

Argos 지능형 침입 탐지 시스템

최종 보고

보안 위협 실시간 감지 및 대응 시스템

팀장 : 이송하

팀원 : 송지연

기존 시스템의 한계점

표층적 분석의 한계

정상적인 통신 포트(80/443)로 위장한 SQL 인젝션, 악성 스크립트와 같은 애플리케이션 계층의 공격을 탐지하지 못합니다.

- 트래픽의 내용이 아닌 '겉 정보'만 분석
- 심층적인 분석 부족
- 정교한 공격 패턴 감지 불가

파편화된 정보의 문제

특정 IP가 특정 포트에 접속했다는 단편적인 사실만 알 수 있을 뿐, 공격의 전체 맥락을 파악할 수 없습니다.

- 전후 행위 파악 불가
- 다른 서버 통신 내용 미상
- 공격 경로 분석 어려움

수동적 대응의 비효율성

문제가 발생한 후에야 수동으로 로그를 분석하기 때문에 실시간 위협에 대한 선제적인 대응이 불가능합니다.

- 대응 시간 지연
- 피해 규모 확대
- 사후 대응에 불과

기존 시스템은 **지능화된 위협에 늦고 단편적으로 대응하는
수동적 구조를 가지고 있어, 자동화된 통합 분석 체계로의 전환이 시급**

일정 관리 - Gantt Chart

프로젝트 진행 현황

전체 프로젝트 진행률



완료된 주요 작업

시스템 아키텍처 설계

프로젝트 목표에 부합하는 확장 가능하고 안정적인 시스템 구조 설계를 완료했습니다.

핵심 데이터 파이프라인 구축

로그 수집 (Filebeat)부터 탐지 (Suricata), 저장 (Elasticsearch), 시각화 (Kibana)에 이르는 실제 데이터 파이프라인을 안정적으로 구축했습니다.

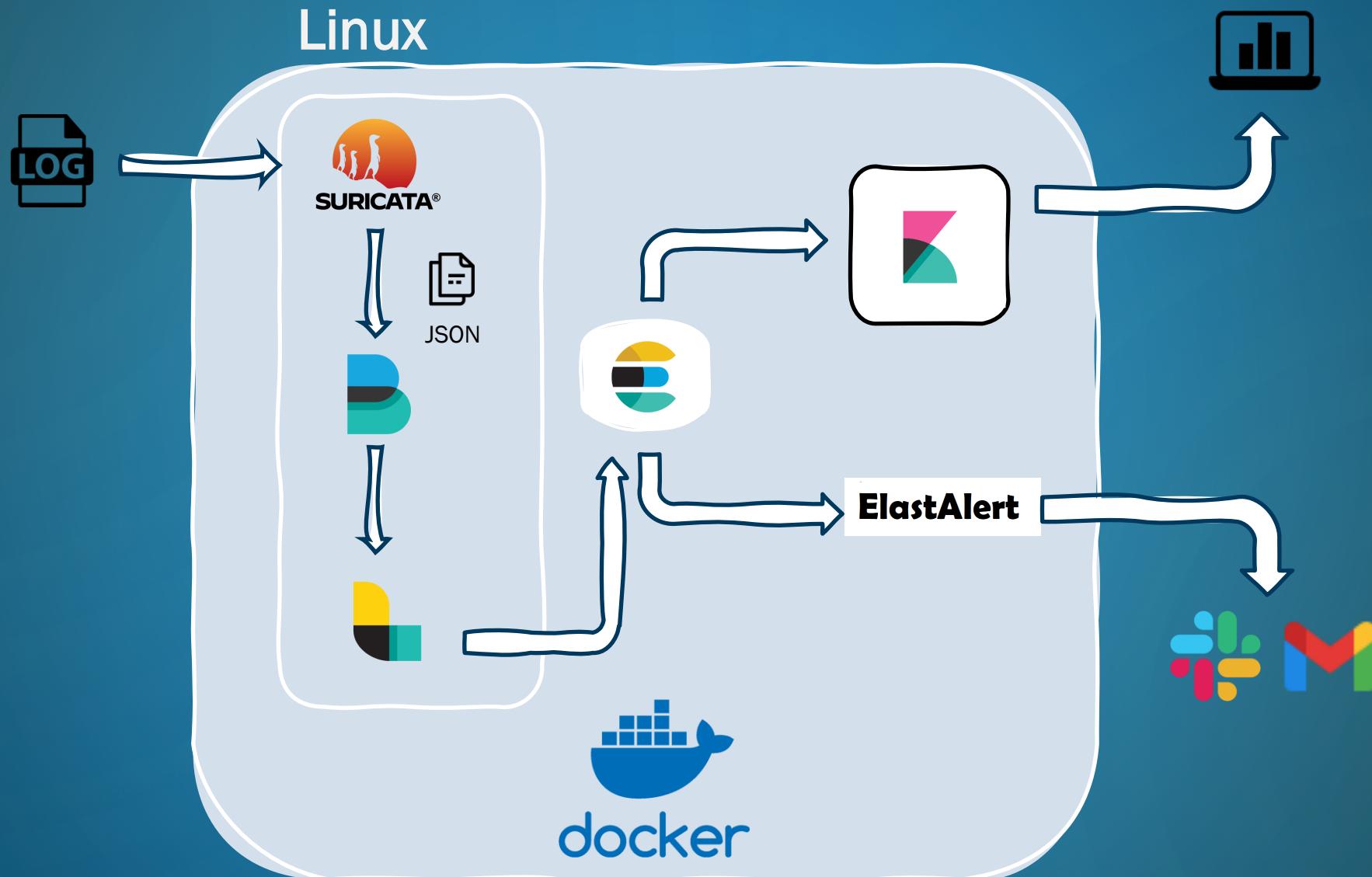
주요 위협 탐지 룰셋 적용

SQL Injection, XSS 등 주요 위협 시나리오를 정의하고 이를 탐지하기 위한 Suricata 룰셋 정책을 구체적으로 구현 및 테스트했습니다.

실시간 통합 대시보드 구성 완료

탐지된 모든 위협 데이터를 실시간으로 모니터링하고 직관적으로 분석할 수 있는 Kibana 통합 대시보드 개발을 완료했습니다.

시스템 아키텍처 및 구성



시스템 환경 구성



인프라



Ubuntu 22.04 LTS ,
Docker version 28.4.0

장기 지원 (LTS) 버전으로
안정성 확보,
컨테이너 환경을 통한
배포 및 관리용이성



CPU: 64-bit, RAM: 8GB 이상



탐지 엔진



8.0

루 기반 네트워크 침입 탐지 시스템
(IDS)



ELK Stack



8.19.4



8.19.4



8.19.4



8.19.4



알림 시스템



2.26.0

Elasticsearch 데이터 기반
실시간 알림 생성

Suricata

- 네트워크 침입 탐지/방지(IDS/IPS) 엔진

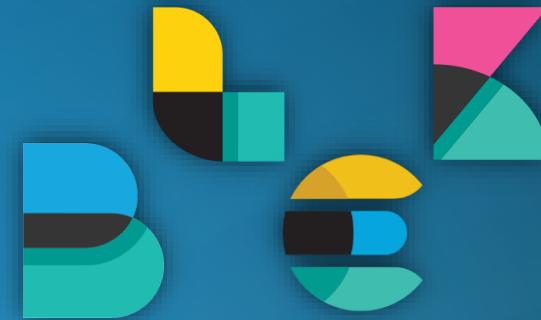


■ 프로젝트 적용 포인트

- 탐지 + 로그(EVE JSON) 수집 용도
- 데이터 흐름
패킷 캡처 → 프로토콜 디코딩(HTTP/SSL/DNS 등) → 정책 매칭 → alert 이벤트 생성 →
`/var/log/suricata/eve.json` → Filebeat/Logstash → Elasticsearch(suricata-*)
- 구성/파일 경로
 - 설정: suricata/suricata.yaml
 - 정책: suricata/rules/ids.rules

Elastic Stack

- Suricata 로그를 대시보드/검색/분석에 제공



프로젝트 적용 포인트

- 역할/구성요소
 - Elasticsearch 8.19.4: 인덱싱·검색·집계(suricata-*)
 - Logstash / Filebeat 8.19.4: 수집·파싱·Enrich(GeoIP, 필드 정규화)
 - Kibana 8.19.4: 대시보드/맵/필터링·탐색
- 데이터 흐름
Suricata(EVE JSON) → Filebeat/Logstash(ECS 맵핑·GeoIP) → Elasticsearch → Kibana(대시보드)
- 구성/파일 경로
 - Filebeat 설정: filebeat/filebeat.yml
 - Logstash 설정: logstash/logstash.yml, logstash/pipeline/pipeline.conf

ElastAlert2

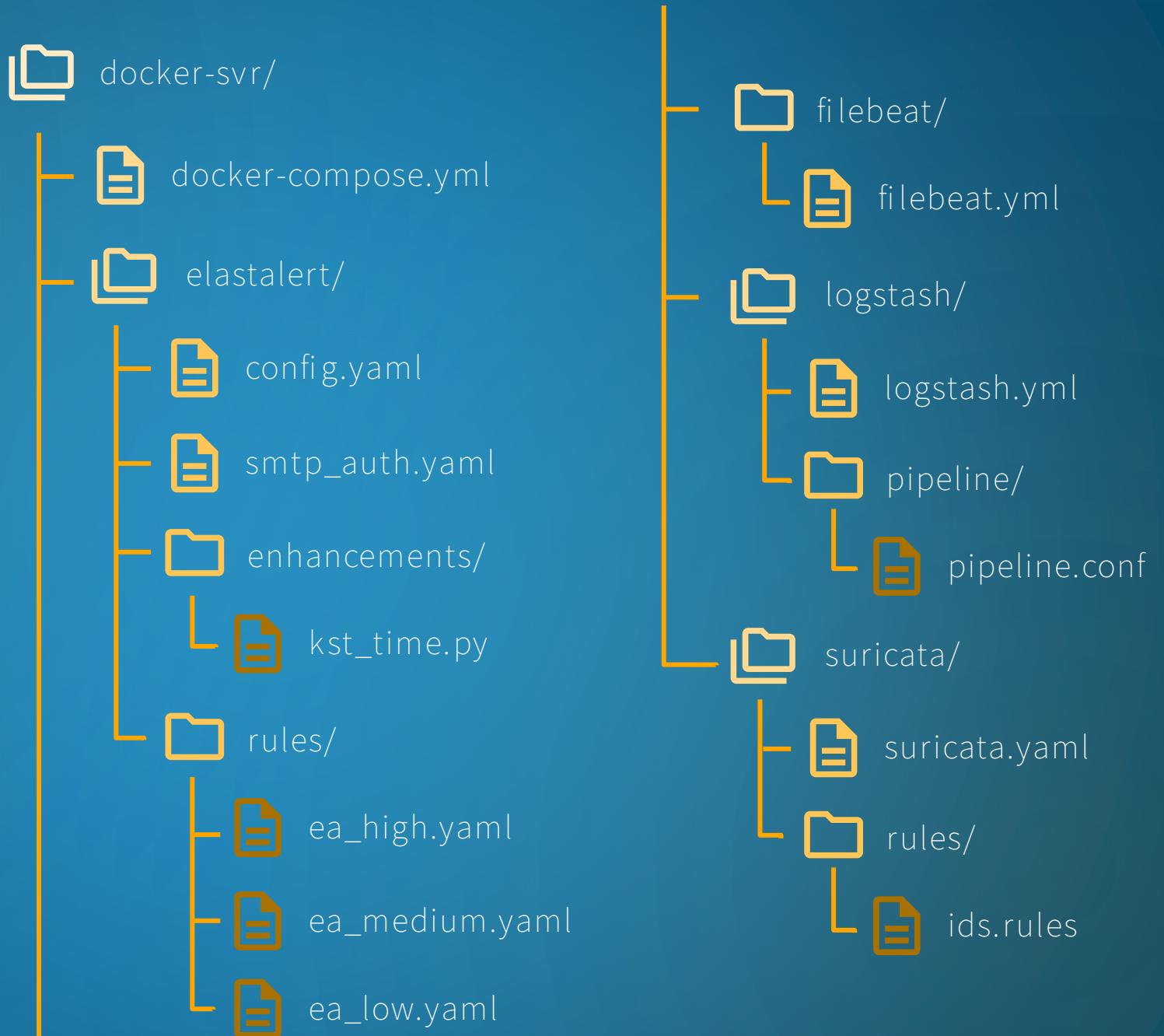
- Elasticsearch 질의 결과가 조건을 만족할 때 실시간 알림을 발송하는 엔진

ElastAlert

| 프로젝트 적용 포인트

- E-mail(SMTP) 알림 발송 용도
- 데이터 흐름
Suricata(EVE JSON) → Filebeat/Logstash(ECS 매팅 · GeoIP) → Elasticsearch → ElastAlert2 (알림)
- 구성/파일 경로
 - 설정: elastalert/config.yaml
 - SMTP 설정: elastalert/smtp_auth.yaml
 - 규칙: elastalert/rules/ea_high.yaml, ea_medium.yaml, ea_low.yaml
 - 기타 스크립트: elastalert/enhancements/kst_time.py(KST 표기)

Docker 디렉터리 구조



Suricata 탐지 정책 _ 정규화

1) 헤더

- 형식: action protocol src_ip src_port -> dst_ip dst_port
- 예시) alert http any any -> \$HOME_NET any

2) 흐름 제약

- flow;
- 효과: 역방향·스캔 노이즈 억제, 오탐·비용 감소

3) sticky buffer 조건

- 정규 패턴
 - http.method; content; → 메서드 한정
 - http.uri.path; content; nocase; → 경로 한정
 - http.request_body; pcre; → 본문 패턴 매칭
- 원칙:
버퍼 → content/pcre 순
가능한 content + nocase 우선

4) 공격 유형 분류 (대분류)

- classtype;

5) 심각도

- priority;

6) 성능/집계 옵션

- fast_pattern;
- detection_filter;

7) 관리 메타

- sid; → 고유 ID
- rev; → 개정 이력

8) 메시지 규칙

- 형식: msg; → 공격유형 분류 (소분류)
- 예시) msg:"SQLi (POST)";

Suricata 탐지 정책_ 웹 애플리케이션 (예시)

SQL Injection (SQL 삽입)

논리기반 탐지

```
# (GET)
alert http any any -> $HOME_NET any (msg:"SQL Logic(GET)"; flow:to_server,established; http.uri.raw; pcre:"/id=.*(%27|')(\+|%20|\s)*or(\+|%20|\s)*1(\+|%20|\s)*(%3d|=)(\+|%20|\s)*1/i";
priority:2; sid:1010101; rev:2; classtype:web-application-attack;)
```

유니언 기반 탐지

```
# (GET)
alert http any any -> $HOME_NET any (msg:"SQL UNION(GET)"; flow:to_server,established; http.uri.raw;
pcre:"/(UNION|%55%4e%49%4f%4e)(?:\+|%20|\\\*.\\*?\\*\|\\s)*(SELECT|%53%45%4c%45%43%54)/i"; priority:2; sid:1010201; rev:3; classtype:web-application-attack;)
```

에러 기반 탐지

```
# (POST)
alert http any any -> $HOME_NET any (msg:"SQL Error-based(POST)"; flow:to_server,established; http.method; content:"POST"; http.request_body;
pcre:"/(EXTRACTVALUE|%45%58%54%52%41%43%54%56%41%4c%55%45|UPDATEXML|%55%50%44%41%54%45%58%4d%4c)\s*/i"; priority:2; sid:1010302; rev:3; classtype:web-application-attack;)
```

블라인드 탐지

```
# 시간기반 (GET)
alert http any any -> $HOME_NET any (msg:"SQL Blind-Time(GET)"; flow:to_server,established; http.uri.raw;
pcre:"/(SLEEP|%53%4c%45%45%50)(?:\+|%20|\\\*.\\*?\\*\|\\s)*(?:\\(|%28)|(BENCHMARK|%42%45%4e%43%48%4d%41%52%4b)(?:\+|%20|\\\*.\\*?\\*\|\\s)*(?:\\(|%28)/i"; priority:2; sid:1010501; rev:3;
classtype:web-application-attack;)
```

Suricata 탐지 정책_ 웹 애플리케이션 (예시)

XSS (Cross-Site Scripting)

반사형(Reflected)

```
# (GET)
alert http any any -> $HOME_NET any (msg:"XSS Reflected(GET)"; flow:to_server,established; http.uri.raw;
pcre:"/((%3c|<)\s*script\b)|((%3c|<)[^>]*\bon(?:error|load|click|mouseover)\b(?:\+|\%20|\s)*(?:=|\%3[dD]))|(\bjavascript\s*:(?:%20|\+)?|\%6a%61%76%61%73%63%72%69%70%74\s*:)/i"; priority:2;
sid:1020101; rev:6; classtype:web-application-attack;)
```

저장형(Stored)

```
# (POST)
alert http any any -> $HOME_NET any (msg:"XSS Stored(POST)"; flow:to_server,established; http.method; content:"POST"; http.request_body; pcre:"/((%3c|<)\s*script\b)|((%3c|<)[^>]*\bon[a-z]+\b(?:\+|\%20|\s)*(?:=|\%3[dD]))|(\bjavascript\s*:(?:%20|\+)?|\%6a%61%76%61%73%63%72%69%70%74\s*:)/i"; priority:2; sid:1020202; rev:6; classtype:web-application-attack;)
```

DOM

```
# (RESP)
alert http $HOME_NET any -> any any (msg:"XSS DOM(RESP)"; flow:from_server,established; file_data;
pcre: "/((location\.(hash|search))|(document\.(URL|location|referrer))|(window\.\name)).{0,120}(document\.write|innerHTML|outerHTML|insertAdjacentHTML|eval|Function|setTimeout|setInterval)|(document\.write|innerHTML|outerHTML|insertAdjacentHTML|eval|Function|setTimeout|setInterval).{0,120}((location\.(hash|search))|(document\.(URL|location|referrer))|(window\.\name))/i";
priority:3; sid:1020303; rev:1; classtype:web-application-activity;)
```

Suricata 탐지 정책_ 웹 애플리케이션 (예시)

Command Injection (명령어 삽입)

In-band

```
# (POST)
alert http any any -> $HOME_NET any (msg:"Cmd Injection In-band(POST)"; flow:to_server,established; http.uri.raw; content:"/vulnerabilities/exec/"; nocase; http.method; content:"POST";
http.request_body; pcre:"/(?:%26%26)%7C%3B|&&|\x7C|\x3B)(?:\+|%20|\s)*(?!(%sleep|ping|timeout)\[|[%5[Bb]|test]\b)(?:id|whoami|uname|ifconfig|pwd|ls|cat|netstat|wget|curl)\b/i"; priority:2;
sid:1030102; rev:11; classtype:web-application-attack;)
```

Blind

```
# Boolean 기반 (GET)
alert http any any -> $HOME_NET any (msg:"Cmd Injection Blind-Boolean(GET)"; flow:to_server,established; http.uri.raw; content:"/vulnerabilities/exec/"; nocase;
pcre:"/(?:%26%26)%7C%3B|&&|\x7C|\x3B|\x60|\$|(|(?:\+|%20|\s)*(?:%65[Bb])|(|(?:\+|%20|\s)*(?:d+)?(?:\+|%20|\s)*(?:eq|ne|lt|le|gt|ge|=|=|(?:\+|%20|\s)*(?:d+)?(?:\+|%20|\s)*(?:%5[Dd])|)|test(?:\+|%20|\s)+(?:e|f|d|w|r|x|s|n|z))/i"; pcre:"/\b(?:id|whoami|uname|ifconfig|pwd|ls|cat|netstat|wget|curl)\b/i";
pcre:"/\b(?:sleep|ping|timeout)\b/i"; priority:2; sid:1030201; rev:5; classtype:web-application-attack;)
```

Out-of-band(OOB)

```
# DNS
alert dns $HOME_NET any -> $EXTERNAL_NET 53 (msg:"Cmd Injection OOB(DNS)"; xbits:isset,cmdi.marker,track ip_src; flow:to_server; dns.query; content:".oob.lab"; nocase; classtype:trojan-
activity; priority:1; sid:1030411; rev:4;)
```

Suricata 탐지 정책 _ 웹 애플리케이션 (예시)

File Inclusion

LFI

```
# (GET)
alert http any any -> $HOME_NET any (msg:"LFI Sensitive(GET)"; flow:to_server,established; http.uri.raw;
pcre:"/(?:etc\passwd|etc\shadow|etc\hosts|proc\self\environ|var\log\auth\log\windows(?:\\|\%5c)win\ini|boot\ini)/i"; classtype:web-application-attack; priority:1;
sid:1040101; rev:2;)
```

RFI

```
# (POST)
alert http any any -> $HOME_NET any (msg:"RFI Attempt(POST)"; flow:to_server,established; http.method; content:" POST" ; http.request_body;
pcre:"/(?:^|&)(?:page|file|include|inc|path|template|tmpl|tpl|module)=(?:https?:\/\/[A-Za-z0-9._:%\/?#=&-]{6,})/i"; classtype:web-application-attack; priority:1; sid:1040202; rev:2;)
```

Malicious Upload

악성 스크립트(.html .js) 업로드

```
# (POST)
alert http any any -> $HOME_NET any (msg:" File Upload HTML/JS+Script(POST)"; flow:to_server,established; http.method; content:" POST" ; http.request_body;
pcre:"/filename\s*=\s*\\"[^\"\n]+?\.(?:html?|js)\\"/i"; pcre:"/(<%3c)\s*script\b/i"; classtype:web-application-attack; priority:1; sid:1050502; rev:2;)
```

Suricata 탐지 정책 _ 서비스 거부 (Dos), 시스템 및 서비스 공격 (예시)

TCP SYN Flood

```
alert tcp any any -> $HOME_NET [80,443] (msg:"SYN-Flood(TCP)"; flags:S; flow:to_server,stateless; threshold:type both,track by_src,count 1000,seconds 5; classtype:attempted-dos; priority:1; sid:2010100; rev:4;)
```

ICMP Smurf

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Smurf-Reply(ICMP)"; itype:0; threshold:type both,track by_dst,count 200,seconds 5; classtype:attempted-dos; priority:1; sid:2020100; rev:2;)
```

Brute Force / Password Spraying

```
# (TCP)
alert tcp any any -> $HOME_NET 22 (msg:"Brute-Force(SSH)"; flags:S; flow:to_server,stateless; threshold:type both,track by_src,count 50,seconds 30; classtype:attempted-recon; priority:2; sid:3010100; rev:1;)
```

Scan/Bruteforce

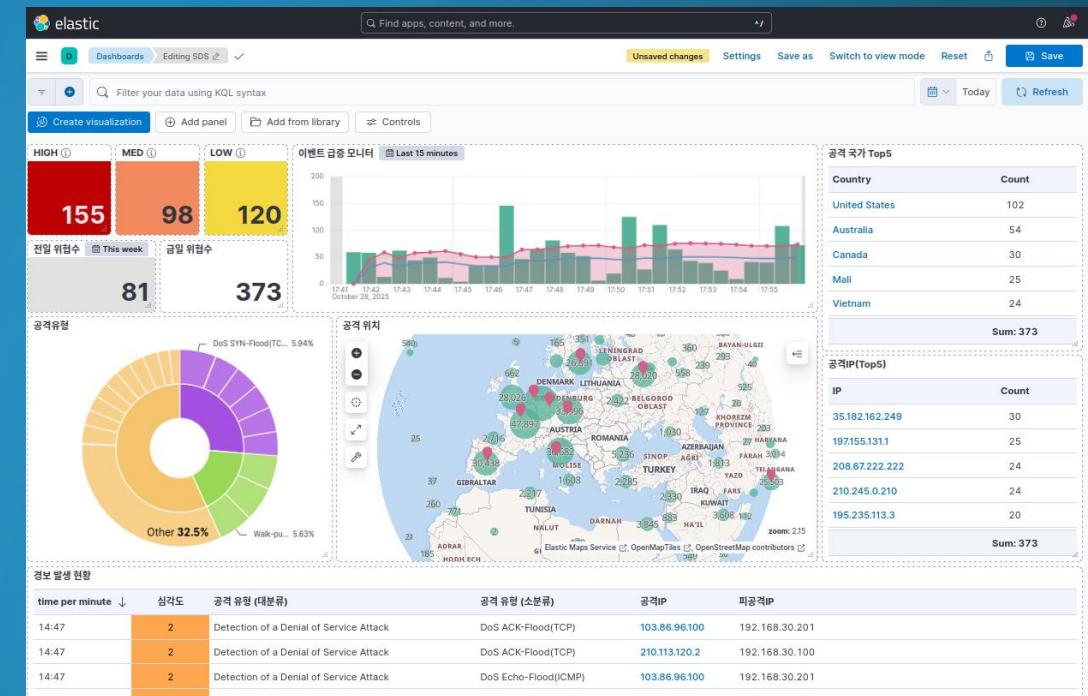
```
# (TCP)
alert tcp any any -> $HOME_NET 445 (msg:"Scan/Bruteforce(SMB)"; flags:S; flow:to_server,stateless; threshold:type both,track by_src,count 80,seconds 30; classtype:attempted-recon; priority:3; sid:3030100; rev:1;)
```

데이터 분석 및 시각화 대시보드

주요 데이터 필드

@timestamp	이벤트 수집/색인 시작
alert.severity	경보 심각도
alert.category.keyword	경보 카테고리
alert.signature.keyword	탐지 종류 이름
source.ip	공격자 IP
dest_ip	희생자 서버 IP
source.geo.country_name	공격자 국가명
source.geo.city_name	공격자 지역명
source.geo.location	IP의 좌표(geo_point)

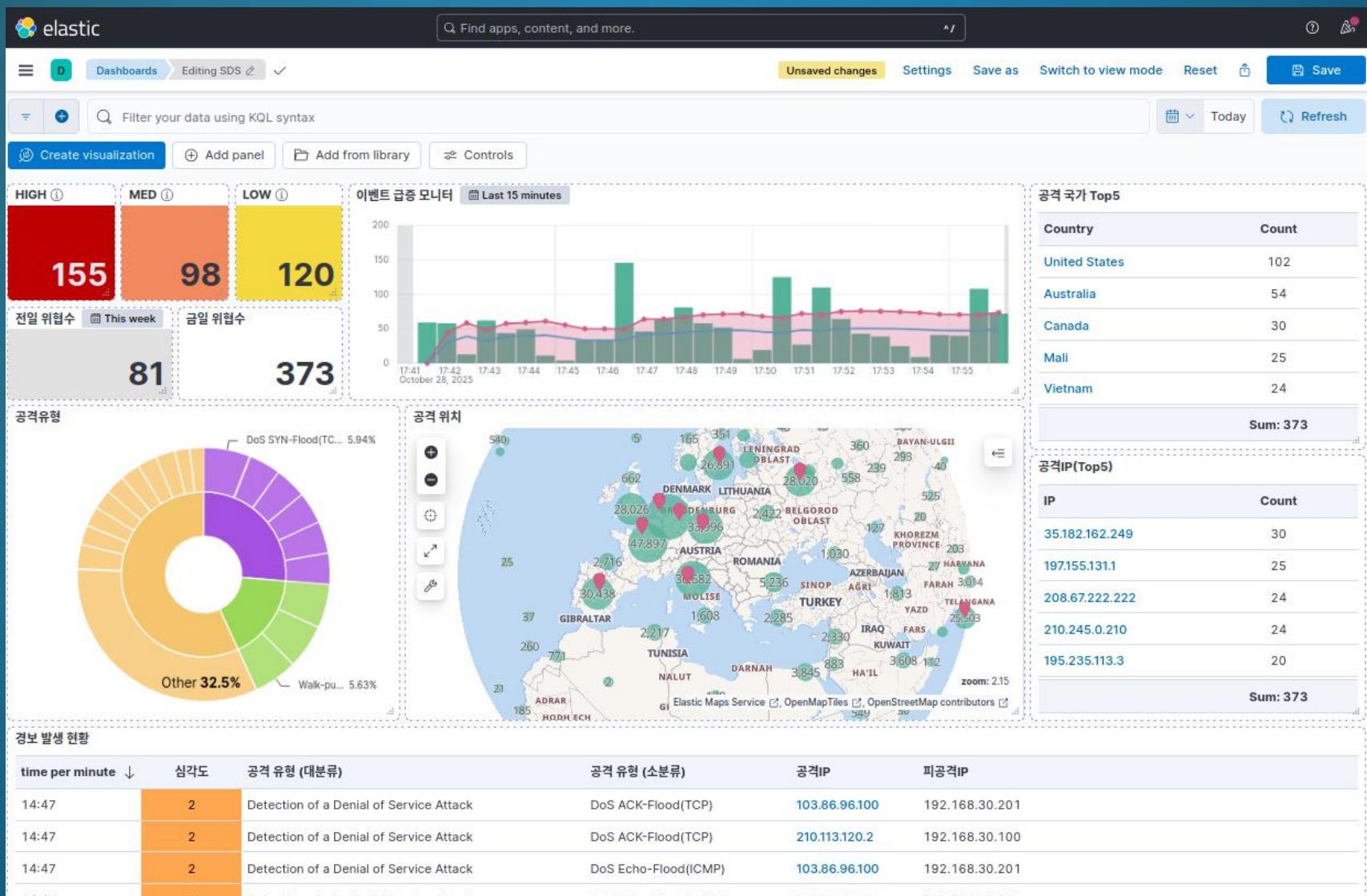
실제 대시보드 스크린샷



탐지된 모든 위협 데이터를 실시간으로 모니터링하고 분석할 수 있습니다.

지리적 위치 기반 공격 추적과 다양한 필터링 옵션을 통해 효율적인 보안 관리를 지원합니다.

대시보드 구성



대시보드 패널 구성

The dashboard displays three main KPI cards:

- HIGH**: Value 201
- MED**: Value 209
- LOW**: Value 128

Below the cards, there are several data visualizations and tables:

- 공격 유형**: Donut chart showing attack types. Legend: DoS SYN-Flood(TCP) 5.94%, Other 32.5%, Walk-up 61.56%
- 공격 위치**: Map visualization showing attack locations.
- 경보 발생 현황**: Table showing events per minute. Data:

time per minute	심각도	공격 유형 (대분류)
14:47	2	Detection of a Denial of Service Attack
14:47	2	Detection of a Denial of Service Attack
14:47	2	Detection of a Denial of Service Attack
- 공격 유형 (소분류)**: Table showing detailed attack types. Data:

공격 유형 (소분류)	공격IP	피공격IP
DoS ACK-Flood(TCP)	103.86.96.100	192.168.30.201
DoS ACK-Flood(TCP)	210.113.120.2	192.168.30.100
DoS Echo-Flood(ICMP)	103.86.96.100	192.168.30.201
- 공격 국가 Top5**: Table showing top 5 countries. Data:

Country	Count
United States	102
Australia	54
Canada	30
Mal	25
Vietnam	24

Sum: 373
- 공격 IP (Top5)**: Table showing top 5 attacking IPs. Data:

IP	Count
35.182.162.249	30
203.67.222.222	25
203.67.222.222	24
203.67.222.222	24
203.67.222.222	20

Sum: 373

1) 심각도 요약 카드 (HIGH/MED/LOW)

- 색상별 카드의 숫자로 해당 심각도의 누적 경보 수를 나타냄
- 선택한 시간 범위에서 심각도별 경보 건수의 총합을 즉시 파악
- 대응 우선순위 수립(High → Med → Low) 가능, 시간 범위 변경 시
부하 변화 비교

대시보드 패널 구성

The dashboard displays the following key metrics:

- 전일 위협수 (This week):** 81
- 금일 위협수 (This week):** 538
- 경보 발생 현황 (time per minute):** Shows three entries at 14:47 for "Detection of a Denial of Service Attack".
- 공격 국가 Top5:**

Country	Count
United States	102
Australia	54
Canada	30
Mali	25
Vietnam	24

Sum: 373
- 공격 IP Top5:**

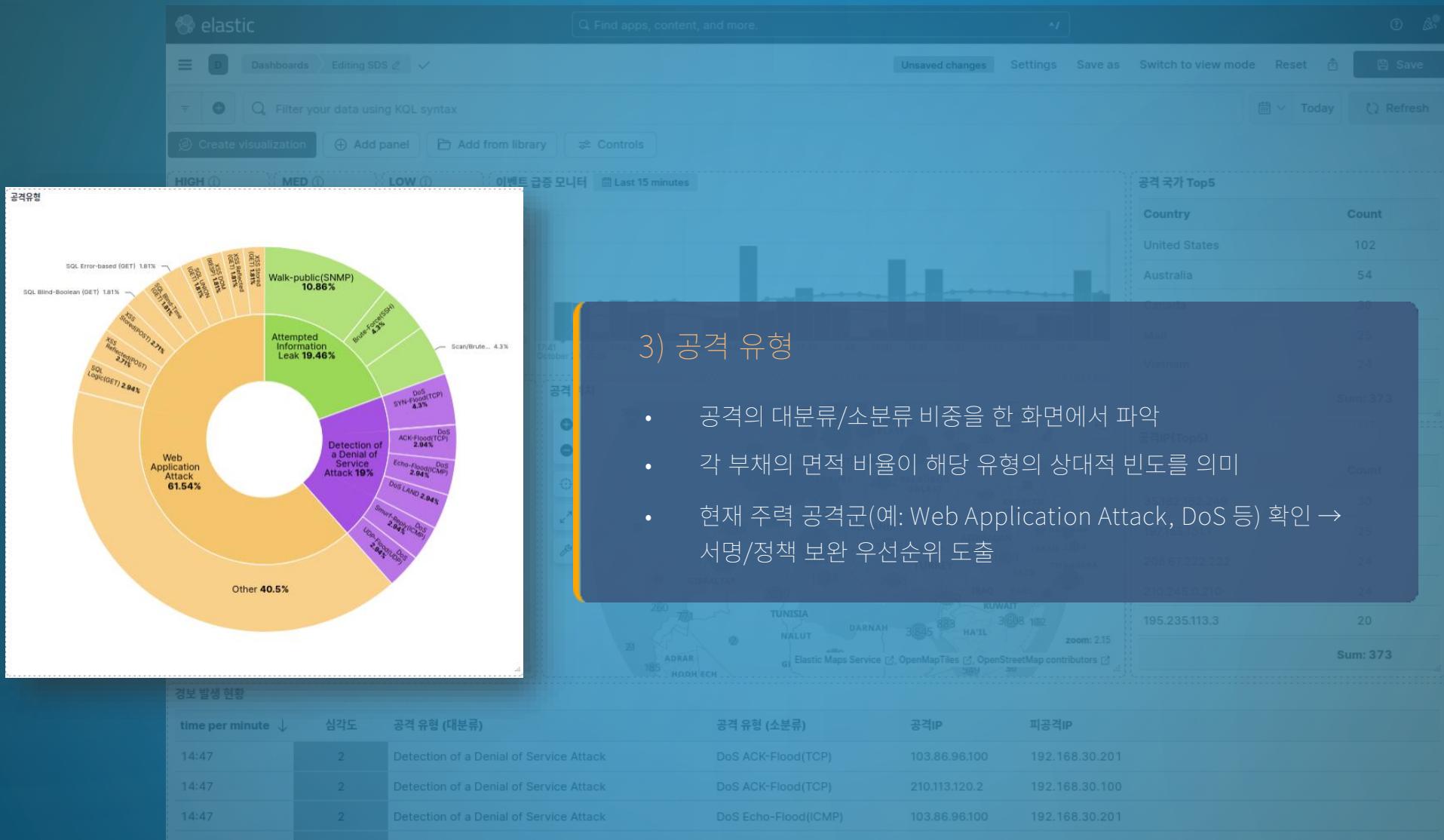
IP	Count
103.86.98.100	25
192.168.30.201	24
208.67.222.222	24
197.155.131.1	20
195.236.113.3	20

Sum: 373

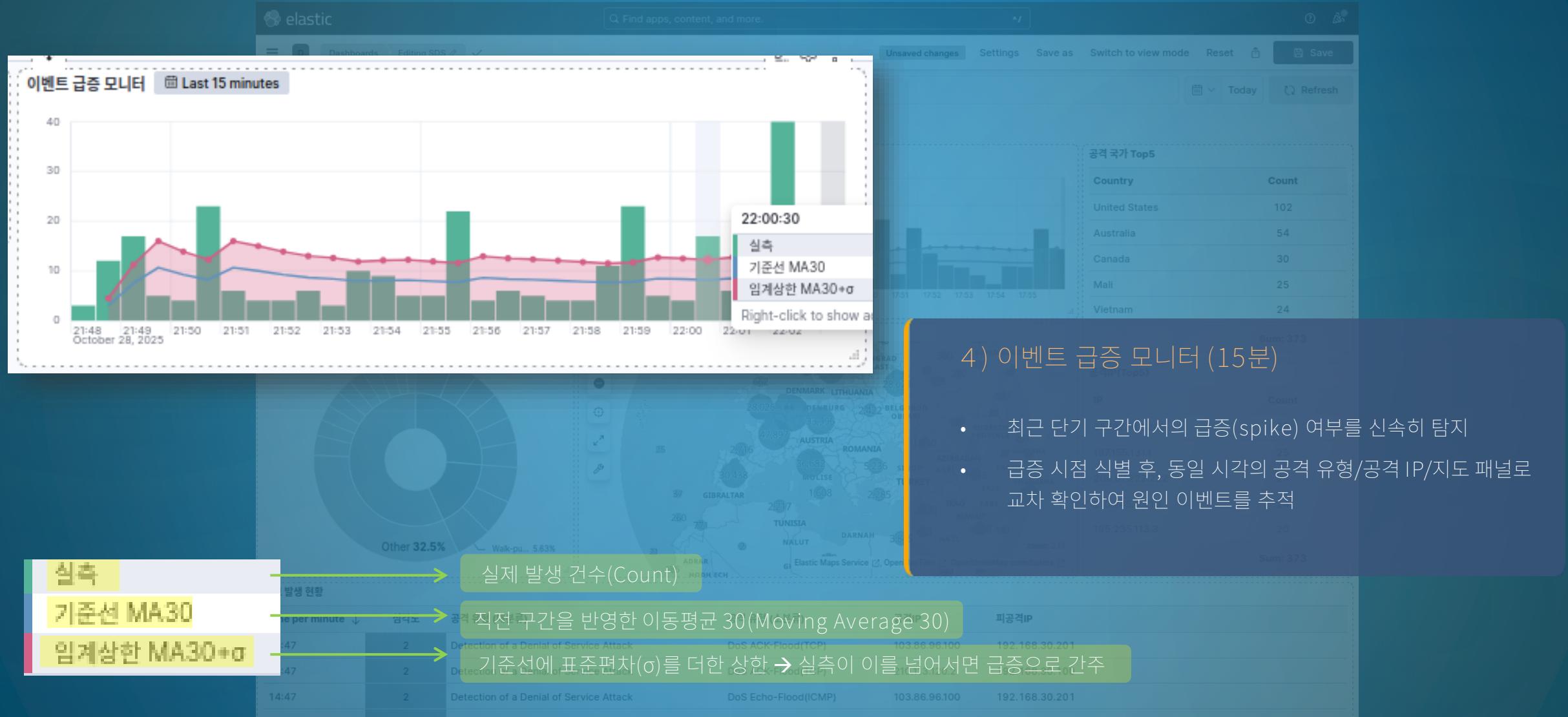
2) 전일 위협수 / 금일 위협수

- 전일(00:00~24:00)과 금일(당일 00:00~현재) 누적 경보 수를 분리 표시
- 두 지표의 절대값/증감을 비교하여 오늘의 상대적 부하를 평가
- 일별 이상 증가 탐지, 운영 리소스 배분 근거로 활용

대시보드 패널 구성



대시보드 패널 구성



대시보드 패널 구성

5) 공격 국가, 공격 IP Top5

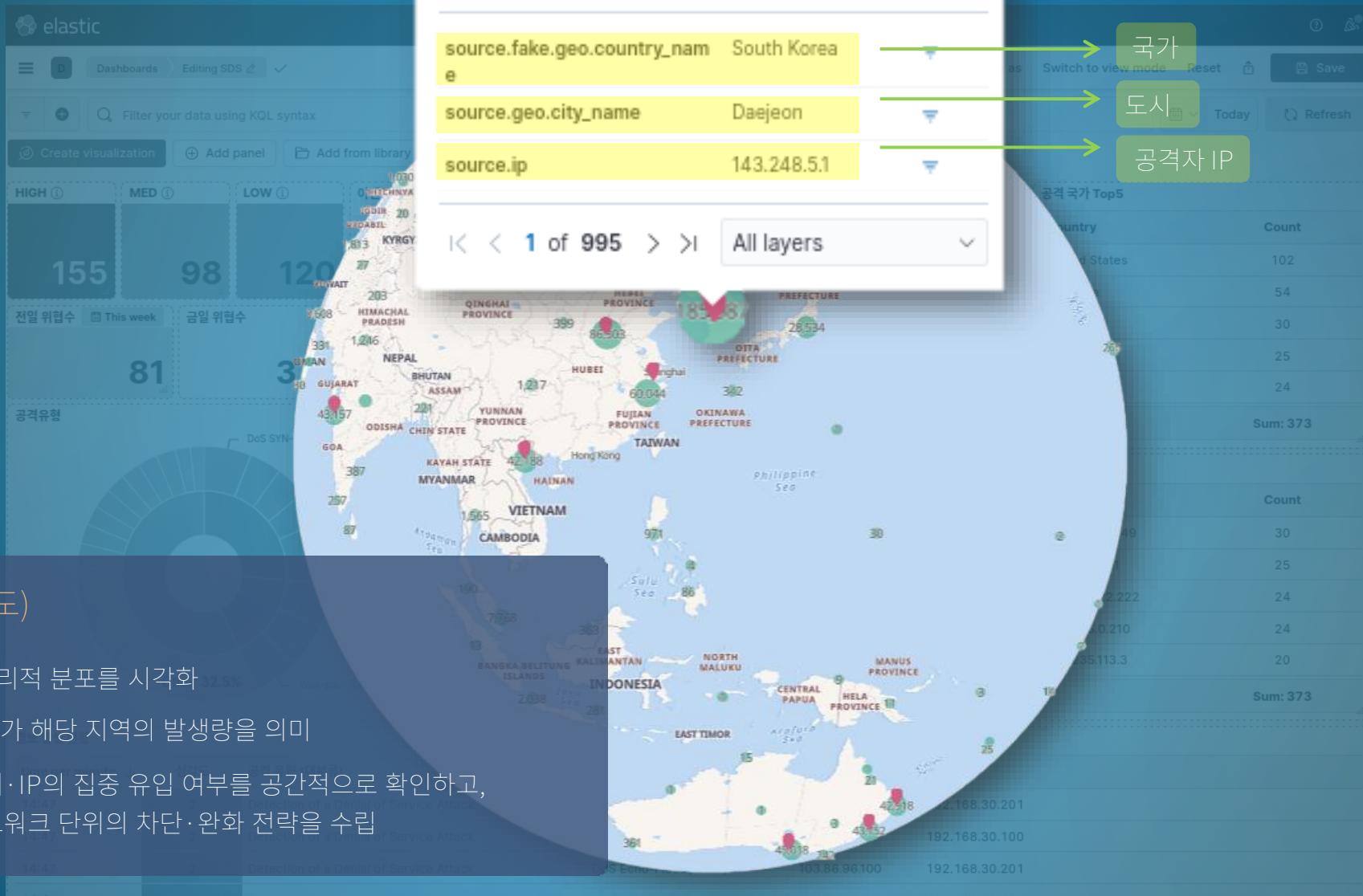
- 국가와 개별 IP 단위의 상위 공격원을 함께 제시하여 빠른 우선대상 선정을 지원
- 국가/지역 단위 차단 정책(Geo-IP, WAF) 방향성 설정에 활용

The screenshot shows two side-by-side dashboards from the Elastic Stack interface. The left dashboard, titled '공격 국가 Top5', displays a table of countries and their attack counts. The right dashboard, titled '공격IP(Top5)', displays a table of IP addresses and their attack counts. Both dashboards have a total count of 538 attacks. The background features a world map with various attack volumes indicated by bubble sizes.

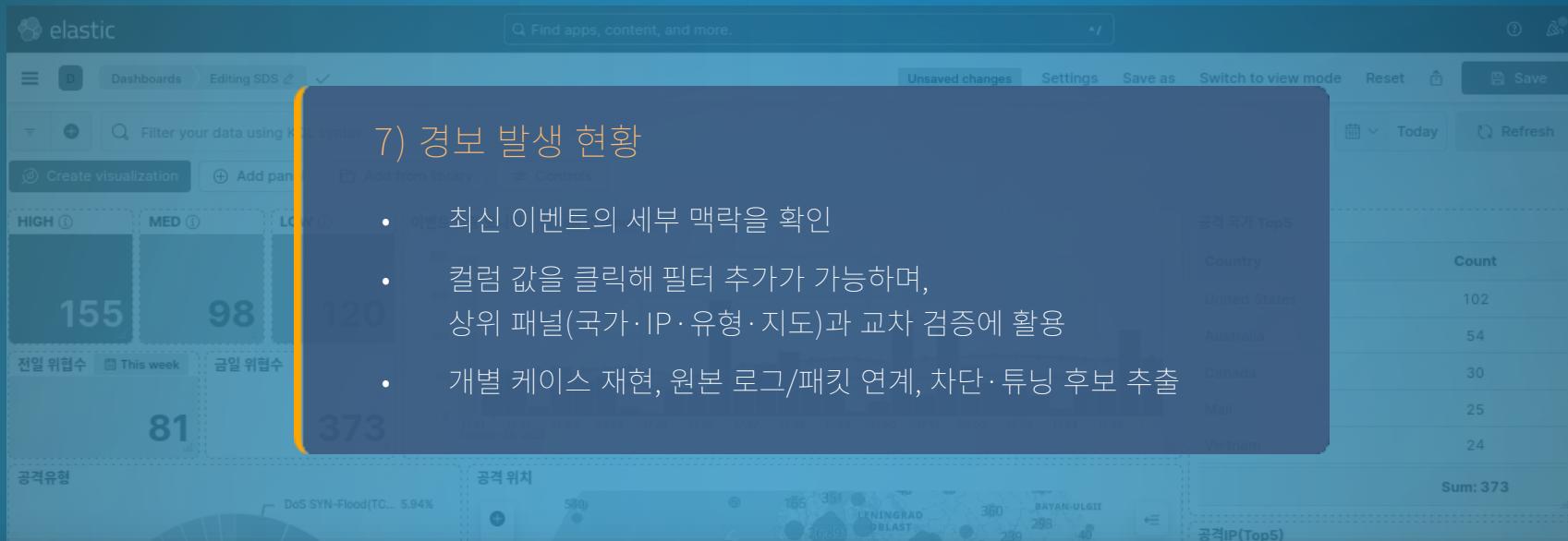
Country	Count
United States	154
Australia	73
Canada	32
South Korea	29
Vietnam	27
Other	223
Sum:	538

IP	Count
35.182.162.249	32
157.240.22.35	27
208.67.222.222	27
210.245.0.210	27
197.155.131.1	26
Other	399
Sum:	538

대시보드 패널 구성



대시보드 패널 구성



경보 발생 현황						
time per minute ↓	심각도	공격 유형(대분류)	공격 유형(소분류)	피공격IP	공격IP	Country
20:55	2	Web Application Attack	XSS Stored(POST)	192.168.30.100	210.113.120.2	South Korea
20:48	1	access to a potentially vulnerable web application	Uploaded File Access(GET)	192.168.30.100	194.116.110.20	Italy
20:44	1	Attempted Denial of Service	Echo-Flood(ICMP)	192.168.30.100	9.9.9.9	United States
20:34	2	Web Application Attack	SQL Error-based(GET)	192.168.30.100	101.100.100.100	New Zealand
20:34	2	Web Application Attack	SQL UNION(POST)	192.168.30.100	193.111.132.132	Czechia
20:29	1	Attempted Denial of Service	SYN-Flood(TCP)	192.168.30.100	201.175.4.29	Mexico
20:28	3	access to a potentially vulnerable web application	CSRF Form-NoToken(RESP)	192.168.30.201	1.1.1.3	Australia
20:28	3	access to a potentially vulnerable web application	CSRF Form-NoToken(RESP)	192.168.30.201	9.9.9.9	United States

실시간 알림 (ElastAlert2 → G-mail)

The image shows two overlapping Gmail windows. The top window displays a list of 393 messages, with several ElastAlert notifications visible. The bottom window shows a detailed view of one specific alert message.

Top Window (List View):

- Search bar: 메일 검색
- Status: 활성
- Message count: 393개 중 1-50
- Messages:
 - ElastAlert: [MED] Alert - 오후 2:46
 - ElastAlert: [LOW] Alert - 오후 2:42
 - ElastAlert: [HIGH] Alert - 오후 2:39
 - ElastAlert: [MED] Alert - 오후 2:39
 - ElastAlert: [LOW] Alert - 오후 2:19
 - ElastAlert: [LOW] Alert - 오후 2:16
 - ElastAlert: [HIGH] Alert - 오후 2:15
 - ElastAlert: [MED] Alert - 오후 2:13
 - ElastAlert: [HIGH] Alert - 오후 2:06
 - ElastAlert: [HIGH] Alert - 오후 2:02

Bottom Window (Detail View):

- Search bar: 메일 검색
- Status: 활성
- Message count: 393개 중 1개
- Message details:
 - From: 2507347007@gospace.kopo.ac.kr (나에게)
 - Date: 오후 2:46 (55분 전)
 - Subject: ElastAlert: [MED] Alert
 - Content:
 - ▶ 200.27.18.2 → 192.168.30.100
 - Sev: 2
 - Cat: Detection of a Denial of Service Attack
 - Sign: DoS SYN-Flood(TCP)
 - Proto: ICMP
 - Iface: ens33
 - Index: suricata-2025.10.28
 - Time: 2025-10-28 14:45:58 KST

탐지 알람 세부 정보 분석

ElastAlert: [HIGH] Alert 받은편지함 ×

2507347007@gspace.kopo.ac.kr
나에게 ▾

🚩 200.27.18.2 → 192.168.30.100 (1410 → 80)

- Sev: 1
- Cat: Attempted Denial of Service
- Sign: SYN-Flood(TCP)
- Proto: TCP
- Iface: ens33
- Index: suricata-2025.10.28
- Time: 2025-10-28 21:06:13 KST

알림 분석표

분석 항목	알림 내용
SRC → DST	공격원/대상 식별
Sev	1=High, 2=Med, 3=Low
Cat	대분류 (ex. DoS, Web App Attack)
Sign	소분류 (탐지 시그니처)
Proto	프로토콜 (ex. TCP/UDP/ICMP)
Iface	유입 인터페이스
Index	저장 위치 (suricata-YYYY.MM.DD)
Time	사건 시각

심각도	내용	목표 대응시간	조치 내용 및 담당
HIGH	서비스 중단·침해로 직결 가능성 높음	5분 이내	즉시 차단·격리
MED	재시도·확산 시 영향 가능	30분 이내	단기 모니터+조건부 차단
LOW	정보수집·오탐 가능	영업일 내	관찰·룰 정비

시연_실제 알림 탐지 확인

Find apps, content, and more.

Switch to view mode Reset Save

Filter your data using KQL syntax

Create visualization Add panel Add from library

전일 위협수 This week 금일 위협수

81 537

HIGH (201) MED (208) LOW (128)

공격유형

Walk-public(SNMP) 10.88%
Brute-Force... 4.31%
Scan/Bri... 4.31%
DoS S... 4.31%
DoS... 2.95%
Other 40.59%

Gmail 메일 검색 활성

ElastAlert: [HIGH] Alert - 오후 9:07
ElastAlert: [HIGH] Alert - 오후 9:03
ElastAlert: [MED] Alert - 오후 9:00
ElastAlert: [HIGH] Alert - 오후 8:57

419개 중 1-50 < >

국가 Top5

Country	Count
United States	154
Australia	73
Canada	32
South Korea	29
Vietnam	27

Sum: 537

공격 위치

Elastic Maps Service OpenMapTiles OpenStreetMap contributors

zoom: 2.07

공격IP(Top5)

IP	Count
35.182.162.249	32
157.240.22.35	27
208.67.222.222	27
210.245.0.210	27
197.155.131.1	26

Sum: 537

경보 발생 현황

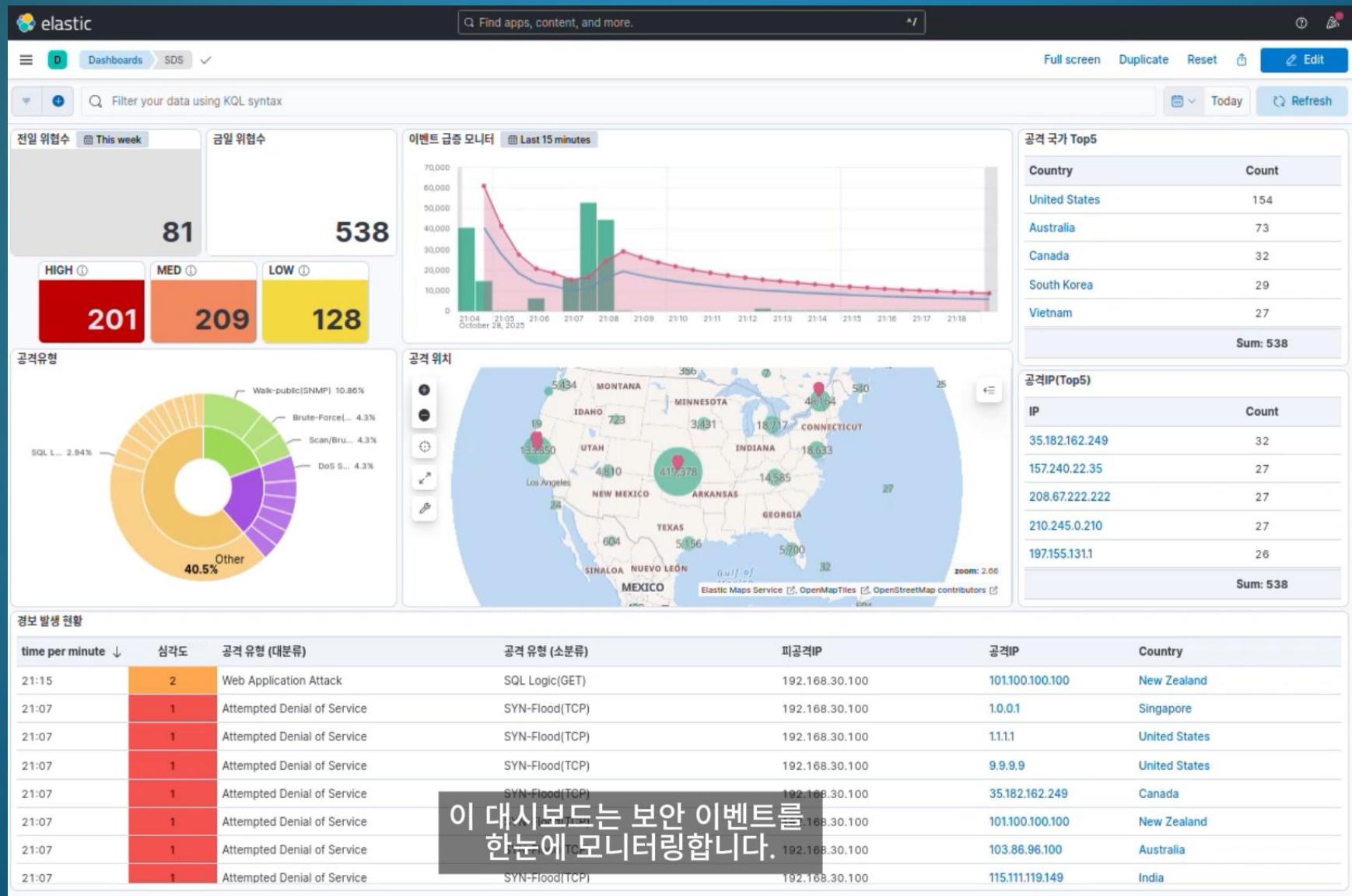
time per minute	심각도	공격 유형 (대분류)	공격 유형 (소분류)	피공격IP	공격IP	Country
21:07	1	Attempted Denial of Service	SYN-Flood(TCP)	192.168.30.100	1.0.0.1	Singapore
21:07	1	Attempted Denial of Service	SYN-Flood(TCP)	192.168.30.100	1.1.1.1	United States

시연_실제 알림 탐지 확인

The screenshot displays a complex monitoring environment with multiple components:

- Elasticsearch Dashboard:** Shows a summary of threat levels (HIGH: 201, MED: 209, LOW: 128) and a donut chart detailing attack types. A value of **538** is circled in blue.
- Gmail Inbox:** Displays several ElastAlert triggered alerts. One alert for [MED] is circled in blue. The total count of alerts is also circled in blue at the bottom right of the inbox area.
- Logstash View:** A table showing log entries. One entry at 21:15 is circled in blue, showing a Web Application Attack. Another entry at 21:07 is circled in red, showing an Attempted Denial of Service.
- Map View:** A world map showing attack locations with green dots indicating the number of attacks per location.
- Table View:** Two tables on the right side showing the top 5 countries and IP addresses for attacks. The total counts for these tables are also circled in blue.

시연_대시보드 필터 활용



성과 결과

탐지·수집

- Suricata 8.x 기반 규칙 세트를 정비하여 DoS 계열(SYN/ACK/UDP/ICMP) 및 웹공격 탐지 항목을 확장
- eve.json 스트림을 Logstash로 안정적으로 수집

적재·스키마

- Elasticsearch 인덱스 템플릿을 정리하여, 핵심 필드의 타입을 표준화
- 인덱스 네이밍/롤오버 전략을 적용하여 일 단위 관리 및 쿼리 성능을 개선

시각화·대시보드

- 필드를 클릭하면 해당 조건으로 필터가 자동 적용되어 관련 이벤트만 집중 분석
- 카테고리·시그니처·Severity(High/Med/Low) 위젯을 구성하여 비율과 추세를 한 화면에서 파악

알림

- ElastAlert2 규칙에서 이메일 알림 라우팅을 구축
- KST 시간, 인덱스, 시그니처, 소스/목적지 IP 등의 핵심 정보를 요약 형식으로 제공
- 메시지만으로도 1차 판단이 가능하도록 함

데이터 보강·시뮬레이션

- 페이크 IP/ GeolP 주입 파이프라인을 마련해 국가/도시 분포가 지도에서 충분히 표현되도록 함

운영·재현성

- Docker Compose로 전 구성요소를 일관되게 실행/재배포 가능

향후 추진 계획

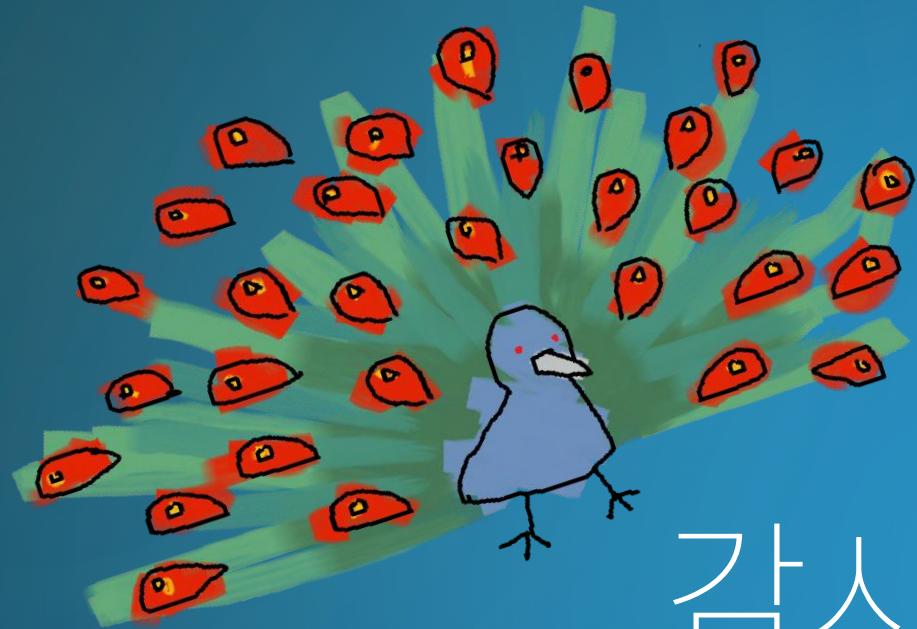
위협탐지 및 분석 고도화 전략

룰 정책 고도화	보안 정보 시각화 확장
최신 공격 트렌드를 반영하여 탐지하기 위해 룰을 정기적으로 업데이트	모니터링 목적에 따라 맞춤형 대시보드 및 리포트 기능을 확장.

시스템 운영 안정화 및 효율화

데이터 파이프라인 안정성

- 메모리 집약적 특성을 가진 Elasticsearch의 성능 저하 위험하므로 안정적인 운영을 위한 성능 테스트 및 튜닝 수행



감사합니다

