

+

One Step
Ahead

한눈에, 한꺼번에, 다같이
빅데이터시대, 차세대 보안관제 프레임워크

이글루시큐리티
이세호팀장

2015. 04.16

Contents

- I. 보안당면과제
- II. 차세대 통합보안관제시스템 구성
- III. 탐지/분석 사례
- IV. 기대효과

I

보안관제 당면과제



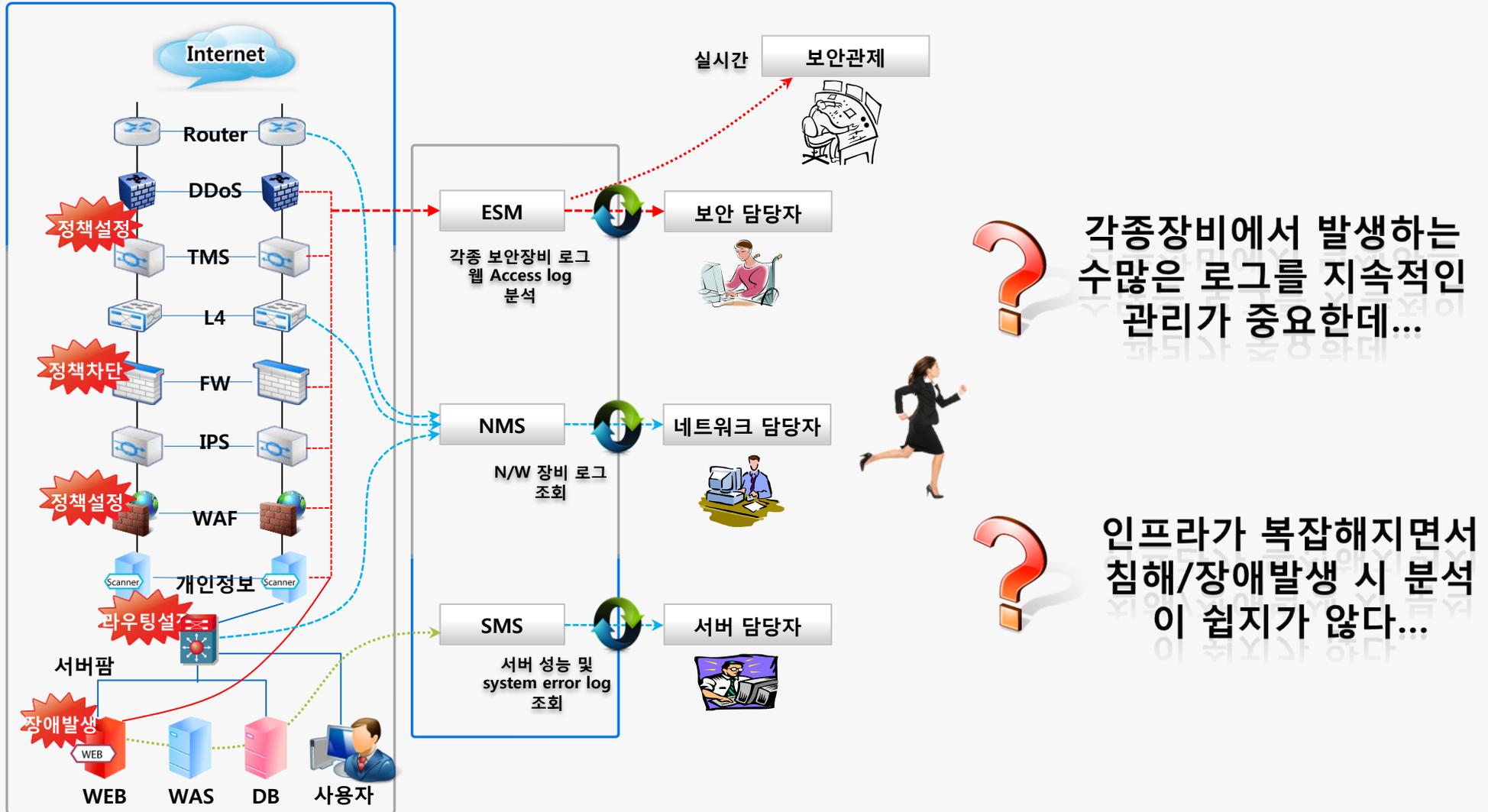
보안관제 주요 업무

보안관제 업무는 관제 업무 뿐만 아니라 다양한 보안업무도 포함하고 있습니다.

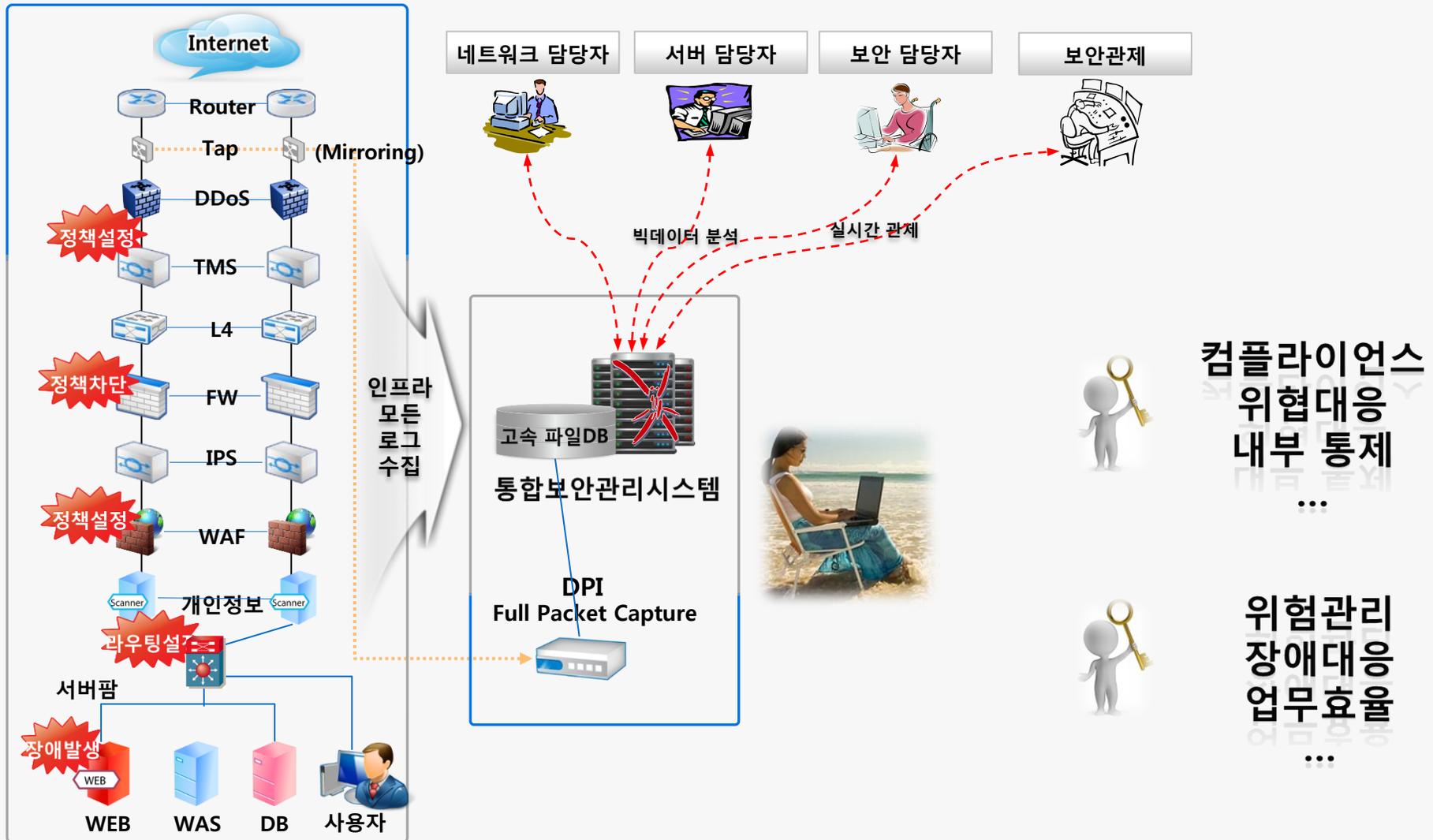


로그 운영/관리 업무의 문제점

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



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



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



지식 기반 정보 분석

내부정보 및 외부 위협정보와
같이 분석해야 한다.



BIG DATA 기반 로그 처리 기술

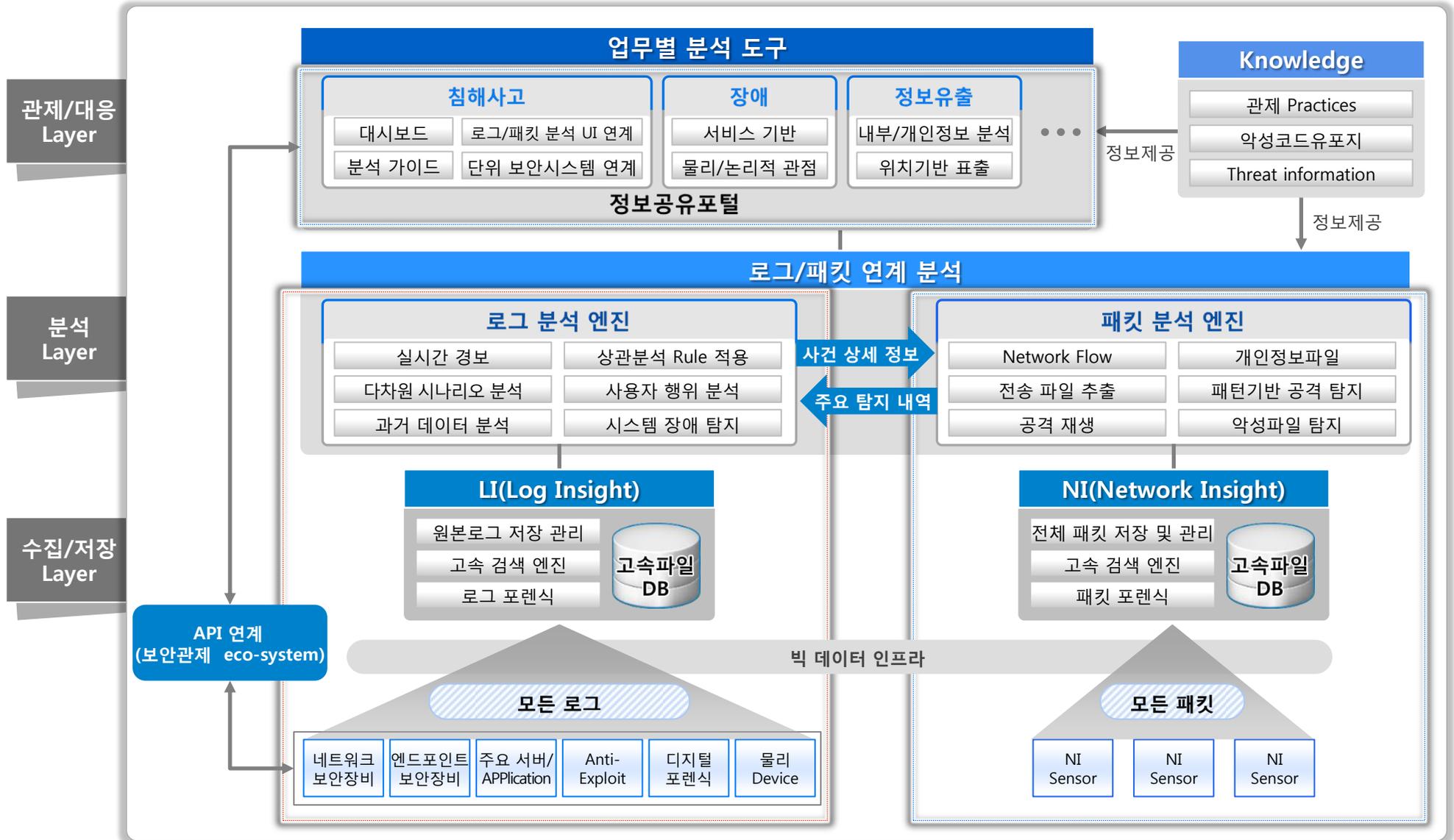
모든 로그를 수집하여
분석해야 한다.



Full Packet Capture

네트워크의 모든 패킷을 저장하고
분석해야 한다.

차세대 보안관제시스템 프레임워크



이글루시큐리티 차세대 보안관제시스템

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

SPIDERTM

WHOIS | 검색어 입력
🔍 검색

Administrator 님 환영합니다
 📄 대시보드 📄 메뉴변경 📄 로그아웃

모니터링
사이버위기단계
보안관제
침해사고대응
네트워크
집중관제
예방활동
정보공유
보고서
관리

업데이트: 2015-01-29

관심
주의
경계

정상
심각

관제요약

위기단계별 관제

침해사고 접수

보안권고문 / 상황전파문 more >

구분	대상기관	제목	접수일자
차단요청	대원초	차단요청입니다	2014.12.26
사고접수	학생교육원	ddos사고.	2014.12.24
사고접수	남해수련원	사고접수 등록	2014.12.24
사고접수	덕유교육원	확인 부탁드립니다	2014.12.24
사고접수	도교육청	사고접수	2014.12.24

최근 사고유형별 통계 일간 | 주간 | 월간

사고유형별	01/25	01/26	01/27	01/28	01/29	01/30
침해사고	0	0	0	0	0	0
차단요청	0	0	0	0	0	0
정책변경	0	0	0	0	0	0

공지 및 소식 전체 | 공지 | 예보발령 | 보안뉴스

[공지사항] 北 OS 불법에 치명적 보안 취약점 📄 2015-01-29 20:28:08.0

[공지사항] 위키리크스, 美정부에 자사 에디터 개인정보 📄 2015-01-29 20:26:49.0

[공지사항] 한.미, 사이버 공격 공동 대응 모색 📄 2015-01-29 20:26:29.0

[예보발령] [관심] 경보발령] 국가공공기관 사이버... 2015-01-29 00:00:00.0

[예보발령] [정상환원] 사이버위기 경보단계 "... 2015-01-29 00:00:00.0

Global IP Top5 정보 공격 | Signature

순위	IP	건수	대비
1	192.168.50.892	368	
2	192.168.50.892	368	
3	192.168.50.892	368	
4	192.168.50.892	368	
5	192.168.50.892	368	

< 2015년 1월 >

일	월	화	수	목	금	토
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

사고신고 대표전화 02-3452-8814

SPIDERTM

서울시 강남구 테헤란로429 원방빌딩6층 135-721 IGLOO SECURITY 전화:02-3452-8814 팩스:02-3452-8815
 COPYRIGHT 2014, IGLOO SECURITY, INC. ALL RIGHTS RESERVED.

차세대 보안관제시스템

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

The screenshot displays a comprehensive dashboard for security management, organized into several functional columns:

- 모니터링 (Monitoring):** Includes a calendar for 2015년 1월 and a 'Global IP Top5 정보' table.
- 사이버위기관제 (Cyber Incident Response):** Features a '위험도 현황' (Risk Status) section with a calendar and a 'Global IP Top5 정보' table.
- 보안관제 (Security Management):** Contains a '관제현황' (Monitoring Status) section with a calendar and a 'Global IP Top5 정보' table.
- 침해사고대응 (Incident Response):** Includes a '침해사고대응' (Incident Response) section with a calendar and a 'Global IP Top5 정보' table.
- 네트워크 (Network):** Features a '네트워크' (Network) section with a calendar and a 'Global IP Top5 정보' table.
- 집중 관제 (Concentrated Management):** Includes a '집중 관제' (Concentrated Management) section with a calendar and a 'Global IP Top5 정보' table.
- 예방활동 (Prevention Activities):** Contains a '예방활동' (Prevention Activities) section with a calendar and a 'Global IP Top5 정보' table.
- 정보공유 (Information Sharing):** Includes a '정보공유' (Information Sharing) section with a calendar and a 'Global IP Top5 정보' table.
- 보고서 (Reports):** Features a '보고서' (Reports) section with a calendar and a 'Global IP Top5 정보' table.
- 관리 (Management):** Contains a '관리' (Management) section with a calendar and a 'Global IP Top5 정보' table.

The 'Global IP Top5 정보' table is as follows:

순위	IP
1	192.168.50.892
2	192.168.50.892
3	192.168.50.892
4	192.168.50.892
5	192.168.50.892

SPIDERTM

서울시 강남구 테헤란로429 임방빌딩6층 135-721 IGLOO SECURITY 전화:02-3452-8814 팩스:02-3452-8815
COPYRIGHT 2014, IGLOO SECURITY, INC. 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.

직관적 침해/장애 이벤트

이벤트에 대한 이력관리

원격접속 및 관리페이지 접속

II 차세대 통합보안관제시스템 구성



실시간 경보 모니터링

관제 보고서 작성 웹해킹 탐지

개인/내부 정보 유출 방지

상황전파

보안장비 가용성 모니터링

DDoS 대응

침해사고 처리

홈페이지 위변조 탐지

침해사고 분석

모의 훈련

APP 취약점 점검

탐지 패턴 업데이트

정보공유

악성코

지침/매뉴얼 개정

IPS 운영 관리

정

관리

컴플라이언스

최신 보안동향 모니터링

해킹 메일 분석

유해 IP, URL 관리

보안관제 업무

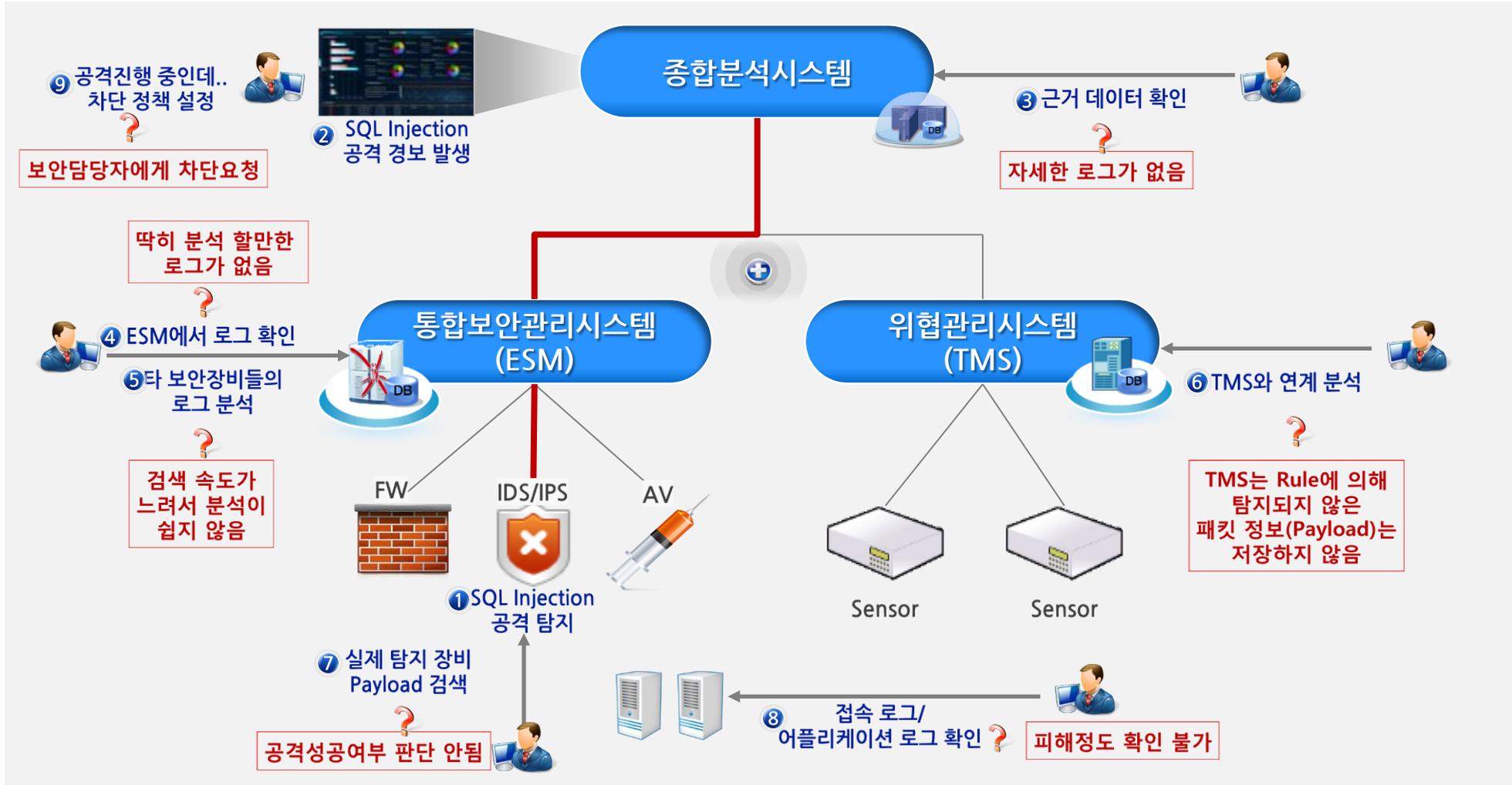


탐지/분석
/대응

기존 보안관제시스템의 문제점

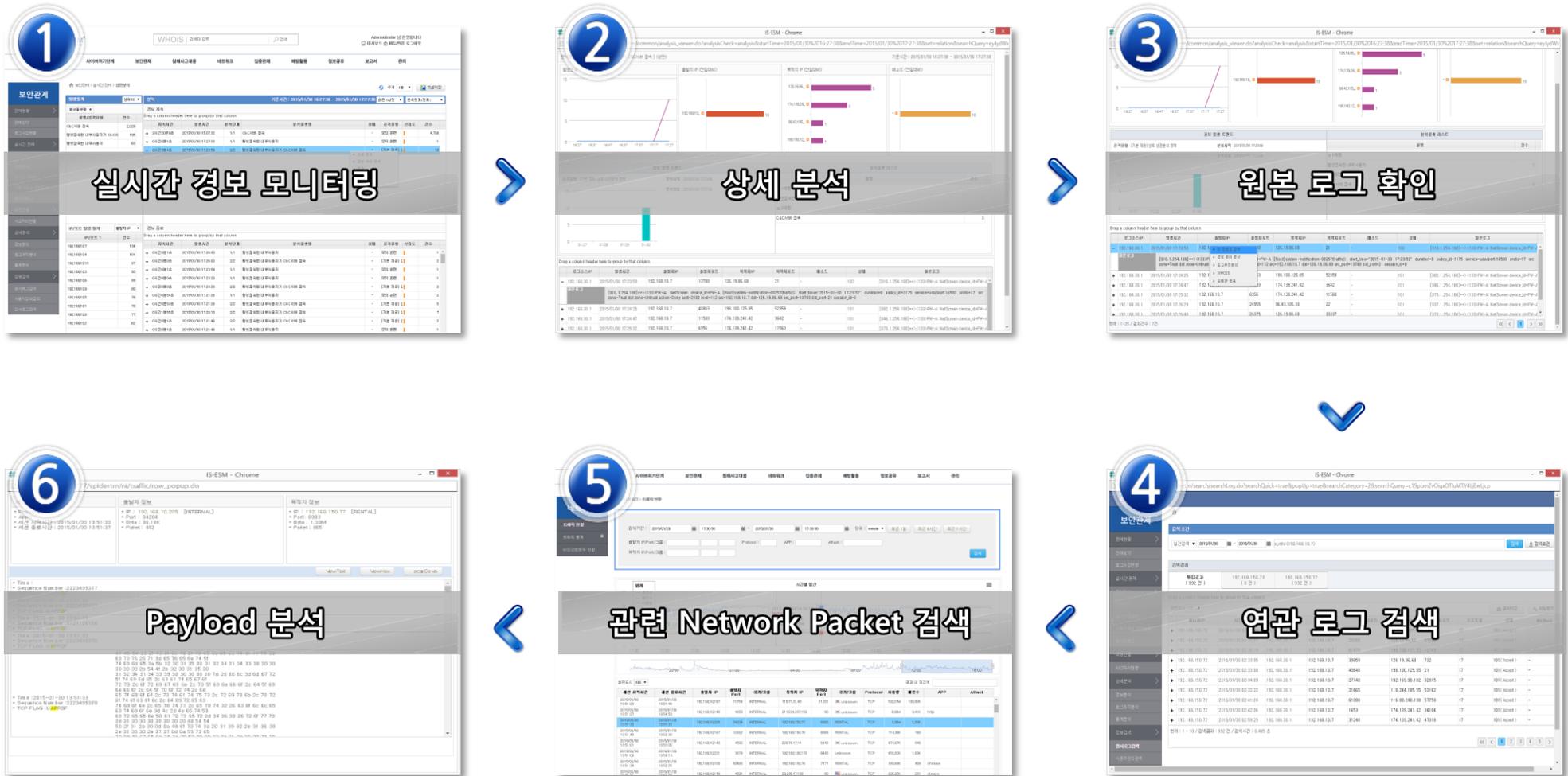
탐지분석대응

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



차세대 통합보안관제시스템의 탐지/분석 업무

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



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	<ul style="list-style-type: none"> In-Memory 방식 	<ul style="list-style-type: none"> In-Memory 방식
분석 시간	<ul style="list-style-type: none"> 1분 	<ul style="list-style-type: none"> 시간에 상관 없음(초/분/시/일/주/월까지 가능)
분석 데이터	<ul style="list-style-type: none"> 실시간 데이터 	<ul style="list-style-type: none"> 실시간 데이터 + 과거 데이터
분석 방법	<ul style="list-style-type: none"> 정해진 필드에 대한 단순 패턴 매칭 (특정 시그니처, 임계치 등) 	<ul style="list-style-type: none"> 모든 필드에 대한 다양한 분석 (패턴, 임계치, 연산자 등 복합 분석)
시나리오 분석	<ul style="list-style-type: none"> 미지원 	<ul style="list-style-type: none"> 단계 별 시나리오 분석 지원



차세대 통합보안관제시스템의 탐지/분석 업무

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



SPIDERTM

WHOIS | 검색어 입력

검색

Administrator 님 환영합니다
대시보드 메뉴변경 로그아웃

모니터링 사이버위기관제 보안관제 침해사고대응 네트워크 집중관제 예방활동 정보공유 보고서 관리

- 보안관제
- 관제현황 >
- 관제 요약
- 로그수집현황
- 실시간 관제 >
- 통합관제
- 상관분석
- 실시간 유해 IP
- 사용자 중심 위반행위
- 실시간로그
- 대응현황 >
- 사고처리현황
- 상세분석 >
- 경보분석
- 로그추적분석
- 통계분석
- 정보검색 >
- 원시로그검색
- 사용자정의검색
- 감사로그검색

보안관제 > 실시간 관제 > 상관분석

주기 1분 엑셀저장

발생단계 상위 10

분석종류명	건수
로명/공격유형	2,028
C&C서버 접속	195
탈넷접속한 내부사용자가 C&C서	63
탈넷접속한 내부사용자	

공격유형 별 Top N

분석 기준시간 : 2015/01/30 16:27:38 ~ 2015/01/30 17:27:38 최근 1시간 분석단계(전체)

경보 지속

Drag a column header here to group by that column

	지속시간	발생시간	분석단계	분석종류명	상태	공격유형	신뢰도	건수
+	2시간20분0초	2015/01/30 15:07:32	1/1	C&C서버 접속	-	모의 훈련		4,768
+	0시간0분1초	2015/01/30 17:27:03	1/1	탈넷접속한 내부사용자	-	모의 훈련		1
+	0시간3분4초	2015/01/30 17:23:59	2/2	탈넷접속한 내부사용자가 C&C서버 접속	-	모의 훈련		10

지속되는 경보 리스트

IP/포트 발생 통계 출발지 IP

IP/포트 수	건수
192.168.10.7	134
192.168.10.4	101
192.168.10.10	97
192.168.10.3	93
192.168.10.6	89
192.168.10.1	80
192.168.10.5	78
192.168.10.1	78
192.168.10.8	77
192.168.10.2	62

IP/Port 별 Top N

경보 종료

Drag a column header here to group by that column

	지속시간	발생시간	분석단계	분석종류명	상태	공격유형	신뢰도	건수
+	0시간0분1초	2015/01/30 17:26:00	1/1	탈넷접속한 내부사용자	-	모의 훈련		1
+	0시간0분0초	2015/01/30 17:26:00	2/2	탈넷접속한 내부사용자가 C&C서버 접속	-	[기본 제공] >		2
+	0시간0분1초	2015/01/30 17:23:59	1/1	탈넷접속한 내부사용자	-	모의 훈련		1
+	0시간0분0초	2015/01/30 17:23:20	1/1	탈넷접속한 내부사용자	-	모의 훈련		1
+	0시간0분0초	2015/01/30 17:23:20	2/2	탈넷접속한 내부사용자가 C&C서버 접속	-	[기본 제공] >		2
+	0시간0분54초	2015/01/30 17:21:26	1/1	탈넷접속한 내부사용자	-	모의 훈련		2
+	0시간0분53초	2015/01/30 17:21:26	2/2	탈넷접속한 내부사용자가 C&C서버 접속	-	[기본 제공] >		5
+	0시간1분55초	2015/01/30 17:20:10	2/2	탈넷접속한 내부사용자가 C&C서버 접속	-	[기본 제공] >		7
+	0시간0분1초	2015/01/30 17:21:46	2/2	탈넷접속한 내부사용자가 C&C서버 접속	-	[기본 제공] >		2
+	0시간0분1초	2015/01/30 17:21:46	1/1	탈넷접속한 내부사용자	-	모의 훈련		1

종료된 경보 리스트

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.

탐지/분석 [텔넷접속한 내부사용자가 C&C서버 접속] (상관)
기준시간 : 2015/01/30 16:27:38 ~ 2015/01/30 17:27:38

2

경보의 발생 추이

출발지 IP (전일대비)

전일 대비 출발지 IP 건수

목적지 IP (전일대비)

전일 대비 목적지 IP 건수

메소드 (전일대비)

전일 대비 메소드 건수

경보 발생 트렌드

경보 발생 트렌드

분석룰셋 리스트

룰명	건수
1레벨	
텔넷접속한 내부사용자	2
2레벨	
C&C서버 접속	8

분석 룰 셋 리스트 및 탐지건수

Drag a column header here to group by that column

그로스IP	발생시간	출발지IP	출발지포트	목적지IP	목적지포트	메소드	상태	원본로그
192.168.30.1	2015/01/30 17:23:59	192.168.10.7	13780	126.19.86.68	21	-	102	[010.1.254.188]==><133>FW-A: NetScreen device_id=FW-A
<div style="border: 1px solid gray; padding: 2px; display: inline-block;"> <ul style="list-style-type: none"> 이 정보로 검색 경보 추이 분석 로그추적분석 WHOIS 유해IP 등록 </div>								
+	192.168.30.1	2015/01/30 17:24:25	192.168.10.7	198.100.125.85	52359	-	101	[082.1.254.188]==><133>FW-A: NetScreen device_id=FW-A
+	192.168.30.1	2015/01/30 17:24:47	192.168.10.7	174.139.241.42	11560	-	101	[046.1.254.188]==><133>FW-A: NetScreen device_id=FW-A
+	192.168.30.1	2015/01/30 17:25:32	192.168.10.7	174.139.241.42	11560	-	101	[073.1.254.188]==><133>FW-A: NetScreen device_id=FW-A

원본로그 형태의 근거 데이터

차세대 통합보안관제시스템의 탐지/분석 업무

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

- 4
- 안관제
- 관제현황 >
- 관제요약
- 로그수집현황
- 실시간 관제 >
- 통합관제
- 상관분석
- 실시간 유해IP
- 사용자중심 위반행위
- 실시간로그
- 대응현황 >
- 사고처리현황
- 상세분석 >
- 경보분석
- 로그추적분석
- 통계분석
- 정보검색 >
- 원시로그검색
- 사용자정의검색
- 감사로그검색

검색조건

일간검색
2015/01/30
부터
2015/01/30
까지
s_info:(192.168.10.7)
검색
↓ 검색조건

연계 검색 조건이 자동으로 적용되어 검색

통합결과 (1,382 건)	192.168.150.73 (0 건)	192.168.150.72 (1,382 건)								
---------------------	---------------------------	-------------------------------	--	--	--	--	--	--	--	--

Drag a column header here to group by that column

화면표시 10
결과저장
파일저장

-	내리지IP	시간(E)	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
-	192.168.150.72	2015/01/30 02:34:40	192.168.30.1	192.168.10.7	200	198.100.125.85	43600	17	101 (Accept)	-
RAW = [028.1.254.188]==><133>FW-A: NetScreen device_id=FW-A [Root]system-notification-00257(traffic): start_time="2015-01-30 02:34:40" duration=0 policy_id=1064 service=dns proto=17 src zone=Trust dst zone=Trust action=Permit sent=2560000 rcvd=32155 src=192.168.10.7 dst=198.100.125.85 src_port=200 dst_port=43600 src-xlated ip=130.1.242.176 port=63572 dst-xlated ip=130.1.240.101 port=53 session_id=516376 reason=Creation , reason = Creation , direction = 4 , xnotel = src zone=Trust dst zone=Trust , mgr_ip = 192.168.150.72 , user_id2 = 516376 , id = 20150130023440825_000000000055288237_20150130.log_L-NetScreen72-379 , HASH = 00e914396e20bdba3135ccf1a249aeacf323997a741eadc85984cb12da2b9061 , risk = 0 , ext1_port = 63572 , s_port = 200 , user_id = null , rcvd = 32155 , d_info = 198.100.125.85 , d_port = 43600 , exd2_port = 53 , protocol = 17 , mgr_time = 20150130023440824 , status = 101 , origin = 192.168.30.1 , s_info = 192.168.10.7 , duration = 0 , category = E001 , exd1 = 130.1.242.176 , exd2 = 130.1.240.101 , exd4 = 1064 , xstatus = Permit , event_time = 20150130023440000 , sent_size = 2560000 , logType = Firewall										
+	192.168.150.72	2015/01/30 02:35:07	192.168.30.1	192.168.10.7	20265	126.19.86.68	57986	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:36:19	192.168.30.1	192.168.10.7	61970	198.100.125.85	12745	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:33:05	192.168.30.1	192.168.10.7	39859	126.19.86.68	732	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:33:00	192.168.30.1	192.168.10.7	43648	198.100.125.85	21	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:34:09	192.168.30.1	192.168.10.7	27740	192.169.98.182	32815	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:32:22	192.168.30.1	192.168.10.7	21665	118.244.185.55	53162	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:41:24	192.168.30.1	192.168.10.7	61088	116.80.248.138	57758	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:42:06	192.168.30.1	192.168.10.7	1653	174.139.241.42	34184	17	101 (Accept)	-
+	192.168.150.72	2015/01/30 02:59:25	192.168.30.1	192.168.10.7	31248	174.139.241.42	47318	17	101 (Accept)	-

현재 : 1 - 10 / 검색결과 : 1,382 건 / 검색시간 : 0.296 초

검색 결과에 대해 원본로그 형태와 파싱된 형태를 모두 제공

1
2
3
4
5
>
>>

과거에는....

시작시간	종료시간	유지시간 (초)	발생 장비	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	192.168.20.53	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

원니지IP	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)	-

원본로그
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 , time = 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 , ext2 = 31 , ext3 = null , ext4 = 내부 , event_time = 20150227170309000 , day = 20150227 , rule_id = 71 , in_nic = eth10 , mgr_time = 20150302212114183_0000000000001562001_20150302log_L-TrusGuardUTM-FW-285 , HASH = 07ab15f0eda8df3f32da88a5f6a30bbce2dd9876e , name = 71 , 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 , rule_code = 141211170602 , duration = null , dnat_type = null , rule_code = 141211170602 , logType = SECURE

참지와 분석의 핵심 정보

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

	메시지IP	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 09:13:25	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 09:13:25	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 > >>

차세대 통합보안관제시스템의 대응/사고처리 업무

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



대응/사고처리 업무 : 사고 접수

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



WHOIS | 검색어 입력 | |

Administrator님 환영합니다
 대시보드 홈 메뉴변경 로그아웃

모니터링
사이버위기단계
보안관제
침해사고대응
네트워크
집중관제
예방활동
정보공유
보고서
관리

침해사고대응

사고처리현황

사고접수

사고이관

사고대응

승인처리

침해사고대응 > 사고접수

접수일자: 2015/01/30 00:00 ~ 2015/01/30 17:34

경보명

분류: 전체

경보단계

공격자IP

공격기권/국가

목적지IP

목적지기권/국가

목적지포트

▶ 미접수 목록

<input type="checkbox"/>	접수방법	접수일시	분류	경보명	경보단계
<input checked="" type="checkbox"/>	자동접수	2013-07-02 00:00	백도어	동일한 소스 IP 에서	주의
<input type="checkbox"/>	수동접수	2012-11-29 14:15	서비스거부공격	기상형 전산망에서	경계
<input type="checkbox"/>	수동접수	2012-10-16 14:15	서비스거부공격	[기상형 신고] 불	심각
<input type="checkbox"/>	자동접수	2011-03-28 20:45	비인가접근	비인가접근으로 판	경계
<input type="checkbox"/>	자동접수	2010-10-14 00:00	서비스거부공격	http robot.tx	주의
<input type="checkbox"/>	자동접수	2010-07-15 14:00	웜/바이러스	m alware-downloa	주의
<input type="checkbox"/>	자동접수	2010-07-15 09:32	웜/바이러스	m alware-downloa	정상
<input type="checkbox"/>	자동접수	2010-07-15 06:11	백도어	dev-trojan-cn(bali	주의
<input type="checkbox"/>	반자동접수	2010-07-14 17:35	웜/바이러스	m alware-downloa	심각
<input type="checkbox"/>	자동접수	2010-07-14 17:15	악해킹	attack-web-zero	경계
<input type="checkbox"/>	반자동접수	2010-07-14 13:55	웜/바이러스	m alware-downloa	주의
<input type="checkbox"/>	반자동접수	2010-07-14 13:35	웜/바이러스	m alware-downloa	관심
<input type="checkbox"/>	반자동접수	2010-07-14 11:34	웜/바이러스	m alware-downloa	정상
<input type="checkbox"/>	반자동접수	2010-07-14 10:57	웜/바이러스	m alware-downloa	경계

기본정보

구분	침해사고
사고일자	2013-07-02 00:00 ~ 2013-07-02 00:01
접수방법	자동접수
분류	백도어

사고정보

경보명	동일한 소스 IP 에서 웹 포트로 원격코드 실행
경보단계	주의
공격자 IP	211.45.162.86
공격 기권/국가	/KR
목적지 IP	10.153.82.11
목적지 기권/국가	/
목적지 port	8100
경보내용	포트 공격발생으로 인한 초동분석 요청

침해사고 정보

네트워크 패킷

관련로그

사고가이드

네트워크 패킷 관련로그 사고가이드

대응/사고처리 업무 : 사고 이관

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



Administrator 님 환영합니다
대시보드 홈 메뉴변경 로그아웃

모니터링
사이버위기단계
보안관제
침해사고대응
네트워크
집중관제
예방활동
정보공유
보고서
관리

침해사고대응

- 사고처리현황
- 사고접수
- 사고이관
- 사고대응
- 승인처리

침해사고대응 > 사고이관

접수일자: 2015/01/30 00:00 ~ 2015/01/30 17:36
검색

경보명: [전체]

분류: [전체]

경보단계: [전체]

접수방법: [전체]

구분: [전체]

검색

접수 목록

접수방법	접수일자	분류	경보명	경보단계
자동접수	2013-07-02 00:00	백도어	동일한 소스 IP 에서	주의
접수	2012-11-29 14:19	서비스거부공격	기상청 전산망에서	경계
접수	2012-10-16 14:19	서비스거부공격	[기상청 신고] 통신	심각
접수	2011-03-28 20:49	비인가접근	비인가접근으로 판단	경계
접수	2010-10-14 00:00	서비스거부공격	http robot.14	주의
접수	2010-07-15 14:00	침사이러스	malware-download	주의

기본정보

구분	침해사고	사고일자	2013-07-02 00:00 ~ 2013-07-02 00:01
접수방법	자동접수	분류	백도어
접수일자	2013-07-02 00:00		
접수자	홍길동		
관리번호	T13-0703001		
처리상태	접수완료		

사고정보

경보명	동일한 소스 IP 에서 웹 포트로 원격코드 실행
경보단계	주의
공격자 IP	211.45.162.86
공격 기관/국가	/KR
목적지 IP	10.153.82.11
목적지 기관/국가	/
목적지 port	8100
경보내용	포트 공격발생으로 인한 초동분석 요청

첨부파일

관계센터	이글루시큐리티_대응요청.pdf
대상기관	이글루시큐리티_대응결과.pdf

수정 | 이관 | 오탐

기본정보

구분: 침해사고

사고일자: 2015/02/02 00:00 ~ 2015/02/02 14:16

접수방법: 수동접수

분류: 전체

접수일자: 2015/02/02 00:00 ~ 2015/02/02 14:16

관리번호: []

처리상태: 접수

사고정보

경보명: []

경보단계: []

공격자 IP: []

공격 기관: []

목적지 IP: []

목적지 기관: []

사고 수정

이관처리

오탐처리

이관

오탐

수정

이관

오탐

네트워크 패킷

관련로그

사고가이드

대응/사고처리 업무 : 사고 대응

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

3

SPIDERTM

WHOIS | 검색어 입력

검색

Administrator 님 환영합니다
대시보드 홈 메뉴변경 로그아웃

모니터링

사이버위기관계

보안관제

침해사고대응

네트워크

집중관제

예방활동

정보공유

보고서

관리

침해사고대응

- 사고처리현황
- 사고접수
- 사고이관
- 사고대응
- 승인처리

침해사고대응 > 사고대응

접수일자: 2015/01/30 00:00 ~ 2015/01/30 17:37

경보명: 전체

분류: 전체

경보단계: 전체

접수방법: 전체

구분: 전체

처리상태: 전체

검색

접수방법 수	접수일시	분류	경보명	경보단계	처리상태
1	2015-01-27 03:51	IPS ATTACK	서비스 거부 공격	심각	접수완료
1	2015-01-26 03:51	DDos	서비스 거부 공격	심각	접수완료
1	2015-01-26 03:51	DDos	서비스 거부 공격	위험	접수완료
1	2015-01-25 03:51	DDos	서비스 거부 공격	심각	접수완료
1	2015-01-25 03:51	Backdoor	서비스 거부 공격	심각	접수완료
1	2015-01-25 03:51	DDos	서비스 거부 공격	심각	접수완료

기본정보 Basis Information

구분	침해사고	사고일자	2013-07-02 00:00 ~ 2013-07-02 00:01
접수방법	자동접수	분류	백도어
접수일자	2013-07-02 00:00	접수자	홍길동
관리번호	T13-0703001	처리상태	접수완료
이관요청자	홍길동	이관승인자	홍길동
이관대상기관	상원교육지원청		
이관사유	침해사고 이벤트가 발생하였습니다.		

사고정보 Incident Information

경보명	동일한 소스 IP 에서 웹 포트로 원격코드 실행
경보단계	주의
공격자 IP	211.45.162.86
공격 기관/국가	/KR
유정자 IP	10.153.82.11

사고이력 Incident History

유해사고분석	공격자분석	피해분석
접수방법	접수일시	분류
자동접수	2015-01-27 03:51	IPS ATTACK
자동접수	2015-01-26 03:51	DDos
수동접수	2015-01-26 03:51	DDos
자동접수	2015-01-25 03:51	DDos
자동접수	2015-01-25 03:51	Backdoor
수동접수	2015-01-25 03:51	DDos

사건 반려

접수된 사고의
대응 완료에
따른
종결요청

종결요청 반려 네트워크 패킷 관련로그 사고가이드

대응/사고처리 업무 : 승인 처리

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

4

SPIDER™

WHOIS | 검색어 입력
🔍 검색

Administrator 님 환영합니다
 ☰ 대시보드 홈 메뉴변경 로그아웃

모니터링
사이버위기관계
보안관제
침해사고대응
네트워크
집중관제
예방활동
정보공유
보고서
관리

- 침해사고대응
- 사고처리현황
 - 사고접수
 - 사고이관
 - 사고대응
 - 승인처리

🏠 침해사고대응 > 승인처리

접수일자: 2015/01/30 00:00 ~ 2015/01/30 17:39

경보명: [전체]

분류: [전체]

경보단계: [전체]

접수방법: [전체]

구분: [전체]

처리상태: [전체]

승인 처리

[검색] [↶]

▶ 승인 대상 목록

접수방법	접수일시	분류	경보명	경보단계	처리상태
<input checked="" type="checkbox"/>	2013-07-02 00:00	백도어	동일한 소스 IP	주의	접수완료
<input type="checkbox"/>	2012-11-29 14:00	서비스거부공격	기상청 전산망에	경계	접수완료
<input type="checkbox"/>	2012-10-16 14:00	서비스거부공격	[기상청 신고]	심각	접수완료

기본정보 Basis Information

구분	침해사고	사고일자	2013-07-02 00:00 ~ 2013-07-02 00:01
접수방법	자동접수	분류	백도어
접수일자	2013-07-02 00:00	접수자	홍길동
관리번호	T13-0703001	처리상태	접수완료
이관요청자	홍길동	이관승인자	홍길동
이관대상기관	상원교육지원청		
이관사유	침해사고 이벤트가 발생하였습니다.		

사고정보 Incident Information

경보명	동일한 소스 IP 에서 웹 포트로 원격코드 실행
경보단계	주의
공격자 IP	211.45.162.86
공격 기관/국가	/KR
목적지 IP	10.153.82.11
목적지 기관/국가	/
목적지 port	8100
경보내용	포트 공격발생으로 인한 초동분석 요청

대응정보 Response Information

조치사항	DDoS 대응장비 현황확인, 설정변경완료
사고의원인	신규 DDoS 유형 공격 발생

첨부파일 Attached File

관계센터	이글루시큐리티_대응요청.pdf
------	------------------

138.74.134.7777의 페이지 내용:

사고 최종 승인

[확인] [취소]

반려요청

[재검] [취소]

대응/사고처리 업무 : 침해사고 전체 처리 현황

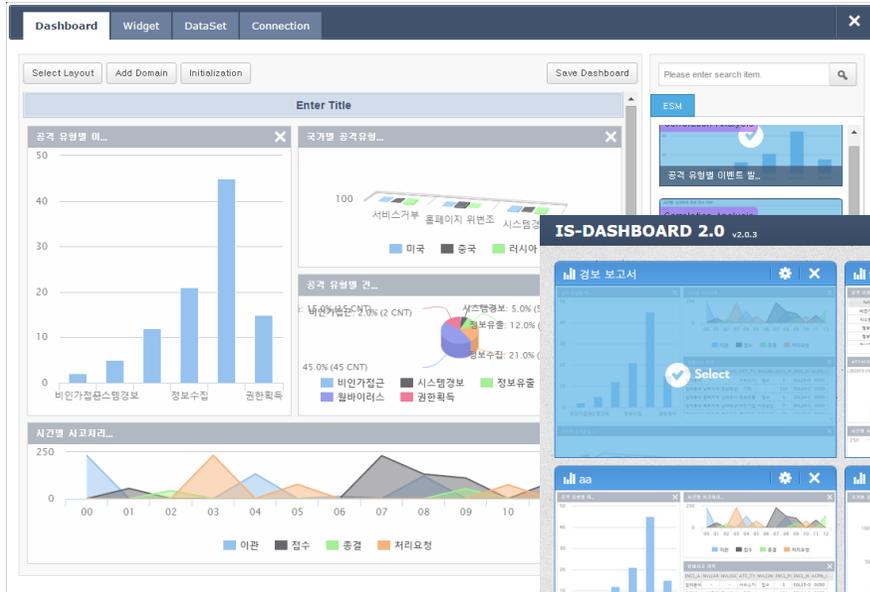
전반적인 침해사고현황 및 사고처리현황을 제공하여 현재 발생된 위협의 건수와 처리 현황을 한눈에 확인할 수 있습니다.



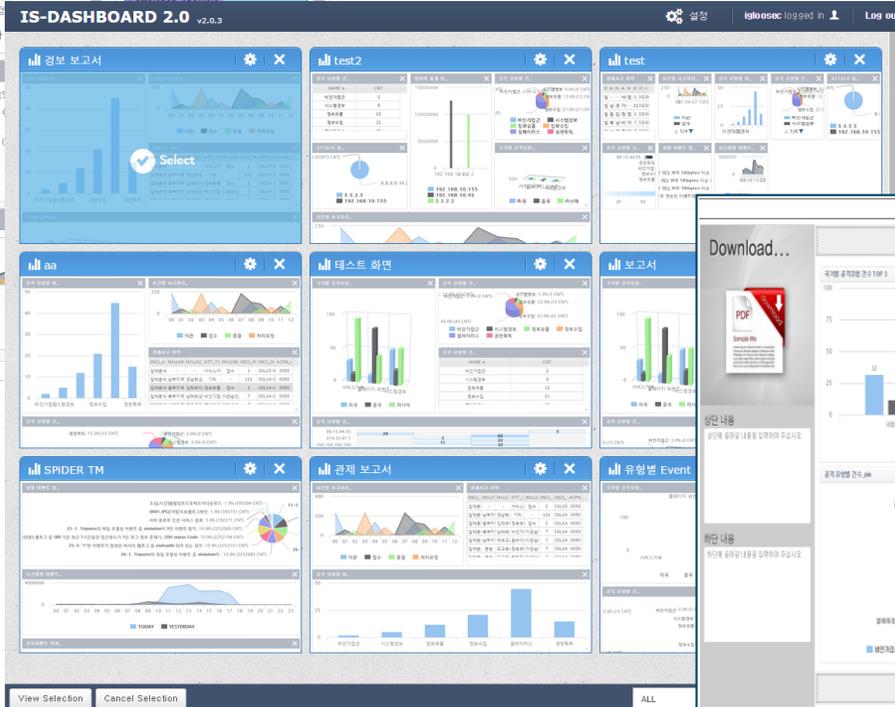
사용자 정의 대시보드 & 레포트

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

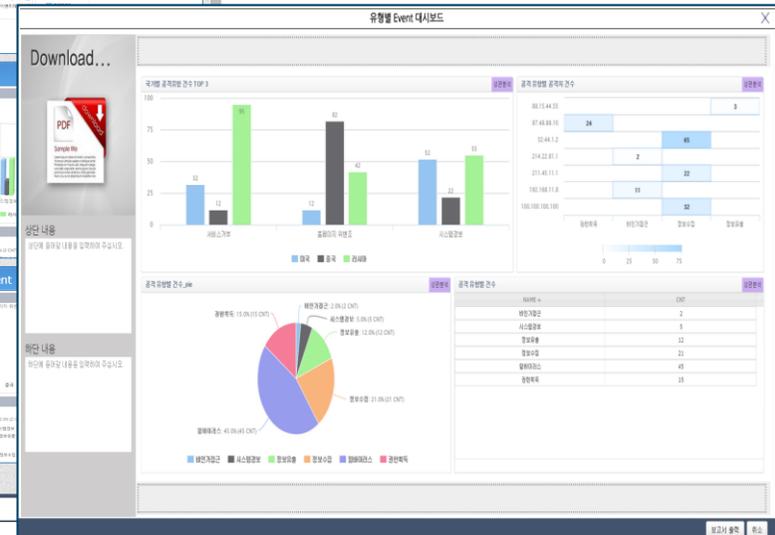
위젯 선택을 통한 템플릿 구현



템플릿을 통한 대시보드 구현



PDF, Excel 출력





차세대 통합보안관제시스템의 예방 업무

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

SPIDERTM

WHOIS | 검색어 입력

검색

Administrator 님 환영합니다
대시보드 홈 메뉴변경 로그아웃

모니터링

사이버위기단계

보안관제

침해사고대응

네트워크

집중관제

예방활동

정보공유

보고서

관리

집중관제

위기단계별 관제

최근 이슈 대응

정기 훈련

모의 훈련

DDoS 대응 훈련

집중관제 > 위기단계별 관제

업데이트 : 2015-01-19



국가사이버안전센터

- [공지사항] 北 OS 불법에 치명적 보안 취약... 2015-01-29 20:28:08.0
- [공지사항] 위키리크스, 美정부에 자사 예디... 2015-01-29 20:26:49.0
- [공지사항] 한,미, 사이버 공격 공동 대응 모... 2015-01-29 20:26:29.0
- [예보발령] [정상환원] 사이버위기 경보단계... 2015-01-19 00:00:00.0
- [보안뉴스] 리눅스 '고스트' 취약점, 보안업계... 2015-01-16 20:36:22.0

현재 위협등급



보안관제센터 대응현황

- [공지사항] 北 OS 불법에 치명적 보안 취약... 2015-01-29 20:28:08.0
- [공지사항] 위키리크스, 美정부에 자사 예디... 2015-01-29 20:26:49.0
- [공지사항] 한,미, 사이버 공격 공동 대응 모... 2015-01-29 20:26:29.0
- [예보발령] [정상환원] 사이버위기 경보단계... 2015-01-19 00:00:00.0
- [보안뉴스] 리눅스 '고스트' 취약점, 보안업계... 2015-01-16 20:36:22.0

금일 보안경고문 / 상황전파문

- [공지사항] 北 OS 불법에 치명적 보안 취약... 2015-01-29 20:28:08.0
- [공지사항] 위키리크스, 美정부에 자사 예디... 2015-01-29 20:26:49.0
- [공지사항] 한,미, 사이버 공격 공동 대응 모... 2015-01-29 20:26:29.0
- [예보발령] [정상환원] 사이버위기 경보단계... 2015-01-19 00:00:00.0
- [보안뉴스] 리눅스 '고스트' 취약점, 보안업계... 2015-01-16 20:36:22.0

국 / 내 외 실시간 뉴스

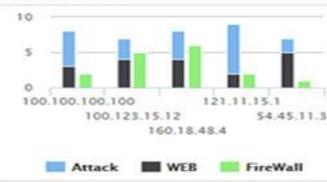
- [공지사항] 北 OS 불법에 치명적 보안 취약... 2015-01-29 20:28:08.0
- [공지사항] 위키리크스, 美정부에 자사 예디... 2015-01-29 20:26:49.0
- [공지사항] 한,미, 사이버 공격 공동 대응 모... 2015-01-29 20:26:29.0
- [예보발령] [정상환원] 사이버위기 경보단계... 2015-01-19 00:00:00.0
- [보안뉴스] 리눅스 '고스트' 취약점, 보안업계... 2015-01-16 20:36:22.0

현황 집중 모니터링

장비 트래픽



시스템 리스소



서비스



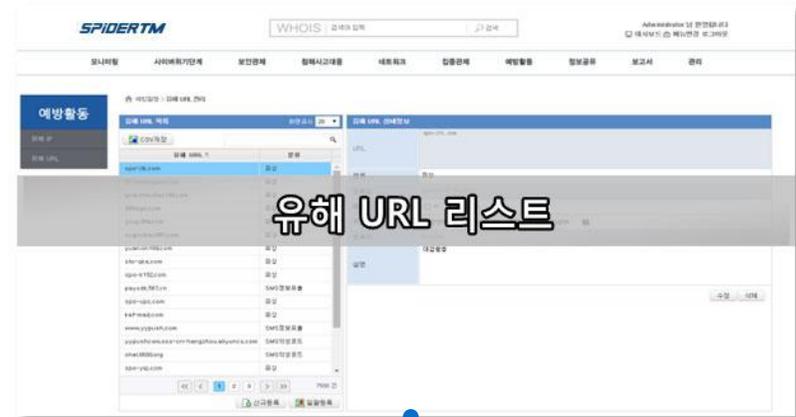
경보 / 이벤트 집중 관제

관제 - 외부

발생시간	분석단계	분석물셋명	상태	공격유형	신뢰도	건수
+ 0시간이전1초	1/1	파괴물테스트	-	비인가접근시		18
+ 0시간이전0초	1/1	프로세스 체크 - telnet	-	변동		10
+ 0시간이전0초	1/1	프로세스 체크 - oracle	-	변동		10
+ 0시간이전0초	1/1	프로세스 체크 - oracle	-	변동		10
+ 0시간이전0초	1/1	프로세스 체크 - telnet	-	변동		10
+ 0시간이전0초	1/1	Ping Check - 플랫폼개발팀	-	변동		1
+ 0시간이전0초	1/1	프로세스 체크 - telnet	-	변동		10
+ 0시간이전0초	1/1	프로세스 체크 - oracle	-	변동		10

차세대 통합보안관제시스템의 예방 업무

이글루시큐리티의 선형기술연구소의 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



KISA
한국인터넷진흥원
유해 IP 정보 등
제공



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

E-MAIL 제공

받는 사람 이세호
 이 메시지가 표시되는 방식에 문제가 있으면 이 메시지는 추적된 대화의 일부입니다. 관련된
 메시지 2015-04-03_malware.zip (397

이글루시큐리티 APPLEDORE (악성
 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://anyangvewon.onmam.com/

정보 공유(대외 서비스)

통신·미디어

멸절한 흠피, 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 이번엔 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)

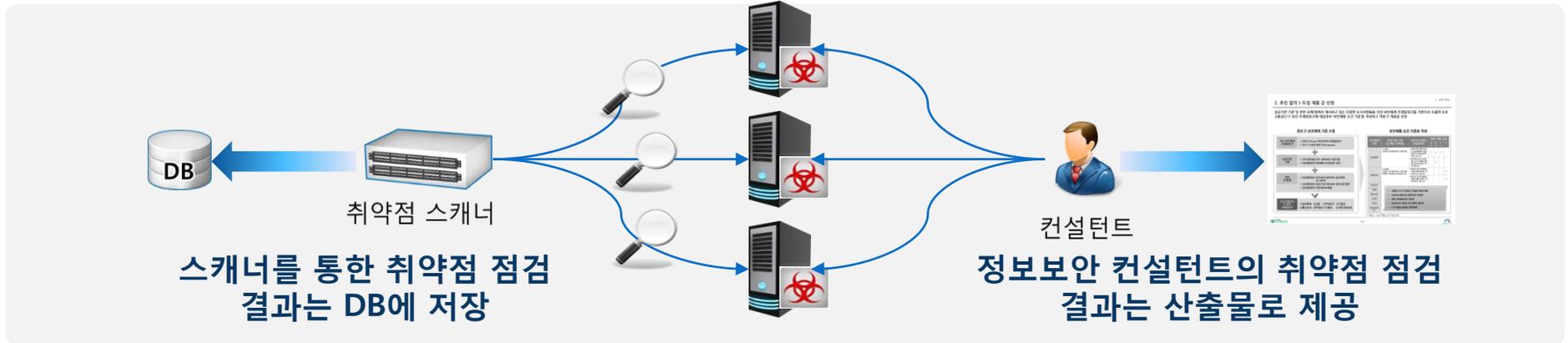


<기독교 음악 BGM과 함께 전파되는 악성코드>

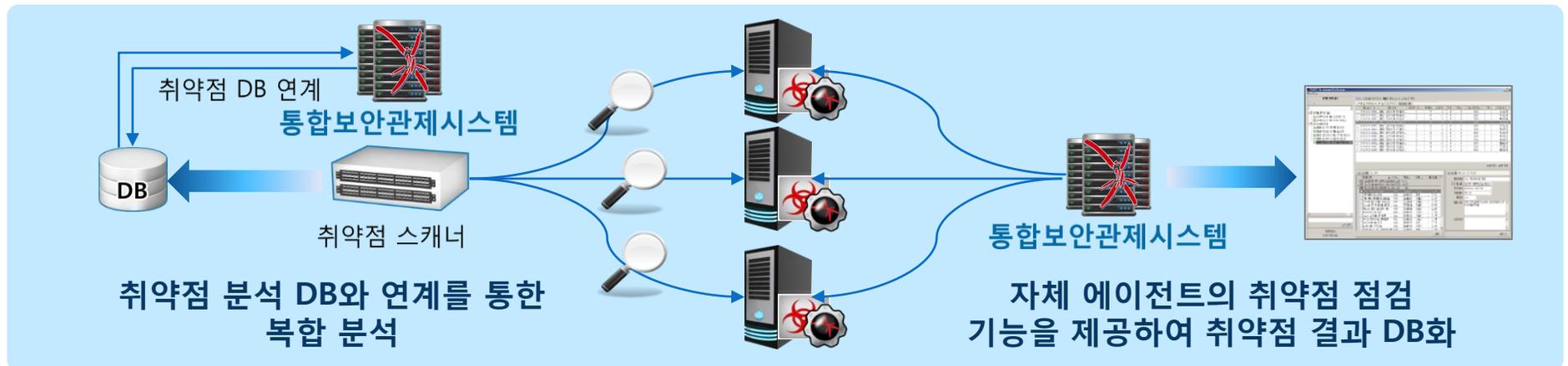
차세대 통합보안관제시스템의 예방 업무

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

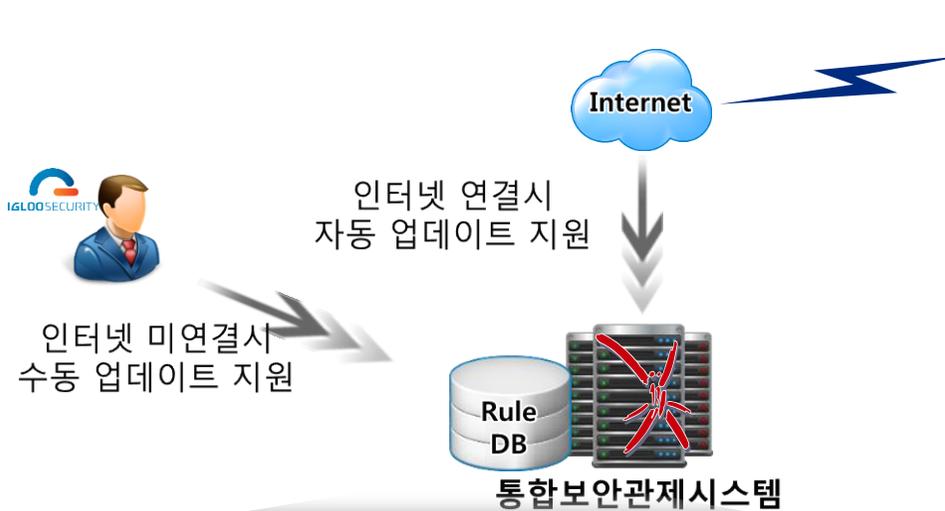


TO-BE



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.



관리 > 설정관리 > 단일경보 관리

분석서버상태 0/0

사용자 정의 룰 2 / 279 목록화 볼 0 / 10 번들볼 0 / 4 그룹등록 그룹수정 그룹삭제

모의 훈련

회만표시 10

입력 상태	종이류	신뢰도	발생주기	발생건수	로그소스	송발지IP	목적지IP	조건경의	매외조건	적용범역	동맹조건
<input type="checkbox"/>	1-1 [Web] Bash Bug 또는 Shell Shock 취약점 공격	1	0	1	로그소스(1)	송발지_100	목적지_FFF	IP_주소도	Any		
<input type="checkbox"/>	1-2 [Web] Bash 취약점 이벤트 발생				로그소스(1)	Any	목적지_FFF	IP_주소도	Any		
<input type="checkbox"/>	1-3 [Web] 웹서비스 IP 접근 금지				로그소스(1)	Any	목적지_FFF	IP_주소도	Any		
<input type="checkbox"/>	2-1 [Web] 동일 송발지 IP에서 다수의 포트				로그소스(1)	Any	목적지_FFF	IP_주소도	Any		
<input type="checkbox"/>	2-2 [Web] 동일 송발지 IP에서 다수의 포트				로그소스(1)	Any	목적지_FFF	IP_주소도	Any		
<input type="checkbox"/>	2-3 [Web] 무효 전송된 이벤트의 size가 5KByte	1	3600	1	로그소스(1)	Any	Any	sent_5k	Any		
<input type="checkbox"/>	3-1 [VPN] 다수의 IP로 동일 ID로 접근 성공(ID 도	1	60	1	로그소스(1)	Any	Any	VPN_Login	Any		
<input type="checkbox"/>	3-2 [VPN] ID 도용 의심 IP로 5Kbytes 이상 패킷이	1	60	1	로그소스(1)	Any	Any	recv_5k_0i	Any		
<input type="checkbox"/>	4-1 [Web] 악성코드 유포시 이벤트 발생	1	60	1	로그소스(1)	Any	발행리스트	Any	Any		
<input type="checkbox"/>	4-2 [Web] 악성코드 유포시 이벤트 발생	1	60	1	로그소스(1)	Any	Any	백신금지	Any		

현재 : 1 - 10 / 검색결과 : 21건

관제 룰 셋 지속적 업데이트

이글루시큐리티 Knowledge Center

국내 환경에 특화된 보안 관제 시나리오 생성

DDoS 탐지 시나리오

내부정보유출탐지 시나리오

악성코드 탐지 시나리오

APT, Webshell 공격 시나리오

솔루션 및 시나리오가 결합된 최상의 보안관제체계 제공

시나리오 개발 TFT 상시 운영

인터넷보안연구소

- 시나리오 개발 TFT 총괄
- 통합보안관리 및 BIG Data Solution 개발 연구 총괄

선행기술연구소

- 악성코드 분석
- 모바일 보안기술 연구 및 개발
- 가상화 기반 연구

보안관제 Rule 설계

IGLOOSECURITY 시나리오 개발 TFT

침해사고대응팀

- 침해사고 대응/분석
- 모의해킹/취약점 점검
- 지능정보안위협 선제적 대응
- 인증/안전진단

기술지원센터

- 취약성 분석을 통한 패턴 정의
- 보안관제시스템(ESM) 기술지원
- 비상대응 전문조직(IG-CERT)을 통한 기술지원

III

탐지/분석 사례



손쉬운 DDoS 분석 사례

공격 분석 흐름



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



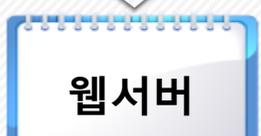
- 61.139.128.99(73%)
- 192.168.12.86(24%)
- 그외 다수의 IP 접근(1~2건)



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



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



- 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

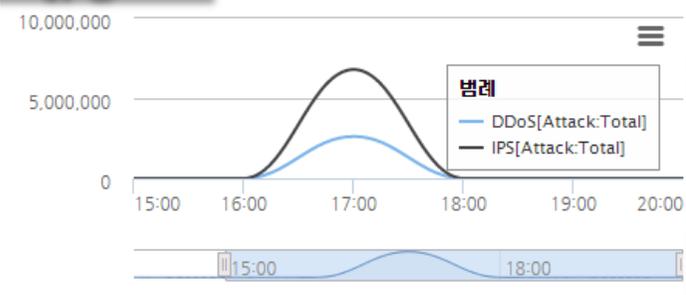
복합공격 - 웹 취약점 Scan 공격

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

IP추적기를 통한 내부 시스템 감염 공격 발견

실시간 분석

DDoS IPS



원래IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	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

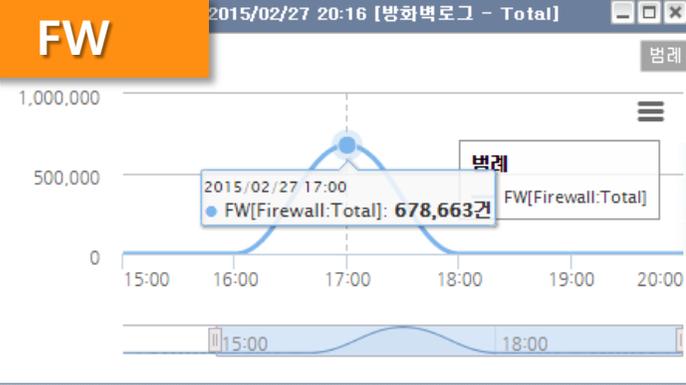
원래IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method	
+	192.168.1.100	2015/02/27 17:47:18	192.168.12.91	61.139.128.99	52249	192.168.12.86	80	UDP(17)	Pass/Detect(101)	UDP Packet Flooding
+	192.168.1.100	2015/02/27 17:47:18	192.168.12.91	61.139.128.99	52249	192.168.12.86	80	UDP(17)	Pass/Detect(101)	UDP 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(101)	UDP Source-IP Flooding
+	192.168.1.100	2015/02/27 17:48:17	192.168.12.91	192.168.12.82	137	192.168.12.255	137	UDP(17)	Pass/Detect(101)	MS WINS Server Registration S

원래IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method	
+	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)	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)	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)	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)	Accept(101)

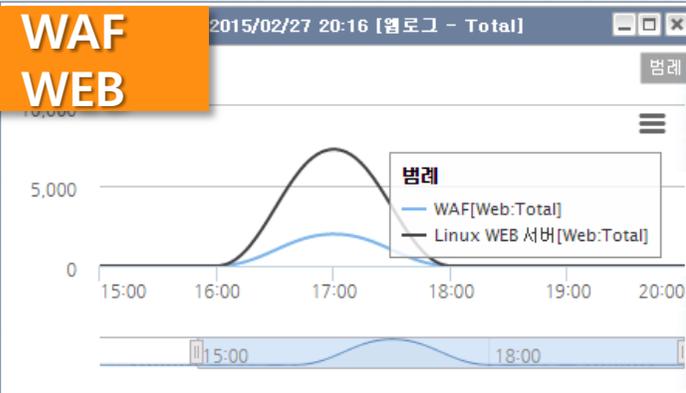
원래IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method	
+	192.168.1.100	2015/02/27 17:35:45	192.168.12.92	61.139.128.99	52610	192.168.12.86	80	TCP(6)	OK/Accept(200)	/perl,tmp
+	192.168.1.100	2015/02/27 17:35:45	192.168.12.92	61.139.128.99	52623	192.168.12.86	80	TCP(6)	OK/Accept(200)	/query,bak
+	192.168.1.100	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/~opSensePostNotThereNoNoat/ Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 6.0; Win64; x64; Trident/6.0)
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 6.0; Windows NT 6.0; Win64; x64; Trident/6.0)
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

FW



WAF WEB



통계 분석 - 유형별

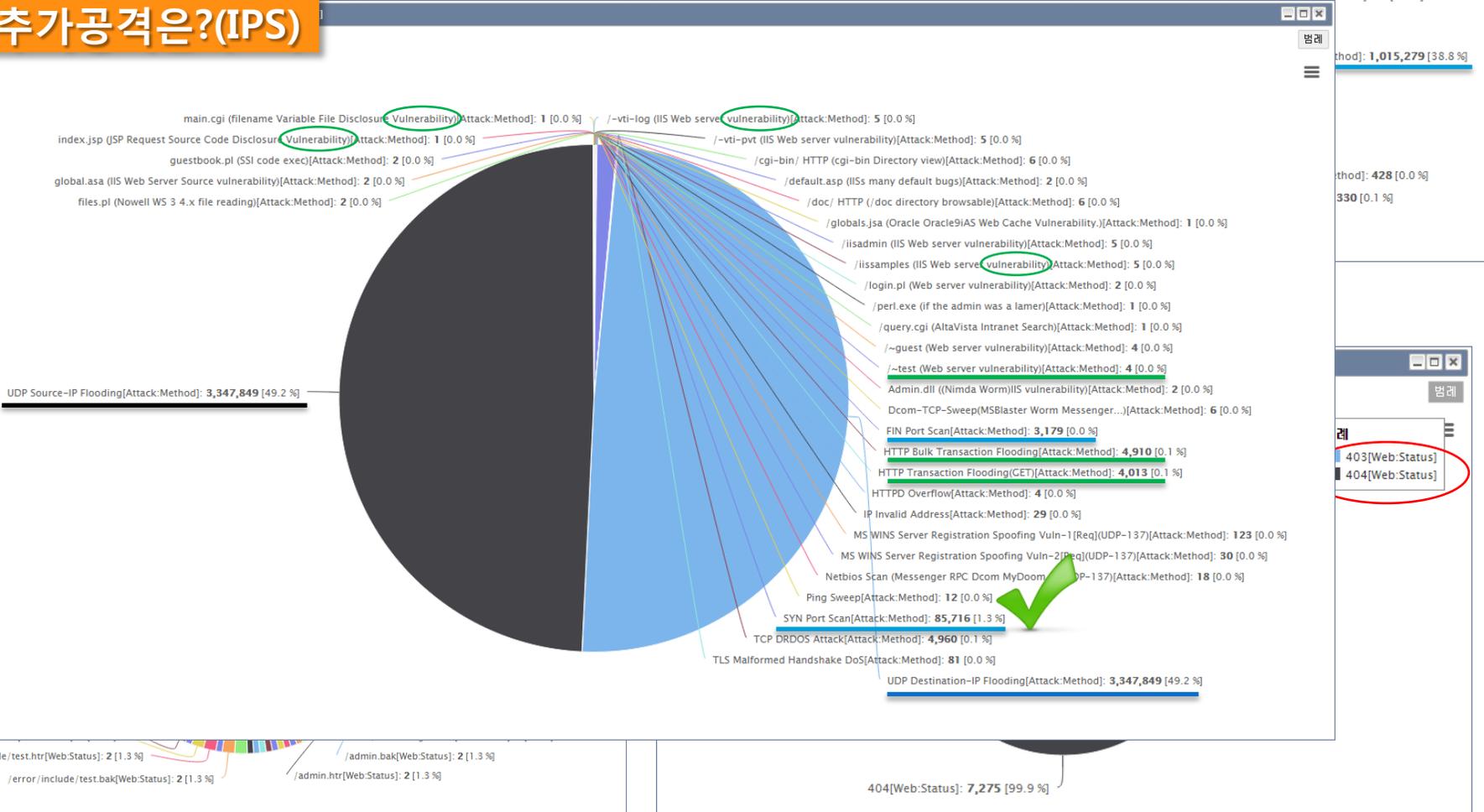
누가?(FW)



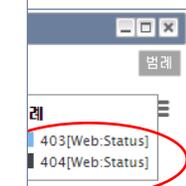
어떤공격?(DDX)



추가공격은?(IPS)



어디로?



이 정보로 검색

쉬운 쿼리 검색

● 검색조건

사건일시 2015/02/27 16:00:00 ~ 2015/02/27 18:00:00

s_info:(61.139.128.99) & d_info:(192.168.12.86)
category:(E002) & method:(*SYN Port Scan*)

검색 ↓ 검색조건

IPS

관리자IP	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

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

× 출발지IP × 목적지IP × Method

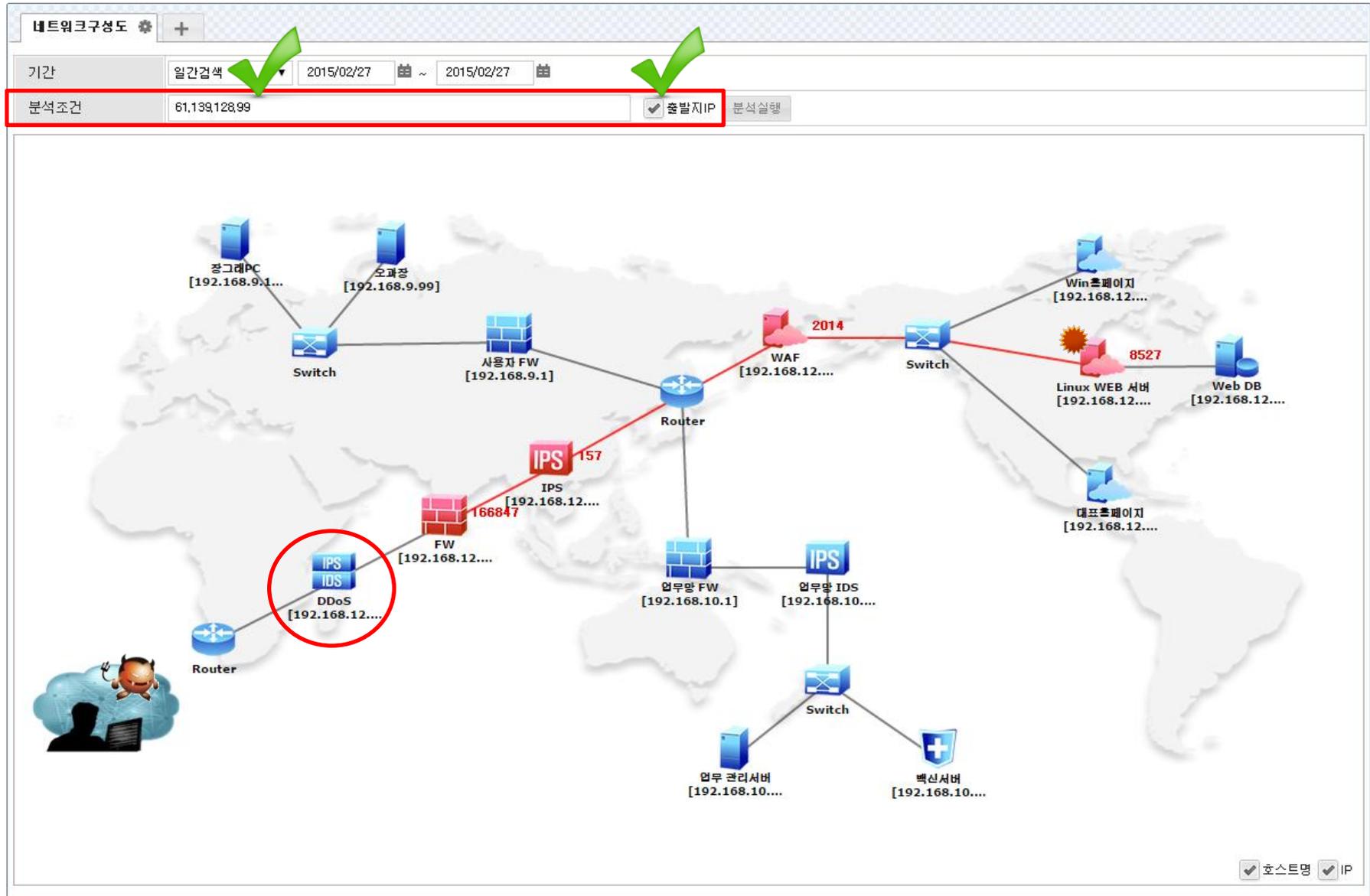
화면표시 20

관리자IP	시간	로그소스IP	출발지IP	출발지포트	목적지IP	목적지포트	프로토콜	상태	Method
-------	----	--------	-------	-------	-------	-------	------	----	--------

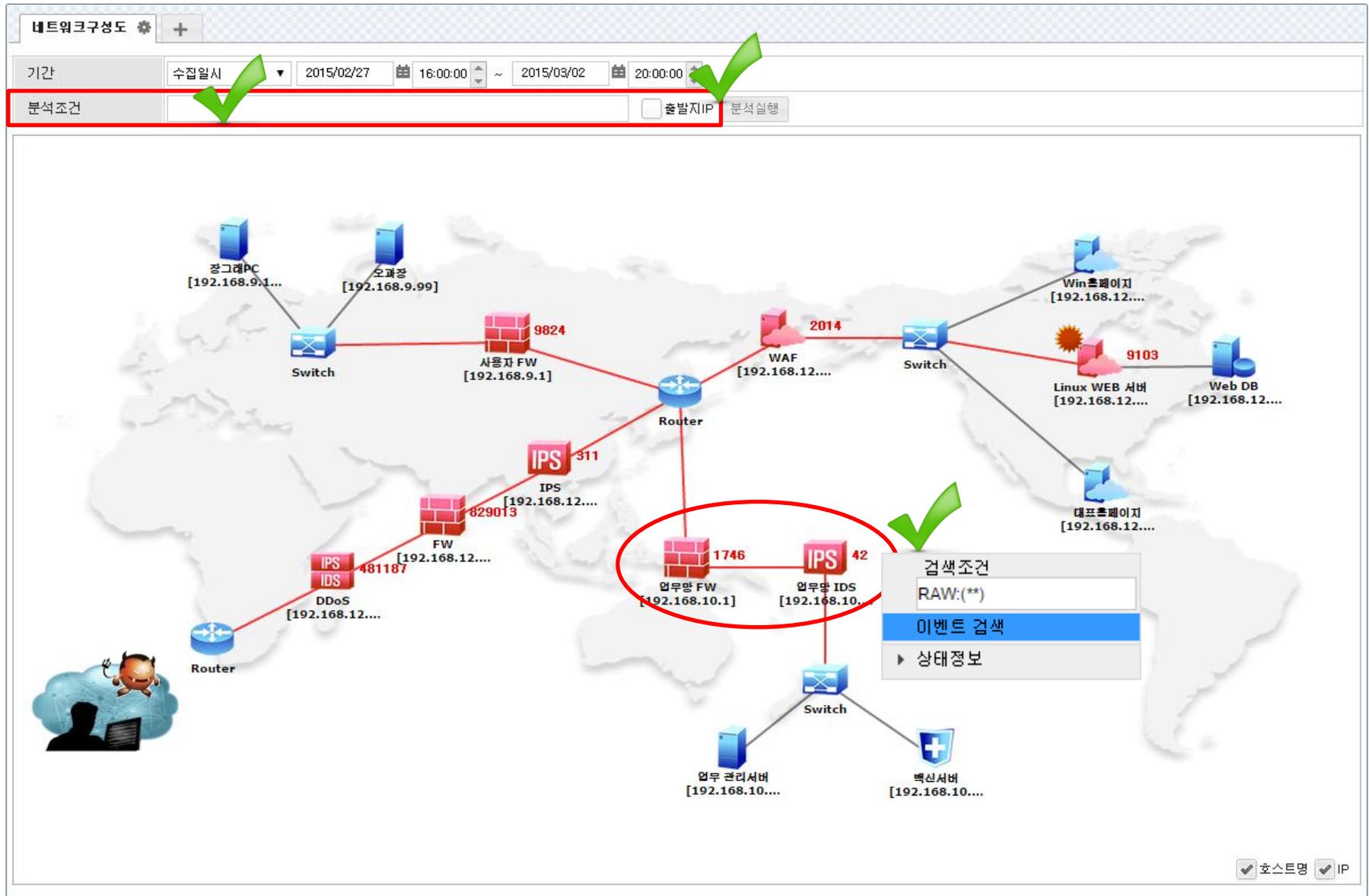
- 61.139.128.99
- 192.168.12.86
- /_vti_log (Web server vulnerability)
- /_vti_pvt (Web server vulnerability)
- /cgi-bin/ (Web server vulnerability view)
- /doc/ HTTP (Web directory browsable)
- /iisadmin (IIS Web server vulnerability)
- /iissamples (IIS Web server vulnerability)
- /~guest (Web server vulnerability)

192.168.1.100	2015/02/27 17:34:31	192.168.12.91	61.139.128.99	55144	192.168.12.86	80	TCP(6)	Pass/Detect/~/guest(Web server vulnera	
---------------	---------------------	---------------	---------------	-------	---------------	----	----------	--	--

“그 중에 하나만...”



"한 눈에, 한꺼번에, 다같이!"



이벤트 검색 & 행위 분석

FW

	메니지IP	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_000000000000049431_E_2015022719, stmp_E-Secure-281, HASH = 23aeaf7a20cd45f23e320bd2d9068d1b38cec12e8ea8637664d61a87617ecd42, 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

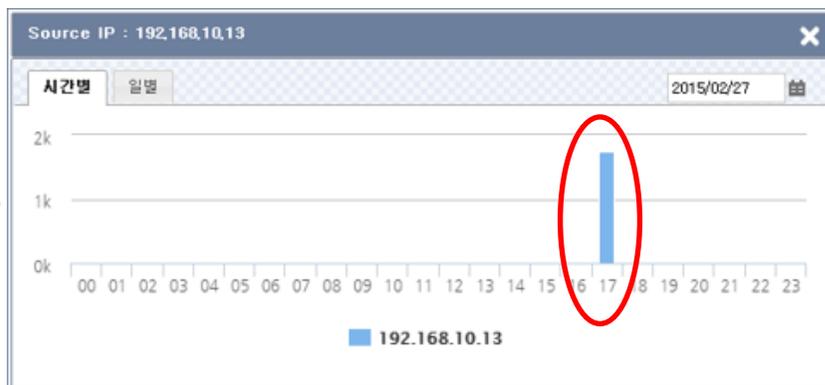
IDS

	메니지IP	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		192.168.12.86	80	TCP(6)	Pass/Detect(101)	TCP SYN Flooding

서버 Session

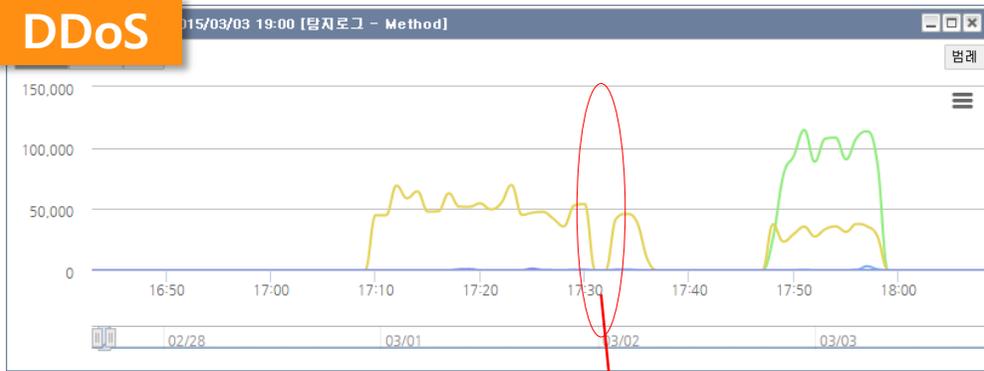
	메니지IP	시간	로그소스IP	출발지IP	목적지IP	목적지포트	프로토콜	상태
+	192.168.1.100	2015/02/27 17:42:59	192.168.12.86	192.168.10.13	39.128.99	51797	TCP(6)	SYN_RCVD
+	192.168.1.100	2015/02/27 17:42:59	192.168.12.86	192.168.10.13	39.128.99	51729	TCP(6)	SYN_RCVD

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

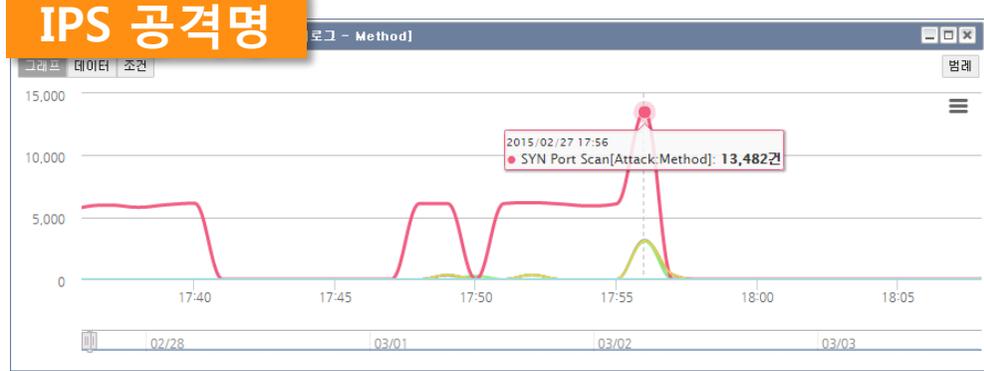


시계열 분석

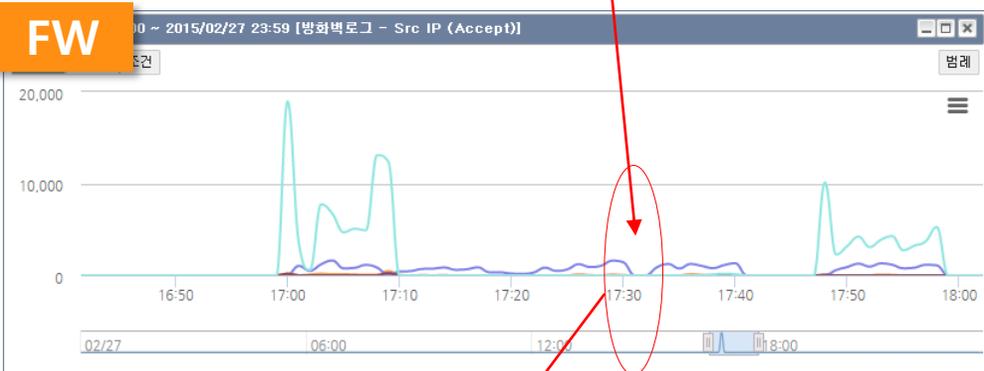
DDoS



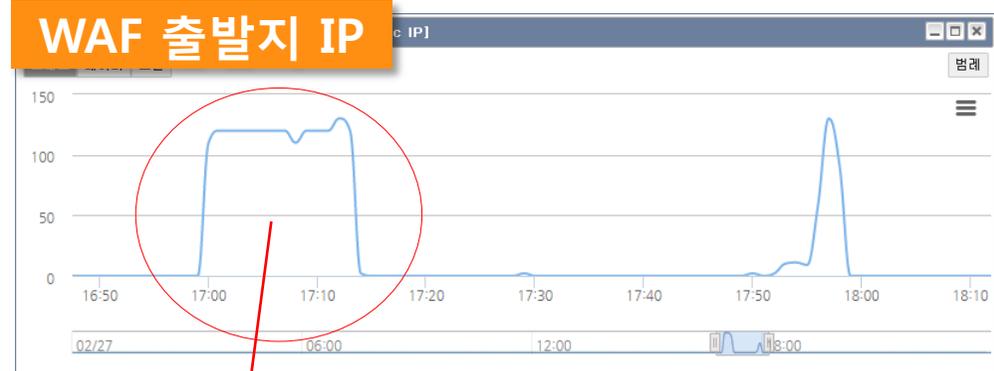
IPS 공격명



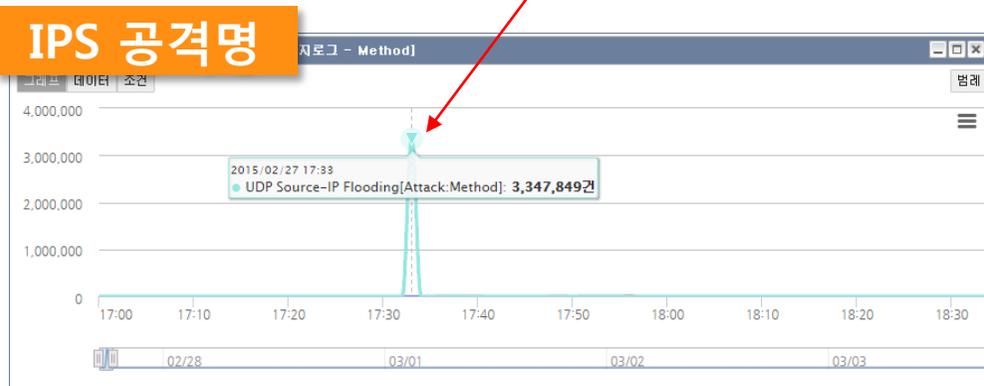
FW



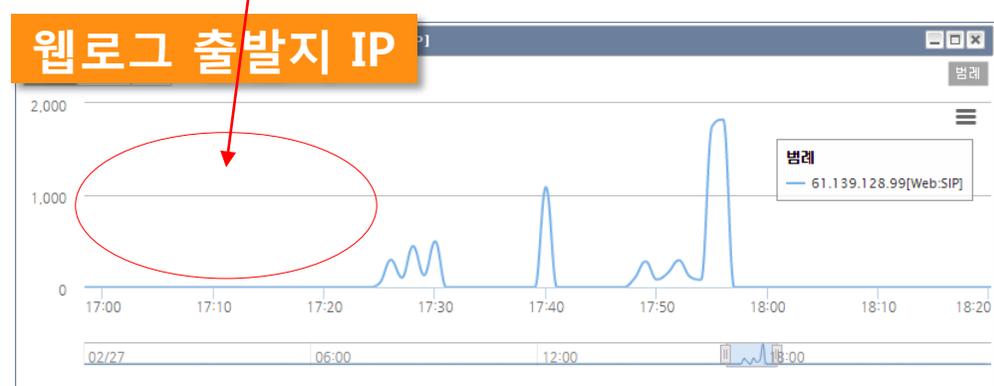
WAF 출발지 IP



IPS 공격명



웹로그 출발지 IP



IV

기대 효과



차세대 통합보안관제시스템 기대효과

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

실시간 경보 모니터링

관제 보고서 작성

기능적 한계로 하지 못했거나
작업 시간이 많이 걸렸던 업무를
손쉽게 해결

DDoS 대응

침해사고 처리

홈페이지 위변조 탐지

APP 취약점 점검

모의 훈련

침해사고 분석

네트워크 취약점 점검

탐지 패턴 업데이트

보안관제 업무



정보공유

악성코드 분석

최신 보안동향 모니터링

방화벽 운영 관리

기존에 하기 힘들었던 업무를
할 수 있도록 이글루시큐리티가
다양한 정보제공 및 지원

Anti-Virus 운영 관리

유해 IP 관리

컴플라이언스

지침/매뉴얼 개정

해킹 메일 분석

감사합니다.