

# 침해 지표를 활용한 침해사고 프로파일링

---

플레인비트 대표

김진국



*[jinkook.kim@plainbit.co.kr](mailto:jinkook.kim@plainbit.co.kr)*











# 발표자 소개

- 김진국 (JK Kim)
- <http://forensic-proof.com>
- <http://facebook.com/proneer>
- 2013.08 – 현재 : (주) 플레인비트 대표
- 2014.04 – 현재 : 한국디지털포렌식학회 교육사업이사
- 2013.08 – 현재 : KITRI BOB 디지털 포렌식 멘토
- 2012.12 – 현재 : 미래창조부 민.관합동조사단 전문가
- 2012.08 – 현재 : 에이콘 출판사 디지털 포렌식 시리즈 에디터
- 2011.11 – 현재 : 포렌식 인사이트(F-INSIGHT) 운영
- 국방부, 법무연수원, 경찰수사연수원, 삼성전자, 삼성SDS, 대한변호사협회 등 다수의 강의 경력
- 코드게이트, 코드엔진, KISA, 삼성SDS, NETSEC-KR 등 다수의 컨퍼런스 발표 및 특강



## 침해 지표(IOC, Indicators Of Compromised)란?

호스트나 네트워크 상에서 침해 혹은 감염을 식별할 수 있는 **포렌식 아티팩트**

| Full Path   |   | Size in Bytes | MD5                              | Owner                  | Created              | Access               | Modified             |
|---|---|---------------|----------------------------------|------------------------|----------------------|----------------------|----------------------|
| C:\Documents and Settings\dfirm00b\Local Settings\Application Data\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}   |    | 0             |                                  | HACKME\dfirm00b        | 2008-04-14 12:00:00Z | 2012-07-06 06:06:29Z | 2008-04-14 12:00:00Z |
| C:\Documents and Settings\dfirm00b\Local Settings\Application Data\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\@ |    | 2048          | 56cd91ad955622a02915252084e09a92 | HACKME\dfirm00b        | 2008-04-14 12:00:00Z | 2012-07-06 09:37:42Z | 2012-07-06 09:37:42Z |
| C:\Documents and Settings\dfirm00b\Local Settings\Application Data\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\L |    | 0             |                                  | HACKME\dfirm00b        | 2008-04-14 12:00:00Z | 2012-07-05 17:30:44Z | 2008-04-14 12:00:00Z |
| C:\Documents and Settings\dfirm00b\Local Settings\Application Data\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\U |    | 0             |                                  | HACKME\dfirm00b        | 2008-04-14 12:00:00Z | 2012-07-05 17:30:44Z | 2008-04-14 12:00:00Z |
| C:\Documents and Settings\dfirm00b\Local Settings\Application Data\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\n |    | 57344         | 190b4b37328d9c6645b40efae6ae945f | HACKME\dfirm00b        | 2008-04-14 12:00:00Z | 2012-07-06 06:06:40Z | 2008-04-14 12:00:00Z |
| C:\WINDOWS\Installer\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}   |    | 0             |                                  | BUILTIN\Administrators | 2008-04-14 12:00:00Z | 2012-07-06 10:01:52Z | 2008-04-14 12:00:00Z |
| C:\WINDOWS\Installer\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\@   |    | 2048          | cdda1a53ecb3a66c1f325e7e9ec97b03 | BUILTIN\Administrators | 2008-04-14 12:00:00Z | 2012-07-06 10:02:42Z | 2008-04-14 12:00:00Z |
| C:\WINDOWS\Installer\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\L   |   | 0             |                                  | BUILTIN\Administrators | 2008-04-14 12:00:00Z | 2012-07-06 02:00:53Z | 2012-07-04 22:44:06Z |
| C:\WINDOWS\Installer\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\U   |  | 0             |                                  | BUILTIN\Administrators | 2008-04-14 12:00:00Z | 2012-07-06 10:01:52Z | 2012-07-04 22:44:10Z |
| C:\WINDOWS\Installer\{235c1d10-b0b5-289f-6f20-91dd1f9a6306}\n   |  | 57344         | 190b4b37328d9c6645b40efae6ae945f | BUILTIN\Administrators | 2008-04-14 12:00:00Z | 2012-07-06 04:33:52Z | 2008-04-14 12:00:00Z |

<https://dfirjournal.wordpress.com/tag/malware/>

## 침해사고 대응 vs. 침해사고 포렌식

### ■ 침해사고 대응 (IR, Incident Response)

- 침해 지표를 이용해 침해 시도를 탐지하거나 차단 (다양한 보안 장비/솔루션, CERT, 관제, ...)
- 침해 지표를 이용해 감염 시스템 식별 후, 식별 원인 및 공격 기제 제거 (치료, 포맷, ...)
- 문제점은?

### ■ 침해사고 포렌식 (IR Forensics)

- 포렌식 침해 지표를 이용해 사고의 원인과 과정을 밝혀냄 ➔ 사고 원인 제거 및 보완
- 포렌식 침해 지표를 관리하여 공격 행위의 사전 탐지 후 대책, 공격 집단 추론

## 전통적 침해 지표와 한계

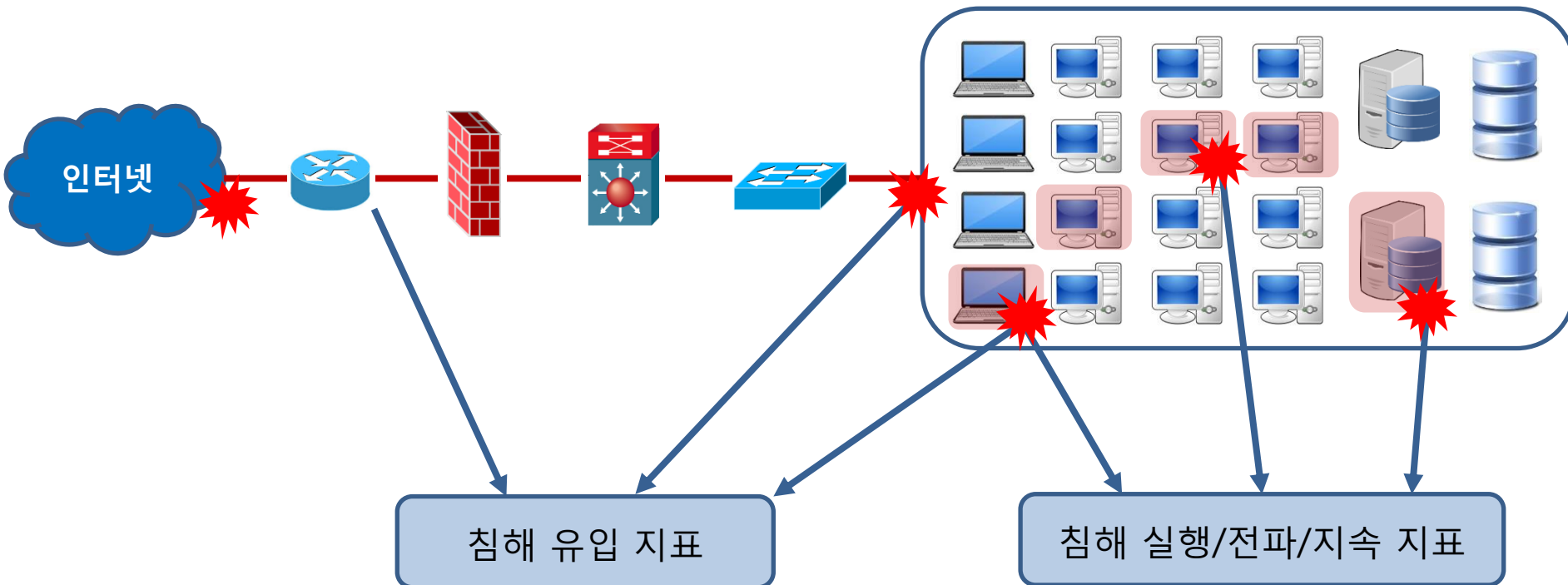
### ■ 전통적 침해 지표

- IP/DOMAIN 주소
- 악성코드 체크섬/해쉬 값 (CRC, MD5, SHA1, SHA256, ...)
- 악성코드 정적/동적 정보 등

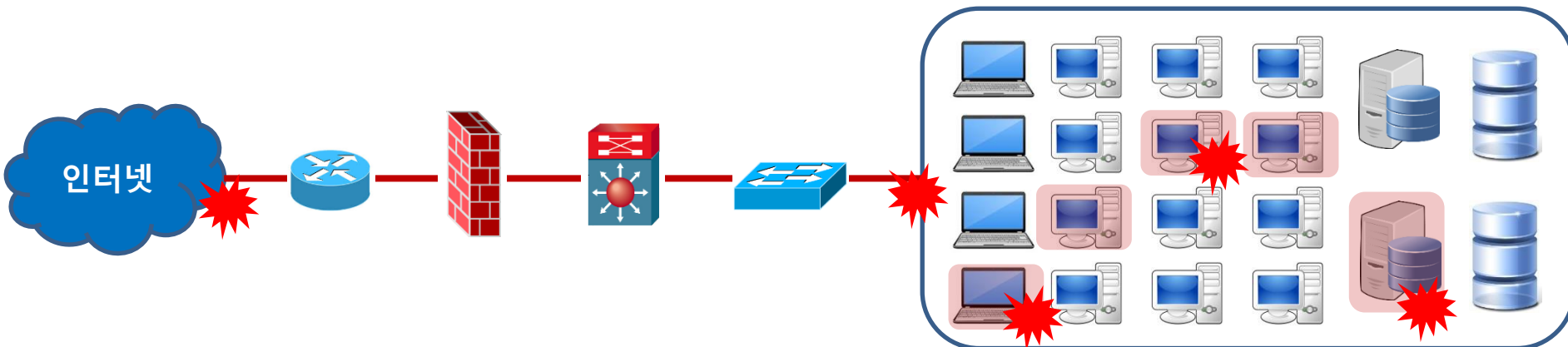
### ■ 기존 지표의 한계

- 패스트 플럭스(Fast-Flux), 도메인 쉐도잉(Domain Shadowing)
- FILELESS 악성코드, 자가삭제 형 악성코드
- 사전 조사를 통한 방어 솔루션/장비 우회

## 포렌식 침해 지표



## 포렌식 침해 지표



### 침해 유입 지표

웹을 통한 유입  
이메일을 통한 유입  
저장매체를 통한 유입  
서비스를 통한 유입

### 침해 실행 지표

실행 파일 실행 흔적  
문서 파일 실행 흔적  
라이브러리 사용 흔적  
비정상 파일명 사용 흔적  
추가 악성코드 다운로드

### 침해 전파 지표

스니핑 흔적  
스푸핑 흔적  
이메일 전파 흔적  
인증 취약점 사용 흔적  
비정상 인증 내역  
원격 접속 흔적

### 침해 지속 지표

자동 실행 흔적  
비정상 폴더 사용 흔적  
은닉 흔적  
삭제 흔적  
루트킷 흔적

## 타임라인 분석

## 포렌식 침해 지표 샘플

http://torrentrg.net/bbs/board.php?bo\_table=torrent\_req&wr\_id=48882

%UserProfile%\Downloads\[tvN]\_....E298.130715.HDTV.XviD-WITH.avi.torrent.exe:Zone.Identifier

%UserProfile%\Downloads\[tvN]\_....E298.130715.HDTV.XviD-WITH.avi.torrent.exe

WinEVTX [7036 / 0x1b7c] Record Number: 2694 Event Level: 4 Source Name:  
Service Control Manager Computer Name: XXXXX Strings: ['Application Experience', '실행',...]

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\\*

HKLM\SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache

HKU\Software\WinRAR SFX

\Program Files\Tiara.torrent

\Program Files\server.exe

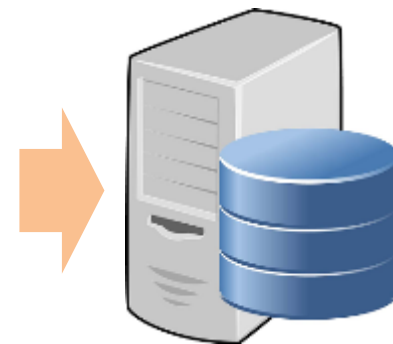
\Windows\D6C0EC4D\svchost.exe

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

\Windows\Tasks\\*

\Windows\System32\Tasks\\*

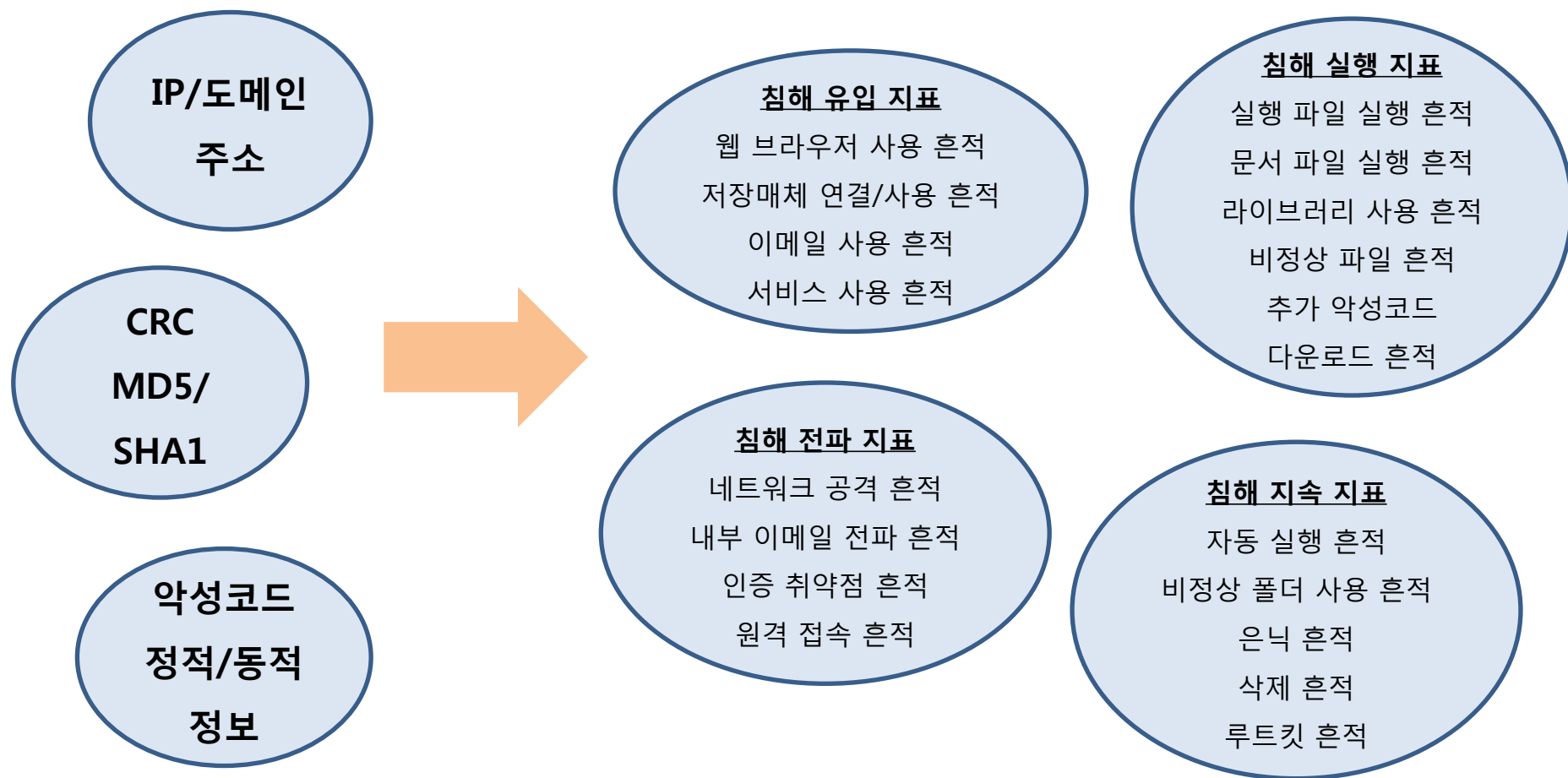
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\\*





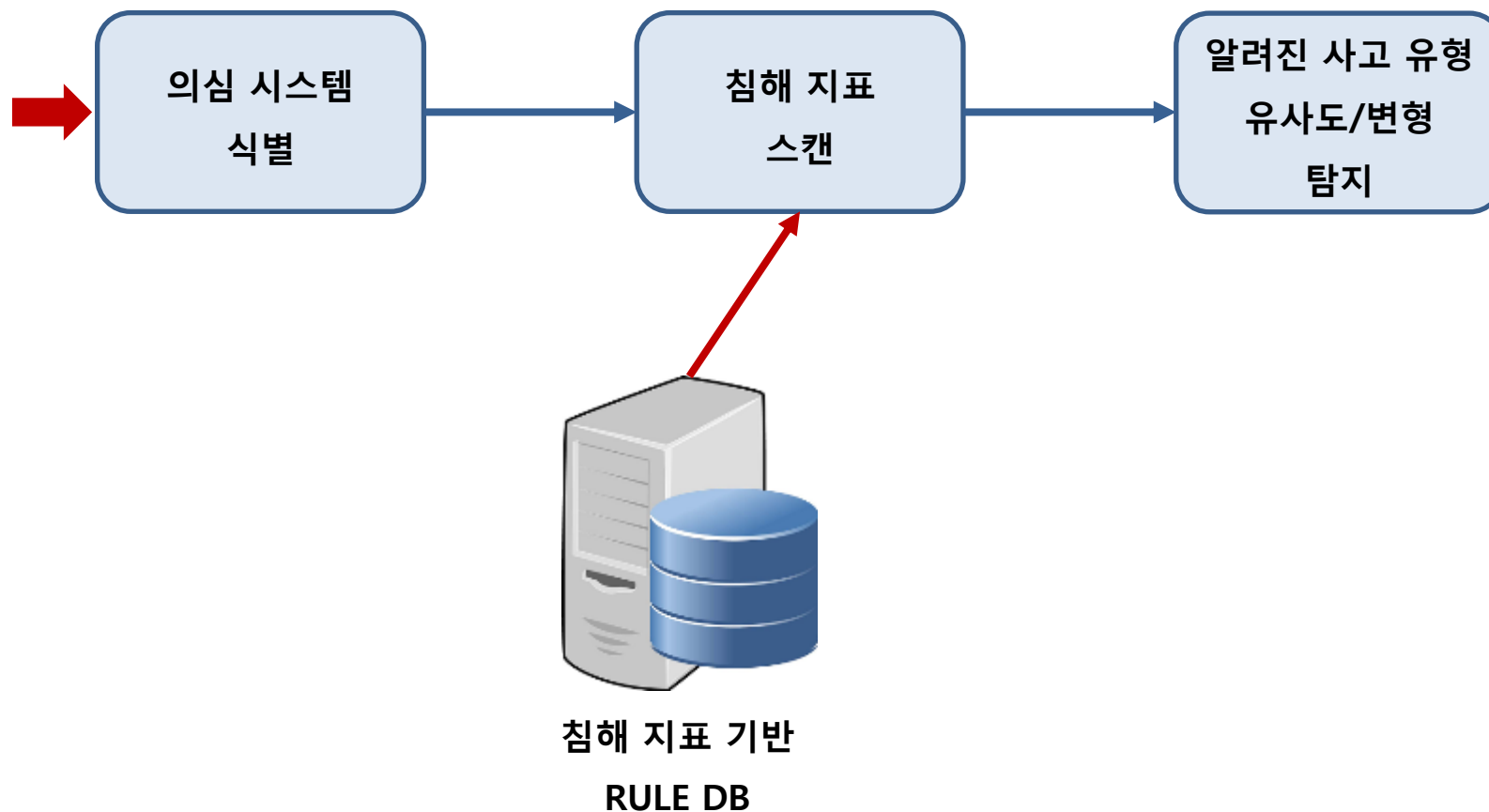
## 침해 지표 관리의 이점 #1

- 전통적 침해 지표를 우회하는 공격에 대한 사전 식별 가능성 ↑



## 침해 지표 관리의 이점 #2

- 침해 지표를 이용해 침해사고 사전 탐지율 ↑



## 침해 지표 관리의 이점 #2 – CASE

- 공격도 유행을 탄다...?

D-Day

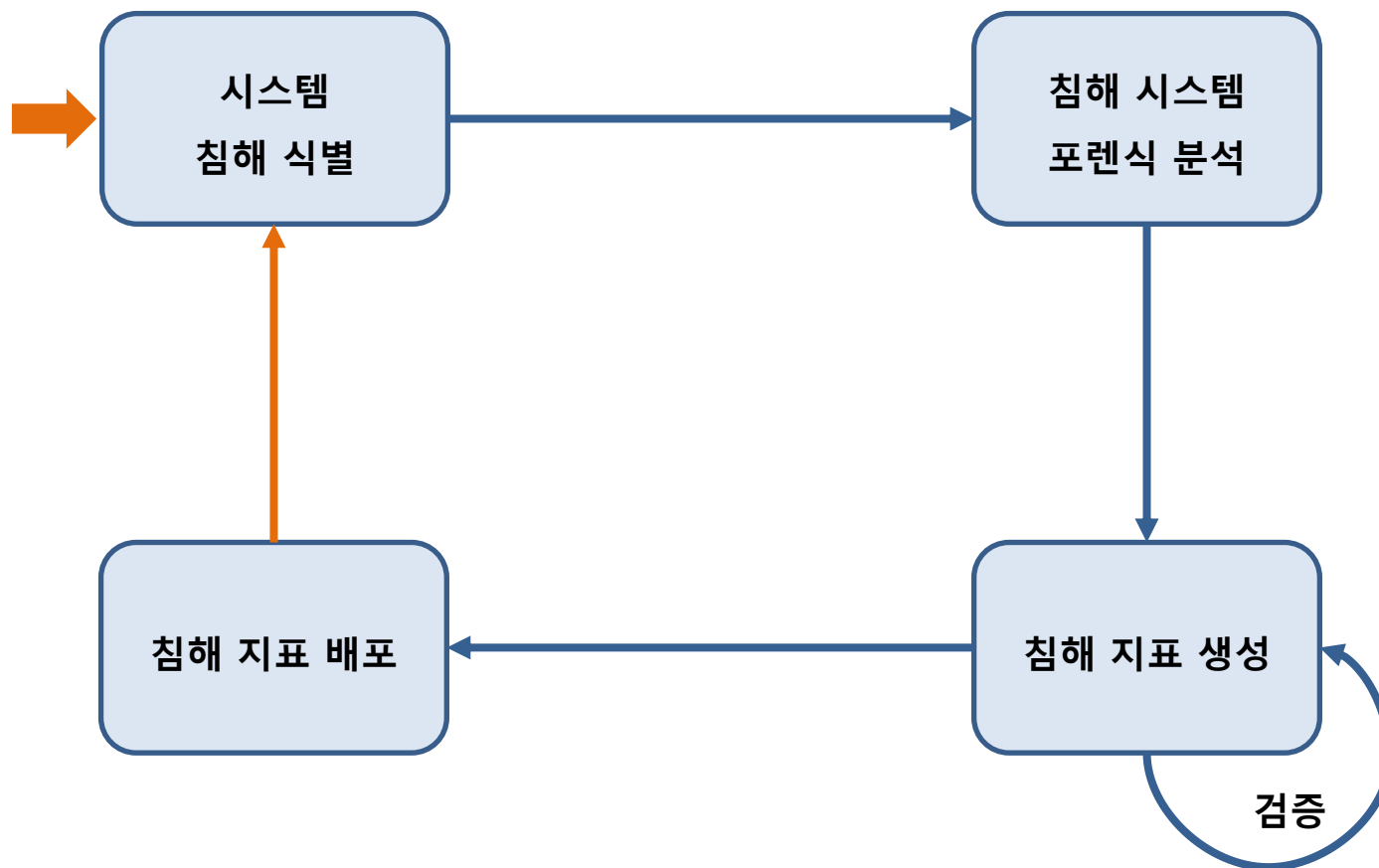
+ 6 Month

+ 13 Month

- 유입 방식
- 전파 방식
- 은닉 방식
- 악성코드 실행 흔적
- 악성코드 정적 내용

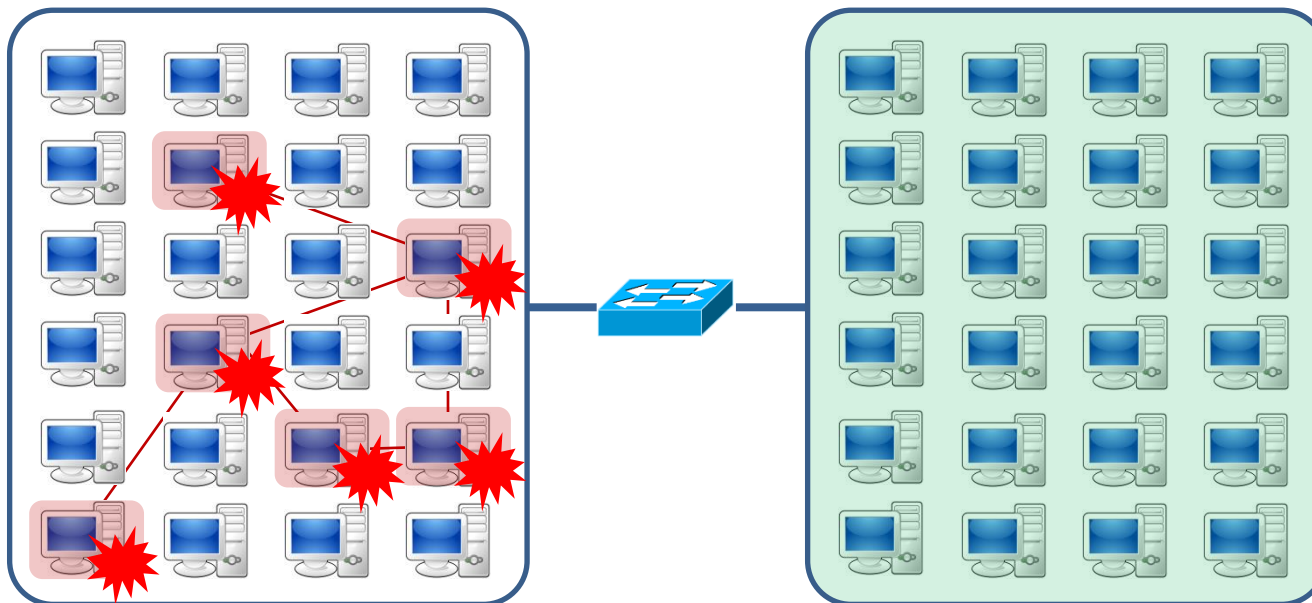
## 침해 지표 관리의 이점 #3

- 추가 감염 시스템 식별 (자가삭제 형, FILELESS 악성코드 식별 가능)



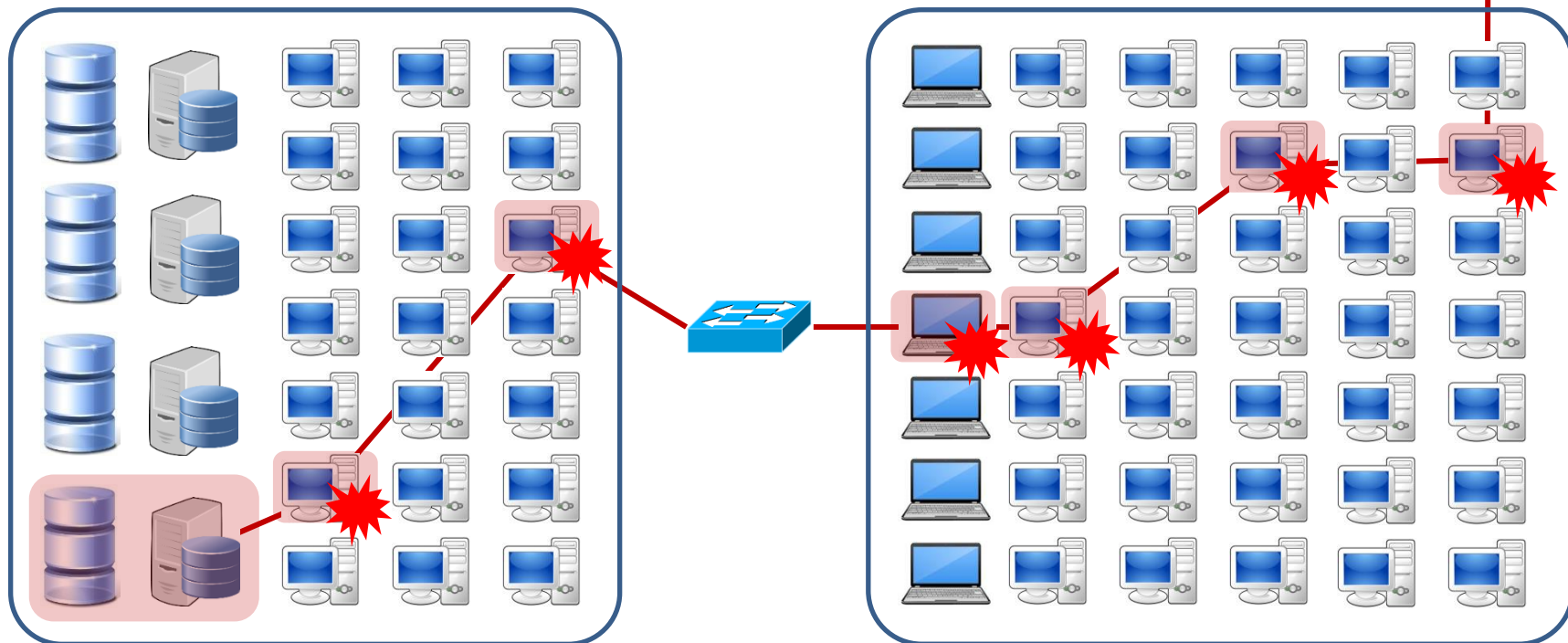
## 침해 지표 관리의 이점 #3 - CASE

- 추가 감염 시스템 식별 - 불확실성 → 확실성!!



## 침해 지표 관리의 이점 #4

- 사고의 원인과 과정을 밝혀 문제점 해결 (포렌식 분석의 이점)



- 일상적 문제 vs. 타겟형 공격의 과정

## 침해 지표 관리의 이점 #5

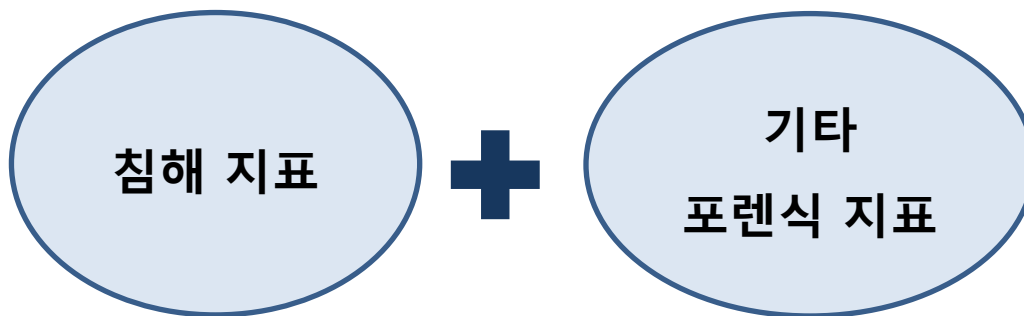
- 기업에 위협이 되는 공격 조직에 대한 시야 제공



## 침해 지표의 확장!

### ■ 호스트 포렌식 침해 지표 ➔ 호스트 인텔리전스 정보

- 정보유출사고 탐지
- ICT 컴플라이언스 준수
- 퇴사자 예측
- 기타 정보 감사





## 어려움 점 #1

- **안티포렌식과의 전쟁**
  - 흔적 삭제는 다행
  - 흔적 조작 → 분석가의 잘못된 판단 유도
  
- **실제 공격 vs. 가장 공격**

## 어려운 점 #2

### ▪ 기본 호스트 정보의 부족 → 침해사고 준비도 마련

- 운영체제 업그레이드
- 파일시스템 로그 강화
- 이벤트 로그 설정 강화 (감사 정책 구성)
- 프리패치 설정 강화
- 로컬 보안 정책 설정
- ... ..

## 어려운 점 #3

- **부적절한 침해사고 대응 절차**
  - 식별 노력이 부족
  - 초기 대응 절차의 부재
  - 신속성의 부족

## 인텔리전스 정보의 결합!!

- 판단 오류 ↓ + 사전 예측력 ↑ + 사후 대응력 ↑ + 폭넓은 시야



