2025 DFiR REPORT

- 조사기간 : 2024년 11월 ~ 12월
- 조사대상 : IR 관련 종사자 150여명

- **귀하의 업무 수행 경력은?**

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

- **귀하의 조직 유형은?**

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

- **주로 어떤 업무를 수행하나요?**

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

2025 DFiR REPORT

Trends 1 : 신뢰된 외부 파트너 활용

Trends 1 : 신뢰된 외부 파트너 활용

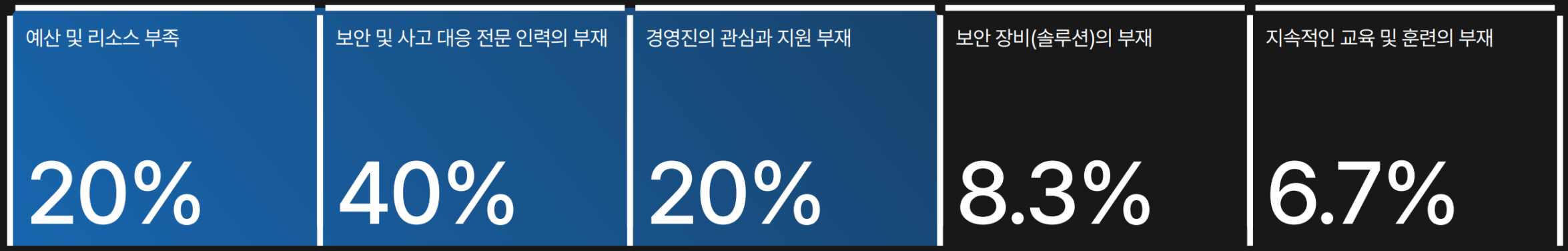
Q) 조직 내 **사고 대응 팀**은 어떤 형태로 구성되어 있나요?

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%

Trends 1 : 신뢰된 외부 파트너 활용

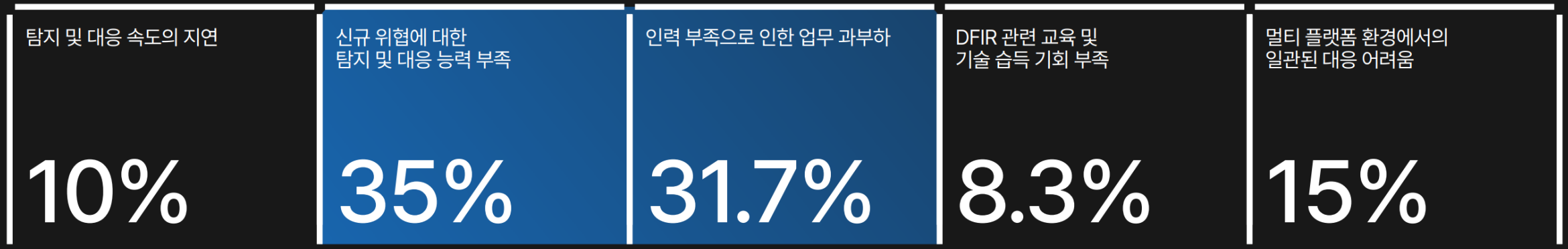
2025 DFIR REPORT

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



Trends 1 : 신뢰된 외부 파트너 활용

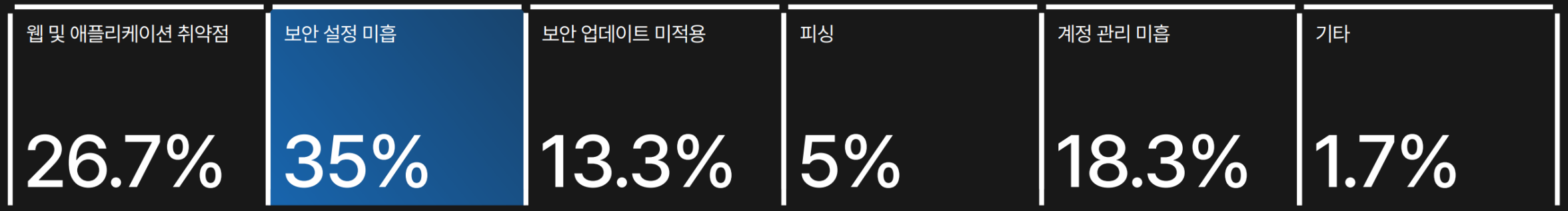
Q) 현재 조직에서 **사고 대응과 관련**해 겪고 있는 가장 큰 문제는 무엇인가요?



Trends 1 : 신뢰된 외부 파트너 활용

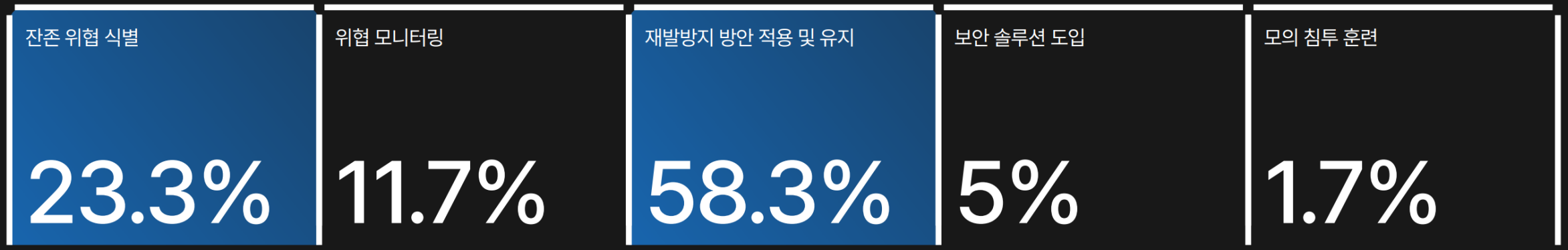
2025 DFIR REPORT

Q) 침해사고 발생하는 **가장 큰 원인**은 무엇인가요?



Trends 1 : 신뢰된 외부 파트너 활용

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



2025 DFiR REPORT

Trends 1 : 신뢰된 외부 파트너 활용

Trends 2 : 클라우드 환경에 대한 조사 역량 개발

Trends 2 : 클라우드 환경에 대한 조사 역량 개발

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

2025 DFiR REPORT

Trends 1 : 신뢰된 외부 파트너 활용

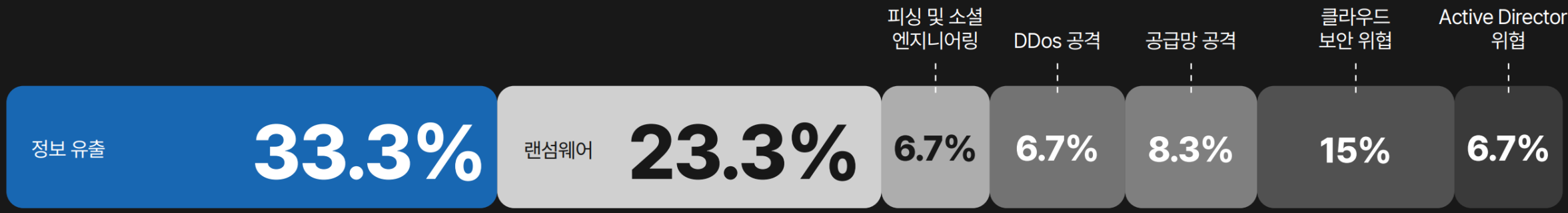
Trends 2 : 클라우드 환경에 대한 조사 역량 개발

Trends 3 : 하이브리드 공격에 대한 연계 대응

Trends 3 : 하이브리드 공격에 대한 연계 대응

2025 DFIR REPORT

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



사고 현장의 문제를 해결하라!

DEFENDER SUMMIT 2025

주최 | PLAINBIT NARUSECURITY Making Sense of the Unknown

왜 DEFENDER SUMMIT 인가?

사고 발생

Readiness + Assurance Consulting		Incident Response Services
Vulnerability Assessment	Red/Purple Team Assessment	Incident Response & Analysis
Web/Mobile Application Security Testing	(Cloud) Penetration Testing	Compromise Assessment
Ransomware Defense Assessment	AD Security Assessment	Post-Incident Risk & Gap Assessment
Insider Threat Assessment	Cloud Security Assessment	Security Awareness & Process Improvement
Source Code Review / Static Code Analysis	Risk Assessment & Management	
Cyber Range Simulation Exercises	Security Maturity Assessment	

최근 대규모 사고 이후에 계속되는 질문

Q) 현재 운용 중인 사고 대응 체계의 개선책을 알려주세요.

Q) 위협을 식별하기 위한 새로운 방법 혹은 접근법이 있나요?

Q) 드러나지 않는 위협을 어떻게 진단해야 할까요?

Q) 보안 통제와 식별을 계속해오고 있는데 뭘 더해야 할까요?

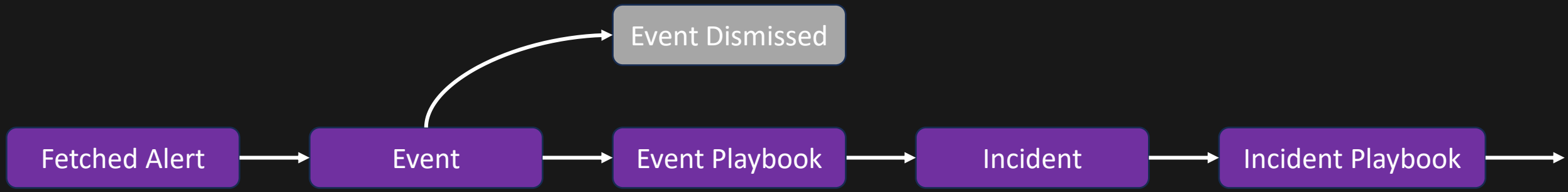
최근 대규모 사고 이후에 계속되는 질문

Q) 현재 운용 중인 사고 대응 체계의 개선책을 알려주세요.

Q) 위협을 식별하기 위한 새로운 방법 혹은 접근법이 있나요?

Q) 드러나지 않는 위협을 어떻게 진단해야 할까요?

Q) 보안 통제와 식별을 계속해오고 있는데 뭘 더해야 할까요?



➔ 이벤트는 평가되어야 하고, 사고로 연결되어야 한다.

➔ 사고의 초기 유입부터 사고로 이어지기까지의 전 과정을

집요하게 분석하고, 각 단계의 인과관계를 논리적으로 연결해야 한다.