PLAINBIT

2025 DFIR REPORT

2025

2025 DFIR REPORT

Table of Contents

01

Executive Summary

2025 DFIR REPORT

01. Summary

Executive Summary

과거의 침해사고 대응은 주로 사고의 표면적인 현상을 조치하는 데 중점을 두었으나, 최근에는 디지털 포렌식 기술을 활용해 사고의 근본 원인을 규명하고 정밀하게 대응하는 방향으로 전환되고 있다.

이런 변화에 따라 침해사고 대응을 단순한 **IR**(Incident Response)이 아닌 **DFIR**(Digital Forensics & Incident Response, 이하 DFIR)로 칭하고 있다.

플레인비트는 이런 변화에 선제적으로 대응하며, DFIR 서비스, 포렌식 조사, 교육, 컨설팅 등 다양한 포렌식 기반 서비스를 종합적으로 제공하고 있다. 최근 디지털 포렌식 및 사고 대응 시장의 주요 트렌드와 과제를 파악하고, 더 나은 시장 환경 조성을 위한 방향성을 모색하고자 200여 명의 실무자를 대상으로 설문조사를 실시했다.

이번 조사는 각 영역의 환경, 운영 현황, 활용 도구 및 서비스에 대한 실무자의 경험을 바탕으로 구성되었으며, 이를 통해 2025년 DFIR 분야에서 주목해야 할 현실적인 흐름과 인사이트를 공유하고자 한다.

주목해야 할 흐름 Top6

- **Digital Forensics**

Trends 1: 새로운 환경에 맞는 디지털 포렌식 기법 연구

Trends 2: 환경 변화에 적합한 다양한 도구 사용

Trends 3: 디지털 포렌식 환경의 자동화

- **Incident Response**

Trends 1: 신뢰된 외부 파트너 활용

Trends 2: 클라우드 환경에 대한 조사 역량 개발

Trends 3: 하이브리드 공격에 대한 연계 대응

02

DFIR Trends for 2025

2025 DFIR REPORT

02.

DFIR Trends for 2025

2.1. Digital Forensics

• **Trends 1:** 새로운 환경에 대응하기 위한 디지털 포렌식 기법 연구 필요

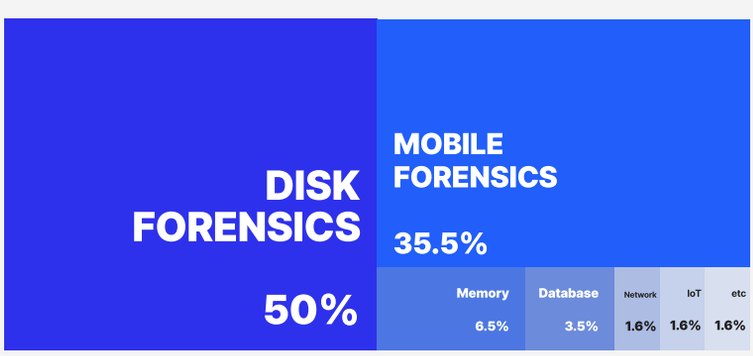
최근 디지털 포렌식의 수요는 전통적인 디스크 기반 분석에서 벗어나 모바일 기기, 클라우드 환경, IoT 및 임베디드 시스템 등 비정형 디지털 환경으로 빠르게 확장되고 있다.

설문조사 결과에 따르면, 여전히 디스크 포렌식이 가장 많이 수행되는 분야로 나타났으나, 최근 가장 비중이 크게 증가한 분야는 모바일 포렌식으로 확인되었다. 이는 실제 수사 및 대응 현장에서 모바일 환경으로의 전환이 빠르게 진행되고 있음을 명확히 반영하는 결과이다.

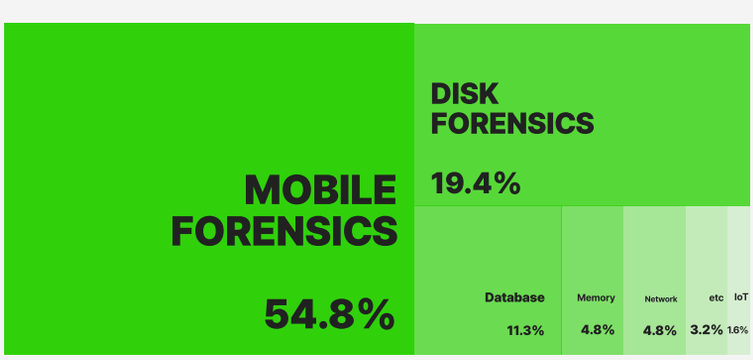
이런 변화는 다양한 기기 유형, 저장 구조, 운영체제 등 새로운 기술 환경에 대응할 수 있는 수집 및 분석 기법의 고도화가 요구됨을 시사한다. 특히 모바일 환경과 임베디드 시스템 중심으로의 전환이 가속화되고 있는 현재, 전통적인 디지털 포렌식 절차를 그대로 적용하기에는 한계가 있어 환경에 맞는 최적화된 분석 절차와 방법론의 재정립이 필요하다.

따라서, 감사 절차부터 수집·분석·보고에 이르는 전체 포렌식 프로세스를 모바일 및 비정형 환경에 맞게 통합적으로 적용할 수 있는 체계적인 포렌식 방법론의 개발이 필요하며, 향후 디지털 포렌식 분야에서는 플랫폼 특성에 맞는 절차의 표준화와 환경별 대응 전략의 정교화가 핵심 과제로 부상할 것으로 예상된다.

Q. 귀하의 조직에서 **가장 많이 다루는 디지털 포렌식 분야**는 무엇인가요?



Q. 귀하의 조직에서 **최근 가장 비중이 늘어난 디지털 포렌식 분야**는 무엇인가요?



2.1. Digital Forensics

• **Trends 2:** 환경 변화로 인해 용도에 맞는 다채로운 도구 사용 필요

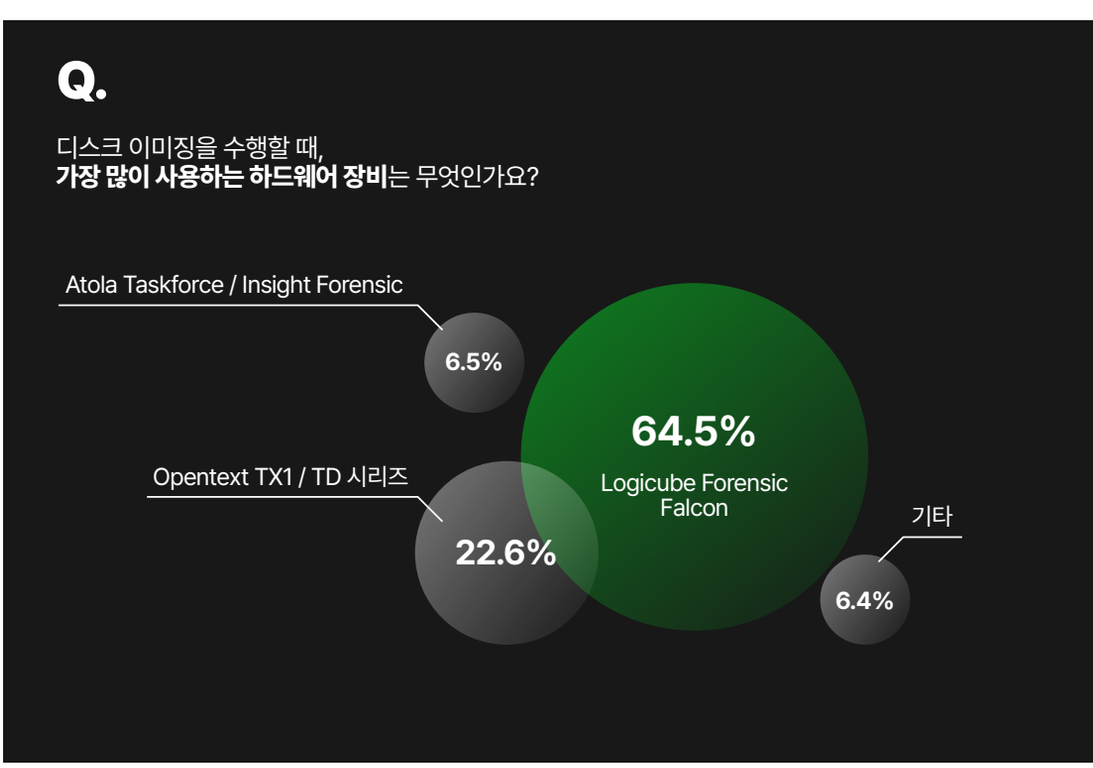
디지털 포렌식 분석 환경은 점차 복잡하고 다변화되고 있으며, 이로 인해 범용적인 단일 도구만으로는 다양한 사건 유형과 분석 목적을 충족하기 어렵다.

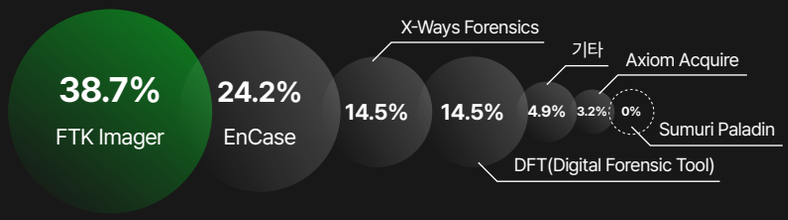
과거에는 하나의 분석 도구에 대한 충분한 이해만으로 상당수의 분석 업무가 가능했으나, 오늘날의 포렌식 환경은 디지털 기기의 다양화, 비정형 데이터의 증가, 안티포렌식 기법의 고도화 등으로 인해 도구 간 기능 차이가 크고 사건별로 요구되는 기능이 상이해졌다. 이에 따라 사건의 유형, 분석 목적, 기능 지원 여부 등을 종합적으로 고려해 상황에 맞는 도구를 유연하게 선택하고 운용할 수 있는 판단력과 활용 능력이 분석가의 필수적인 역량으로 요구되고 있다.

실제로 사용자의 일반적인 행위를 추적하거나 감사 목적의 분석에는 Magnet AXIOM과 같은 통합형 분석 도구가 효과적이며, 비정형 데이터 중심의 정밀한 키워드 기반 분석에는 X-Ways Forensics와 같은 도구가 더 적합한 사례로 들 수 있다.

최근에는 안티포렌식 기법이 고도화되고 일반화됨에 따라, 단일 도구나 단일 데이터셋만으로는 충분한 증거 확보가 어려운 환경이 되었다. 이는 도구 간 교차 검증, 다양한 이미지 형식과 이질적인 데이터 유형을 유기적으로 연계해 통합 분석할 수 있는 프레임워크의 필요성을 강하게 시사한다.

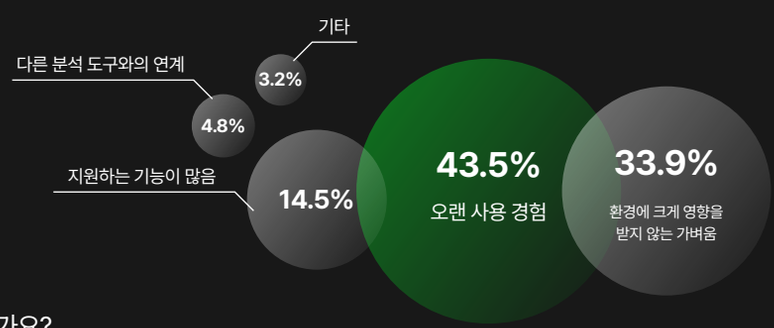
또한 디지털 포렌식 시장은 수집과 분석 기능이 명확히 구분된 구조를 가지고 있으며, 특정 기업이 시장을 지배하거나 독점하는 대표적인 소프트웨어가 부재한 상태이다. 따라서, 포렌식 분석의 신뢰성과 정확성을 확보하기 위해서는 단일 도구 의존에서 벗어나, 도구간 기능적 차이를 이해하고 분석 목적에 따라 적절히 활용할 수 있는 분석가의 전문성 확보가 무엇보다 중요하다.





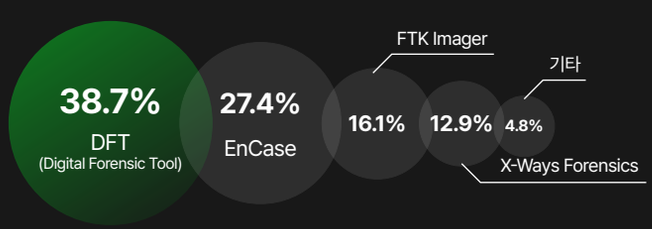
Q.

가장 많이 사용하는 **이미징 소프트웨어**는 무엇인가요?



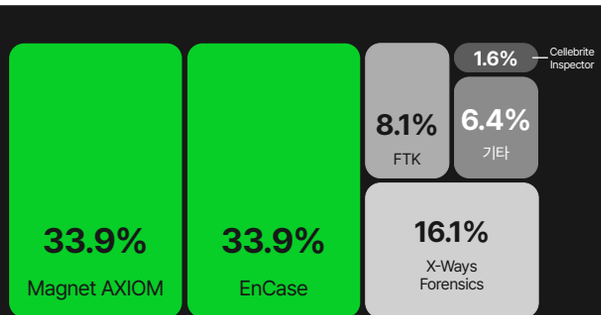
Q.

위 이미징 소프트웨어를 **가장 많이 사용하는 이유**는 무엇인가요?



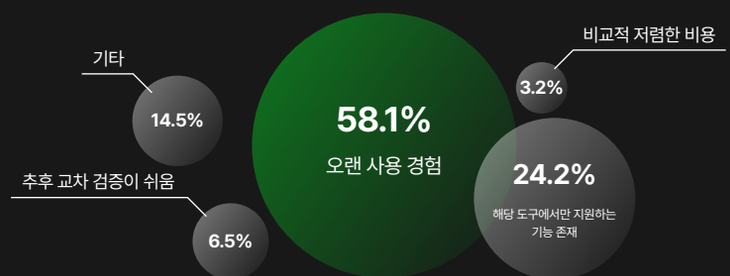
Q.

귀하의 조직에서 가장 많이 사용하는 **선별 수집 소프트웨어**는 무엇인가요?



Q.

디스크 포렌식 분석을 수행할 때 **가장 많이 사용하는 도구**는 무엇인가요?



Q.

위 도구를 **가장 많이 사용하는 이유**는 무엇인가요?

2.1. Digital Forensics

• **Trends 3:** 디지털 포렌식 환경에 대한 자동화

조직 내 디지털 포렌식 관련 인력은 작년 대비 큰 변화 없이 고정된 상태를 유지하고 있는 반면, 관련 예산은 일정 부분 증가한 것으로 확인됐다. 이는 디지털 포렌식의 조직 내 중요도가 상승했음을 시사하지만, 인력 충원은 이루어지지 않은 채 증가한 업무량을 기존 인력이 감당해야 하는 상황임을 보여준다.

더불어, 디지털 포렌식의 대상이 되는 데이터는 해마다 꾸준히 증가하고 있으며, 이에 따라 수사관이나 분석가가 처리해야 하는 데이터의 양과 복잡성 또한 지속적으로 확대되고 있다. 그러나, 분석을 담당하는 전문 인력은 대부분 고정된 상태에 머물러 있어, 이러한 구조적 제약 속에서 분석 업무의 자동화는 선택이 아닌 필수 과제로 부상하고 있다.

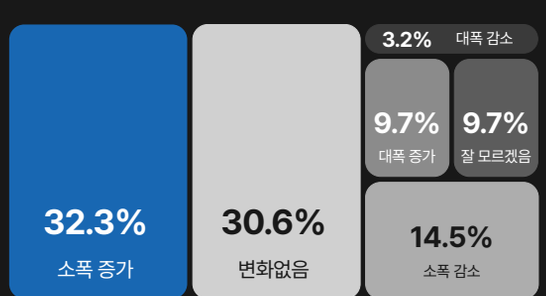
현재 포렌식 분석가가 수행하는 분석 업무 중 2/3은 단순한 작업들을 반복하고 있어, 분석 효율성이 저해되고 있다. 이에 따라 정형화된 반복 업무와 단순한 작업은 자동화하고, 디지털 포렌식 전문가는 자동화로 대체할 수 없는 고도화된 분석과 정밀한 판단이 요구되는 업무에 집중할 수 있도록 환경을 개선할 필요가 있다.

분석 자동화는 단순 업무 경감을 위한 기술적 수단을 넘어, 한정된 자원으로 방대한 디지털 증거에 대응하기 위한 전략적 전환의 핵심으로 작용할 수 있다.

향후 디지털 포렌식 조직의 운영 모델을 효율 중심으로 전환하고, 자원 운용의 효율성을 극대화하기 위해서도 디지털 포렌식 환경의 체계적 자동화 구축이 필수적이다.

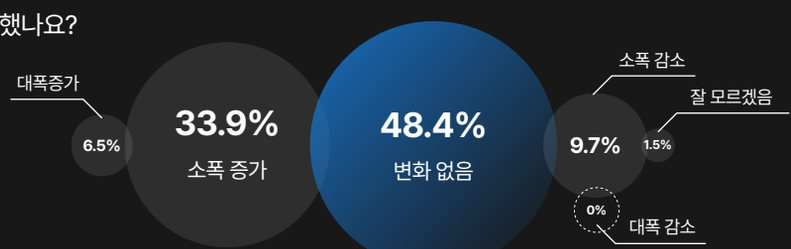
Q.

귀하의 조직에서 올해 **디지털 포렌식 관련 예산**은 작년 대비 어떻게 변화했나요?



Q.

귀하의 조직에서 **디지털 포렌식 관련 인원**은 작년 대비 어떻게 변화했나요?



2.2. Incident Response

• **Trends 1:** 신뢰된 외부 파트너 활용

많은 조직이 내부 사고 대응 인력이 부족해 침해사고 발생 시 효과적인 대응 체계를 수립하거나 위협을 종합적으로 파악하는 데 한계를 겪고 있다. 사고 대응에는 다양한 리소스가 종합적으로 요구되지만, 이를 충족하기 위한 인력 확보와 그 외 기술을 학습시키기 위해서는 상당한 비용이 수반되기 때문에, 현실적으로 많은 조직이 **EDR**(Endpoint Detection and Response) 솔루션을 우선 도입하는 추세다.

그러나, 업무 환경이 점차 다양화되고 복잡해짐에 따라 사이버 위협도 더욱 지능적이고 정교해지고 있으며, 단순히 보안 제품을 도입해 위협을 탐지하고 대응하는 것만으로는 모든 사고를 막기에는 역부족이다. 그럼에도 불구하고 여전히 일부 조직에서는 보안 제품 도입만으로 위협이나 사고가 예방될 것이라는 신뢰를 가지고 있으며, 이를 운영하고 해석할 수 있는 전문 인력이 부재한 상황에서는 큰 효과를 기대하기 어렵다.

최근 보안의 트렌드는 **'제로트러스트(Zero Trust)' 모델**로 진화하고 있으며, 이는 공격자의 접근을 무조건 차단하는 것을 넘어서, 침해가 발생하더라도 이를 사고로 확산시키지 않고 무력화하거나 피해를 최소화하는 것에 초점을 맞춘다. 즉, 지능화된 위협에 대해 무조건적인 방어보다는, 사고 발생 이후의 신속한 대응과 피해 확산 방지를 통해 비즈니스 연속성을 확보하는 전략이 강조되고 있다.

이에 따라 자체적으로 DFIR 팀을 운영하기 어렵거나 전문 인력을 확보하기 어려운 조직의 경우, 비용 대비 효과적인 외부 전문 파트너 서비스를 활용하는 것이 경제적일 뿐만 아니라 실질적인 문제 해결에도 도움이 된다. 즉, 조직은 조직의 핵심 역량에 집중하고, 사고 대응 영역은 신뢰할 수 있는 외부 파트너와 협업함으로써 전체적인 보안 역량을 높이는 것이 더욱 효과적이다.

최근에는 DFIR 서비스를 ***연간 구독형**(*SaaS: 클라우드 기반 서비스) 형태로 제공하는 사례도 증가하고 있다. 이에 따라 사고 대응의 전 과정을 아웃소싱 방식으로 운영하거나, SaaS 기반 DFIR 서비스를 조직 내부 위협 인사이트 확장 도구로 활용하는 접근은 효율적이고 전략적인 대응 방식으로 주목할 수 있다.

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

독립적인 사고 대응 팀이 있다.	IT 또는 보안팀 내에 사고 대응 담당이 포함되어 있다.	외부 DFIR 서비스 제공자와 계약해 운영한다.	사고 대응 팀이 존재하지 않는다.
31.7%	36.7%	1.7%	30%

Q. 침해사고가 발생하는 **가장 큰 환경적인 요인**은 무엇인가요?

예산 및 리소스 부족	보안 및 사고 대응 전문 인력의 부재	경영진의 관심과 지원 부재	보안 장비(솔루션)의 부재	지속적인 교육 및 훈련의 부재
20%	40%	20%	8.3%	6.7%

Q. 침해사고가 발생하는 **가장 큰 원인**은 무엇인가요?

웹 및 애플리케이션 취약점	보안 설정 미흡	보안 업데이트 미적용	피싱	계정 관리 미흡	기타
26.7%	35%	13.3%	5%	18.3%	1.7%

Q. 침해사고 대응 후 **가장 중요하다고 생각하는 것**은 무엇인가요?

잔존 위협 식별	위협 모니터링	재발방지 방안 적용 및 유지	보안 솔루션 도입	모의 침투 훈련
23.3%	11.7%	58.3%	5%	1.7%

Q. 현재 조직에서 **사고 대응과 관련**해 겪고 있는 가장 큰 문제는 무엇인가요?

탐지 및 대응 속도의 지연	신규 위협에 대한 탐지 및 대응 능력 부족	인력 부족으로 인한 업무 과부하	DFIR 관련 교육 및 기술 습득 기회 부족	멀티 플랫폼 환경에서의 일관된 대응 어려움
10%	35%	31.7%	8.3%	15%

Q. 귀하의 조직에서 활용하는 **사고 대응 절차**가 있나요?

절차별 구체적인 방안이 정의되어 있다.	단계별 절차만 정의되어 있다.	정의는 되어 있지 않지만 경험적으로 대응하고 있다.	사고 대응을 수행하고 있지 않다.
33.3%	28.3%	31.7%	6.7%

2.2. Incident Response

• **Trends 2:** 클라우드 환경에 대한 조사 역량 개발

최근 몇 년간 클라우드 환경으로의 인프라 전환이 빠르게 진행되면서, DFIR 관점에서도 클라우드 환경에 대한 전문적인 대응 역량 확보의 필요성이 커지고 있다. 이번 설문조사의 응답자의 대부분이 앞으로 클라우드 환경에 대한 사고 대응 역량 개발의 필요성을 최우선으로 선택했다는 점은 기존 사고 대응 체계가 클라우드 보안 위협에 효과적으로 대응하지 못하고 있음을 나타낸다.

클라우드는 이제 단순한 트렌드를 넘어 모든 산업 영역에서 핵심적인 IT 인프라로 자리잡고 있다. 이러한 변화 속에서 사고 발생 시 클라우드 특성을 고려하지 않은 기존의 대응 방식은 오히려 분석을 지연시키고, 중요한 데이터 확보의 기회를 놓치는 결과로 이어질 수 있다.

그럼에도 많은 조직에서는 여전히 전통적인 온프레미스 조사 기법을 클라우드 환경에 그대로 적용하려는 시도가 많다. 하지만 클라우드 특유의 구조(가상화, 분산 저장소, 세분화된 권한 모델 등)로 구성되어 있어 기존 방법론만으로는 사고 원인을 추적하는 데 한계를 갖는다.

또한, 다수의 조직들이 클라우드 환경을 비용 절감 또는 운영 편의성 목적으로 도입하고 있지만, 실제 보안을 위한 별도의 설정을 적용하지 않거나 기본 설정만으로 충분하다고 오해하는 경우가 많다. 이로 인해 사고 발생 시 로그 부재, 대응 지연 등의 문제로 이어지고 있다.

클라우드 환경은 단순히 VM(호스트)만으로 구성되는 것이 아니라 마켓플레이스에서 제공되는 수많은 Add-on 서비스, SaaS 연동 도구, 관리형 서비스 등이 함께 사용된다. 따라서, 사고 분석 시 단순 호스트 이미지 수집에 그치지 않고, 클라우드 플랫폼에서 제공하는 다양한 로그의 확보와 분석이 반드시 병행되어야 한다.

이런 문제를 근복적으로 해결하기 위해서는, '클라우드 환경에서의 침해사고를 어떻게 분석할 것인가'에 대한 체계적인 방법론 개발이 반드시 필요하다. 기존 온프레미스 기반 분석 방식이 가진 한계를 극복하고, 클라우드 인프라의 특성을 반영한 실질적인 분석 방안이 연구되어야 한다.

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

2.2. Incident Response

• **Trends 3:** 하이브리드 공격에 대한 연계 대응

최근 사이버 위협은 단순한 침해를 넘어, 복합적이고 정교한 형태의 하이브리드 공격으로 빠르게 진화하고 있다. 공격자는 시스템에 침투한 이후, 단일한 목적이 아닌 다수의 목적을 동시에 달성하기 위한 전략적 행위를 수행하는 것이 일반적이다.

대표적인 예로, 랜섬웨어 공격의 경우 파일 암호화 이전에 데이터를 선제적으로 유출한 뒤, 복호화 키에 대한 협상이 결렬될 경우 데이터 유출을 추가 협상 수단으로 활용하는 이중 갈취 전략이 보편화되고 있다. 또한, 웹 서버 침해 사례에서는 다른 해킹의 공격 경유지로 활용, 연동된 데이터베이스의 탈취 및 삭제, 소스코드와 데이터 유출을 협박 수단으로 삼는 방식도 자주 볼 수 있다.

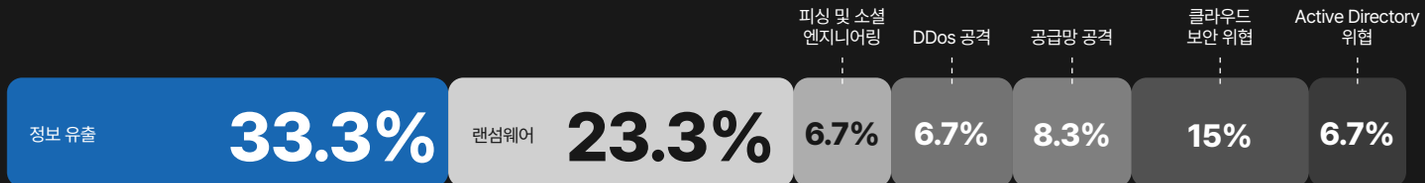
현실에서는 대부분의 조직이 이러한 복합적 위협에 대해 단편적이고 사후적인 대응에 머물고 있는 실정이다. 예를 들어, 랜섬웨어 사고 발생 시 복호화 키 확보를 위한 협상이나 시스템 초기화 중심의 복구 작업에 집중하고, 정보 유출과 같은 추가 피해에 대한 대응은 피해가 가시화된 이후에야 수동적으로 시작되는 경우가 많다.

그 결과, 공격자의 명시적인 목적(예. 금전 요구, 데이터 파괴 등)에만 대응이 집중되고, 그 과정에서 수행된 은밀한 침투 행위나 부가 목적에 대한 분석과 대응은 이루어지지 않는 경우가 대부분이다. 이는 하이브리드 위협이 단일 목적 중심의 기존 사고 대응 체계로는 효과적으로 다루기 어렵다는 것을 보여주며, 다중 목적 기반 공격에 대응할 수 있는 정밀하고 연계된 대응 체계 구축의 필요성을 시사한다.

더 큰 문제는, 여전히 많은 조직이 랜섬웨어 대응과 데이터 유출 탐지를 서로 다른 보안 영역으로 분리해 인식하고 있다는 점이다. 이로 인해 공격을 전체적인 흐름 속에서 통합적으로 분석하고 대응하기 어려운 구조적인 한계가 발생하고 있다.

하이브리드 공격은 예외적인 위협이 아니라, 일상적인 공격 방식으로 인식되어야 한다. 이에 따라 조직은 복구 중심의 대응 방식에서 벗어나, 공격의 전 단계를 포괄하는 가시성 확보, 그리고 위협의 전반적인 흐름을 파악할 수 있는 통합적 대응 체계를 갖추어야 한다.

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



03

Wrap Up

2025 DFIR REPORT

03.

Wrap Up

Conclusion

본 설문의 결과는 디지털 포렌식과 침해사고 대응 분야가 직면한 현실과 앞으로 나아가야 할 방향성을 제시하고 있다.

각 영역을 대표하는 핵심 메시지는 다음과 같다.

• Digital Forensics

도구의 한계를 넘어, 사람과 체계로 완성하는 포렌식

디지털 포렌식 환경은 이제 단순한 기술 기반 분석을 넘어, 복잡하게 변화하는 환경에 능동적으로 대응할 수 있는 전략적 사고와 체계적인 분석 역량이 요구되는 분야로 진화하고 있다.

모바일, 클라우드, IoT/임베디드 등으로 분석 대상이 확장됨에 따라, 포렌식 분석가는 더 이상 하나의 도구나 방식에 의존해 문제를 해결하기 어려운 현실에 직면해 있다. 데이터는 더욱 다양해졌고, 사용자의 행위는 더 은밀해졌으며, 분석해야 할 범위와 복잡도 또한 크게 증가하고 있다. 이에 따라, 사건 중심 사고에서 환경 중심 사고로의 전환, 그리고 정형화된 절차에서 유연한 분석 체계로의 전환이 필요한 시점이다.

도구의 한계를 뛰어넘어 분석가의 전문성, 분석 절차의 표준화, 자동화 기술의 접목, 그리고 이를 뒷받침할 수 있는 지속 가능한 분석 프레임워크의 구축은 디지털 포렌식 분야가 다음 단계로 도약하기 위한 핵심 요소가 될 것이다.

지금 우리가 마주한 변화는 단순히 새로운 도구를 익히는 것을 넘어, 기술과 절차, 그리고 사람의 역량이 균형을 이루는 종합적인 분석 체계를 구축해 나가는 과정이다. 이러한 접근을 통해 디지털 포렌식은 단순한 분석을 넘어 사고의 실체를 밝히고 조직의 대응 전략을 강화하는 핵심 기술로 자리잡게 될 것이다.

Conclusion

• Incident Response

보이지 않는 위협엔, 보이는 신뢰가 필요하다.

보안은 위기가 발생했을 때보다 위협을 조용히 막아내며 본래의 역할을 수행할 때 진가를 발휘하는 영역이다. 사고가 발생하지 않았다는 것은 단순히 '운이 좋았던 것'이 아니라, 사전에 설계된 보안 체계가 침묵 속에서 효과적이고 안정적으로 운영되고 있었음을 의미할 수 있다.

그러나, 조직 내부에서 이미 위협이나 침해 시도가 발생하고 있었음에도 이를 탐지하지 못한 채 '문제가 없는 것처럼 보이는 침묵'이라면 말은 다르다.

단순히 사고가 없다는 이유만으로 안심할 것이 아니라, 우리 조직이 실제로 안전한지 아니면 놓치고 있는 신호가 없는지를 끊임없이 점검해야하고 이를 대응하기 위해 역량을 개발하거나 체계를 마련해야 한다.

만약 이러한 점검을 조직 내부에서 독자적으로 수행하기 어렵다면, 신뢰할 수 있는 외부의 파트너 서비스를 통해 정기적으로 검증해 그 침묵이 진짜 '안전'을 의미하는지를 확인하고 대응하는 체계적인 접근이 필요하다.

이러한 관점에서 최근에는 조직 내 실제 사고 발생 여부를 확인하기 위한 '침해 평가 서비스', 그리고 엔드포인트 및 네트워크 전반을 상시 모니터링하고, 사고 발생 시 전문 DFIR팀이 즉각 대응하는 연계 서비스가 주목받고 있다.

이는 보안 체계의 실효성을 객관적으로 검증하고, 조직의 침묵이 진짜 '안전'을 의미하는지 확인하는 핵심 수단이 될 것이다.

04

[별첨]
설문조사 전체결과

2025
DFIR
REPORT

04.

4-1

[별첨] 설문 조사 전체 결과

- ## 4.1. Digital Forensics

디지털 포렌식 환경

- 귀하의 업무 수행 경력은 얼마나 되시나요?

문항	응답률
1~3년	30.6%
4~6년	17.7%
7~9년	24.2%
10~14년	22.6%
15년 이상	4.8%

- 귀하는 주로 어떤 업무를 수행하고 계신가요?

문항	응답률
분석	46.8%
범죄 수사	17.7%
부정조사 및 내부 감사	19.4%
eDiscovery	1.6%
연구	9.7%
기타	4.8%

- 귀하의 조직은 어떤 유형에 속하나요?

문항	응답률
소상공인/중소기업	9.7%
중견기업	9.7%
대기업	14.5%
공공기관	24.2%
수사기관	33.9%
학계	8%

- 귀하의 조직에서 올해 디지털포렌식 관련 예산은 작년 대비 어떻게 변화했나요?

문항	응답률
대폭 증가	9.7%
소폭 증가	32.3%
변화 없음	30.6%
소폭 감소	14.5%
대폭 감소	3.2%
잘 모르겠음	9.7%

- 귀하의 조직에서 디지털포렌식 관련 인원은 작년 대비 어떻게 변화했나요?

문항	응답률
대폭 증가	6.5%
소폭 증가	33.9%
변화 없음	48.4%
소폭 감소	9.7%
대폭 감소	0%
잘 모르겠음	1.5%

[별첨] 설문 조사 전체 결과

디지털 포렌식 현황

- 귀하의 조직에서 가장 많이 다루는 디지털포렌식 분야는 무엇인가요?

문항	응답률
디스크 포렌식	50%
모바일 포렌식	35.5%
네트워크 포렌식	1.6%
메모리 포렌식	6.5%
데이터베이스 포렌식	3.2%
IoT 포렌식	1.6%
기타	1.6%

- 귀하의 조직에서 최근 가장 비중이 늘어난 디지털포렌식 분야는 무엇인가요?

문항	응답률
디스크 포렌식	19.4%
모바일 포렌식	54.8%
네트워크 포렌식	4.8%
메모리 포렌식	4.8%
데이터베이스 포렌식	11.3%
IoT 포렌식	1.6%
기타	3.2%

- 귀하의 조직에 정보의 완전 삭제나 정보저장매체를 폐기하기 위한 절차가 마련되어 있나요?

문항	응답률
마련되어 있다.	75.8%
마련되어 있지 않으나, 계획 중이다.	12.9%
마련되어 있지 않으며, 계획도 없다.	6.5%
잘 모르겠음	4.8%

- 귀하의 조직에 정보의 완전 삭제나 정보저장매체 폐기를 어떻게 수행하고 있나요?

문항	응답률
디지털포렌식 부서 자체적으로 수행	74.2%
전산팀에 의뢰해 회사 차원에서 수행	17.7%
외부 업체에 의뢰해 수행	3.2%
잘 모르겠음	4.8%

- 귀하의 조직에 재해나 사고로부터 데이터를 보호하기 위한 재해복구(Disaster Recovery) 환경이 구축되어 있나요?

문항	응답률
구축되어 있다.	48.4%
구축되어 있지 않으나, 구축 계획 중이다.	22.6%
구축되어 있지 않으며, 계획도 없다.	22.6%
잘 모르겠음	6.4%

[별첨] 설문 조사 전체 결과

디지털 포렌식 도구

- 귀하의 디지털포렌식 도구 도입을 검토할 때 가장 중요한 고려사항은 무엇인가요?

문항	응답률
책정 예산 및 판매 금액	32.3%
도구의 성능	58.1%
제조사나 유통사의 기술 지원	4.8%
기타	4.8%

- 디스크 이미징을 수행할 때 가장 많이 사용하는 하드웨어 장비는 무엇인가요?

문항	응답률
Opentext TX1 / TD 시리즈	22.6%
Logicube Forensic Falcon	64.5%
Atola Taskforce / Insight Forensic	6.5%
Media Cube	0%
기타	6.4%

- 디스크 이미징 장비를 선택할 때 가장 중요한 고려사항은 무엇인가요?

문항	응답률
병렬 수행 여부	6.5%
이미징 속도	67.7%
배드 섹터 등 정보저장매체 오류 처리	21%
완료 리포트의 내용	3.2%
기타	8.1%

- 가장 많이 사용하는 이미징 소프트웨어는 무엇인가요?

문항	응답률
FTK Imager	38.7%
X-Ways Forensics	14.5%
EnCase	24.2%
Axiom Acquire	3.2%
Sumuri Paladin	0%
DFT(Digital Forensic Tool)	14.5%
기타	4.9%

- 위 이미징 소프트웨어를 가장 많이 사용하는 이유는 무엇인가요?

문항	응답률
오랜 사용 경험	43.5%
지원하는 기능이 많음	14.5%
환경에 크게 영향을 받지 않는 가벼움	33.9%
다른 분석 도구와의 연계	4.8%
기타	3.2%

- 귀하의 조직에서 가장 많이 사용하는 선별 수집 소프트웨어는 무엇인가요?

문항	응답률
DFT(Digital Forensic Tool)	38.7%
X-Ways Forensics	12.9%
EnCase	27.4%
FTK Imager	16.1%
기타	4.8%

- 디스크 포렌식 분석을 수행할 때 가장 많이 사용하는 도구는 무엇인가요?

문항	응답률
Magnet AXIOM	33.9%
X-Ways Forensics	16.1%
EnCase	33.9%
FTK	8.1%
Cellebrite Inspector	1.6%
Forensic Explorer	0%
기타	6.4%

- 위 도구를 가장 많이 사용하는 이유는 무엇인가요?

문항	응답률
오랜 사용 경험	58.1%
해당 도구에서만 지원하는 기능 존재	24.2%
추후 교차 검증이 쉬움	6.5%
비교적 저렴한 비용	3.2%
기타	8%

[별첨] 설문 조사 전체 결과

디지털 포렌식 도구

- 모바일 포렌식 수집 도구로 가장 많이 사용하는 도구는 무엇인가요?

문항	응답률
Cellebrite UFED, Inseyets, Premium / Phisical Analyzer	17.7%
MD-NEXT	75.8%
Magnet GRAYKEY / VERAKEY	3.2%
Oxygen	1.6%
XRY	0%
기타	1.6%

- 모바일 포렌식 분석 도구로 가장 많이 사용하는 도구는 무엇인가요?

문항	응답률
Cellebrite UFED, Inseyets, Premium	12.9%
MD-RED	80.6%
Magnet AXIOM	3.2%
Oxygen	1.6%
XRY	0%

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

문항	응답률
획득과 분석을 서로 다른 도구로 수행하기 위해서(예: Inseyets로 획득 후 MD-RED로 분석)	30.6%
도구에 따라 복구되는 데이터 양이 상이하므로	38.7%
분석 결과의 완전성을 검증하기 위해서	24.2%
기타	6.4%

- 디지털포렌식 능력 향상을 위해 수강하고 싶은 교육 과정은 무엇인가요?

문항	응답률
로그 및 아티팩트 분석	29.4%
모바일 수집과 분석	20.1%
클라우드 수집과 분석	23.2%
디지털포렌식 도구 활용	24%
기타	3.3%

04.

4-2

[별첨] 설문 조사 전체 결과

- ## 4.2. Incident Response

침해사고 대응 환경

- 귀하의 업무 수행 경력은 얼마나 되시나요?

문항	응답률
1~3년	31.7%
4~6년	26.7%
7~9년	10%
10~14년	25%
15년 이상	6.7%

- 귀하는 주로 어떤 업무를 수행하고 계신가요?

문항	응답률
사고 조사	33.4%
보안 CERT/관제	13.3%
보안 솔루션/인프라 운영	30%
보안 컨설팅	3.3%
연구/개발	10%
위협 인텔리전스	10%

- 귀하의 조직은 어떤 유형에 속하나요?

문항	응답률
소상공인/중소기업	26.7%
중견기업	23.3%
대기업	20%
공공기관	16.7%
수사기관	11.7%
비영리단체	1.7%

- 조직 내 사고 대응 팀의 구조는 어떤 형태로 구성되어 있나요?

문항	응답률
독립적인 사고 대응 팀이 있다.	31.7%
IT 또는 보안팀 내에 사고 대응 담당이 포함되어 있다.	36.7%
외부 DFIR 서비스 제공자와 계약해 운영한다.	1.7%
사고 대응 팀이 존재하지 않는다.	30%

[별첨] 설문 조사 전체 결과

침해사고 대응 환경

- 침해사고 대응을 위해 귀하가 보유하고 있는 상용 솔루션의 유형은 무엇인가요?

문항	응답률
로그 분석 - SIEM, Splunk, ELK 등	31.4%
포렌식(원인 분석) - X-Ways Forensics, Magnet AXIOM, Cyber Triage 등	19%
인텔리전스 - VirusTotal, Criminal IP, ATIP, QUAXAR 등	24.7%
악성코드 분석 - IDA, Joe SandBox, Anyrun, Hybrid Analysis 등	5.7%
기타	19.2%

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

문항	응답률
안티바이러스(백신)	30%
(웹)방화벽	31.7%
DDoS 방어	1.7%
IDS/IPS	15%
패치관리시스템	0%
접근제어시스템	20%
기타	1.6%

- 현재 귀하의 조직에서 운영 중인 보안 솔루션 중 탐지/대응 관점에서 가장 효과적으로 판단되는 솔루션은 무엇인가요?

문항	응답률
EDR/XDR	55%
MSS/MDR	1.7%
SIEM	25%
SOAR	6.7%
기타	11.6%

- 앞으로 어떤 환경에 대한 사고 대응 역량 개발이 필요하다고 생각하시나요?

문항	응답률
macOS	6.7%
모바일	3.3%
클라우드	61.7%
IoT	10%
공급망	15%
기타	3.3%

[별첨] 설문 조사 전체 결과

사고 대응 현황

- 귀하가 속한 조직에서 가장 대응이 시급하다고 생각되는 보안 위협은 무엇인가요?

문항	응답률
랜섬웨어	23.3%
정보 유출	33.3%
피싱 및 소셜 엔지니어링	6.7%
DDos 공격	6.7%
공급망 공격	8.3%
클라우드 보안 위협	15%
Active Directory 위협	6.7%

- 침해사고가 발생하는 가장 큰 환경적인 요인은 무엇인가요?

문항	응답률
예산 및 리소스 부족	20%
보안 및 사고 대응 전문 인력의 부재	45%
경영진의 관심과 지원 부재	20%
보안 장비(솔루션)의 부재	8.3%
지속적인 교육 및 훈련의 부재	6.7%

- 최근 침해사고가 발생하는 가장 큰 원인은 무엇인가요?

문항	응답률
웹 및 애플리케이션 취약점	26.7%
보안 설정 미흡	35%
보안 업데이트 미적용	13.3%
피싱	5%
계정 관리 미흡	18.3%
기타	1.7%

- 침해사고 대응 후 가장 중요하다고 생각하는 것은 무엇인가요?

문항	응답률
잔존 위협 식별	23.3%
위협 모니터링	11.7%
재발방지 방안 적용 및 유지	58.3%
보안 솔루션 도입	5%
모의 침투 훈련	1.7%

- 현재 조직에서 사고 대응과 관련해 겪고 있는 가장 큰 문제는 무엇인가요?

문항	응답률
탐지 및 대응 속도의 지연	10%
신규 위협에 대한 탐지 및 대응 능력 부족	35%
인력 부족으로 인한 업무 과부하	31.7%
DFIR 관련 교육 및 기술 습득 기회 부족	8.3%
멀티 플랫폼 환경에서의 일관된 대응 어려움	15%

- 사고 대응 활동에서 경영진의 역할 중 가장 중요한 것은 무엇인가요?

문항	응답률
사고 대응 시 충분한 예산 및 자원 할당	36.7%
사후 재발방지 대책의 지원	21.7%
사고 발생 시 빠른 의사결정	11.7%
정기적인 DFIR 정책과 절차 리뷰 참여	6.7%
전사적인 보안 인식 및 중요성 메시지 전달	23.3%

- 귀하의 조직에서 활용하는 사고 대응 절차가 있나요?

문항	응답률
절차별 구체적인 방안이 정의되어 있다.	33.3%
단계별 절차만 정의되어 있다.	28.3%
정의는 되어 있지 않지만 경험적으로 대응하고 있다.	31.7%
사고 대응을 수행하고 있지 않다.	6.7%

[별첨] 설문 조사 전체 결과

사고 대응 서비스

- 사고 대응과 관련해 외부 서비스의 필요성을 느끼시나요?

문항	응답률
매우 필요하다	68.3%
조금 필요하다	28.3%
필요하지 않다	0%
해당하지 않음	3.3%

- 사고 대응과 관련해 필요한 외부 서비스는 무엇인가요?

문항	응답률
악성코드 분석	15%
위협 인텔리전스(다크웹 포함)	16.7%
사고 원인 분석	33.3%
재발방지 대책 마련	31.7%
공격자 협상	1.7%
대응 전 솔루션 마련	1.7%

- 사고 대응 관련 외부 서비스를 이용할 때 추가적으로 기대하는 효과는 무엇인가요?

문항	응답률
신속한 침해사고 대응	51.7%
내부 인력의 업무 부담 감소	11.7%
정보보호 수준 향상	15%
대응 인사이트 습득	20%
신뢰도가 높은 제3자가 분석한 결과 보고서	1.7%

- 사고 대응 서비스 제공자와의 협력에서 가장 필요한 부분은 무엇인가요?

문항	응답률
체계적인 의사 소통	26.7%
협업 툴을 활용한 실시간 상황 공유	10%
지속적인 상황 공유와 투명한 정보 제공	25%
최신 위협 정보 및 트렌드 제공	13.3%
조직 맞춤형 대응 방안 제시	20%
기밀 유지	5%

- 사고 대응 이후 작성하는 보고서의 가장 중요한 요소는 무엇이라고 생각하시나요?

문항	응답률
사고 원인과 경로의 정확한 분석	51.7%
사고의 범위와 피해 규모	1.7%
대응 과정에서 확인된 취약한 설정(취약점)	15%
향후 사고 예방을 위한 구체적 권고 사항	26.7%
기술적 용어와 분석 내용의 쉬운 설명	5%

- 침해사고 대응과 관련해 가장 필요한 교육은 무엇이라고 생각하시나요?

문항	응답률
로그 및 아티팩트 분석	38.4%
타겟형 공격 분석	16.7%
악성코드 분석	18.3%
위협 인텔리전스 활용	26.7%

- 사고 대응 관련 외부 서비스를 이용하려고 할 때 가장 중요한 고려사항은 무엇인가요? (1~3순위 선택)
  - 1순위 - 서비스 업체의 전문성 및 경험
  - 2순위 - 서비스 비용
  - 3순위 - 서비스 품질(체계)

플레인비트 2025 DFIR 트렌드 보고서

2025 DFIR REPORT

PLAINBIT

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