

AlertNow 서비스 누구보다 잘 사용하기

DevOps 개발팀 김의종
2022. 07. 15

AlertNow 서비스 소개

효율적인 장애 관리의 중요성

고객

서비스 장애가 빈번하게 발생하면
서비스에 대한 신뢰도가 점차
낮아지며 결국에는 서비스를 이탈할
가능성이 높음



서비스 제공자

안정적인 서비스 운영을 하고자
노력하지만 장애는 예고 없이
찾아오기 때문에 사전 예방 및 빠른
대응이 필요함

SLM (Service Level Management) 관리가 중요함

효율적인 장애 관리를 위해 필요한 것

- 빠르고 정확한 인시던트 발생 사실 전파
- 담당자 미확인 시 대체 처리 담당자 확보 및 알림 전달
- 발생 인시던트에 대한 정확한 내용 전달
- 신속한 인시던트 처리
- 인시던트 발생 및 처리에 대한 이력 관리
- MTTA/MTTR 지표에 대한 현황 확인

- MTTA : Mean Time to Acknowledge
- MTTR : Mean Time to Resolve



AlertNow

AlertNow 서비스를 통한 기능 확장 및
효율적인 이벤트 관리 업무 수행

IT 장애 관리의 신속한 인지와 조치를 위한 AlertNow

AlertNow는 SaaS기반의 다양한 환경의 모니터링 도구에서 발생하는 알림을 통합관리하고 신속한 대응을 지원하여 비즈니스를 지켜주는 “국내 최초” 알림 통합 관리 솔루션입니다.

Collect

하루에도 수 없이, 3rd party monitoring tool에서 발생하는 알림을 중복 제거하고 AlertNow로 연동하여 통합 관리를 하게 됩니다

Delivery

일련의 프로세스과정 (알림 중복제거 → 라우팅 룰 → 개인설정)을 통해서 Right time, Right Person 알림을 전송하게 됩니다.



모니터링과 인시던트 관리 서비스의 비교

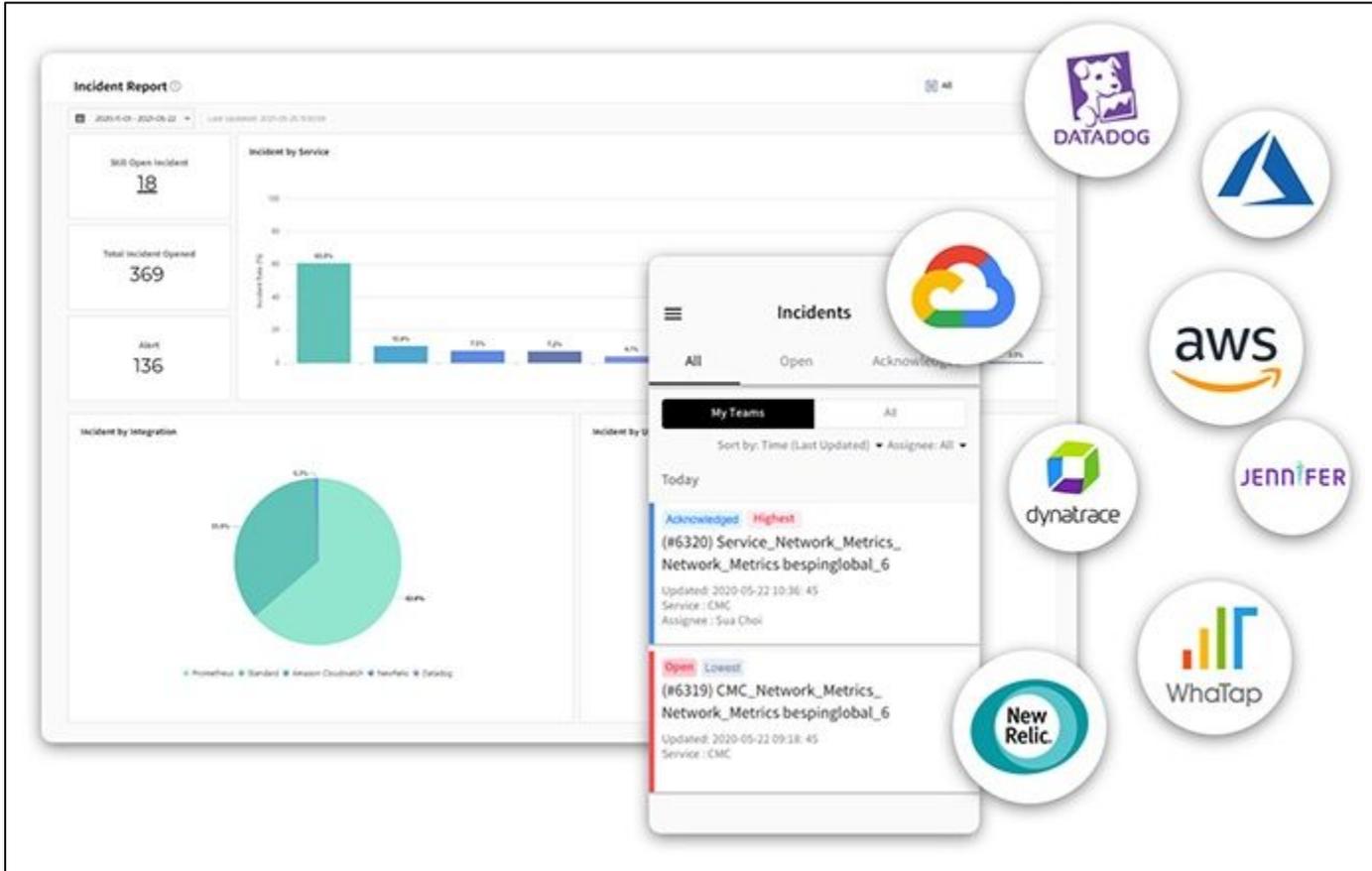
모니터링 서비스

- 서비스 운영 중 발생할 수 있는 이슈 및 오류에 대비하기 위해 데이터를 수집하고 기록하는 기능을 제공하는 서비스
- 인프라 모니터링과 애플리케이션 모니터링
- Amazon CloudWatch, Datadog, Newrelic, Prometheus, WhaTap 등

인시던트 관리 서비스

- 서비스 중단이나 품질 저하를 일으킬 수 있는 IT 이슈를 관리해 서비스 품질을 최대한 높은 수준으로 유지하는 기능을 제공하는 서비스
- 모니터링 서비스에서 알려주는 이상 현상들 간의 우선순위를 정하고, 어떤 팀이 확인해야 하는지 구분하고, 해결 이후 이슈를 종결시키는 모든 과정을 포함함
- Pagerduty, OpsGenie, Splunk On-call, AlertNow

모니터링과 인시던트 관리 서비스의 통합



모니터링과 인시던트 관리를 통합해
운영한다면 더 효율적인 서비스 운영이
가능

- 다양한 알람 통합
- 이슈 전달의 정확도 향상
- 다양한 알림 채널 활용
- MTTA/MTTR 지표 개선
- 팀원들의 생산성 향상

AlertNow 서비스의 특징

통합

- AWS CloudWatch, Azure Alerts, Google Cloud Monitoring, Datadog, NewRelic, Prometheus 등 약 30 여개의 모니터링 서비스 연동 지원
- 업무 시스템, 자체 모니터링 솔루션을 위한 연동 인터페이스 제공

알림

- Email, SMS, VoiceCall, 모바일 앱, 카카오톡, 텔레그램, Slack 등 다양한 알림 수단 제공
- 알람 종류, 등급에 따른 개인 별 수신 방법 설정
- 알림 수단을 통한 인시던트 상태 변경 기능 제공

이벤트 관리

- Escalation, Schedule, Team 기능을 통한 이벤트 발생 시 알림 수신 담당자 지정 기능 제공
- 동일 이벤트 데이터에 대한 중복 제거 및 긴급도 설정 기능 제공

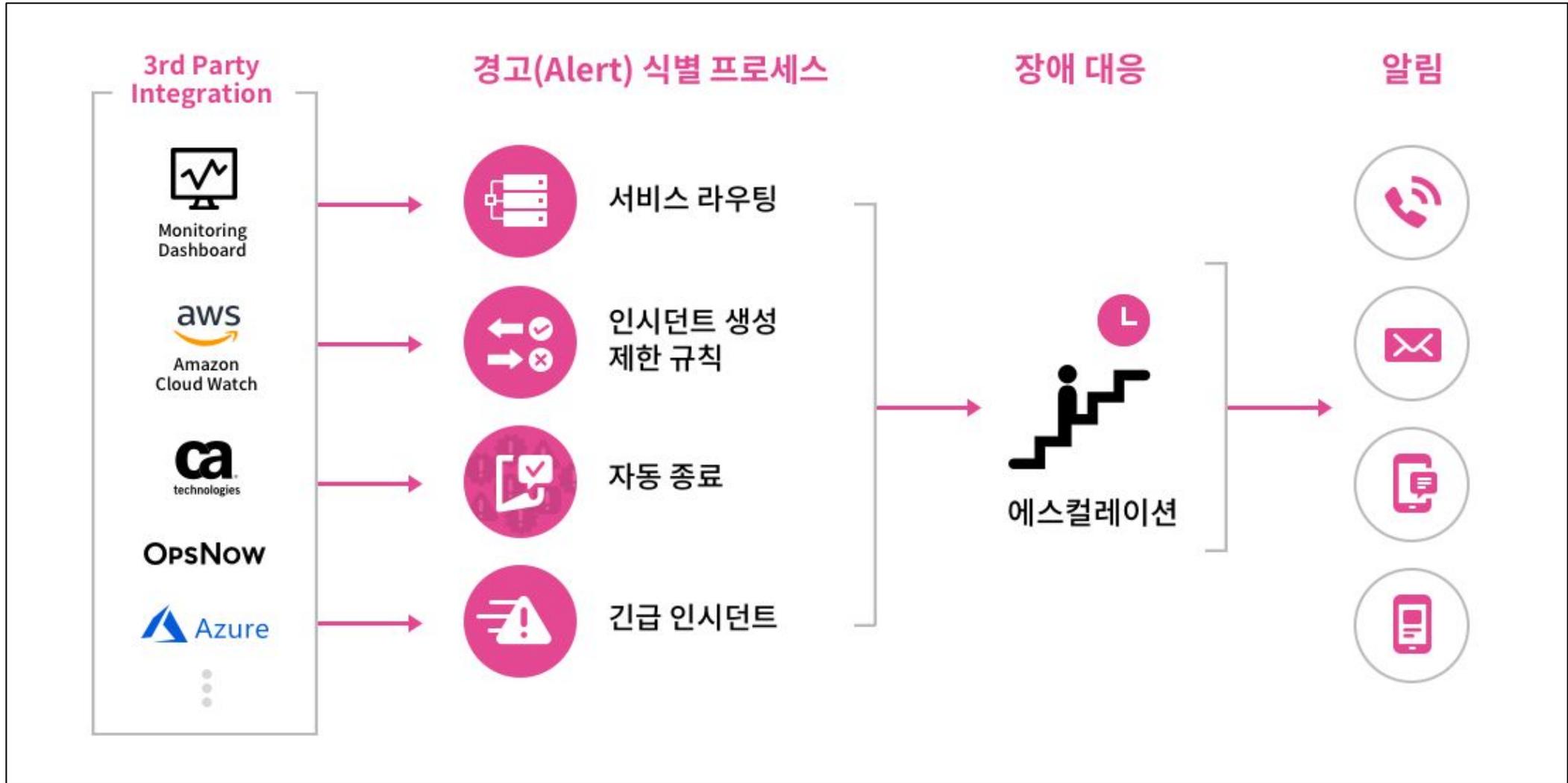
이벤트 분석

- 서비스 별 인시던트 MTTA, MTTR 지표 제공
- 서비스, 긴급도, 모니터링 유형 별 인시던트 발생 통계 데이터 제공
- 알림 수단, 시간대 별 알림 전송 통계 데이터 제공

“다양한 비즈니스 환경에 적합한 인시던트 관리 프로세스와 도구 제공”

- 다중 모니터링 서비스 구성 환경에서 통합 이벤트 관리
- 다양한 알림 수단 및 Escalation 기능을 통해 신속하고 누락 없는 인시던트 발생 사실 인지
- 동일 이벤트에 대한 중복 제거 기능으로 꼭 필요한 인시던트에 집중
- 조건에 따른 인시던트 처리 담당자를 지정하여 효율적인 인시던트 관리
- 인시던트를 빠르게 처리하고 그 지표를 관리

AlertNow 서비스 - Main Process



AlertNow 서비스 주요 기능 - Integration

Integration

Cloud 벤더에서 제공하는 모니터링 도구 및 다양한 3rd party 모니터링 도구와의 인티그레이션을 지원합니다.

❖ 알림 통합

3rd Party Monitoring Tools 발생하는 알림의 통합

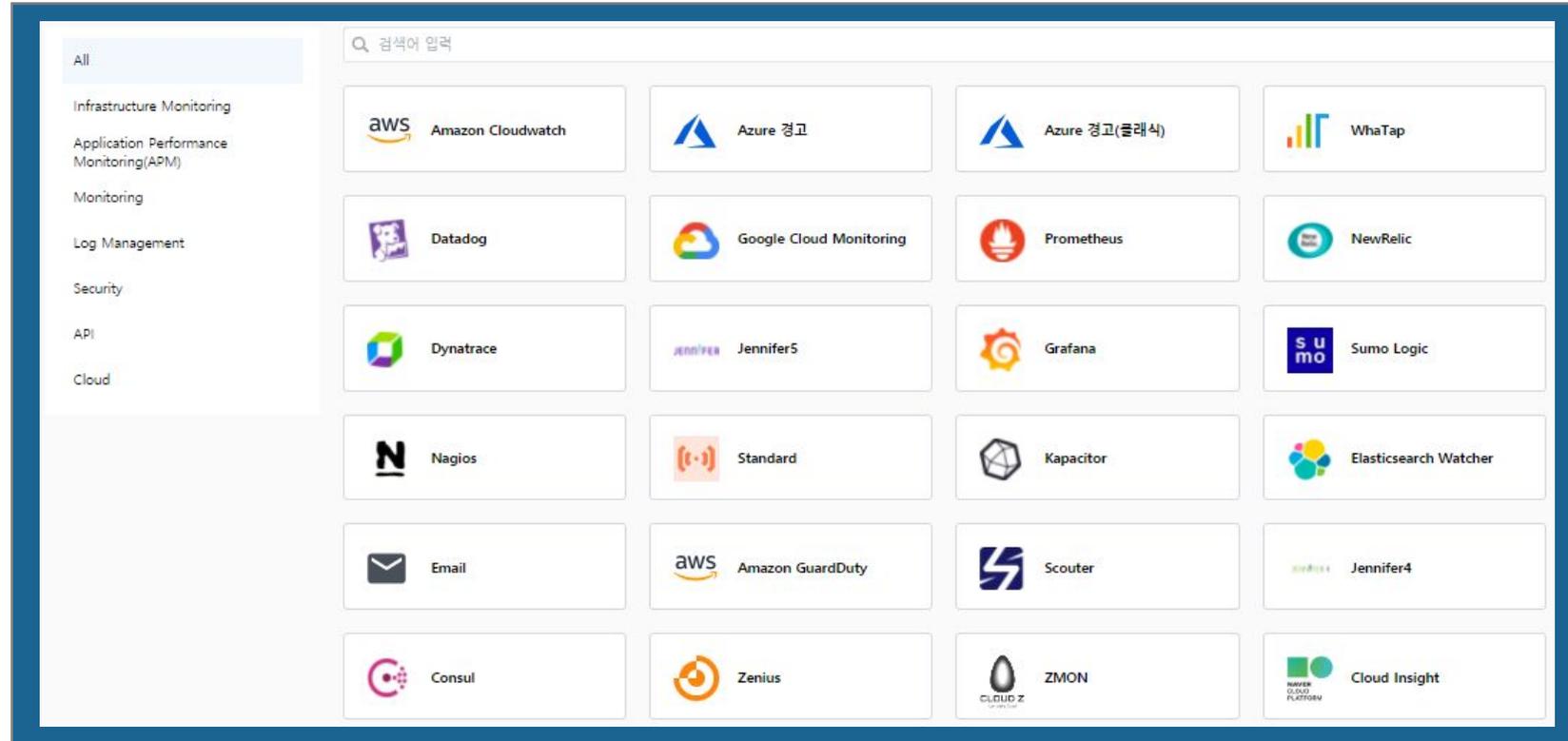
❖ 다중 라우팅

Metric 또는 Summary에 따라 조건별로 인시던트를 라우팅 하여 서비스 단위로 관리

❖ 고객요건에 따른 지속적인 Integration 추가

현재 30+ 인티그레이션 제공

인티그레이션에서, 고객의 요건에 기반하여 지속적인 인티그레이션 추가 계획



Incidents

인시던트는 AlertNow의 메인 서비스 페이지로, 중복이 제거된 알림을 “인시던트” 라는 용어로 정의 되어 관리 합니다

- **인시던트 리스트**

조회기간 동안 날짜/상태/긴급도 별 필터를 사용하여 인시던트 발생 현황을 빠르게 파악

- **인시던트 별 상세 히스토리 파악**

인시던트 상세페이지에서 상태 변경/ 알림 전파/ 코멘트 등의 활동이력 점검

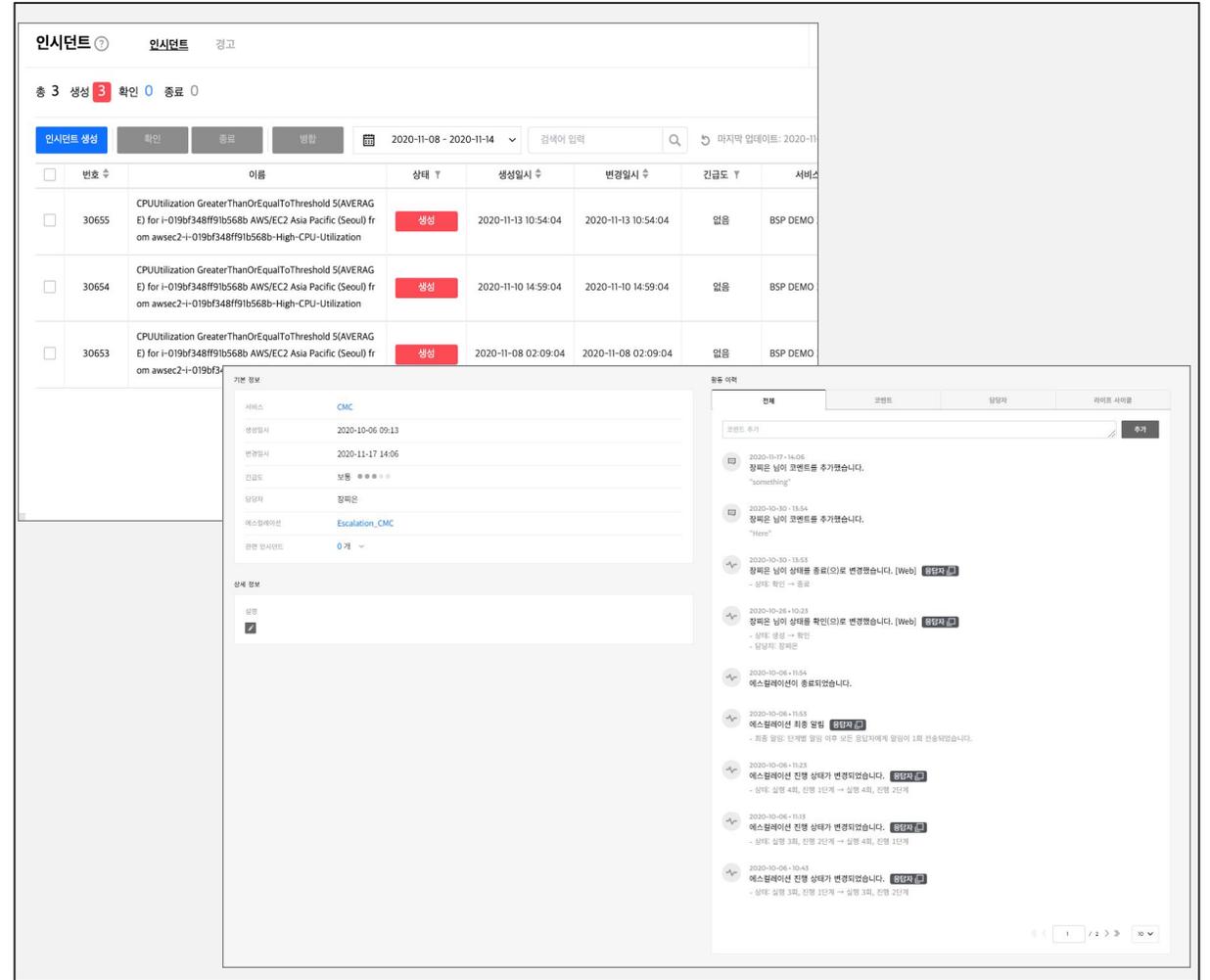
상세페이지에서 상태를 변경하거나 담당자 변경

- **3가지 상태(생성/확인/종료) 관리**

생성 : 3rd Party tool에서 최초로 알림이 발생

확인 : 담당자가 할당되고 알림 발생이 인지된 상태

종료 : 처리 완료



Escalation

STEP별로 수신자를 지정하여, 인시던트의 단계적 전파
“Never miss the alarms”

- **에스컬레이션의 종료 조건 지정**

알림 수신을 종료할 인시던트의 상태 조건 선택

- **활용도가 높은 단계적 수신자 설정 옵션들**

각각의 단계에서는 사용자/스케줄/팀/팀에서의 랜덤 사용자 지정 가능

STEP실행 후 다음 단계로 에스컬레이션 하거나 현재 단계 반복

- **최종 알림**

에스컬레이션 이후에도 응답이 없는 경우 추가 알림 전파

1. 종료 조건

에스컬레이션을 종료할 인시던트 상태

확인 ▾

2. 단계별 알림 인시던트 발생 시 다음 규칙에 의해 알림이 전송됩니다.

에스컬레이션 실행 횟수, 시간 및 응답자를 설정합니다.

에스컬레이션 실행 1 회

1

응답자 [동답자 입력]

장패: 사용자 ▾

스케줄 ▾

모든 팀 구성원 ▾

다음 단계 임의로 선정된 팀 구성원 ▾

2

응답자 [동답자 입력] 이전 모든 단계 응답자 포함

김의중 X CMC NOC Team X

다음 단계 실행 ▾ 간격 30 분

+ 에스컬레이션 단계 추가 최대 20개

3. 최종 알림

단계별 알림 이후, 모든 응답자에게 알림을 전송합니다.

미사용 사용

Scheduling

일정에 따라 인시던트 알림을 수신할 담당자를 지정합니다.

- **시간 별, 로테이션 별 알림 수신자 설정**
시간대별 담당자를 지정하거나,
Daily/weekly/Custom으로 rotation주기 설정
- **멀티 레이어 제공**
다중 레이어를 통해 동시간대 여러 명이 알림
수신 가능
- **오버라이딩**
사용자가 부재 중일 경우 대체 담당자 지정 가능

스케줄 정보

현재 스케줄	<div style="display: flex; gap: 5px;"> 안소영 2020-11-15 18:29 ~ 2020-11-16 18:00 </div> <div style="display: flex; gap: 5px; margin-top: 5px;"> 김관리자 2020-11-15 18:29 ~ 2020-11-16 18:00 </div>
내 다음 스케줄	내 다음 스케줄이 없습니다.
우선 담당자	설정된 우선 담당자가 없습니다.
응답자	<div style="display: flex; gap: 5px;"> 이우성 이혜영 안소영 박수용 최형진 김관리자 Uijong Kim </div>
팀	해당 스케줄을 사용하는 팀이 없습니다.
에스컬레이션	설정된 에스컬레이션이 없습니다.

타임라인
캘린더

오늘 < > 2020년 11월 15일 - 2020년 11월 28일
1일 1주 2주 한 달

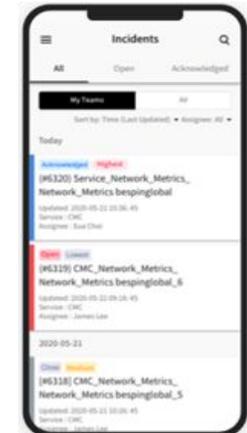
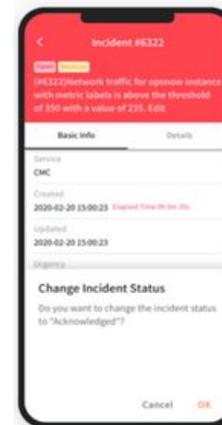
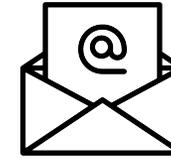
	11/15 일	11/16 월	11/17 화	11/18 수	11/19 목	11/20 금	11/21 토	11/22 일	11/23 월	11/24 화	11/25 수	11/26 목	11/27 금	11/28 토
1	안소영	이혜영	이우성	안소영	이혜영	이우성	안소영	이혜영	이우성	안소영	이혜영	이우성	안소영	>>
2	이수진	최형진	이수진											
3	김관리자	Uijong Kim	김관리자	>>										

AlertNow 서비스 주요 기능 - Notification

Notification

시간과 장소에 구애 받지 않고 다양한 알림 수단을 통한 인시던트를 관리 합니다.

- **내 손안의 알람 관리**
SMS, Voice call, Email, 카카오톡, Slack, 텔레그램을 통한 알림 수신 및 모바일 앱 지원
- **양방향 서비스 제공**
인시던트 생성 알림 뿐만 아니라 상태 변경 기능 제공
- **Wake Up Call**
AlertNow 모바일 앱 만의 Wake Up call 기능을 통해 수면시간에도 알람에 대해 즉각적으로 반응 할 수 있는 강력한 알람 기능 제공



AlertNow 서비스 주요 기능 - System Report

System Report

시스템의 전반적인 인시던트의 발생 현황을 파악하고 안정성을 점검 하는 지표 입니다.

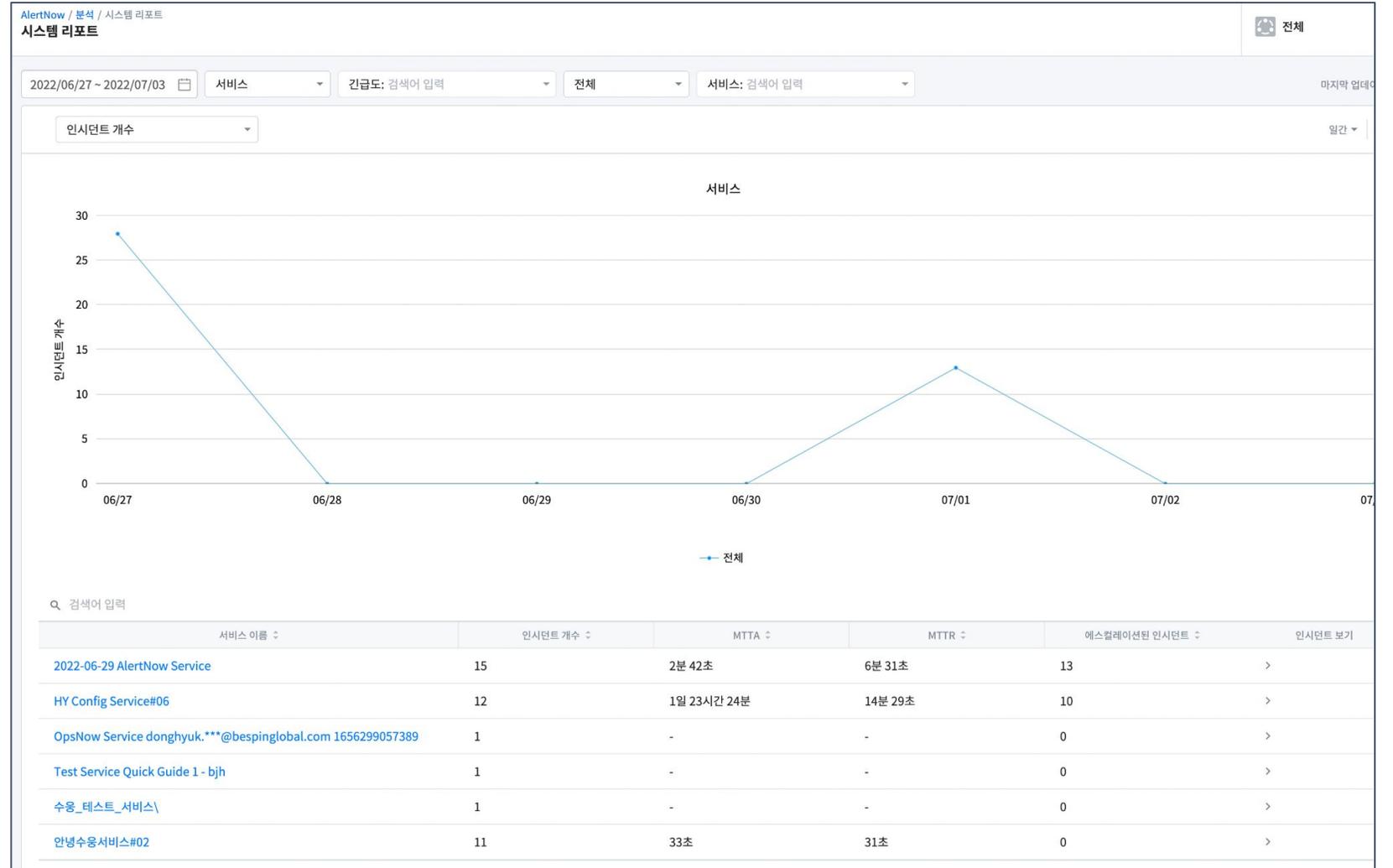
❖ 시스템 서비스 안정화 지표 확인

서비스와 에스컬레이션 기준으로 인시던트 발생 현황 파악. 평균 MTTA, MTTR 확인 가능.

- MTTA : Mean Time to Acknowledge
- MTTR : Mean Time to Resolve

❖ CSV다운로드

Raw데이터를 한번에 조회 하여 다운로드 가능



AlertNow 서비스 주요 기능 - Incident Report

Incident Report

발생한 인시던트를 상세하게 분석하여 시각화 한 그래프를 제공합니다.

❖ 인시던트 통계 데이터 제공

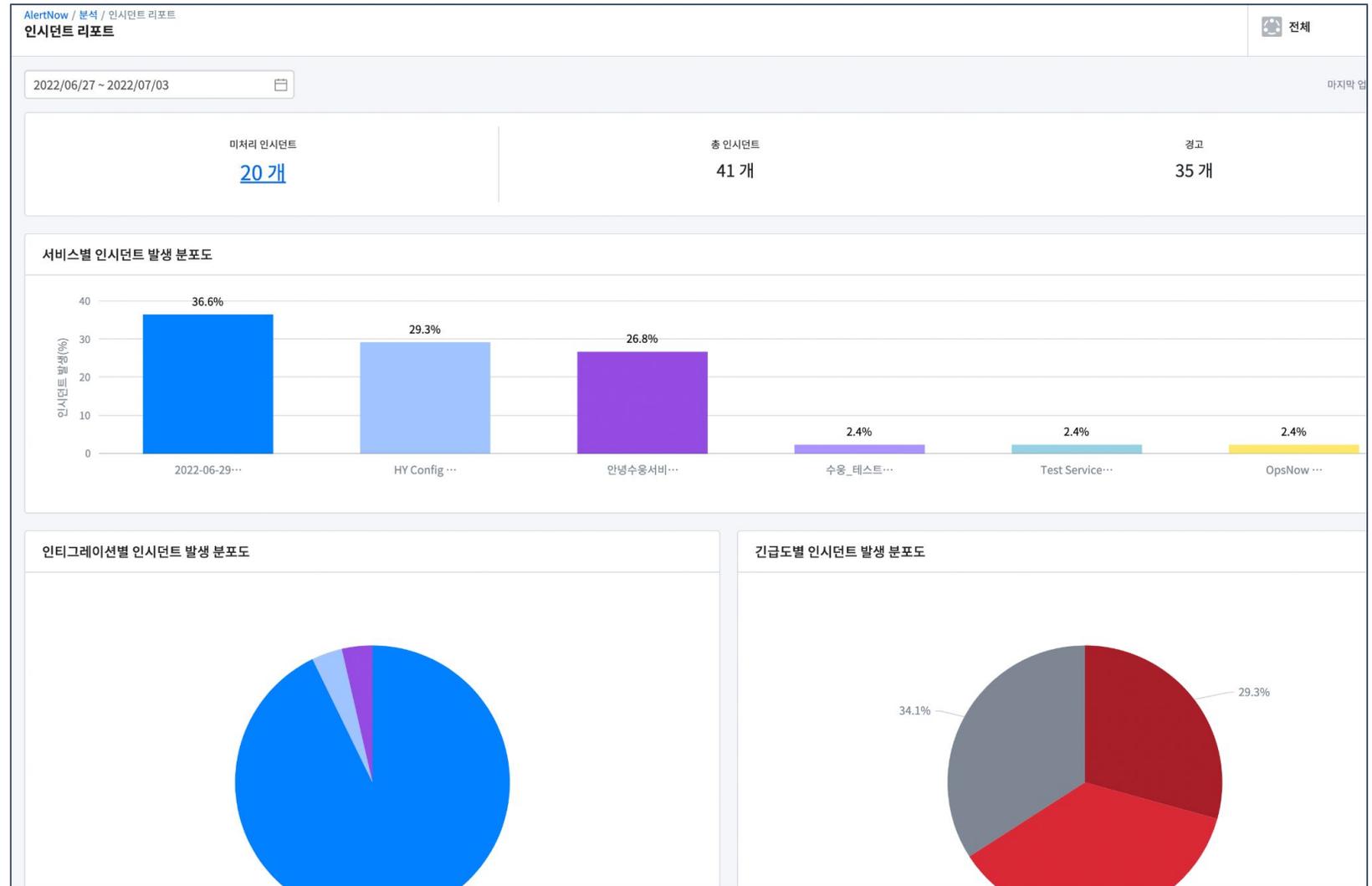
서비스 / 긴급도 / 인티그레이션 별 발생 추이

❖ 인시던트 발생 추이

X축 : 시간, Y축: 요일 히트 맵을 통한 인시던트 발생추이를 확인하고 발생에 대한 예측 지표로 확인

❖ Daily 발생 현황 확인

조회 기간 내의 인시던트 생성, 확인을 한눈에 확인

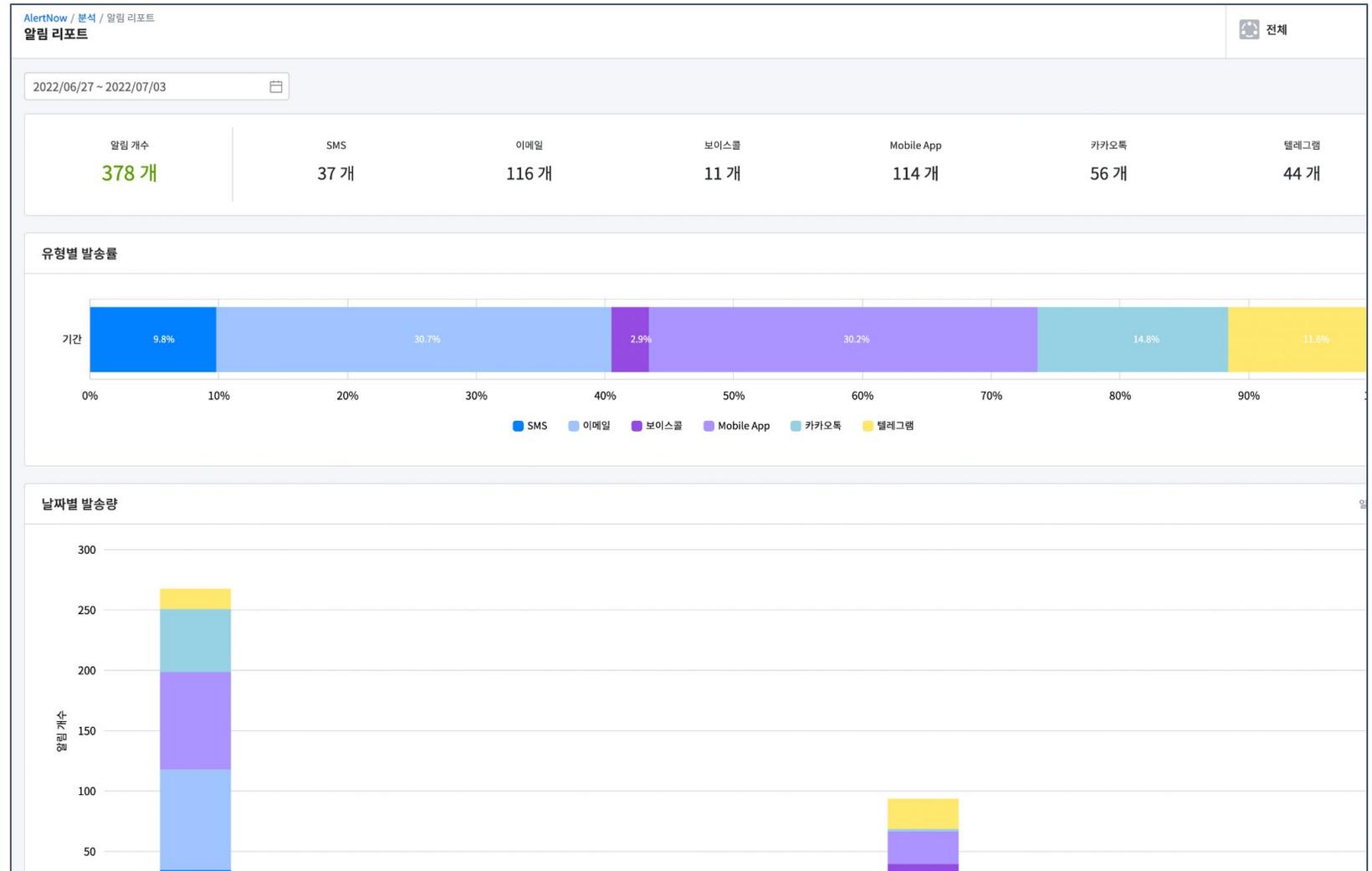


AlertNow 서비스 주요 기능 - Notification Report

Notification Report

SMS/ 이메일/ 보이스콜/ 모바일 발송 분포에 대한 그래프를 제공합니다.

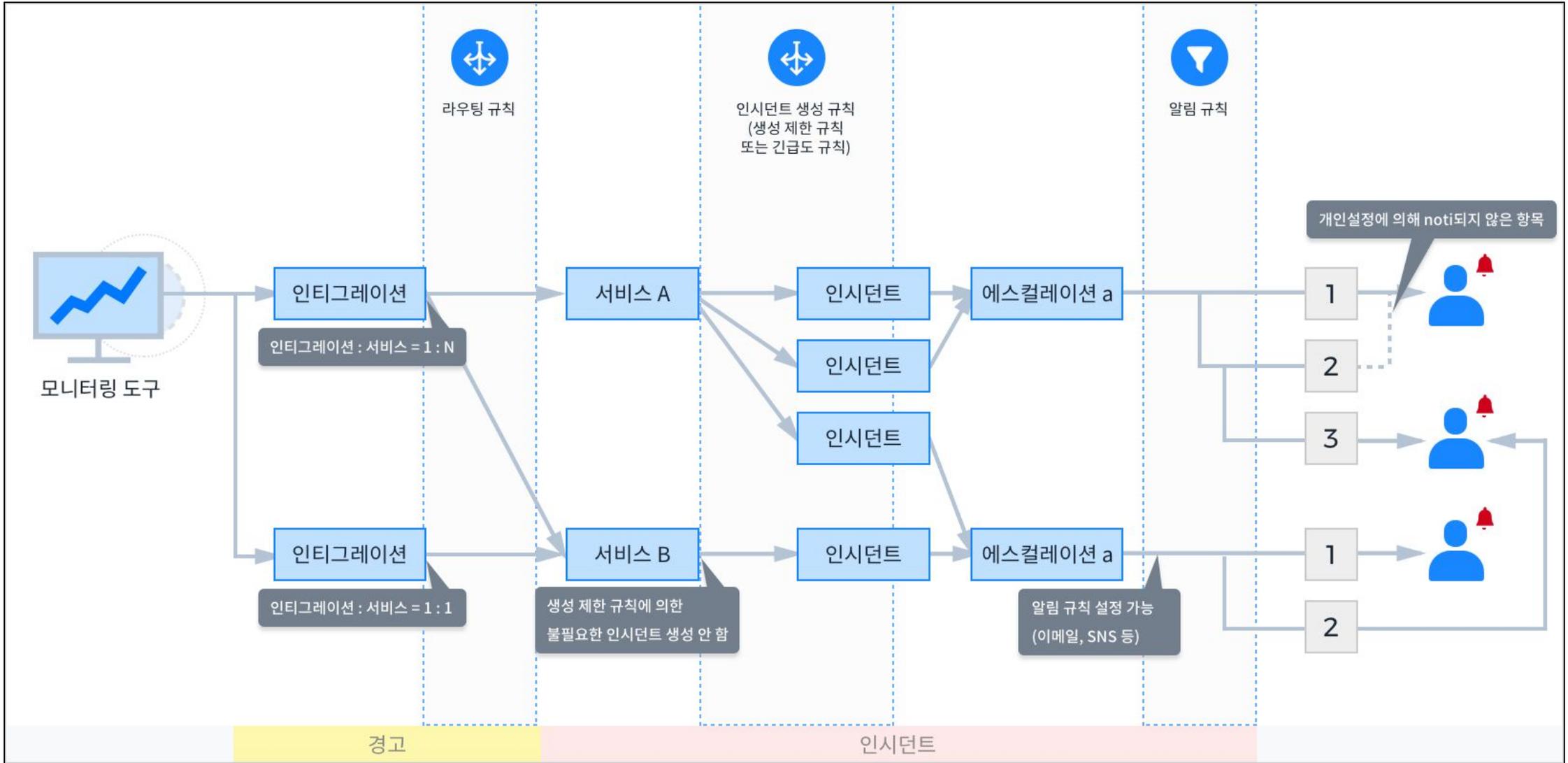
- ❖ Notification Method에 대한 사용 분포
SMS / 이메일 / 보이스콜 / 모바일 앱 등에 대한 사용량 확인
- ❖ Daily 발송 리스트 확인
일별 Notification 발송 량 확인
- ❖ CSV다운로드
Raw데이터를 한번에 조회 하여 다운로드 가능



AlertNow 서비스 데모

운영 유형 별 AlertNow 설정 사례

AlertNow 서비스를 활용한 IT 장애 대응 프로세스



단일 Integration을 이용하여 AlertNow 서비스를 연동하는 경우

서비스 라우팅 규칙 서비스에 인티그레이션을 매핑하여 경고를 수신하고 관리할 수 있습니다.

기본 서비스

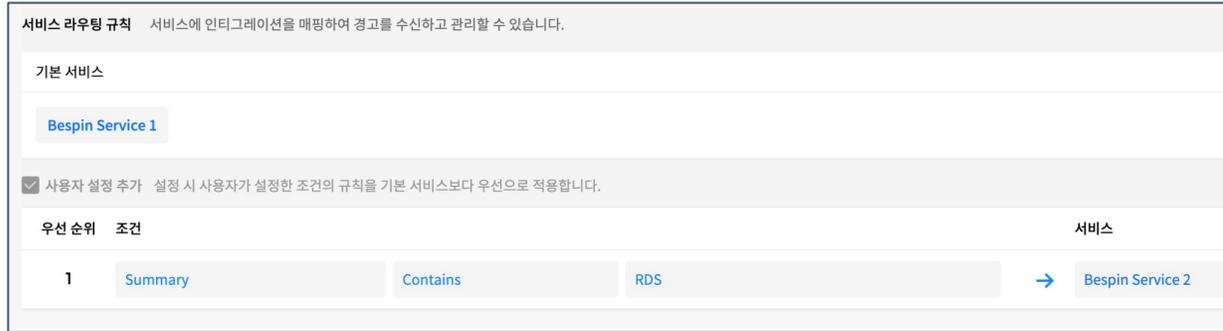
Bespin Service 1

사용자 설정 추가 설정 시 사용자가 설정한 조건의 규칙을 기본 서비스보다 우선으로 적용합니다.

우선 순위	조건	서비스
1	Summary Contains RDS	→ Bespin Service 2

- 인시던트의 제목에 “RDS” 라는 문자열이 포함되어 있는 경우 -> Bespin Service 2에 인시던트 생성
- 인시던트의 제목에 “RDS” 라는 문자열이 포함되어 있지 않은 경우 -> Bespin Service 1에 인시던트 생성

특정 키워드를 이용하여 인시던트 발생 알림 필터링



- Bespin Service 1 : 에스컬레이션, 스케줄 등 필요한 라우팅 설정
- Bespin Service 2 : 라우팅 규칙을 지정 안함으로 설정
- 인시던트의 제목에 “RDS” 문자열이 포함되어 있으면 Bespin Service 2에 인시던트가 생성되기 때문에 인시던트 생성에 대한 Notification을 수신하지 않게 됨



예정되어 있는 작업이 있는 경우 예외 처리

상태



유지보수 즉시 추가

5분 15분 30분 60분

유지보수 일정(최대 5개)

+ 유지보수 일정 추가

상태



진행 중인 유지보수

2022/07/07 05:35 ▶ 2022/07/07 06:35

생성자: Uijong Kim

시간 추가 종료

유지보수 일정 추가

시작 시간 2022-07-07 05:35 - 종료 시간 2022-07-07 06:35

생성자 Uijong Kim

설명 설명 입력

취소 확인

인시던트	인티그레이션	라우팅 규칙	인시던트 생성 규칙	익스텐션	유지보수 이력
유지보수 이력을 확인할 수 있습니다.					
<< >> 1					
시작 시간	종료 시간	상태	생성자		
2022-07-07 05:35:00	2022-07-07 06:35:00	진행 중	Uijong Kim		

공식 지원하지 않는 웹훅 방식의 메신저 연동하기

이름 *

익스텐션 유형 *

 Generic Webhook

서비스 *

알림 이벤트 ⓘ

에스컬레이션 담당자 지정 확인 종료

URL Encode

사용 미사용

URL *

Method *

```
{
  "cards": [
    {
      "header": {
        "title": "${SERVICE_NAME}",
        "subtitle": "${INCIDENT_NAME}"
      },
      "sections": [
        {
          "widgets": [
            {
              "textParagraph": {
                "text": "- <b>STATUS</b>: ${STATUS}<br>- <b>CREATE_DATE</b>: ${CREATE_DATE}<br>- <b>MODIFY_DATE</b>: ${MODIFY_DATE}"
              }
            },
            {
              "buttons": [
                {
                  "imageButton": {
                    "icon": "DESCRIPTION",
                    "onClick": {
                      "openLink": {
                        "url": "${INCIDENT_URL}"
                      }
                    }
                  }
                }
              ]
            }
          ]
        }
      ]
    }
  ]
}
```

Standard Integration을 이용한 API 연동 방식

필드	이름	데이터 유형	필수 여부	설명	기본값	예제
summary	요약 정보	String	필수	이벤트의 내용을 식별할 수 있는 정보		Threshold Crossed: 1 datapoint [31.84234972677596 (19/12/19 17:40:00)] was greater than or equal to the threshold (90.0)
event_id	이벤트 ID	String	선택	event_id 데이터가 존재하지 않는 경우에는 자동 설정됨 (단, status가 ack, close인 경우에는 필수임)	UUID	129335065553
status	상태 정보	String	선택	이벤트의 상태를 나타내는 필드 유효한 값 - open: 이벤트 생성 - ack: 이벤트 확인 - close: 이벤트 종료	open	open
urgency	긴급도	String	선택	시스템에 영향을 미치는 정도 또는 우선 순위와 관련된 이벤트의 긴급도를 나타내는 필드 유효한 값 - highest: 매우 높음 - high: 높음 - medium: 중간 - low: 낮음 - lowest: 매우 낮음 - none: 없음	none	high

URL: `https://{DOMAIN}/integration/standard/v1/{APIKEY}`

Method: POST

Content-Type: application/json

Body: 아래 내용 참조

event_time	발생 시간	String	선택	이벤트가 발생한 시간 Timestamp(ISO 8601) 형식의 데이터	현재 시간	2019-12-19T17:40:00+09:00
metric_name	메트릭 이름	String	선택	메트릭 유형을 확인할 수 있는 정보		CPUUtilization
threshold	임계치	String	선택	메트릭 임계치		90
metric_value	메트릭 값	String	선택	메트릭 측정 값		93.1
resource_name	리소스 이름	String	선택	이벤트가 발생한 시스템의 호스트 이름과 같이 사람이 식별할 수 있는 정보		i-9c09acd49a25
event_type	이벤트 유형	String	선택	이벤트의 유형을 식별할 수 있는 정보		INFO
custom_details	세부 정보	JSON	선택	추가 정보 필드		{ "ping time": "1500ms", "load avg": 0.75 }

Email을 이용한 AlertNow 연동 방식

AlertNow 2022-07-06 Email Integration

기본 정보

인TEGRATION 유형	Email
인TEGRATION 키	alert.email.6edee9@alertnow-integration.com  
생성 제한 규칙	이메일 제목마다 다른 인시던트로 간주하여 새 인시던트 생성 
생성자	Uijong Kim

서비스 라우팅 규칙 서비스에 인TEGRATION을 매핑하여 경고를 수신하고 관리할 수 있습니다.

기본 서비스

[2022-06-29 AlertNow Service](#)

사용자 설정 추가 설정 시 사용자가 설정한 조건의 규칙을 기본 서비스보다 우선으로 적용합니다.

alert.email.6edee9@alertnow-integration.com

AlertNow Email Integration Test 2022-07-06

Test Message

김의종 **Uijong Kim** / DevOps 개발팀
uijong.kim@bespinglobal.com
M +82-10-4740-3158
KR 06627 서울특별시 서초구 강남대로 327 대릉서초타워 13F

BESPIN GLOBAL
HELPING YOU ADOPT CLOUD.

국내 최다 클라우드 인증 자격을 보유한 MSP • 국내 유일 ISO 인증을
확보한 MSP • 가트너가 인정한 한중일 유일한 MSP
www.bespinglobal.com • ISO 27001:2013 • ISO 9001:2015 Certified

스마트한 클라우드 관리와 디지털 전환 방법! **FinOps Community**에 함께 공유해요.
F www.facebook.com/groups/finops.community1

#413394 생성

AlertNow Email Integration Test 2022-07-06

확인 종료

상세 정보

메시지 원시 데이터

```
{
  "subject": "AlertNow Email Integration Test 2022-07-06",
  "FROM": "uijong.kim@bespinglobal.com",
  "to": "alert.email.6edee9@alertnow-integration.com",
  "body": "<div dir='ltr'>Test Message</div><br clear='all'><div dir='ltr' class='gmail_signature' data-smartmail='gmail_signature'>
"
}
```

Email 콘텐츠를 이용하여
AlertNow 인시던트 생성 가능

주요 고객들의 AlertNow 사용 사례

AlertNow 서비스 사용 - S사 사례 (1)



“서비스 안정성을 위해 24시간 모니터링 팀(NOC)을 운영하고 있고 이를 유지하기 위해 엄청난 비용을 지출하고 있습니다. 늘어나는 인시던트 발생에 대처하기 위해 증가하는 운영 비용이 걱정입니다.”

AlertNow 서비스 사용 - S사 사례 (2)



“서비스에 중요한 알림을 받지 못하거나 너무 많은 알림으로 인해 중요한 알림의 처리가 누락될까 걱정이 됩니다.”

“주야 구분없이 수시로 울리는 알림 때문에 퇴근 후에도 주말에도 쉬는게 쉬는 것 같지가 않습니다.”

AlertNow 서비스 사용 - S사 사례 (3)



“효율적인 서비스 운영을 위해 KPI 기반의 운영 체계 구축과 팀원들의 퍼포먼스를 측정하여 관리하고 싶습니다.”

AlertNow 서비스 사용 - S사 사례 (4)

2019년 공식적으로 S사의 DevOps Tool 로 등록 되어 2022.07월 현재까지 40개의 프로젝트, 5개 이상의 국가에서 AlertNow가 적용 되었습니다.

“
Cost Down
”



★ **Noc를 AlertNow를 통한 자동화로 운영비용 10% 절감**



Cost Saving → **Protect Service** → **Reducing Notification** → **Performance**

운영 비용 절감
인시던트 발생, 전파, 처리의 전 과정을 자동화한 플랫폼으로 적은 인력으로도 효율적인 모니터링 팀 운영이 가능

알림 누락 방지
이슈 발생 즉시 담당자에게 알림을 전달하고, 일정 시간 내 적절한 조치가 취해지지 않을 경우 상위 단계 담당자에게 알림을 전달하여 누락을 방지

알림의 소음에서 해방
3중 필터링 기능을 통해 중복 그리고 중요하지 않은 알림을 제거하여, 운영 담당자가 확인해야 할 알림의 양이 최대 80%까지 감소

KPI 기반 퍼포먼스 측정
인시던트 생성부터 확인까지의 평균 시간(MTTA) 측정, 인시던트 확인부터 종료까지의 평균 시간(MTTR) 측정 등 서비스 운영 현황에 대한 통찰력을 확보

AlertNow 서비스 사용 - A사 사례 (1)



“평일 주간에는 상주하여 모니터링 하는 인력이 있으니 야간과 주말, 휴일에만 알림을 받고 싶습니다.”

AlertNow 서비스 사용 - A사 사례 (2)

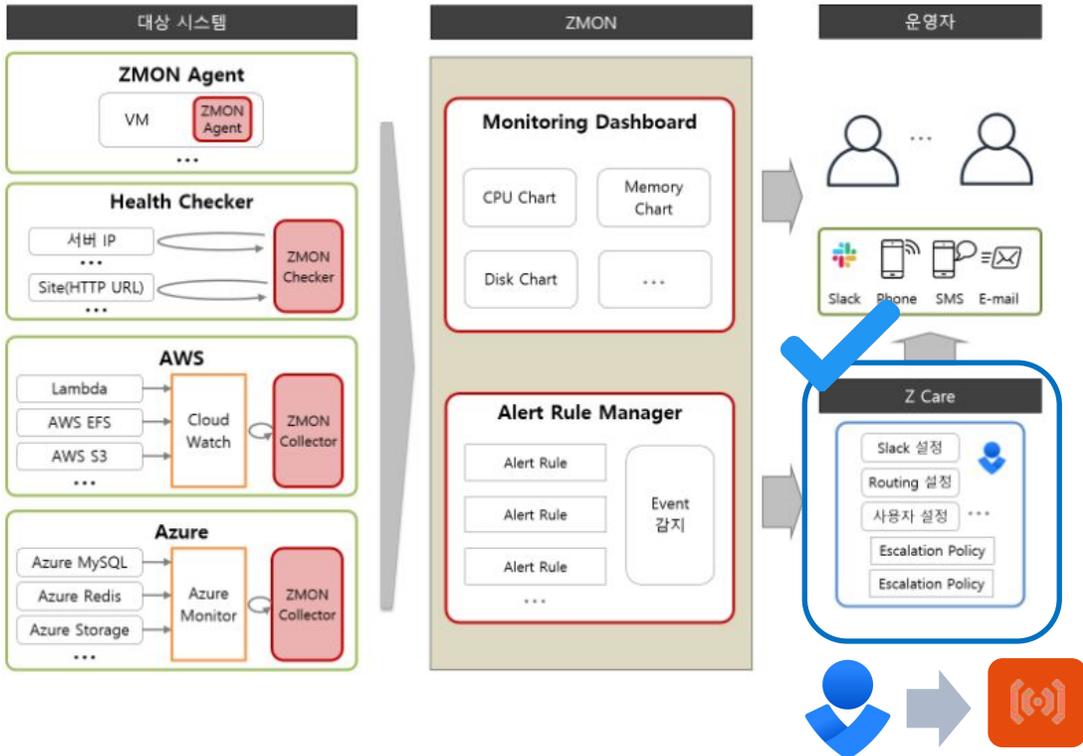
100개가 넘는 쇼핑몰, 300개 이상의 모니터링 툴 통합, 중요도에 따른 알림 수단 설정으로 알림의 피로에서 해방



AlertNow 서비스 사용 - SK 사례

- “고객사 요구사항 우선 대응 + 다국어 + 빠른 고객지원 + 구간할인 제공” -> 기존 OpsGenie 고객에서 AlertNow로 대체
- 베스핀 글로벌 x SK 기술 협약 MOU 체결

SK의 Cloud Monitoring Tool 에서 Z Care 포지셔닝 (OpsGenie 대체)



강력한 고객지원 & 고객사 요청기능 우선 개발

- 고객 요청에 의한 기능 개발 리스트

Category	기능 상세
Integration	- SK, SK C&C 내부에서 사용하고 있는 Zmon과 연동
Extension	- Slack 에서 / + Command 기능 : 서비스에 접속하지 않아도 Slack에서 명령어로 인스턴트 확인 및 생성
Escalation	- 에스컬레이션 단계에 사용자, 스케줄 뿐만 아니라, 팀과 랜덤 팀원을 매핑 하는 기능
New	- Audit : 시스템 설정의 변경 사항에 대한 감시 기능
Routing Rules	- 서비스에서 Routing Target이 에스컬레이션/사용자/스케줄/No one
Scheduling	- 일괄 Overriding





다국어 지원 (영문/중문/일어/국문) 고객 지원 구간 할인

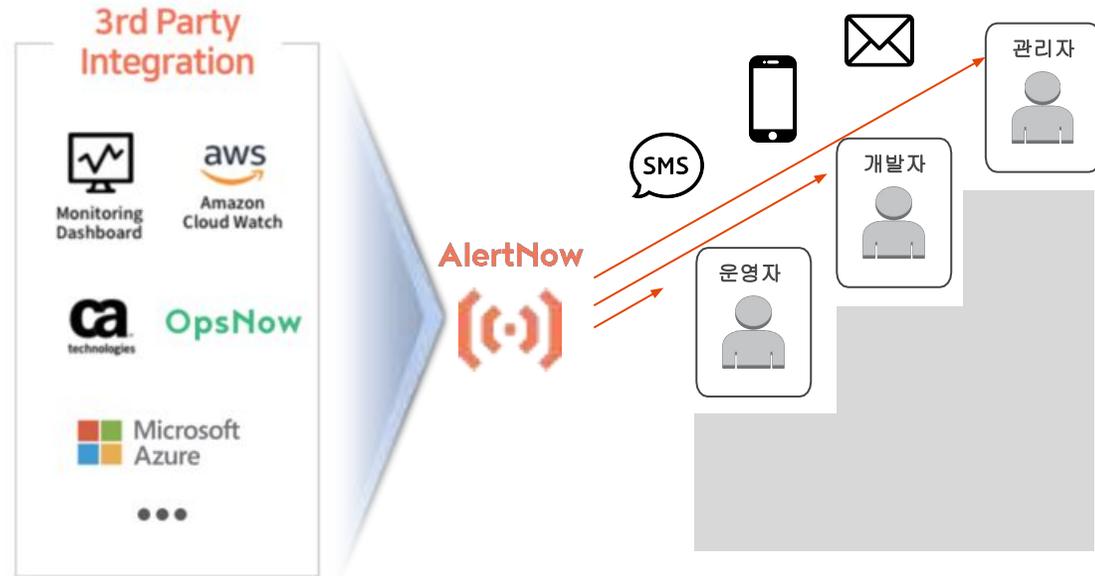
AlertNow 서비스 사용 - 직방 사례

전사 “모든 비즈니스의 통합 알림 Tool”로 자리 매김

[기존 사례] 3rd party monitoring

배경 및 요구사항

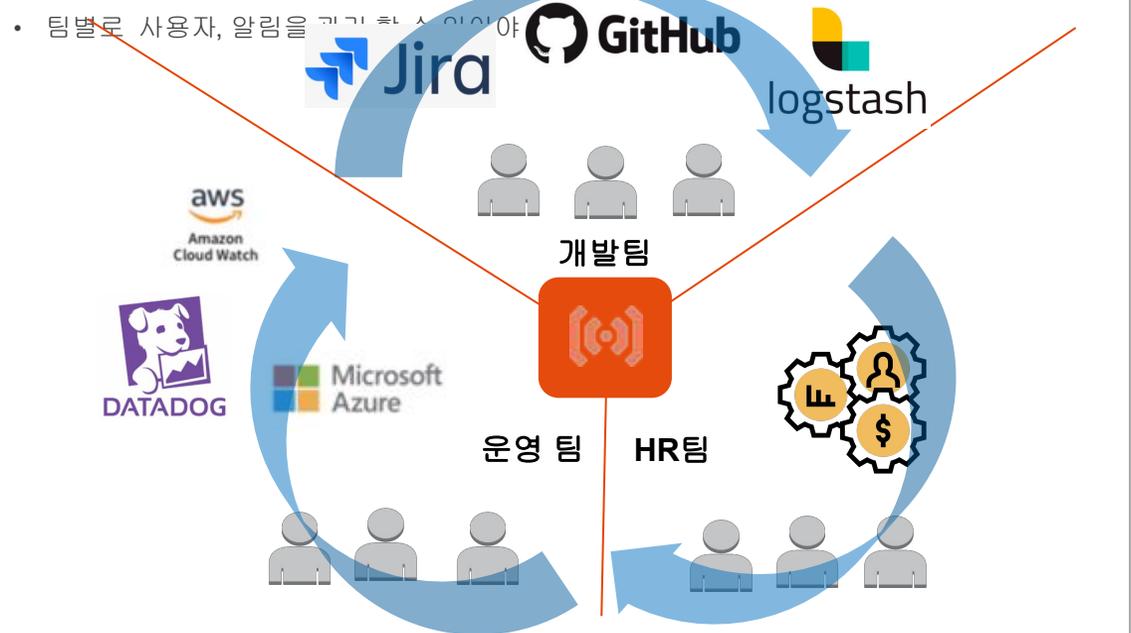
- 중복되는 알림을 제거
- 여러 가지 모니터링 툴에서 발생하는 알림을 한 번에 통합 관리
- Right Time. Right Person



[직방] 이벤트 통합 알림 툴

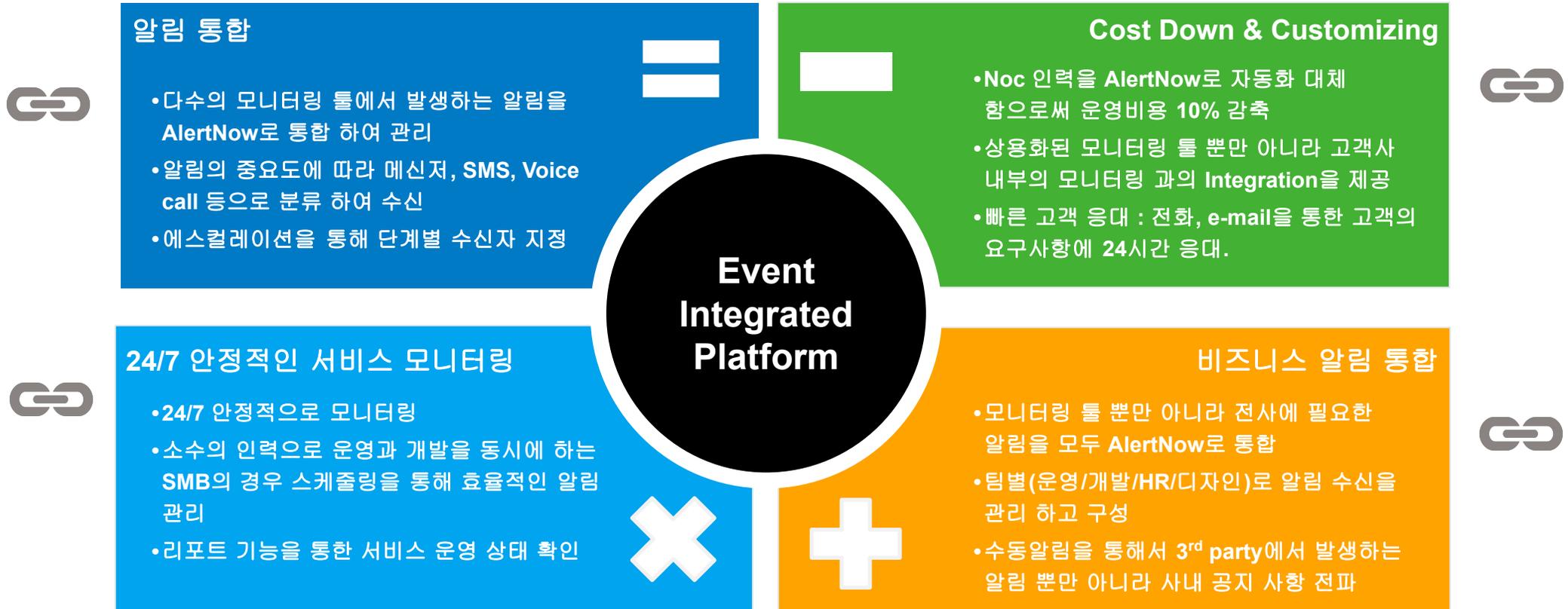
배경 및 요구사항

- 개발팀 / 운영팀 / 디자인팀 / PM팀 등 팀별로 받아야 하는 알림이 필요, 즉 전사 공지 툴이 필요함
- 모니터링 툴 뿐만 아니라 ITSM 툴과 연동을 해서 알림을 받아야 함
- 팀별로 사용자, 알림을 관리 할 수 있어야 함



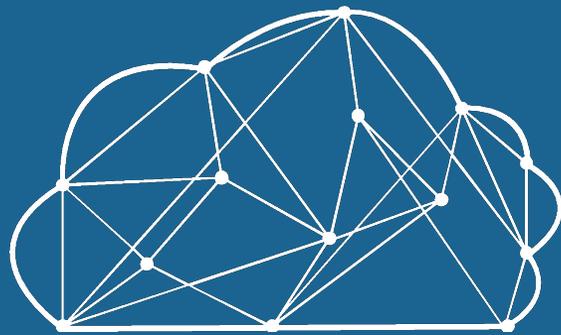
AlertNow Value Proposition

“운영 비용 감축(Cost Down), 통합성(Integration), 확장성(Scalability) 확보”



AlertNow Q&A





THANK YOU.

BESPIN GLOBAL