사에 따르면, 보안 전문가들은 XDR에서 다음과 같은 결과를 가장 중요하게 생각합니다(그림 2 참조).

- **탐지 및 우선순위 설정을 위한 고충실도 알림.** 보안 관제 팀의 40%가 사이버 공격의 진행 상황을 추적하는 자세한 타임라인을 포함한 알림을 시기적절하고 정확하게 받아보기를 원합니다. 자세한 정보가 있으면 대응 조치의 우선순위를 설정하고, 사이버 공격의 근본 원인과 범위를 정확하게 알아내서 해당 보안 컨트롤을 강화하기 위한 복구 업데이트를 구축할 수 있습니다.

- **중앙 관리 허브.** 보안 관제 분석가의 38%는 하나의 인터페이스에서 보안 정책의 생성과 관리, 보안 컨트롤 구성, 보안 활동 조회 작업을 처리하고 싶어 합니다. XDR은 보안 컨트롤을 통합함으로써 보안 명령과 컨트롤을 집중시킬 수 있습니다.

- **엔드포인트에서 클라우드까지 점점 늘어나는 공격 표면 커버.** 보안 관제 분석가의 37%가 늘어나는 공격 표면 전체로 위협 탐지 및 대응 기능을 확장하고자 합니다. 이는 엔드포인트, 네트워크, 서버, 클라우드 워크로드 등의 모든 컨트롤 포인트에서 XDR을 통합하고 시각화한다는 것을 의미합니다. 일부 XDR 솔루션에는 이메일 보안, 웹 보안, SaaS 보안 등의 다른 컨트롤도 포함되겠지만, 전체 공격 킬 체인에서 악성/수상한 활동을 추적한다는 목표에는 변함이 없습니다. 이 기능은 MITRE ATT&CK 프레임워크에 XDR을 일치시키는 데도 도움이 됩니다.

그림 2. 보안 효과에 대한 XDR 결과



출처: Enterprise Strategy Group

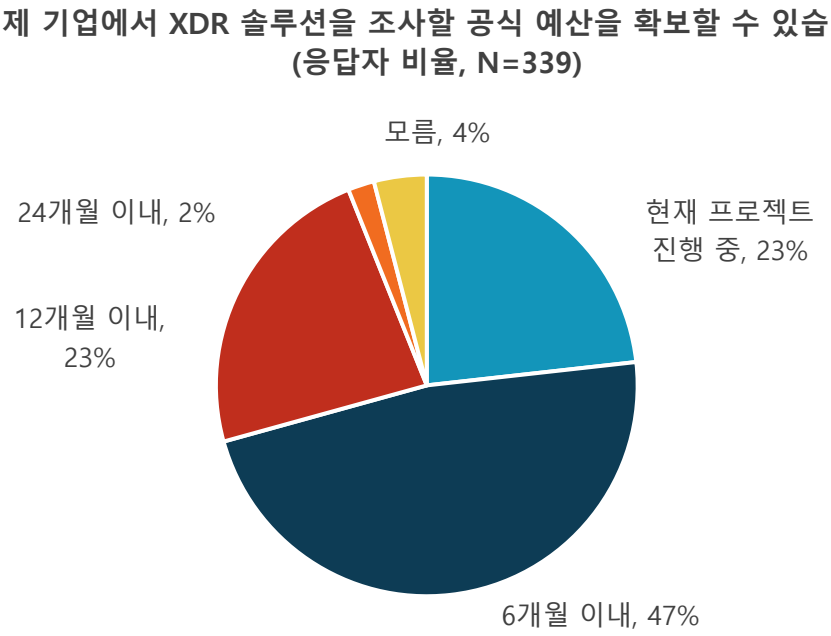
서비스는 여전히 위협 탐지에서 중요한 비중을 차지합니다. 특히, XDR과 같은 지능적 솔루션 세트로 옮기는 것이 중요합니다. 설문조사 응답자의 35%가 기업에서 이미 관리형 탐지 및 대응(MDR) 서비스를 사용하고 있다고 답했고 38%는 MDR 서비스 도입 프로젝트를 추진 중이라고 답했습니다. 서비스에 의존하는 경향은 XDR에서도 나타납니다. 기업의 45%가 배포 서비스(예: 프로젝트 관리, 테스트, 시범 운영, 구현)를 사용하기를 원했고, 35%는 계획 서비스(예: 평가, 프로젝트 디자인 및 계획)를 사용하기를 원했습니다. 이런 곳에 도움이 필요한 CISO라면 참조 아키텍처와 배포 가이드, XDR 모범 사례 전략을 제공하는 XDR 공급업체 및/또는 서비스 공급업체와 협력해야 합니다.

2021년 XDR 전망

XDR은 2020년에 갓 태어난 기술이지만, ESG 조사 보고서는 2021년이 기술 혁신과 구현을 중심으로 XDR에 대한 움직임이 늘어나는 해가 될 것이라는 결과를 내놓았습니다. 전반적인 위협 탐지 및 대응과 관련된 여러 가지 당면 과제를 인식한 대부분 기업이 XDR이 어떤 도움이 될지 알아보고자 합니다. 예를 들어, 다음과 같은 경향이 나타났습니다.

- **기업들이 이미 XDR로 움직이는 추세입니다.** 조사 결과에 따르면, 기업의 약 1/4(23%)이 XDR 프로젝트를 추진하고 있습니다. EDR과 네트워크 탐지 및 대응(NDR) 등의 두 컨트롤을 맞춤형으로 통합하는 프로젝트 등이 해당합니다. 또한, 기업의 70%가 향후 12개월 이내에 XDR 예산이 확보될 것으로 생각합니다(그림 3 참조). 보안 효과를 개선하고 보안 관제를 간소화해야 할 필요성을 얼마나 절실하게 생각하는지 알 수 있습니다.

그림 3. XDR 예산 계획



출처: Enterprise Strategy Group

- **XDR은 기존 보안 컨트롤을 대체할 수 있습니다.** 기업의 절반(48%)가량이 기존 컨트롤을 XDR로 교체할 의향이 있다고 답했고, 나머지 47%는 XDR의 효과를 신뢰할 수 있다면 그럴 의향이 있다고 답했습니다. 어떤 컨트롤이 교체될까요? 가장 가능성이 큰 영역은 엔드포인트와 네트워크 보안이지만, XDR은 플랫폼이기 때문에 다른 영역도 교체해야 할 수 있습니다. 흥미롭게도 많은 기업이 클라우드 기반 위협 탐지와 대응 컨트롤에서 시작해서 더욱 포괄적인 XDR 아키텍처로 나아갈 수도 있습니다.

- **기업에서는 XDR 센서/에이전트를 인프라에 추가하려고 할 것입니다.** 기업의 3/4(76%) 이상이 필요성이 생기거나 XDR이 상당한 이점을 제공한다면 새로운 센서나 에이전트를 추가할 의향이 있다고 답했습니다. 이 응답도 기업에 보안 개선이 얼마나 절실한지 보여줍니다. 더 많은 데이터를 수집, 처리, 분석해야 할 필요성이 생긴다면 더 나은 결과를 얻기 위해 XDR로 바꿀 의향이 있습니다.

더 큰 진실

ESG 조사 결과에 따르면, 위협 탐지 및 대응 요구 사항에 걸맞은 인력, 프로세스, 기술을 갖추지 못한 기업이 많습니다. 직원은 과중한 업무 부담에 시달리고 생산성 효율이 저하되어 있으며, 적절한 규모의 사이버 보안 인력이나 보안 분석 기술이 부족합니다. 프로세스는 수동인 경우가 많고, IP 주소 조회와 같이 반복적 작업이 대부분입니다. 위협 탐지 및 대응 프로세스는 대개 서로 통합되지 않은 포인트 도구 여러 개를 활용하기 때문에 엔터프라이즈 보안 동향을 이해하는 범위가 좁아질 수밖에 없습니다. CISO는 인력, 프로세스, 기술에서 소심한 변화를 추구한다면 작은 이익만 취할 수 있을 뿐, 정말로 필요한 혁신적 변화는 이룰 수 없다는 것을 깨달아야 합니다.

변화의 움직임이 보이는 듯하지만, 보안 기술 공급업체는 보안 전문가가 시급히 필요하다는 것을 깨달았고 XDR이라는 긴밀히 통합된 전체적 보안 플랫폼을 통해 이 문제를 해결하고 자합니다. XDR는 새로운 제품일 수 있지만, 2021년부터는 빠르게 발전할 것으로 생각합니다. 이번 ESG 조사 분석 보고서에 공개된 데이터에 따르면, XDR이 기대한 만큼의 성능을 보이기만 한다면 많은 기업에서 환영할 것으로 보입니다.

기업이 XDR을 평가할 때는 다음을 고려해야 합니다.

- **작게 시작하되, 계획은 크게 잡으세요.** CISO는 특히 취약하거나 복잡한 영역에 단기적 XDR 활동을 집중해야 합니다. 예를 들어, 수년 전부터 기존 엔드포인트 보안에 불만이 나왔고 최근 들어서는 클라우드 워크로드와 관련된 악성/수상한 활동에 대한 가시성을 개선해달라는 요청이 많았습니다. 따라서 엔드포인트 보안이나 클라우드 워크로드, 또는 그 두 가지에서 모두 시작하면 좋을 듯합니다. 도입을 시작한 이후에는 18~36개월 정도로 적절히 기간을 설정하고 공격 표면 전체를 커버하는 것을 목표로 삼아 XDR을 단계별로 도입해야 합니다. 각 제품 도입 단계는 통합의 이익을 달성하는 것을 기준으로 측정해야 합니다.

- **고급 분석을 찾으세요.** 선도적인 XDR 솔루션은 콘텐츠(공급업체 규칙 세트, 커뮤니티 기여, 머신 러닝 알고리즘 등)로 차별화를 꾀할 것입니다. 경험이 풍부한 위협 조사 팀이 분석 혁신과 지속적인 콘텐츠 업데이트에 노력하는 공급업체를 찾아야 합니다.

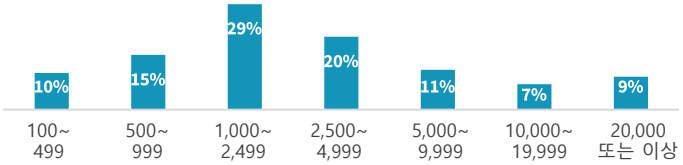
- **프로세스 자동화는 중요합니다.** XDR이 단기간 내에 완전한 SOAR과 승부를 겨루기는 어렵겠지만 선도적인 XDR 플랫폼이라면 인시던트 대응과 위협 완화를 중심으로 프로세스 자동화를 지원해야 합니다. 악성 IoC가 발견되면 XDR이 엔드포인트에서 퍼블릭 클라우드까지 모든 인프라에 차단 규칙을 자동 적용해야 합니다.

응답자 방법론 및 인구 통계학적 특성

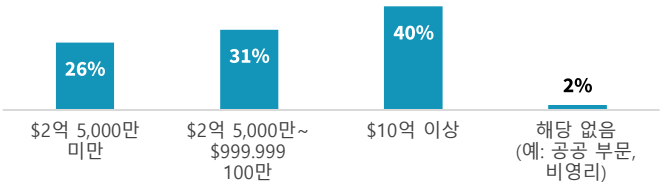
ESG는 이 보고서에서 데이터를 수집하기 위해 2020년 10월 6일부터 2020년 10월 13일까지 북미 지역(미국 및 캐나다)의 민간 및 공공 부문 기업에서 일하는 IT 및 사이버 보안 전문가를 대상으로 종합적인 온라인 설문조사를 실시했습니다 이 설문조사 대상으로 선정된 응답자는 탐지 및 대응 전략, 프로세스, 기술의 평가, 구매, 관리에 직접 관여하는 IT 및 사이버 보안 전문가입니다. 모든 응답자에게는 설문조사를 완료하는 보상으로 현금 및/또는 현금 등가물을 제공했습니다.

자격 요건에 맞지 않는 응답자를 제외하고, 중복 응답을 제거하고, 나머지 완료된 응답을 데이터 무결성을 확보하기 위해 (여러 가지 기준으로) 심사를 끝내고 나자 최종적인 샘플로 IT 및 사이버 보안 전문가 388명이 남았습니다.

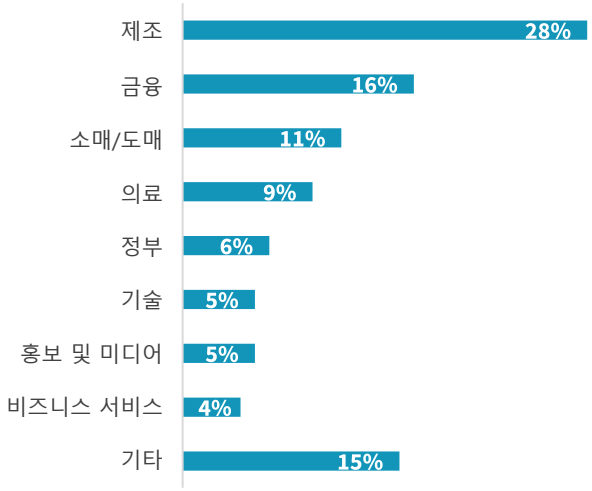
직원 수 기준 응답자



연 매출 기준 응답자.



산업 기준 응답자.



기업의 창립 연수 기준 응답자.