



(주)에스아이그룹

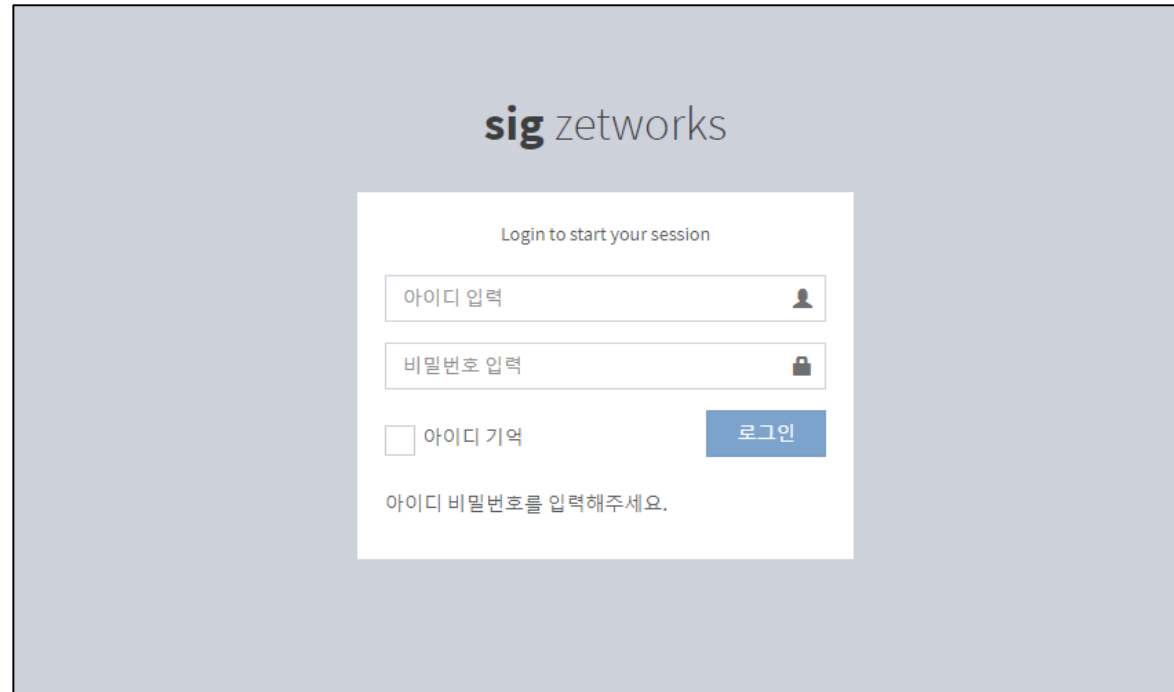
01 _ Zetworks Services 소개

Faith & Innovation IT Service Partner

로그 통합 및 시각화 서비스 소개

현업 운영에 필요한 실시간 데이터 수집 및 시각화

보안장비, 네트워크 장비, 주요 서버, 어플리케이션 로그 등 분야별 로그를 실시간 취합하여 각 고객사의 중요도에 맞게 시각화 합니다.



The image shows a login interface for 'sig zetworks'. The page has a light gray background with the company logo at the top center. Below the logo is a white login form with the following elements:

- Header: "Login to start your session"
- Input field: "아이디 입력" (ID Input) with a user icon on the right.
- Input field: "비밀번호 입력" (Password Input) with a lock icon on the right.
- Checkbox: "아이디 기억" (Remember ID) with an unchecked checkbox.
- Button: "로그인" (Login) in a blue box.
- Text: "아이디 비밀번호를 입력해주세요." (Please enter your ID and password.)

서비스 소개

로그 통합 및 시각화 서비스 소개

| 핵심 기능 활용은 선별된 오픈소스 활용, 운영상 부족한 부분은 자체 개발을 통해 가성비 및 편리함을 고객에게 서비스합니다.

보안장비 로그분석

시스템 AUDIT 분석

시스템 자원 현황 분석

HIDS 탐지 로그 및
네트워크 장비
로그분석

인증 프락시를 통한
고비용의 서브스크립션
절감 및 운영자별
접근제어

시스템 및 IP 기반
모든 장비
Health Check

네트워크 어플리케이션
Health Check



One Stop Service

수집된 로그 무결성
확보

상관분석
DASHBOARD

파일로그 실시간 취합
및
실시간 대시보드

RDBMS(oracle, mssql,
mysql) 데이터 취합
및 대시보드

SYSLOG 실시간 수집

시스템 프로세스
단위까지 정보 취합

업무 프로세스
최적화 대시보드 구현



02 _ 서비스 주요 기능

Faith & Innovation IT Service Partner

주요 기능

서비스 주요 기능

| 다양한 대량의 데이터 실시간 시각화를 통해 의미 있는 정보 전환 제공

System Availability

- 프로세스별 메모리, CPU 점유량 표기
- 전체 CPU, MEM 증가 시 해당 프로세스 추출
- 기존 SNMP의 일간, 주간, 월간, 년간에 따른 평균값의 변화 단점 해결
- 시스템 이벤트와 상태 정보를 동일 대시보드에 가시화하여 신속한 원인 분석
- DISKIO 파티션별 출력
- 정확한 데이터를 통한 시스템 설계에 활용

Network Security

- syslog, netflow, sflow 등의 실시간 수집
- 주요 위협에 대한 실시간 가시성 제공
- 인터넷 및 내부 네트워크 접근에 대한 어플리케이션 분류, 웹접속 분류, tcp/ip 접속 분류, 침입 분류등을 실시간 가시화
- 트래픽 유발 인터넷 접속 유입(DoS, 업무시간 인터넷 과다 사용 등)에 대한 신속, 정확한 대시보드를 제공
- 내부 트래픽 검출 환경 시 네트워크 저하 현상에 대한 실시간 대응 가능

개인정보보호

- 각종 어플리케이션에서 생성되는 로그(파일, DB)를 실시간 수집 및 검색 가능 환경 구현
- 네트워크 접근 기록 수집 및 검색
- 시스템 로그 원격 저장 및 검색
- 개인정보보호법에서 지정된 일정기간 접근 기록을 안전한 장소에 보관해야 되는 부분 해결(상용 로그서버 대체)

Data Visualization

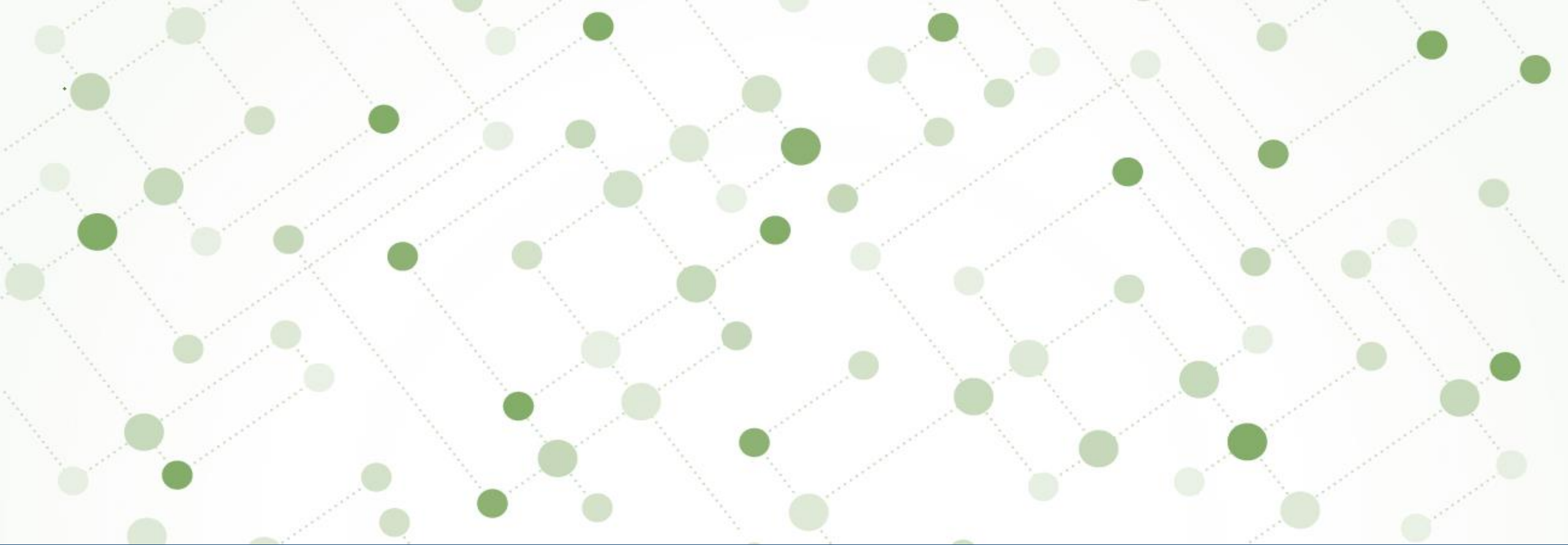
- MES, ERP등에 누적된 생산정보 등을 Collector를 통해 실시간 indexing하여 ERP등에서 장시간 개발을 통하여 구축 가능한 BI 솔루션 부분 대체 가능
- 현재 고객사 불량 및 생산 현황에 부분 적용 중, 관련 query 및 view table 제공시 연동 작업 가능

상관 분석

- 시스템 자원 변화, 네트워크 접속 변화등을 시계열로 동일 대시보드에 출력하여 상하 연관 관계등 분석 활용
- 시스템, 어플리케이션, 네트워크, 보안 등에서 발생하는 로그의 컬럼 포맷을 통일화 하여 조건 검색에 용이하도록 구성
- 파일서버 접근 기록 및 퇴사전 인터넷 사용 패턴에 대한 실시간 상호 분석 가능등 활용

고객 요구 반영

- 권한별 대시보드 접근 제한
- 단일 모니터에서 다양한 대시보드 슬라이드 뷰 제공
- 외부 웹 관리 페이지 통합 연동 관리
- 오픈소스의 부족한 검색 인터페이스 개선
- 추가 비용 발생 부분의 리포팅 부분 제공
- 일일 로그량, 연동 장비 수 등과 지불 비용이 비례하지 않은 합리적 구축 기회 제공
- 데이터 loss 없이 수집 가능한 구현 경험 축적



03 _ Zetworks Framwork 기능 소개

Faith & Innovation IT Service Partner

🔍 사용자 및 부관리자 생성, 호스트, 뷰어, 슬라이드 목록, 게시물 관리

→ 작업 지시, MA 작업 등에 대한 공지 및 기록 관리를 할 수 있도록 반영, 모니터링 시 참조 내용 기록

The screenshot displays the 'sig zetworks' admin interface. The left sidebar contains a menu with items like '마이페이지', '기초 코드', '접근제어 관리', '관리자', '사용자 목록', '호스트 목록', '뷰 목록', '뷰 그룹 목록', '슬라이드 목록', '게시판 정보 설정', '게시판 그룹 설정', '일반 뷰어', '슬라이드 뷰어', and '게시판 목록'. The main content area is titled '게시물 목록 게시판' and shows a 'Board List' with two options: '작업 공지 사항' (selected) and '운영자 요청 사항'. Below this is a search filter section with fields for '제목' (Title), '작성자' (Author), '시작일자' (Start Date), and '종료일자' (End Date), along with '검색' (Search) and '리프레시' (Refresh) buttons. A table below the filters displays one post:

#	제목	등록자	등록일시
1	zetworks - log manger를 사용해주세요서 감사합니다.	관리자	2018-04-17 10:51

At the bottom of the page, there is a footer with 'Copyright 2018. sigroup. All rights reserved.', 'SIGroup All rights reserved.', and 'Version 1.0.0'.

Zetworks 기능 일반 뷰어

🔍 등록된 뷰어 그룹별 목록 관리 및 조회

→ 사용자 선택 메뉴에 대한 상세 페이지 출력(사전 뷰 목록, 그룹에 등록된 부분을 업무 범위에 따른 접근 권한 할당)

관리자 설정

운영자 권한 뷰어 목록 접근

뷰 그룹 관리 관리자

뷰 그룹 상세

호스트 침입탐지

뷰 그룹 이름 호스트 침입탐지

순번 4

수정 삭제 목록

뷰 등록 등록

뷰 선택(+)

[내부 테스트용] 시스템 리소스 상관 분석

저장

뷰 그룹 권한 등록

뷰 그룹 권한(+)

관리자

저장

뷰 그룹 권한 목록

이름	회사명	부서명	직책명
홍길동	(주)에스아이그룹	기술팀	과장
대니얼	(주)에스아이그룹	개발팀	대리

뷰 그룹 권한 목록

호스트 이름	뷰 이름	삭제
내부 테스트용	호스트 침입탐지 현황(VOSSEC)	삭제
내부 테스트용	호스트 침입탐지 정책 모니터링	삭제

시스템 상태 분석

Add a filter

System Navigation (Metricbeat System)

System Overview | Hosts Overview | Containers overview

Number of hosts (Metricbeat System) CPU Usage Gauge (Metricbeat Sys... Memory Usage Gauge (Metricbeat... Disk used (Metricbeat System) Inbound Traffic (Metricbeat System) Outbound Traffic (Metricbeat Syst...

5

CPU Usage 2.91%

Memory Usage 56.92%

Disk used 64.85%

Inbound Traffic 499.8KB/s Total Transferred 279.7GB

Outbound Traffic 6.9KB/s Total Transferred 2.4GB

Top Hosts By CPU (Realtime) (Metricbeat System)

Host	CPU Usage
zetworks.siggroup.co.kr	28.11%
SRV101	15%
elk.siggroup.co.kr	12.51%
WIN-CDH30LSMOAP	6.59%
zentyal	3.47%

Top Hosts By Memory (Realtime) (Metricbeat System)

Host	Memory Usage
elk.siggroup.co.kr	80.90%
WIN-CDH30LSMOAP	62.52%
zetworks.siggroup.co.kr	56.09%
zentyal	54.01%
SRV101	31.03%

Hosts histogram by CPU usage (Metricbeat System)

Hosts

Legend: 0% - 20%, 20% - 40%, 40% - 60%, 60% - 80%

Zetworks 기능

슬라이드 뷰어

🔍 지정 인터벌에 따라 개별 페이지 전환 목록 작성

→ 단일 모니터에 인터벌에 따른 다양한 관리 화면을 자동 전환 출력하여 관제 또는 모니터링에 적합하도록 구현

The image displays the 'sig zetworks' interface. On the left, a sidebar menu lists various management functions. The main area is titled '슬라이드 관리' (Slide Management) and shows a '관계 상황판' (Relationship Status Panel) with a table of slides. A yellow box highlights the '슬라이드 업로드 등록' (Slide Upload Registration) section, which includes fields for '뷰 선택' (View Selection) set to '[TKLOG] UTM IPS 현황', '인터벌 시간(초)' (Interval Time) set to 120, and '순서' (Order) set to 1. Below this is a table of existing slides.

호스트 이름	뷰 이름	인터벌시간(초)	순번	삭제
내부 테스트용	시스템 리소스 상관 분석	60	1	✕ 삭제
내부 테스트용	호스트 침입탐지 현황(OSSEC)	60	2	✕ 삭제
내부 테스트용	UTM 종합 상황판	60	3	✕ 삭제
TKLOG	UTM 국가별 접속 현황	30	4	✕ 삭제

An arrow points from the '인터벌 시간(초)' field to a text label: '출력 목록 및 순서, 인터벌 지정' (Output list and order, interval specification). Below the slide management section, a '시스템 리소스 상관 분석' (System Resource Correlation Analysis) dashboard is visible, showing various charts and tables. A blue arrow points from the '시스템 리소스 상관 분석' dashboard to a text label: '60초 후 화면전환' (Screen transition after 60 seconds).

The dashboard includes a 'UTM 국가별 접속 현황' (UTM Country Connection Status) section with a bar chart and two tables. The first table shows the top 5 countries by count:

Country	Count
Republic of Korea	69,220
United States	5,479
China	2,912
Russia	679
Japan	620

The second table shows the top 5 countries by IP count:

Country	Count
United States	2,907
China	2,912
Republic of Korea	1,465
Republic of Korea	1,233
Seychelles	836

Zetworks 기능

자체 검색화면 및 리포팅

🔍 검색 조건과 GRID 연동을 통한 별도 페이지 제공, 고객사 요구 맞춤 리포팅 제공

- 고객의 요구에 맞는 리포팅 및 대시보드 제공
- PDF, Image 등 추출 가능

FireWall Log UTM Log

UTM Log Firewall Search

2018-10-16 00:00:00 ~ 2018-10-29 00:00:00

#	시간	방화벽	FailRuleID	Action	로그생성구분	출발지국가	출발지IP	출발지ZONE	출발지PORT	목적지IP	목적지ZONE	목적지IP
14586415	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.134	VLAN2	50772	52.52.14.99	WAN	80	
14586414	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.134	VLAN2	60905	8.8.8.8	WAN	53	
14586413	2018-10-29 09:00:00	XIS105	34	Allowed	ICMP ERROR MESSAGE	186.124.140.168			1.252.12.70			
14586412	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	54034	216.58.197.109	WAN	443	
14586411	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.134	VLAN2	55739	8.8.8.8	WAN	53	
14586410	2018-10-29 09:00:00	XIS105	0	Denied	Appliance Access	186.115.80.51		6668	1.252.12.70		5543	
14586409	2018-10-29 09:00:00	XIS105	22	Allowed	Firewall Rule	192.168.2.162	VLAN2		112.218.44.165	WAN		
14586408	2018-10-29 09:00:00	XIS105	22	Allowed	Firewall Rule	192.168.2.162	VLAN2		106.242.76.139	WAN		
14586407	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	54725	216.58.197.109	WAN	443	
14586406	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	54726	216.58.200.202	WAN	443	
14586405	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	54724	203.248.252.2	WAN	53	
14586404	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	55211	203.248.252.2	WAN	53	
14586403	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	54833	216.58.199.3	WAN	443	
14586402	2018-10-29 09:00:00	XIS105	34	Allowed	Firewall Rule	10.77.77.81	VLAN2	55211	8.8.8.8	WAN	53	
14586401	2018-10-29 09:00:00	XIS105	0	Denied	Appliance Access	10.77.77.66		136	10.77.77.235			

Sankey Chart UTM Log

Sankey Chart

2018-10-28 00:00:00 ~ 2018-10-29 00:00:00

10.77.77.54 → 443 → 58.123.220.77

10.77.77.76 → 997

10.77.77.195 → 83

10.77.77.200 → 5553

192.168.2.162 → 161

206.76.697.213
48.750.54.206
173.237.28.6
176.52.186.710
64.233.168.100
173.198.208.254
192.168.1.100
172.16.108.176
205.185.216.69
8.8.8.8
202.91.155.404
202.91.155.404
173.168.199.176
186.115.80.168
8.8.8.8

siggroup All rights reserved. Version 1.3.0



04 _ 활용 사례 샘플

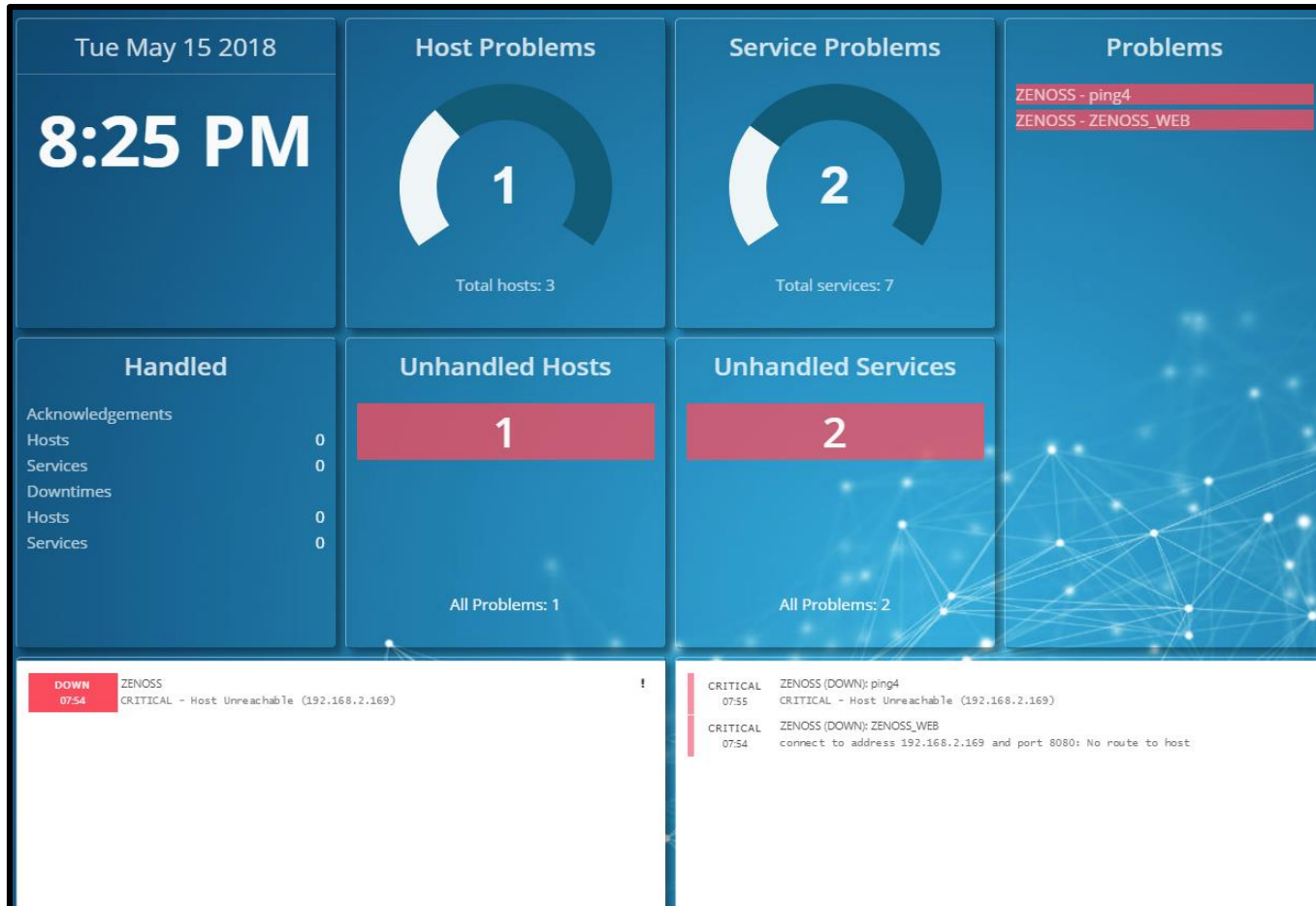
Faith & Innovation IT Service Partner

샘플 스크린 샷

실시간 시스템 및 TCP/UDP/HTTP URL Health Check

🔍 운영중인 각종 시스템 및 IP 주소를 가진 모든 단말 상태 모니터링 및 Alert 발생

→ 시스템 다운 발생 시 주요 네트워크 서비스 어플리케이션 정상 동작 유무 실시간 확인 시 용이(작업 후 발생하는 관리자 부주의 리스크 최소화)



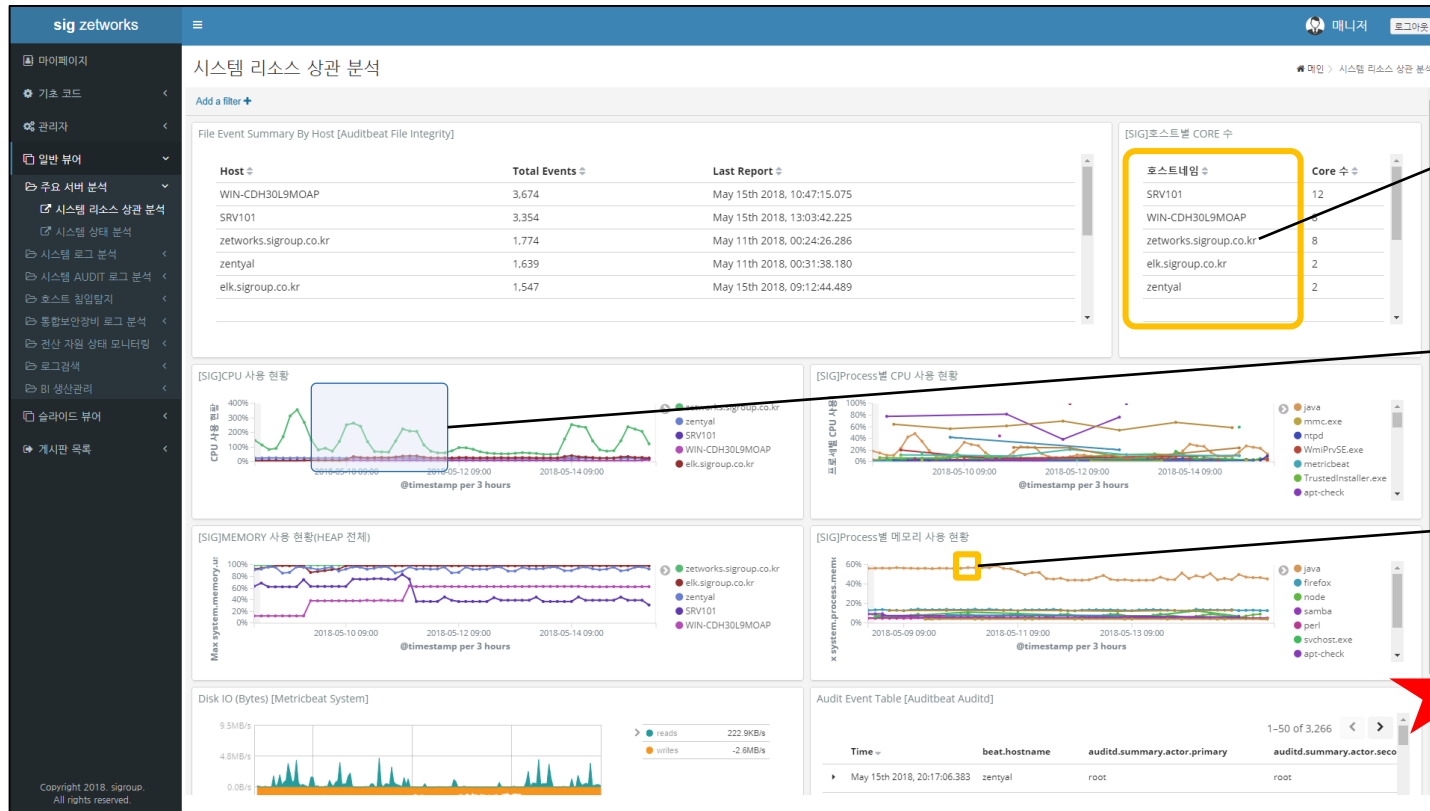
Alert 발생 시 메일 발송 및 SMS 발송 가능

샘플 스크린 샷

시스템 리소스 상관 분석

시계열 라인차트를 활용하여 CPU, MEM, , Process, DISKIO 연관 분석

→ 단순 자원에 대한 사용량 + 주요 실행 프로세스를 동일 기준으로 표현하여 부하 발생 시 신속한 어플리케이션 검출 가능



호스트 선택 필터 시 해당 호스트에 관한 정보로 전체 차트 변경

지정 기간 영역 Drag 시 해당 기간 데이터를 모든 정보 변경

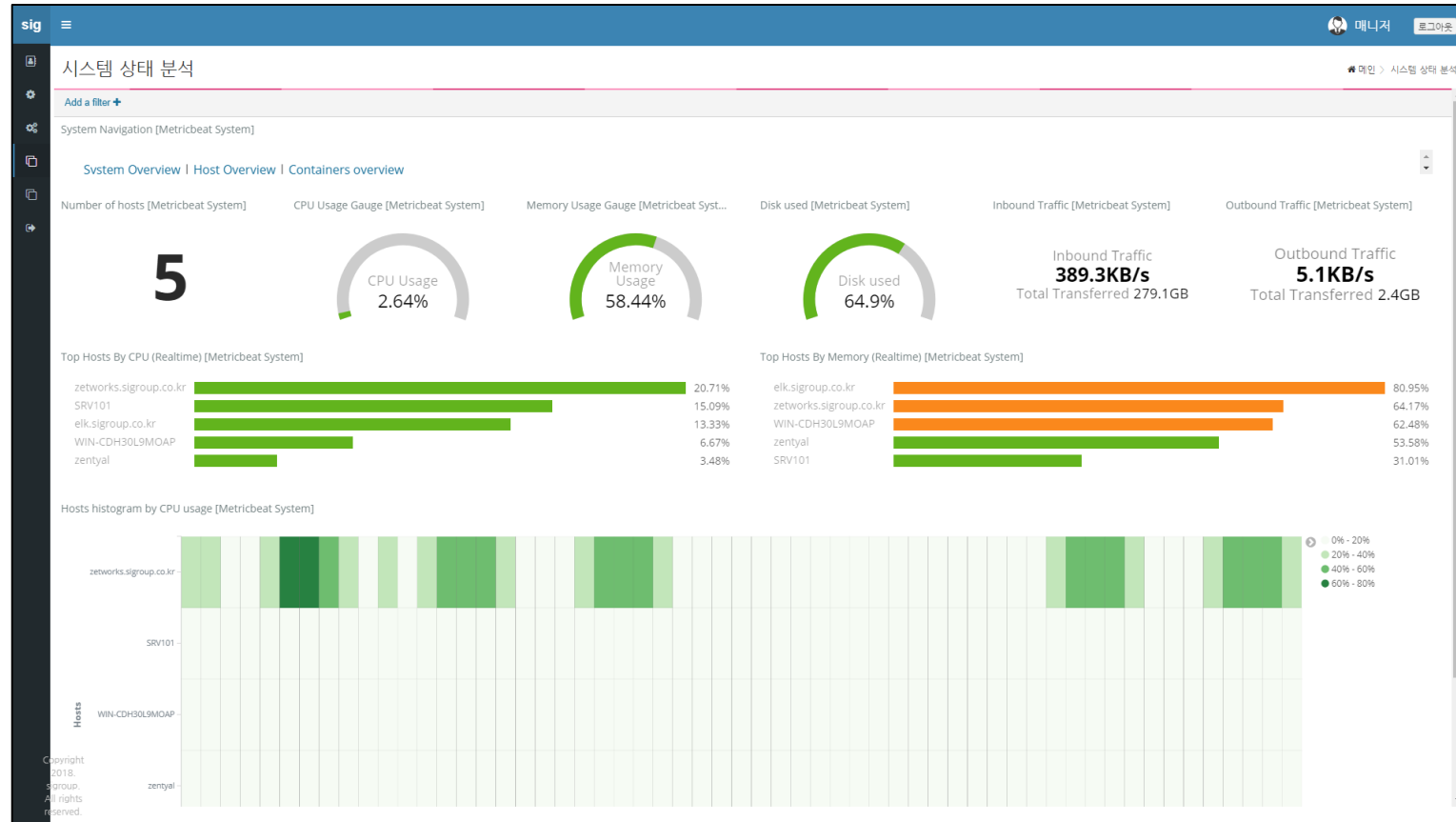
프로세스 선택 시 해당 프로세스 포함된 호스트 및 관련 필터로 변경

화면에 보이는 모든 요소들은 선택 시 필터 항목으로 동작함(기본적으로 실시간 데이터 반영됨)

샘플 스크린 샷

시스템 상태 모니터링

🔍 게이지를 활용한 직관적인 현재 상태 출력에 용이(인터페이스 트래픽 정보 포함)

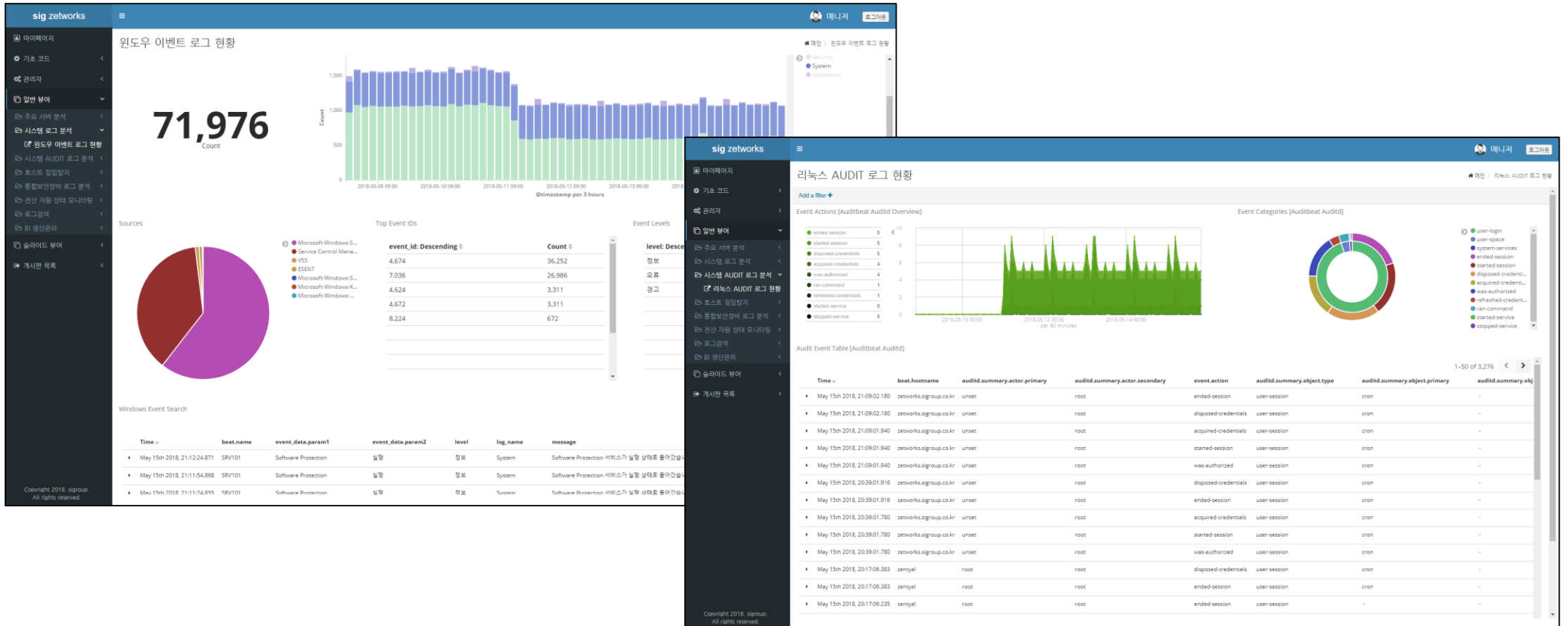


샘플 스크린 샷

윈도우 및 리눅스 이벤트 로그 현황

🔍 서버 Agent 설치를 통한 실시간 이벤트 로그 취합 및 관리

→ 특정 이벤트 선별 출력 대시보드 생성등에 활용

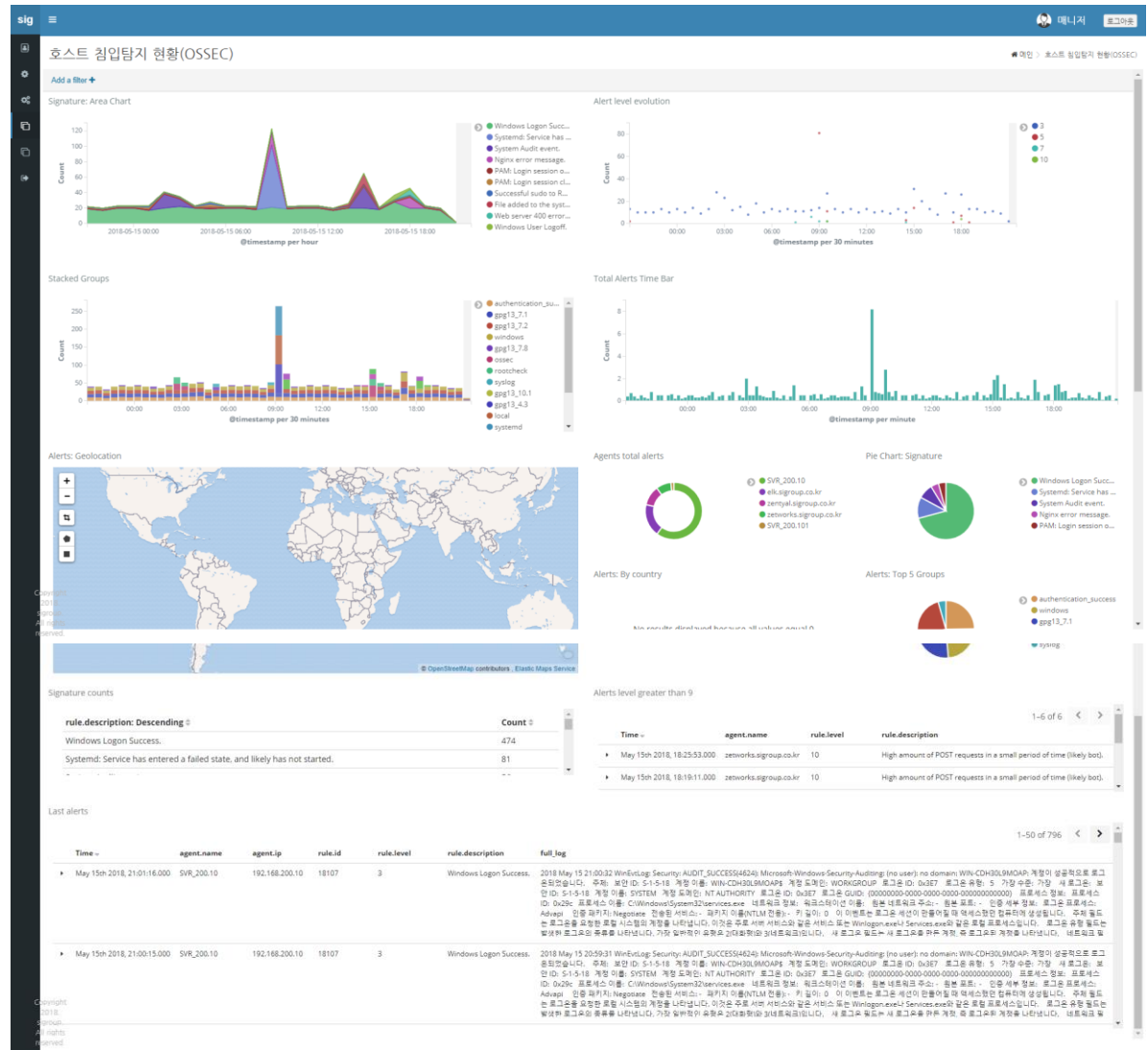
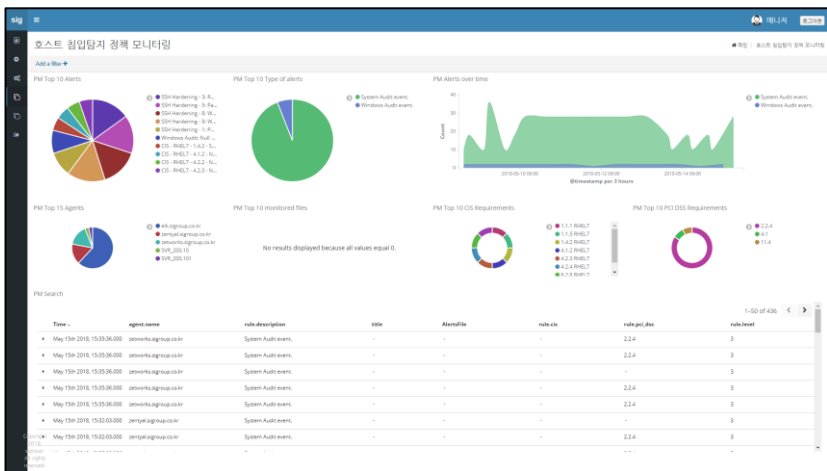


샘플 스크린 샷

HIDS 이벤트 현황

OSSEC Agent(windows,linux, Aix 등)를 활용한 호스트침입탐지 대시보드

- 루트킷 탐지를 포함하여 취약점 설정 파일 분석 등 많은 정보 제공, 네트워크 소켓 오픈, 로그인 시도 등 시스템 자원과 결합 대시보드 생성으로 연관 분석 활용
- 네트워크 IPS 로그와 동일 시계열로 배치 활용 등



샘플 스크린 샷

통합보안장비 종합상황판

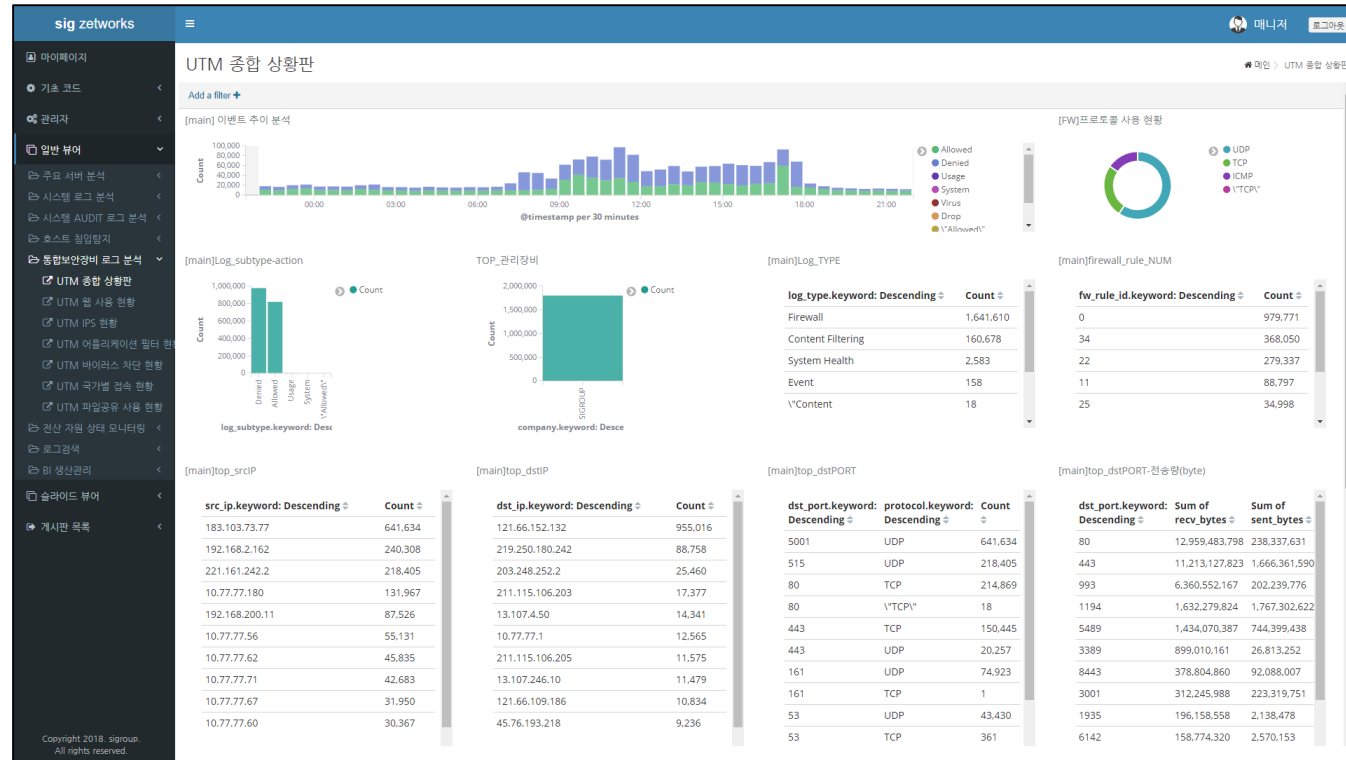
UTM 및 차세대 방화벽 이벤트 종류에 따른 다양한 네트워크 사용 현황 분석

→ 방화벽 정책 수립 시 ANY OPEN 정책에서 출발지 목적지 서비스 등으로 고객과 업무 흐름(수주간 데이터 수집후)을 분석 후 필요한 정책 수립

대부분의 고객의 경우 자사 업무 흐름에 대해 모르는 경우가 많음, 필요한 정책외 모두 차단 할 수 있는 보안 접근 컨설팅 가능

→ 최근 다양한 정보를 제공하는 차세대 또는 UTM 장비의 경우 가치높은 정보 제공(국가 차단, 어플리케이션 차단, 웹차단, 프락시 차단 등)

→ 인터넷 속도 저하시 실시간 전송 현황을 통한 정확한 원인 규명, 관리자의 실수로 인한 잘못된 정책 즉각 검출 가능 활용

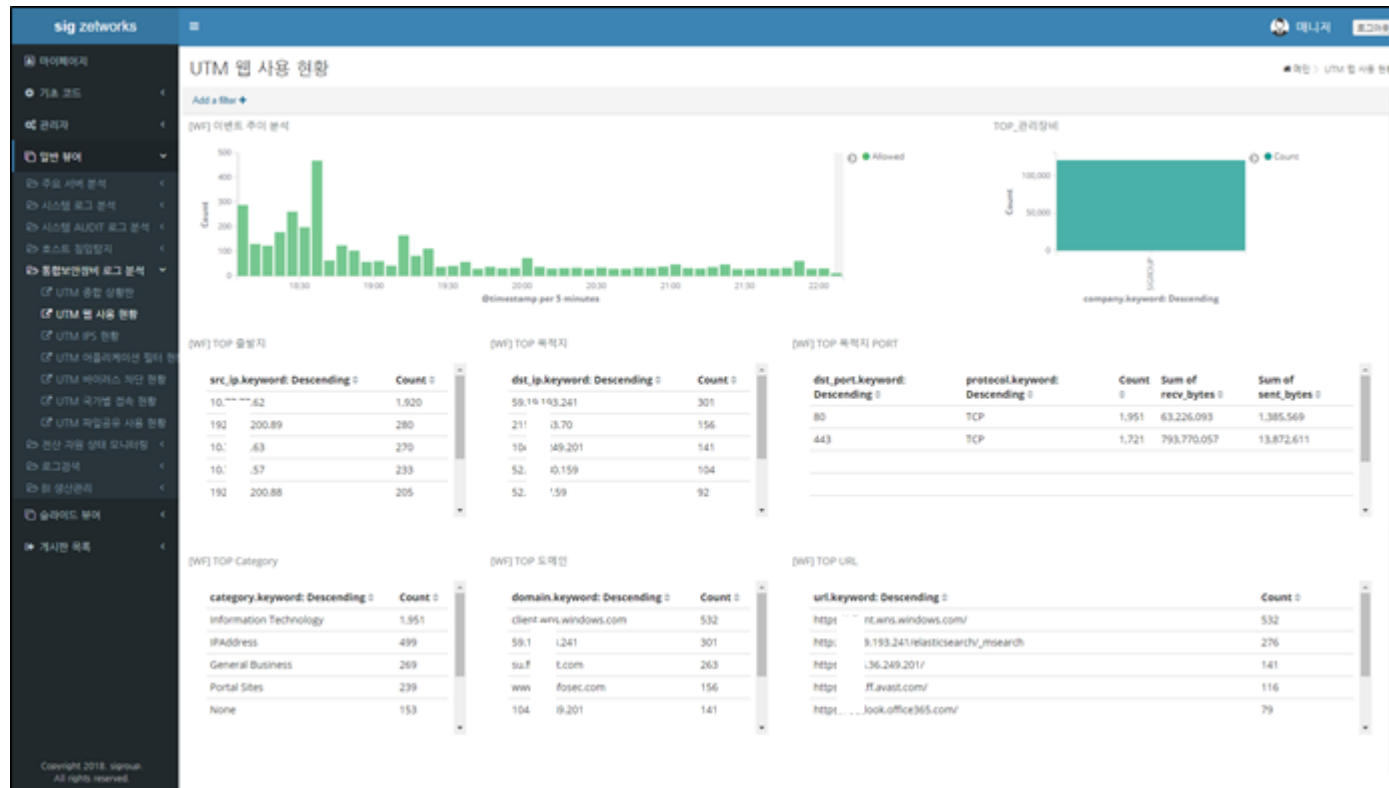


샘플 스크린 샷

웹 사용 현황

🔍 인터넷의 가장 위험하고 가장 정보가 많은 웹 사용에 대한 내.외부 현황 분석, 대부분 방화벽에서 정보 제공

- 악성코드, 랜섬웨어 유입의 가장 위험한 서비스인 웹에 대한 정보를 축적 활용하여 유용하고 필요한 사이트만 허용함으로써 90% 이상의 위험으로부터 보호
- 1개월 TOP 1000, 10000 사이트, 사용량 많은 우선순위로 출력 시 수초 이내 결과 도출 가능
- 이직을 준비하는 경우 구인 사이트 접속이 많은 것을 활용하여 구인사이트 접속 분석 전용 대시보드를 실시간 출력하여 보안팀에서 활용한 사례도 있음

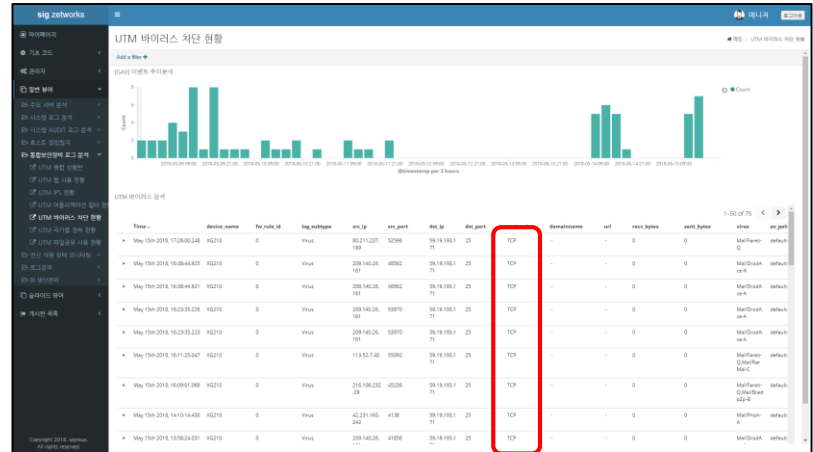
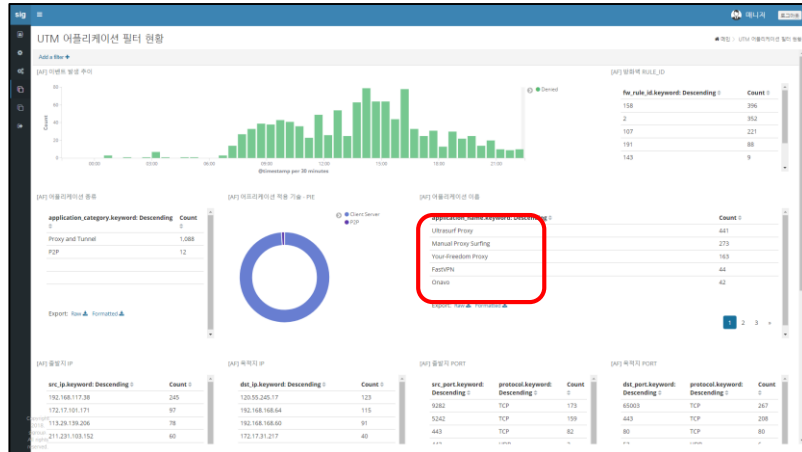
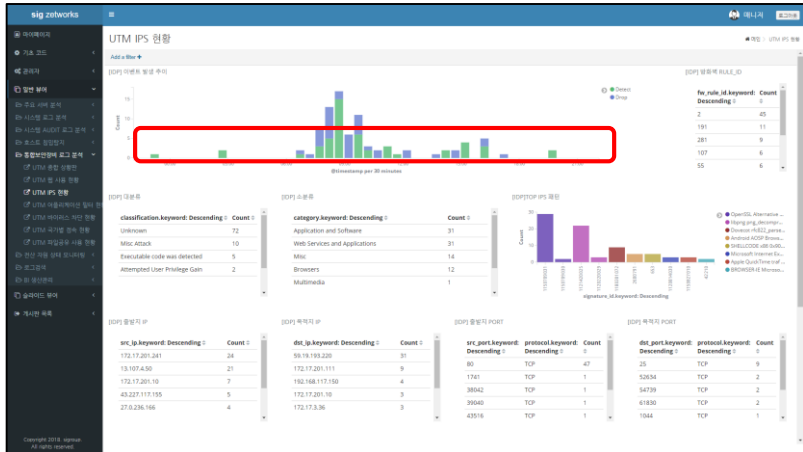


샘플 스크린 샷

IPS, 어플리케이션 필터, GAV 차단 현황

IPS, APP Filter, Gateway AnitVirus 등 다양한 필터에 대한 대시보드 구현

- IPS, APP Filter은 중요하지만 오탐으로 인하여 결국 모니터링으로 운영되는 경우가 많음, 기존 환경으로는 오탐 시그니처 검출이 어렵기 때문
- 실시간 및 누적된 정보를 통하여 오탐 발생 시 신속하게 원인 규명 후 정책 반영
- 지속 적인 공격 시도 등은 단일 발생 로그로는 탐지가 어렵기 때문에 주요 위험 서비스 등에 대한 장시간 변화를 시각화 하여 검출에 활용 및 정책 반영
- 예로 각종 서비스에 대한 행동 패턴을 알고 있는 관리자면 UDP 53번은 접속 수가 많고 데이터량이 적은 DNS 등에 대한 특징을 쉽게 볼 수 있는 대시보드를 구현하여 전송, 접속, 공격패턴 등을 상관 분석하여 DDoS 등 검출에 활용
- 어플리케이션 필터 정책 중 Proxy Tunnel 등은 C&C 등에 활용이 많이 됨으로 실시간 대시보드를 통해 단말 정밀 스캔등을 통하여 사전 확산 방지 등에도 활용

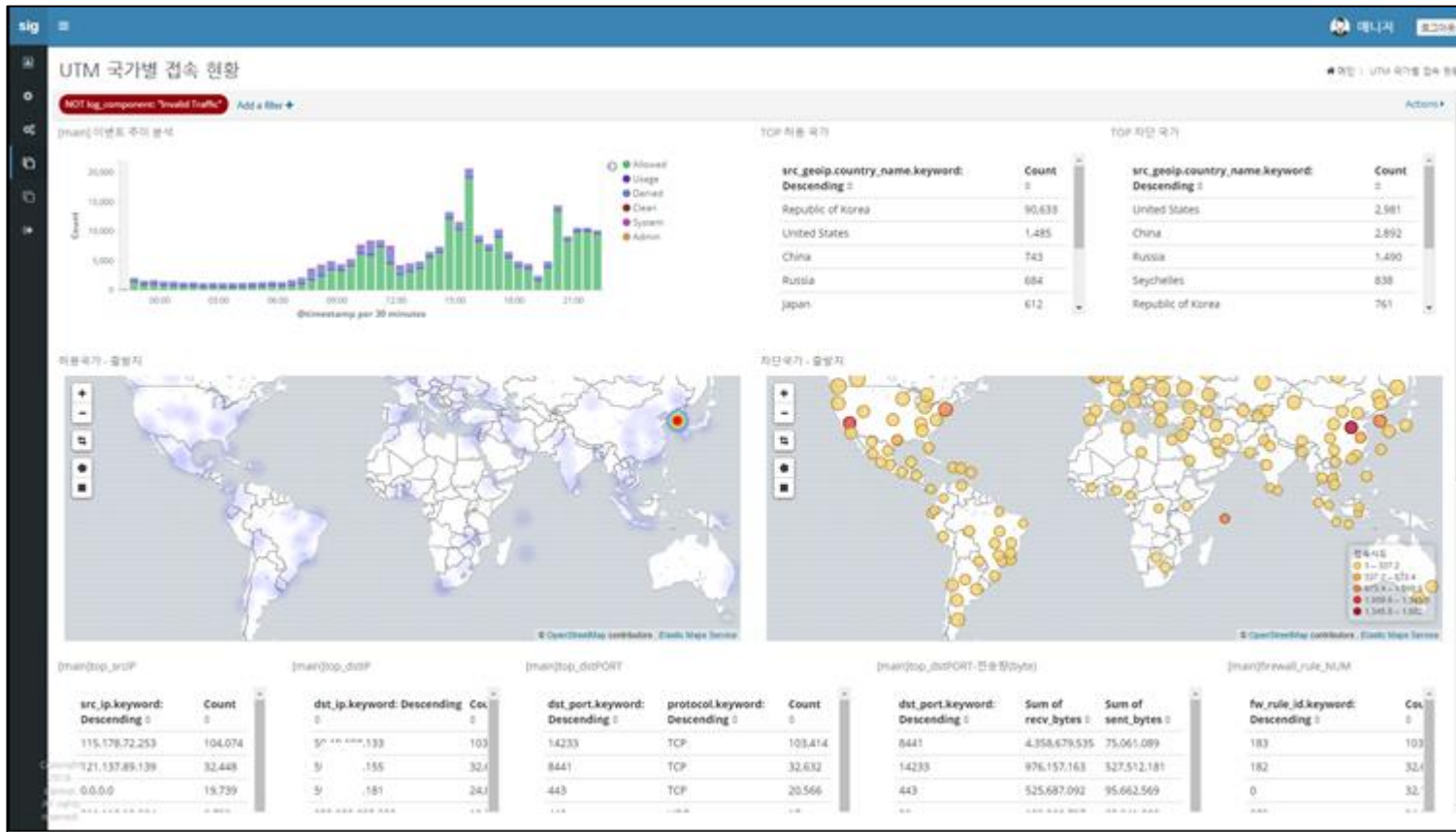


샘플 스크린 샷

국가별 접속 현황

🔍 출발지 및 목적지 IP 주소를 실시간 국가 DB와 비교 Tag 처리하여 정보 수집

- 대다수의 기업은 전세계를 상대로 대외 서비스 및 내부→외부 접속을 하는 경우는 없음
- 국가 정보와 위험 서비스 등 불필요한 접속으로 위협에 처할 수 있음으로 내,외부 불필요한 국가에 대한 접속을 차단 정책을 도출하기 위한 대시보드 구현
- 국내 고객을 위한 웹서버를 전세계에 오픈하여 위험도를 높일 필요가 없는 부분이 단적인 예



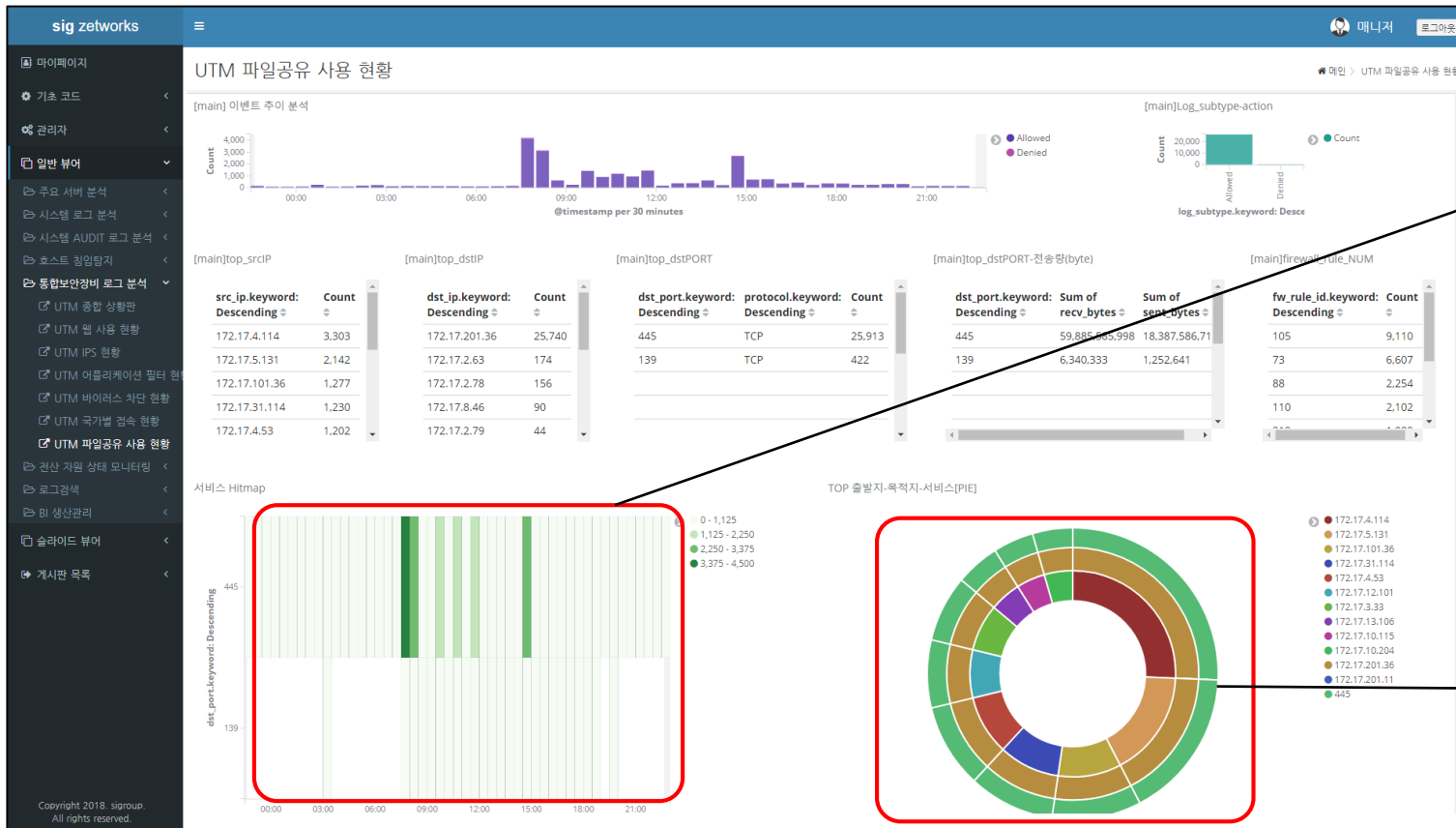
샘플 스크린 샷

특정 이벤트 시 신속 대응 대시보드 활용 사례

🔍 파일공유(CIFS, SMB, Netbios) 프로토콜을 이용한 확산형 랜섬웨어 대응 대시보드(생성 10분정도 소요)

→ 파일공유 프로토콜을 활용한 랜섬웨어 전파 특징을 활용하여 신속하게 대시보드를 제공하여 검출된 단말을 격리하여 위협으로부터 고객사 보호

→ 네트워크 활동 특징에 따른 시각화(현재로부터 24시간 데이터 실시간 대시보드)



특정 시간 활동 후 중단한 단말을 찾기 위해 시계열과 빈도를 시각화

** 많은 빈도 발생 시간대를 Drag 하여 도넛 차트를 통해 해당 단말 검출

1level 출발지, 2level 목적지, 3level 목적지 포트

• 1level 한개에서 2level 다수 차트 발생 시 주의단말 → 공유 등을 다수를 대상으로 동시에 발생되진 않음, 악성코드 전파를 위해서는 필요

🔍 각종 로그 형태 맞는 검색 조건 및 검색 결과 차트를 배치하여 사용자 편의 제공

→ NoSQL 검색 엔진 기반에 검색 조건을 필터함으로 저사양의 서버에서도 신속한 결과 출력(수초)

→ 단점 : 내보내기 기능이 없음, 자체 개발로 해결 진행 중

sig networks

통합보안장비 로그 검색

src_ip.keyword:"10.77.77.51" Add a filter +

[UTM] 검색 조건

출발지: 10.77.77.51, 목적지: Select...

프로토콜: Select..., 목적지 포트: Select...

[main] 이벤트 주이 분석

Count vs @timestamp per 3 hours

Network Basic Search

Time	device_name	fw_rule_id	log_subtype	src_ip	src_port	srczone	dst_ip	dst_port	dstzone	protocol	recv_bytes	sent_bytes
May 15th 2018, 23:01:38.019	XG105	34	Allowed	10.77.77.51	51056	VLAN_2	203.248.252.2	53	WAN	UDP	124	69
May 15th 2018, 23:01:08.012	XG105	34	Allowed	10.77.77.51	51056	VLAN_2	203.248.252.2	53	WAN	UDP	0	0
May 15th 2018, 23:01:04.863	XG105	34	Allowed	10.77.77.51	65150	VLAN_2	65.55.252.93	443	WAN	TCP	132	190
May 15th 2018, 23:00:55.867	XG105	34	Allowed	10.77.77.51	65150	-	65.55.252.93	443	-	TCP	0	0
May 15th 2018, 23:00:49.615	XG105	34	Allowed	10.77.77.51	65141	VLAN_2	65.55.252.93	443	WAN	TCP	132	280
May 15th 2018, 23:00:40.607	XG105	34	Allowed	10.77.77.51	65141	-	65.55.252.93	443	-	TCP	0	0
May 15th 2018, 23:00:39.616	XG105	34	Allowed	10.77.77.51	65150	VLAN_2	65.55.252.93	443	WAN	TCP	0	0
May 15th 2018, 23:00:34.592	XG105	34	Allowed	10.77.77.51	65133	VLAN_2	65.55.252.93	443	WAN	TCP	132	280
May 15th 2018, 23:00:25.596	XG105	34	Allowed	10.77.77.51	65133	-	65.55.252.93	443	-	TCP	0	0
May 15th 2018, 23:00:24.592	XG105	34	Allowed	10.77.77.51	65141	VLAN_2	65.55.252.93	443	WAN	TCP	0	0
May 15th 2018, 23:00:22.343	XG105	0	Denied	10.77.77.51	138	-	10.77.77.255	138	-	UDP	0	0
May 15th 2018, 23:00:19.567	XG105	34	Allowed	10.77.77.51	65109	VLAN_2	65.55.252.93	443	WAN	TCP	132	332
May 15th 2018, 23:00:10.571	XG105	34	Allowed	10.77.77.51	65109	-	65.55.252.93	443	-	TCP	0	0
May 15th 2018, 23:00:09.568	XG105	34	Allowed	10.77.77.51	65133	VLAN_2	65.55.252.93	443	WAN	TCP	0	0
May 15th 2018, 22:59:54.534	XG105	34	Allowed	10.77.77.51	65109	VLAN_2	65.55.252.93	443	WAN	TCP	0	0
May 15th 2018, 22:48:20.131	XG105	0	Denied	10.77.77.51	138	-	10.77.77.255	138	-	UDP	0	0

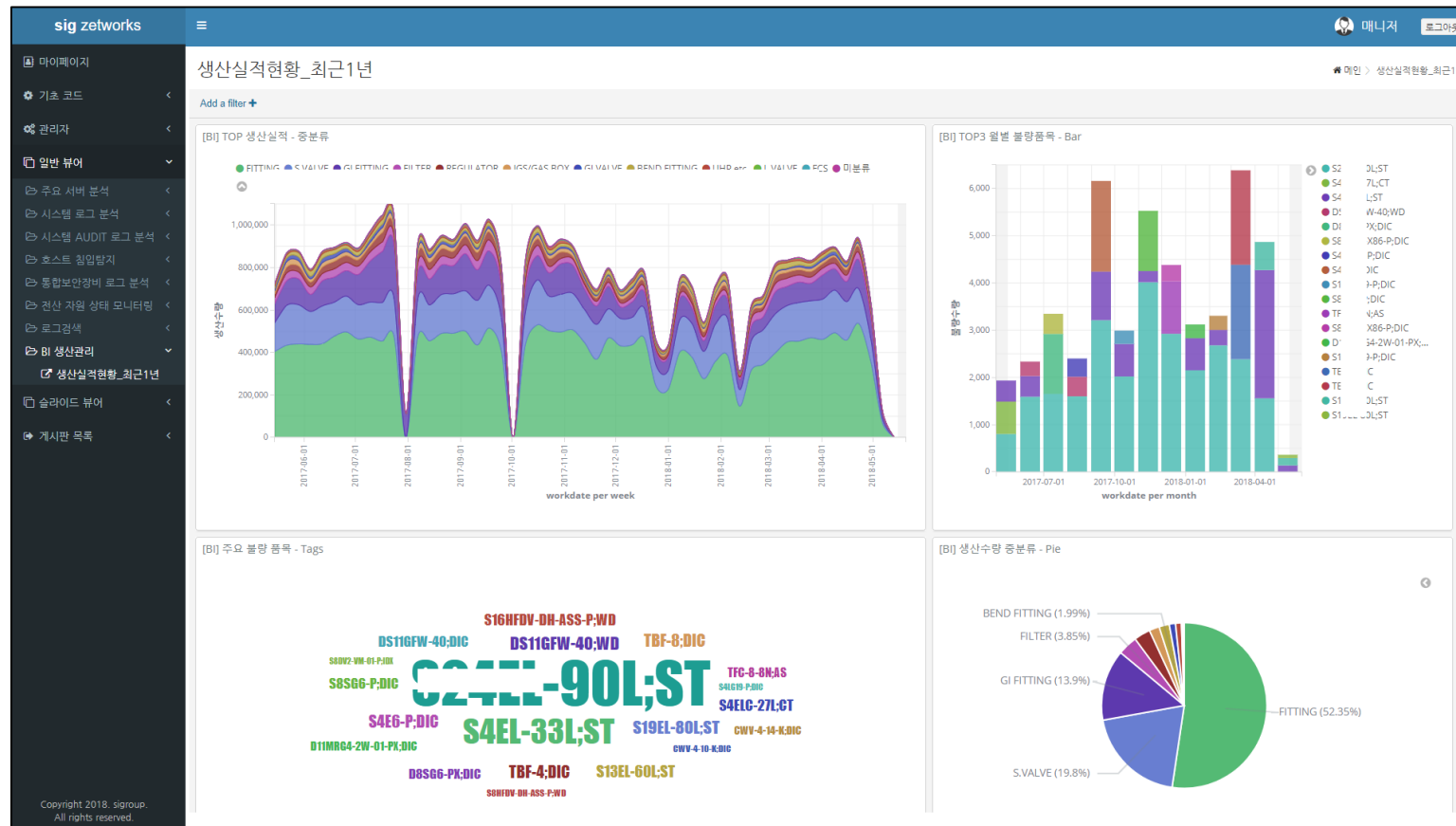
Copyright 2018. sigroup. All rights reserved.

샘플 스크린 샷

ERP RDBMS View Table Insert, Delete, Update Query를 통한 데이터화

🔍 생산 관리 BI 구현 테스트(실제 고객사)

- 상용 개발 도입된 제품보다 활용 및 실시간 처리가 용이하다는 평가
- 기존 솔루션 1일 1번 마감처리를 실시간 처리 및 장기간 신속 분석이 가능한 구조로 변경

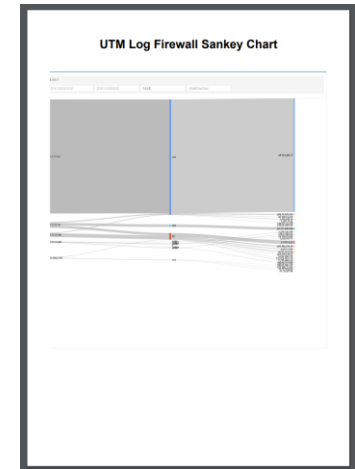
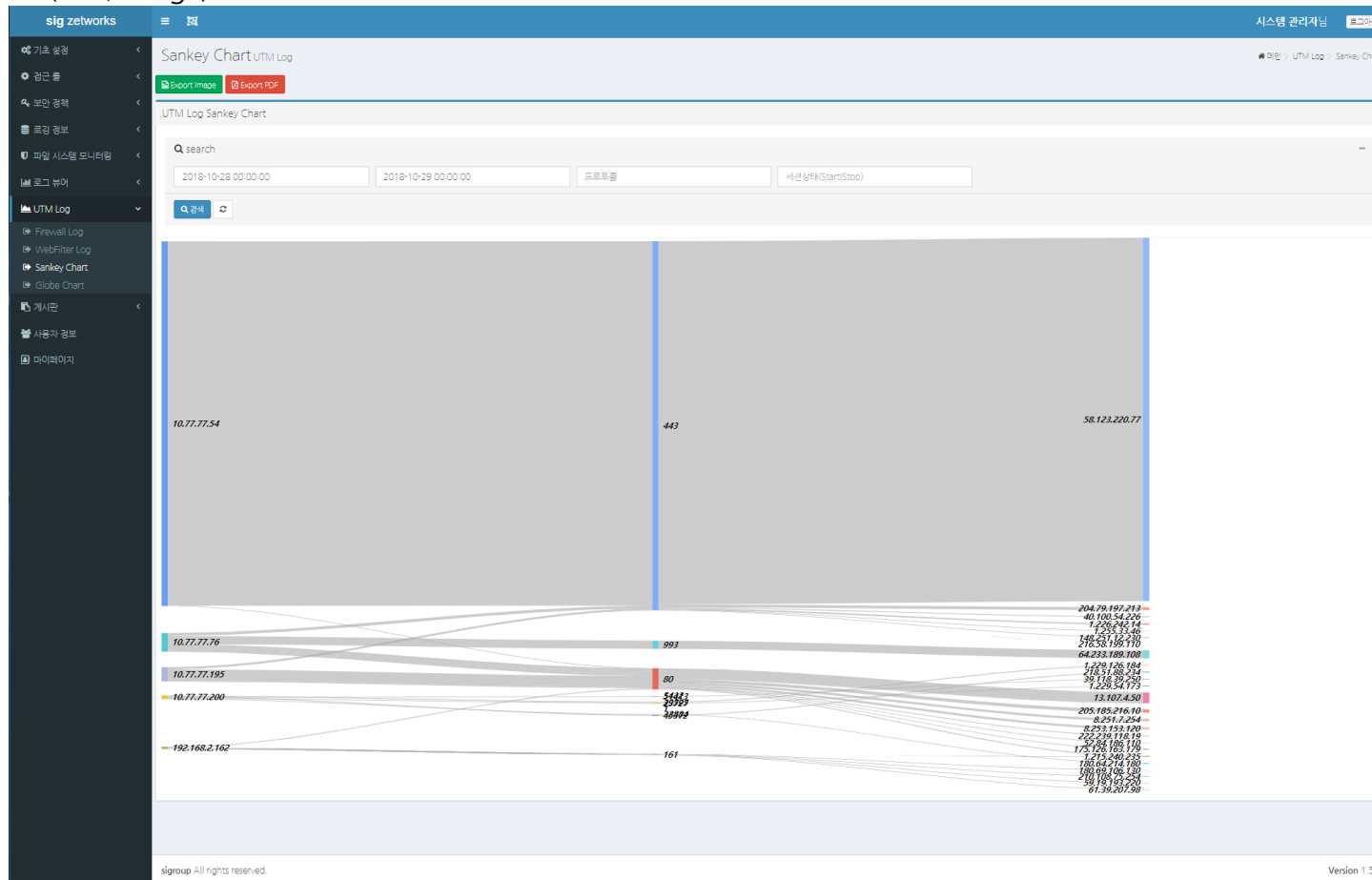


샘플 스크린 샷

네트워크 트래픽 분석 결과 데이터화

네트워크 트래픽에 대한 면밀한 분석 결과 시각화

- 출발지 IP와 목적지 IP 간의 트래픽을 사용하는 Port별 사용량을 시각화
- 조직 내/외부의 네트워크 트래픽을 Process, Port, Service 간의 정의가 가능하며, 이를 통한 보안정책 강화
- Report 추출 가능(PDF, Image)



샘플 스크린 샷

인증 프락시를 통한 관리자 권한 설정

🔍 내부 관리자별 접근 권한 관리

→ 관리자별 권한 제어, 그룹 권한 제어를 통해 대쉬보드 접근 제어

The screenshot displays the 'sig networks' management console. The left sidebar contains a navigation menu with items like '기초 설정', '로그 뷰어', '호스트 관리', and '뷰어 관리'. The main content area is titled '뷰어 정보 설정' and shows configuration options for a user group. Key fields include '그룹명' (Group Name), '그룹순서' (Group Order) set to 1, and '사용여부' (Usage) set to '예' (Yes). Below these, there is a '뷰어 권한' (Viewer Permission) section with a dropdown menu currently showing '이현수 [개발팀 [sigroup > 개발팀]]'. A '뷰어 이름' (Viewer Name) field is also present. At the bottom of the form, there are '저장' (Save) and '목록' (List) buttons. The footer of the page includes 'sigroup All rights reserved.' and 'Version 1.5.0'.



감사합니다.

Faith & Innovation IT Service Partner