2025.09

Vol.14

글로벌 시장동향보고서

사이버 위협 인텔리전스

(Cyber Threat Intelligence)

과학기술정보통신부 서울특별시 서울테크노파크 SEOULTECHNOPARK

본 보고서는 과학기술정보통신부에서 시행하는 연구개발지원단 육성·지원사업의 일환으로 과학기술정보통신부와 서울특별시의 지원을 받아 서울연구개발지원단(서울테크노파크 전략기획팀)에서 작성한 연구보고서입니다.

글로벌 시장동향보고서

사이버 위협 인텔리전스

(Cyber Threat Intelligence)

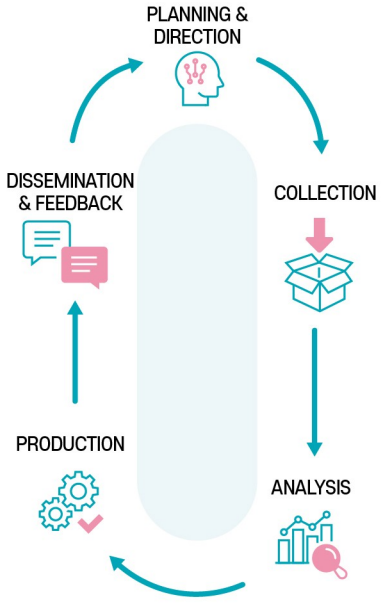
목차

1. 개요

1.1 시장 정의

» 사이버 위협 인텔리전스(CTI; Cyber Threat Intelligence)는 사이버 공격에 대한 정보를 수집하고, 분석해 이해관계자에게 제공하는 일련의 프로세스로 사전에 위협을 파악하고 대응하여 사이버 보안 방어 전략을 개선시키는 것을 의미

- 시스템과 네트워크에 대한 공격 방법은 진화하기 때문에 지속적으로 새로운 취약점이 발견됨에 따라 기업은 CTI를 활용해 새로운 위협에 대한 정보를 인지하여 스스로를 보호해야 함
- CTI는 사이버 공격에 대한 정보를 정리, 분석, 개선해 새로운 위협을 학습하고 이를 활용해 진행 중인 공격을 중단하거나 완화하는 데 도움을 줌으로써 조직을 보호할 수 있음
- 보안 분석가는 여러 소스에서 원시 위협 정보와 보안 관련 정보를 수집한 후 데이터 상관관계를 파악하고 분석하여 실제 위협이나 잠재적 위협에 대해 심층적으로 이해할 수 있는 추세, 패턴 및 관계를 밝혀냄으로써 위협 인텔리전스를 생성함
- 위협 인텔리전스 수명주기(Lifecycle)는 모든 물리적 및 사이버 보안 프로그램을 위한 기본 프레임워크로 계획(Planning & Direction), 수집 및 처리(Collection), 분석(analysis), 생산(Production), 배포 및 피드백(Dissemination & Feedback)의 사이클로 이루어짐



수명 주기 (Life Cycle)	내용
계획 (Planning)	CTI 활동의 목표와 범위를 설정 - 조직의 구성원 식별, 필요한 자원 확보
수집 (Collection)	CTI활동을 위한 정보 수집 및 의미 있는 정보로 변환 - 정보 출처 식별 및 정보 수집 도구·기술 선택 - 정보의 정확성 및 신뢰성 검증
분석 (Analysis)	수집한 정보를 분석하여 위협을 식별하고 평가 - 위협의 종류, 범위, 심각성 평가
생산 (Production)	데이터 분석을 통해 논리적인 결론을 도출 - 위협에 대응하기 위한 조치 계획 및 권장 사항
배포 및 피드백 (Dissemination & Feedback)	위협에 대한 정보 전파 및 CTI 활동 효과 평가 - 정보의 형식과 전달 방법 선택 - 구성원들의 피드백 수집 및 지속적인 개선

출처 : Flashpoint (2021.02)

[그림 1] 위협 인텔리전스 수명 주기 5단계

- 위협 인텔리전스 라이프사이클은 관련된 이해관계자, 설정된 요구 사항, 라이프사이클 특정 인스턴스의 전반적인 목표에 따라 다양한 유형의 인텔리전스를 생성하며, 크게 전술적, 운영, 전략적 3가지로 분류할 수 있음

〈표 1〉 위협 인텔리전스 유형

유형	내용
전술적 위협 인텔리전스	• 보안 운영 센터에서 진행 중인 사이버 공격을 탐지하고 대응하는 데 사용 • 명령 및 제어 서버와 관련된 IP 주소, 알려진 멀웨어 및 랜섬웨어 공격과 관련된 파일 해시, 피싱 공격과 관련된 이메일 제목 줄 등 주로 일반적인 침해지표(Indicators of Compromise, IoC)에 중점을 둠 • 전술적 위협 인텔리전스는 인시던트 대응 팀이 오탐을 걸러내고 실제 공격을 차단하는 것 외에도, 위협 헌팅 팀이 지능형 지속 위협(APT)을 비롯해 기타 활동 중이지만 숨겨진 공격자를 추적하는 데에도 이용
전략적 위협 인텔리전스	• 글로벌 위협 환경과 그 안에서 조직의 위치에 대한 높은 수준의 인텔리전스 • 전략적 위협 인텔리전스는 CEO 및 기타 경영진과 같은 IT 외부의 의사 결정권자에게 조직이 직면한 사이버 위협에 대한 정보를 제공 • 주로 지정학적 상황, 특정 산업의 사이버 위협 동향, 조직의 특정 전략적 자산이 표적이 된 방법 또는 이유와 같은 문제에 중점을 두며, 이해관계자는 전략적 위협 인텔리전스를 사용하여 광범위한 조직 위험 관리 전략 및 투자를 사이버 위협 환경에 맞게 조정
운영 위협 인텔리전스	• 알려진 위협 행위자의 TTP와 행동(예: 사용하는 공격 벡터, 악용하는 취약점 및 대상 자산)을 자세히 설명하기 때문에 '기술 위협 인텔리전스'라고도 불리며, 운영 위협 인텔리전스는 조직이 미래의 공격을 예측하고 예방하는 데 도움을 줌 • CISO, CIO 및 기타 정보 보안 의사 결정권자는 운영 위협 인텔리전스를 사용하여 조직을 공격할 가능성이 있는 위협 행위자를 파악하고 공격을 막기 위한 보안 제어 및 기타 조치로 대응

출처 : IBM (2025.08.09. 접속)

1.2 시장 트렌드

» 기업들은 경쟁이 치열한 사이버 보안 업계에서 위협 인텔리전스 역량을 강화하기 위해 인공지능(AI)과 머신러닝(ML) 기술을 도입

- 위협 인텔리전스 플랫폼은 첨단 기술을 활용하여 방대한 양의 데이터를 신속하게 분석할 수 있는 역량을 강화하여 기업이 새로운 위협에 신속하게 대응할 수 있도록 지원
- 위협 분석 및 탐지 절차를 자동화하는 기업은 사이버 보안 운영을 개선하고, 데이터 유출 위험을 줄이며, 비즈니스 연속성을 보장할 수 있으며, 이는 궁극적으로 기업이 브랜드 이미지를 보호하고 디지털 시대의 도래에 따른 소비자 신뢰를 높이는 데 도움이 될 수 있음
- 2024년 2월, ServiceNow의 새로운 위협 인텔리전스 플랫폼인 위협 인텔리전스 보안 센터(TISC)가 cGTM(Controlled Go-To-Market) 모드로 성공적으로 출시되었으며, 이는 SOC 팀이 위협에 효율적으로 대응하는 데 있어 큰 진전

지정학적 위협과 국가 차원의 위협의 증가에 따른 우려에 대응하기 위하여 위협 인텔리전스에 대한 시장 투자가 증가

- 기업들은 잠재적인 지정학적 위험, 적대적 행동, 그리고 새로운 사이버 위협에 대한 실행 가능한 통찰력을 제공하는 위협 인텔리전스 시스템을 도입하여 국가 차원의 위협과 지정학적 우려에 대응
- 기업은 지정학적 위협 정보를 활용하여 위협 환경에 영향을 미치는 지정학적 요인에 대한 통찰력을 확보하고, 잠재적 사이버 공격을 예측하며, 이에 대응하기 위한 선제적 조치를 취할 수 있음
- 이러한 추세를 활용하여 보안 및 위협 인텔리전스 스타트업인 Silobreaker는 2023년 6월 RANE(Risk Assistance Network + Exchange)이라는 새로운 글로벌 위협 인텔리전스 기능을 출시했으며, Silobreaker는 글로벌 위험 정보 제공업체 RANE의 기업 지정학적 정보를 자체 플랫폼에 통합하여 사이버 위협 정보팀에 사이버 공격의 위험을 증가시킬 수 있는 세계적 사건에 대한 실시간 지식을 제공

딥페이크 기술과 관련된 운영 및 평판 위협에 대한 인식이 높아짐에 따라 딥페이크 탐지 솔루션 개발이 시장에서 주목받고 있음

- 기업들은 왜곡된 멀티미디어 자료의 영향을 발견하고 최소화하기 위해 특별히 개발된 고급 위협 인텔리전스 프로그램에 투자
- 이러한 솔루션은 인공지능과 고급 알고리즘을 활용하여 기업에 딥페이크 위협으로부터 선제적인 보안 및 방어 기능을 제공하고, 고객 신뢰를 유지하고 브랜드 평판을 보호하며, 더 나아가 가짜 오디오 및 비디오 콘텐츠의 확산으로 인한 평판 및 재정적 피해 가능성을 방지함

〈표 2〉 위협 인텔리전스 기술 시장 동향

구분	내용
트렌드 (Trends)	• 중소기업 접근성 확대: 사이버 위험이 모든 규모의 기업에 영향을 미치면서, 중소기업도 위협 인텔리전스를 보다 쉽게 활용 가능 • UEBA 부상: 조직 네트워크 내 사용자 활동을 추적 및 분석하는 사용자 및 엔티티 행위 분석(UEBA)이 위협 인텔리전스의 핵심 요소로 부상 • 양자 컴퓨팅 리스크 인식: 양자 컴퓨팅 발전으로 기존 암호화 기술에 대한 잠재적 위험 인식 확산 • 제로 트러스트 아키텍처 전환: 위협 인텔리전스를 제로 트러스트 프레임워크에 통합해 사용자, 기기, 앱의 신뢰성을 지속적으로 검증 • 행동 기반 생체인식 활용: 마우스 움직임, 타이핑 속도 등 행동 패턴 분석을 통해 내부 위협 탐지
기회 (Opportunities)	• 산업별 특화 솔루션 개발: 헬스케어, 금융, 에너지 등 산업별 맞춤형 위협 인텔리전스 솔루션 제공 기회 • IoT 보안 특화 서비스: 사물인터넷(IoT) 확산에 따른 보안 특화 위협 인텔리전스 서비스 제공 가능성

구분	내용
	• 협력적 정보 공유 시스템 구축: 조직 간 위협 인텔리전스 공동 교환 시스템 개발 • 모바일 보안 시장 확대: 모바일 기기 의존도 증가에 따른 모바일 중심 위협 인텔리전스 수요 증가 • 교육·훈련 사업 기회: 위협 인텔리전스 기술 관련 교육 및 훈련 과정 제공
도전 (Challenges)	• 고도화되는 공격 대응: 랜섬웨어, 지능형 지속 공격(APT) 등 점점 복잡해지는 사이버 공격에 대응 위해 지속적 기술 개선 필요 • 과거 데이터 의존 문제: 기존 위협 인텔리전스가 과거 데이터에 치중해 새로운 위협 탐지 지연 가능성

출처 : Future Market Insights. (April 11, 2024)

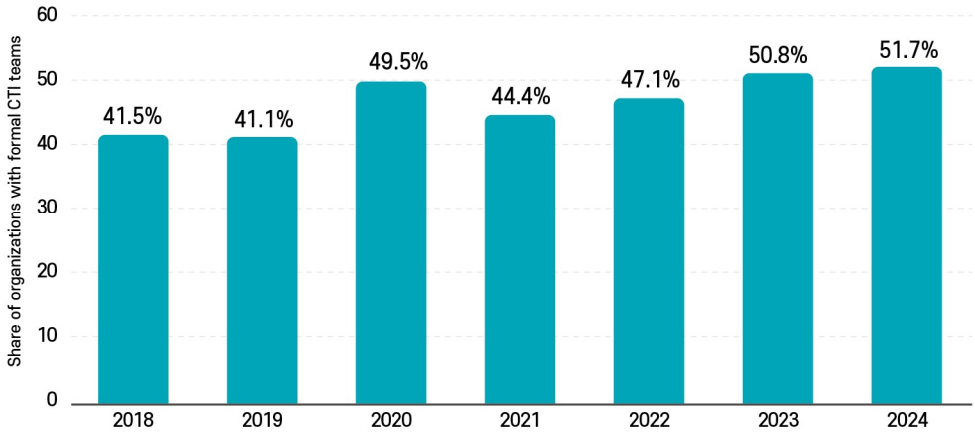
2. 시장 동향

2.1 사이버 위협 인텔리전스 현황 및 전망

» 2024년 글로벌 설문 조사*에 따르면, 거의 52%의 조직이 사이버 위협 인텔리전스(CTI)에 전담 리소스를 투자한 것으로 나타남

* 글로벌 22개 산업 전문가 대상으로 2024년 설문조사 실시, 811명 응답

- 2018년에는 전체 조직의 41.5%가 공식적인 CTI 팀을 보유하고 있었으며, 2024년에는 51.7%로 약 10%p 이상 증가하여, 절반 이상의 조직이 CTI 역량을 공식적으로 갖춘 것으로 나타남

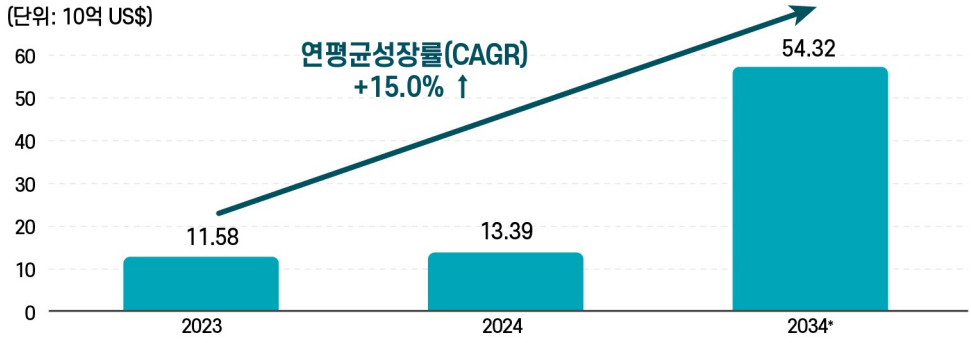


출처 : Statista (2024), Future Market Insights 재인용

[그림 2] 사이버 위협 인텔리전스 전담 리소스 보유 조직 비율 (2018~2024)

글로벌 위협 인텔리전스 시장 규모는 2024년부터 2034년까지 연평균성장률 15%를 기록하며 2034년에 543억 2천만 달러에 달할 것으로 전망

- 2023년 시장 규모는 약 115억 8천만 달러였으며, 2024년에는 약 133억 9천만 달러로 소폭 증가했으며, 2034년에는 시장 규모가 약 543억 2천만 달러에 달할 것으로 예상되어, 2024년 대비 약 4배 이상 성장할 것으로 전망

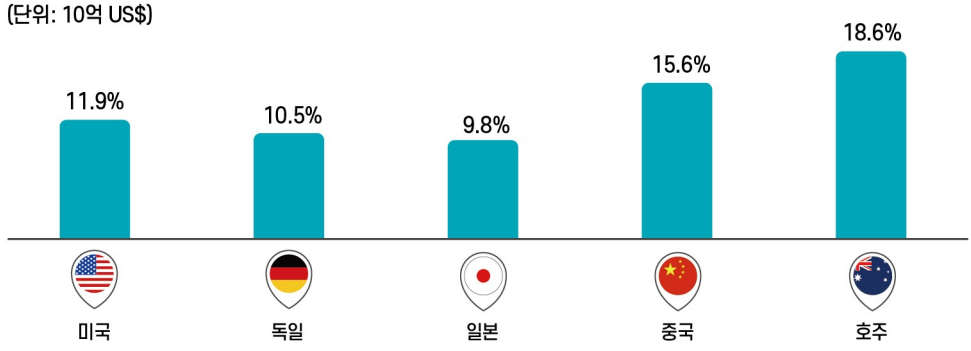


출처 : Statista (2024), Future Market Insights 재인용

[그림 3] 위협 인텔리전스 시장 전망 (2024~2034년)

- 배포 모드를 기준으로 볼 때, 클라우드 기반 세그먼트는 2024년에 위협 인텔리전스 시장 점유율의 62.80%를 차지할 것으로 예상되며, 수많은 기업이 IT 인프라를 클라우드로 이전함에 따라, 클라우드 환경과 완벽하게 호환되는 위협 인텔리전스 솔루션에 대한 수요가 증가
- 업계 기준으로 금융 서비스 제공업체(BFSI) 부문이 2024년에 위협 인텔리전스 시장 점유율의 25.40%를 차지했으며, 이는 디지털 자산 보호와 안전한 거래 환경 조성을 위한 핵심 보안 아키텍처로 위협 인텔리전스 솔루션이 부상하고 있는 것을 반영

대부분의 국가에서 규제·정책 주도와 산업 특화전략을 성장의 핵심 동력으로 하고 있으며, 중국은 디지털 헬스케어·스마트 시티, 미국은 정부·산업 협력, 독일은 오픈소스 인텔리전스, 일본은 공급망 회복력이 주요 성장 요인



출처 : Statista (2024), Future Market Insights 재인용

[그림 4] 위협 인텔리전스 시장 국가별 연평균성장률 (2024~2034년)

- 국가별 2024년부터 2034년까지의 연평균성장률을 살펴봤을 때, 호주는 가장 높은 성장률(18.6%)를 기록할 것으로 예상

〈표 3〉 국가별 위협 인텔리전스 시장 성장 동향

국가	내용
	**〈미국 정부 이니셔티브 및 자금 지원 시장 개발〉** • 미국의 위협 인텔리전스 수요는 2034년까지 연평균 11.90% 성장할 것으로 예상 • 사이버 보안에 대한 미국 정부의 적극적 접근(CISA 설립 등)이 시장 성장 촉진 • 공공 및 민간 부문은 사이버 보안 R&D 프로젝트에 대한 정부 자금 및 보조금을 통해 협력, 혁신 촉진 및 시장 확장 • FS-ISAC 및 ISACs와 같은 기관 주도의 산업 협력 및 정보 공유 프로그램이 미국 사이버 보안 환경 개선에 기여 • 산업 전반에서 위협 인텔리전스 공유를 장려하는 협력 전략은 사이버 공격 대응력을 강화하고 시장 확대를 촉진
	**〈오픈소스 인텔리전스(OSINT) 채택 증가로 시장 성장 가속〉** • 독일의 위협 인텔리전스 시장은 2034년까지 연평균 10.50% 성장할 것으로 예상 • OSINT는 독일에서 높이 평가되며, 위협 인텔리전스 이니셔티브에 자주 포함 • 더 많은 독일 기업이 사이버 보안 이니셔티브를 지원하기 위해 OSINT 기술을 활용함에 따라 시장 성장 • 혁신적이고 신뢰할 수 있는 OSINT 공급업체들이 지역 수요에 맞춘 솔루션 제공으로 시장 내 입지 강화 • 독일의 위협 환경은 APT 및 복잡한 사이버 위협이 특징이며, 이에 대응 가능한 고도 탐지 및 대응 솔루션 수요 증가
	**〈공급망 회복력 이니셔티브로 매출 확대〉** • 일본의 위협 인텔리전스 매출은 2034년까지 연평균 9.80% 성장할 것으로 예상 • 자연재해 및 기타 장애 발생 시 공급망 복원력 향상을 위한 노력으로 시장 성장 촉진 • 공급망 위험 및 취약성에 대한 통찰력을 제공하는 위협 인텔리전스 솔루션을 최우선 과제로 설정 • 공공 서비스, 운송, 에너지 등 중요 인프라 보호를 위한 전략적 초점이 시장 성장을 견인 • 엄격한 규제 환경으로 인해 중요 인프라 보안 공급업체 제품 수요 증가
	**〈디지털 헬스케어 이니셔티브로 수요 급증〉** • 중국의 위협 인텔리전스 수요는 2034년까지 연평균 15.60% 성장할 것으로 예측 • 원격 의료 및 의료 정보 기술의 광범위한 활용을 포함한 디지털 헬스케어 전략이 시장 성장 촉진 • 의료 기관들은 개인 의료 정보 보호를 위한 사이버 보안 솔루션을 최우선으로 함 • 디지털 헬스케어 부문 변화로 의료 데이터 보호 역량을 갖춘 공급업체 수요 증가 • IoT 및 AI를 통합한 스마트 시티 계획으로 위협 인텔리전스 수요 증가 • 스마트 시티 사업에서 철저한 위협 인텔리전스 솔루션이 도시 인프라 및 네트워크 보호에 핵심

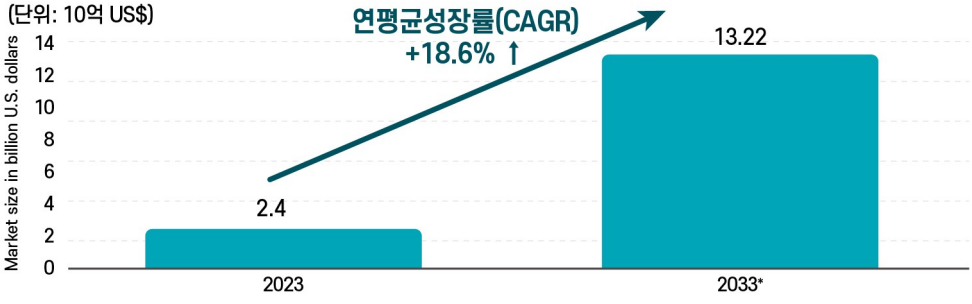
국가	내용
	**〈데이터 주권 규제 준수가 성장 촉진〉** • 호주의 위협 인텔리전스 매출은 2034년까지 연평균 18.60% 성장할 것으로 예상 • 데이터 주권과 법적 체계(NDB 제도, APPs)에 대한 우선순위가 시장 성장 견인 • 데이터 보호법 준수 및 데이터 주권 유지와 관련된 사이버 보안 문제를 해결하는 솔루션이 우선시됨 • 중요 인프라 보안법(Security of Critical Infrastructure Act)은 중요 서비스의 사이버 보안 강화를 반영 • 규제 준수를 지원하고 중요 서비스의 고유한 보안 요구를 해결하는 솔루션이 시장 내 최우선 과제 • 주요 산업의 사이버 보안 규제 모니터링을 지원하는 제품 제공 기업들이 시장 성장 가속화

출처 : Future Market Insights. (April 11, 2024)

2.2 위협 사냥 시장 현황 및 전망

» 위협 사냥 시장(Threat hunting market)의 규모는 2023년 약 24억 달러로 추산되며, 연평균성장률 18.6%를 보이며 2033년에는 약 132억 2천만 달러에 이를 것으로 예상

- 위협 사냥(Threat Hunting)은 네트워크, 엔드 포인트 및 데이터셋을 통한 사전 예방적 보안 검색으로, 기존 도구로 탐지되지 않은 악의적이거나 의심스럽거나 위험한 활동을 검색
- 기존의 방식은 사전에 정의된 탐지 규칙과 알고리즘에만 의존하는 단점을 위협 사냥은 공격행위에 맞춰 대응하며, 아직 탐지되지 않은 멀웨어나 C2 서버를 찾아낼 수 있다는 장점이 있음



출처 : Statista (2024), Future Market Insights 재인용

[그림 5] 위협 사냥 시장 전망 (2023 vs 2033년)

- 위협 유형에 따라 시장은 APTS (Advanced Persistent Thatss), 맬웨어 및 랜섬웨어, 내부자 위협, 피싱 및 사회 공학 등으로 나뉘며, APTS (Advanced Persistent Threats) 솔루션 세그먼트는 기업이 요구하는 솔루션의 복잡성으로 인해 시장을 지배하고 있으며, 위협을 적극적으로 감지하고 은밀하고 장기적인 침입을 찾아야 할 필요성과 함께 시장을 지배

〈표 4〉 위협 사냥 관련 기업 동향

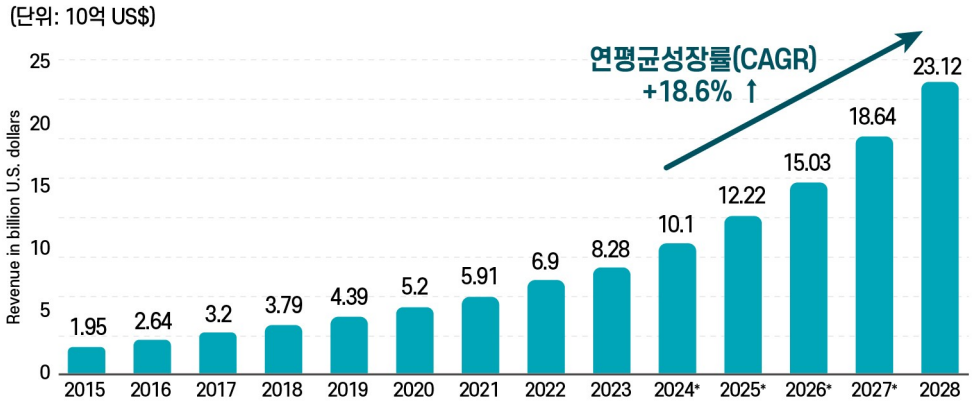
구분	내용
Mandiant	• 2022년 9월, 맨디언트는 구글에 54억 달러라는 거액에 인수되었으며, 클라우드 사이버 보안 분야에서 구글의 기준을 한 단계 끌어올려 심각한 위협 탐지 솔루션 제공에 더욱 유리한 위치를 점하게 됨
HORNETSECURITY	• 2024년 3월, 호넷시큐리티 그룹은 프랑스 이메일 보안 분야 선두 기업인 알토스팸(Altospam)을 인수했으며, 인수를 통해 사이버 위협으로부터 조직을 방어하는 고급 위협 탐지 기능을 통해 호넷시큐리티의 이메일 보안 솔루션 역량이 더욱 강화될 것으로 예상
LEONARDO	• 2024년 10월, 이탈리아의 Leonardo Defense SA 자매 회사는 사이버 방어 부문의 위협 사냥 역량을 강화하기 위해 약 12개의 국내외 사이버 보안 기업을 인수 및 합병 대상으로 선정하는 평가 라운드를 진행

출처 :Future Market Insights (2025.05)

2.3 지능형 지속 공격 보호 시장 현황 및 전망

» 글로벌 지능형 지속 공격(Advanced Persistent Threat) 보호 시장은 2028년에 230억 달러 규모에 달할 것으로 예상

- 지능형 지속 지속적 위협(Advanced Persistent Threat, APT)은 허가 없이 컴퓨터 네트워크에 액세스하는 은밀한 위협 행위자로, 은밀하고 지속적인 해킹 프로세스가 특징으로 종종 초기 타협, 측면 이동 및 데이터 추출을 포함하는 여러 단계를 포함하고 있으며, 위협 행위자의 목적은 조직에 피해를 입히거나 도난, 감시 또는 방해를 통해 정보를 얻는 것임
- APT 공격은 일반적으로 오랜 시간 동안 감지되지 않기 때문에 공격자는 목표를 달성하기 위해 공격 주기를 거칠 시간이 충분
- APT 보호 시장은 장기간 취약점을 이용하는 정교하고 목표로하는 사이버 공격에 대한 조직을 보호하는 데 중점
- 글로벌 APT 시장 규모는 2015년 약 19억 5천만 달러였으며, 이후 매년 꾸준한 성장세를 기록하며 2020년에는 52억 달러, 2023년에는 82억 8천만 달러로 증가
- 2024년 글로벌 APT 시장 규모는 약 101억 달러에 이를 것으로 예상되며, 향후 연평균 성장률 23.0%를 보이며 2028년에는 231억 2천만 달러를 돌파하여 2015년 대비 약 12배 이상 성장할 것으로 예상



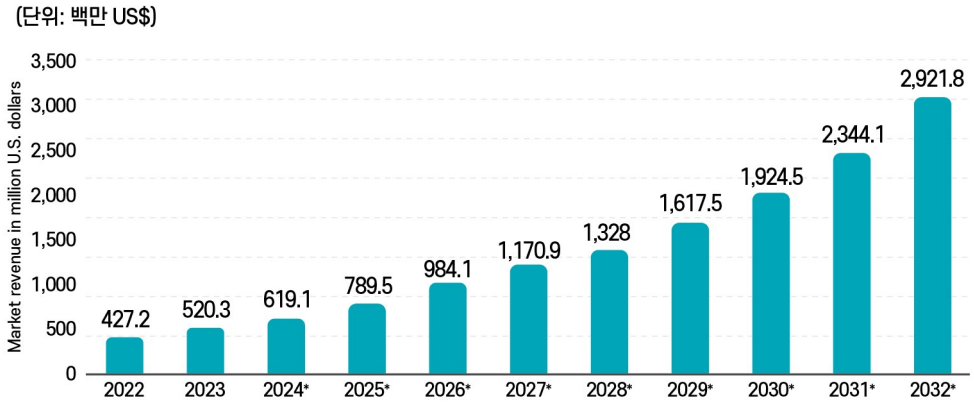
출처 : Statista (2024), The Radicati Group 재인용

[그림 6] 글로벌 APT 보호 시장 매출 추이 및 전망 (2015~2028년)

2.4 다크 웹 인텔리전스 시장 현황 및 전망

다크 웹 인텔리전스 시장(Dark web intelligence market)은 2023년에 약 5억 2천만 달러로 추산되었으며, 2032년 거의 30억 달러에 도달할 것으로 전망

- 다크 웹 인텔리전스는 다크 웹이라고 알려진 인터넷의 숨겨진 부분과 관련된 정보를 수집, 분석 및 배포하는 것을 의미하며, 다크 웹은 딥 웹의 한 부분으로, 사용자와 웹사이트 운영자가 익명을 유지하거나 추적할 수 없도록 하는 Tor와 같은 특수 소프트웨어를 통해서만 접근할 수 있음
- 다크 웹에서 수집한 인텔리전스는 사이버 보안 전문가, 법 집행 기관 및 정보 기관이 사이버 위협, 불법 활동을 탐지하고 예방하고 사이버 범죄 행동, 추세 및 새로운 위협에 대한 실행 가능한 인텔리전스를 수집하는 데 필수적으로, 여기에는 도난된 데이터 모니터링, 위협 행위자 식별 및 조직 네트워크 내의 잠재적 취약성 발견이 포함됨
- 다크 웹에서 범죄 활동으로 인한 총 수익은 연간 약 15억 달러에 달할 것으로 예상되며, 사이버 범죄자는 다크 웹을 사용하여 DDOS 공격, 맬웨어 공격, 사회 공학 및 자격 증명 기반 공격을 포함한 다양한 유형의 범죄를 수행
- Prey project 설문 조사에 따르면, 2023년 다크 웹에서 가장 생산적인 불법 디지털 상품에는 온라인 뱅킹, 암호화폐 계좌, 전자 지갑이 포함되며, 다크웹에서 랜섬웨어 기반 암호화폐 범죄는 1억 7,600만 달러에 달함
- 다크웹 인텔리전스 시장은 2022년 시장 규모는 약 4억 2,720만 달러였으며, 이후 시장은 매년 꾸준한 성장세를 보여 2024년 6억 1,910만 달러, 2026년 9억 8,410만 달러, 2028년 13억 2,800만 달러에 이를 것으로 전망
- 특히 2029년 이후 성장 속도가 가속화되어 2030년에는 19억 2,450만 달러, 2031년에는 23억 4,410만 달러, 2032년에는 약 29억 2,180만 달러에 도달할 것으로 예측



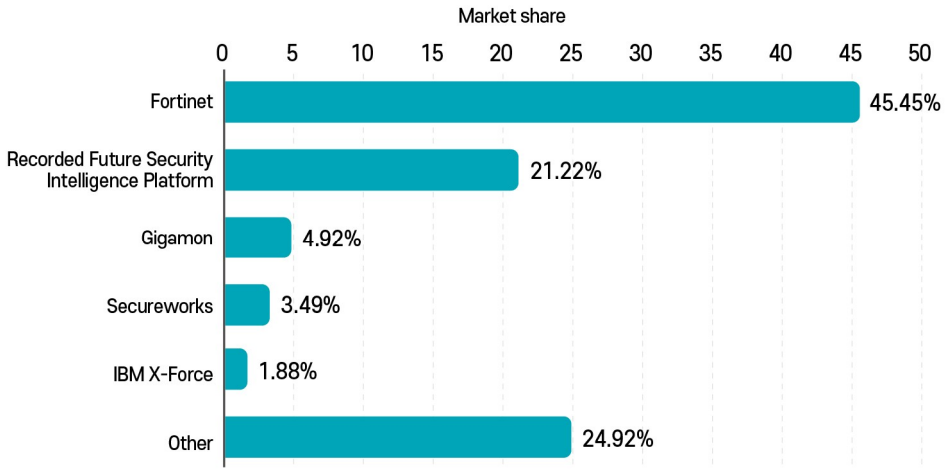
출처 : Statista (2024), GlobeNewswire; Market.us 재인용

[그림 7] 글로벌 다크 웹 인텔리전스 시장 매출 추이 및 전망 (2022~2032년)

2.5 주요 기업

» 2024년 전 세계 위협 인텔리전스 소프트웨어 시장에서 Fortinet이 45.45%의 점유율로 업계를 선도하였으며, Recorded Future Security Intelligence Platform이 21.22%를 차지하며 2위를 기록

- Gigamon은 4.92%, Secureworks는 3.49%, IBM X-Force는 1.88%의 점유율을 보였으며, 이 외의 기타 벤더들이 차지하는 비중은 24.92%로 집계
- Fortinet과 Recorded Future 두 기업이 시장의 과반 이상을 점유하며, 나머지 업체들은 상대적으로 분산된 경쟁 구조를 보이고 있음



출처 : Statista (2024), Datanyze 재인용

[그림 8] 글로벌 위협 인텔리전스 소프트웨어 시장 점유율 현황 (2024년)

다양한 기업들이 사이버 위협 인텔리전스 플랫폼을 운영하고 있음

- 사이버 위협 인텔리전스 플랫폼은 외부 위협과 내부 로그 파일을 처리하여 보안 팀을 위해 우선 순위가 지정되고 상황에 맞는 알림을 생성하거나 보안 대응 도구를 강화할 수 있도록 도움

〈표 5〉 사이버 위협 인텔리전스 제공 주요 기업, 플랫폼 및 기술 특징

기업	CTI 플랫폼 명칭	정보 공유 관련 주요 기술 특징
ANOMALI	Anomali ThreatStream	• 기계학습(ML) 알고리즘을 사용하여 위협의 심각도를 반영한 점수의 신뢰도 • 글로벌 위협의 MITRE ATT&CK 매핑 • 2,000ro 이상의 조직과 위협 가시성 공유
IBM	X-Force Exchange	• 플랫폼 타 사용자와 위협 인텔리전스 협업 정보 공유 • 타임라인 보기를 사용하여 시간 경과에 따라 변화하는 위험 수준 관찰 정보 • IP 주소별 인텔리전스 및 URL 평판
INTSIGHTS	Threat Intelligence Platform	• 실시간 위협 우선 순위 지정 • 맬웨어, 피싱사기 및 위협 행위자(공격자) 조사 • 통합되고 효율적인 위협 관리를 위해 기본 IoC(침해 지표) 설계
LOOKINGGLASS	Cyber Solutions	• 공격, 조직의 환경 및 위협 환경을 기반으로 위협 순위에 대한 신뢰도 점수 • 자산을 그룹 및 하위 그룹으로 분류하여 분류된 위험 프로필을 모니터링 • 알려진 명령 및 제어 노드 연결을 감지하기 위해 인터넷에 액세스할 수 있는 자산 및 네트워크를 모니터링
Recorded Future	Recorded Future	• 신원을 모니터링하고 잠재적으로 손상된 계정에 대해 경고 • 조직의 공격을 탐지하고 모니터링 • 다크 웹소스에 대해 사전적 예방이 가능한 모니터링
solarwinds	Security Event Manager	• 규정 준수를 위한 주문형 자동 보고서 • 자동화된 위협 탐지 및 대응 기술
ThreatConnect	ThreatConnect	• 선제적이로 자동적인 보안을 위한 로우 코드 자동화 • 위협 확산 분석

출처 : SEP Inside (2023.06)

참고문헌

- Statista. (2024.08). Security Service : market data & analysis
- Flashpoint (2021.02). The Five Phases of the Threat Intelligence Lifecycle
- IBM (2025.08.09. 접속). 위협 인텔리전스란 무엇인가요? (https://www.ibm.com/kr-ko/topics/threat-intelligence)
- Future Market Insights. (April 11, 2024). Threat detection system market size worldwide from 2023 to 2034 (in billion U.S. dollars)* [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1364162/global-threat-detection-system-market-value
- Future Market Insights. (April 11, 2024). Threat hunting market size worldwide in 2023 and 2033 (in billion U.S. dollars)* [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1364173/global-threat-hunting-market-value/Future Market Insights (2025.05) Threat Hunting Market Size, Share, and Industry Analysis (https://www.fortunebusinessinsights.com/threat-hunting-market-112244)
- The Radicati Group. (March 3, 2024). Revenue from advanced persistent threat (APT) protection market worldwide from 2015 to 2027 (in billion U.S. dollars) [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/497945/advanced-persistent-threat-market-worldwide/
- GlobeNewswire. (February 14, 2024). Dark web intelligence market revenue worldwide from 2022 to 2032 (in million U.S. dollars) [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/1461403/global-dark-web-intelligence-market-size/
- Datanyze. (February 21, 2024). Vendor share in the threat intelligence software market worldwide in 2024 [Graph]. In Statista. Retrieved January 19, 2025, from https://www.statista.com/statistics/818165/threat-intelligence-security-services-spending-worldwide/
- SEP Inside (2023.06), 사이버 보안 표준 및 관련 특허 동향