One Step
Ahead

한눈에, 한꺼번에, 다같이

빅데이터시대, 차세대 보안관제 프레임워크

이글루시큐리티
이세호팀장

2015. 04.16

IGLOOSECURITY

Contents

I 보안관제 당면과제

보안관제 주요 업무

보안관제 업무는 관제 업무 뿐만 아니라 다양한 보안업무도 포함하고 있습니다.

실시간 경보 모니터링

탐지 패턴 업데이트

정보공유

웹해킹 탐지

악성코드 분석

지침/매뉴얼 개정

관제 보고서 작성

방화벽 운영 관리

개인/내부 정보 유출 방지

IPS 운영 관리

상황전파

방화벽 정책 설정

보안장비 가용성 모니터링

Anti-Virus 운영 관리

DDoS 대응

컴플라이언스

침해사고 처리

최신 보안동향 모니터링

서버 취약점 점검

홈페이지 위변조 탐지

침해사고 분석

해킹 메일 분석

네트워크 취약점 점검

모의 훈련

유해 IP, URL 관리

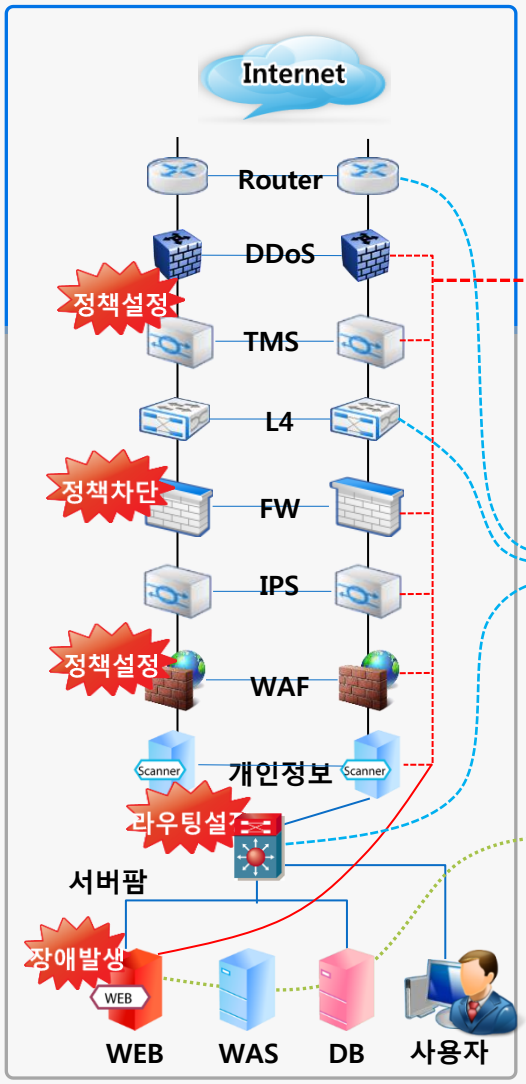
APP 취약점 점검

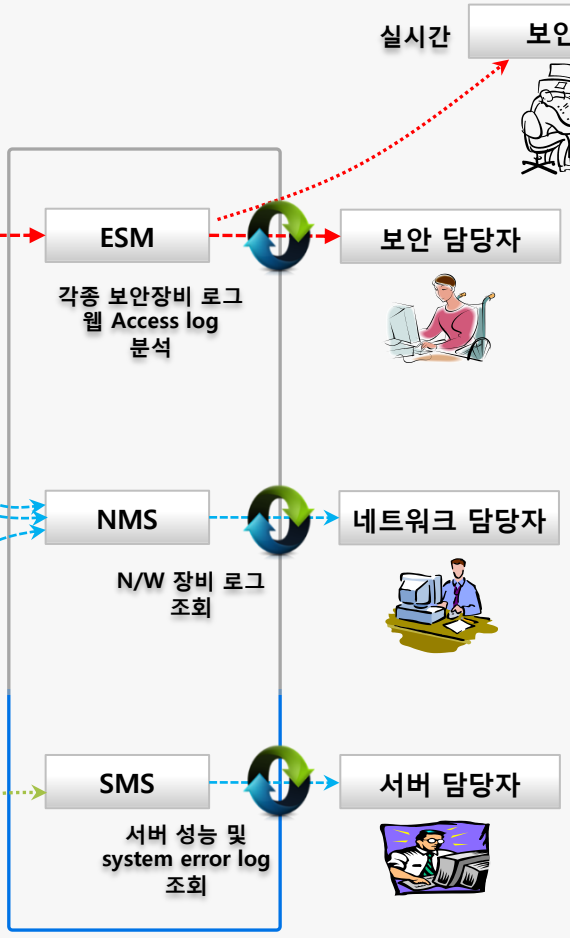
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

로그 운영/관리 업무의 문제점

침해냐? 장애냐? /'보안, 네트워크, 서버의 로그 > 개별 검색 '





각종장비에서 발생하는
수많은 로그를 지속적인
관리가 중요한데...

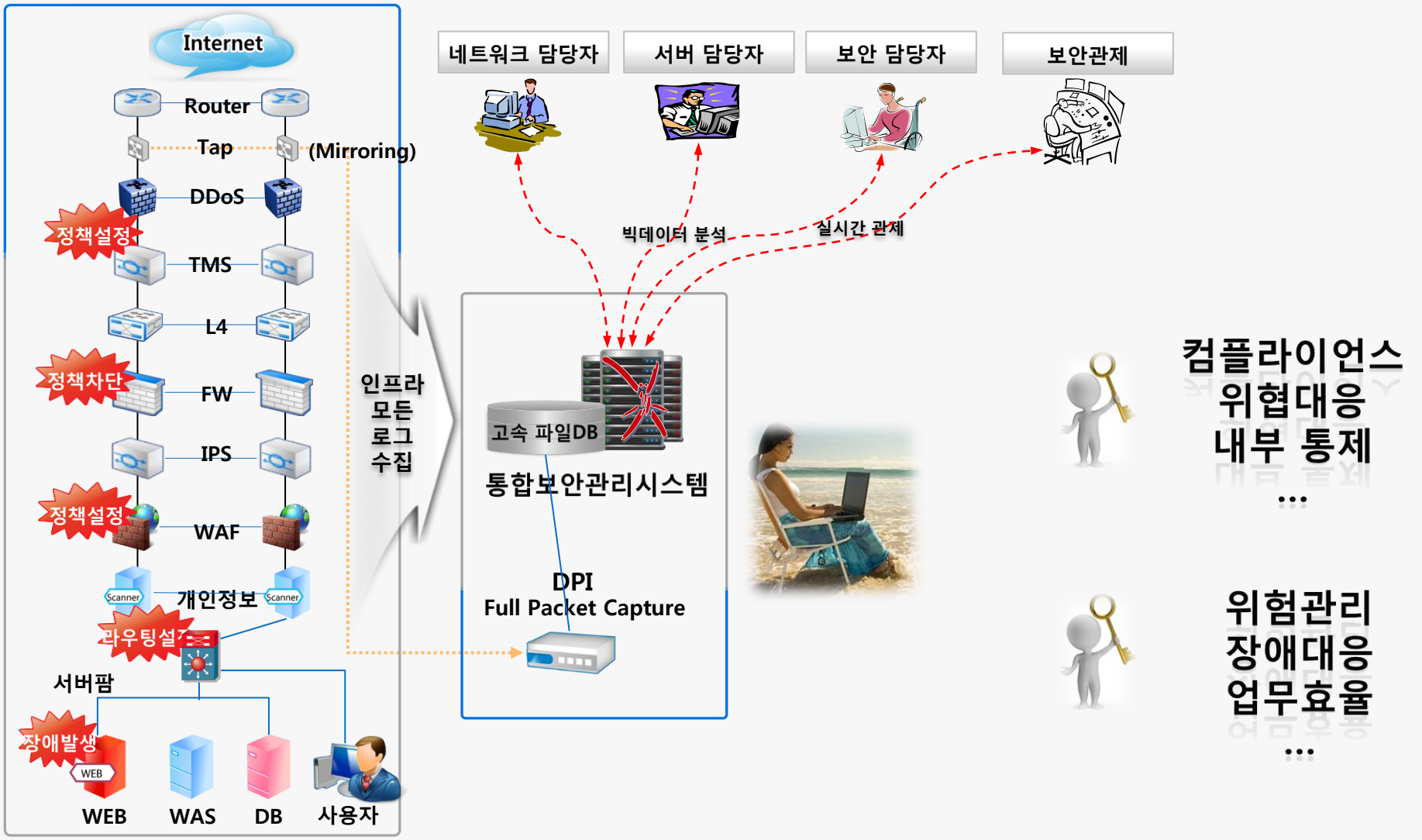
인프라가 복잡해지면서
침해/장애발생 시 분석
이 쉽지가 않다...

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

로그 운영/관리 업무 개선

'보안, 네트워크, 서버의 로그 통합 관리 및 분석(검색)시간 단축 '



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

기존 보안관제시스템의 문제점

기존 보안관제시스템의 기능적 한계로 인해 관제 효율성이 많이 부족했습니다.

통합보안관제시스템

위협관리시스템

종합분석시스템

- 대용량 로그 처리의 한계
- 비정형 로그의 수집/분석 불가
- 검색속도의 한계
- 분석 기간/방법의 한계
- 대응기능의 부재

- 패턴기반(알려진 공격)의 탐지
- 패턴기반의 한정된 payload 수집
- 어플리케이션 인지 기능 미비
- 송수신 파일에 대한 분석 불가
- 피해현황 확인의 한계

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 보안관제시스템

지식 기반 정보 분석

내부정보 및 외부 위협정보와
같이 분석해야 한다.

BIG DATA 기반
로그 처리 기술

모든 로그를 수집하여
분석해야 한다.

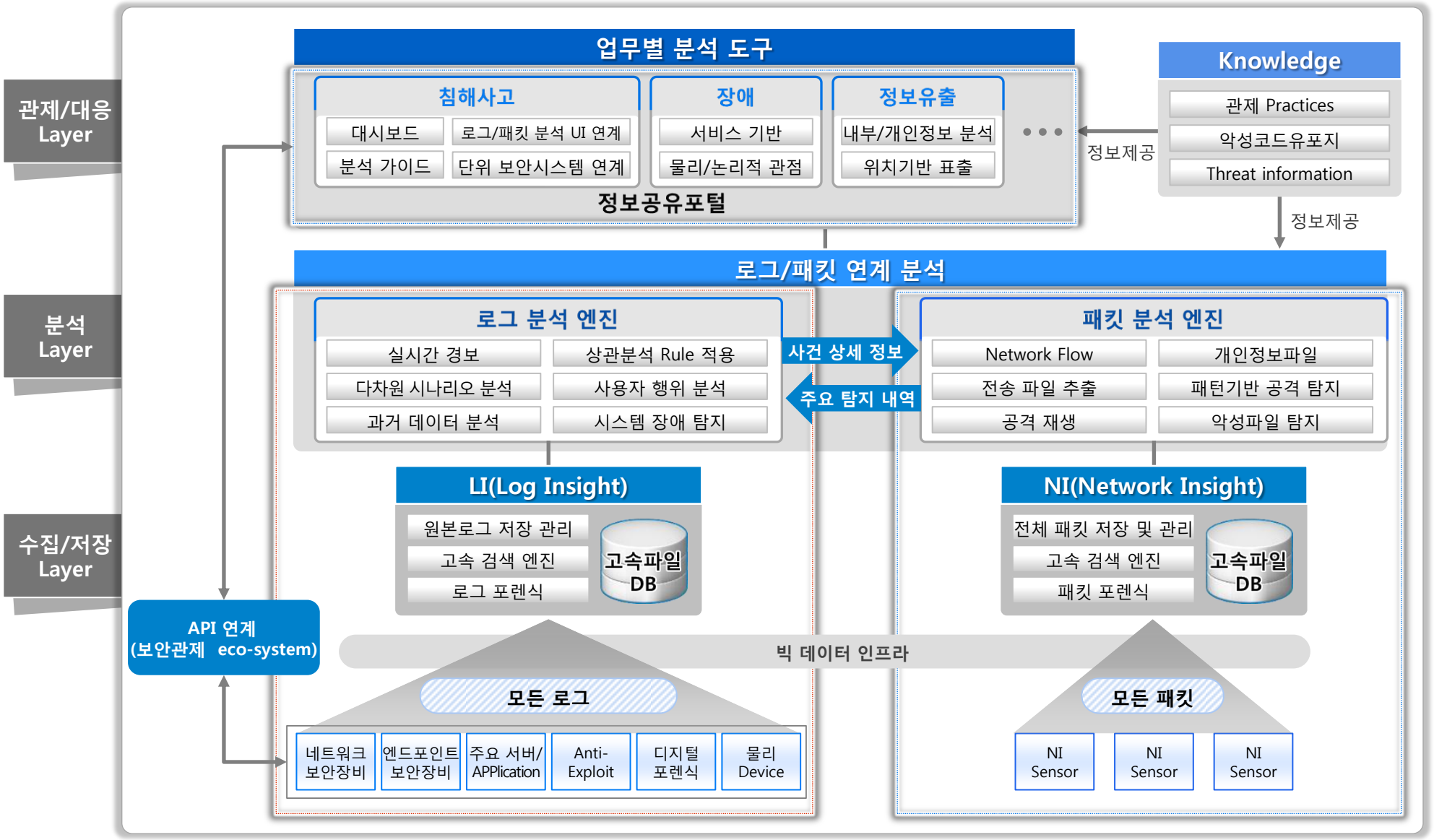
Full Packet Capture

네트워크의 모든 패킷을 저장하고
분석해야 한다.

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 보안관제시스템 프레임워크



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

이글루시큐리티 차세대 보안관제시스템

이글루시큐리티는 차세대 통합보안관제시스템을 통해 모든 보안관제 업무를 수행할 수 있도록 보안관제 업무에 최적화 된 기능들을 구현했습니다.

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 보안관제시스템

이글루시큐리티는 차세대 통합보안관제시스템을 통해 모든 보안관제 업무를 수행할 수 있도록 보안관제 업무에 최적화 된 기능들을 구현했습니다.

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

차세대 통합보안관제시스템의 운영/관리 업무

3D Network Topology Map을 제공하여 침해와 장애상황에 대한 직관적인 상황 인지, 시스템 침해/장애의 이력관리, 서비스 중심의 가용성 모니터링을 통한 내부 IT 인프라의 운영 업무를 지원합니다.

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

Ⅱ 차세대 통합보안관제시스템 구성

보안관제 주요 업무

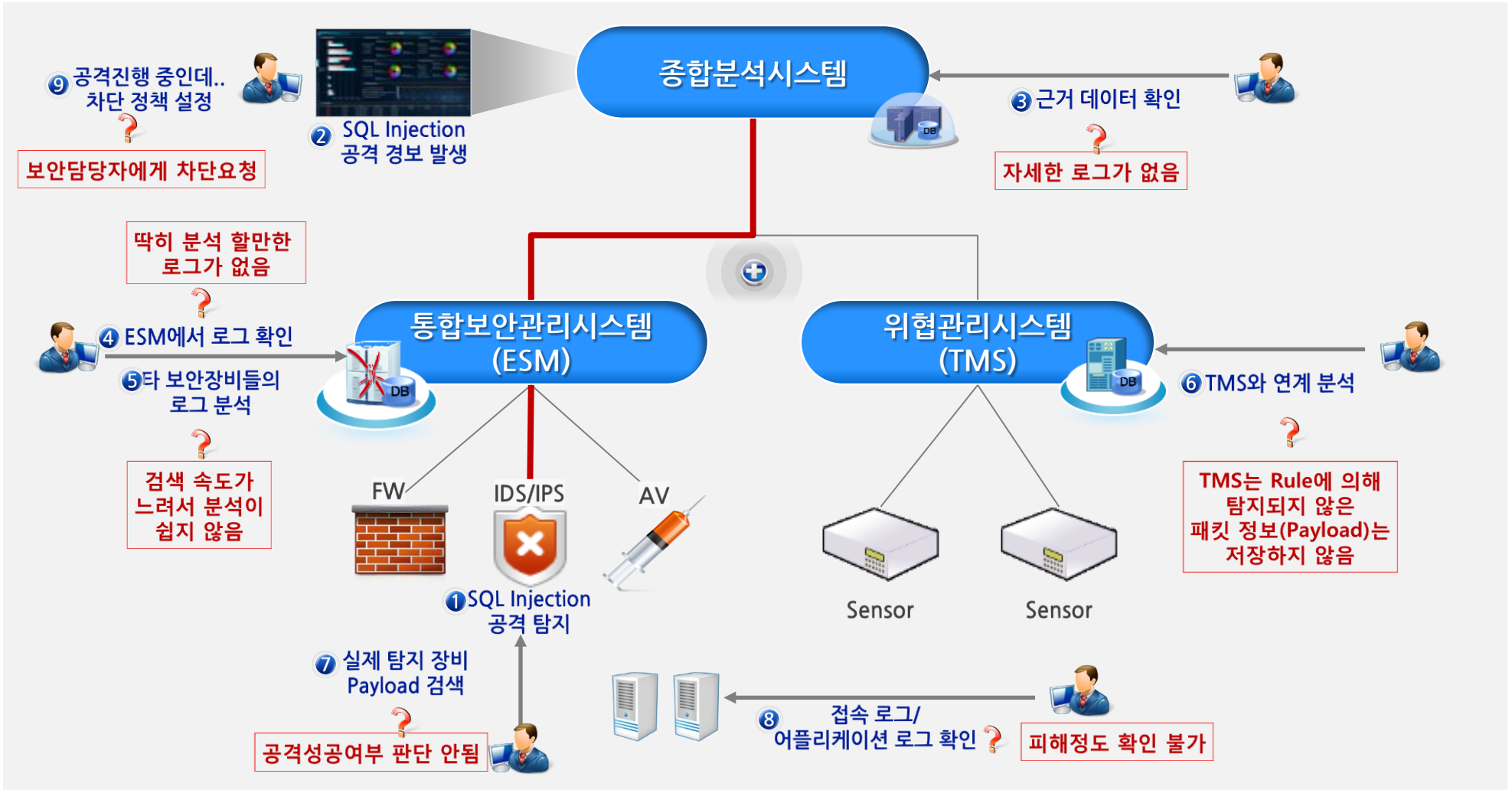
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

기존 보안관제시스템의 문제점

탐지분석대응

보안관제의 가장 기본이 되는 '탐지/분석/대응' 업무의 경우 기존 시스템의 기능적 한계로 인해 관제 효율성이 많이 부족했습니다.

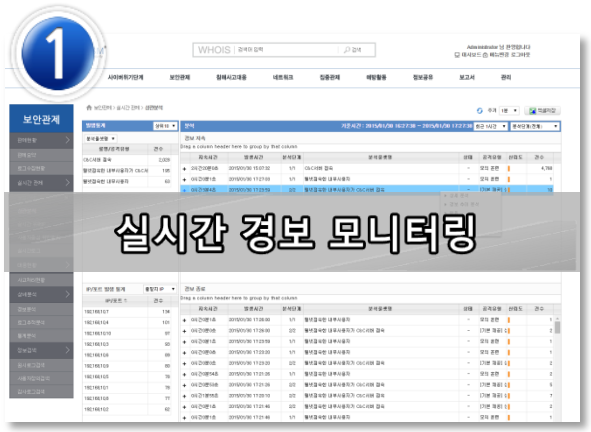


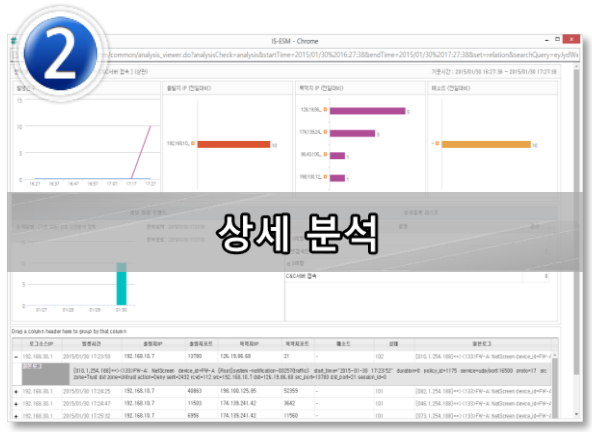
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

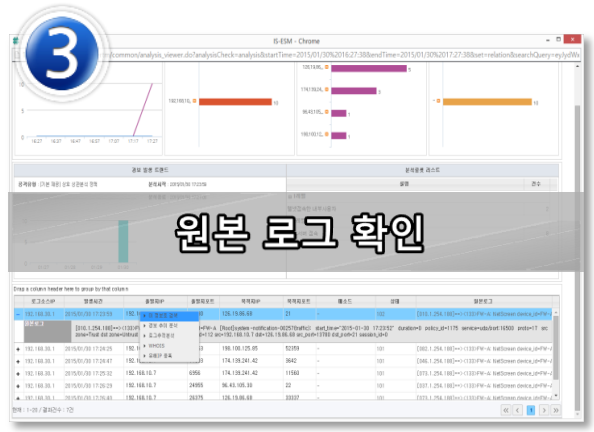
IGLOOSECURITY

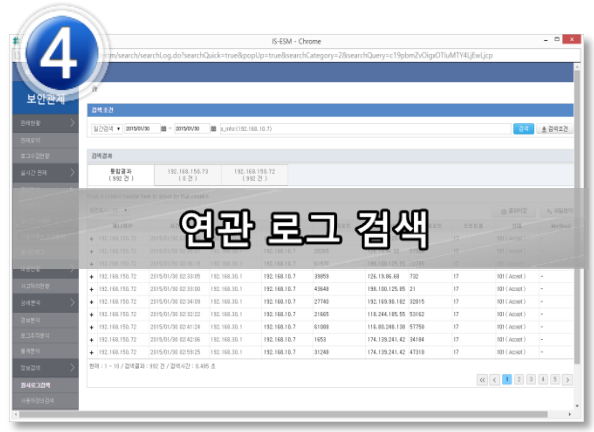
차세대 통합보안관제시스템의 탐지/분석 업무

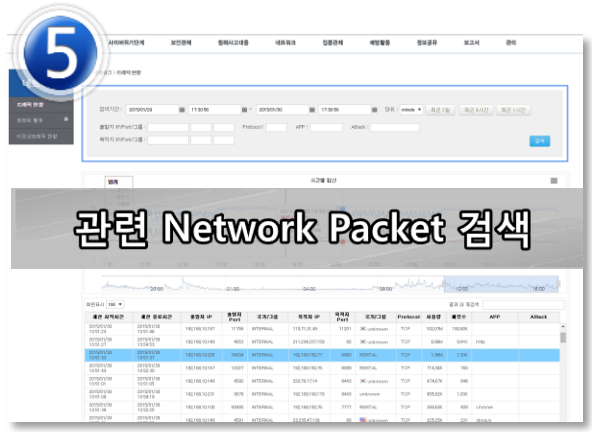
이글루시큐리티의 차세대 보안관제시스템은 최초 탐지부터 로그/패킷 분석까지 일원화 된 관제 환경을 구성하여 관제 업무의 효율성을 제공합니다.

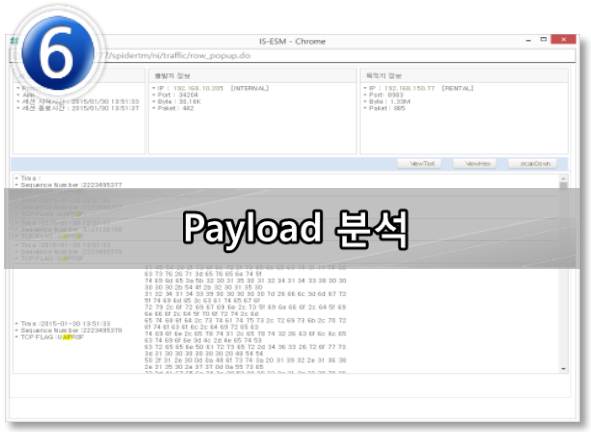












Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 탐지/분석/대응 업무

이글루시큐리티는 다양한 분석을 위해 분석엔진을 고도화 하여 다양한 관점의 상관분석을 통한 보다 의미 있는 분석 결과를 도출할 수 있는 기반을 마련했습니다.

분석엔진의 고도화

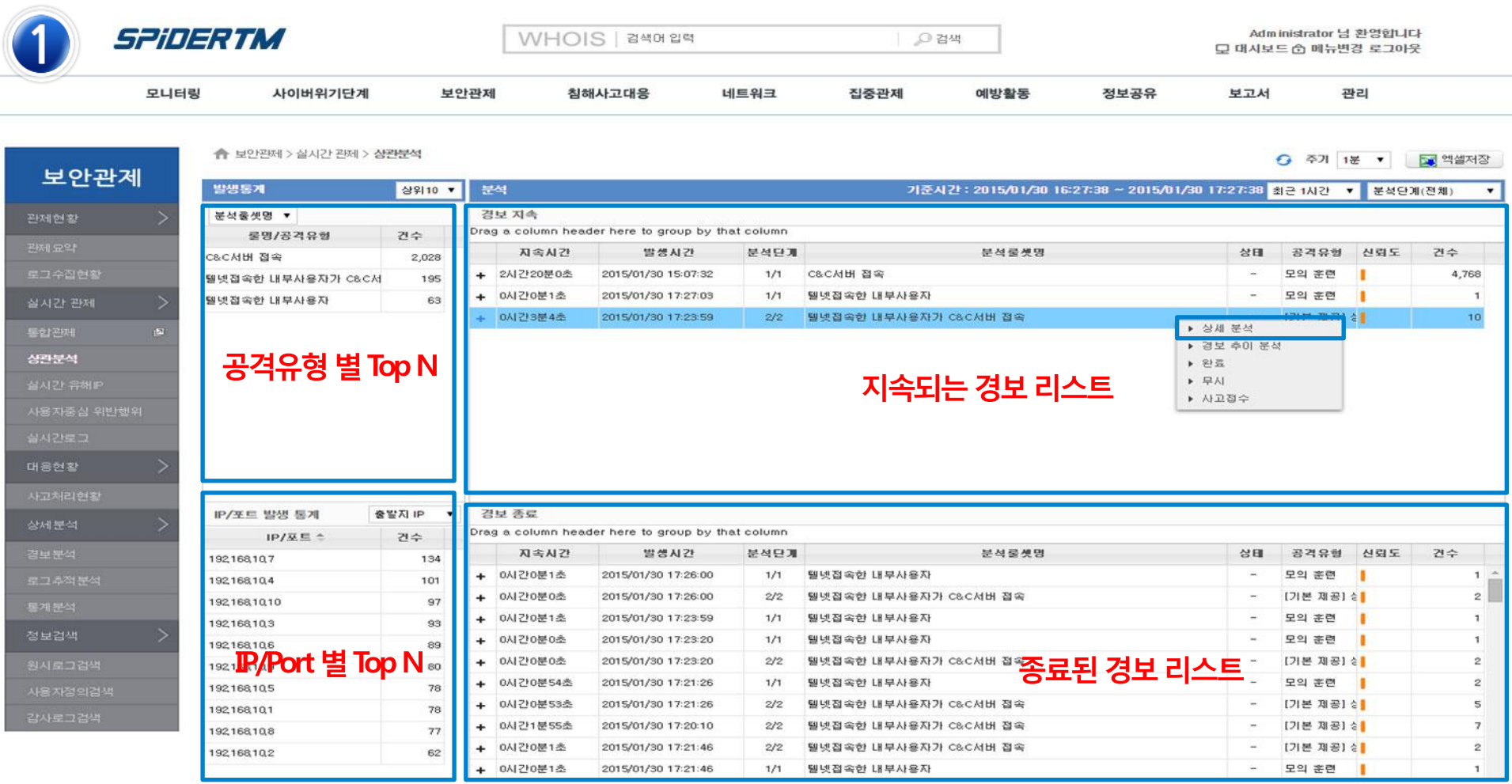
구분	기존 자사 제품(SPiDER TM 3.1)	차세대 통합보안관제시스템
분석 방식	• In-Memory 방식	• **In-Memory 방식**
분석 시간	• 1분	• **시간에 상관 없음(초/분/시/일/주/월까지 가능)**
분석 데이터	• 실시간 데이터	• **실시간 데이터 + 과거 데이터**
분석 방법	• 정해진 필드에 대한 단순 패턴 매칭 (특정 시그니처, 임계치 등)	• **모든 필드에 대한 다양한 분석 (패턴, 임계치, 연산자 등 복합 분석)**
시나리오 분석	• 미지원	• **단계 별 시나리오 분석 지원**

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 탐지/분석 업무

실시간으로 분석된 상관분석 결과에 대해 분석 단계 별 진행상태를 파악할 수 있는 관제 화면을 제공합니다.

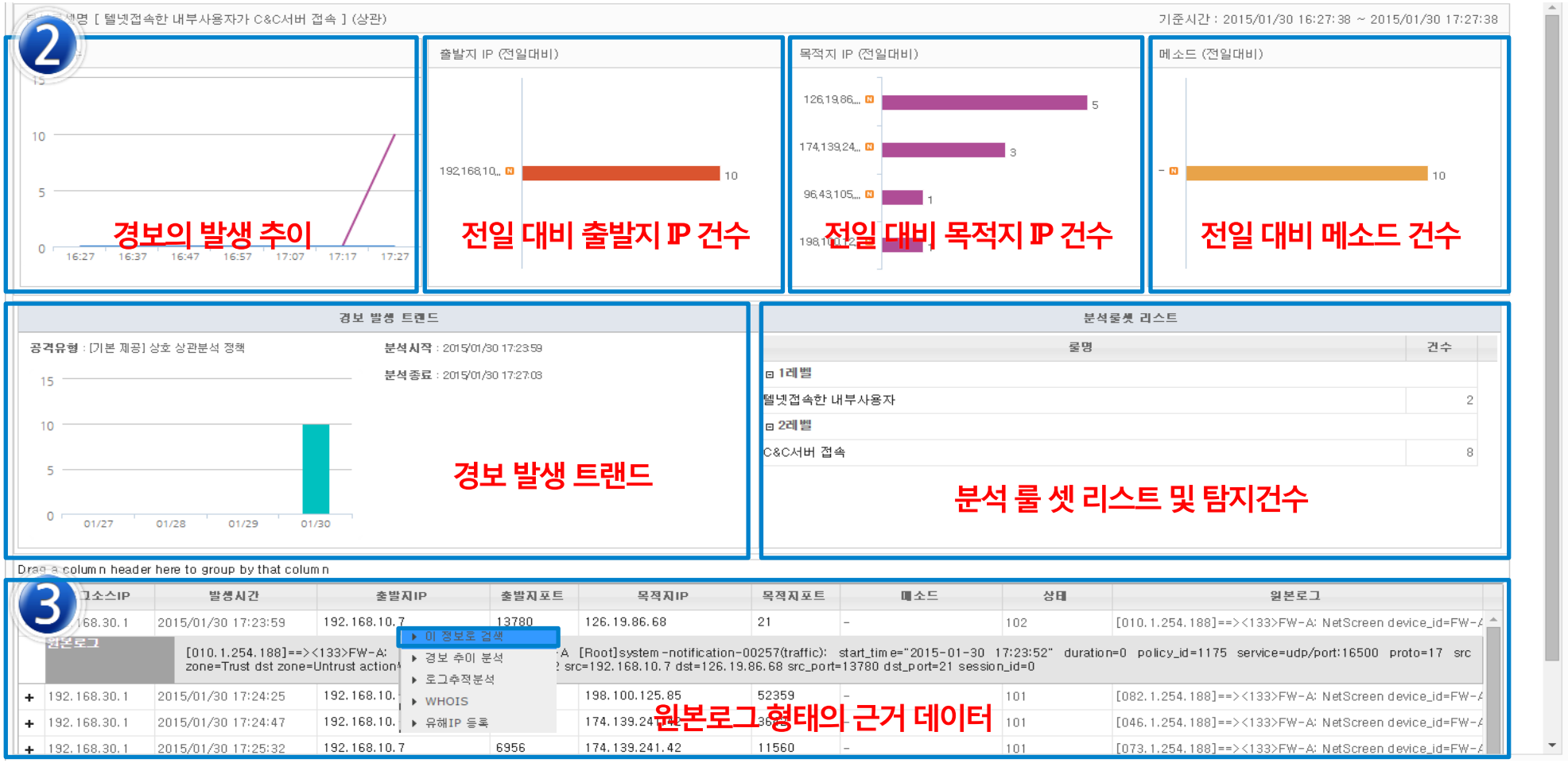


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 탐지/분석 업무

분석된 결과에 대한 상세분석을 통해 공격의 추이 및 IP, 공격 유형 등의 통계정보와 원본로그 형태의 근거 데이터를 제공하여 전반적인 공격 정보를 쉽게 파악할 수 있습니다.

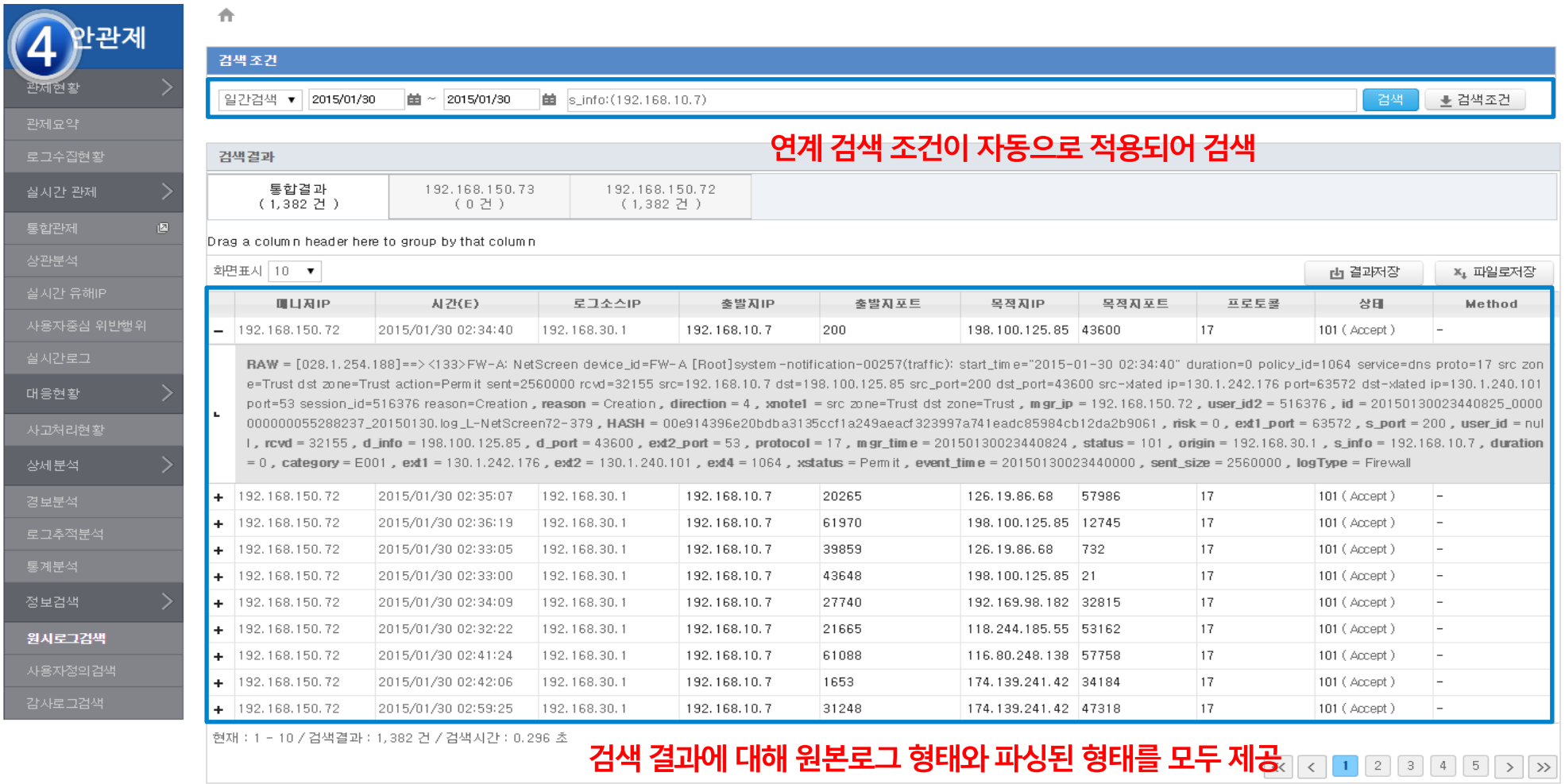


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 탐지/분석 업무

BIG DATA 기반의 고속파일DB를 통해 빠른 속도의 검색 결과를 제공하여 로그분석의 효율성을 제공합니다.

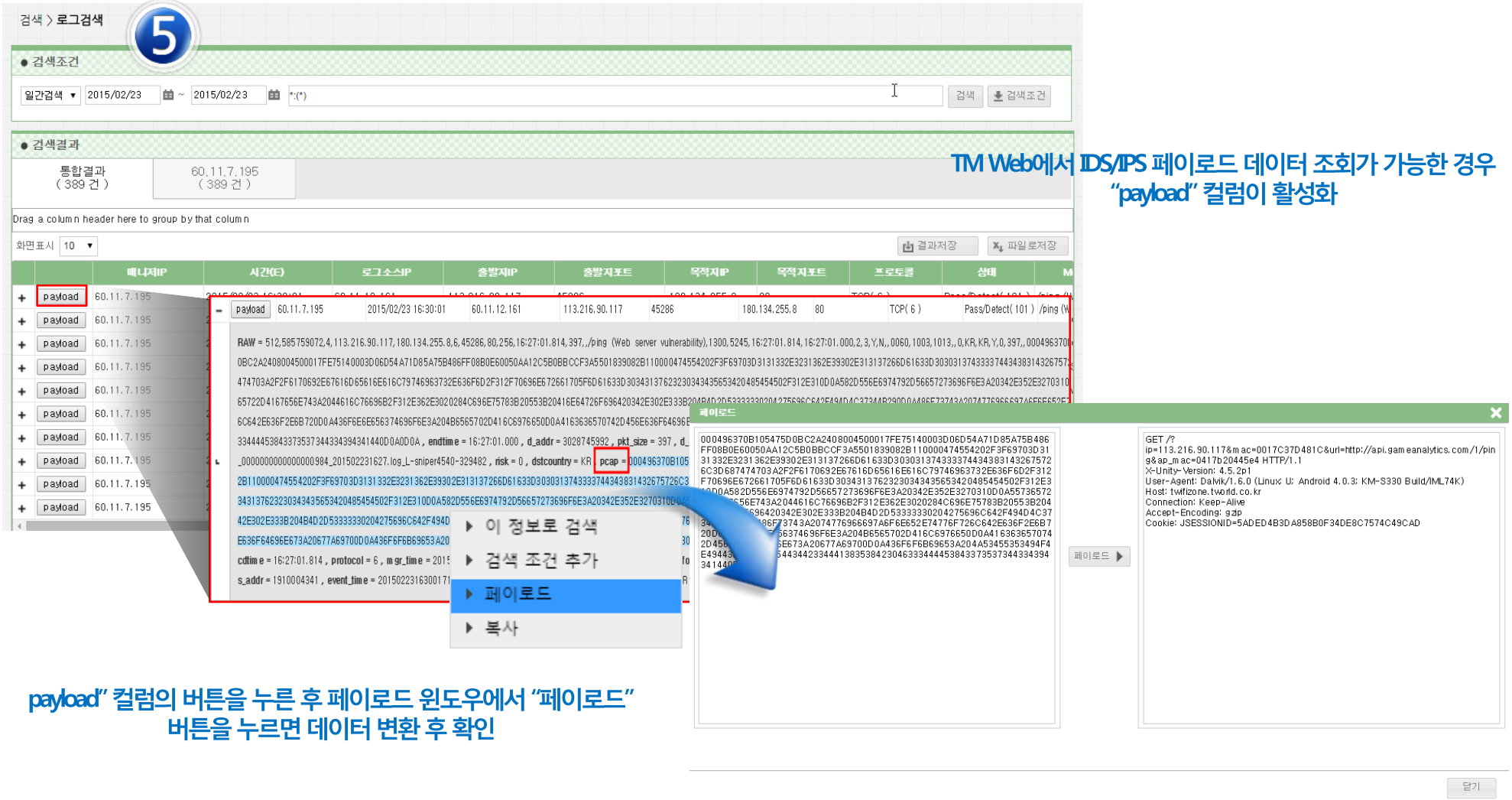


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

Payload 분석

DPI 엔진이 없는 경우 IPS 장비의 Payload 연계를 통해, 해당 IPS장비에 접속 없이 바로 Payload 분석 기능을 제공하여 보다 효율적인 분석 정보를 제공합니다.

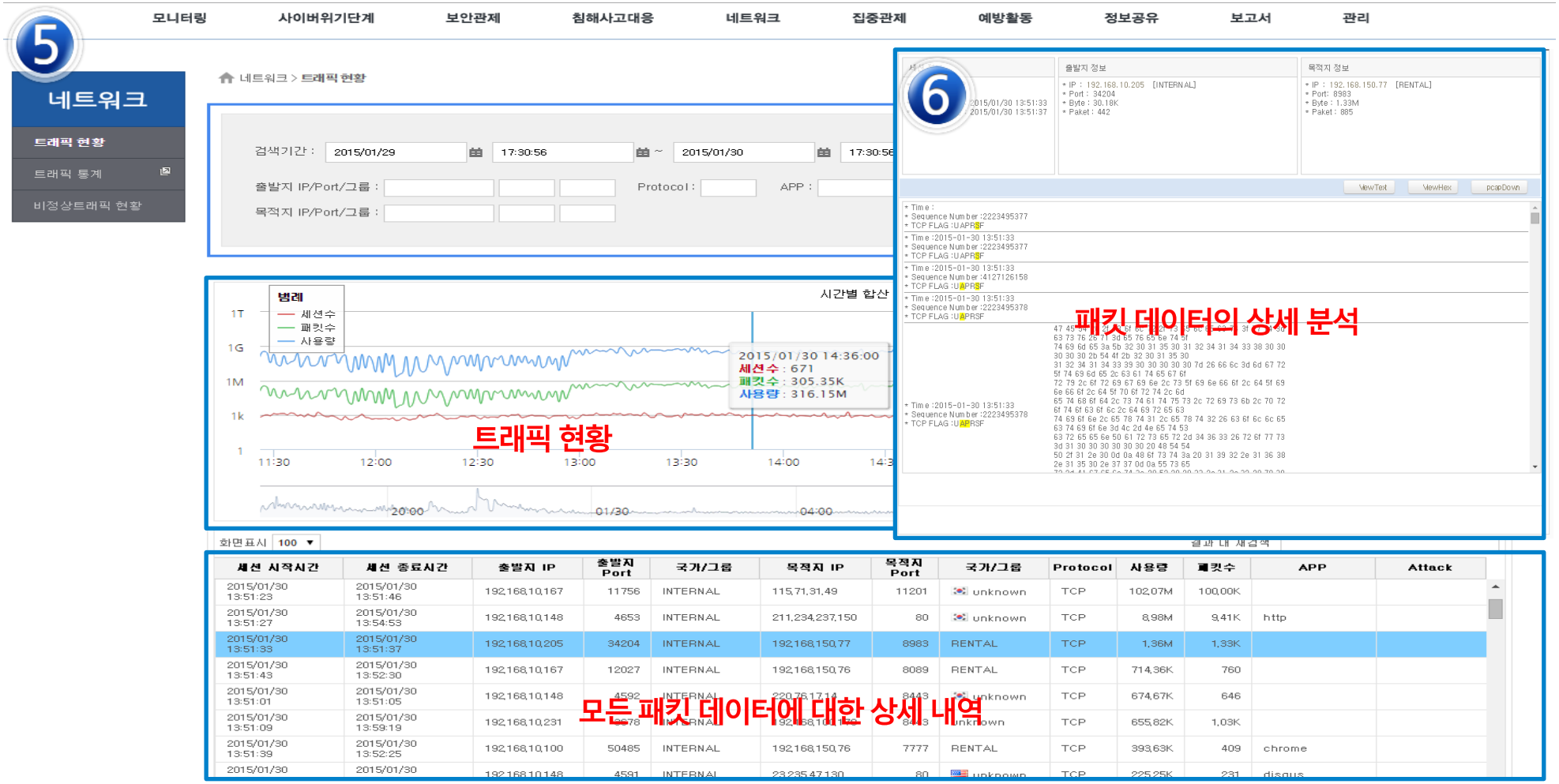


payload" 컬럼의 버튼을 누른 후 페이로드 윈도우에서 "페이로드" 버튼을 누르면 데이터 변환 후 확인

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

차세대 통합보안관제시스템의 탐지/분석 업무

모든 패킷 데이터의 수집/저장을 통해 공격에 대한 Payload 분석을 제공하여, 공격의 유효성을 판단하는 강력한 근거 자료를 제공합니다.



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

파싱

과거에는....

시작시간	종료시간	유지시간(초)	발생장비	방화벽 정책ID	상태	출발지 IP	출발지 포트	목적지 IP	목적지 포트	프로토콜	Zone
2014-08-12 13:25:17	2014-08-12 13:25:23	3	FW1	288	허용	145.23.43.22	2563	192.168.200.53	53	UDP	INT

에이전트...	수집일시	Source IP	Source Port	Destination IP	Destination Port	통신방향 ▽	Protocol	결과	위험도	횟수
FW	2015-03-01 오후 10:06:00	145.23.43.22	2563	192.168.200.53	53	Out->In	UDP	Accept	Middle	1
FW	2015-03-01 오후 10:06:00	145.23.43.22	1056	192.168.100.110	80	Out->In	UDP	Drop	High	3
FW	2015-03-01 오후 10:06:00	145.23.43.22	100	192.168.100.110	80	Out->In	TCP	Accept	Other	1

지금은.....

송신패킷 수	수신패킷 수	송신바이트 수	수신바이트 수	유지시간(초)	TCP플래그	정책ID
2	2	64	64	0	S sa A / FA fa A	71

	에니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
-	192.168.1.100	2015/02/27 17:03:09	192.168.9.1	192.168.9.100	34102	192.168.12.86	80	TCP(6)	Accept(101)	-

RAW = 3'0'1'1'03f445'1020'20150227'17:03:09'3'6'141211170602'192.168.9.100'34102'192.168.12.86'80'eth10'eth2''''64'2'64'2''31'1''S sa A / FA fa A'내부'외부'71'N/A'4'''' , count = 1 , reason = 1 , dnat_ip = null , sent_pk = 2 , type = 1 , ti = 17:03:09 , encrypt = 0 , s_port = 34102 , tcp_flag = S sa A / FA fa A , rcvd_data = 64 , nat_id = N/A , status = 101 , rcvd_pkt = 2 , s_info = 192.168.9.100 , mprotocol = TCP , ext5 , snat_type = null , category = E001 , ext1 = 3 , ext = 31 , ext3 = null , ext4 = 내부 , event_time = 20150227170309000 , day = 20150227 rule_id = 71 in_nic = eth10 , mgr _port = null , snat_ip = null , out_nic = th2 , version = 3 , id = 20150302212114183_0000000000001562001_20150302log_L-TrusGuardUTM-FW-285 , HASH = 07ab15f0eda df3f32da88a5f6a30bbce2dd9876e , name = 5 , d_info = 192.168.12.86 , d_port = 80 , protocol = 6 , mgr_time = 20150302212114184 , sent_data = 64 , origin = 192.168.9.1 , mstatus = 1020 , dnat_port = null , product = TrusGuard , = 4 , duration = null , dnat_type = null , rule_code = 141211170602 , logType = SECURE

원본로그

탐지와 분석의 핵심 정보

Copyright © IGLOO SECURITY, INC. 2014. All rights reserved.

IGLOOSECURITY

검색 속도 : 그래서 빨라야 한다.

일반공공 기관 하루 수집량
5천만건~1억건

● 검색조건

일간검색 ▼ 2015/03/02 ~ 2015/03/02 *:(*) 검색 검색조건

● 검색결과

통합결과 (140,270,524 건) | 192.168.1.100 (140,270,524 건)

Drag a column header here to group by that column

화면표시 10 ▼ 결과저장 파일로저장

	매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.139	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.154	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.186	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.160	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.155	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.191	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.187	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:2	192.168.9.1	37.9.62.66	44383	192.168.9.169	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:2	192.168.9.1	37.9.62.66	44383	192.168.9.157	19	UDP(17)	Drop(102)	-
+	192.168.1.100	2015/03/02 09:13:25	192.168.9.1	37.9.62.66	44383	192.168.9.161	19	UDP(17)	Drop(102)	-

현재 : 1 - 10 / 검색결과 : 140,270,524 건 / 검색시간 : 2.712 초

현재 : 1 - 10 / 검색결과 : 283,544,462 건 / 검색시간 : 5.467 초

현재 : 1 - 10 / 검색결과 : 869,577,714 건 / 검색시간 : 11.662 초

현재 : 1 - 10 / 검색결과 : 140,270,524 건 / 검색시간 : 2.712 초

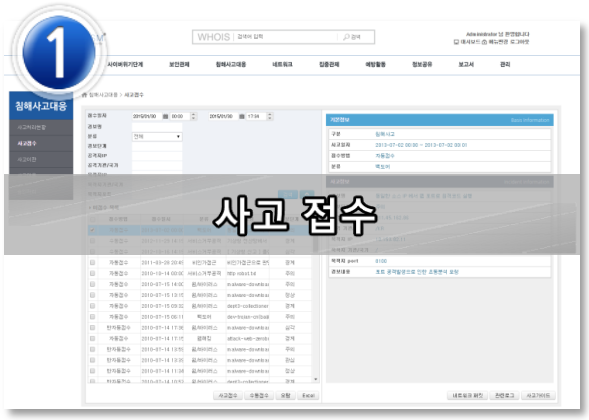
« < 1 2 3 4 5 > »

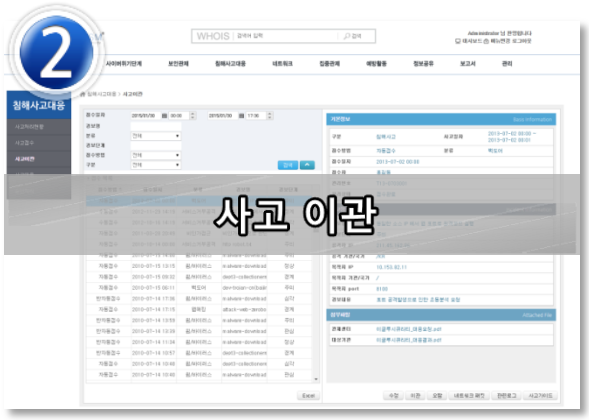
Copyright © IGLOO SECURITY, INC. 2014. All rights reserved.

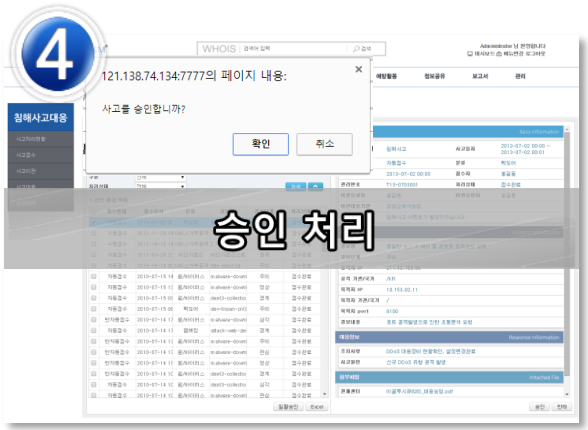
IGLOOSECURITY

차세대 통합보안관제시스템의 대응/사고처리 업무

분석된 경보 이벤트에 대해 체계화된 침해사고 대응 프로세스를 제공하여 신속한 사고처리 업무를 진행할 수 있도록 지원합니다.



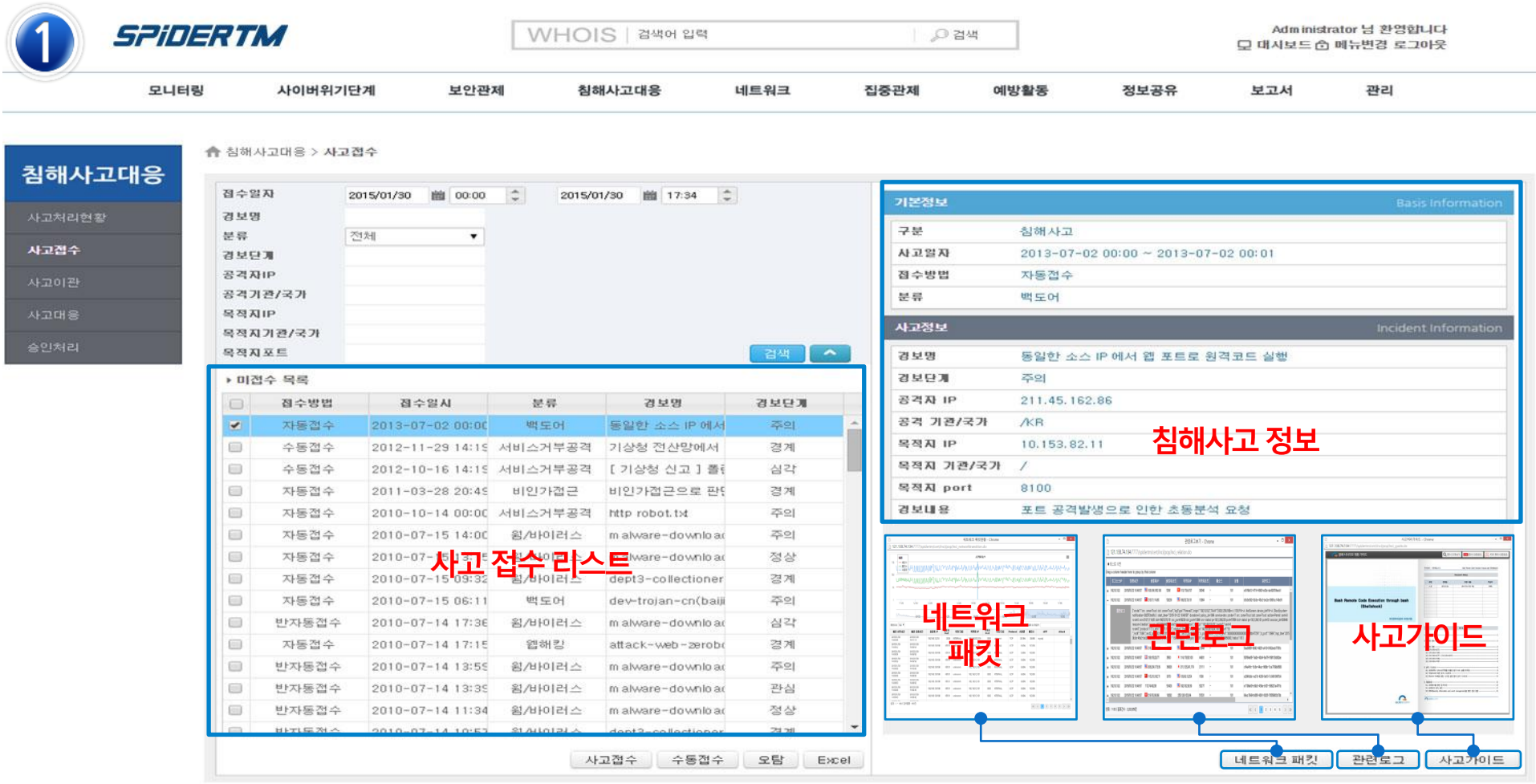




Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

대응/사고처리 업무 : 사고 접수

사고접수는 자동 또는 수동으로 접수되며, 접수된 사고의 네트워크 패킷, 관련로그, 사고 가이드에 대한 정보도 함께 제공합니다.

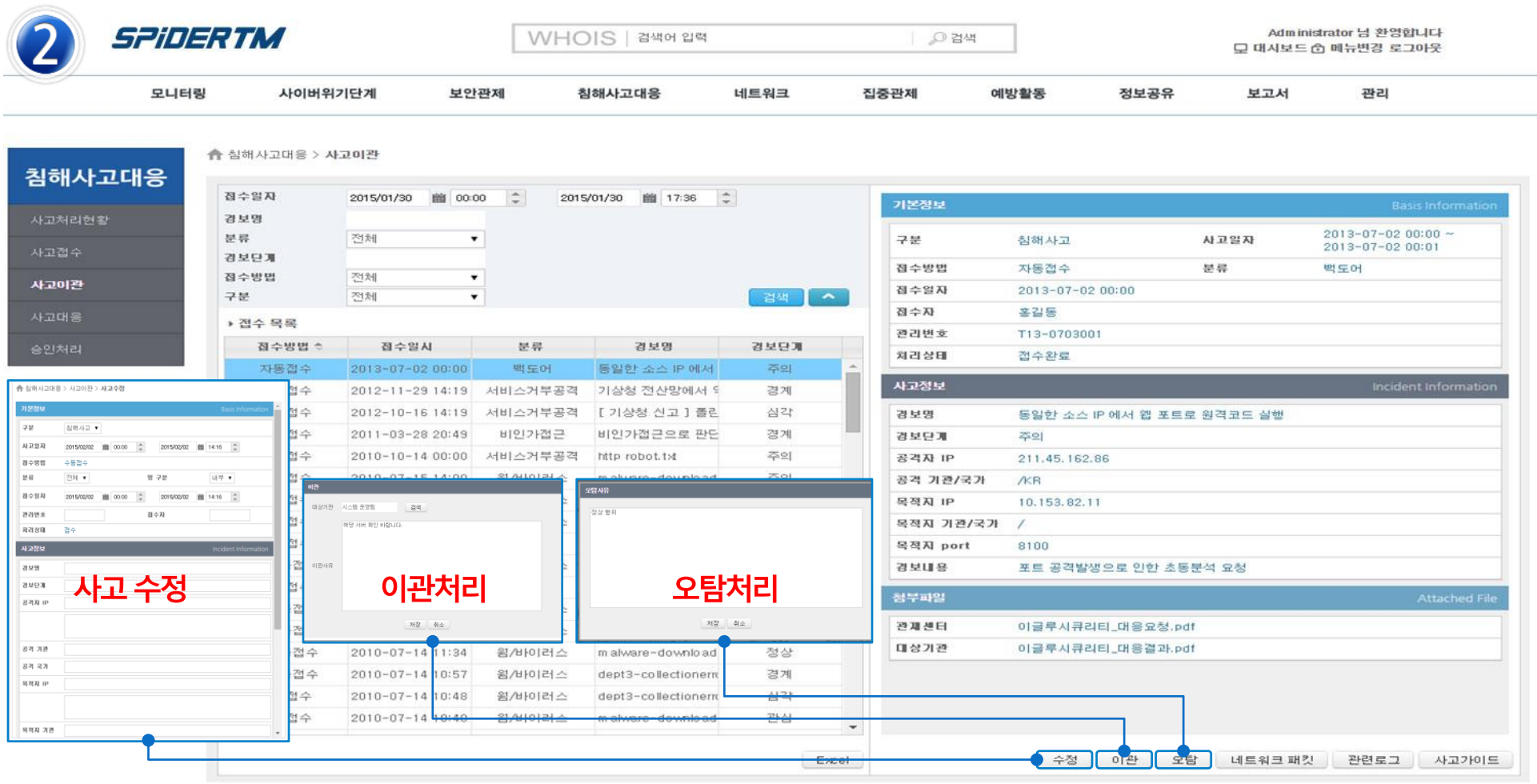


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

대응/사고처리 업무 : 사고 이관

접수된 사고는 담당자 이관을 통해 다음 단계로 진행되거나, 오탐처리로 인한 사건 종결을 진행합니다.

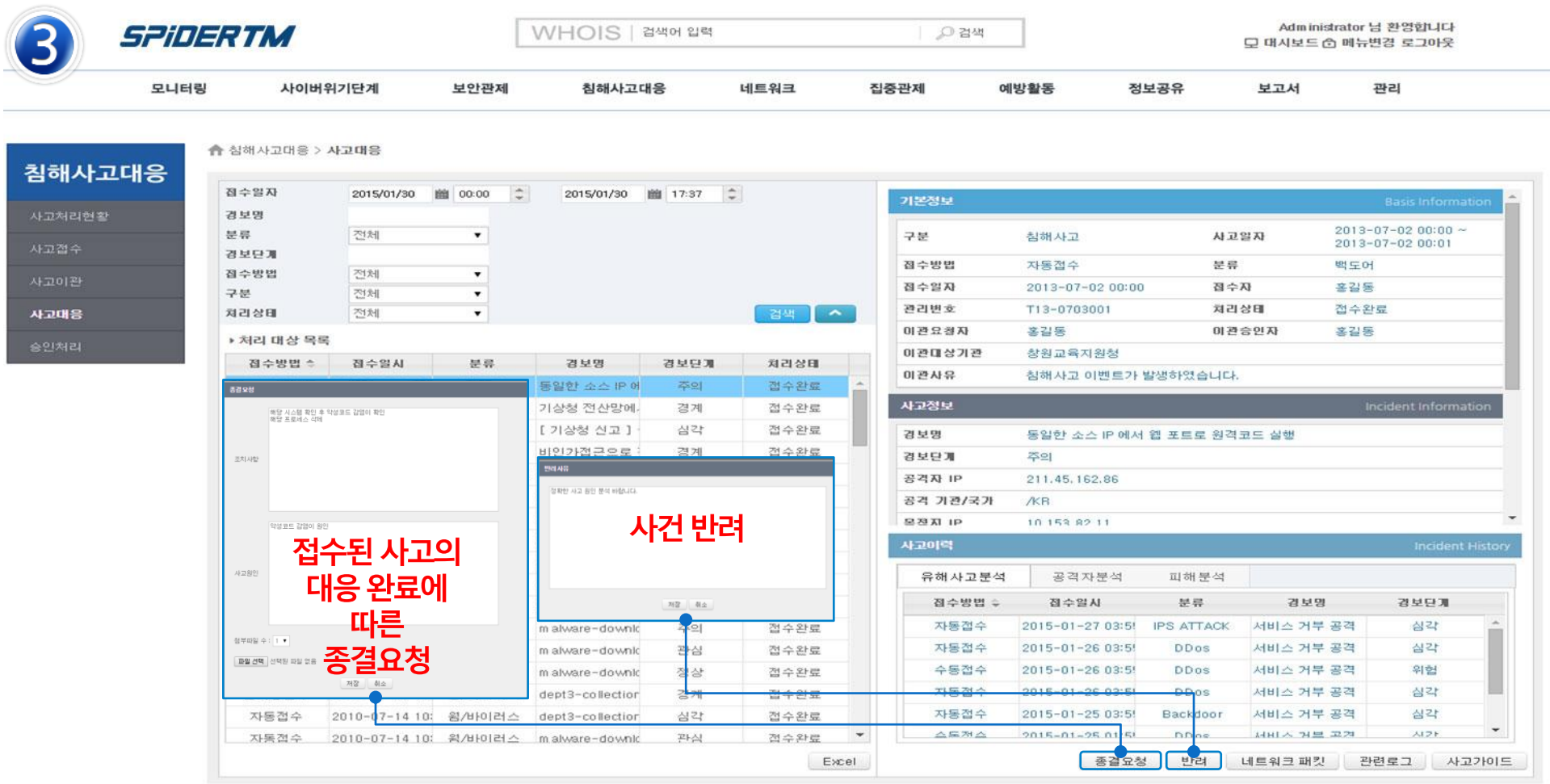


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

대응/사고처리 업무 : 사고 대응

접수된 사고의 대응 완료 시 사건에 대한 종결을 요청하여 다음 단계로 진행됩니다.



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

대응/사고처리 업무 : 승인 처리

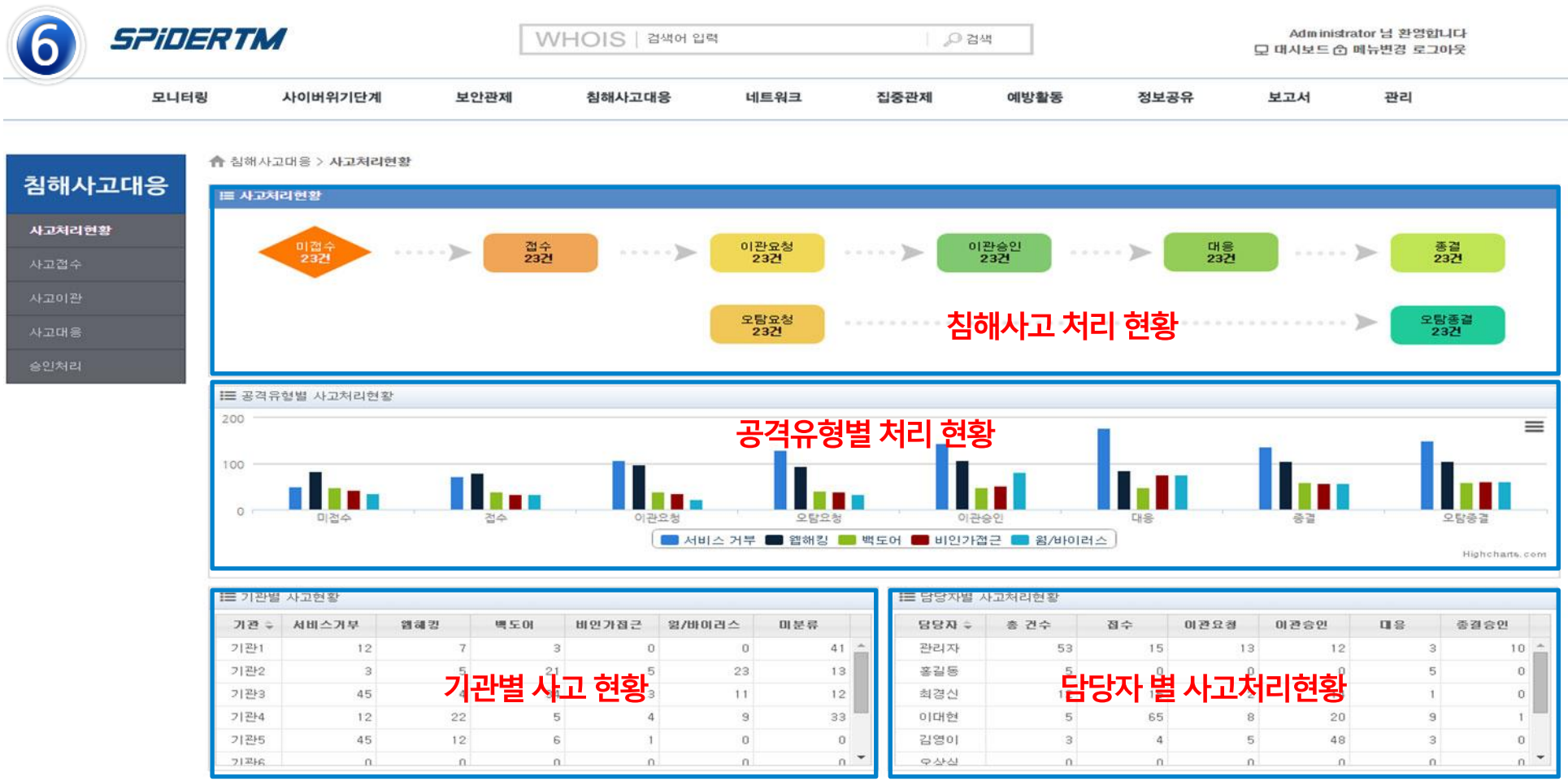
탐지/분석/대응이 모두 완료된 사고의 사건을 종결 시켜 사건을 마무리 합니다.

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

대응/사고처리 업무 : 침해사고 전체 처리 현황

전반적인 침해사고현황 및 사고처리현황을 제공하여 현재 발생된 위협의 건수와 처리 현황을 한눈에 확인할 수 있습니다.



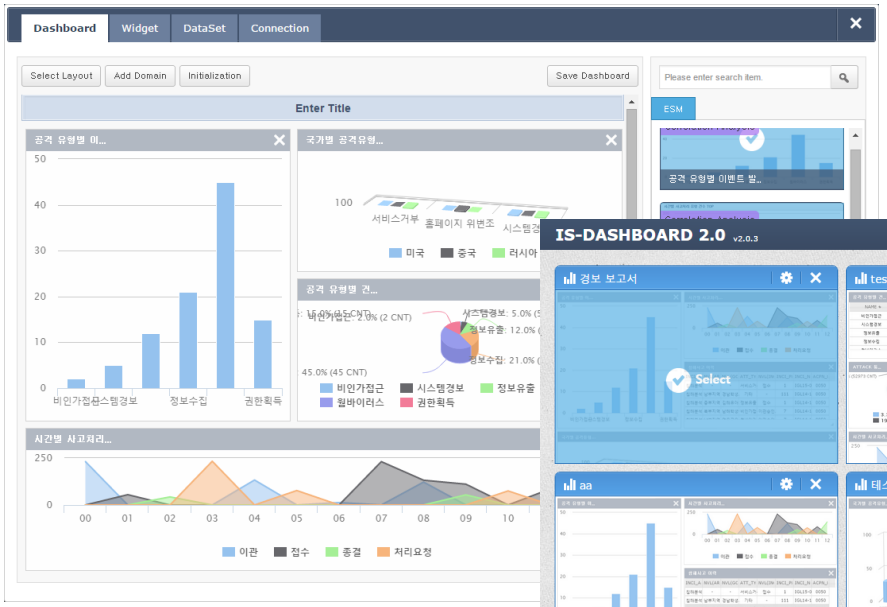
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

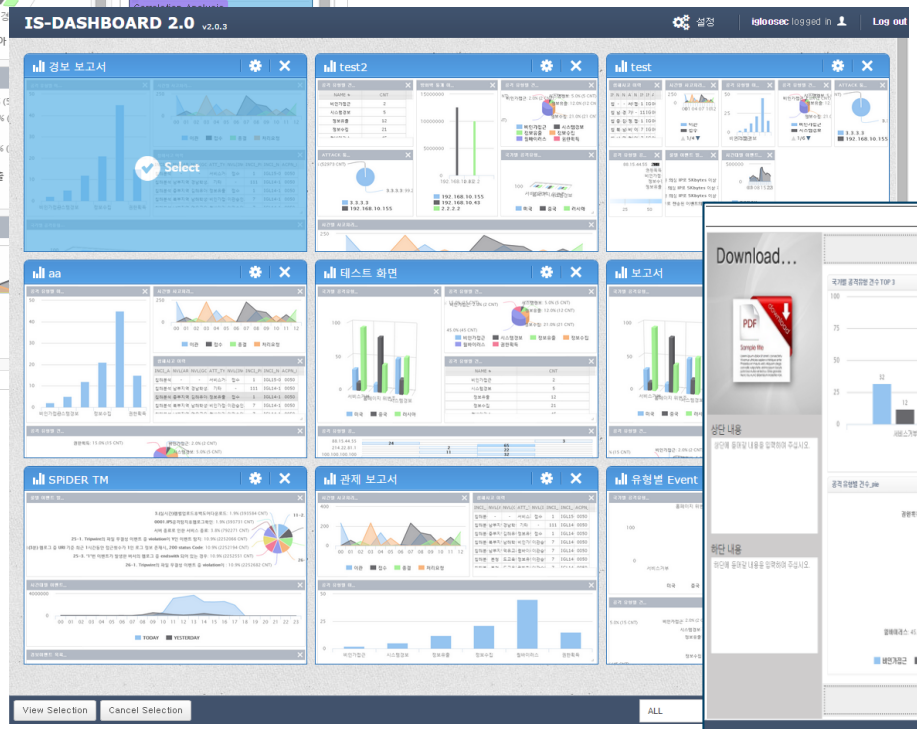
사용자 정의 대시보드 & 레포트

위젯 선택을 통한 템플릿 구현으로 사용자가 원하는 형태의 대시보드로 표출, 또한 PDF, Excel 출력 가능

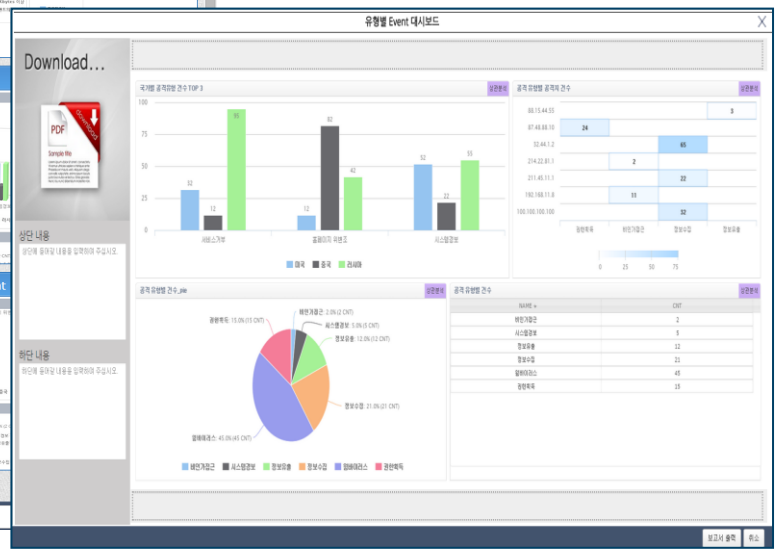
위젯 선택을 통한 템플릿 구현



템플릿을 통한 대시보드 구현



PDF, Excel 출력



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

보안관제 주요 업무

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 예방 업무

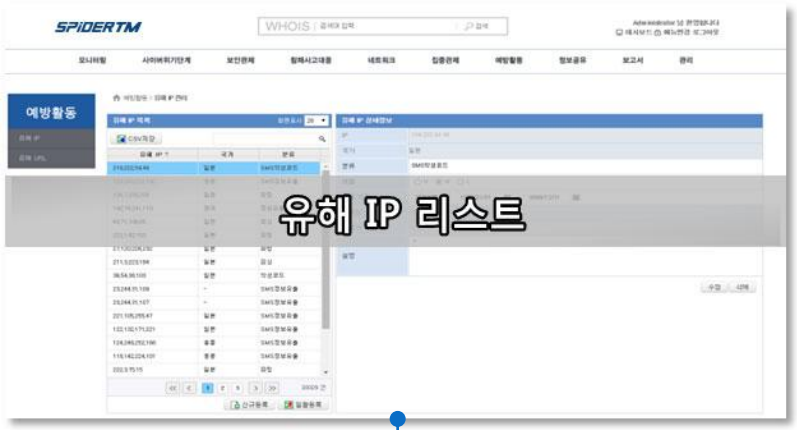
집중관제 기능을 통해 정기/모의 훈련, DDoS 대응 훈련 등 특화된 관제 업무를 제공합니다.

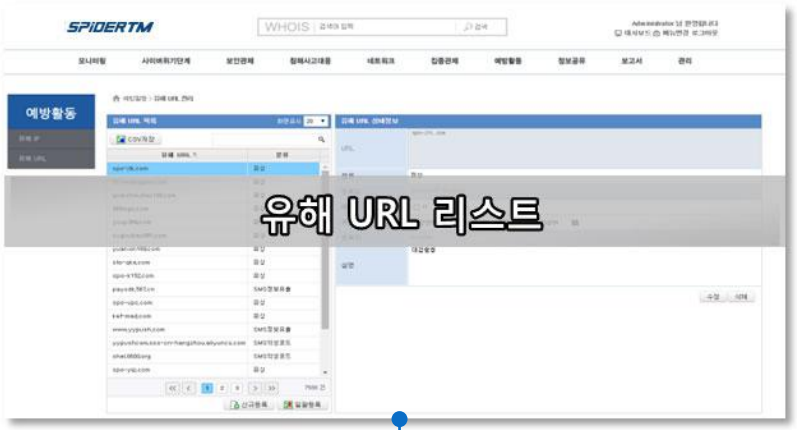
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 예방 업무

이글루시큐리티의 선행기술연구소의 악성코드 유포지 자동수집 시스템인 애플도어 시스템과 KISA에서 제공하는 유해 IP 리스트 등을 토대로 K-Center를 통해 다양한 보안위협정보를 제공합니다.





K-Center 제공 정보

유해 IP/URL	취약 포트	악성 URL
해킹 정보	취약점분석 보고서	관제 룰 셋

DB

통합보안관제시스템

KISA
한국인터넷진흥원

유해 IP 정보 등 제공

IGLOOSECURITY

DB

이글루시큐리티 K-Center

애플도어 수집시스템
(악성코드 유포지 자동 수집)

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

APPLEDORE(악성코드 경유지/유포지 추적 시스템) 일일 관측 정보

E-MAIL 제공

받는 사람 이세호

이 메시지가 표시되는 방식에 문제가 있으면 이
이 메시지는 추적된 대화의 일부입니다. 관련된

메시지 2015-04-03_malware.zip (397

이글루시큐리티 APPLEDORE (악성코

관측 기간: 2015-04-02 09:00 ~ 2015

TIME	SEED URL
2015-04-03 07:47:29	http://www.npcsh.com/
2015-04-03 02:43:21	http://www.bbosasi.com/
2015-04-02 21:37:26	http://www.insu24.net/
2015-04-02 19:14:04	http://www.npcsh.com/
2015-04-02 18:08:33	http://yhspirit.onmam.com/
2015-04-02 18:08:22	http://www.eklove.or.kr/
2015-04-02 18:06:44	http://anyangyewon.onmam.com/

정보 공유(대외 서비스)

통신·미디어

멀쩡한 홈피, 방

유명 교회·방송 관련 사

강은성 기자 esther@dt.co.kr

[2015년 03월 30일자 8면 기사]

[단독] 갤럭시S6 국내 최저가 & 사은품은 어디?

국내 유명
코드에 감
의 각별한
어도비 플

들을 대상으로 하는 파밍
있는 사실이 확인됐다"면
검 및 치료를 하고 취약점

분석 보고서(고객 서비스)

문서번호: 1503-3 애플도어 이슈 분석 보고서

1. C교회와 유명 채용 사이트 그리고 악성코드

2015년 3월 국내 서울 소재 C교회 방문자를 감염시키는 악성코드가 발견되었다. 이러한 교회 홈페이지를 통한 악성코드 감염은 최근 지속적으로 발견되고 있어, 사용자들의 각별한 주의를 요구하고 있다.

특히 이번에 발견된 악성코드 유포 체인에서 국내 유명 채용사이트의 특정 URL이 악성코드 유포 체인으로서 이용되고 있다는 점이 특이한 점이다.

공격방식의 특이한 점은, 방문자가 교회 홈페이지를 방문하게 되면, 홈페이지에서 방문자들에게 기독교 음악을 백그라운드 음악으로 틀어주고 있는데, 이 음악 재생기가 안타깝게도 악성코드로 이동하는 경로로 이용되고 있는 것이 포착되었다. (아래 그림)

<기독교 음악 BGM과 함께 전파되는 악성코드>

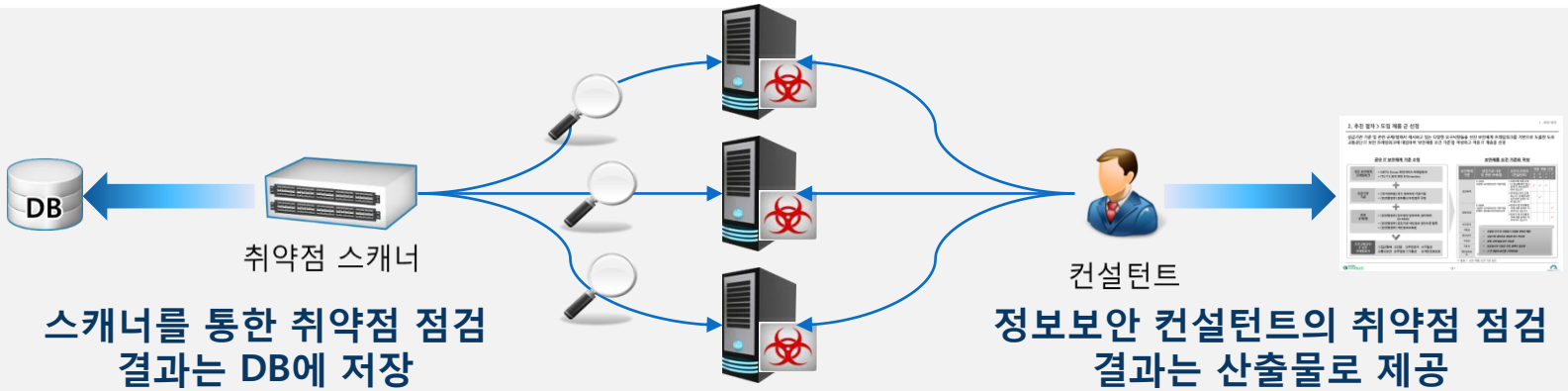
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 예방 업무

취약점 점검 결과를 분석 룰과 결합하여 보다 의미 있는 분석결과를 제공합니다. 또한 취약점 점검 스캐너가 없는 경우 자체 취약점 관리 기능을 제공하여 취약점 관리체계를 마련합니다.

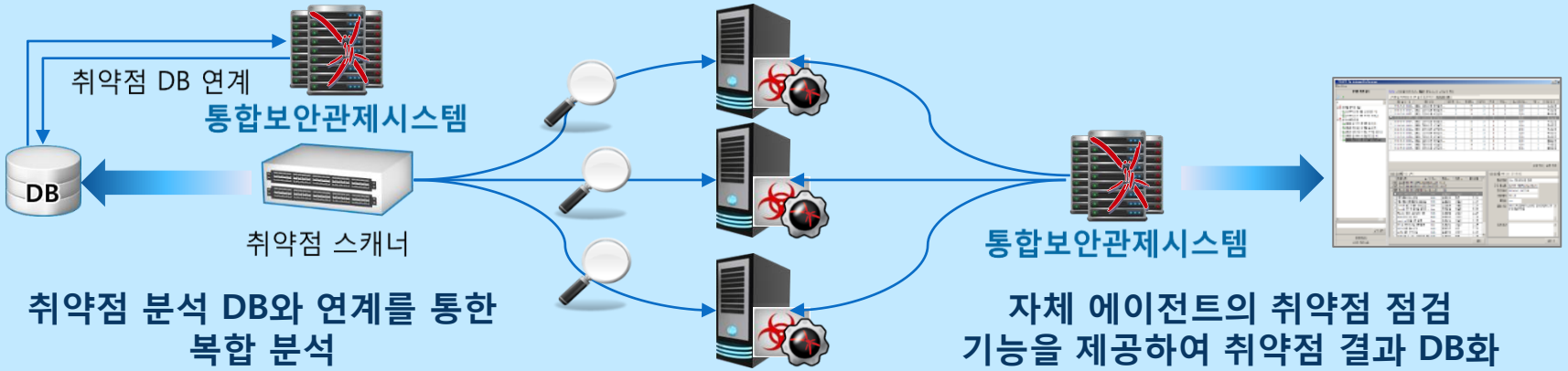
AS-IS



스캐너를 통한 취약점 점검 결과는 DB에 저장

정보보안 컨설턴트의 취약점 점검 결과는 산출물로 제공

TO-BE



취약점 분석 DB와 연계를 통한 복합 분석

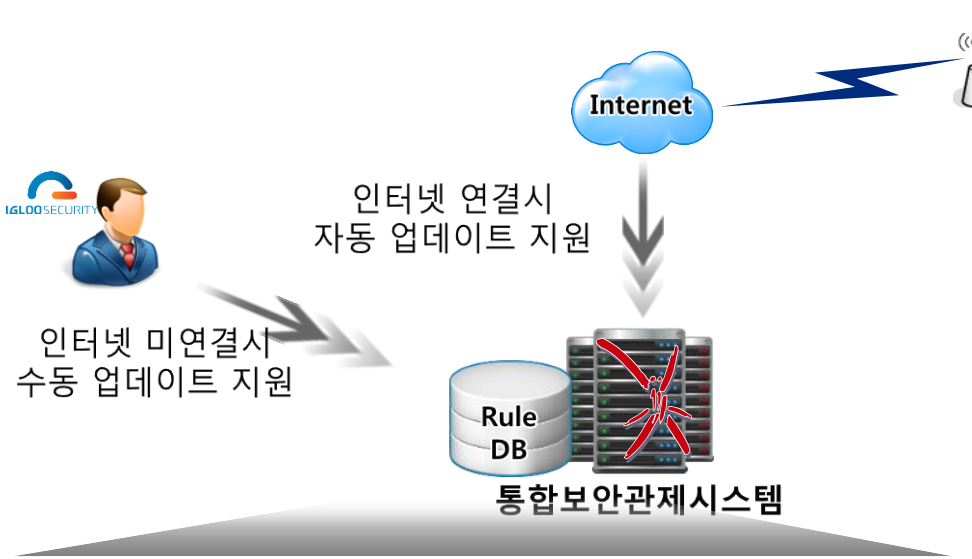
자체 에이전트의 취약점 점검 기능을 제공하여 취약점 결과 DB화

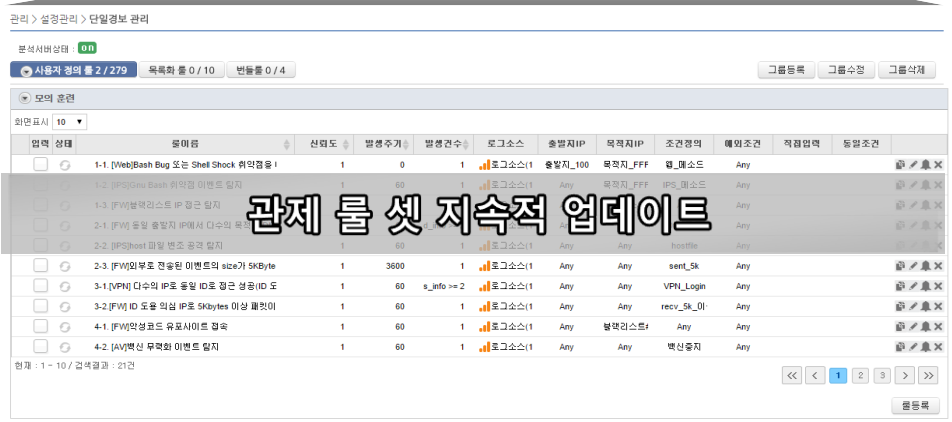
Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

차세대 통합보안관제시스템의 운영/관리 업무

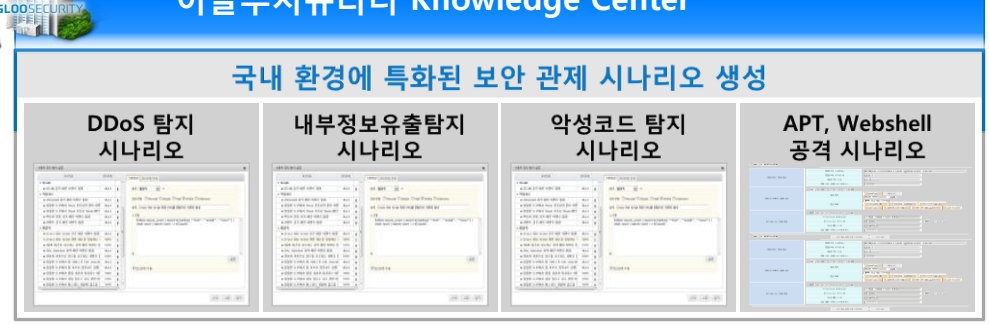
나날이 발전하는 침해공격에 대응하기 위해 자체 시나리오 TFT를 통한 지속적인 관제 룰 셋을 개발하여 고객사의 관제 룰 셋을 지속적으로 업데이트 합니다.





이글루시큐리티 Knowledge Center

국내 환경에 특화된 보안 관제 시나리오 생성



솔루션 및 시나리오가 결합된
최상의 보안관제체계 제공

시나리오 개발 TFT 상시 운영

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

Ⅲ 탐지/분석 사례

손쉬운 DDoS 분석 사례

공격 분석 흐름

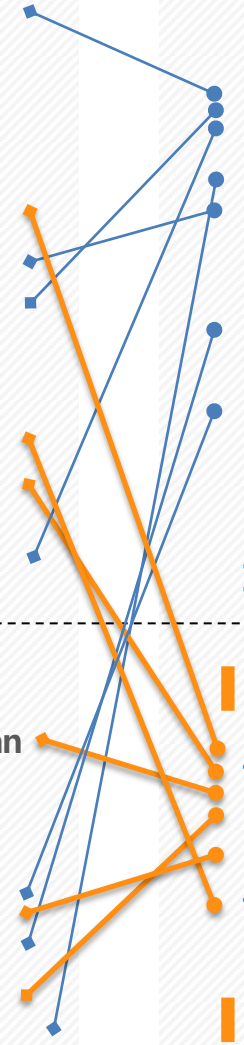
DDX
- TCP Tear Drop(60%)
- ICMP Tear Drop(38.8%)
- 그외 6가지 형태 공격 탐지

FW
- 61.139.128.99(73%)
- 192.168.12.86(24%)
- 그외 다수의 IP 접근(1~2건)

IPS
- SYN, FIN Port Scan(2%)
- x .Vulnerability(1~3건)
- UDP Source-IP Flooding(49.2%)
- UDP Destnation IP(49.2%)

WAF
- 웹상태코드 : 200
- HTR ISAPI Filter Vulnerability Scan
- Backup Files Disclosure-1 Filter

웹서버
- 웹상태코드 : 404, 414
- URI : /cat is fine too~~
  /xx.tmp, xx.bak, xx.htr, xx.inc
- Session : SYN_RCVD, FIN_WAIT2



DDoS 공격 분석

- 대역폭 소모 공격
  - 출발지IP 변조 후 TCP, UDP 프로토콜의 대량 트래픽을 발생
  - 해당 웹서버에서 확인 결과 변조 IP로 응답을 위한 syn rcvd 다수 발생
- 웹 서비스 거부 공격 (LOIC툴 공격)
  - 웹로그에 /와 cat is fine too~ 의 반복문자열
  - 웹상태코드 414 발생

INSIGHT 발견

복합공격 – 웹 취약점 Scan 공격

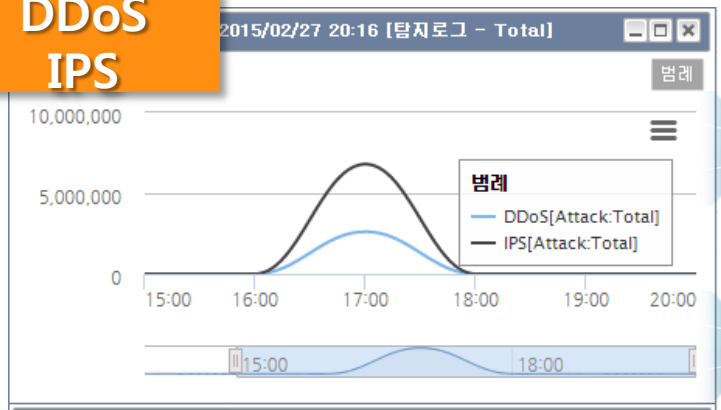
- 유해 IP로 등록된 중국 IP에서 다수 접근하여 해당 웹서버로 취약점 Scan 공격
  - 웹 상태코드 404 발생
- 추가 공격을 위한 서비스 포트 스캔

IP추적기를 통한 내부 시스템 감염 공격 발견

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

실시간 분석

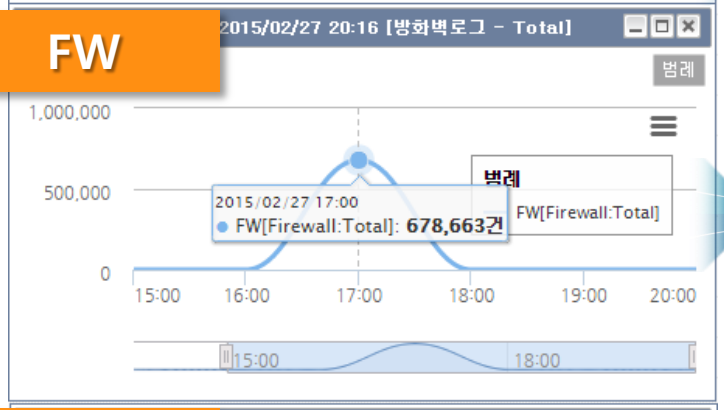
DDoS IPS



매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포	프로토콜	상태	Method
IP Invalid TTL Packet									
+ 192.168.1.100	2015/02/27 17:16:12	192.168.12.93	192.83.196.93	11	192.168.12.86	0	ICMP(1)	Pass/Detect(101)	IP Invalid TTL Pack
TCP Tear Drop									
+ 192.168.1.100	2015/02/27 17:16:20	192.168.12.93	93.4.247.117	4111	192.168.12.86	80	TCP(6)	Pass/Detect(101)	TCP Tear Drop
+ 192.168.1.100	2015/02/27 17:16:20	192.168.12.93	189.212.189.90	4209	192.168.12.86	80	TCP(6)	Pass/Detect(101)	TCP Tear Drop

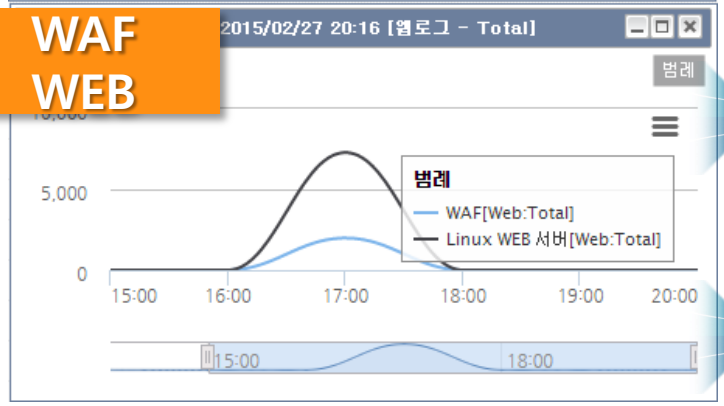
매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포	프로토콜	상태	Method
+ 192.168.1.100	2015/02/27 17:47:18	192.168.12.91	61.139.128.99	52249	192.168.12.86	80	UDP(17)	Pass/Detect	UDP Packet Flooding
+ 192.168.1.100	2015/02/27 17:47:18	192.168.12.91	61.139.128.99	52249	192.168.12.86	80	UDP(17)	Pass/Detect	UDP Destination-IP Flooding
+ 192.168.1.100	2015/02/27 17:47:18	192.168.12.91	61.139.128.99	52249	192.168.12.86	80	UDP(17)	Pass/Detect	UDP Source-IP Flooding
+ 192.168.1.100	2015/02/27 17:48:17	192.168.12.91	192.168.12.62	137	192.168.12.255	137	UDP(17)	Pass/Detect	MS WINS Server Registration S

FW



매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태
+ 192.168.1.100	2015/02/27 17:12:46	192.168.12.90	145.167.250.42	40519	192.168.12.86	80	TCP(6)	Accept(101)
+ 192.168.1.100	2015/02/27 17:12:43	192.168.12.90	159.101.92.15	38741	192.168.12.86	80	TCP(6)	Accept(101)
+ 192.168.1.100	2015/02/27 17:12:43	192.168.12.90	156.106.184.68	42513	192.168.12.86	80	TCP(6)	Accept(101)
+ 192.168.1.100	2015/02/27 17:12:46	192.168.12.90	187.171.1.241	44262	192.168.12.86	80	TCP(6)	Accept(101)

WAF WEB



매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포	프로토콜	상태	Method
+ 192.168.1.100	2015/02/27 17:35:45	192.168.12.92	61.139.128.99	52610	192.168.12.86	80	TCP(6)	OK/Accept(200)	/perl.tmp
+ 192.168.1.100	2015/02/27 17:35:45	192.168.12.92	61.139.128.99	52623	192.168.12.86	80	TCP(6)	OK/Accept(200)	/query.bak
+ 192.168.1.100	2015/02/27 17:35:45	192.168.12.92	61.139.128.99	52635	192.168.12.86	80	TCP(6)	OK/Accept(200)	/query.htr
+ 192.168.1.100	2015/02/27 17:35:45	192.168.12.92	61.139.128.99	52636	192.168.12.86	80	TCP(6)	OK/Accept(200)	/query.inc

시간	로그소스IP	출발지IP	출발지	목적지IP	목적지	프로토콜	상태	Method
2015/02/27 17:31:18	192.168.12.86	61.139.128.99	0	192.168.12.86	0	TCP(6)	Not Found(404)	/cgi-bin/~opSensePostNotThereNoNoator/ Mozi
2015/02/27 17:31:22	192.168.12.86	61.139.128.99	0	192.168.12.86	0	TCP(6)	Not Found(404)	/cgi-bin/~admin/ Mozilla/4.0 (compatible: MSIE 6
2015/02/27 17:33:07	192.168.12.86	61.139.128.99	0	192.168.12.86	0	TCP(6)	Other(999)	cat is fine too, Desudesudesu~A cat is fine too
2015/02/27 17:33:07	192.168.12.86	61.139.128.99	0	192.168.12.86	0	TCP(6)	Other(999)	cat is fine too, Desudesudesu~A cat is fine too

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

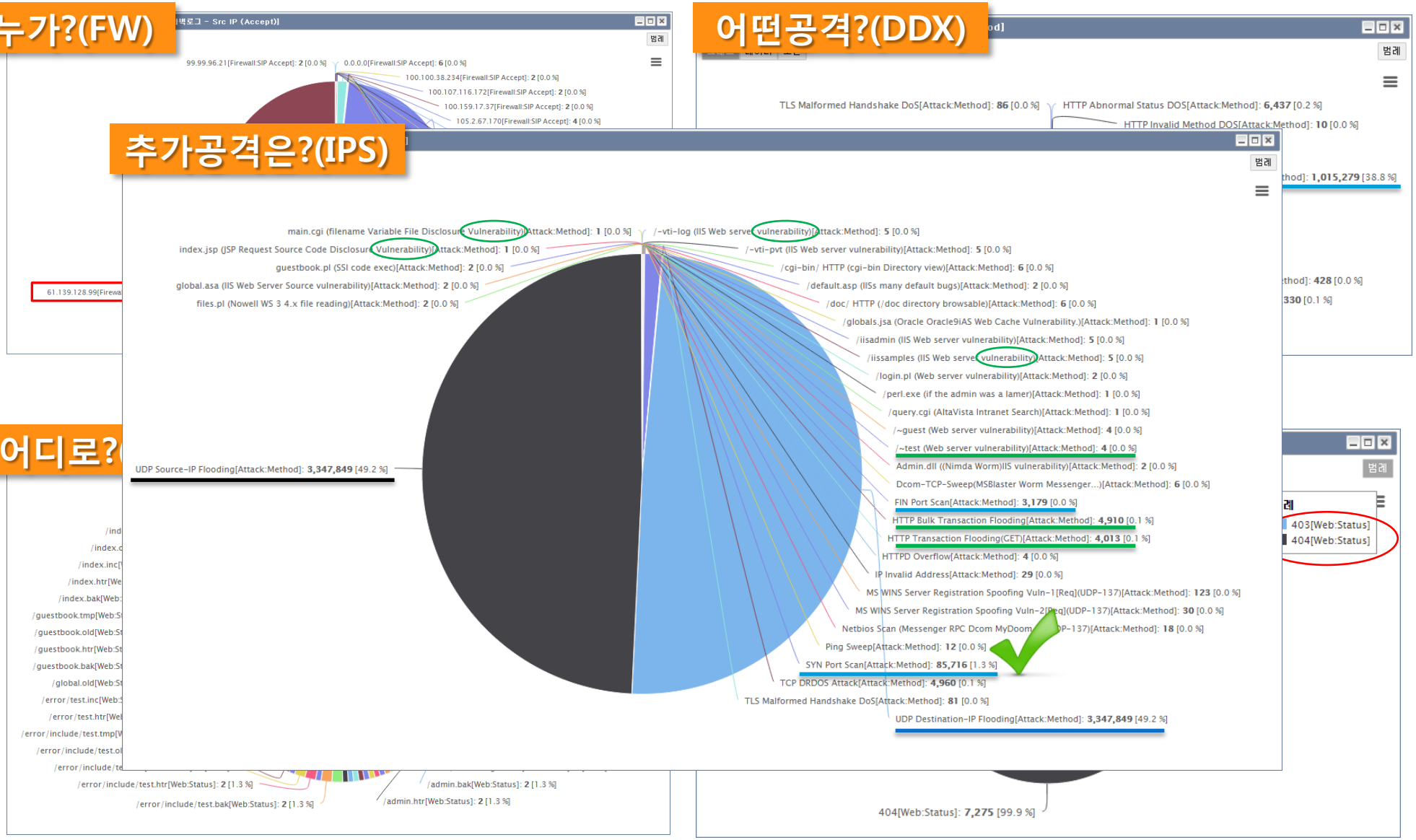
통계 분석 - 유형별

누가?(FW)

어떤공격?(DDX)

추가공격은?(IPS)

어디로?

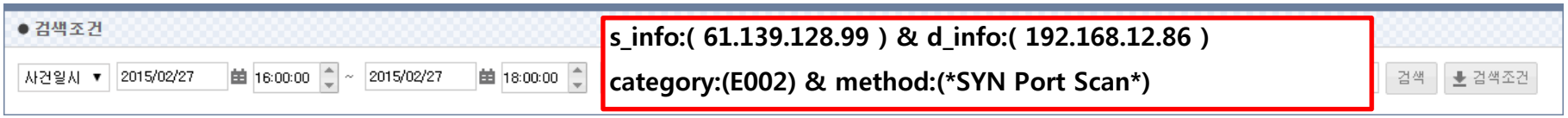


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

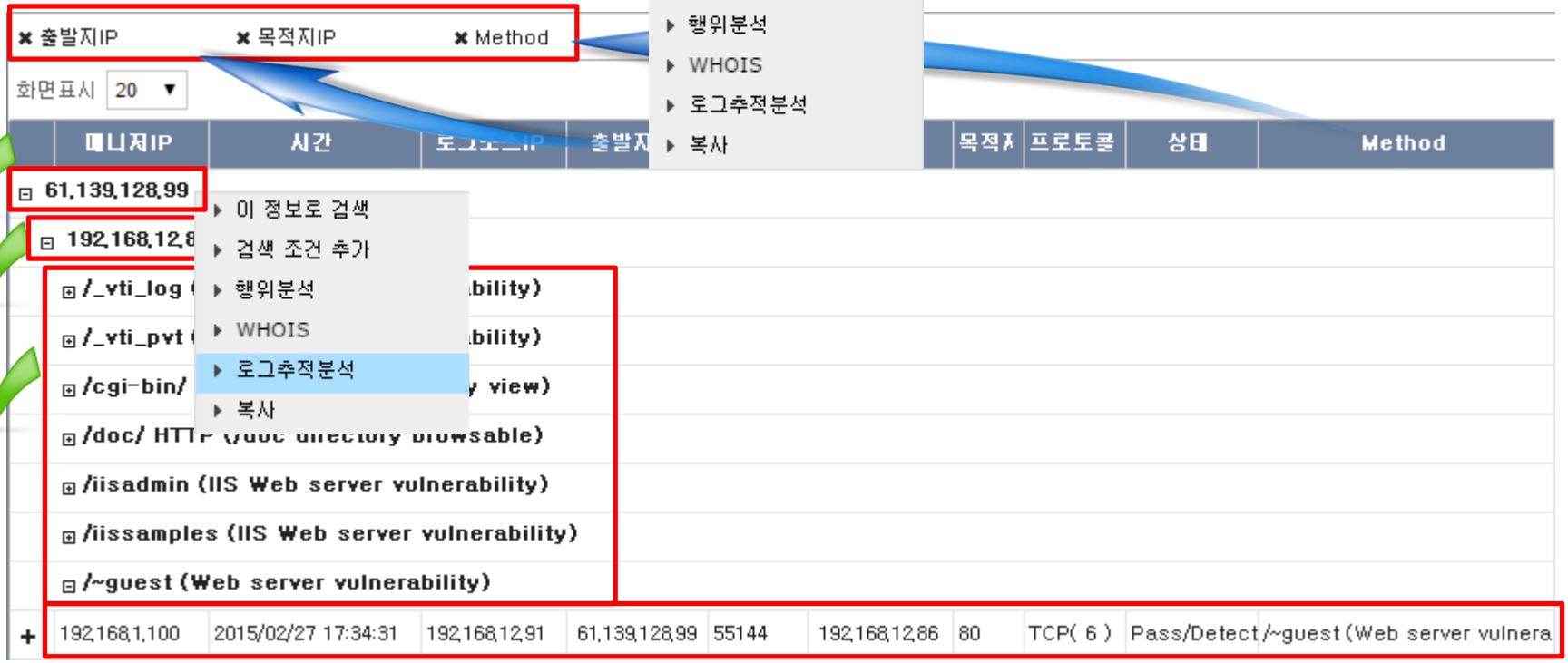
이 정보로 검색

쉬운 쿼리 검색



IPS

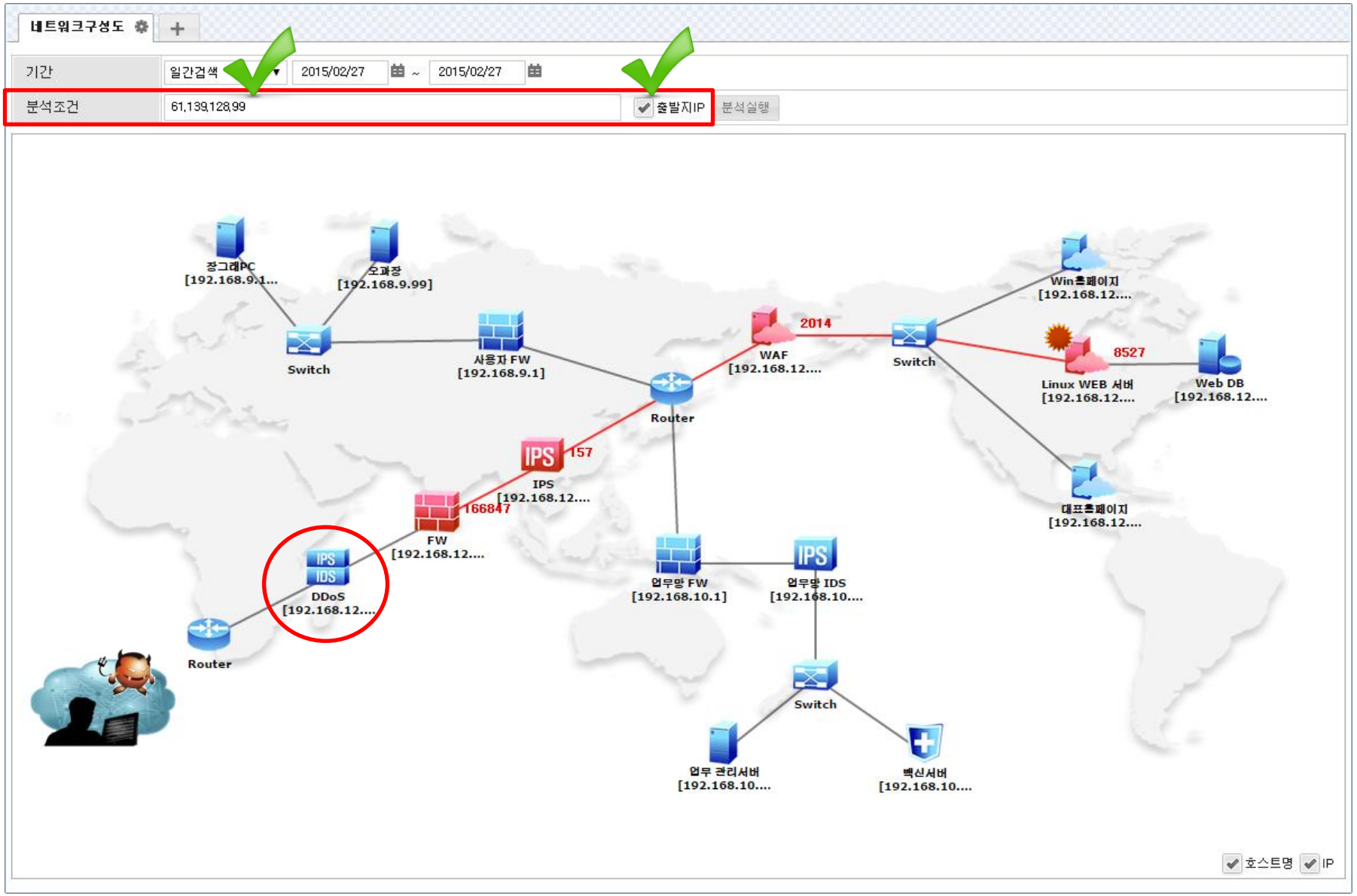
	매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
+	192.168.1.100	2015/02/27 17:39:54	192.168.12.91	61.139.128.99	56436	192.168.12.86	16	TCP(6)	Pass/Detect(101)	SYN Port Scan
+	192.168.1.100	2015/02/27 17:40:55	192.168.12.91	61.139.128.99	58360	192.168.12.86	1938	TCP(6)	Pass/Detect(101)	SYN Port Scan



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

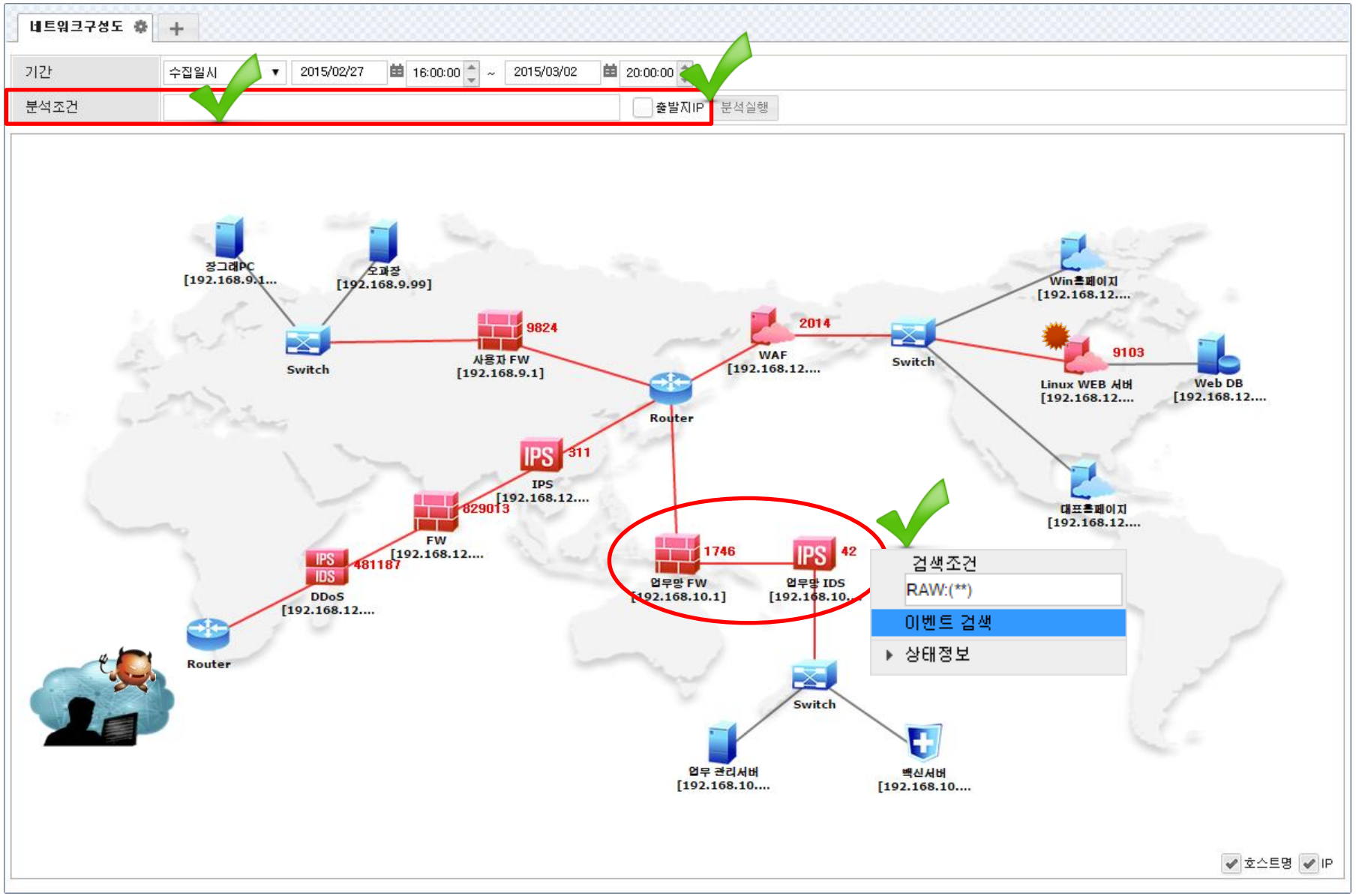
“그 중에 하나만…”



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

“한 눈에, 한꺼번에, 다같이! "



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

이벤트 검색 & 행위 분석

FW

	매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
+	192.168.1.100	2015/02/27 17:32:51	192.168.10.1	192.168.10.13	58870	192.168.12.86	80	TCP(6)	Accept(101)	null
−	192.168.1.100	2015/02/27 17:32:51	192.168.10.1	192.168.10.13	58870	192.168.12.86	80	TCP(6)	Accept(101)	null

RAW = 281:20150227 170101:192.168.12.1,100:E001:20150227 173251:192.168.10.1:4:192.168.10.13:3232238659:58870:192.168.12.86:3232238678:80:6:::101:0:0:::::- -::FW:start_time=2015-02-27 17:32:51, end_time=- -, message=Session created, rule_id=1:::1: , **d_addr** = 3232238678 , **count** = 1 , **direction** = 4 , **link** = null , **mgr_ip** = 192.168.1.100 , **id** = 20150227192652532_00000000000000049431_E_2015022719stmp_E-Secure-281 , **HASH** = 23aeaffa29cd45f23e320bd2d9068d1b38cec12e8ea8637864d61a87617ecdf2 , **risk** = 0 , **s_port** = 58870 , **d_info** = 192.168.12.86 , **user_id** = null , **d_port** = 80 , **note** = start_time=2015-02-27 17:32:51, end_time=- -, message=Session created, rule_id=1 , **evt_size** = 0 , **mgr_time** = 20150227192652532 , **protocol** = 6 , **status** = 101 , **extend** = null , **origin** = 192.168.10.1 , **s_info** = 192.168.10.13 , **ext5** = null , **product** = FW , **category** = E001 , **ext1** = null , **ext2** = null , **sequence** = 281 , **ext3** = null , **s_addr** = 3232238659 , **ext4** = - - , **event_time** = 20150227173251000 , **method** = null , **logType** = SECURE

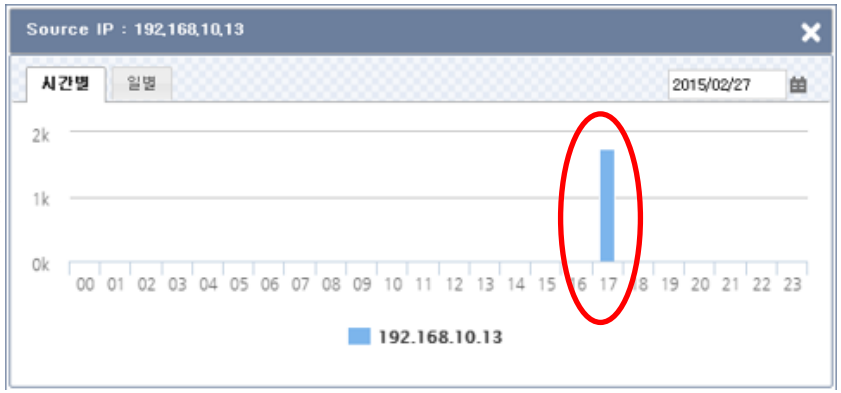
IDS

	매니저IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
+	192.168.1.100	2015/02/27 17:32:24	192.168.12.93	192.168.10.13	4787	192.168.12.86	80	TCP(6)	Pass/Detect(101)	TCP Tear Drop
+	192.168.1.100	2015/02/27 17:32:24	192.168.12.93	192.168.10.13			80	TCP(6)	Pass/Detect(101)	TCP SYN Flooding

- 이 정보로 검색
- 검색 조건 추가
- 행위분석
- WHOIS
- 로그추적분석
- 복사

서버 Session

	매니저IP	시간	로그소스IP	출발	목적지IP	목적지포트	프로토콜	상태
+	192.168.1.100	2015/02/27 17:42:59	192.168.12.86	192.168.12	139.128.99	51797	TCP(6)	SYN_RCVD
+	192.168.1.100	2015/02/27 17:42:59	192.168.12.86	192.168.12	139.128.99	51729	TCP(6)	SYN_RCVD

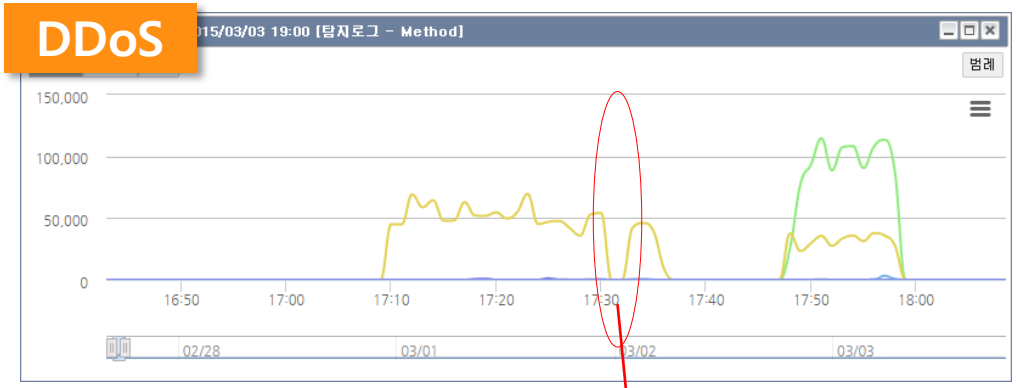


Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

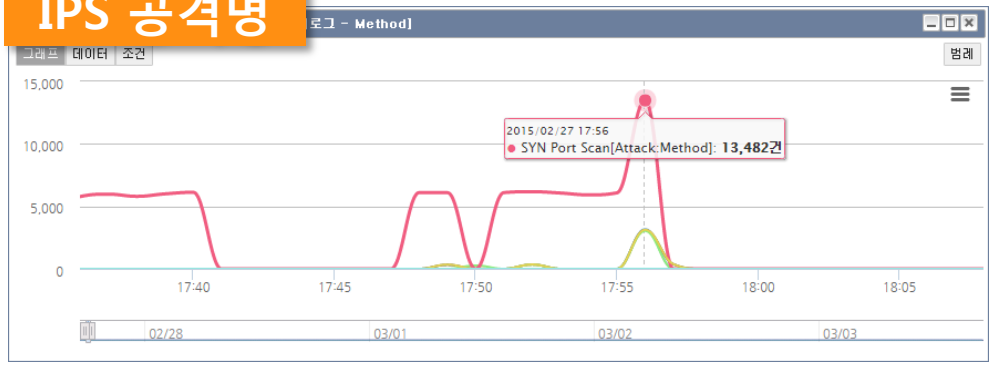
IGLOOSECURITY

시계열 분석

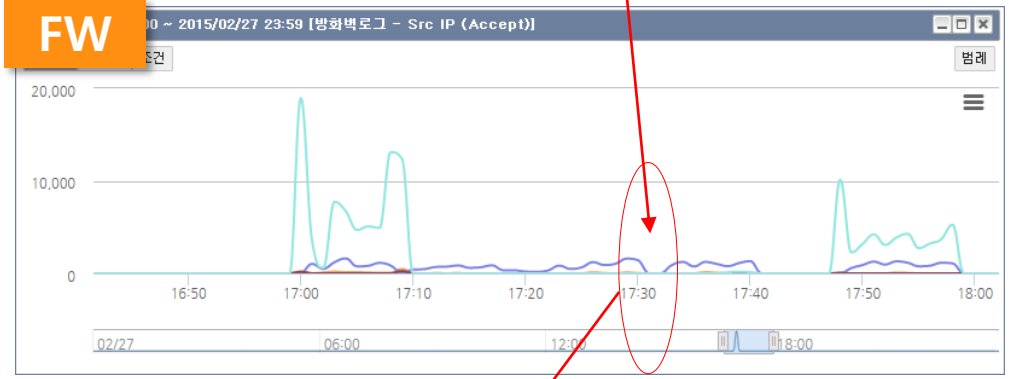
DDoS



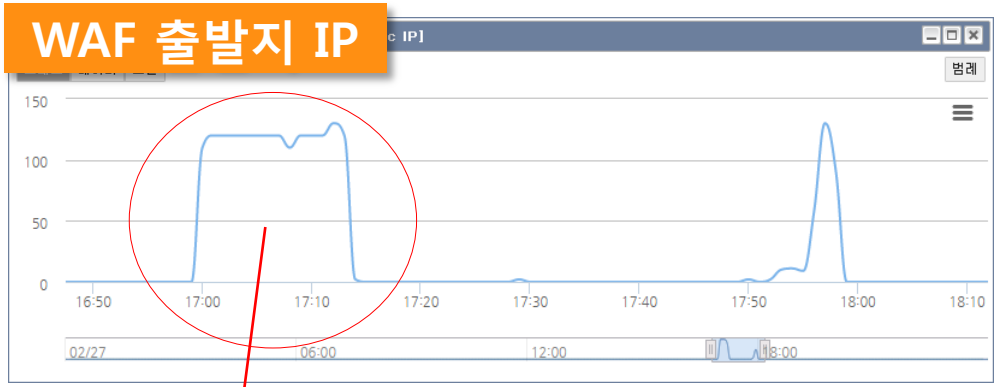
IPS 공격명



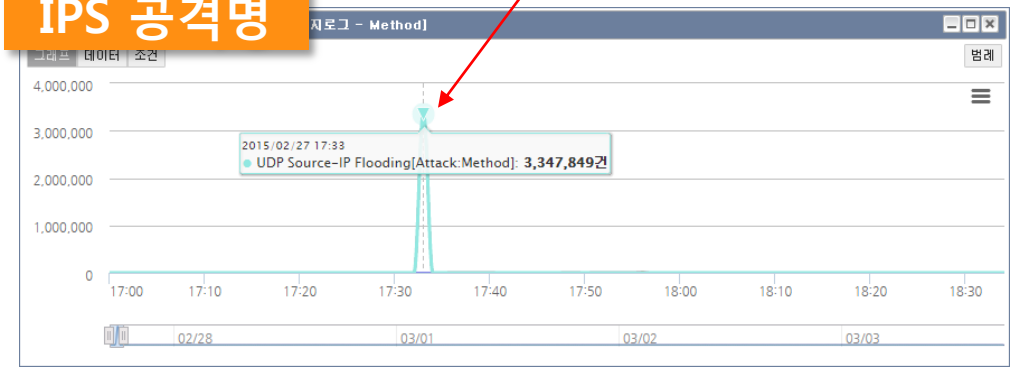
FW



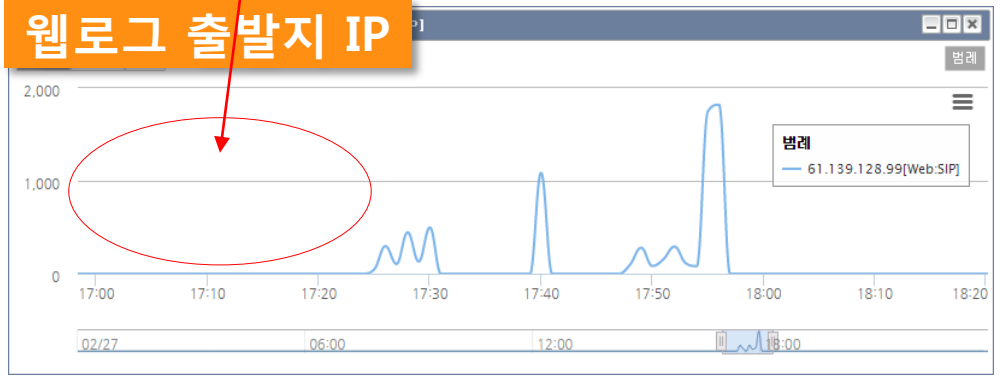
WAF 출발지 IP



IPS 공격명



웹로그 출발지 IP



Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

IV 기대 효과

차세대 통합보안관제시스템 기대효과

이글루시큐리티는 차세대 통합보안관제시스템을 통해 보안관제 업무를 성공적으로 수행할 수 있도록 지원합니다.

Copyright © IGLOO SECURITY, INC. 2015. All rights reserved.

IGLOOSECURITY

감사합니다.