TREND MICRO

Security
TRENDS 2018

SK infosec

Security TRENDS 2018

SK infosec
EQST Group 이재우

MSS를 위한 Threat Intelligence Data 대응력 강화

(Make your threat intelligence data more responsible for MSS)

EQST 소개

- **R&D**
  - Asset DT화
  - 취약점자동화
  - 모의해킹자동화

- **취약점 연구**
  - 신규/기존 취약점 연구
  - 사고 사례 분석
  - 공격방어 Tool 제작

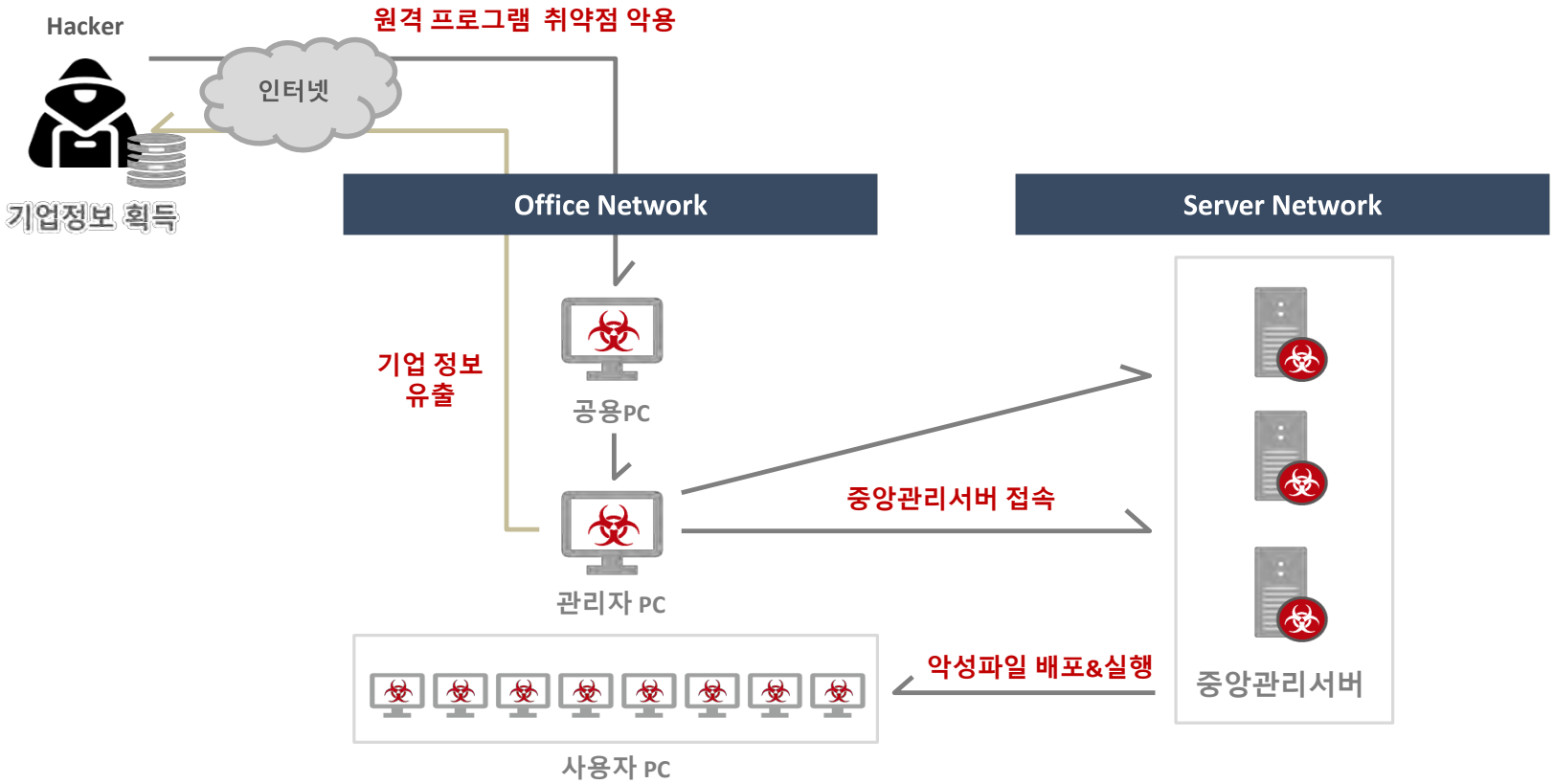
- **Incident Response**
  - 초기 침투 원인 분석
  - 공격자 경로 추적
  - 사고 원인 및 대책 수립

- **모의해킹**
  - Penetration TEST
  - Web/Mobile
  - Reversing
  - Red Teaming

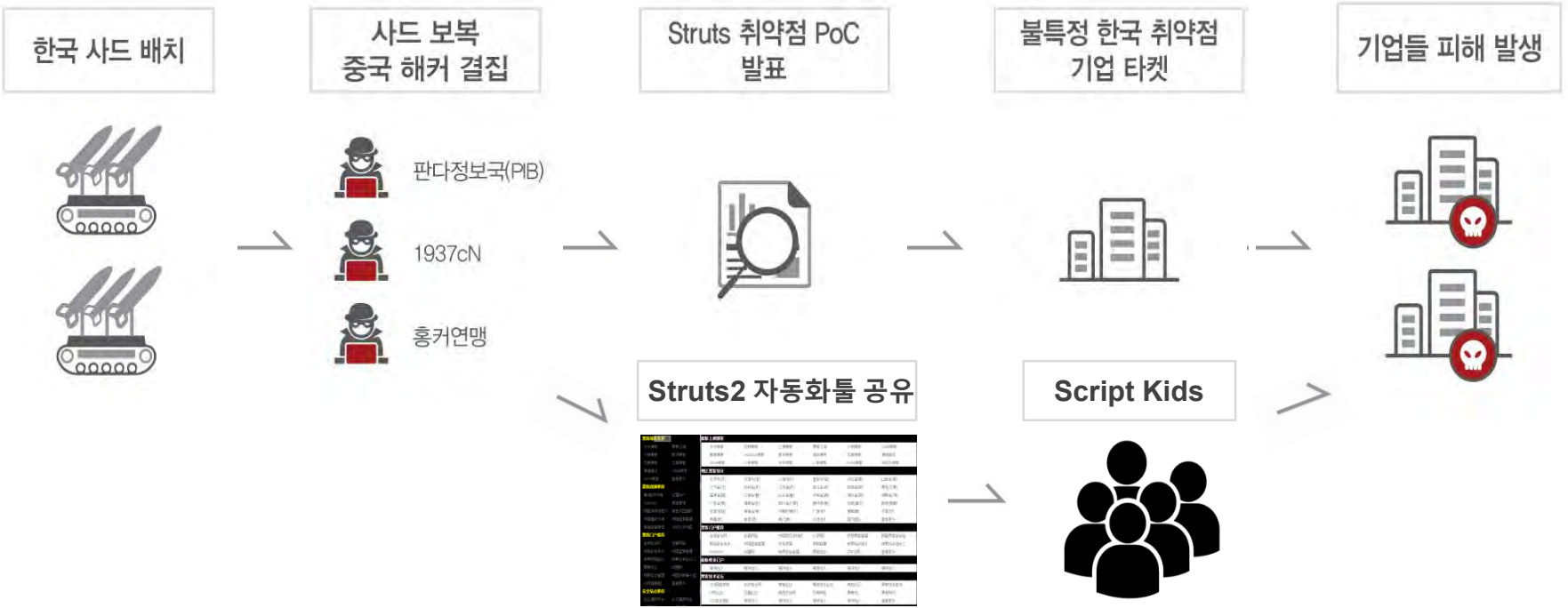
- **Threat Intelligence**
  - Attack Group Trace
  - Threat Data Collect/Analysis
  - Threat Data 연구

- **취약점진단**
  - Vulnerability Assessment
  - SourceCode Analysis
  - IoT/Cloud

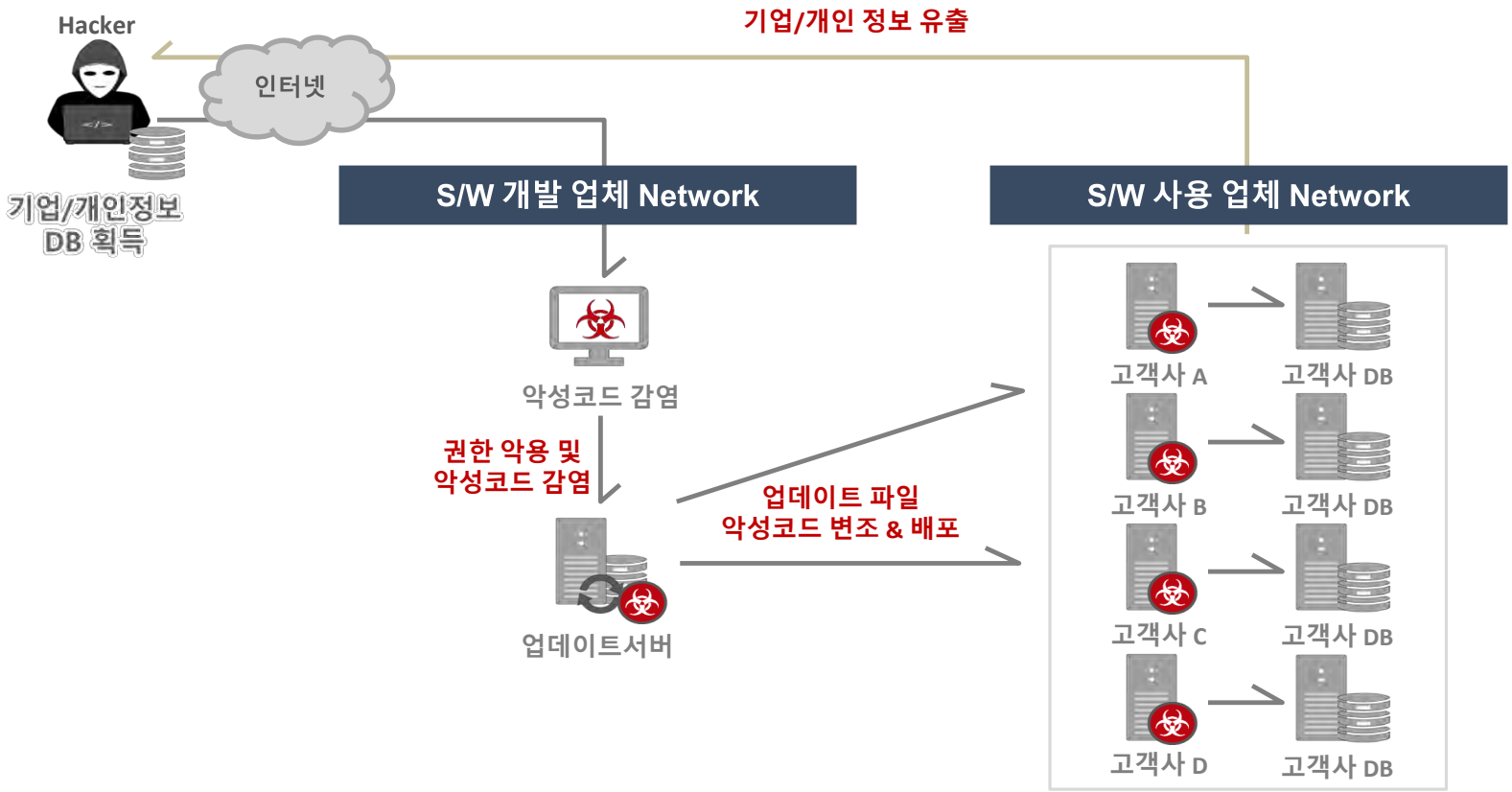
공격 사례 - 관리서버


Hacker
원격 프로그램 취약점 악용
인터넷
기업정보 획득
Office Network
Server Network
기업 정보 유출
공용PC
관리자 PC
중앙관리서버 접속
악성파일 배포&실행
중앙관리서버
사용자 PC

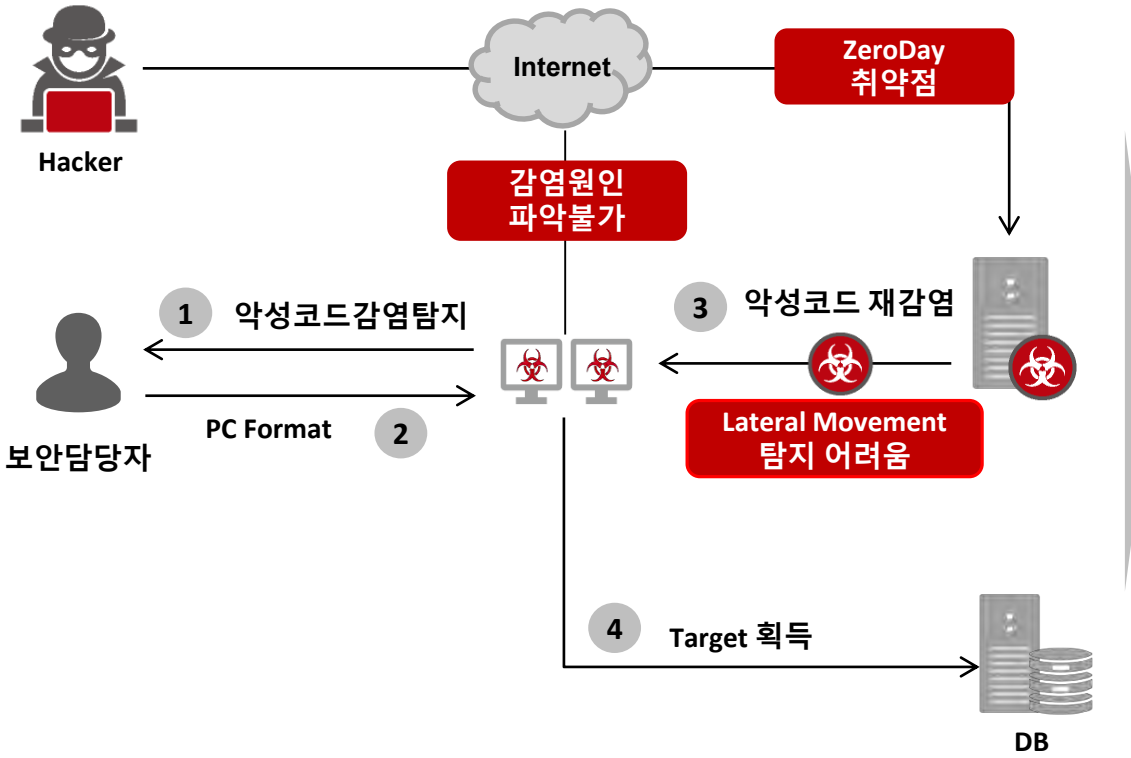
공격 사례 – Zero Day



최근 공격 사례 – S/W공급망



해킹 대응 한계점



【한계점】

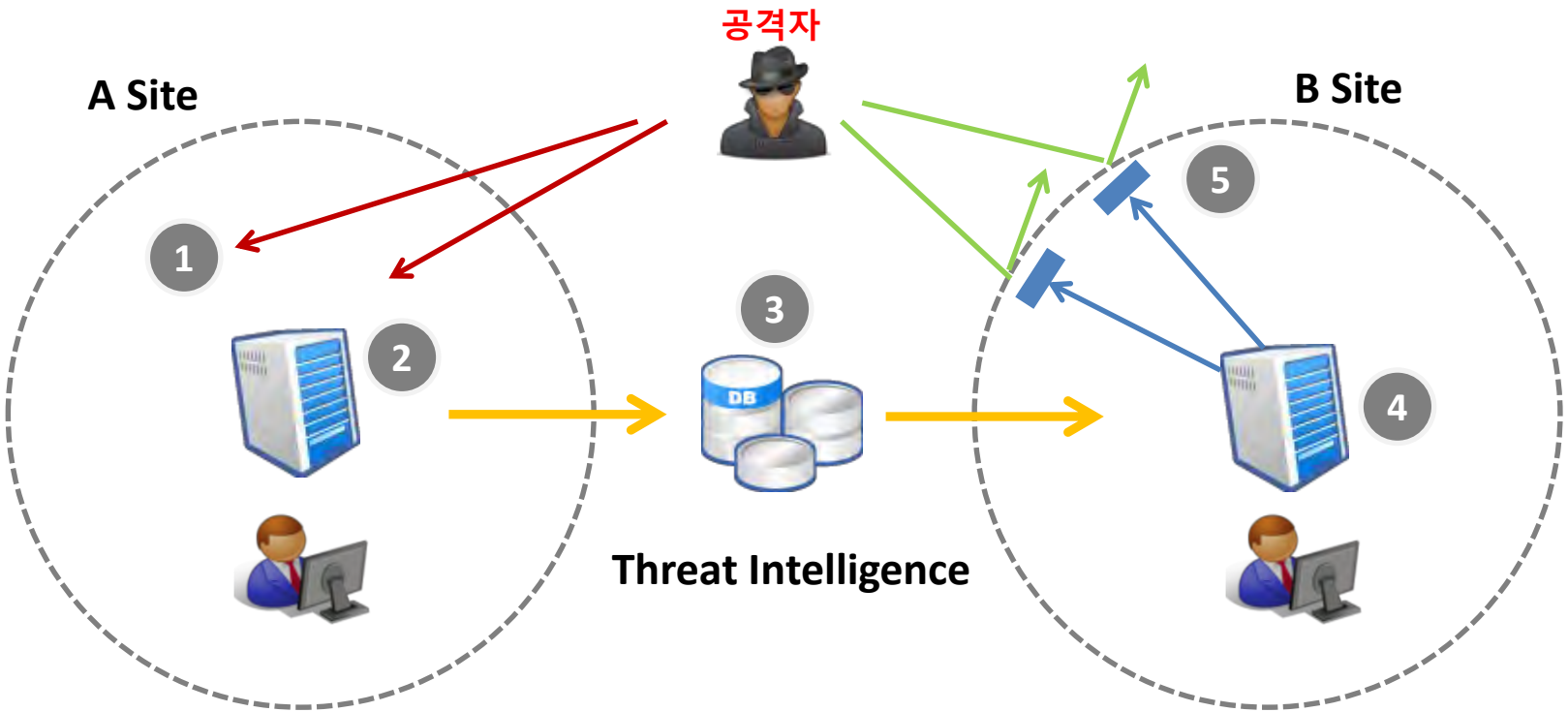
1. 악성코드 감염 원인 파악 어려움
2. 분석 및 대응 장시간 소요
3. Movement 확인 어려움

What Need?

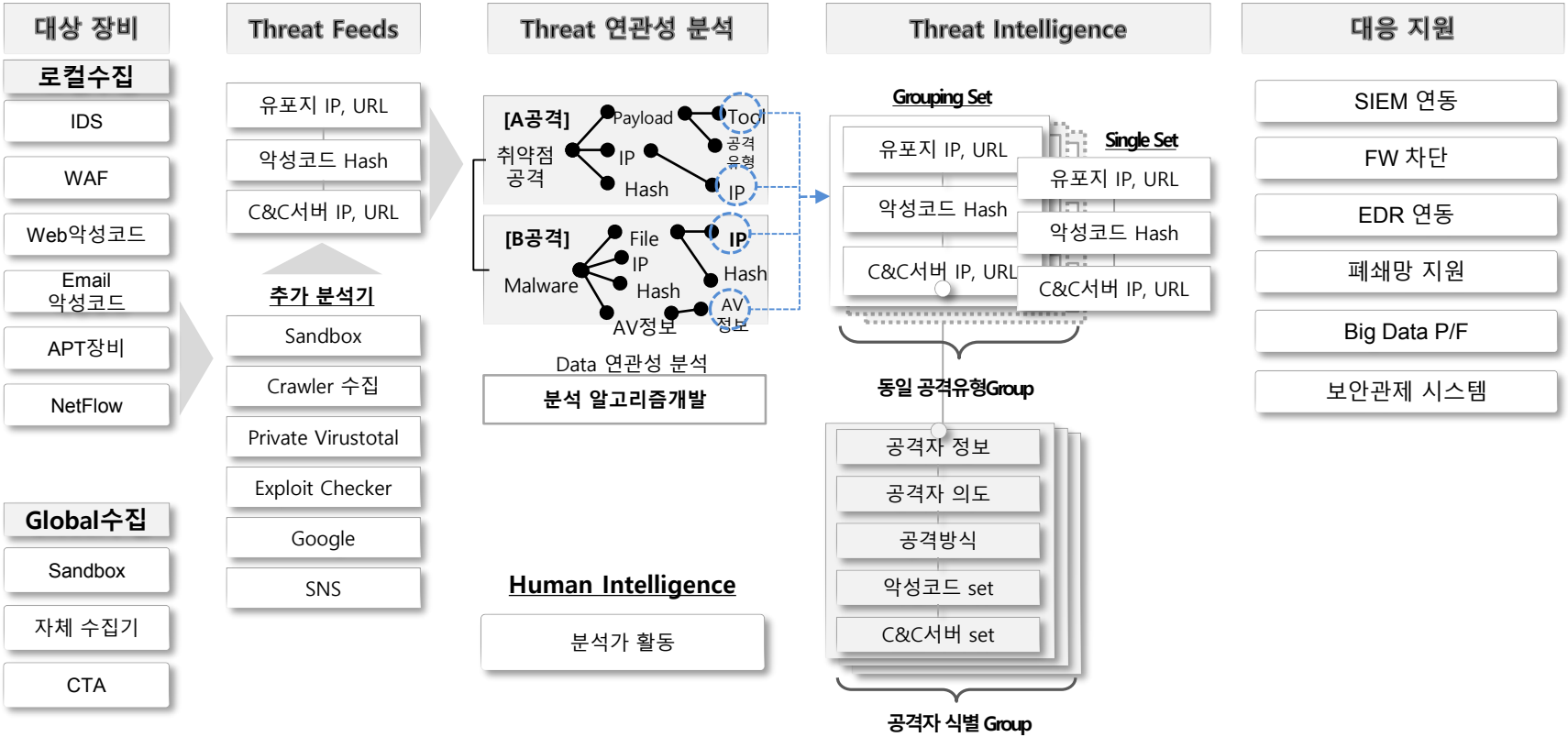
- ✓ 매우 빠르고, 알려지지 않은 해킹 경로 및 공격 Tool 사용
- ✓ 초기 감염에 대한 원인 파악 매우 어렵고 대응 장시간 소요
- ✓ Single Layer Data만으로는 탐지 및 대응에 한계성 존재

"Intelligence Data에 대한 확장 및 실시간 대응 중요성"

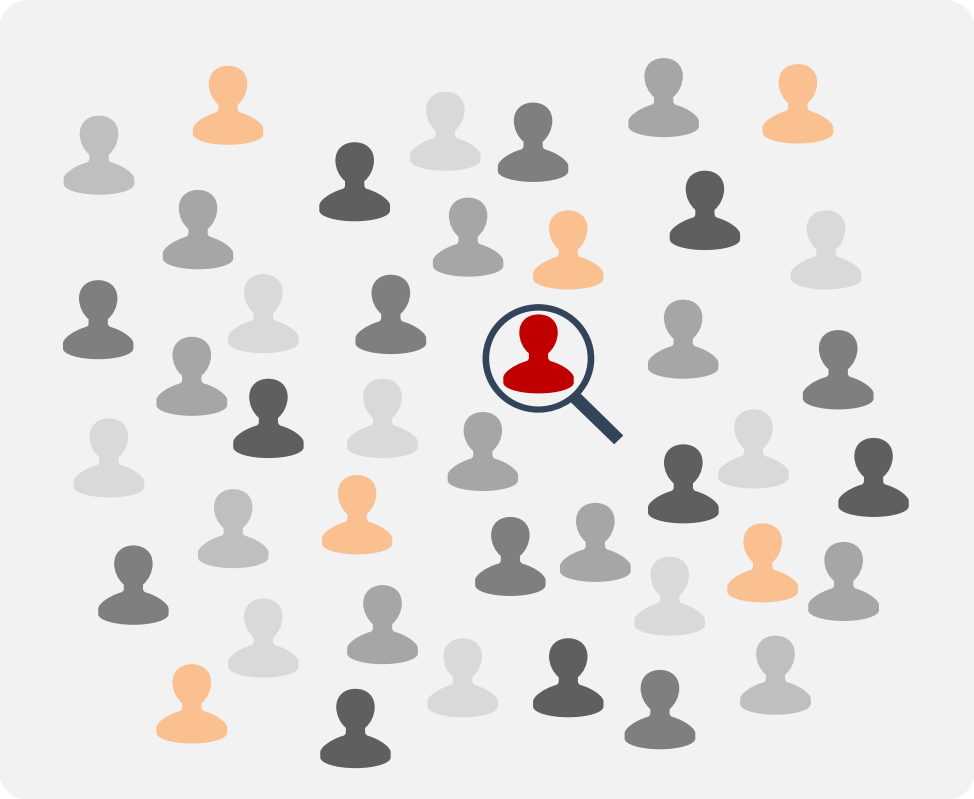
Intelligence 개요



Intelligence 구조



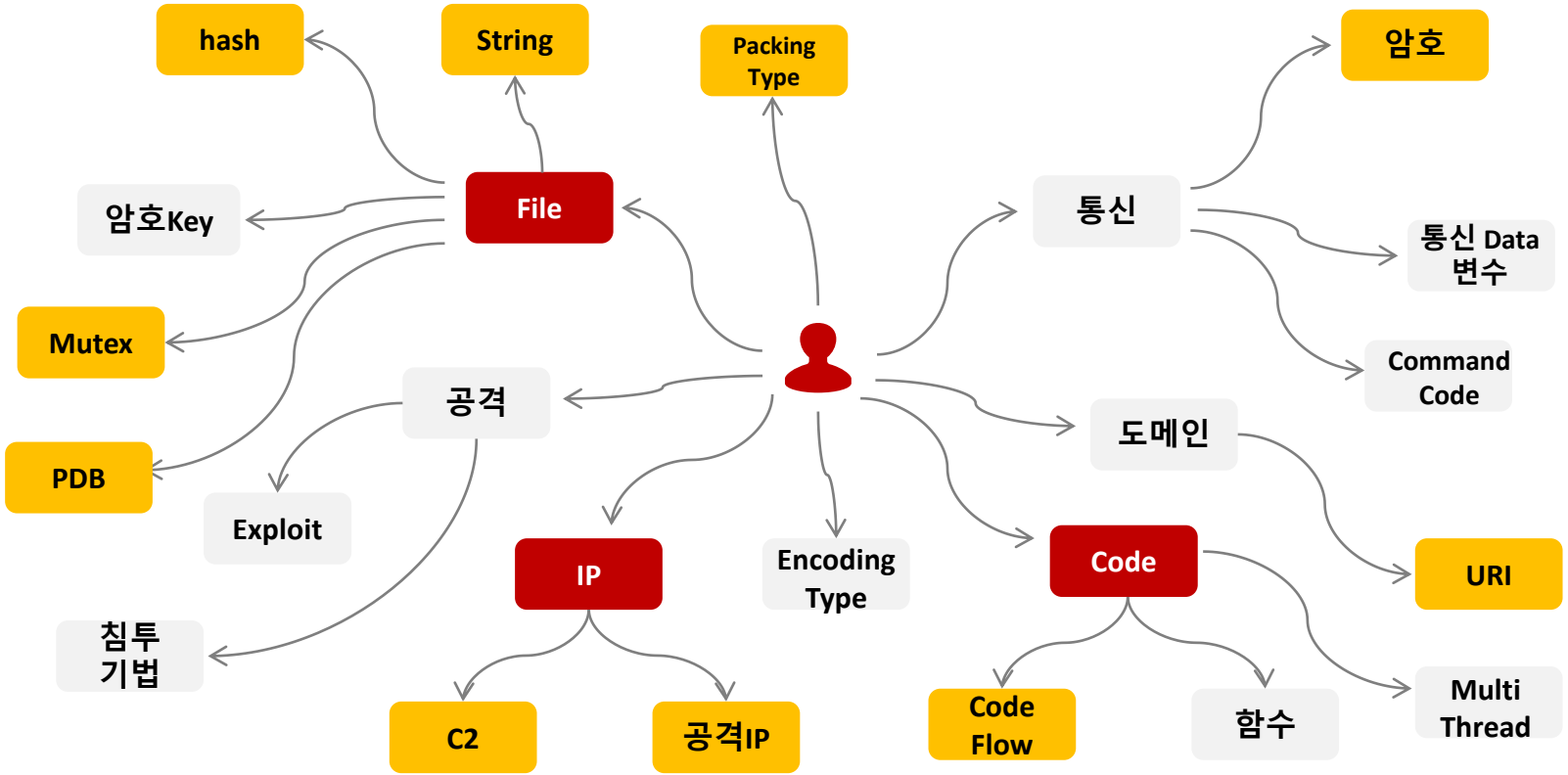
Profiling?



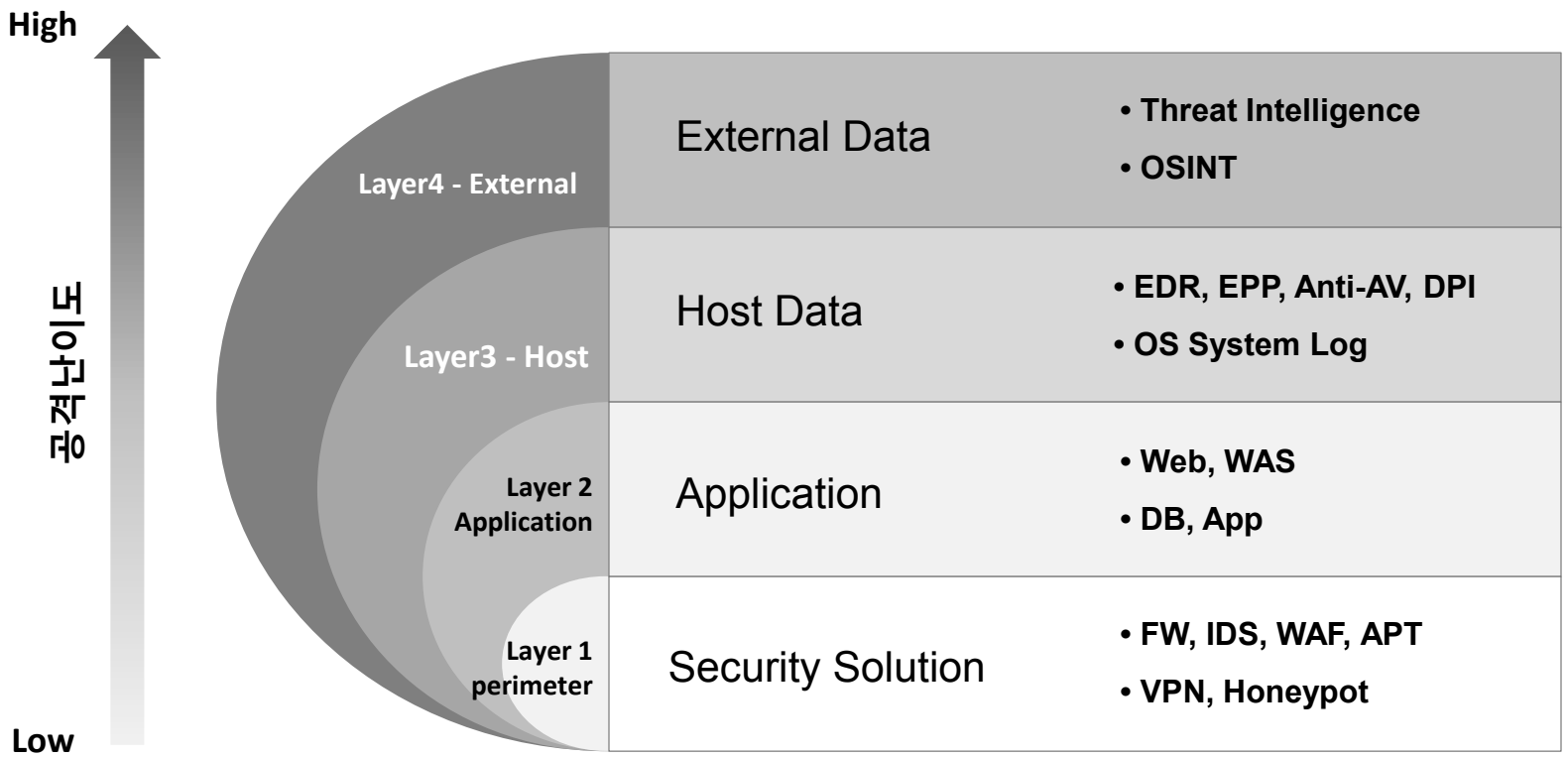
【Profiling 목적】

1. 주요 공격자 Group 기반 해킹 목적 및 Target 식별
2. 공격자 IoC Relation 확인을 통한 신속한 판단
3. 공격자 별 대응 Level에 대한 판단 기준

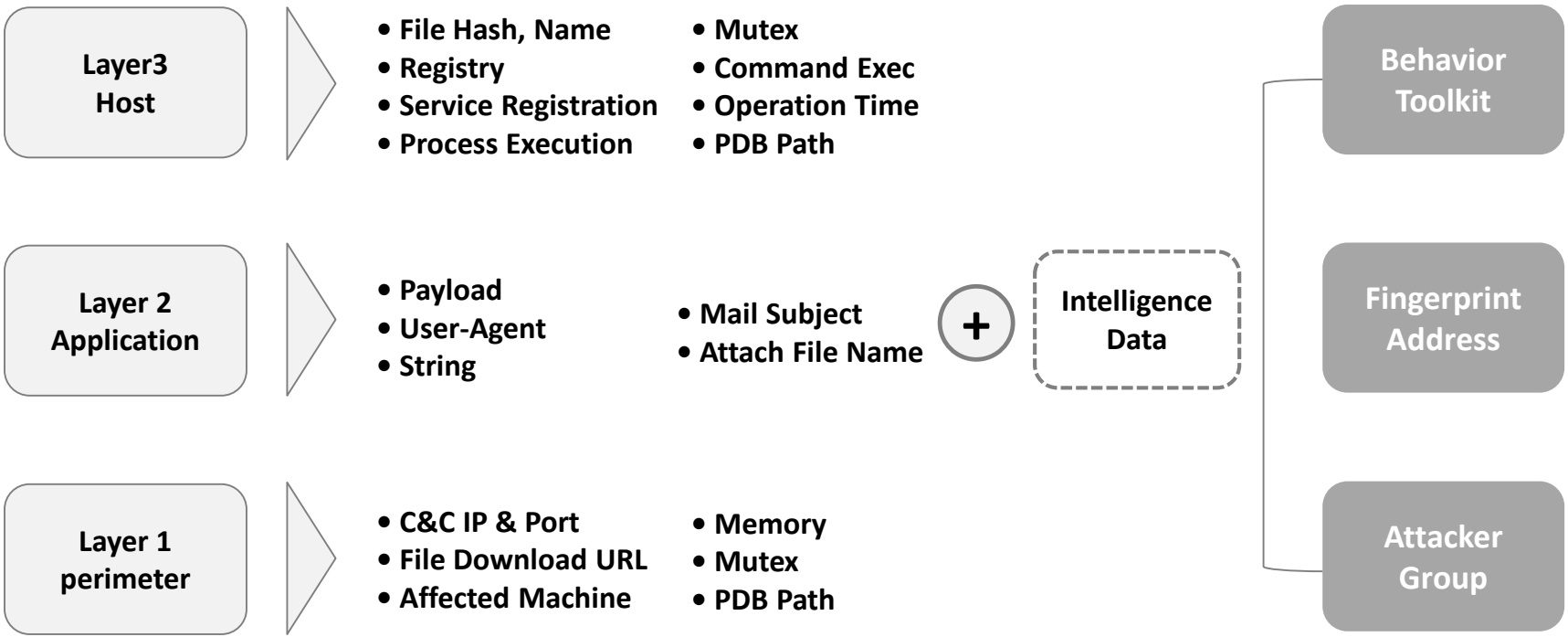
Profiling Data



Profiling 대상 로그



From Logs to Responsibility



Sample Case

FW Log

Apr 1 15:00:12 KGFW1 1,2018/04/01 15:00:11,013201001781,TRAFFIC,end,0,2018/04/01 15:00:11,211.218.76.85,165.141.246.183,0.0.0.0,0…..

Time	Src IP	Src Port	Src Geo	DstIP
DstPort	DataSize	Action	Protocol	

IPS Log

"logDttm": "20180401T175939+0900", "srcIp": "126.XX.XX.XX", "count": 1, "category2": "SQL_Injection", "rawData": "SNMP=Default:0| :URL……

Time	Src IP	Src Port	Src Geo	DstIP
DstPort	DataSize	Action	Protocol	
RawData	Domain	URI	UserAgent	

FW Log + Threat Intelligence Data

AttackType_Description: "공격자가 무차별 대입 공격을 통해 ID/PW 및 시스템 권한 획득"
SrcIP_AttackType_History: "SSH Brute-Force", "RDP Brute-Force", "Include Injection"
SrcIP_Hacking_Tool: ”Brute-Force tool ”
Persistence Connection: “Y”

FW Log	**AttackType_Description**	**SrcIP_AttackType_History**
SrcIP_Hacking_Tool	**Persistence Connection**	

IPS Log + Threat Intelligence Data

AttackType: "SQL_Injection"
AttackType_Description: "공격자가 조작된 SQL Query을 삽입해 웹서버 DB 정보 유출”
SrcIP_AttackType_History: "SQL Injection", "RDP Brute-Force", "Include Injection"
SrcIP_Hacking_Tool: "BSQL"
Raw_Match: "AND 1=1 UNION ALL SELECT 1?NULL","information_schema.tables", "xp_cmdshel“
Persistence Connection: “Y”
Hacking_group_History:”Dragonfly”

기존 IDPS 로그	**AttackType_Description**	**SrcIP_Hacking_Tool**
AttackType	**SrcIP_AttackType_History**	**Persistence Connection**
Hacking_group_History	**Raw_Match**	

Sample Case

APT Log

"deviceModel": “-”, "eventNm": "Http File Transfer", "category2": "Execution", "rawData": "http://96elba4acdwd32x2.fryrids.com/10232", "signature": "infection-match“……

Time	Src IP	Src Port	Src Geo	DstIP
DstPort	DataSize		Action	Protocol
RawData	Domain	URI	FileHash	

EDR Log

Apr 1 15:48:10 EDR1 124.66.XX.XX 12312e123125seawd23e1e12e9171 54322 WIN-4fwefkwkdkkwd 66a64044c27b4dc3ff567f652d4c12e060 c:\Windwos\system32\flash.swf 234.exe File Detection PID:684 High

Time	AgentIP	FileHash	FilePath
Processname	EventName	PID	Severity

APT Log + Threat Intelligence Data

AttackType: "Malicious File Download"
AttackType_Description: “악의적 URL로의 접근을 통해 악성 파일 다운로드 시도를 탐지함“
Domain_History: "악성코드 배포이력 27건 존재“
Filehash_Reputaion:“Rootkit“
File_Pdb_Path:”c:\malware\hack.pdb”
Persistence Connection: “Y”
Mutex:”sdkfhksdlhjf”
Hacking_Group:”Group123”

기존 APT 로그	AttackType	AttackType_Description
Domain_History	Filehash_Reputation	Persistence Connection
File_Pdb_Path	Mutex	Hacking_Group

EDR Log + Threat Intelligence Data

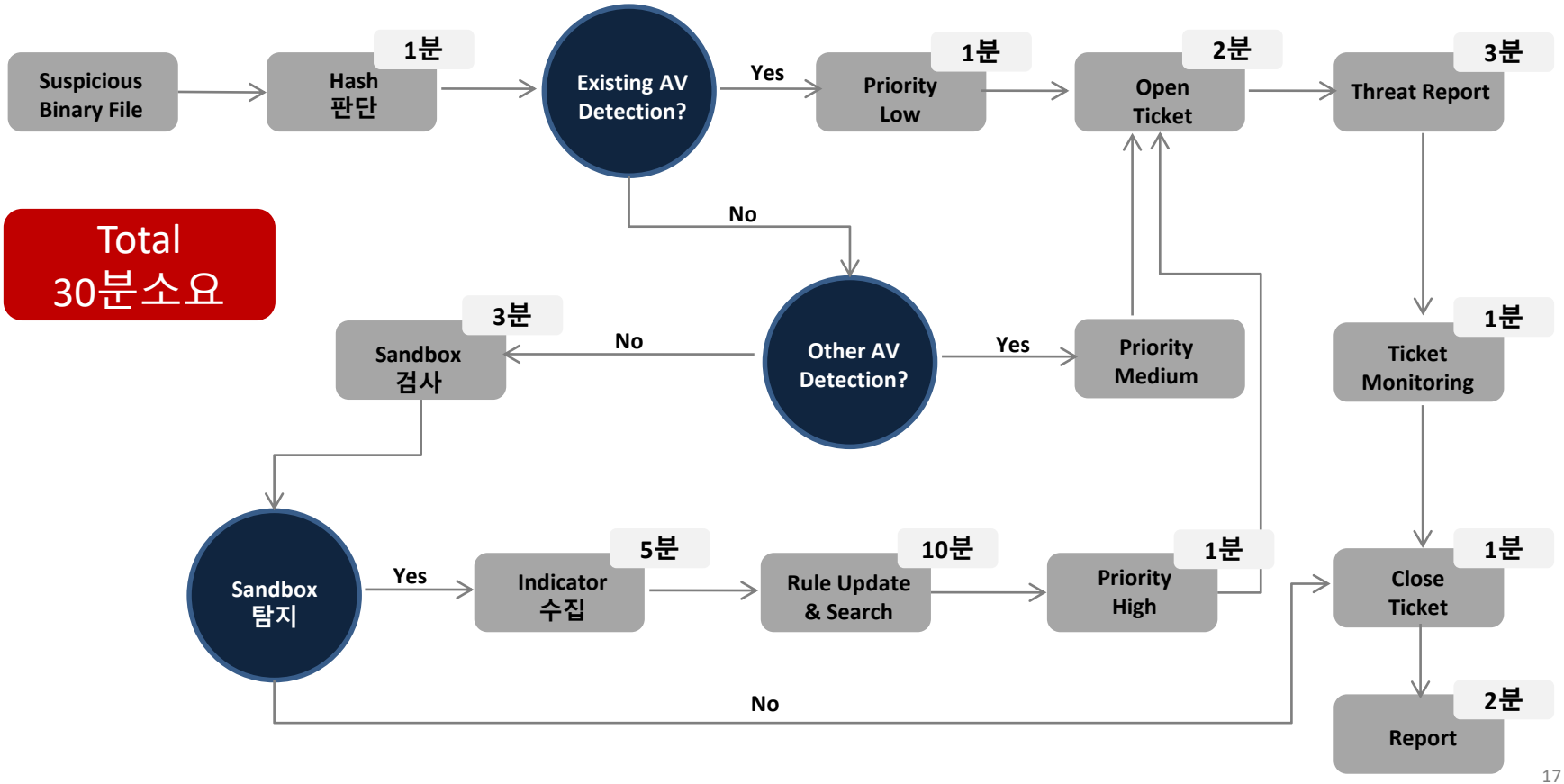
DstIP_Malicious_URL_history:"http://sdfngoaeor.ru/sdf.exe, http://sadffelkwjf.com/flash.html"
DstIP_File_Hash_C2:"4b420703c60ad834798b72e6cd1ce4fa, 35910deac00c7203b1dfb4c6de8bc0e0, 9fed2deb88db24caec3ce98574a71276“
DstPort_Desciption:"Not Well_known_Port"
DstPort_History:"악성파일 프로세스명 3개와 동일한 Port를 사용함“
Filehash_Reputaion:"Backdoor_RAT"
C2&Port_Hacking_group:”APT28”
Persistence Connection: “Y”
Mutex:”sdkfhksdlhjf”
File_Pdb_Path:”c:\malware\hack.pdb”

기존 EDR 로그	DstIP_Malicious_URL_History	DstIP_File_Hash_C2	
DstPort_Description	DstPort_History	Persistence Connection	Filehash_Reputation
Processname_Reputation	Mutex	C2&Port_Hacking_Group	File_Pdb_Path

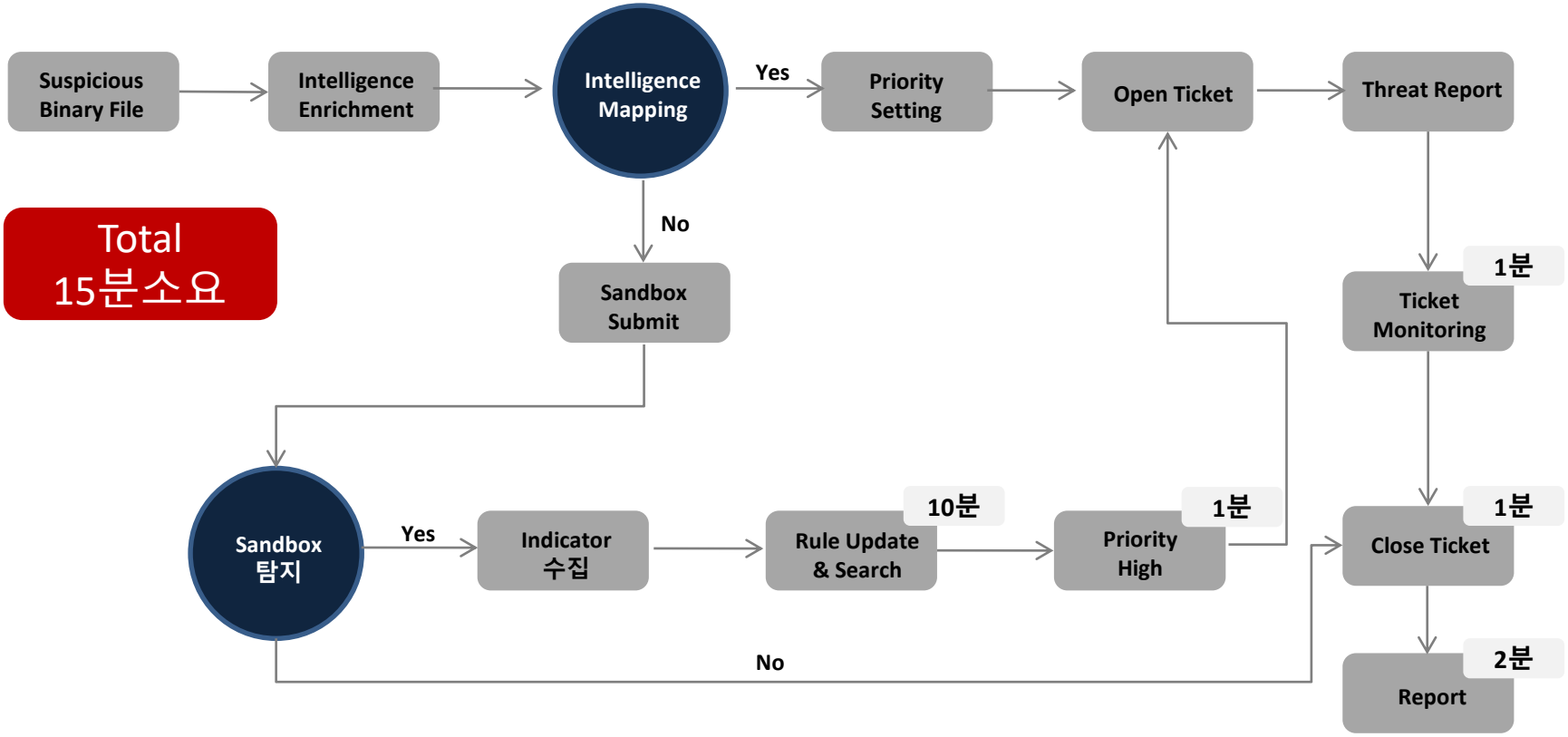
MSS 변화 필요

구분	Step1 Prevent	Step2 Detect	Step3 Response	Step4 Report	Step5 공유 및 개선
현재	• 보안정보 제공서비스 • 최신공격 분석 보고서 • Black IP 차단 • 취약점 분석 	SIEM • 발생로그 분석 • 침해징후 탐지 • 해킹 인지 및 판단 • 해킹 대응 진행	• 공격자대응 • Black IP 등록 • 공격자 IP 차단 • 악성파일 C2차단 • 악성파일삭제요청 • 침해위협발생 보고서 작성 • 고객요청사항 처리	• 정기 관제 보고서 • 침해위협발생 결과 보고서 • 요청사항 처리결과 보고서	• 보안장비 보안정책 업데이트 • 조치사항에 대한 처리 확인
한계점	Threat Data Coverage & Depth	Event 분석 및 해킹 판단 장시간 소요	Automated Process 적용 어려움		

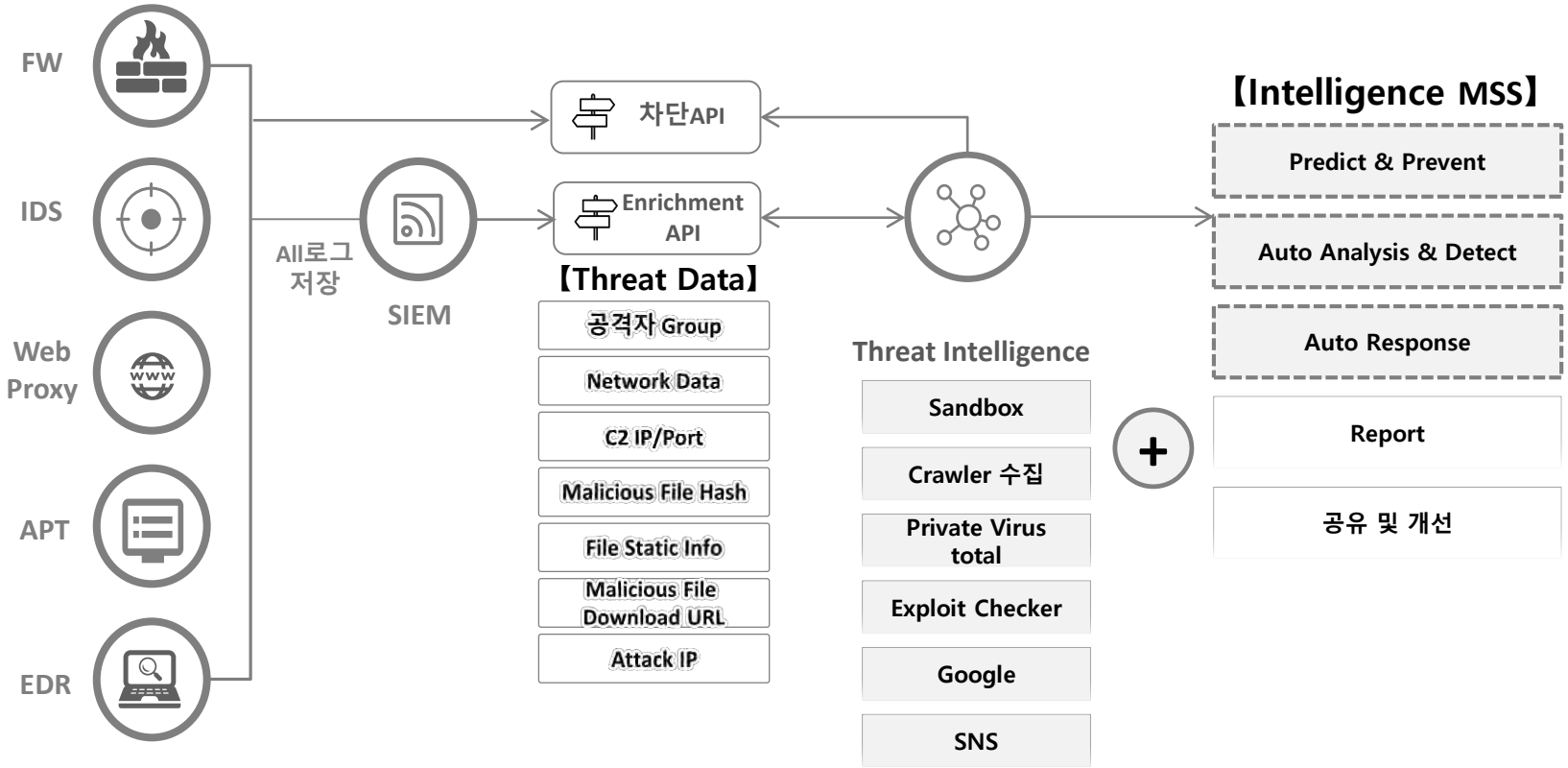
MSS Process


Suspicious Binary File
Hash 판단
1분
Existing AV Detection?
Yes
Priority Low
1분
Open Ticket
2분
Threat Report
3분
No
Total 30분소요
Other AV Detection?
No
Sandbox 검사
3분
Yes
Priority Medium
Ticket Monitoring
1분
Sandbox 탐지
Yes
Indicator 수집
5분
Rule Update & Search
10분
Priority High
1분
Close Ticket
1분
No
Report
2분

MSS + Intelligence

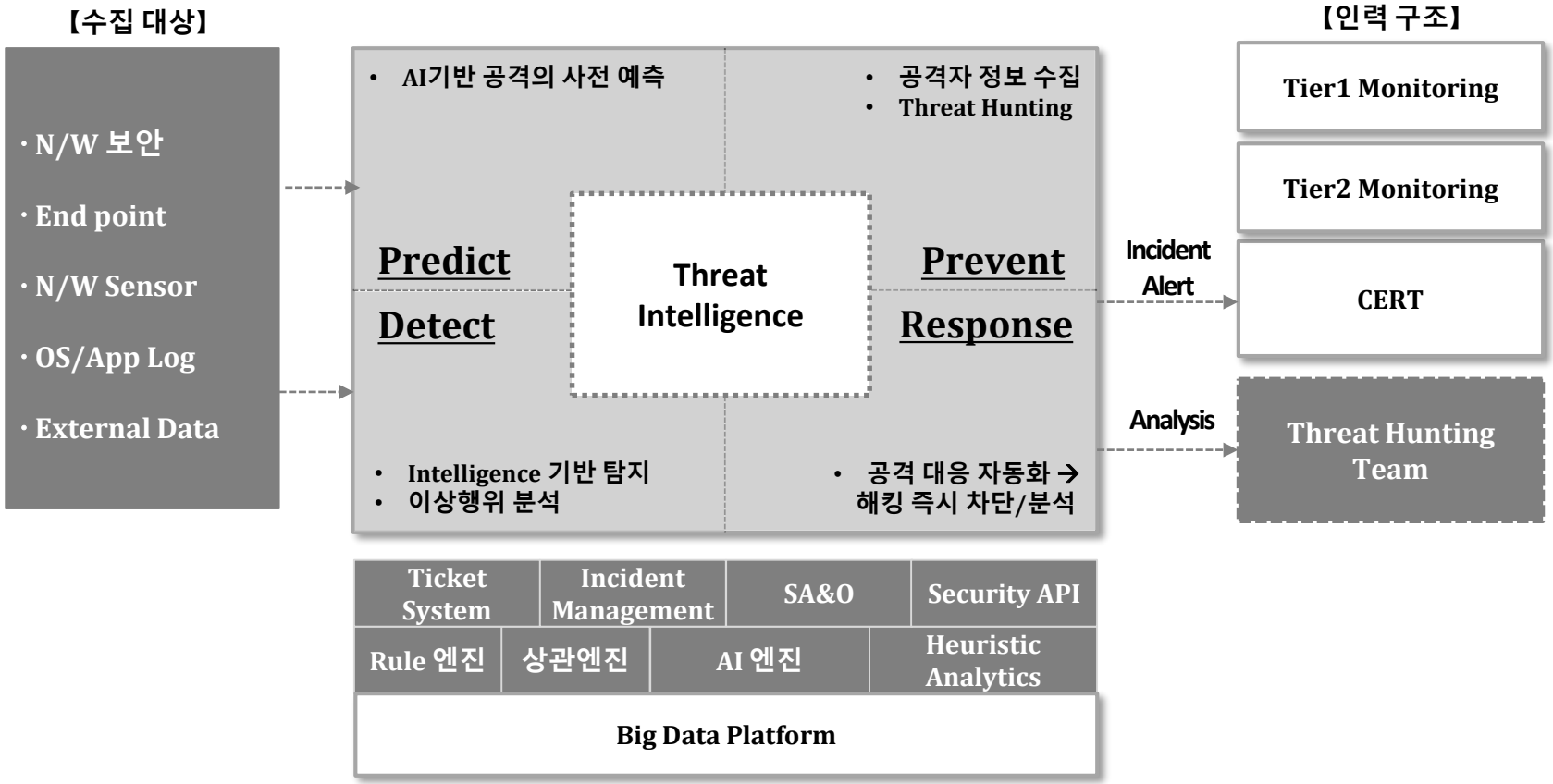


Intelligence MSS



Intelligence Managed Detection and Response

TREND MICRO | Security TRENDS 2018



맺는말


향후 공격 원인 파악 및
대응 매우 어려움
Data를 확장하고 Intelligence
하게 만들어야 함
Real-Time 대응 관점에서 MSS와
Intelligence를 결합해야 함
Intelligence 기반의 탐지/대응
신기술 도입 및 Researcher 역할 중요

TREND MICRO

Security
TRENDS 2018

THANK YOU

SK infosec
EQST Group 이재우