길어진 Dwell Time:
탐지와 대응 사이에 남겨진 침해의 결과

DFIR 서비스팀

장원희 팀장

PLAINBIT

CONTENTS

Dwell Time 현황

- 기술은 더 정교해졌지만, 탐지는 더 늦어졌다

Dwell Time 현황

Dwell Time?

- **침해 발생 시점 → 탐지될 때까지의 시간**
  - 공격자가 침투한 이후 탐지되기까지 조직 내에 머문 시간
  - 조직이 위협을 얼마나 늦게 인지했는지를 나타내는 리스크의 척도
    - ✓ Dwell Time이 길어질수록 원인 규명 난이도↑, 피해 범위가 확대됨 (내부망 확산, 데이터 유출 등)

Dwell Time 현황

PLAINBIT

- **Dwell Time 통계가 점차 짧아지고 있음**
  - 2024년 기준 외부 통보 11일, 내부 탐지 10일
  - 사고 대응 서비스에 대한 분석 비용 지불이 가능한 기업 = 보안이 잘 되어 있음!

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11
External	—	—	—	—	320	107	186	184	141	73	28	19	13	11
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9	10

▲ M-Trend 2025(Mandiant)

Dwell Time 현황

- Dwell Time 통계가 점차 짧아지고 있음
  - 2024년 기준 외부 통보 11일, 내부 탐지 10일
  - 사고 대응 서비스에 대한 분석 비용 지불이 가능한 기업 = 보안이 잘 되어 있음!

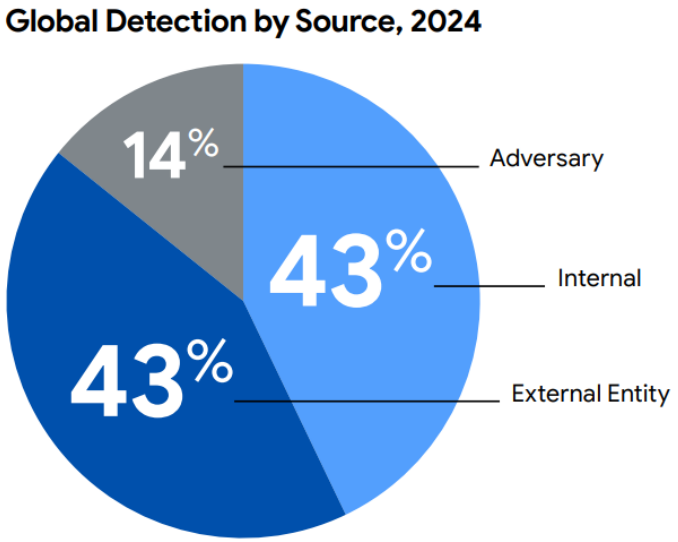
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11
External	—	—	—	—	320	107	186	184	141	73	28	19	13	11
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9	10

▲ M-Trend 2025(Mandiant)

왜 Dwell Time이 점차 감소할까?

Dwell Time 현황

- **보안 탐지 체계의 전반적 향상**
  - EDR, XDR, SIEM등의 확산으로 실시간 탐지 능력 강화
- **조직 내부에서 직접 침해를 탐지한 비율 증가**
  - 조직 내부에서 침해 징후를 감지할 수 있는 인력 및 시스템 증가
- **랜섬웨어 공격 방식의 변화**
  - 은밀하게 오랜 기간 머무르기보다는 빠르게 실행한 후, 공격자가 스스로 사고를 알리는 경우 多
- **사고 대응 능력 강화**
  - MDR(Managed Detection and Response) 등 외부 대응 서비스 도입 증가

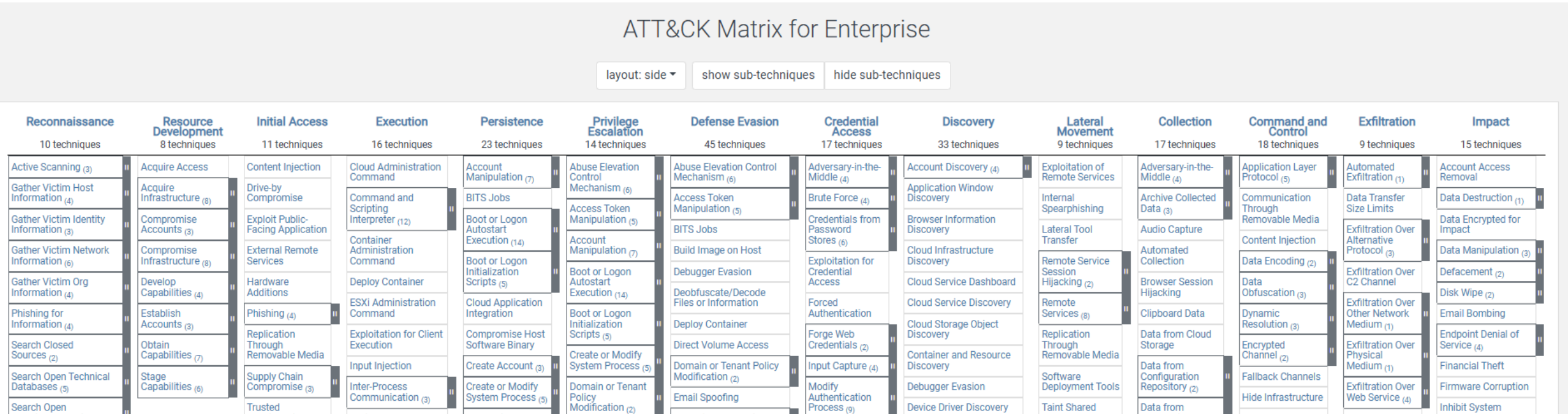


▲M-Trend 2025(Mandiant)

Dwell Time 현황

PLAINBIT

- **공격 패턴의 반복성과 예측 가능성 ↑**
  - 많은 공격 그룹이 공격에서 TTPs(전술, 기술, 절차)를 재사용하거나 변형된 형태로 반복
  - MITRE ATT&CK 기반 탐지 룰, 행동 기반 탐지(IoA) 등을 통해 유사 공격 패턴을 조기에 식별하기 쉬워짐
  - 보안 커뮤니티 및 벤더의 위협 인텔리전스 공유가 활발해짐



Dwell Time 현황

PLAINBIT

- 공격 패턴의 반복성과 예측 가능성 ↑
  - 많은 공격 그룹이 공격에서 TTPs(전술, 기술, 절차)를 재사용하거나 변형된 형태로 반복
  - MITRE ATT&CK 기반 탐지 룰, 행동 기반 탐지(IoA) 등을 통해 유사 공격 패턴을 조기에 식별하기 쉬워짐
  - 보안 커뮤니티 및 벤더의 위협 인텔리전스 공유가 활발해짐

완전히 대응이 쉬워졌다는 과장된 표현!

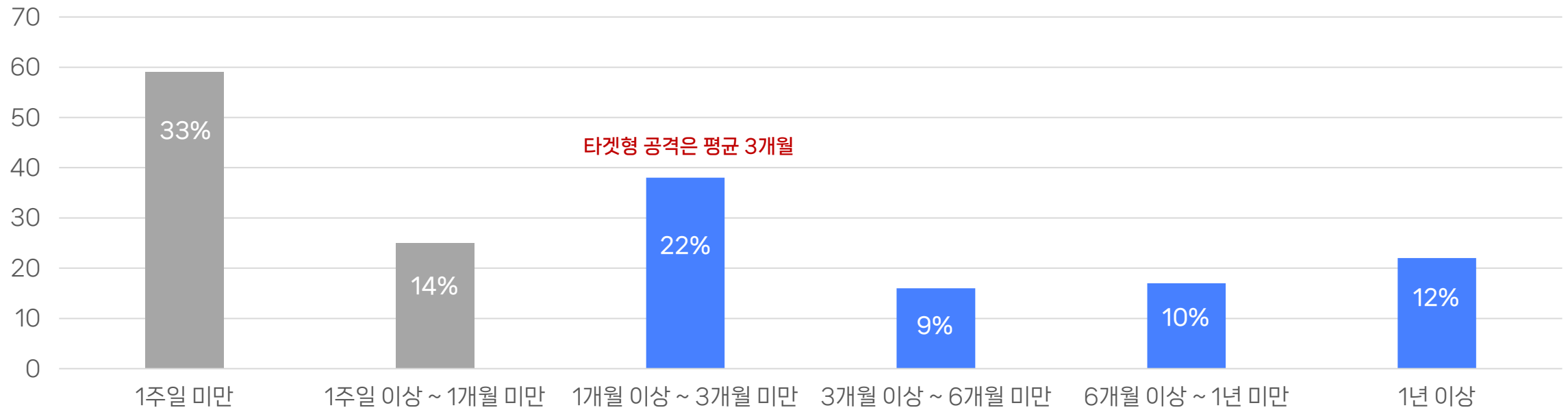
공격자들은 끊임없이 기존 TTPs를 변형하고 탐지를 우회하는 방식으로 진화

(Living off the Land 기법, 파일리스 공격, 정상 툴의 악용 등으로 정적 시그니처 기반 탐지 회피)

Dwell Time 현황

PLAINBIT

- **사고 분석 서비스 대상 기준으로 평균 162일에 해당 (최근 3년)**
  - 70% 이상이 외부기관이나 제3자를 통해 사고 사실 최초 인지
  - 피해가 가시화되는 유형의 사고(랜섬웨어, 웹 페이지 변조 등)는 주로 Dwell Time이 1주일 미만에 해당
  - 로그 부재 등으로 인해 실제 침투 시점을 확인할 수 없는 사례가 다수 존재



사고 대응 관점에서의 Dwell Time

- 무시된 수차례의 침해 신호는 결국 사고로 이어졌다

사고 대응 관점에서의 Dwell Time

PLAINBIT

사고 대응 과정에서 자주 듣는 질문

- 어떻게 빠른 시일 내에 피해가 확산된 건가요?
- 백신도 있고, EDR도 있는데 왜 탐지하지 못한 건가요?
- 저희가 볼 땐 아무 이상이 없었는데, 뭐가 문제였던 건가요?
- 해당 이벤트가 왜 위협인가요?
- 공격자는 그동안 내부에서 무엇을 할 수 있었나요?
- 왜 원인을 확인하지 못하는 건가요?
- 피해가 어디까지 확산됐으며, 확산된 이유는 무엇인가요?
- 위협이 아직도 잔존하고 있나요?

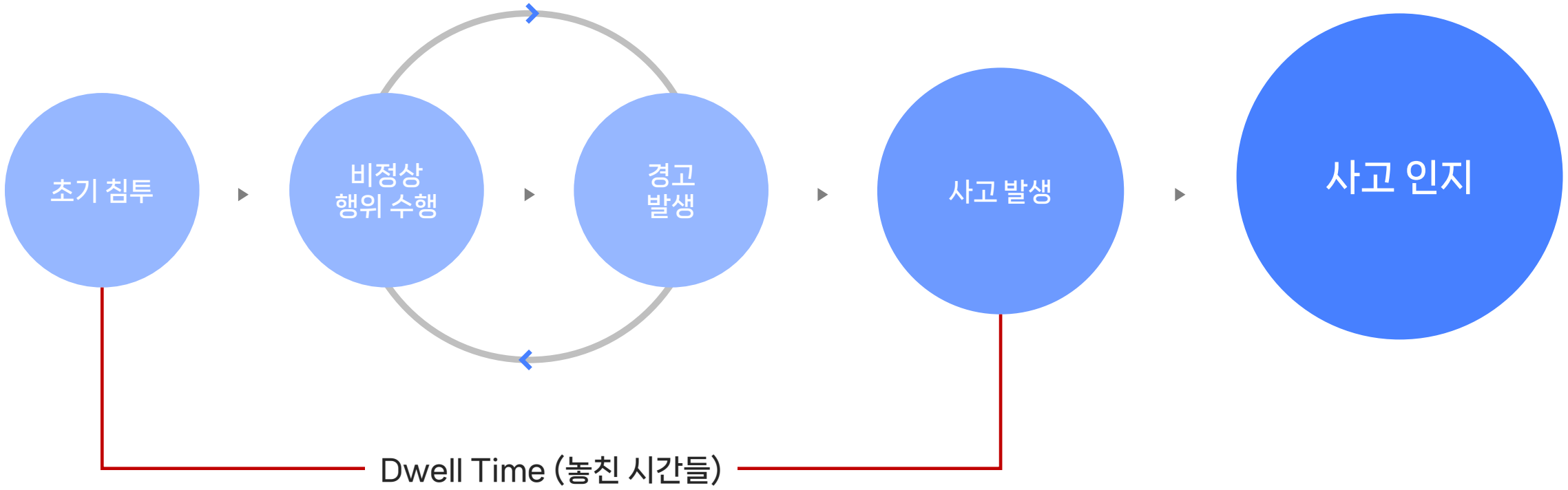
모든 질문은 결국

Dwell Time에 대한 궁금증이었다.

사고 대응 관점에서의 Dwell Time

우리는 언제 인지했는가?

- **수많은 경고가 있었지만, 우리는 '결과'로 인지했다**
  - 표면적으로 드러나는 위협만 처리 → 랜섬웨어 감염, 정보 유출(기밀정보, 개인정보), 데이터베이스 조작/삭제, 웹 페이지 변조 등
  - 사고가 발생한 후 돌이켜보면 수많은 이벤트들이 사고를 경고하고 있었음



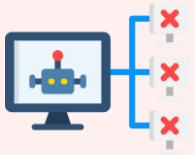
사고 대응 관점에서의 Dwell Time

PLAINBIT

우리는 언제 인지했는가?

- **충분히 위협을 인지하고 사고를 무력화할 수 있는 기회는 많았다**

비정상 로그인 시도



내부 이동

네트워크 스캐닝

공격 계정 생성

악성 프로그램 실행/설치

악성 스크립트 실행

악성 작업스케줄/
서비스 실행

주기적인 C2 통신

길어진 Dwell Time에 따른 대응의 한계

- **조사 데이터 부재**
  - **원인 규명 및 침해 전파 경로 식별을 위한 로그 부재**
    - ✓ 저장 용량 부족으로 인해 저장 주기 초과, 로그 백업 체계 부재, 공격자 삭제 등
  - **공격의 중간 또는 결과에 대한 흔적만 존재**
    - ✓ 공격 전후 시점의 흐름 파악이 불가해 공격자 행위 재구성이 어려움

길어진 Dwell Time에 따른 대응의 한계

- **피해 범위 추적이 어려움**
  - **Dwell Time이 길어질수록 공격 양상이 다르게 나타남** → 조사 대상 스코프 결정의 딜레마 발생
    - ✓ 1차 사고와 N차 사고 간의 공격 양상이 달라 내부 이동 범위 추적이 어려움
    - ✓ 예) 1차 사고: 기존의 계정 활용해 RDP 접근, 2차 사고: 공격 계정 생성 후 Chrome Remote Desktop 활용
  - **위협 모니터링 체계 부재로 단기간 내 동일 위협 파악이 어려움**
    - ✓ 백도어 통신 등 잔존하는 위협을 파악하는 데 어려움
  - **재발 방지 대책이 범용적으로 수립됨**
    - ✓ 정확한 공격 경로와 행위 흐름을 팡가하지 못해 재발 방지 대책 수립의 근거 부족

Dwell Time, 어떻게 줄일까?

- Dwell Time을 줄이는 것은 기술이 아니라 준비다

Dwell Time, 어떻게 줄일까?

PLAINBIT

우리는 답을 알고 있다

- **조직 내 위협 이벤트 분류 체계 마련**
  - 조직 내 위협 이벤트에 대해 정탐과 오탐을 분류 (장애인가? 사고인가?)
  - 이벤트 원인을 처리할 수 있는 조직과 사람이 필요

- **위협 이벤트 탐지하고 공격 행위를 분석하기 위한 아티팩트 로그화 필요**
  - 포렌식 기반 분석을 통해 흔적을 기반으로 공격자 행위 재구성 필요
  - 공격 행위를 분석할 수 있는 아티팩트를 로그화
  - 위협을 식별하기 위해서는 사람의 판단이 필요함
  - **신뢰할 수 있는 비즈니스 파트너 활용**

위협에 대한 경고는 충분했다.

침해는 사고로 이어졌고,
무시된 경고들은 사고를 예방할 수 있었던 기회였다.

PLAINBIT

신뢰된 DFIR 파트너와 함께
끊임없이 위협을 의심하고 대응해야 한다.

PLAINBIT