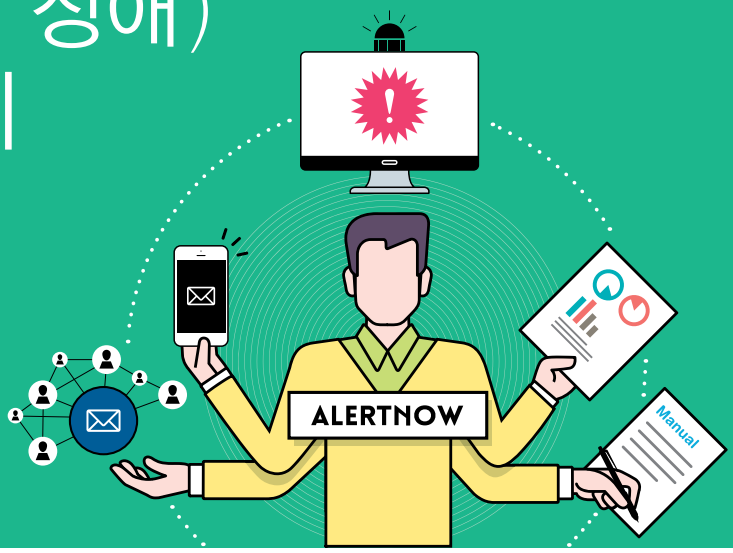
CLOUD INSIGHT

인시던트(a.k.a. IT 장애) 기똥차게 관리하기

Alarm,
Automation,
and AlertNow



인시던트(Incident), 그게 뭐지?

"전 세계 IT 팀의 65%는 인시던트 관리를 최우선 과제로 꼽고 있습니다"[1]

IT 업계에 있다 하더라도 친숙하지 않은 용어들이 있죠. 인시던트(Incident)도 그중 하나일 겁니다. 영어 사전에 검색해보면 '불쾌한 일, 무력이 개입되는 사건, 분쟁, 사고'라고 설명하는데요. 좀 더 설명하자면 크거나 혹은 작은, 좋을 수도 나쁠 수도 있고, 의도가 있을 수도, 없을 수도 있는 모든 일반적인 사건과 사고를 뜻합니다.

그럼 IT 세상에서 발생할 수 있는 사건과 사고 무엇일까요?
인시던트는 'IT 장애'로 재해석 할 수 있습니다. 따라서 인시던트를 관리한다는 것은 IT 장애를 관리한다는 것으로 이해하고 해석할 수 있습니다.

오픈소스 솔루션 레드햇(Red Hat)의 폴 코미어 CEO는 '모든 기업은 소프트웨어(SW) 기업'이라고 했습니다.
그 어느 때보다 수많은 온라인 서비스가 세상을 지배하고 있습니다. 이런 서비스에 인시던트, 'IT 장애'가 발생하면 어떻게 될까요? 고객이 사용하는 서비스가 먹통이 되면서, 기업은 매출과 브랜드에 막심한 손해가 발생할 것입니다. 보안 인시던트, IT와는 연관이 없는 비즈니스 인시던트는 좀 더 높은 수준의 개념이 적용됩니다. 우리가 생각하는 IT 장애에는 보안 말고도 무수히 많은 요소가 있습니다.

1 출처: 9 Best Practices to Improve Incident Management, Gartner

인시던트 발생부터 해결까지 아래 5가지 순서를 거치게 됩니다.

1 인시던트 파악, 로깅 및 카테고리화하기

대부분의 경우에 사용자 리포트, 솔루션 분석 또는 수동적으로 인시던트를 파악하고 있습니다. 한번 인시던트가 발생하게 되면 어딘가에 기록이 되고, 조사와 카테고리화가 진행됩니다. 분류, 즉 카테고리화가 중요한 이유는 인시던트 처리 방법과 대응 리소스를 확인해 우선순위를 결정하는 데 활용하기 때문입니다.

2 인시던트 알람 전송 및 담당자 전달 (Escalation)

인시던트가 발생한 이후에는 인시던트가 발생했다는 알람이 만들어집니다. 크리티컬 하지 않은 인시던트는 알람 없이 해결되는 경우도 있지만, 대부분 알람 발생 여부가 기록되거나, 알람이 생성되도록 합니다. 자동으로 관리할 수 있다면 인시던트 알람을 더욱 효과적으로 관리할 수 있게 됩니다. 더 알아보기

3 조사 및 진단

인시던트가 담당자에게 할당되고 나면, 인시던트의 유형이나 원인에 대해서 분석을 시작합니다. 인시던트는 내부 직원 또는 고객, 국가 기관에 인시던트 발생 이후 예상되는 서비스 중단과 해결 방안에 대해 알리는 것이 신뢰도 확보를 위해 좋습니다.

4 해결 및 복구

인시던트의 근본적인 원인을 제거하고, 서비스와 시스템을 완전히 정상 상태로 만드는 것입니다. 인시던트가 재발하지 않도록 단순 삭제보다 인시던트를 자세히 분석해 추후 동일한 문제가 생기지 않도록 하는 것이 핵심입니다.

5 인시던트 종료

인시던트가 마무리되었다면 이를 문서화하고 수행한 내용에 대해 평가하는 것이 좋습니다. 앞으로 발생할 수 있는 인시던트를 예방하고 효과적으로 대응하기 위한 것입니다.

인시던트 알람 과부하를 방지하는 것은 인시던트 관리 중 가장 중요합니다. 한 사람이나 한 팀이 모든 알람을 다 받는다면, 중요한 인시던트는 간과될 수 있으며, 대응 시간이 더 길어집니다. 방지하기 위해서는 인시던트가 어떻게 분류되고 어느 팀과 담당자에게 전달되어야 하는지 정확하게 정의해야 합니다. 특히 24*7 지원이 필요한 글로벌 서비스는 직원들의 교대 시에도 인시던트가 누락되거나 서비스가 다운되어 있지 않도록 더욱 각별히 관리해야 합니다.

효율적인 인시던트 관리가 매우 중요한 이유 6가지

인시던트는 피해갈 수는 없습니다. 하지만 인시던트를 잘 관리하고, 해결해나간다면 그 또한 기업과 서비스의 자산이 됩니다. 인시던트 관리는 그 자체만으로 하나의 프로세스, 솔루션이 될 수 있습니다. 모든 규모의 비즈니스에서 인시던트는 매우 중요한 요소이며, 업계 규정 준수 표준을 충족하기 위해 잘 관리 해야 합니다.

효율적인 인시던트 관리는 IT 팀이 취약점과 문제를 신속하게 해결하도록 합니다. 신속한 대응을 통해 인시던트가 미치는 부정적인 영향을 줄이고, 손해를 완화하며, 시스템과 서비스가 계획한 대로 잘 돌아가도록 합니다.

만약 인시던트를 중요하게 생각하지 않고 특별히 관리하지 않는다면, 중요한 데이터를 잃거나, 다운타임으로 인해 생산성과 수익이 감소하게 될 것이며, 최악의 경우 SLA 위반에 따라 책임을 지게 될 수도 있습니다. 사소한 인시던트 하나에도 소중한 시간을 할애해야 하는 이유입니다.

아래는 인시던트 관리가 중요한 이유 6가지를 나타냅니다.

1. 인시던트를 예방합니다.
2. MTTR (Mean Time to Resolution), 평균 인시던트 해결 시간이 개선됩니다.
3. 다운타임을 감소하거나, 제거할 수 있습니다.
4. 데이터 정확성이 높아집니다.
5. 무엇보다 고객 경험을 개선합니다.
6. 비용을 절감할 수 있습니다. 더 알아보기

인시던트를 잘 관리하고 있는지 확인하려면 아래 질문에 답해야 합니다.

- 어떤 팀과 담당자가 인시던트 수습에 더 많은 시간을 할애하고 있나요?
- SLA 내에서 발생한 사고에 대해 어떻게 대응하고 있나요?
- 인시던트들의 에스컬레이션 횟수와 통계를 확인할 수 있나요?
- 인시던트를 담당하는 직원들의 변동 추세가 어떤가요? 공백이 생기지 않나요?
- 인시던트 알람에 피로도가 어떻게 되나요?

위 질문들에 잘 답변하려면 인시던트를 관리하는 시스템이 잘 갖춰진 경우에만 가능할 것입니다. 다음 장에서는 인시던트를 어떻게 관리해야하는지, 필요한 것은 무엇인지, 어떤 도구들이 있는지 알아보겠습니다.

정답은, 인시던트 관리 자동화!

아직도 많은 기업과 조직은 수동적인 인시던트 전달 및 대응으로 인해 팀 간 협업 불화, 응답 시간 단축이라는 어려움을 겪고 있습니다. 이를 위해 애자일(Agile), 데브옵스(DevOps)와 같은 방법론을 도입해 활용하고 있으나, 더욱 근본적으로는 인시던트 그 자체를 효과적으로 관리하는 것 또한 필요합니다. 특히 인시던트를 자동화하는 것은 신속한 대처를 통해 다운타임을 감소할 수 있게 합니다.

이를 위해 IT 담당자들은 중앙집중형 인시던트 관리 시스템에 투자해야 하고, 인시던트 관리 기능 통합을 통해 업무를 최대한 자동화 해야 합니다. 데브옵스를 활용 중이라면 모니터링 툴 체인과 통합할 수 있는 자동화 시스템을 활용해야 합니다. 슬랙이나, 카카오톡, 문자, 전화 등 인시던트 알람과 전파를 위한 소통 방식 또한 개선되어야 합니다.

자동화에 포함될 수 있는 기능은 아래와 같습니다.

- 인시던트 파악하기
- 인시던트에 영향을 받는 담당자들과 커뮤니케이션
- 올바른 담당자에게 인시던트 할당
- 전체 라이프 사이클에 걸친 인시던트 추적
- SLA 위반 시 자동 에스컬레이션
- 인시던트 해결 및 마무리
- 보고서 생성

인시던트 관리를 자동화하는 툴(Tool)이 꼭 갖춰야 할 기능은 무엇일까요?

- 일별, 주별, 월별 스케줄링 및 담당자 지정이 가능한 사용자 친화적인 UI/UX
- 지리적으로 분산된 팀의 인시던트 관리 지원
- 단계 별 수신자 지정 및 인시던트 전달

- 불필요한, 비효율적인 알람 제거
- 다양한 채널을 통한 알람 전달 및 소통: 전화, 문자, 이메일, 메신저 등
- 자동 리포트 생성 및 프로세스 개선
- 모바일 앱 지원
- 다양한 모니터링 도구와 연동 및 통합 가능: Amazon CloudWatch, Azure Monitor, Google Cloud Monitoring, Jira Service Desk, Datadog, NewRelic, Dynatrace, Zendesk

인시던트 관리 자동화 솔루션 ALERTNOW 알아보기

인시던트 관리를 자동화하면 인시던트 전달과 담당자에게 전달하는 데 걸리는 시간, 전달받은 인시던트에 대한 통찰력, 조정이 필요한 알람 등에 가시성을 확보할 수 있습니다.

오픈소스나 사내에서 직접 개발하는 경우도 있지만, 구현이 오래 걸리고 지원이 어려우며 유지보수가 용이하지 않다는 단점이 있습니다. 최근에는 AlertNow, Atlassian OpsGenie, Service Now와 같은 SaaS(Software as a Service) 솔루션을 활용하기도 합니다.

모든 기업이 IT 회사가 되는 세상에서 인시던트 관리에 대한 필요성은 점점 더 커질 것입니다. DevOps 및 IT 조직이 인시던트를 효과적으로 빠르게 해결하는 데 도움이 될 솔루션을 선택하세요. 여러분의 조직에 딱 맞는 솔루션을 찾기 위해서는 단순히 인기 있는 솔루션을 고려하는 것 이상이 필요합니다.

연관 콘텐츠

효과적인 인시던트 대응을 위해 조직이 갖춰야 할 5가지
지속적인 모니터링과 자동화로 이벤트 매니지먼트 개선하는 방법
인시던트 관리에 대한 확실한 안내서
다음에는 피해갈 수 있다! 클라우드 장애 대비를 위한 3가지 고려사항

클라우드에 대해 더 알고 싶으세요?

지금 바로 베스핀글로벌 전문 컨설턴트에게 문의하세요.
클라우드 전문가가 차근차근 설명해 드립니다.

Contact us

베스핀글로벌에 대해 더 알고 싶다면
아래 링크를 클릭해주세요.

Website

베스핀글로벌
소셜미디어 팔로우로
최신 소식을 가장 먼저 받아보세요.

- 페이스북
- 링크드인
- 유튜브
- RSS

BESPIN GLOBAL
HELPING YOU ADOPT CLOUD.