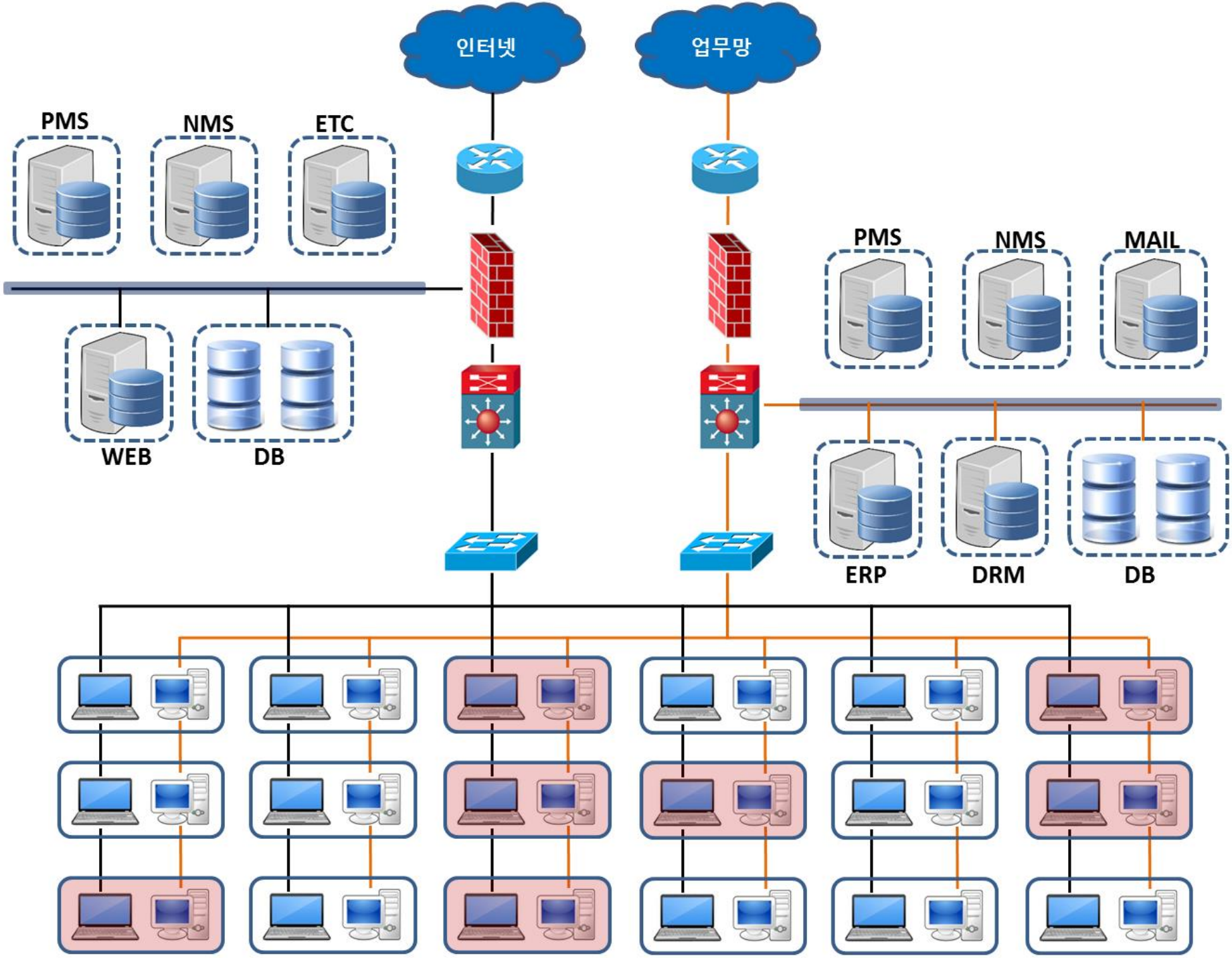
어떻게 가져갔는가? 그리고…

플레인비트 대표

김진국

jinkook.kim@plainbit.co.kr

어떻게 가져갔는가?


인터넷
업무망
PMS
NMS
ETC
WEB
DB
PMS
NMS
MAIL
ERP
DRM
DB

- 무엇을 조사해야 하는가?

라이브 데이터?

로그 vs. 아티팩트

어떻게 가져갔는가?

PLAINBIT

- **정보자산이 어디에 저장되어 있는가?**
  - **데이터베이스** (레코드, DB파일, 백업파일)
  - **파일서버** (파일)
  - **개인 PC, 노트북** (파일)
  - **… …**

- **정보자산이 어디에 저장되어 있는가?**
  - **데이터베이스**

✓ 데이터베이스 로그 조사 ➔ 우선 순위를 고려한 증거 보존!!

SQL Server	MySQL	Oracle
• Transaction Log	• General Query Log	• Redo Log
• Default Trace	• Slow Query Log	• TNS Listener Log
• Error Log	• DDL (metadata) Log	• Trace Files
• Application Log (Event Log)	• Error Log	• Sqlnet Log
• Cache (Memory)	• Binary Log	• Sysdba Audit Log
	• Cache (Memory)	

✓ 데이터베이스가 외부에서 접근이 가능한 경우?

- 네트워크 및 웹 서버 로그

어떻게 가져갔는가?

PLAINBIT

- **정보자산이 어디에 저장되어 있는가?**
  - **데이터베이스**
  - **파일서버**
    - ✓ 파일서버 로그 조사 ➔ **조사를 위한** 로그가 설정되어 있는가?

어떻게 가져갔는가?

PLAINBIT

- **정보자산이 어디에 저장되어 있는가?**
  - **데이터베이스**
  - **파일서버**
  - **개인 PC, 노트북**
    - ✓ 정보 자산의 접근 혹은 유출을 어떻게 추적할 수 있을까? ➔ 로그 및 아티팩트 상호 분석
    - ✓ **조사를 위한** 로그 혹은 아티팩트가 설정되어 있는가?

- 어떻게 외부로 가져가는가?

인터넷 이용?

내부망 이동

인터넷이 자유로운 곳까지...

PLAINBIT

- **내부망 이동은 어떻게 탐지하는가?**
  - 공격에서 확보한 감염 시스템 이용 ➔ 내부 클라이언트
  - 클라이언트에서 무엇을 볼 것인가?
    - ✓ 이벤트 로그 (클라이언트 인증, 공유 폴더, RDP 등)
    - ✓ 공격자 거주 흔적 (공격자 선호 경로, 파일명 패턴 등)

PLAINBIT

- 내부망 이동은 어떻게 탐지하는가?
  - 이벤트 로그 (EVTX)

이벤트 ID	이벤트 로그	설명
1000	System	BSOD, WER
4624/4625	Security	계정 로그온 성공 (로그온 유형 판단)
4648	Security	명시적 자격 증명을 사용하여 로그인 시도
4728/4729	Security	글로벌 그룹에 사용자 추가/제거
4732/4733	Security	도메인 로컬 그룹에 사용자 추가/제거
4756/4757	Security	유니버설 그룹에 사용자 추가/제거
5140	Security	네트워크 파일 공유 접근
4697	Security	서비스 설치
4097	Application	윈도우 문제 보고
7000,7001,7022, 7023,7024,7026, 7031,7032,7034	System	윈도우 서비스 실패 또는 크래시
…	…	…

어떻게 가져갔는가?

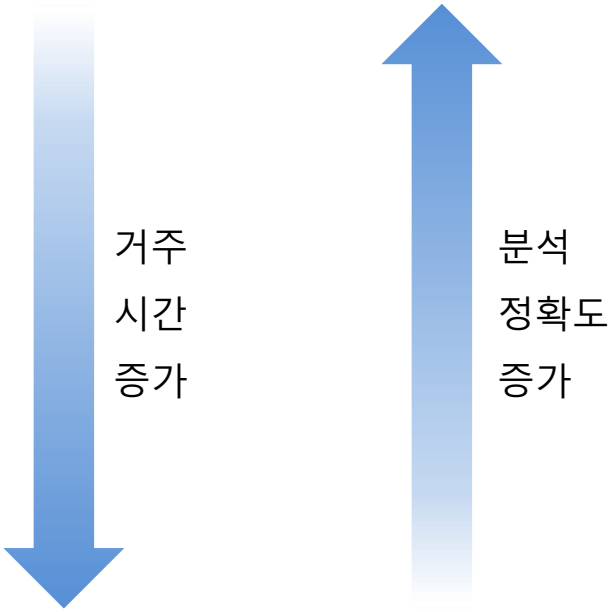
PLAINBIT

- **내부망 이동은 어떻게 탐지하는가?**
  - **공격자 거주 흔적 ➔ 선호 경로**
    - ✓ 시스템 경로 (%SystemRoot%₩[sub]₩[sub]) (dllcache, drivers, WOW64, …)
    - ✓ 사용자 기본 경로 (%SystemDrive%₩Users₩[sub]) (Default, Public)
    - ✓ 사용자 데이터 경로 (%UserProfile%₩AppData₩[sub], %SystemDrive%₩ProgramData₩[sub])
    - ✓ 휴지통 경로 (₩$Recycle.Bin₩)
    - ✓ 시스템 볼륨 경로 (₩System Volume Information₩)
    - ✓ 임시 경로 (%Temp%, %LocalAppData%₩Microsoft₩Windows₩Temporary Internet Files₩)
    - ✓ 알려진 경로
      - %SystemDrive%₩Intel
      - %SystemDrive%₩HNC
      - … …

어떻게 가져갔는가?

PLAINBIT

- **내부망 이동은 어떻게 탐지하는가?**
  - **공격자 거주 흔적 ➔ 선호 경로**
    - ✓ 파일시스템 로그
    - ✓ MFT / INDX 슬랙 조사
    - ✓ 볼륨 섀도 복사본
    - ✓ 프리패치
    - ✓ 호환성 아티팩트
    - ✓ 윈도우 문제 보고
    - ✓ … …



어떻게 가져갔는가?

PLAINBIT

- **내부망 이동은 어떻게 탐지하는가?**
  - **공격자 거주 흔적 ➔ 파일명 패턴**
    - ✓ 공격자 선호 파일 조사 (.vbs, .bat, .exe, .dll, .
    - ✓ 한 글자 파일명
    - ✓ 랜덤한 문자나 숫자로만 이뤄진 파일명
    - ✓ 확장자 변경으로 시그니처 불일치
    - ✓ 대체 데이터 스트림 (ADS, Alternative Data Stream)
    - ✓ 압축 파일 조사 (.rar, .zip) (주로 분할 압축 사용)
    - ✓ … …

- 어디로 가져가는가?

해외 서버 vs. 국내 서버

그리고…

PLAINBIT

- **침해사고 준비도**

침해사고에 따른 비용을 최소로 하고, 신속하고 효과적으로 대응하기 위한 조직의 준비능력

- 사고 가능성을 낮추기 위한 사전적 투자 X
- 사고 발생 시 피해를 최소화하는데 목적을 둔 사전적 투자 O
- **준비 능력**
  - ✓ 사후, 사고를 조기에 식별하기 위한 준비
  - ✓ 사후, 빠르고 효과적으로 대응하여 피해를 최소화하기 위한 준비
  - ✓ 사후, 사고의 원인과 과정을 밝혀내기 위한 준비

준비도를 갖추기 어려운 이유?

사고 발생의 필연성을

인정할 수 있는가...?

어떻게 인지되었는가?

누가 인지하였는가?

침해사고의 일반적

- **SAFENET'S BREACH LEVEL INDEX**

2014.01

~

2014.12

RANK	ORGANIZATION BREACHED	DATE BREACHED	RECORDS BREACHED	LOCATION	INDUSTRY	SOURCE OF BREACH	TYPE OF BREACH	RISK SCORE
1	Home Depot	9/2/2014	109,000,000	United States	Retail	Malicious Outsider	Financial Access	10.0
2	JPMorgan Chase	8/27/2014	83,000,000	United States	Financial	Malicious Outsider	Identity Theft	10.0
3	CyberVor	8/5/2014	1,200,000,000	Global	Technology	Malicious Outsider	Account Access	10.0
4	eBay	5/21/2014	145,000,000	United States	Retail	Malicious Outsider	Identity Theft	10.0
5	Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	1/20/2014	104,000,000	South Korea	Financial	Malicious Insider	Identity Theft	10.0
6	Benesse	7/15/2014	48,600,000	Japan	Education	Malicious Insider	Identity Theft	9.8
7	Websites for online games, movie ticketing and ring tone downloads	8/21/2014	27,000,000	South Korea	Technology	Malicious Outsider	Identity Theft	9.6
8	AliExpress	12/8/2014	300,000,000	China	Retail	Accidental Loss	Account Access	9.5
9	Korean Medical Association, Association of Korean Medicine and Korean Dental Association	2/17/2014	17,000,000	South Korea	Healthcare	Malicious Outsider	Identity Theft	9.4
10	Northwestern city of Verden	4/3/2014	18,000,000	Germany	Government	Malicious Outsider	Financial Access	9.3
11	Naver	3/28/2014	25,000,000	South Korea	Technology	Malicious Outsider	Account Access	9.3
12	Korea Telecom	2/15/2014	12,000,000	South Korea	Technology	Malicious Outsider	Identity Theft	9.3
13	Serbian State	12/13/2014	7,276,604	Serbia	Government	Malicious Outsider	Identity Theft	9.1
14	Pandora TV	9/9/2014	7,450,000	South Korea	Other	Malicious Outsider	Identity Theft	9.1

PLAINBIT

어떻게 처리되었는가?

사고로 인한 잠재위협이

모두 제거되었는가?

사고에 대한 인식의 문제

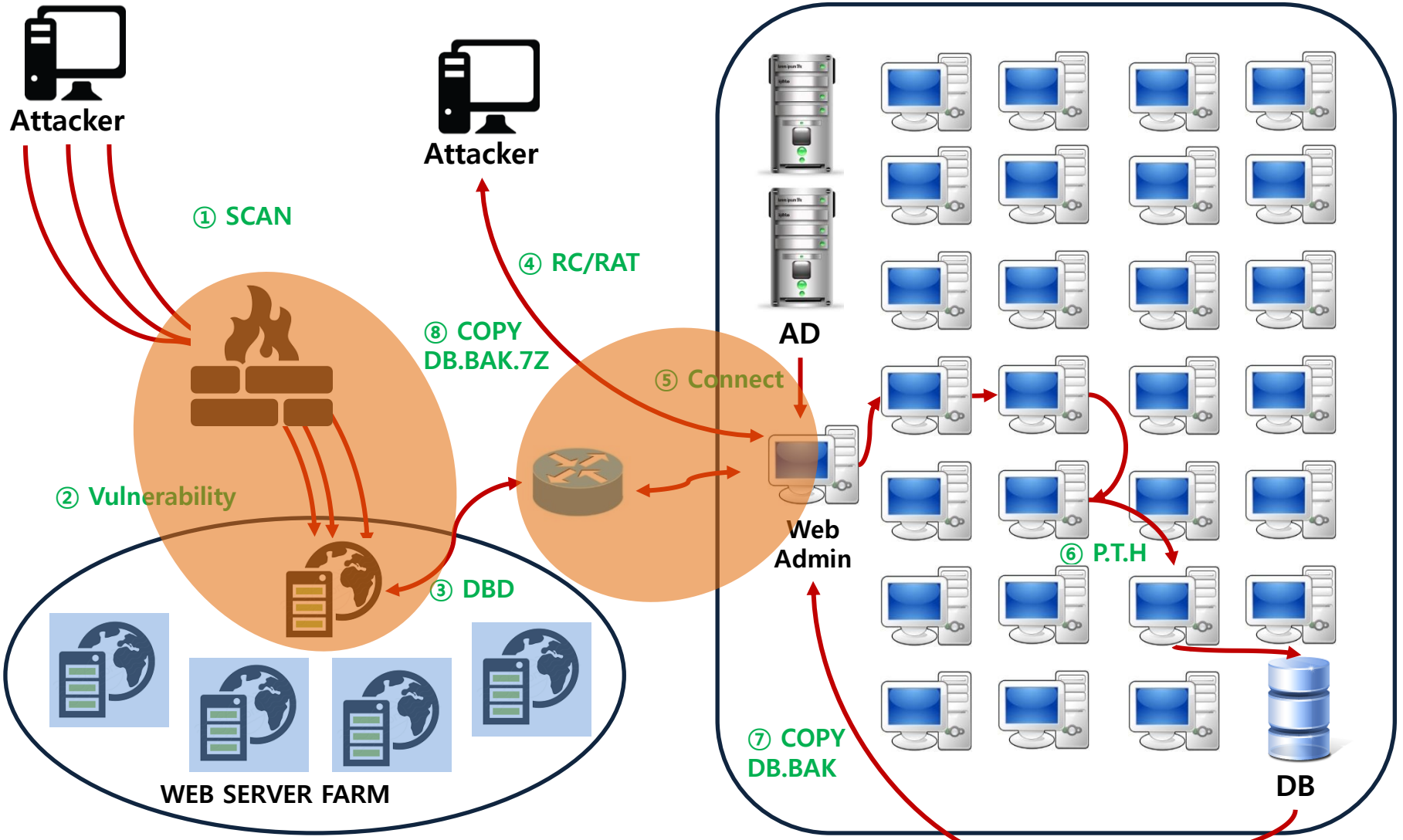
"사고를 막아보자"

"사고를 조기에 식별하고 사후 대응을 체계화하여 피해를 최소화하자 "

침해사고 준비도

PLAINBIT

- APT 혹은 타겟형 공격



침해사고 준비도

PLAINBIT

1. 클라이언트 설정을 강화하자!!

- **클라이언트 설정**
  - ✓ 운영체제 업그레이드
  - ✓ 프리패치 설정 강화
  - ✓ NTFS 파일시스템 로그 설정 강화
  - ✓ NTFS 파일시스템 접근 시간 갱신 강화
  - ✓ 로컬 방화벽 설정 강화
  - ✓ 볼륨 섀도 복사본 설정 강화
  - ✓ 이벤트 로그 설정 강화

- **클라이언트 데이터는 다양한 사고에 활용할 수 있음**
  - ✓ 내부자 유출, 정보감사 등

2. 모니터링(식별)을 강화하자!!

- 차단보다는 모니터링이 필요!!
- 공격자의 목적은 흔적 최소화가 아님
- 고 위험군 분류 (연구직, 영업직, 임원, 마케팅팀 등) 모니터링
- 사전에 관리된 침해사고 지표 모니터링

3. 신속한 대응 절차를 마련하자!!

- 침해사고의 골든 타임은 얼마인가?
- 사고 담당은 어느 부서에서 할 것인가?
- 사고 식별 시 초기 대응 방안 마련, 사고 대상 별 데이터 수집 절차 마련
- 사고 위험도 별 대응 절차 마련

4. 인력을 활용하자!!

- 장비/솔루션은 인력을 보완하는 역할 ➔ 판단은 사람이!
- 식별된 징후에 대해 분석할 수 있는 새로운 역할의 '분석팀' 필요
- 자체적인 인력을 구성하기 어렵다면 ➔ 외부의 전문 감사 서비스 활용
- 대응보다는 원인 파악에 초점을 맞춘 분석!

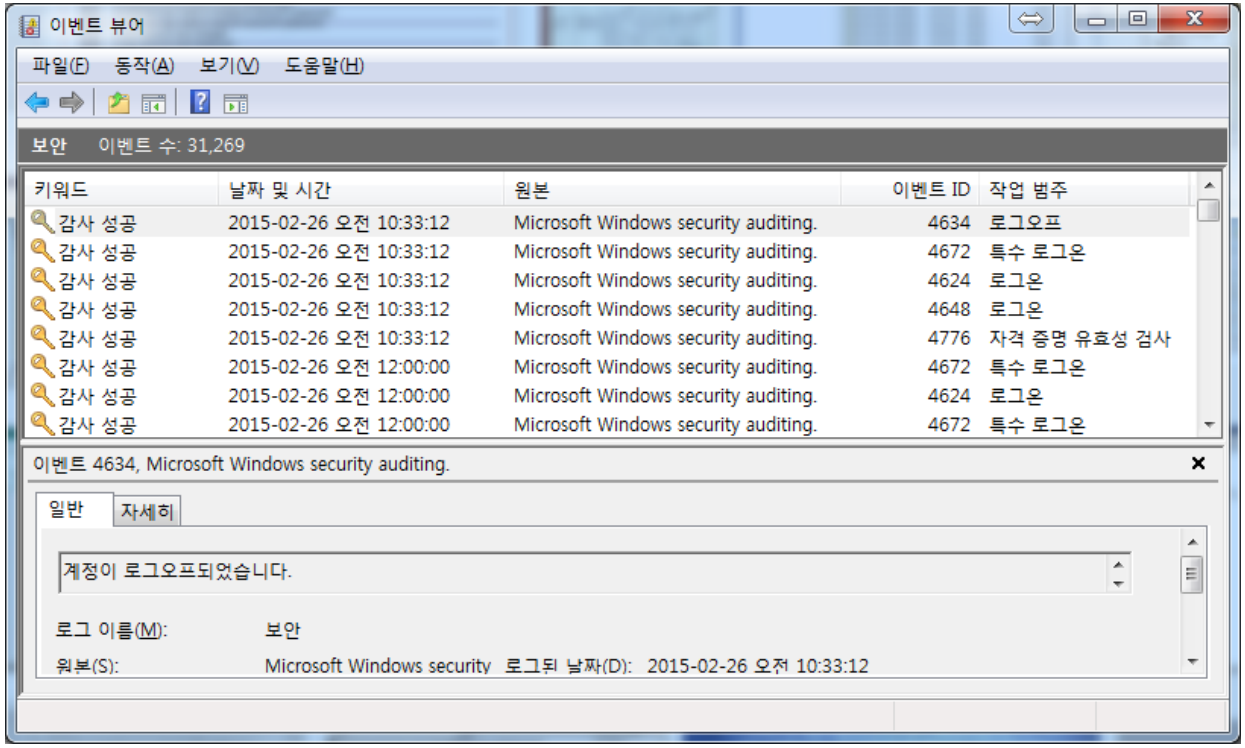
- **평시** ➔ 정기/상시 감사, 위협 요인에 대한 다양한 정보 수집 및 샘플 테스트
- **전시** ➔ 사고의 원인과 과정을 분석하여 보안성 강화

5. 관리 정책을 강화하자!!

- 타겟형 공격의 많은 부분은 관리적 문제의 허점
- 이미 갖추고 있는 정책이라도 익숙해지면 취약해지기 마련
- 조직의 보안 문제를 수준별로 분류하고 그에 따른 관리정책 마련
- 마련된 정책은 지속적으로 모니터링하여 준수 여부를 감독!!!

6. 로그 설정을 강화하자!!

- 포렌식 아티팩트 중 사실 증명이 가장 정확한 흔적
- 이미 갖추고 있는 장비 및 솔루션의 로그 설정 강화
- 목적에 맞는 클라이언트 로그 설정 강화



7. 형상 관리를 하자!!

- 포맷은 답이 아니다!
- 목적/위험도에 따라 보존 절차 마련 ➔ 추후 원인 파악, 법률적 대응에 활용
- 저장장치 보관이 가능하다면 최소 3개월 이상 보관
- 용량이 부담된다면 압축하여 용량 최소화
- 사건 유형에 따라 조사에 필요한 데이터만 보관

8. 침해사고 지표를 관리하자!!

- 침해사고를 식별할 수 있는 포렌식 아티팩트 ➔ 침해 유입, 실행, 지속 아티팩트
- 대부분 타겟형 공격은 대상 조직의 유형에 따라 유사한 패턴을 보임
- 안티 포렌식 기법으로 인해 파일 기반의 지표 활용도 감소
- 분석 인력을 통해 지속적인 지표 업데이트

```
OR
    File Section Name contains .stub
    File Name contains mdmcpq3.PNF
    File Name contains mdmeric3.PNF
    File Name contains oem6C.PNF
    File Name contains oem7A.PNF
    AND
        DriverItem/DeviceItem/AttachedToDriverName contains fs_rec.sys
        DriverItem/DeviceItem/AttachedToDriverName contains mrxsmb.sys
        DriverItem/DeviceItem/AttachedToDriverName contains sr.sys
        DriverItem/DeviceItem/AttachedToDriverName contains fastfat.sys
    AND
        File Name contains mrxcls.sys
        File CertificateSubject contains Realtek Semiconductor Corp
    AND
        File Name contains mrxnet.sys
        File CertificateSubject contains Realtek Semiconductor Corp
    AND
        Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\ImagePath
        Registry Text contains mrxcls.sys
    AND
        Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
        Registry Text contains mrxnet.sys
```

9. 가상 시뮬레이션 훈련을 시행하자!!

- 국내에서 정보보호가 가장 잘 이루어지고 있는 조직은…?
- 사고 대응력은 경험적 능력에 좌우!! ➔ 실제 사고를 당해봐야 하는가?
- 실제와 유사한 반복적인 모의 훈련 ➔ 침해사고 영향을 직원들에게 내재화

"보안은 사람이 문제다"

"보안은 사람이 답이다"

질문 및 답변