PLAINBIT

2026

플레인비트
2026 DFIR TRENDS REPORT

DFIR REPORT

INDEX
목차

1. Executive Summary

Executive Summary

설문개요

최근 디지털 환경은 클라우드 서비스의 확산, 다양한 기기와 계정을 동시에 사용하는 업무 방식의 일반화, 그리고 AI 기술의 빠른 도입 등으로 인해 더욱 복잡해지고 있다. 이러한 변화는 디지털 포렌식과 침해사고 대응의 대상과 범위를 크게 확장시키고 있으며, 단일 시스템이나 특정 환경만을 중심으로 사고를 분석하고 대응하던 기존 방식으로는 점점 한계가 드러나고 있다.

사고 대응 과정에서는 지속적인 탐지와 대응 역량을 유지하는 것이 중요해지고 있으며, 동시에 디지털 포렌식 영역에서는 클라우드 환경에서의 증거 확보, 여러 기기와 서비스에 분산된 데이터를 연계하여 분석하는 기술, AI기반 분석 결과의 신뢰성을 확보하기 위한 절차 마련이 핵심 과제로 부상하고 있다. 또한, 조직 내부에서 관리되지 않는 계정이나 Shadow IT와 같은 보이지 않는 자산이 새로운 공격 표면으로 작용하면서 사고 대응과 포렌식 분석의 범위 역시 조직 외부와 공급망 영역까지 확대되고 있는 상황이다.

플레인비트는 이러한 변화에 대응해 디지털 포렌식 조사, DFIR 서비스, 교육, 컨설팅 등 포렌식 기반 서비스를 지속적으로 제공하고 있으며, 실제 현장에서 나타나는 변화와 과제를 보다 객관적으로 파악하기 위해 약 300여 명의 실무자를 대상으로 설문조사를 실시했다.

이번 조사는 디지털 환경의 변화에 따라 포렌식과 사고 대응 방식의 변화를 파악하고, 이를 통해 2026년 DFIR 분야에서 주목해야 할 핵심 기술 변화와 운영 방향에 대한 인사이트를 공유하고자 한다.

주목해야 할 흐름 Top6

Digital Forensics

Trends 1
클라우드 환경에 대한 포렌식 증거 확보 절차 마련 필요
Trends 2
디지털 포렌식 분야에서 AI 활용 확대에 따른 신뢰성 검증 및 절차 정립 필요
Trends 3
크로스 디바이스 환경에서 사용자 행위 연계 분석 역량 확보 필요

Incident Response

Trends 1
신규 위협 대응을 위한 지속적인 탐지 및 대응 역량 확보 필요
Trends 2
AI를 활용한 사고 대응 역량 개발
Trends 3
관리되지 않는 계정과 Shadow IT가 만드는 보이지 않는 공격 표면

2. Trends to Watch in DFIR for 2026

PLAINBIT

Trends to Watch in DFIR for 2026

2.1. Digital Forensics

DFIR REPORT 2026

2.1. DIGITAL FORENSICS

Trends 1.
클라우드 환경에 대한 포렌식 증거 확보 절차 마련 필요

PLB Insight | 클라우드 사고 조사에서 반복되는 증거 확보 지연과 조사 범위의 한계를 줄이기 위해 서비스별 로그 보존 및 수집 절차 마련이 필요하다.

주요 동향

최근 조직의 IT 환경은 온프레미스 중심에서 클라우드 기반 서비스로 빠르게 전환되고 있으며, 이에 따라 디지털 포렌식의 대상과 범위도 기존의 물리적 시스템 중심에서 다양한 클라우드 서비스와 계정 기반 환경으로 확대되고 있다. 그러나, 이러한 환경 변화에도 불구하고 클라우드 및 SaaS 환경에서의 증거 확보 절차와 분석 체계는 아직 충분히 정립되지 않은 경우가 많다.

설문조사 결과에 따르면, 클라우드 포렌식 증거 보존 및 분석 체계를 마련하고 있지 않다고 응답한 비율이 70% 이상으로 나타났으며, 상당수 조직이 클라우드 기반 서비스에 대한 포렌식 절차를 준비하지 못한 것으로 확인됐다. 이는 사고 발생 시 필요한 로그와 증거 데이터를 적시에 확보하지 못하거나 서비스 사업자와의 협조 절차가 명확하지 않아 조사 과정이 지연될 가능성이 있음을 의미한다.

주요 이슈 및 시사점

실제 침해사고 대응 과정에서도 클라우드 및 SaaS 환경의 로그 확보 여부가 사고 조사 기간과 분석 가능 범위를 좌우하는 사례가 반복적으로 확인됐다. 사고 조사가 시작된 시점에 이미 로그 보존기간이 만료됐거나 감사 로그가 사전에 활성화되지 않아 계정 로그인, 설정 변경, 데이터 접근 및 외부 반출 행위를 충분히 추적하지 못하는 경우가 있었다. 또한, 증거 수집에 필요한 관리자 권한을 즉시 확보하지 못하거나 서비스별 로그 제공 범위와 요청 절차를 사전에 파악하지 않아 초기 분석이 지연되는 문제도 발생했다.

수행한 사고 대응 사례를 종합하면, 클라우드 포렌식의 성패는 사고 발생 이후의 분석 기술뿐만 아니라 사고 이전에 로그, 권한 및 수집 절차를 얼마나 준비했는지에 따라 크게 좌우된다. 동일한 유형의 계정 탈취나 정보 유출 사고라도 감사 로그의 활성화 여부와 보존기간에 따라 공격자의 접근 경로와 행위 범위를 확인할 수 있는 수준에 큰 차이가 발생한다.

대응 방향 및 제언

클라우드 환경에서는 데이터가 조직 내부의 물리적 장비에만 존재하지 않으며, 서비스 제공자의 정책과 기술적 제약에 따라 접근 권한과 확보 가능한 데이터의 범위가 제한될 수 있다. 따라서, 기존의 디스크 기반 포렌식 절차를 그대로 적용하기보다 조직에서 사용하는 클라우드 및 SaaS 서비스를 식별하고, 서비스별로 확보 가능한 인증·접근·감사·설정 변경 로그와 데이터의 위치를 사전에 정리할 필요가 있다.

아울러 사고 조사에 필요한 핵심 로그의 활성화 여부와 보존기간을 점검하고, 서비스의 기본 보존정책만으로 충분한 조사 기간을 확보하기 어려운 경우에는 별도의 저장체계를 마련해야 한다. 긴급 증거 수집에 필요한 권한과 담당자를 사전에 지정하고, 콘솔 및 API를 통한 로그 추출, 스냅샷 생성, 서비스 사업자에 대한 데이터 보존 요청 및 협조 절차도 함께 문서화할 필요가 있다.

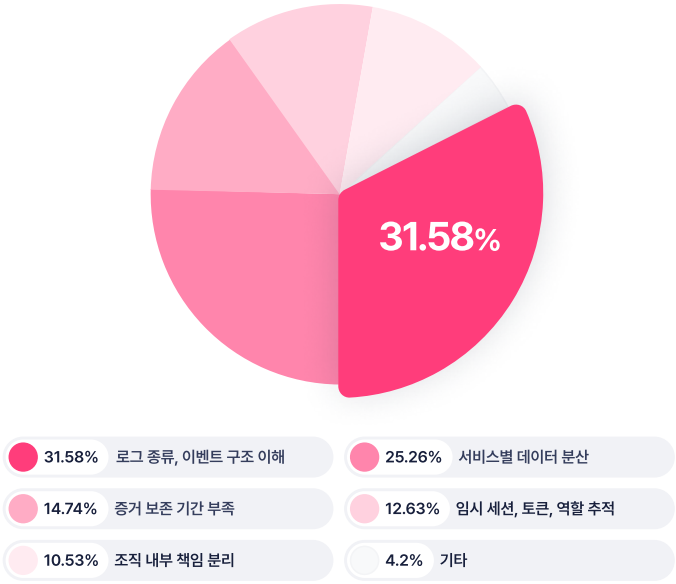
클라우드 포렌식은 사고가 발생한 이후 증거를 수집하는 활동에 그치지 않고, 평상시부터 필요한 증거가 생성·보존되고 실제로 수집 가능한지를 관리하는 과정으로 접근해야 한다. 이를 위해 서비스별 증거원과 보존 상태를 정기적으로 점검하고, 모의 수집을 통해 필요한 로그와 데이터가 실제 분석 가능한 형태로 확보되는지 검증하는 것이 필요하다.

Research

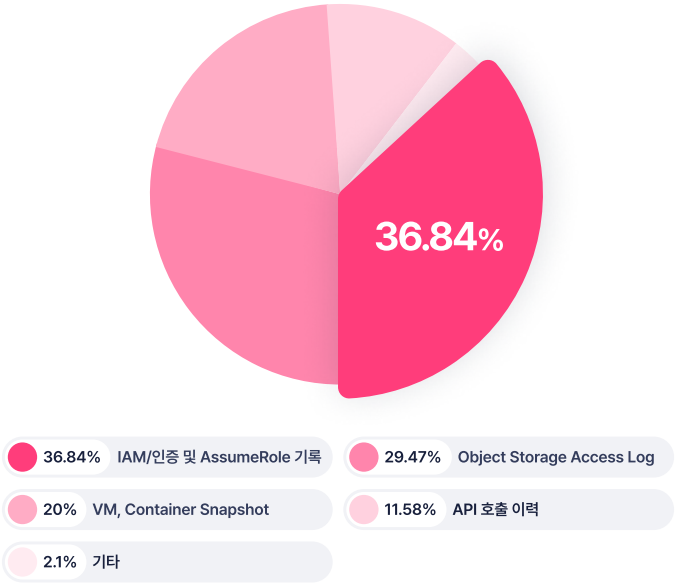
(1) 디지털 포렌식 환경

조직 내에 클라우드(AWS, Azure, GCP 등)에 대한 **포렌식 증거 보존/분석 체계**가 마련되어 있으신가요?

클라우드 포렌식(AWS, Azure, GCP 등)에서 **가장 어려운 점**은 무엇인가요?

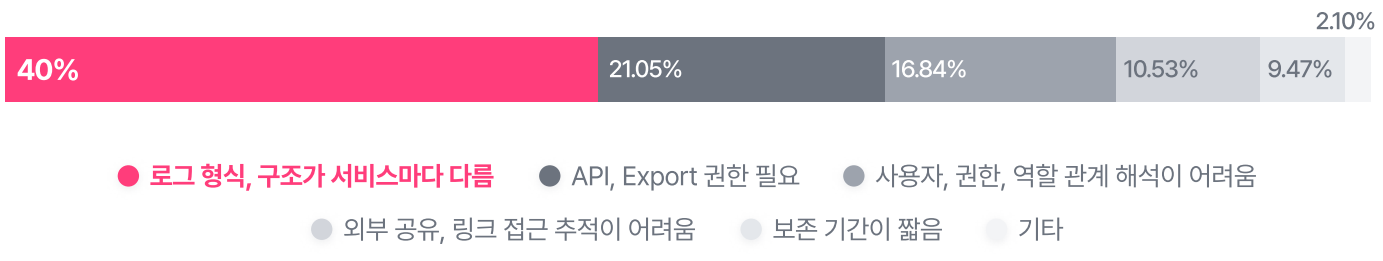


클라우드 환경의 포렌식에서 **가장 중요하다고 생각하는 증거 소스**는 무엇인가요?



조직 내에 SaaS(예: Slack, M365, Google Workspace, Confluence 등) 기반 증거 확보 시 **포렌식 절차**가 마련되어 있나요?

클라우드 포렌식에서 **가장 어려운 요소**는 무엇이라고 생각하시나요?



2.1. DIGITAL FORENSICS

Trends 2.
디지털 포렌식 분야에서 AI 활용 확대에 따른 신뢰성 검증 절차 정립 필요

PLB Insight | AI가 도출한 아티팩트 분석 결과의 신뢰성과 정확성을 객관적으로 증명할 수 있는 운영 기준 정립이 필요하다.

주요 동향

최근 생성형 AI와 자동화 기술의 발전으로 디지털 포렌식 분야에서도 대량의 데이터를 분석하고 반복적인 업무를 효율화하기 위한 AI 활용이 확대되고 있다. 대량의 파일과 아티팩트를 분류하거나 분석 결과를 요약하고 보고서 초안을 작성하는 과정에서 AI를 보조적으로 활용하는 사례가 증가하고 있으며, 이는 분석가의 업무 부담을 줄이고 핵심적인 판단과 의사결정에 집중할 수 있도록 지원하는 수단으로 주목받고 있다.

설문조사 결과에서도 AI는 참고자료 검색과 문서 요약, 파일 식별 등의 보조 업무를 중심으로 활용되고 있는 것으로 나타났다. 향후 AI가 효과적으로 개선할 수 있는 업무로는 대량 파일 및 아티팩트 분류가 가장 높은 비율로 선택됐으며, 이는 디지털 포렌식 분석 과정에서 AI가 반복적인 데이터 처리와 분석 대상 선별을 지원할 가능성이 높다는 점을 보여준다. 다만, AI 기반 분석 결과를 실제 증거로 활용하기 위해서는 결과의 신뢰성과 정확성을 객관적으로 검증할 수 있는 체계가 필요하다. 설문에서도 AI 활용이 어려운 이유로 분석 결과에 대한 신뢰성 검증 문제와 데이터 반출 제한 등 보안 및 법적 제약이 주요 요인으로 나타났다. 또한, AI 자동화를 실무에 적용하기 위해서는 관련 법적 절차의 정립과 도구의 품질 보증, 검증용 데이터셋 구축 등이 선행돼야 한다는 의견이 제시됐다.

주요 이슈 및 시사점

실제 디지털 포렌식 분석 업무에 AI를 적용·검토하는 과정에서도 AI가 생성한 결과를 별도의 확인 절차 없이 그대로 활용하기에는 여러 한계가 있었다. AI가 파일이나 아티팩트의 의미를 잘못 분류하거나 원본 데이터의 일부 맥락을 누락한 상태로 결과를 요약할 수 있으며, 실제 연관성이 확인되지 않은 여러 행위를 하나의 공격 흐름으로 연결해 해석할 가능성도 존재한다. 사건의 전체 맥락과 시스템 환경에 대한 정보가 충분히 제공되지 않으면 기술적으로 타당해 보이지만 실제 조사 결과와는 다른 결론이 도출될 수 있다.

동일한 데이터를 분석하더라도 사용한 모델과 버전, 프롬프트 및 실행 조건에 따라 결과가 달라질 수 있다는 점도 고려해야 한다. AI가 제시한 결과에 원본 아티팩트의 위치와 판단 근거가 명확하게 연결되지 않으면 분석가가 정확성을 다시 확인하기 어렵고, 동일한 분석 과정을 재현하기도 어렵다. 수사·소송·감사 과정에서 해당 결과가 어떤 데이터와 조건을 기반으로 도출됐는지를 설명하는 데에도 한계가 발생할 수 있다.

대응 방향 및 제언

현실적으로 AI는 분석가의 판단을 대체하거나 분석 결과를 단독으로 확정하는 수단보다는, 대량의 데이터에서 우선 검토 대상을 선별하고 반복적인 정리 업무를 지원하는 보조 도구로 활용하는 것이 적절하다. AI가 도출한 결과를 최종 분석에 활용하기 위해서는 원본 파일과 아티팩트, 로그 및 기존 포렌식 도구의 결과와 대조하고 분석가의 검토를 거쳐 판단 근거를 확인할 수 있어야 한다.

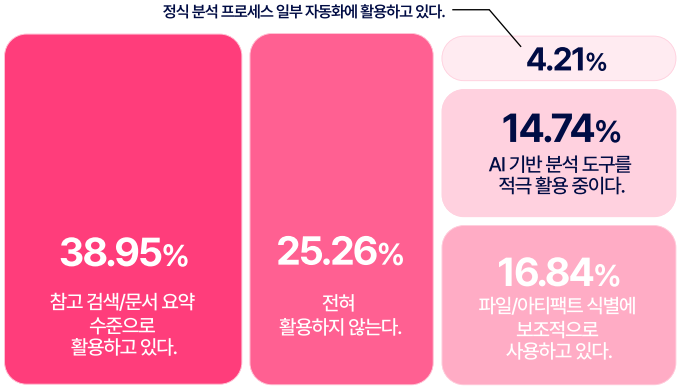
이를 위해 조직은 사용한 모델과 버전, 프롬프트, 입력 데이터, 실행 시점, 생성 결과 및 검토 이력을 기록해 분석 과정의 재현성과 추적 가능성을 확보해야 한다. 또한, 정답이 확인된 검증용 데이터셋을 활용해 정확도와 오탐·미탐 유형을 정기적으로 점검하고, 모델 변경 시 재검증하는 절차가 필요하다. 외부 AI 서비스 활용 시에는 민감정보 입력 제한, 비식별화, 내부 구축형 AI 적용 기준 등 데이터 보호 절차도 함께 마련해야 한다.

디지털 포렌식에서 AI 활용의 핵심은 기술 도입 자체보다 AI가 도출한 결과를 어떤 방식으로 검증하고 기록하며 분석가의 판단과 결합할 것인지가 중요하다. AI 분석 결과를 신뢰할 수 있는 증거로 활용하기 위해 원본 대조, 분석가 검토, 재현성 확보, 도구 품질 검증 및 데이터 보호가 포함된 검증 절차와 운영 기준을 체계적으로 마련해야 한다.

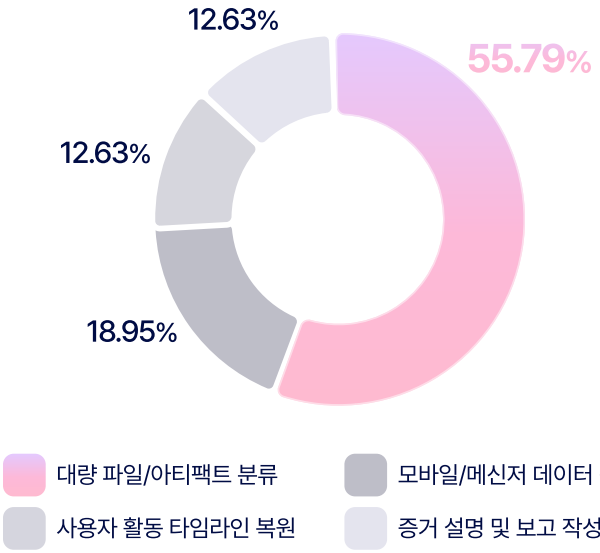
Research

(2) 디지털 포렌식 현황

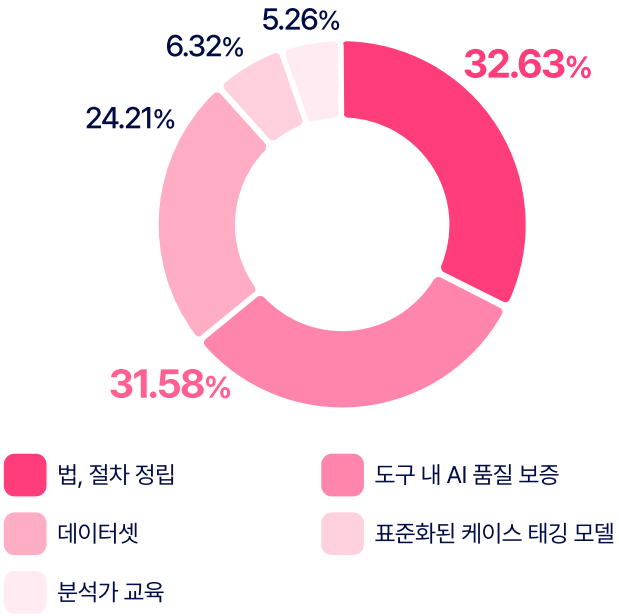
디지털 포렌식 분석에서 **AI**를 활용하고 계신가요?



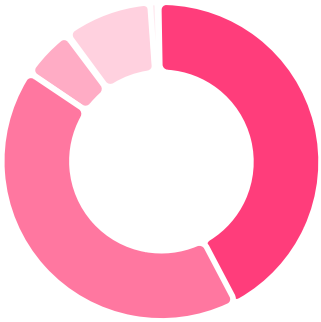
디지털 포렌식 분석에서 AI가 어떤 부분을 **가장 효과적으로 개선**할 수 있다고 생각하시나요?



디지털 포렌식 AI 자동화가 현실화되기 위해 **가장 먼저 필요한 요소**는 무엇이라고 생각하시나요?



디지털 포렌식에서 **AI 활용이 어려운 이유**는 무엇인가요?



AI 분석 결과의 신뢰성 검증이 어려움	42.86%
증거 데이터 반출/업로드 불가 (보안/법적 제약)	42.11%
분석가의 업무 방식과 맞지 않음	5.26%
조직 내부 교육/도입 가이드 부족	9.02%
정형화된 범죄유형을 정의하기 곤란함	0.75%

2.1. DIGITAL FORENSICS

Trends 3.
크로스 디바이스 환경에서 사용자 행위 연계 분석 역량 확보 필요

PLB Insight

디지털 포렌식의 핵심은 개별 매체의 분석이 아니라, PC·모바일·클라우드에 분산된 데이터를 통합해 사용자의 전반적인 행위 흐름을 시간 순서대로 재구성하는 역량에 있다.

주요 동향

최근 디지털 환경에서는 하나의 사용자가 단일 기기만을 사용하는 경우가 줄어들고 있으며, 업무와 개인 활동이 PC, 모바일 기기, 클라우드 서비스, 메신저 등 다양한 플랫폼에 분산되어 이루어지는 것이 일반적인 형태로 자리 잡고 있다. 이에 따라, 디지털 포렌식 분석도 특정 기기 하나를 중심으로 수행하는 방식에서 벗어나, 여러 기기와 계정 및 서비스에 분산된 데이터를 종합적으로 분석하는 방식으로 변화하고 있다.

설문조사 결과에서도 동일 사용자에 대해 여러 기기를 동시에 분석해야 하는 사례가 증가하고 있는 것으로 나타났으며, 데이터가 서로 다른 위치에 저장되거나 동기화 범위가 명확하지 않아 분석 과정에서 어려움을 겪는 경우가 적지 않은 것으로 확인됐다. 모바일 기기와 클라우드 서비스 간 데이터 동기화, 계정 기반 접근 기록, 다양한 타임존 환경에서 생성된 로그를 하나의 사건 흐름으로 재구성하는 과정은 기존의 단일 매체 분석보다 높은 수준의 분석 역량을 요구한다.

주요 이슈 및 시사점

실제 디지털 포렌식 및 침해사고 대응 과정에서도 과거에는 사용자 PC 한 대의 분석만으로 주요 행위를 확인할 수 있는 경우가 많았으나, 최근에는 동일 사용자의 PC와 모바일 기기를 함께 분석하거나 클라우드 계정 및 메신저·이메일 기록까지 추가로 확인해야 사건의 전체 흐름을 파악할 수 있는 사례가 증가하고 있다.

PC에서는 파일 생성과 실행 흔적이 확인되고, 모바일 기기에서는 관련 메시지나 인증 행위가 발견되는 등 하나의 사용자 행위가 여러 기기와 서비스에 나뉘어 기록되는 경우도 나타나고 있다. 이처럼 일부 기기만을 분석하면 사건의 시작과 이후 행위가 서로 단절되어 보이거나, 사용자 의도와 행위 순서를 잘못 판단할 가능성이 있다.

계정 로그인, 파일 전송, 클라우드 동기화, 다중인증 승인과 같은 행위는 각각 다른 기기와 서비스에 흔적이 남을 수 있어, 개별 기기 분석만으로는 행위 간 연관성을 충분히 설명하기 어렵다. 이는 디지털 포렌식의 분석 단위가 저장매체나 기기 중심에서 사용자와 계정 중심으로 이동하고 있음을 보여준다.

대응 방향 및 제언

조사가 착수되는 순간부터 분석 대상 사용자가 이용한 PC와 모바일 기기, 클라우드 계정, 이메일 및 메신저 등 관련 데이터의 범위를 함께 식별해야 한다. 단순히 확보된 기기를 순차적으로 분석하는 것이 아니라, 사용자 계정과 기기 간 연동 관계, 데이터 동기화 여부, 접속 이력과 인증 기록을 기준으로 수집 우선순위와 분석 범위를 결정할 필요가 있다.

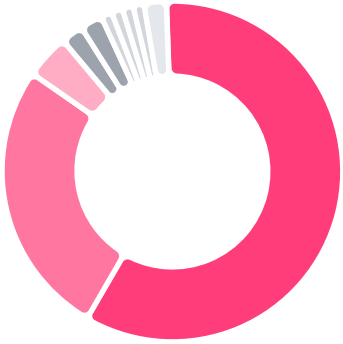
여러 기기와 서비스에서 수집된 데이터는 타임존과 시간 정확성을 확인한 후, 계정, 기기 식별자, IP 주소, 파일 해시 등 공통 식별정보를 기준으로 연계해 통합 타임라인을 구성해야 한다. 이와 함께 데이터의 출처와 동기화·중복 여부를 구분할 수 있도록 수집 정보를 명확히 기록해야 한다.

수집 범위는 사건 유형과 조사 목적에 따라 단계적으로 확대하고, 개인정보 및 업무 외 데이터의 불필요한 수집을 최소화할 수 있도록 접근 권한과 분석 범위에 대한 기준을 마련해야 한다. 크로스 디바이스 환경에서는 개별 기기에서 발견된 흔적을 각각 해석하는 것만으로 사건의 전체 맥락을 파악하기 어렵다. **PC, 모바일, 클라우드 및 계정 기반 서비스에 분산된 데이터를 사용자 행위를 중심으로 연결하고, 시간 순서에 따라 재구성할 수 있는 수집·분석 절차와 통합 타임라인 분석 역량을 확보하는 것이 중요하다.**

Research

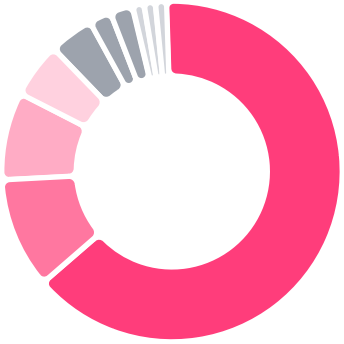
(3) 디지털 포렌식 도구

조직에서 **가장 많이 다루는 디지털 포렌식 분야**는?



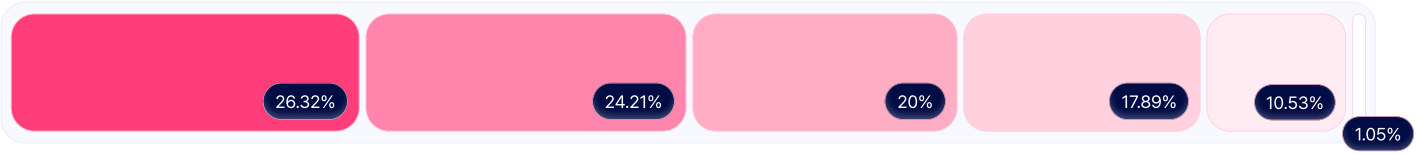
모바일 포렌식	**58.95%**
디스크 포렌식	26.32%
클라우드 포렌식	4.21%
IoT 포렌식	2.11%
메모리 포렌식	2.11%
AI 포렌식	1.05%
IoT 제외 전부	1.05%
네트워크 포렌식	1.05%
데이터베이스 포렌식	1.05%
멀티미디어 포렌식	2.10%

조직에서 **가장 비중이 늘어난 디지털 포렌식 분야**는?



모바일 포렌식	**64.21%**
클라우드 포렌식	10.53%
디스크 포렌식	8.42%
데이터베이스 포렌식	5.26%
IoT 포렌식	4.21%
네트워크 포렌식	2.11%
메모리 포렌식	2.11%
AI 포렌식	1.05%
apple product	1.05%
영상분석	1.05%

크로스 디바이스 분석에서 **가장 어려운 부분**은 어떤거라고 생각하시나요?

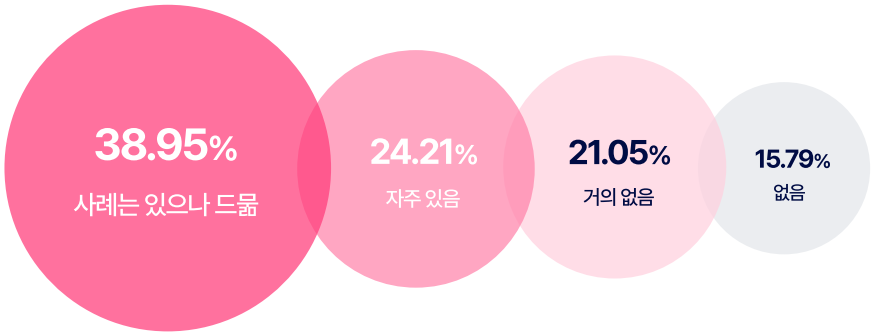


- **데이터 저장 위치가 기기마다 상이함** 26.32%
- **동기화 데이터의 범위 불명확** 24.21%
- **타임스탬프, 타임존 불일치** 20%
- **계정과 실제 사용자 동작에 대한 행위 분석** 17.89%
- **세션 및 토큰 공유 판단의 어려움** 10.53%
- **기타** 1.05%

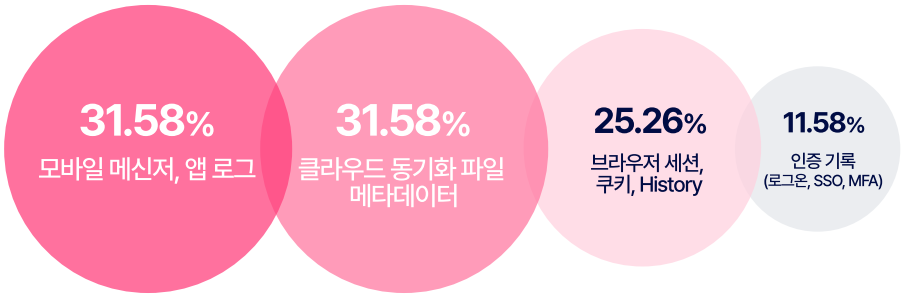
Research

(3) 디지털 포렌식 도구

포렌식 분석 시 **동일 사용자의 여러 기기**(PC, 모바일, 가상환경, VDI) 활동을 연결해 분석한 경험이 있으신가요?



크로스 디바이스 환경에서 **가장 핵심 증거가 되는 데이터**는 무엇이라고 생각하시나요?



PLAINBIT

Trends to Watch in DFIR for 2026

2.2. Incident Response

DFIR REPORT 2026

2.2. INCIDENT RESPONSE

Trends 1.
신규 위협 대응을 위한 지속적인 탐지 및 대응 역량 확보 필요

PLB Insight

중요한 것은 어떤 솔루션을 도입했는가가 아니라,
탐지된 위협을 얼마나 빠르고 지속적으로 확인·판단·대응할 수 있는가이다.

주요 동향

많은 조직이 EDR, SIEM 등 다양한 보안 솔루션을 도입하며 위협 탐지 체계를 강화하고 있다. 그러나, 실제 침해사고 대응 과정에서는 보안 장비를 보유하고 있음에도 신규 위협을 신속하게 식별하고 대응하는 데 어려움을 겪는 사례가 반복되고 있다. 조직 내에서 크리티컬한 위협으로 인식되는 정보 유출 사고 역시 기술 자체의 부족보다는 탐지된 이상 행위를 지속적으로 확인하고 대응할 수 있는 운영 역량의 부족에서 비롯되는 경우가 많다.

보안 환경이 복잡해지고 공격 기법이 빠르게 변화하면서 단순히 보안 솔루션을 도입하는 것만으로는 모든 위협에 효과적으로 대응하기 어려운 상황이 되고 있다. 실제로 많은 조직이 EDR을 도입하고 있음에도 이를 지속적으로 모니터링하고 탐지된 이벤트의 위험도를 판단하며 필요한 대응 조치를 수행할 수 있는 전문 인력과 운영체계를 충분히 확보하지 못해 대응이 지연되거나 사고로 이어지는 사례가 발생하고 있다.

주요 이슈 및 시사점

실제 침해사고 대응 과정에서도 보안 솔루션이 위협 징후를 사전에 탐지했지만 담당자가 이를 정상 행위나 단순 오탐으로 판단해 후속 분석이 이루어지지 않거나, 야간·휴일에 발생한 경보가 즉시 확인되지 않아 공격자의 활동이 장기간 지속된 사례가 반복적으로 확인됐다. EDR 에이전트가 일부 핵심 시스템에 설치되지 않았거나, SIEM에 필요한 로그가 연계되지 않아 공격 흐름을 충분히 추적하지 못한 경우도 있었다. 다수의 경보가 누적되는 환경에서는 실제 대응이 필요한 위협이 다른 이벤트에 묻혀 초기 대응 시점을 놓치기도 했다.

이러한 사례를 종합하면 사고 대응의 성패는 보안 솔루션의 도입 여부보다 탐지 범위와 로그 수집 상태를 지속적으로 점검하고, 발생한 경보의 우선순위를 판단해 실제 대응으로 연결할 수 있는 운영체계에 의해 좌우된다. 계정 탈취, 내부 확산, 정보 유출과 같은 공격은 하나의 고위험 경보로 명확하게 나타나기보다 여러 시스템에서 발생한 작은 이상 징후가 누적되는 형태로 진행될 수 있어, 개별 경보가 아닌 행위의 연관성과 변화 추이를 지속적으로 확인해야 한다.

대응 방향 및 제언

조직은 우선 EDR과 SIEM이 실제 핵심 자산과 계정을 충분히 모니터링하고 있는지 점검하고, 로그 미수집 구간과 탐지 사각지대를 정기적으로 식별해야 한다. 탐지된 경보는 위험도와 업무 영향을 기준으로 우선순위를 구분하고, 경보 확인부터 분석, 격리, 계정 차단, 증거 보존 및 보고까지 이어지는 대응 절차와 담당자의 역할을 사전에 정의할 필요가 있다. 반복적으로 발생하는 오탐은 탐지정책을 조정하되, 예외 처리 과정에서 실제 공격 징후가 제외되지 않도록 검토 이력과 승인 절차도 함께 관리해야 한다.

또한, 대응 속도와 품질을 객관적으로 확인할 수 있도록 경보 확인 시간, 분석 착수 시간, 조치 완료 시간, 미처리 경보 수 등의 운영 지표를 관리하고, 실제 공격 시나리오를 기반으로 탐지·대응 훈련을 정기적으로 수행해야 한다. 내부 인력만으로 상시 모니터링과 신속한 대응이 어려운 경우에는 MDR, 사고 대응 리테이너 또는 외부 전문 인력을 활용해 야간·휴일을 포함한 대응 공백을 보완하는 방안도 고려할 필요가 있다.

최근 사고 대응의 흐름은 새로운 보안 기술을 지속적으로 추가하는 방식에서, 기존에 도입한 보안 솔루션이 실제 위협 탐지와 대응에 활용될 수 있도록 운영 역량을 강화하는 방향으로 이동하고 있다. **결국 사고 대응 역량은 어떤 보안 솔루션을 보유하고 있는지가 아니라, 탐지된 위협을 놓치지 않고 신속하게 판단 필요한 조치를 지속적으로 수행할 수 있는 체계를 갖추고 있는가에 의해 결정된다.**

Research

(1) 침해사고 대응 환경

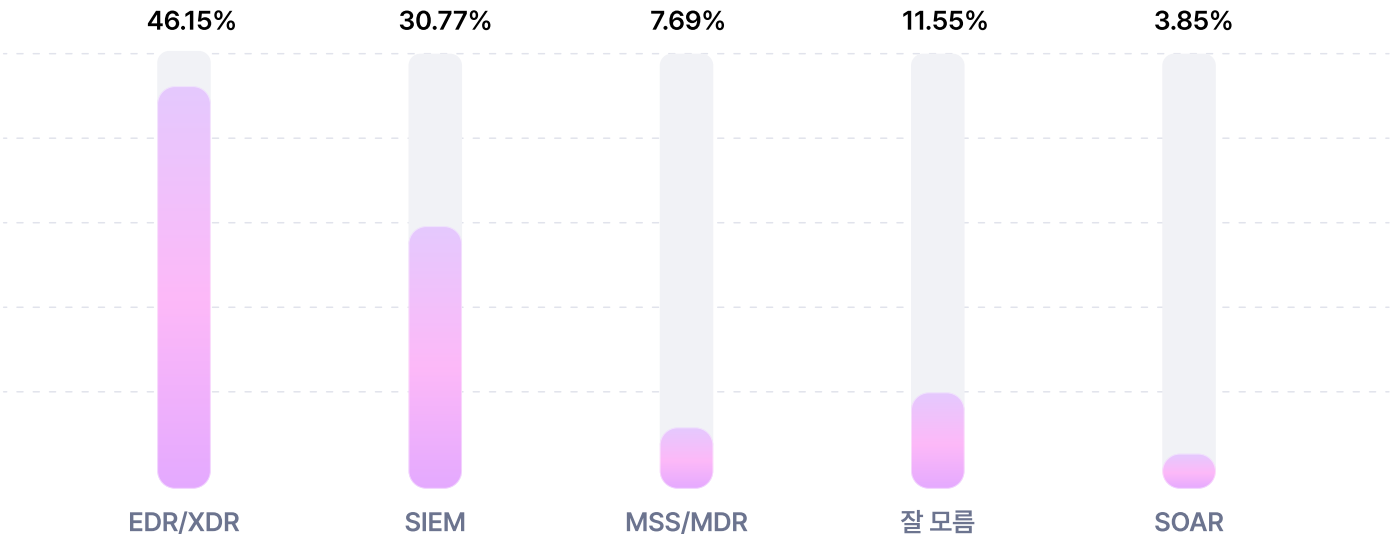
조직 내 **사고 대응 팀의 구조**는 어떤 형태로 구성되어 있나요?

IT 또는 보안팀 내에 사고 대응 담당이 포함되어 있다.	**46.15%**
독립적인 사고 대응 팀이 있다.	42.31%
사고 대응 팀이 존재하지 않는다.	11.54%

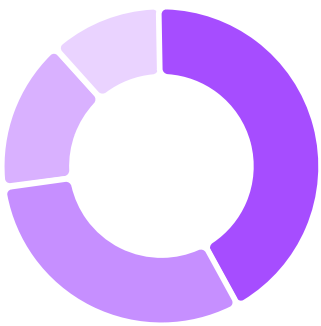
침해사고 대응을 위해 귀하가 보유하고 있는 **상용 솔루션의 유형**은 무엇인가요? (모두 선택)

로그 분석 (SIEM, Splunk, ELK 등)	**27.27%**
악성코드 분석 (IDA, Joe SandBox, Anyrun, Hybrid Analysis 등)	**27.27%**
인텔리전스 (VirusTotal, Criminal IP, ATIP, QUAXAR 등)	24.24%
포렌식(원인 분석) (X-Ways Forensics, Magnet AXIOM, Cyber Triage 등)	12.12%
기타	9.09%

현재 귀하의 조직에서 운영 중인 보안 솔루션 중 탐지/대응 관점에서 **가장 효과적이라고 판단되는 솔루션**은 무엇인가요?

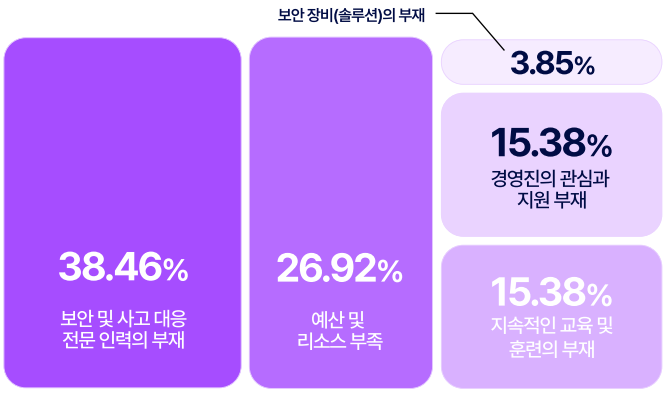


현재 조직에서 사고 대응과 관련해 겪고 있는 **가장 큰 문제**는 무엇입니까?

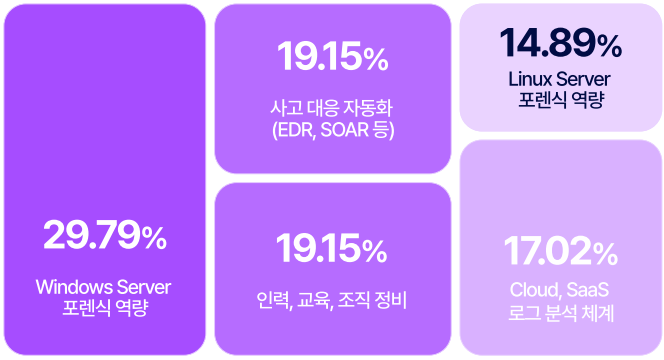


신규 위협에 대한 탐지 및 대응 능력 부족	**42.31%**
탐지 및 대응 속도의 지연	30.77%
인력 부족으로 인한 업무 과부하	15.38%
DFIR 관련 교육 및 기술 습득 기회 부족	11.54%

침해사고가 발생하는 **가장 큰 환경적인 요인**은 무엇인가요?



귀하의 조직에서 **가장 필요한 역량**은 무엇이라고 생각하시나요?



2.2. INCIDENT RESPONSE

Trends 2.
AI를 활용한 사고 대응 역량 개발

PLB Insight

AI 자체가 조직의 보안 경쟁력이 될 수는 없으므로, 데이터 보호와 결과 검증 등 분석가의 책임하에
AI를 실전 대응 도구로 길들이는 '운영 역량의 확보'가 사고 대응 속도와 품질을 높이는 핵심 열쇠이다.

주요 동향

많은 조직이 사고 대응 과정에서 증가하는 분석 업무와 전문 인력 부족으로 인해 대응 속도와 품질을 동시에 유지하는 데 어려움을 겪고 있다. 다양한 보안 장비와 시스템에서 생성된 로그를 수집·정리하고, 다수의 이벤트 중 조사 대상을 선별하며, 분석 결과를 문서화하는 업무에는 많은 시간이 소요된다. 이러한 반복 작업이 지연되면 사고 초기 단계에서 필요한 판단과 대응 조치도 함께 늦어질 수 있다.

최근에는 이러한 문제를 해결하기 위한 방안으로 생성형 AI를 포함한 다양한 AI 기술을 사고 대응 업무에 적용하려는 시도가 증가하고 있다. AI는 대량의 로그와 탐지 이벤트를 빠르게 분류하고, 의심스러운 행위의 우선순위를 제시하거나 여러 시스템에서 확인된 정보를 하나의 타임라인으로 정리하는 데 활용할 수 있다. 조사 결과 요약과 보고서 초안 작성 등 반복 업무를 보조함으로써 분석가가 사고 범위 판단과 대응 전략 수립에 집중하도록 지원하는 역할도 기대된다.

주요 이슈 및 시사점

수행한 침해사고 대응 사례를 종합하면, 사고 초기에는 EDR, 방화벽, 인증 시스템, 서버 및 클라우드 등 서로 다른 환경에서 확보한 데이터를 정리하고 연관성을 확인하는 데 상당한 시간이 소요된다. 수집된 로그의 형식과 시간 기준이 서로 다르거나 분석 대상 시스템이 많은 경우, 공격 흐름을 구성하기 위한 전처리와 반복 검토가 초기 대응 속도에 직접적인 영향을 미친다. 이러한 영역은 AI를 활용해 분석 대상의 범위를 좁히고, 우선 확인이 필요한 행위와 데이터를 제시함으로써 실질적인 업무 효율을 높일 수 있는 부분이다.

다만, AI가 제시한 결과만으로 사고 원인이나 피해 범위를 확정하는 것은 어렵다. 정상적인 관리 행위를 공격자의 활동으로 잘못 판단하거나, 서로 관련되지 않은 이벤트를 하나의 공격 흐름으로 연결할 수 있으며, 조직의 시스템 구성과 업무 맥락이 충분히 반영되지 않으면 기술적으로는 자연스럽지만 실제 상황과 다른 분석 결과가 제시될 수 있다.

대응 방향 및 제언

AI는 모든 사고를 자동으로 탐지·대응하는 수단보다 초기 분류, 로그 요약, 공격 흐름 정리, 유사 이벤트 검색 등 분석가의 판단 범위를 좁히고 반복 업무를 줄이는 보조 도구로 활용하는 것이 적절하다. 사고 여부, 영향 범위, 침해 원인 및 대응 조치 등 주요 판단은 원본 데이터와 기존 분석 도구의 결과를 근거로 분석가가 검토해야 한다.

실제 업무 적용을 위해서는 단계별 AI 활용 범위와 검토 기준을 정의하고, AI 분석 결과가 원본 로그 및 이벤트와 연결되도록 해야 한다. 고위험 판단이나 차단·격리 등 주요 대응 조치는 담당자의 승인을 거치도록 하며, 모델·버전·프롬프트·입력 데이터·실행 결과 및 수정 이력을 기록해 재현성과 추적 가능성을 확보할 필요가 있다.

또한, 과거 사고 및 모의훈련 데이터를 활용해 정확도와 오탐·미탐을 지속적으로 검증하고, 외부 AI 활용 시에는 민감정보 입력 제한, 비식별화 및 내부 구축형 AI 적용 기준 등 데이터 보호정책을 함께 마련해야 한다.

결국 AI 기반 사고 대응 역량은 솔루션 도입 자체보다 AI의 활용 범위를 명확히 하고, 결과를 검증·통제하며 기존 사고 대응 절차에 안정적으로 통합할 수 있는 운영체계를 갖추는 것이 중요하다. 향후 조직의 사고 대응 경쟁력은 AI를 얼마나 많이 사용하는가보다, 실제 대응 업무에 얼마나 정확하고 안전하게 활용할 수 있는가에 의해 결정될 것이다.

Research

(2) 사고 대응 현황

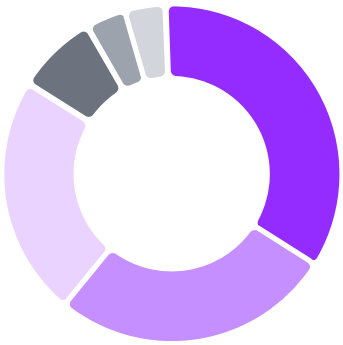
귀하의 조직은 DFIR 업무를 위해 **AI를 활용**하고 계신가요?

- **시범적으로 일부 영역에서만 활용 중이다.** 61.54%
- 전혀 활용하고 있지 않다. 19.23%
- 다수의 영역에서 적극 활용 중이다. 15.38%
- 정식 업무 프로세스에 제한적으로 포함되어 있다. 3.85%

DFIR 업무에서 **주로 사용하는 AI 유형**은 무엇인가요?

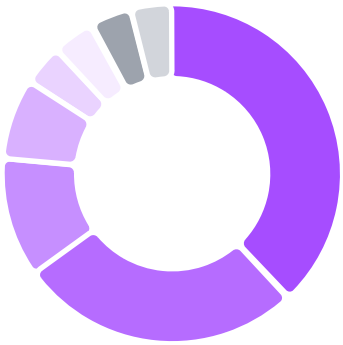
- **생성형 AI (예: ChatGPT, Claude 등)** 65.38%
- 자체 학습 또는 사내 모델 (Large/SBERT 등) 15.38%
- SIEM/EDR 내 내장형 AI 분석 기능 11.54%
- 오픈소스 ML 기반 포렌식/탐지 엔진 3.85%
- 기타 3.85%

AI 사용 시 **가장 기대되는 효과**는 무엇인가요?



분석 속도 향상	**34.62%**
분석 인력의 부담 감소	26.92%
분석 속도 향상, 분석 인력의 부담 감소	23.08%
신규 인력 온보딩 시간 단축	7.69%
고객/경영진 설명 품질 향상	3.85%
분석 인력의 부담 감소, 신규 인력 온보딩 시간 단축, 고객/경영진 설명 품질 향상	3.85%

AI 활용 시 **가장 우려하는 부분**은 무엇인가요?



내부 데이터 반출 우려 (보안/규정 준수)	**38.46%**
AI 결과의 신뢰성 검증 어려움	26.92%
실전 로그/아티팩트 해석 정확도 제한	11.54%
내부 데이터 반출 우려 (보안/규정 준수), AI 결과의 신뢰성 검증 어려움	7.69%
조직 내부 정책 변화의 어려움	3.85%
AI 결과의 신뢰성 검증 어려움, 실전 로그/아티팩트 해석 정확도 제한	3.85%
내부 데이터 반출 우려 (보안/규정 준수), AI 결과의 신뢰성 검증 어려움, 조직 내부 정책 변화의 어려움	3.85%
보안	3.85%

2.2. INCIDENT RESPONSE

Trends 3.
관리되지 않는 계정과 Shadow IT가 만드는 보이지 않는 공격 표면

PLB Insight | 공격 표면 관리(ASM)를 넘어 조직 내부와 연계 생태계 전반의 자산 현황을 실시간으로 식별하는 '가시성 중심의 보안 체계'로 전환해야 한다.

주요 동향

많은 조직이 External Attack Surface Management(EASM)와 취약점 관리 등을 통해 외부에 노출된 공격 표면을 줄이는 데 집중하고 있다. 그러나, 실제 침해사고 대응 과정에서는 외부에 공개된 시스템뿐만 아니라, 조직이 존재 여부와 사용 현황을 정확히 파악하지 못한 계정과 자산이 공격의 시작점이 되는 사례가 반복적으로 확인되고 있다. 보안 통제의 적용 여부를 판단하려면 먼저 조직이 보유하고 있거나 연결되어 있는 계정과 자산을 식별할 수 있어야 하지만, 실제 환경에서는 이 기본적인 가시성이 충분히 확보되지 않은 경우가 많다.

업무 환경이 복잡해지고 협력사 및 유지보수 인력과의 협업이 증가하면서 조직 내부에는 공식적인 절차를 거치지 않고 생성된 테스트 서버, 임시 시스템, 클라우드 인스턴스, SaaS 서비스와 같은 Shadow IT가 지속적으로 늘어나고 있다. 프로젝트 종료 후에도 삭제되지 않은 계정, 퇴직자 및 부서 이동자의 권한, 장기간 사용되지 않은 관리자 계정 등도 함께 누적되고 있다. 이러한 자산과 계정은 보안정책이 적용되지 않거나 소유자와 관리 책임이 불분명한 경우가 많아, 공격자가 새로운 취약점을 악용하지 않더라도 기존 접근 권한을 이용해 내부 시스템에 접근할 수 있는 경로가 된다.

주요 이슈 및 시사점

수행한 침해사고 대응 사례를 종합하면, 공격자는 반드시 최신 취약점이나 고도화된 공격 기법만을 이용하지 않았다. 관리되지 않는 테스트 서버와 임시 시스템, 외부에 노출된 원격접속 서비스, 장기간 변경되지 않은 계정정보와 같은 기존 관리 공백을 초기 침투와 내부 확산에 활용하는 경우가 확인됐다.

사고 조사 과정에서 조직이 해당 자산의 존재를 뒤늦게 인지하거나, 자산 소유자와 관리 부서를 즉시 확인하지 못해 조사 범위와 대응 대상을 다시 설정해야 하는 경우도 있었다. 랜섬웨어 사고에서는 공격자가 관리되지 않는 시스템을 주요 거점으로 활용하거나, 유지보수 및 원격지원 목적으로 생성된 계정을 통해 내부 시스템에 접근하는 사례가 발생할 수 있다. 이러한 계정은 업무상 필요에 따라 높은 권한을 보유하는 경우가 많지만, 접속 가능한 시스템과 사용기간이 명확하게 제한되지 않거나 다중인증과 접속기록 관리가 적용되지 않는 경우도 있다.

이로 인해 정상적인 유지보수 행위와 공격자의 계정 악용을 구분하기 어려워지고, 최초 침투 시점과 실제 피해 범위를 확인하는 데에도 시간이 소요될 수 있다. 유지보수사와 협력사 계정이 여러 고객사를 지원하는 과정에서 동일하거나 유사한 방식으로 운영되는 점도 구조적인 위험요인이다. 특정 협력사의 계정이 탈취되거나 원격접속 환경이 침해되면 동일한 계정정보, 접속 방식 또는 관리도구를 사용하는 다른 조직으로 공격이 확산될 수 있다. 따라서, 협력사 계정은 조직 내부 계정과 별개로 관리할 대상이 아니라, 조직의 전체 공격 표면에 포함된 접근 주체로 인식해야 한다.

대응 방향 및 제언

조직은 ASM을 통해 확인되는 외부 노출 자산뿐만 아니라 내부 자산관리시스템, 클라우드 관리 콘솔, 인증시스템, 원격접속 기록 등을 연계해 실제 운영 중인 자산과 계정 현황을 정기적으로 점검해야 한다. 신규 서버와 클라우드 자원은 소유자, 사용 목적, 운영 기간 및 관리부서를 등록하도록 하고, 미등록 또는 소유자가 불분명한 자산은 별도의 확인 및 접근 제한 절차를 적용할 필요가 있다.

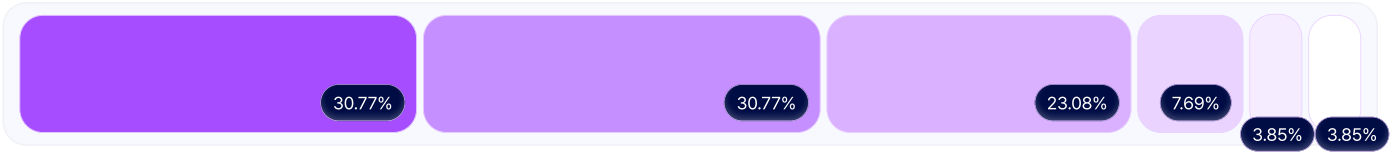
계정은 생성부터 변경·만료·삭제까지 전 수명주기를 관리하고, 장기 미사용 및 퇴직자 계정은 정기적으로 비활성화해야 한다. 특히 고권한·외부접속·협력사 계정은 사용기간과 권한 범위를 제한하고 다중인증을 적용하며, 접속 및 주요 행위 기록을 보존해 실제 사용자를 추적할 수 있어야 한다.

보이지 않는 공격 표면을 줄이기 위해서는 외부 노출 여부만 확인하는 것을 넘어, 내부·클라우드·협력사 환경에 연결된 자산과 계정을 지속적으로 식별하고 소유자, 권한, 사용기간 및 접속이력을 관리하는 체계를 갖추는 것이 중요하다. 결국 보안 운영의 핵심은 새로운 통제 수단을 추가하는 것보다 조직의 자산과 계정 현황을 얼마나 정확하게 파악하고 통제할 수 있는가에 있다.

Research

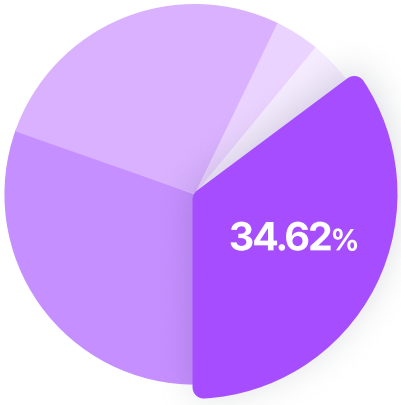
(3) 사고 대응 서비스

사고 대응 시 **원인을 파악하기 어려웠던 이유**는 무엇인가요?



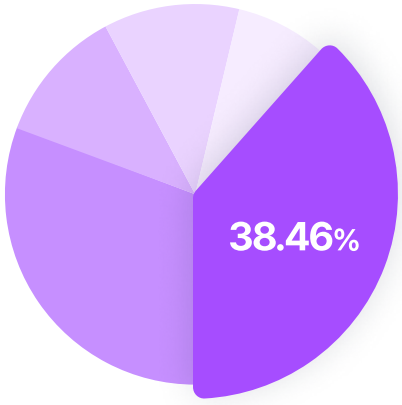
- **유지보수, 외부 협력사 단말 관리 불투명** 30.77%
- **로그 보존 기간 또는 로그 수집 범위 부족** 30.77%
- **미등록 서버, VM, Container 존재** 23.08%
- **SSH Key 또는 계정 공유 또는 재사용** 7.69%
- **잘 모름** 3.85%
- **로그가 여러 위치에 분산 (클라우드, SaaS, VM, vSphere 등)** 3.85%

유지보수사, 협력사, 외부 파견 인력은 조직 자산에 **어떤 방식으로 접속**하고 있나요?



- 34.62% 기업지급 장비
- 30.77% 원격접속 VPN
- 26.92% 개인 노트북
- 3.85% 관리단말
- 3.85% 잘 모름

외부 인력에 대한 계정(유지보수사, 협력사 등)은 **어떤 형식으로 발급**되나요?

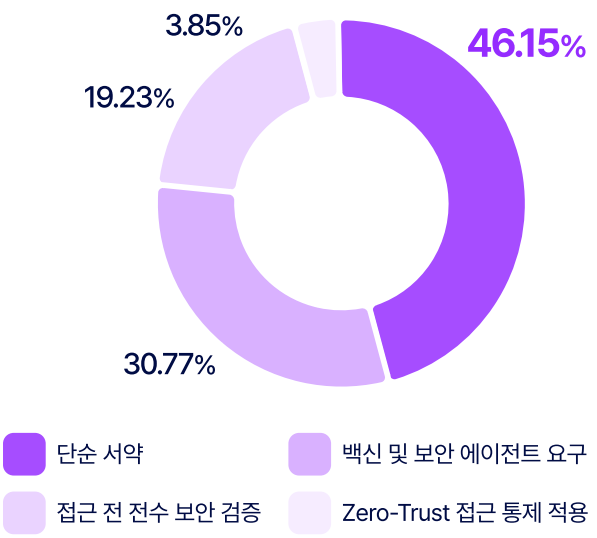


- 38.46% 개별 + 공유 혼용
- 30.77% 100% 개별 계정
- 11.54% 공용 계정
- 11.55% 기타
- 7.69% 외부 인력이 관리하는 시스템은 외부 인력이 자체적으로 설정해 활용

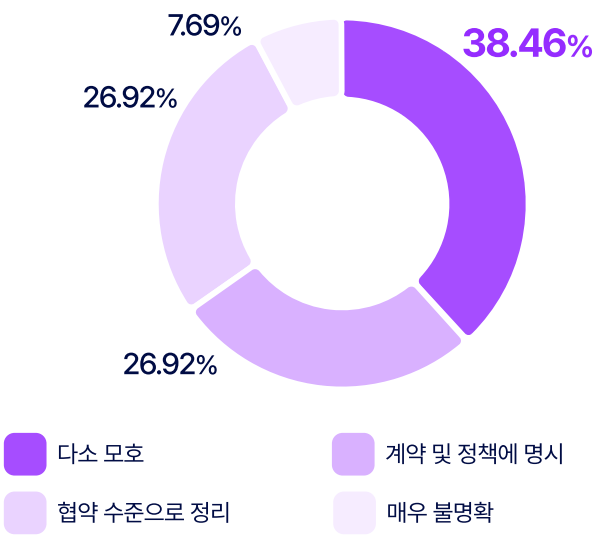
조직 내 자산 현황(서버, PC, VM, 클라우드)을 **중앙에서 일원화해 관리**하고 계신가요?

대체로 관리하고 있다.	**38.46%**
대부분 관리하고 있다.	23.08%
일부 부서만 해당된다.	19.23%
전혀 아니다.	15.38%
중앙에서 일원화해 관리하고 있다.	3.85%

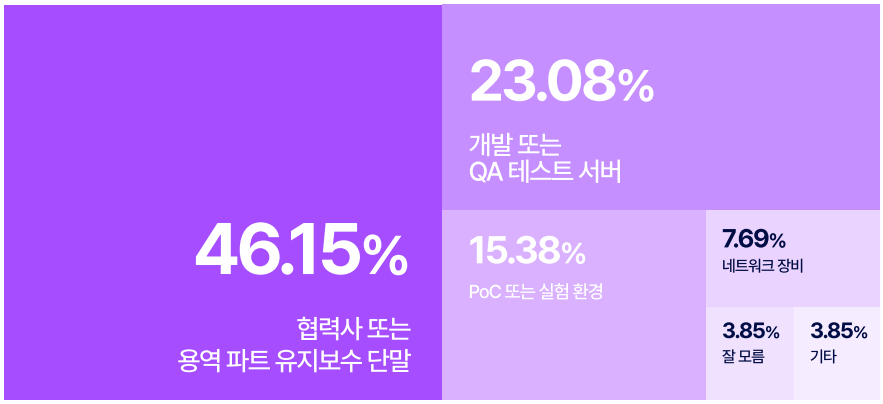
외부 인력 장비에 대한 **보안 준수 요구 수준**은 어느정도인가요?



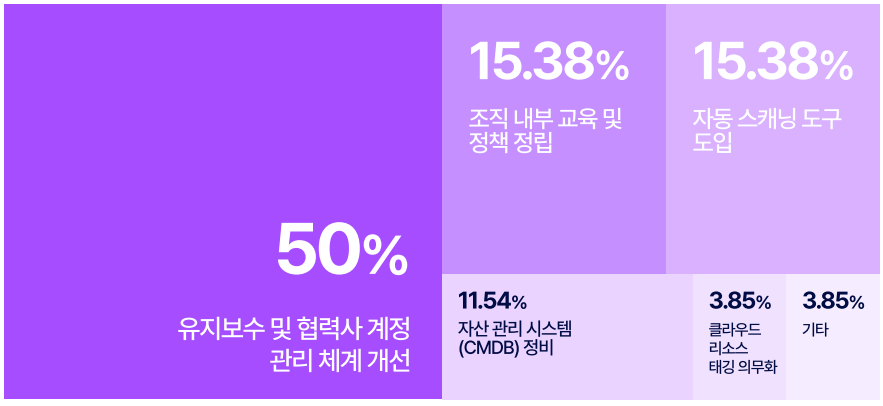
조직 내에서 외부 인력에 관련한 사고 발생 시 **책임 및 조치 기준**이 **명확**한가요?



Shadow Asset(공식적으로 등록·관리되지 않거나, 조직의 IT·보안 관리 체계 밖에서 존재하는 자산) 발생이 **가장 심한 영역**은 어디인가요?



Shadow IT/Asset 문제를 줄이기 위해 **가장 필요한 조치**는 무엇이라고 생각하시나요?



3. Wrap Up

Wrap Up | 결론

본 설문의 결과는 디지털 포렌식과 침해사고 대응 분야가 직면한 현식적인 변화와 앞으로 준비해야 할 핵심 과제를 보여주고 있다.

기술 환경은 빠르게 변화하고 있으며, 그에 따라 분석 대상과 대응 방식 역시 점점 더 복잡해지고 있다. 이제 조직은 단순히 사고를 처리하는 수준을 넘어, 변화하는 환경 속에서 지속적으로 대응 역량을 유지하고 검증할 수 있는 체계를 갖추어야 하는 시점에 와 있다.

각 영역을 대표하는 핵심 메시지는 다음과 같다.

Digital Forensics

| 증거는 한 곳에 남지 않는다. 연결해야 비로소 사건이 보인다.

디지털 포렌식 환경은 더 이상 특정 시스템이나 단일 저장 매체를 중심으로 이루어지지 않는다. 클라우드 서비스의 확산, 모바일 기기와 다양한 디지털 환경의 일반화는 데이터와 사용자 행위를 여러 시스템과 계정에 분산시키고 있으며, 이에 따라 사건의 단서를 찾기 위해서는 다양한 환경에 분산된 데이터를 종합적으로 수집하고 분석하는 역량이 요구되고 있다.

하나의 사건이 여러 기기와 서비스에 걸쳐 동시에 흔적을 남기는 환경에서는 단일 기기 중심 분석만으로 사건의 전체 흐름을 설명하기 어려워지고 있다. 이러한 변화는 디지털 포렌식의 중심이 저장매체 분석에서 사용자 행위 분석으로 이동하고 있음을 의미하며 분석 대상의 확대와 함께 분석 절차와 기술 역시 더욱 정교해지고 있다.

최근에는 대량의 데이터를 처리하고 분석하는 과정에서 AI 기술을 활용하려는 시도가 증가하고 있으나, 분석 결과를 실제 증거로 활용하기 위해서는 신뢰성을 확보할 수 있는 절차와 기준이 반드시 필요하다. 따라서, 향후 디지털 포렌식은 단순히 데이터를 분석하는 기술을 넘어 다양한 환경에서 확보된 증거를 연결하고 검증할 수 있는 체계적인 분석 역량을 중심으로 발전해 나갈 것으로 보인다.

Incident Response

| 사고는 발견되는 순간이 아니라, 놓친 순간에 시작된다.

침해사고는 단일 공격으로 갑작스럽게 발생하기보다 장기간에 걸쳐 조용히 진행되는 경우가 많다. 공격자는 조직 내부에 침투한 이후 일정 기간 동안 탐지를 피하며 권한을 확장하고, 필요한 자산과 계정을 확보한 뒤 본격적인 공격을 수행하는 경우가 일반적인 양상으로 자리잡고 있다.

이러한 환경에서는 단순히 사고가 발생했을 때 대응하는 방식만으로는 충분하지 않으며, 조직 내부에서 발생하고 있는 이상 징후를 지속적으로 탐지하고 대응할 수 있는 체계가 무엇보다 중요해지고 있다. 관리되지 않는 계정이나 Shadow IT와 같이 조직이 충분히 인지하지 못한 자산이 새로운 공격 표면으로 작용하면서 사고 대응의 범위는 조직 내부뿐 아니라 외부 협력사와 서비스 환경까지 확대되고 있다.

최근에는 AI 기술을 활용해 위협을 신속하게 분석하고 대응하려는 시도가 증가하고 있으며, 이러한 기술을 효과적으로 활용하기 위해서는 단순한 도구 도입을 넘어 지속적인 운영 역량과 대응 체계를 함께 확보하는 것이 필요하다. 향후 사고 대응의 경쟁력은 새로운 보안 기술을 얼마나 도입했는지가 아니라 변화하는 위협 환경 속에서 이를 지속적으로 운영하고 대응할 수 있는 역량을 얼마나 안정적으로 유지하고 있는가에 의해 결정될 것이다.

PLAINBIT

별첨. 디지털 포렌식 시장 조사 현황

DFIR REPORT 2026

별첨. 디지털 포렌식 시장 조사 현황

1. 국내 디지털 포렌식 업체

국내 디지털 포렌식 시장에서 최근 3년간 안정적인 매출 성장을 기록한 주요 업체들을 분석한 결과, 사업 영역은 크게 리셀링, 디지털 포렌식 솔루션 개발, 서비스 분야로 구분되는 것으로 나타났다. 분석 대상 기업은 리셀링 분야 11개사, 개발 분야 9개사, 서비스 분야 8개사로 확인되었으며, 리셀링 기업의 비중이 가장 높은 것으로 분석되었다.

현재 국내 시장은 해외 솔루션 유통 중심의 리셀링 기업과 자체 기술 기반의 개발 기업, 전문 분석 및 대응 서비스를 제공하는 서비스 기업이 공존하는 구조를 형성하고 있는 것으로 분석된다.

2. 디지털 포렌식 매출 구조 변화

각 사업 영역 별로 최근 3년의 매출 구조를 분석한 결과, 전체 사업 영역 중 리셀링 부문의 성장세가 가장 크게 나타난 것으로 확인되었다.

사업영역구분	매출(천원)		
	2023	2024	2025
리셀링	91,160,665	101,242,054	131,085,208
개발	32,667,820	36,262,498	36,751,865
서비스	35,957,497	37,266,086	37,571,111

리셀링 부문 매출은 2023년 약 911억 6천만 원에서 2025년 약 1,310억 9천만 원 규모로 증가했으며, 최근 3년간 약 43.8% 증가한 것으로 나타났다. 이는 디지털 포렌식 및 보안 솔루션 수요 증가에 따라 제품 및 라이선스 공급이 확대된 영향으로 분석된다. 또한, 최근 디지털 포렌식 솔루션의 리셀링 방식이 기존 일회성 구매 중심에서 연간 구독 및 유지 비용 기반 구조로 변화한 점 역시 매출 증가에 영향을 미친 것으로 보인다.

개발 부문 매출은 약 326억 7천만 원에서 약 367억 5천만 원 수준으로 증가하며 최근 3년간 약 12.5% 성장했다. 전반적으로 안정적인 매출 흐름을 유지하고 있으며, 자체 기술 개발과 솔루션 고도화를 지속적으로 추진하면서 안정적인 사업 구조를 유지하고 있는 것으로 분석된다.

서비스 부문 매출은 약 359억 6천만 원에서 약 375억 7천만 원 수준으로 증가하며 최근 3년간 약 4.5% 성장했다. 리셀링 및 개발 부문 대비 성장률은 상대적으로 낮은 수준이나, 국내 시장 특성상 디지털 포렌식 및 침해사고 대응 업무를 외부 전문 업체에 의뢰하는 비율이 아직 높지 않은 점이 영향을 미친 것으로 보인다. 최근에는 침해사고 대응 전문성과 디지털 포렌식 분석 역량에 대한 수요가 증가하고 있는 관계로 외부 전문 서비스 시장 또한 점진적인 성장세를 이어가고 있는 것으로 판단된다.

3. DFIR 사업 특성에 따른 시장 동향

| 전체 시장 규모

나라장터를 기준으로 DFIR (Digital Forensics and Incident Resonse) 시장의 전체 사업 규모는 약 528억 원 수준으로 확인되었다. 사업 유형별로는 디지털 포렌식 및 증거분석 분야가 약 217억 원 규모로 가장 높은 비중(약 41%)을 차지하는 것으로 나타났으며, 침해사고 대응 분야가 약 152억 원(약 29%) 규모로 뒤를 이었다.
가상자산 분야는 약 97억원(약 18%) 규모로 확인되었으며, 최근 가상자산 추적, 범죄 수사 체계 구축 수요 증가에 따라 관련 시장이 빠르게 확대되고 있는 것으로 분석된다. 사이버 범죄 및 수사 분야는 약 62억원(약 12%) 규모로 나타났으며, 디지털 증거 수집과 분석 체계 구축, 전문 수사 역량 강화 중심의 사업이 지속적으로 추진되고 있는 것으로 확인되었다.

| 사업 유형별 시장 비중

사업유형	사업금액	비중
디지털 포렌식/증거분석	약 217억	41%
침해사고 대응	약 152억	29%
가상자산	약 97억	18%
사이버범죄/수사	약 62억	12%

국내 디지털 포렌식 및 사이버 조사 시장은 단순 증거 분석 중심 구조에서 벗어나, 침해사고 대응, 가상자산 추적, AI 기반 분석, 자동화 및 클라우드 대응 등으로 빠르게 확장되고 있는 것으로 나타났다. 또한, 단순 장비를 구매하는 것보다 운영 및 대응 체계 중심으로 확대되고 있으며, 신규 구축 중심 시장에서 유지관리 및 고도화 사업 비중이 증가하고 있는 것으로 나타났다. 공공 및 수사기관을 중심으로 전문 분석 체계 고도화 수요가 지속적으로 증가하고 있으며, 향후에는 AI 및 자동화 기술을 접목한 통합형 분석 플랫폼 수요 또한 확대될 것으로 전망된다.

| 분야별 사업 특성에 따른 동향

DFIR 시장은 분석 플랫폼과 전문 솔루션 도입을 중심으로 성장해 왔으나, 최근에는 침해사고 대응 분야를 중심으로 전문 서비스 수요가 확대되고 있다. 또한, 가상자산 분야에서도 분석 지원 서비스와 운영 지원 사업이 등장하면서 시장은 단순 구축 중심에서 분석, 운영, 대응 서비스가 결합된 통합 서비스 형태로 점진적으로 발전하고 있는 것으로 나타났다.

| 각 분야별 사업 유형에 따른 사업비 규모 분류

구분	디지털 포렌식 및 증거분석	침해사고 대응	가상자산	사이버 범죄 및 수사
시장 규모	217억	152억	97억	62억
주요 투자 영역	분석솔루션 (SW)	침해사고 대응 서비스	추적 및 분석 솔루션	수사 분석 체계 구축
주요 사업 유형	SW 중심 산업	대응 서비스	추적 및 분석 솔루션	수사 분석 체계 구축
구축 및 솔루션 비중	75%	22%	82%	69%
운영 및 서비스 비중	20%	78%	13%	24%
교육 및 연구 비중	5% 내외	1% 내외	5%	7%

1. 디지털 포렌식 및 증거 분석

디지털 포렌식 분야는 분석 도구 라이선스 구매, 모바일 및 PC 포렌식 장비 구축, 분석 서버 및 워크스테이션 도입, 유지관리 사업 등을 중심으로 시장이 형성되어 있는 것으로 나타났다. 또한, 모바일 포렌식, 클라우드 포렌식, AI 기반 분석, Deepfake 탐지 등 신규 기술 분야로 적용 범위가 확대되면서 관련 사업 수요도 증가하는 추세를 보이고 있다. 사업 유형별로는 소프트웨어 라이선스 구매 및 유지관리 사업과 분석 환경 통합 구축 사업이 전체 사업비의 약 68%를 차지하는 것으로 나타났으며, 이를 통해 디지털 포렌식 시장이 분석 플랫폼 및 전문 솔루션 중심의 구축형 시장 구조를 유지하고 있는 것으로 보인다.

| 사업 유형별 사업비 규모 분류

사업유형	규모	비중
분석솔루션(SW)	약 94억	43%
통합 구축 사업(SW+HW)	약 54억	25%
분석 인프라(HW)	약 15억	7%
운영 및 기술지원	약 44억	20%
교육 및 연구	약 10억	5%
합계	약 217억	

2. 침해사고 대응

침해사고 대응 분야는 침해사고 조사 및 후속조치 지원, 침해사고 대응체계 구축, 악성코드 분석, 대응훈련 및 모의훈련 사업을 중심으로 시장이 형성되어 있는 것으로 나타났다. 최근에는 단순 대응체계 구축을 넘어 AI 기반 분석 지원, 위협 헌팅(Threat Hunting), 자동화 기능 개발 등 대응 역량 고도화를 위한 사업이 확대되는 추세를 보이고 있다. 사업 유형별로는 원인분석, 후속조치, 위협 헌팅, 대응훈련 운영 등 전문 서비스 사업이 전체 사업비의 약 77%를 차지하는 것으로 나타났으며, 대응체계 구축 사업은 약 22% 수준으로 분석되었다. 이를 통해 침해사고 대응 시장은 솔루션 및 인프라 구축보다는 전문 인력 기반의 분석 및 대응 역량 확보를 중심으로 형성된 서비스 중심 시장의 특성을 보이고 있다.

| 사업 유형별 사업비 규모 분류

사업유형	규모	비중
침해사고 대응 서비스	약 118억	77%
침해사고 대응체계 구축(SW+HW)	약 33억	22%
교육 및 연구	약 1억	1%
합계	약 152억	

3. 가상자산

가상자산 분야는 거래 추적 및 분석 솔루션 도입, 가상자산 범죄 분석, AML(자금세탁방지) 관련 연구, 블록체인 기반 수사 지원 사업 등을 중심으로 시장이 형성되어 있는 것으로 나타났다. 수사기관과 금융기관을 중심으로 가상자산 범죄 수사 및 자금 흐름 분석 수요가 증가함에 따라, 가상자산 추적 및 분석 체계 구축 사업이 지속적으로 확대되고 있는 것으로 확인되었다.

사업 유형별로는 Chainalysis, TRM Labs, QLUE 등 전문 추적 및 분석 솔루션 도입 사업이 전체 사업비의 약 82%를 차지하는 것으로 나타났으며, 분석 지원 서비스는 약 13%, 교육·연구 분야는 약 5% 수준으로 분석되었다. 최근에는 민간 전문업체를 활용한 분석 지원 서비스와 압수 가상자산 관리 서비스 등 운영 지원 사업이 등장하면서, 단순 솔루션 도입 중심 시장에서 분석 및 운영 서비스가 결합된 형태로 시장이 점진적으로 발전하고 있는 것으로 보인다.

| 사업 유형별 사업비 규모 분류

사업유형	규모	비중
추적 및 분석 솔루션	약 80억	82%
분석 지원 서비스	약 13억	13%
교육 및 연구	약 5억	5%
합계	약 97억	

4. 사이버 범죄 및 수사

사이버범죄 및 수사 분야는 디지털 증거 확보 체계 구축, 수사 장비 구매, 분석 프로그램 도입, 전문 교육 및 수사 지원 체계 강화 사업을 중심으로 시장이 형성되어 있는 것으로 나타났다. 최근에는 OSINT(Open Source Intelligence), 악성코드 분석, 로그 분석 등 실무 중심의 전문 교육 수요가 증가하고 있으며, 수사 과정에서 활용되는 디지털 분석 역량 강화를 위한 투자도 지속적으로 확대되는 추세를 보이고 있다.

사업 유형별로는 수사 분석체계 구축 사업이 전체 사업비의 약 69%를 차지하는 것으로 나타났으며, 수사시스템 운영 및 고도화 사업은 약 24%, 교육 및 협력 사업은 약 7% 수준으로 분석되었다. 이를 통해 사이버범죄 및 수사 분야는 전문 분석 서비스 활용보다 자체 수사 역량 확보를 위한 분석 체계와 수사 인프라 구축에 중점을 두고 있으며, 지속적인 시스템 운영과 전문인력 양성을 통해 수사 역량을 강화하는 방향으로 시장이 형성되고 있는 것으로 보인다.

| 사업 유형별 사업비 규모 분류

사업유형	규모	비중
수사 분석체계 구축	43억	69%
수사시스템 운영 및 고도화	14억	24%
교육 및 협력	5억	7%
합계	62억	

PLAINBIT

별첨. 설문조사 전체 결과

별첨. 설문조사 전체 결과

귀하의 **업무 수행 경력**은 얼마나 되시나요?

1~3년	24.21%
4~6년	**48.42%**
7~9년	8.42%
10~14년	11.58%
15년 이상	7.37%

귀하는 주로 **어떤 업무**를 수행하고 계신가요?

분석	**49.47%**
범죄 수사	23.16%
연구	20.00 %
부정 조사 및 내부 감사	5.26%
디지털 포렌식 현장지원	1.05%
신사업기획	1.05%

귀하의 조직은 **어떤 유형**에 속하나요?

수사기관 (특사경 포함)	**57.89%**
학계	20.00%
공공기관 (수사기관 제외)	10.53%
대기업	4.21%
소상공인/중소기업	4.21%
중견기업	2.11%
기타	1.05%

귀하의 조직에서 올해 **디지털 포렌식 관련 예산은 작년 대비 어떻게 변화**했나요?

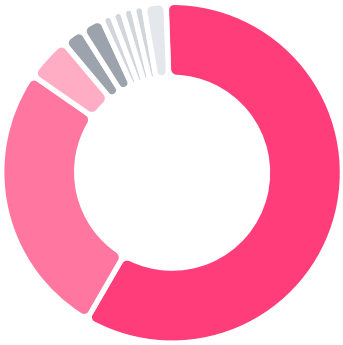
조직 내 **디지털 포렌식 전담 인력은 어떤 형태로 구성**되어 있나요?

전담 인력 존재	**30.53%**
전문팀 운영	29.47%
일부 업무 병행	27.37%
부분적으로 수행	7.37%
전혀 없음	5.26%

조직 내 **디지털 포렌식 관련 인원은 작년 대비** 어떻게 변화했나요?

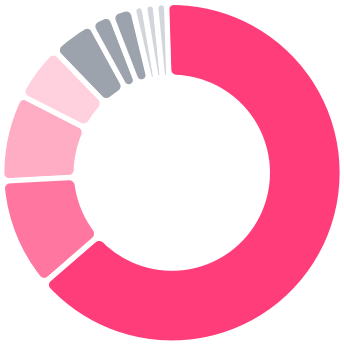
변화 없음	**60.00%**
소폭 증가	27.37%
기타	7.37%
대폭 증가	3.16%
소폭 감소	2.11%

조직에서 **가장 많이 다루는 디지털 포렌식 분야**는?



모바일 포렌식	**58.95%**
디스크 포렌식	26.32%
클라우드 포렌식	4.21%
IoT 포렌식	2.11%
메모리 포렌식	2.11%
AI 포렌식	1.05%
IoT 제외 전부	1.05%
네트워크 포렌식	1.05%
데이터베이스 포렌식	1.05%
멀티미디어 포렌식	2.10%

조직에서 **가장 비중이 늘어난 디지털 포렌식 분야**는?



모바일 포렌식	**64.21%**
클라우드 포렌식	10.53%
디스크 포렌식	8.42%
데이터베이스 포렌식	5.26%
IoT 포렌식	4.21%
네트워크 포렌식	2.11%
메모리 포렌식	2.11%
AI 포렌식	1.05%
apple product	1.05%
영상분석	1.05%

디지털 포렌식 **분석에서 AI를 사용**하고 계신가요?

참고 검색/문서 요약 수준으로 활용하고 있다.	**38.95%**
전혀 활용하지 않는다.	25.26%
파일/아티팩트 식별에 보조적으로 사용하고 있다.	16.84%
AI 기반 분석 도구를 적극 활용 중이다.	14.74%
정식 분석 프로세스 일부 자동화에 활용하고 있다.	4.21%

디지털 포렌식 분석에서 **AI가 어떤 부분을 가장 효과적으로 개선**할 수 있다고 생각하시나요?

대량 파일/아티팩트 분류	**55.79%**
모바일/메신저 데이터 정리	18.95%
사용자 활동 타임라인 복원	12.63%
증거 설명 및 보고 작성	12.63%

디지털 포렌식에서 **AI 활용이 어려운 이유**는 무엇인가요?

AI 분석 결과의 신뢰성 검증이 어려움	**42.86%**
증거 데이터 반출/업로드 불가 (보안/법적 제약)	42.11%
분석가의 업무 방식과 맞지 않음	5.26%
조직 내부 교육/도입 가이드 부족	9.02%
정형화된 범죄유형을 정의하기 곤란함	0.75%

디지털 포렌식 **AI 자동화가 현실화되기 위해 가장 먼저 필요한 요소**는 무엇이라고 생각하시나요?

법, 절차 정립	**32.63%**
도구 내 AI 품질 보증	31.58%
데이터셋	24.21%
표준화된 케이스 태깅 모델	6.32%
분석가 교육	5.26%

디지털 포렌식 수행 시 **가장 큰 어려움**은 무엇인가요?

데이터 암호화	**31.72%**
데이터 양 증가	30.34%
인력 부족	15.17%
시간, 장비, 예산 부담	12.41%
법적 요구 대응 부담	9.66%
기타	0.69%

디지털 포렌식 분석에서 **가장 시간을 많이 소모하는 단계** 는 무엇인가요?

아티팩트 수집	**37.89%**
파일, 레지스트리, 로그 파싱	34.74%
보고서 작성	18.95%
타임라인 구성	7.37%
사건과 연관성있는 내용 검색 및 분석	1.05%

조직 내에 클라우드 (AWS, Azure, GCP 등)에 대한 **포렌식 증거 보존/분석 체계가 마련**되어 있으신가요?

마련되어 있지 않다.	**76.84%**
마련되어 있다.	20.00%
기타	3.15%

클라우드 포렌식 (AWS, Azure, GCP 등)에서 **가장 어려운 점**은 무엇인가요?

로그 종류, 이벤트 구조 이해	**31.58%**
서비스별 데이터 분산	25.26%
증거 보존 기간 부족	14.74%
임시 세션, 토큰, 역할 추적	12.63%
조직 내부 책임 분리	10.53%
기타	4.2%

클라우드 환경의 포렌식에서 **가장 중요하다고 생각하는 증거 소스**는 무엇인가요?

IAM/인증 및 AssumeRole 기록	**36.84%**
Object Storage Access Log	29.47%
VM, Container Snapshot	20.00%
API 호출 이력	11.58%
기타	2.10%

SaaS 기반의 클라우드 포렌식에서 **가장 어려운 요소**는 무엇이라고 생각하시나요?

로그 형식, 구조가 서비스마다 다름	**40.00%**
API, Export 권한 필요	21.05%
사용자, 권한, 역할 관계 해석이 어려움	16.84%
외부 공유, 링크 접근 추적이 어려움	10.53%
보존 기간이 짧음	9.47%
기타	2.10%

포렌식 분석 시 동일 사용자의 여러 기기(PC, 모바일, 가상환경, VDI) 활동을 **연결해 분석한 경험**이 있으신가요?

사례는 있으나 드묾	**38.95%**
자주 있음	24.21%
거의 없음	21.05%
없음	15.79%

크로스 디바이스 분석에서 **가장 어려운 부분**은 어떤거라고 생각하시나요?

데이터 저장 위치가 기기마다 상이함	**26.32%**
동기화 데이터의 범위 불명확	24.21%
타임스탬프, 타임존 불일치	20.00%
계정과 실제 사용자 동작에 대한 행위 분석	17.89%
세션 및 토큰공유 판단의 어려움	10.53%
기타	1.05%

크로스 디바이스 환경에서 **가장 핵심 증거가 되는 데이터**는 무엇이라고 생각하시나요?

모바일 메신저, 앱 로그	**31.58%**
클라우드 동기화 파일 메타데이터	31.58%
브라우저 세션, 쿠키, History	25.26%
인증 기록(로그온, SSO, MFA)	11.58%

귀하의 디지털 포렌식 도구 도입을 검토할 때 **가장 중요한 고려사항**은 무엇인가요?

도구의 성능	**50.53%**
책정 예산 및 판매 금액	38.95%
제조사나 유통사의 기술 지원	10.53%

디스크 이미징을 수행할 때 **가장 많이 사용하는 하드웨어 장비**는 무엇인가요?

Logicube Forensic Falcon	**52.63%**
Opentext TX1 / TD 시리즈	30.53%
Atola Taskforce / Insight Forensic	8.42%
기타	6.3%
Media Cube	2.1%

디스크 이미징 장비를 선택할 때 **가장 중요한 고려사항**은 무엇인가요?

이미징 속도	**49.47%**
배드 섹터 등 정보저장매체 오류 처리	30.53%
병렬 수행 여부	13.68%
완료 리포트의 내용	5.26%
기타	1.05%

가장 많이 사용하는 이미징 소프트웨어는 무엇인가요?

EnCase	**26.32%**
FTK Imager	26.32%
DFT(Digital Forensic Tool)	25.26%
X-Ways Forensics	14.74%
Axiom Acquire	6.32%
기타	1.05%

위 도구를 **가장 많이 사용하는 이유**는 무엇인가요?

오랜 사용 경험	**47.37%**
해당 도구에서만 지원하는 기능 존재	32.63%
추후 교차 검증이 쉬움	9.47%
기타	6.30%
비교적 저렴한 비용	4.21%

모바일 포렌식 **수집 도구로 가장 많이 사용하는 도구**는 무엇인가요?

MD-NEXT	**51.58%**
Cellebrite UFED, Inseyets, Premium / Physical Analyzer	30.53%
Magnet GRAY268KEY / VERAKEY	6.32%
기타	6.30%
Oxygen	3.16%
XRY	2.11%

모바일 포렌식 **분석 도구로 가장 많이 사용하는 도구**는 무엇인가요?

MD-RED	**61.05%**
Cellebrite UFED, Inseyets, Premium / Physical Analyzer	23.16%
Magnet AXIOM	6.32%
기타	5.25%
Oxygen	2.11%
XRY	2.11%

두 개 이상의 모바일 포렌식 도구로 교차 분석을 수행하는 경우, 이유는 무엇인가요?

획득과 분석을 서로 다른 도구로 수행하기 위해서 (예: Inseyets로 획득 후 MD-RED로 분석)	**41.05%**
도구에 따라 복구되는 데이터 양이 상이하므로	29.47%
분석 결과의 완전성을 검증하기 위해서	26.32%
기타 (검증의 필요성을 느끼고 있으나 Final Mobile Forensic이 더 이상 유지보수를 제공하지 않음, 획득도구에 따라 획득가능 범위가 달라 획득은 다양하게 진행하나 통상 분석과 선별은 RED사용, 사용자 친화적 환경으로 일반수사관이 보다 쉽게 이해, 무응답)	3.15%

디지털 포렌식 능력 향상을 위해 수강하고 싶은 교육 과정은 무엇인가요?(모두 선택)

로그 및 아티팩트 분석	**25.57%**
모바일 수집과 분석	24.66%
디지털포렌식 도구 활용	24.66%
클라우드 수집과 분석	23.29%
기타	1.83%

조직 내에 **SaaS(예: Slack, M365, Google Workspace, Confluence 등) 기반 증거 확보 시** 포렌식 절차가 마련되어 있나요?

마련되어 있지 않다.	**71.58%**
마련되어 있다.	25.26%
기타	3.15%

귀하의 **업무 수행 경력**은 얼마나 되시나요?

1~3년	26.92%
4~6년	**34.62%**
7~9년	11.54%
10~14년	3.85%
15년 이상	23.08%

귀하는 주로 **어떤 업무**를 수행하고 계신가요?

보안 CERT/관제	**19.23%**
연구/개발	**19.23%**
보안 컨설팅	**19.23%**
보안 솔루션 운영	15.38%
위협 인텔리전스	11.54%
사고 조사	11.54%
마케팅	3.85%

귀하의 조직은 **어떤 유형**에 속하나요?

공공	23.08%
소상공인/중소기업	**57.69%**
대기업	7.69%
중견기업	7.69%
기타	3.85%

조직 내 **사고 대응 팀의 구조는 어떤 형태**로 구성되어 있나요?

IT 또는 보안팀 내에 사고 대응 담당이 포함되어 있다.	**46.15%**
독립적인 사고 대응 팀이 있다.	42.31%
사고 대응 팀이 존재하지 않는다.	11.54%

침해사고 대응을 위해 귀하가 **보유하고 있는 상용 솔루션의 유형**은 무엇인가요?(모두 선택)

로그 분석 - SIEM, Splunk, ELK 등	**27.27%**
악성코드 분석 - IDA, Joe SandBox, Anyrun, Hybrid Analysis 등	**27.27%**
인텔리전스 - VirusTotal, Criminal IP, ATIP, QUAXAR 등	24.24%
포렌식(원인 분석) - X-Ways Forensics, Magnet AXIOM, Cyber Triage 등	12.12%
기타	9.09%

현재 귀하의 조직에서 **운영 중인 보안 솔루션 중** 예방/차단 관점에서 **가장 효과적이라고 판단되는 솔루션**은 무엇인가요?

(웹)방화벽	**38.46%**
IDS/IPS	30.77%
접근제어시스템	15.38%
안티바이러스(백신)	11.54%
기타	3.85%

현재 귀하의 조직에서 **운영 중인 보안 솔루션 중** 탐지/대응 관점에서 **가장 효과적이라고 판단되는 솔루션**은 무엇인가요?

EDR/XDR	**46.15%**
SIEM	30.77%
MSS/MDR	7.69%
잘 모름	11.55%
SOAR	3.85%

앞으로 **어떤 환경에 대한 사고 대응 역량 개발**이 필요하다고 생각하시나요?

클라우드	**46.15%**
모바일	34.62%
공급망	7.69%
macOS	3.85%
IoT	3.85%
기타	3.85%

귀하가 속한 조직에서 **가장 대응이 시급하다고 생각되는 보안 위협**은 무엇인가요?

정보 유출	**42.31%**
클라우드 보안 위협	15.38%
공급망 공격	15.38%
랜섬웨어	15.38%
피싱 및 소셜 엔지니어링	7.69%
Active Directory 위협	3.85%

침해사고가 발생하는 **가장 큰 환경적인 요인**은 무엇인가요?

보안 및 사고 대응 전문 인력의 부재	**38.46%**
예산 및 리소스 부족	26.92%
지속적인 교육 및 훈련의 부재	15.38%
경영진의 관심과 지원 부재	15.38%
보안 장비(솔루션)의 부재	3.85%

최근 침해사고가 발생하는 **가장 큰 환경적인 요인**은 무엇인가요?

웹 및 애플리케이션 취약점	**38.46%**
보안 설정 미흡	30.77%
피싱	19.23%
보안 업데이트 미적용	7.69%
잘 모름	3.85%

현재 조직에서 **사고 대응과 관련해 겪고 있는 가장 큰 문제**는 무엇인가요?

신규 위협에 대한 탐지 및 대응 능력 부족	**42.31%**
탐지 및 대응 속도의 지연	30.77%
인력 부족으로 인한 업무 과부하	15.38%
DFIR 관련 교육 및 기술 습득 기회 부족	11.54%

사고 대응 시 **원인을 파악하기 어려웠던 이유**는 무엇인가요?

유지보수, 외부 협력사 단말 관리 불투명	**30.77%**
로그 보존 기간 또는 로그 수집 범위 부족	**30.77%**
미등록 서버, VM, Container 존재	23.08%
SSH Key 또는 계정 공유 또는 재사용	7.69%
잘 모름	3.85%
로그가 여러 위치에 분산 (클라우드, SaaS, VM, vSphere 등)	3.85%

유지보수사, 협력사, 외부 파견 인력은 **조직 자산에 어떤 방식으로 접속**하고 있나요?

기업지급 장비	**34.62%**
원격접속 VPN	30.77%
개인 노트북	26.92%
관리단말	3.85%
잘 모름	3.85%

외부 인력에 대한 계정(유지보수사, 협력사 등)은 **어떤 형식으로 발급**되나요?

개별 + 공유 혼용	**38.46%**
100% 개별 계정	30.77%
공용계정	11.54%
외부 인력이 관리하는 시스템은 외부 인력이 자체적으로 설정해 활용	7.69%
기타	11.55%

외부 인력 **장비에 대한 보안 준수 요구 수준**은 어느 정도 인가요?

단순 서약	**46.15%**
백신 및 보안 에이전트 요구	30.77%
접근 전 전수 보안 검증	19.23%
Zero-Trust 접근 통제 적용	3.85%

조직 내에서 **외부 인력에 관련한 사고 발생 시 책임 및 조치 기준이 명확**한가요?

다소 모호	**38.46%**
계약 및 정책에 명시	26.92%
협약 수준으로 정리	26.92%
매우 불명확	7.69%

조직 내 자산 현황(서버, PC, VM, 클라우드)을 **중앙에서 일원화해 관리**하고 계신가요?

대체로 관리하고 있다.	**38.46%**
대부분 관리하고 있다.	30.77%
일부 부서만 해당된다.	11.54%
전혀 아니다.	7.69%
중앙에서 일원화해 관리하고 있다.	11.55%

Shadow Asset(공식적으로 등록·관리되지 않거나, 조직의 IT·보안 관리 체계 밖에서 존재하는 자산) **발생이 가장 심한 영역**은 어디인가요?

협력사 또는 용역 파트 유지보수 단말	**46.15%**
개발 또는 QA 테스트 서버	23.08%
PoC 또는 실험 환경	15.38%
네트워크 장비	7.69%
잘 모름	3.85%
기타	3.85%

Shadow IT · Asset 문제를 줄이기 위해 가장 필요한 조치는 무엇이라고 생각하시나요?

유지보수 및 협력사 계정 관리 체계 개선	**50.00%**
조직 내부 교육 및 정책 정립	15.38%
자동 스캐닝 도구 도입	15.38%
자산 관리 시스템(CMDB) 정비	11.54%
클라우드 리소스 태깅 의무화	3.85%
기타	3.85%

귀하의 조직에서 **가장 필요한 역량**은 무엇이라고 생각하시나요?

Windows Server 포렌식 역량	**29.79%**
사고 대응 자동화 (EDR, SOAR 등)	19.15%
인력, 교육, 조직 정비	19.15%
Cloud, SaaS 로그 분석 체계	17.02%
Linux Server 포렌식 역량	14.89%

조직 환경에서 **Container 기반 서비스(Docker, Kubernetes)**를 운영하고 계신가요?

운영하지 않고 있다.	**50.00%**
일부 서비스에 대해서만 운영하고 있다.	46.15%
운영하고 있다.	3.85%

Container 침해 분석에서 가장 어려운 점은 무엇이라고 생각하시나요?

런타임에서 흔적이 사라짐	**30.77%**
분석 가이드 부재	26.92%
로그 보존 기간 짧음	23.08%
Host와 Container간 경계 이해 어려움	15.38%
기타	3.85%

내부 서버/시스템이 **가상화(vSphere, ESXi, Hyper-V) 환경**에서 운영되고 있나요?

일부 운영되고 있다.	**69.23%**
대부분 운영되고 있다.	19.23%
운영되고 있지 않다.	11.54%

조직 내에서 침해 조사 시 **vCenter, ESXi 로그 확보체계가 마련**되어 있으신가요?

일부 로그만 확보하도록 마련되어 있다.	**53.85%**
마련되어 있다. (정기 보존 및 조회 가능)	26.92%
요청 시 복잡한 절차가 필요하다.	11.54%
마련되어 있지 않다.	7.69%

귀하의 조직은 **DFIR 업무를 위해 AI를 활용**하고 계신가요?

시범적으로 일부 영역에서만 활용 중이다.	**61.54%**
전혀 활용하고 있지 않다.	19.23%
다수의 영역에서 적극 활용 중이다.	15.38%
정식 업무 프로세스에 제한적으로 포함되어 있다.	3.85%

DFIR 업무에서 **주로 사용하는 AI 유형**은 무엇인가요?

생성형 AI (예: ChatGPT, Claude 등)	**65.38%**
자체 학습 또는 사내 모델(Large/SBERT 등)	15.38%
SIEM/EDR 내 내장형 AI 분석 기능	11.54%
오픈소스 ML 기반 포렌식/탐지 엔진	3.85%
기타	3.85%

AI 사용 시 **가장 기대되는 효과**는 무엇인가요?

분석 속도 향상	**34.62%**
분석 인력의 부담 감소	26.92%
분석 속도 향상, 분석 인력의 부담 감소	23.08%
신규 인력 온보딩 시간 단축	7.69%
고객/경영진 설명 품질 향상	3.85%
분석 인력의 부담 감소, 신규 인력 온보딩 시간 단축, 고객/경영진 설명 품질 향상	3.85%

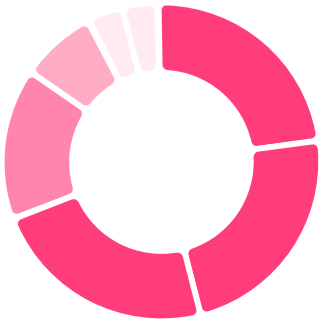
AI 활용 시 **가장 우려하는 부분**은 무엇인가요?

내부 데이터 반출 우려 (보안/규정 준수)	**38.46%**
AI 결과의 신뢰성 검증 어려움	26.92%
실전 로그/아티팩트 해석 정확도 제한	11.54%
내부 데이터 반출 우려, AI 결과의 신뢰성 검증 어려움	7.69%
조직 내부 정책 변화의 어려움	3.85%
AI 결과의 신뢰성 검증 어려움, 실전 로그/아티팩트 해석 정확도 제한	3.85%
내부 데이터 반출 우려, AI 결과의 신뢰성 검증 어려움, 조직 내부 정책 변화의 어려움	3.85%
보안	3.85%

사고 대응과 관련해 **외부 서비스의 필요성**을 느끼시나요?

조금 필요하다.	**42.31%**
매우 필요하다.	26.92%
해당하지 않음.	15.38%
필요하지 않다.	15.38%

사고 대응과 관련하여 **필요한 외부 서비스**는?



사고 원인 분석	**23.08%**
위협 인텔리전스(다크웹 포함)	**23.08%**
악성코드 분석	**23.08%**
재발방지 대책 마련	15.38%
연간 구독형 서비스(사고 대응, 위협 모니터링 등)	7.69%
기타(없음)	3.85%
잔존 위협 평가 (침해 평가)	3.85%

사고 대응 관련 외부 서비스를 이용할 때 **추가적으로 기대하는 효과**는 무엇인가요?

신속한 침해사고 대응	**50.00%**
내부 인력력의 업무 부담 감소	26.92%
정보보호 수준 향상	11.54%
대응 인사이트 습득	11.54%

1순위 사고 대응 관련 외부 서비스를 이용하려고 할 때 **가장 중요한 고려사항**은 무엇인가요? (1~3순위 선택)

서비스 업체의 전문성 및 경험	**50.00%**
서비스 비용	23.08%
서비스 업체의 인지도	15.38%
서비스 품질 (체계)	7.69%
서비스 보안유지 (NDA)	3.85%

2순위 사고 대응 관련 외부 서비스를 이용하려고 할 때 **가장 중요한 고려사항**은 무엇인가요? (1~3순위 선택)

서비스 업체의 전문성 및 경험	**34.62%**
서비스 업체의 인지도	23.08%
서비스 비용	23.08%
서비스 품질 (체계)	15.38%
최신 장비 보유 여부	3.85%

3순위 사고 대응 관련 외부 서비스를 이용하려고 할 때 **가장 중요한 고려사항**은 무엇인가요? (1~3순위 선택)

서비스 업체의 인지도	**38.46%**
서비스 비용	26.92%
서비스 업체의 전문성 및 경험	19.23%
서비스 품질 (체계)	15.38%

사고 대응 서비스 제공자와의 **협력에서 가장 필요한 부분**은 무엇인가요?

협업 툴을 활용한 실시간 상황 공유	**30.77%**
조직 맞춤형 대응 방안 제시	23.08%
체계적인 의사 소통	19.23%
지속적인 상황 공유와 투명한 정보 제공	15.38%
기밀 유지	7.69%
최신 위협 정보 및 트렌드 제공	3.85%

사고 대응 이후 작성하는 **보고서의 가장 중요한 요소**는 무엇이라고 생각하시나요?

사고의 범위와 피해 규모	**38.46%**
대응 과정에서 확인된 취약한 설정 (취약점)	26.92%
사고 원인과 경로의 정확한 분석	19.23%
향후 사고 예방을 위한 구체적 권고사항	15.38%

침해사고 대응과 관련해 **가장 필요한 교육**은 무엇이라고 생각하시나요?

타겟형 공격 분석	**42.31%**
로그 및 아티팩트 분석	23.08%
악성코드 분석	23.08%
위협 인텔리전스 활용	7.69%
기타	3.85%

플레인비트

2026 DFIR TRENDS REPORT

PLAINBIT | 경기도 성남시 분당구 대왕판교로 670, A동 504호
TEL. 031)8016-0912 | FAX. 031)8016-0913