



전략적 필요성으로 카오스 엔지니어링에 투자

AWS 권장 가이드



AWS 권장 가이드: 전략적 필요성으로 카오스 엔지니어링에 투자

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

소개	1
가동 중지 비용 및 카오스 엔지니어링	2
카오스 엔지니어링의 채택 과제	3
카오스 엔지니어링의 누적 효과	3
Grassroots 이니셔티브	6
카오스 엔지니어링 목표	7
목표에서 ROI로 이동	8
경제적 고려 사항	8
고객 경험 및 신뢰 유지	8
ROI 정량화	9
ROI 정량화에 대한 전체적인 접근 방식	10
전략적 필요에 따른 카오스 엔지니어링	11
카오스 엔지니어링을 조직에 통합	12
경영진 동의 받기	13
예방 역설	14
결론	16
리소스	17
부록 A	18
탄력적 아키텍처 목표	18
서비스 복구 목표	18
사용자 경험 목표	18
지표 기반 목표	18
규정 준수 목표	19
부록 B	20
양적 측정	20
정성적 측정	21
부록 C	22
문서 기록	24
용어집	25
#	25
A	26
B	28
C	30
D	33

E	37
F	39
G	40
H	41
정보	43
L	45
M	46
O	50
P	52
Q	55
R	55
S	58
T	61
U	63
V	63
W	64
Z	65
.....	lxvi

전략적 필요성으로 카오스 엔지니어링에 투자

Adrian Hornsby, Amazon Web Services

2025년 1월([문서 기록](#))

카오스 엔지니어링 관행은 제어된 중단을 사용하여 시스템 문제와 중단 및 기타 인시던트를 방지할 기회를 식별합니다. 카오스 엔지니어링은 복원력 있는 시스템을 개선하는 데 필수적이 되었지만 널리 채택되면 오해, 문화적 저항, 리소스 및 비즈니스 가치를 정량화하는 방법에 대한 장애물에 직면합니다. 초기 목표를 설정하면 카오스 엔지니어링 작업을 시작하는 데 도움이 되는 반면, 투자 수익률(ROI)을 정량화하면 특히 경제 압박 상황에서 지속적인 투자가 정당화됩니다.

이 전략 문서는 정량적 운영 개선과 정성적 조직적 이점을 모두 포착하기 위한 전체적인 접근 방식을 간략하게 설명합니다. 궁극적인 목표는 카오스 엔지니어링을 지속적인 비용 정당화 연습이 아닌 사이버 보안과 유사한 전략적 필요성으로 취급하는 것입니다.

가동 중지 비용 및 카오스 엔지니어링의 출현

[ITIC\(Information Technology Intelligence Consulting\)](#)는 기업의 90%가 가동 중지 시간당 300,000 USD를 초과하여 비용을 지출하고, [41%가 시간당 1~500만 달러를 초과하는](#) 것으로 추정합니다. 즉각적인 수익 손실 외에도 가동 중지로 인해 규정 준수 실패, 주가 하락, 상당한 완화 비용, 브랜드 손상 등 장기적인 문제가 발생할 수 있습니다.

가동 중지는 일반적으로 수익 창출 온라인 시스템과 관련이 있지만 부정적인 영향은 그 이상으로 확장됩니다. 모든 대기업과 조직은 기본 수익 모델에 관계없이 HR 및 급여와 같은 내부 시스템의 가용성에 크게 의존합니다.

이러한 핵심 내부 서비스에 영향을 미치는 가동 중지는 회사의 기능 수행을 방해하여 상당한 운영 중단과 재정적 영향을 초래할 수 있습니다. 결과 문제에는 다음이 포함될 수 있습니다.

- 직원 및 공급업체에 대한 지불 지연
- 고객 주문 또는 거래를 처리할 수 없음
- 손상된 보안 시스템에서 허용하는 민감한 데이터 침해
- 생산성 및 수익 기회 손실
- 규정 미준수에 대한 규제 처벌
- 브랜드 평판 손상

카오스 엔지니어링은 의도적으로 제어된 중단을 초래합니다. 카오스 엔지니어링을 사용하여 장애에 대한 시스템의 응답을 이해하거나 확인하는 것은 시스템 복원력을 개선하는 중요한 관행이 되었습니다. 카오스 엔지니어링을 통해 조직은 문제를 사전에 발견하고, 복원력 메커니즘을 검증하고, 궁극적으로 예상치 못한 가동 중지 및 관련 비용의 위험을 줄일 수 있습니다. 카오스 엔지니어링의 이점은 다음과 같습니다.

- 기술 부채 노출
- 작동 중인 근력 운동
- 시스템에 대한 신뢰 구축
- 장애 지점 식별
- 모니터링 및 관찰성 개선
- 실험 기반 학습 지원
- 향상된 복원력을 제공하여 가동 중지 시간 단축

시스템이 점점 더 복잡해지고 고객 기대치가 높아짐에 따라 카오스 엔지니어링의 중요성이 커지고 있습니다. 가트너는 계획되지 않은 가동 중지 시간을 줄이고 복원력을 개선하기 위해 조직에게 카오스 엔지니어링을 중요한 관행으로 권장합니다.

카오스 엔지니어링의 채택 과제

카오스 엔지니어링은 시스템 복원력을 개선하는 데 점점 더 중요한 관행이지만 채택은 다음과 같은 장애물에 직면할 수 있습니다.

- 위험에 대한 오해 – 일반적인 오해는 카오스 엔지니어링은 프로덕션 환경에서만 수행되므로 과도한 위험에 대한 우려로 이어집니다. 이러한 지각은 카오스 엔지니어링 관행의 체계적이고 통제된 특성에 대한 이해 부족에서 비롯됩니다. [AWS Well-Architected Framework](#)에 명시된 대로 먼저 비프로덕션 환경에서 결함 시뮬레이션을 수행합니다.
- 장기 비즈니스 가치 – 카오스 엔지니어링의 이점은 점진적으로 누적되므로 비즈니스 가치를 정량화하고 초기 투자를 정당화하기가 어렵습니다. ROI가 느리면 조직이 카오스 엔지니어링을 우선시하고 유지하기가 어렵습니다.
- 기술 및 전문 지식 격차 - 카오스 엔지니어링에는 조직 내에서 쉽게 사용할 수 없는 고유한 기술 및 전문 지식 세트가 필요합니다. 이러한 전문 지식을 구축하거나 확보하는 것은 특히 실무를 처음 접하는 조직과 리소스가 제한된 조직에 상당한 장벽이 될 수 있습니다.

이 전략 문서의 나머지 부분은 주로 카오스 엔지니어링의 비즈니스 가치를 보여주는 두 번째 과제에 초점을 맞출 것입니다.

카오스 엔지니어링의 누적 효과

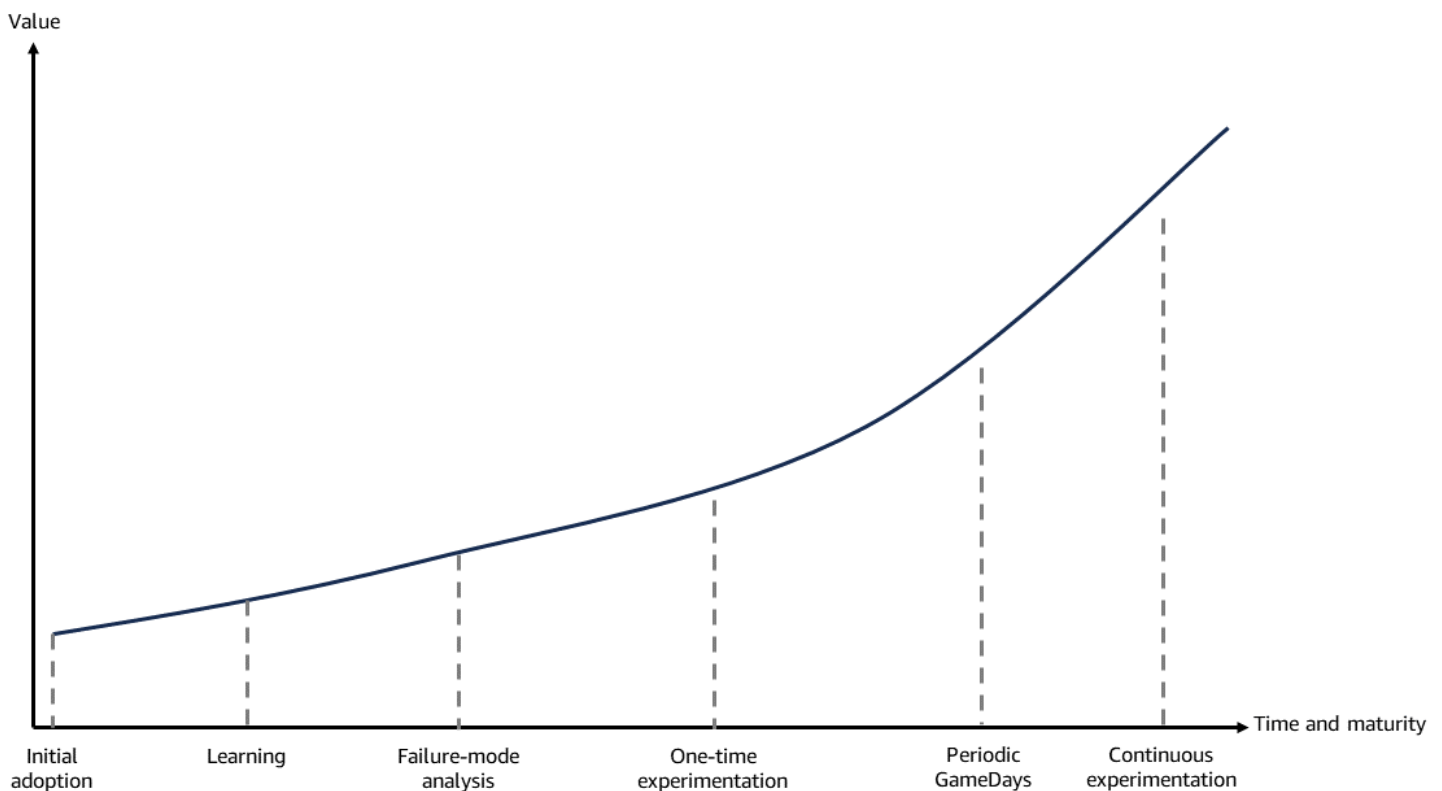
시작 및 종료 날짜가 잘 정의된 기존 기술 프로젝트와 달리 카오스 엔지니어링은 지속적인 학습과 시스템 복원력의 지속적인 개선의 지속적인 관행입니다. 시간 경과에 따른 카오스 엔지니어링 복합의 이점.

시스템이 진화하고 점점 더 복잡해짐에 따라 새로운 장애 모드가 나타납니다. 잠재적 문제를 식별하려면 더 많은 카오스 실험이 필요합니다. 문제 해결에는 몇 달이 걸릴 수 있으며, 특히 시스템과 프로세스가 복잡한 대기업이나 외부 서비스 공급자가 결함을 소유한 경우에는 더욱 그렇습니다.

학습 및 개선의 기회로서 실패를 수용하기 위한 문화적 전환은 수년에 걸쳐 증가하며 조직 내에서 복잡해집니다. 카오스 엔지니어링 실험 자동화 및 지원 도구 개발에 대한 투자는 카오스 엔지니어링 관행을 지속적으로 간소화하고 개선합니다. 시스템 복원력에 대한 이러한 제도적 지식과 이해를 구축하는 것은 시간이 지남에 따라 누적되는 점진적인 프로세스입니다. 카오스 엔지니어링을 통해 개발된 지식, 프로세스 및 도구는 지속적으로 진화하는 시스템과 함께 관행이 성숙해짐에 따라 가치를 높입니다.

다음 다이어그램은 카오스 채택이 다음 단계로 진행됨에 따라 시간이 지남에 따라 가치가 증가하는 방식을 보여줍니다.

- 초기 채택
- 학습
- 장애 모드 분석
- 일회성 실험
- 주기적 GameDays
- 지속적 실험



다이어그램에서 볼 수 있듯이 카오스 엔지니어링의 이점은 시스템에 결함이 주입되기 전에 시작되는 경우가 많습니다. 카오스 실험 자체를 계획하고 설계하는 프로세스는 즉각적인 가치를 제공합니다. 시스템의 잠재적 장애 시나리오, 단일 장애 지점 및 불확실성 영역을 식별하면 개선으로 이어집니다.

예를 들어 장애 시나리오를 작성하고 장애 모드 및 효과 분석(FMEA)이라는 프로세스인 잠재적 계단식 효과를 논의하면 간과되었을 수 있는 명백한 약점이나 격차를 발견하는 데 도움이 됩니다. 조직은 시스템에 의도적인 중단이 발생하기 전에도 이러한 문제를 사전에 해결할 수 있습니다. 자세한 내용은 [복원력 분석 프레임워크](#)를 참조하세요.

또한 카오스 엔지니어링 이니셔티브를 수반하는 시스템 관찰성 및 모니터링에 대한 집중도가 높아지면 즉시 이점을 제공하기 시작합니다. 시스템 동작 및 장애 모드에 대한 가시성을 개선하면 팀이 시스템의 정상 작동 조건을 더 잘 이해하는 데 도움이 됩니다. 또한 가시성이 향상되면 팀이 운영 조건이 한계에 도달했을 때 어떻게 저하, 적응 및 실패하는지 이해하는 데 도움이 됩니다.

일회성 실험 모드와 주기적 GameDay 모드는 모두 연속 실험 모드에 비해 더 수동적인 접근 방식입니다. 엔지니어가 관찰과 실험을 통해 가설을 적극적으로 구체화하고 구체화하는 보다 실습적이고 탐색적인 프로세스가 필요합니다.

반면 연속 실험 모드는 본질적으로 더 자동화됩니다. 이 모드는 제어되고 반복적인 방식으로 승인되고 검증된 가설을 실행하는 데 중점을 둡니다. [전용 카오스 파이프라인을 통해](#) 개발 프로세스에서 자동화 및 통합을 사용하여 일관되고 반복 가능한 실험을 보장합니다.

Grassroots 카오스 엔지니어링 이니셔티브

카오스 엔지니어링 여정은 엔지니어링 팀이 요구 사항을 식별하고 카오스 엔지니어링을 독립적으로 실험하기 시작하는 풀루트 수준에서 시작하는 경우가 많습니다.

이 풀루트 접근 방식에서 팀은 카오스 엔지니어링 사례를 실험, 학습 및 구체화합니다. 카오스 엔지니어링의 가치는 다음과 같은 가시적인 결과를 통해 입증할 수 있습니다.

- 인시던트 감소
- 향상된 관찰성
- 더 빠른 복구 시간
- 개선되고 지속적인 시스템 복원력

Grassroots 카오스 엔지니어링 이니셔티브는 일반적으로 특정 조직 조건에서 나타납니다. 팀에 과도한 관료적 장벽 없이 실험하고 혁신할 수 있는 자유가 있는 높은 수준의 엔지니어링 자율성을 갖춘 환경이 필요합니다. 카오스 실험을 이해하고 구현하기 위한 기술적 기반을 제공하기 때문에 복원력 엔지니어링 또는 분산 시스템에 대한 현지 전문 지식이 매우 중요합니다. 가장 중요한 것은 이러한 이니셔티브가 카오스 엔지니어링의 가치를 이해하는 열의를 가진 개인인 카오스 챔피언에게 의존하는 경우가 많다는 것입니다. 카오스 챔피언은 카오스 엔지니어링 채택을 지지하고, 동료들을 교육하고, 초기 실험을 주도할 의향이 있습니다. 조직의 자유, 기술적 전문 지식, 의욕적인 챔피언이 없으면 잠재적 이점에 관계없이 풀루트 카오스 엔지니어링 노력은 거의 근본적이지 않습니다.

카오스 엔지니어링 채택에서 목표의 역할

초기 목표는 조직 내 풀루트 카오스 엔지니어링 작업에서 유기적으로 나타나는 것이 일반적입니다. 이러한 팀 또는 그룹은 자체적으로 반복되는 문제를 해결해야 하기 때문에 더 높은 수준에서 명시적인 승인이나 우선순위 지정 없이 카오스 엔지니어링 사례를 살펴보는 경우가 많습니다.

팀은 이러한 결과를 사용하여 더 광범위한 조직 채택을 위한 설득력 있는 사례를 구축하여 효과적으로 다른 팀의 근거가 될 수 있습니다.

풀루트 노력의 이점이 무시하기에는 너무 중요해지면 이러한 팀은 노력과 지식을 리더십으로 높이고 목표를 설정할 수 있습니다. 이렇게 향상된 가시성을 통해 조직 전체의 복원력 목표를 쉽게 채택할 수 있으며 카오스 엔지니어링 구현에 필요한 지원과 리소스로 이어질 수 있습니다.

목표, 특히 리더십이 주도하고 상당한 중단에 대응하여 수립된 목표는 카오스 엔지니어링 관행 채택을 촉진시키는 데 중요한 역할을 합니다. 일반적인 유형의 목표는 다음과 같습니다.

- 단일 장애 지점(SPOF)을 식별하고 줄이기 위한 가용성 목표
- 중단 또는 장애로부터 복구할 수 있는 능력을 개선하기 위한 서비스 복구 목표
- 특정 서비스 수준 목표(SLOs 충족하기 위한 사용자 경험 목표
- 알려진 가용성 위험을 완화하고 권장 복원력 조치를 구현하는 진행 상황을 추적하는 지표 기반 목표
- 운영 복원력을 입증하기 위한 규제 및 규정 준수 목표

이러한 목표 유형 중 일부와 Amazon 및 기타 조직이 카오스 엔지니어링 채택 중에 목표를 사용한 방법에 대한 자세한 내용은 [부록 A](#)를 참조하세요.

이러한 목표는 설득력 있는 정당화 역할을 하며 카오스 엔지니어링 채택을 촉진하기 위한 대상 지정되고 실행 가능한 접근 방식을 제공합니다. 처음에는 목표가 기존 ROI 지표의 프록시 역할을 합니다. 목표는 정량화 가능한 복원력 ROI 계산을 얻기 어려울 수 있는 강력한 근거를 제공합니다. 도입 초기에 이러한 목표가 없으면 카오스 엔지니어링 관행은 효율성을 보여주고 더 광범위한 조직 동의를 얻는 데 실패할 위험이 있습니다.

목표에서 ROI 측정으로의 전환

관행이 성숙해지고 초기 목표가 달성되면 결국 목표 설정에서 카오스 엔지니어링의 실질적인 재정적 이점인 투자 수익(ROI) 정량화로 전환됩니다. 교대 근무는 두 가지 주요 이유에서 비롯됩니다.

- 경제적 고려 사항
- 고객 경험 및 신뢰 유지

경제적 고려 사항

경제 성장과 건전한 재무 상황에서 기업은 카오스 엔지니어링 전략의 특정 목표를 설정하는 데 광범위한 근거가 필요하지 않은 경우가 많습니다. 그러나 금융 환경의 변화로 인해 많은 조직이 투자를 재평가하게 되었으며 카오스 엔지니어링 구현은 정량화된 ROI를 제공해야 합니다.

이제 이러한 기업은 카오스 엔지니어링 관행의 가치와 영향을 보여주기 위해 명확하고 전통적인 ROI 지표를 설정해야 합니다. 이 문제는 [예방 역설](#)로 인해 더욱 복잡해집니다. 예방 역설은 이해관계자가 회피된 재해를 과소 평가하는 경향이 있기 때문에 인시던트를 성공적으로 방지하여 투자를 정당화하기가 더 어려울 때 발생합니다. 운영 우수성 문화가 깊이 정체된 조직도 ROI 지표를 사용하여 카오스 엔지니어링의 지속적인 채택을 정당화해야 한다는 압박에 직면합니다.

고객 경험 및 신뢰 유지

목표 기반 복원력을 유지하는 것은 장기적으로 어려울 수 있습니다. 복구 시간 목표 달성과 같은 초기 목표가 충족되면 다음 주요 중단이 발생할 때까지 지속적인 카오스 엔지니어링 투자를 정당화하는 것이 어려워집니다. 투자 흐름과 ebb는 사후 대응적인 톱니 주기를 생성합니다. 새로운 중단이 발생할 때마다 복원력에 대한 투자는 근본 원인을 해결하는 새로운 목표로 급증합니다. 새 목표가 충족되면 다음 인시던트까지 투자가 감소하여 사후 대응 루프를 다시 시작합니다.

이 사후 대응적 접근 방식을 주도하는 중단은 고객에게 부정적인 영향을 미칩니다. 핵심 질문: 고객이 보다 탄력적인 경쟁자를 위해 서비스 공급자를 중단하기 전에 허용할 수 있는 주요 중단 횟수

카오스 엔지니어링의 ROI 정량화

현재 카오스 엔지니어링을 위한 장기 투자 수익률(ROI)을 정량화하기 위한 포괄적인 방법론 또는 실제 데이터를 제공하는 게시된 리소스는 거의 없습니다.

[카오스 엔지니어링의 비즈니스 사례](#) 백서에서 Netflix는 카오스 엔지니어링의 ROI를 계산하는 데 유용한 방정식을 제공합니다. 이 방정식은 카오스 엔지니어링 여정을 시작하는 조직에 출발점을 제공합니다.

이 방정식을 사용하려면 다음 비용을 정확하게 추정해야 합니다.

- 예방 가능한 중단 및 예방할 수 없는 중단
- 카오스 엔지니어링 프로그램 구현 비용
- 혼란으로 인한 피해 비용

혼란으로 인한 유해는 카오스 엔지니어링 실험의 일환으로 시스템에 의도적으로 장애 또는 난기류를 주입하여 발생하는 부정적인 영향 또는 중단을 말합니다. 이 방정식에서는 예방 가능한 중단 및 예방 불가능한 중단 비용, 카오스 엔지니어링 프로그램 구현 비용, 카오스로 인한 피해 비용을 추정해야 합니다.

카오스 엔지니어링 프로그램으로 방지할 수 있는 문제를 확실하게 결정하는 것은 어려운 작업입니다. 문제의 근본 원인을 살펴보고 카오스 엔지니어링 실험이 문제를 식별하는 데 어떻게 도움이 되었는지 추측하는 가상 분석이 필요합니다. 최신 시스템은 매우 복잡하며 다양한 구성 요소, 서비스 및 타사 라이브러리 간의 상호 의존성과 상호 작용이 많기 때문에이 분석은 어렵습니다. 또한 시스템의 결함은 비결정적인 경우가 많으며 결함을 유발하는 조건은 숨김에서 완전히 이해하기 어려울 수 있습니다.

Netflix에서 제안한 접근 방식에는 몇 가지 제한이 있지만 카오스 엔지니어링을 탐색하기 시작하는 조직에 좋은 토대가 됩니다. 이 방정식은 비용과 잠재적 이점을 추정하는 데 도움이 되며, 이는 이러한 프로그램 구현에 대한 결정을 내리는 데 도움이 됩니다. 그러나 조직이 카오스 엔지니어링 여정에서 더 발전함에 따라 ROI 평가를 확장하여 보다 전체적인 관점을 통합하는 것이 중요합니다.

이 전체적인 접근 방식은 운영 중단 감소 및 엔지니어링 비용의 직접적인 이점을 포착할 뿐만 아니라 조직의 전반적인 복원력에 미치는 장기적이고 혁신적인 영향을 강조합니다. 카오스 엔지니어링의 복합적인 이점과 광범위한 조직적 효과를 포착하여 카오스 엔지니어링의 진정한 가치와 영향을 보다 정확하게 표현합니다.

ROI 정량화에 대한 전체적인 접근 방식

전체적인 ROI 평가는 정량적 측정뿐만 아니라 정성적 요인도 고려해야 합니다. 전체적인 접근 방식에는 장기간에 걸쳐 대규모로 카오스 엔지니어링을 수행하는 조직의 실제 데이터가 필요합니다. 수집한 방정식 접근 ROI 데이터를 통해 풀루트 프로젝트 및 목표에서 시작하는 데이터를 사용할 수 있습니다.

양적 측정은 수량 또는 빈도에 중점을 둡니다. 측정값은 객관적이며 통계적으로 분석할 수 있습니다. 예를 들면 설문 조사, 실험 및 데이터 분석이 있습니다. 양적 측정에는 다음이 포함될 수 있습니다.

- 인시던트 지표
- 비용
- 개선 사항
- 규정 준수
- 채택률
- 고객 만족도

정량적 측정값을 추적하면 카오스 엔지니어링의 직접적인 운영 이점을 입증할 수 있습니다.

정성적 측정은 설명적이며 경험과 의견을 이해하는 데 중점을 둡니다. 종종 주관적이며 수치적으로 쉽게 측정할 수 없습니다. 카오스 엔지니어링의 경우 정성적 측정은 광범위한 조직적 영향을 포착합니다. 정성적 측정에는 다음이 포함될 수 있습니다.

- 직원 신뢰도
- 문화 전환
- 공동 작업
- 훈련 효과
- 인재 보존
- 브랜드 평판
- 경쟁 우위

정량적 재무 영향과 정성적 조직적 이점을 모두 고려하면 복원력 문화를 조성하면서 지속적인 카오스 엔지니어링 투자에 대해 더 많은 정보를 바탕으로 결정을 내릴 수 있습니다.

이러한 조치 및 관련 인시던트 분류 프레임워크에 대한 자세한 내용은 [부록 B](#) 및 [부록 C](#)를 참조하세요.

전략적 필요성으로 ROI에서 카오스 엔지니어링으로 전환

ROI를 모니터링하려는 유혹이 있지만 카오스 엔지니어링의 가치를 측정하는 데 따른 문제로 인해 조직이 전략적 복원력 투자보다 즉각적이고 단기적인 효율성을 우선시하는 경우가 많습니다. 이 접근 방식은 카오스 엔지니어링을 복원력의 주요 동인으로 간과하고 중단 방지의 경쟁 이점을 간과합니다. 카오스 엔지니어링의 실제 가치는 향후 장애를 방지하는 데 있습니다. 카오스 엔지니어링은 장기적인 비즈니스 연속성을 지원합니다.

ROI에 집중하는 대신 카오스 엔지니어링을 사이버 보안처럼 취급하세요. Forbes 기사 [Cybersecurity As A strategic investment: How ROI Optimization Can Lead To A More Secure Future](#)에 설명된 대로 사이버 보안은 조직의 비용 센터 또는 의무 비용으로 간주되어서는 안 됩니다. 이러한 사고방식은 시간이 지남에 따라 강력한 사이버 보안 조치가 제공할 수 있는 전략적 가치를 인식하지 못하기 때문입니다. 대신에 작성자는 사이버 보안을 경쟁 우위를 창출하는 장기 투자로 취급하기 위한 관점을 전환함으로써 조직은 각 시장 내에서 혁신, 운영 효율성 및 차별화를 위한 새로운 수단을 모색할 수 있다고 주장합니다. 이 접근 방식을 채택함으로써 작성자는 최고 정보 보안 책임자(CISOs)가 경영진의 동의와 자금 조달을 더 잘 보호할 수 있다는 결론을 내립니다. 그런 다음 점점 더 위험한 사이버 환경에서 경쟁자를 능가할 수 있도록 회사를 포지셔닝할 수 있습니다. 사이버 보안의 이러한 장기적이고 전략적인 가치 창출은 카오스 엔지니어링 사례에 내재된 지속적인 개선과 병렬화됩니다.

보안은 조직의 자산 운영 및 보호 능력을 보호하는 반면, 카오스 엔지니어링은 핵심 시스템 및 서비스의 가용성, 신뢰성 및 복구 가능성을 보장하는 데 도움이 됩니다. 장기적인 가치와 경쟁 우위를 실현하려면 카오스 엔지니어링을 지속적인 정당화가 필요한 이니셔티브가 아닌 핵심 역량과 전략적 필수 요소로 취급하십시오.

다음 다이어그램은 카오스 엔지니어링이 잔디 루트에서 목표 및 ROI로 발전하여 전략이 되는 과정을 보여줍니다.



풀루트 수준에서 개별 팀은 일반적으로 현지 요구 사항에 따라 독립적으로 실험합니다. 이러한 실험은 인시던트 감소와 관찰성 개선을 통해 가치를 보여주는 숙련된 엔지니어의 지지를 받습니다.

이러한 노력이 성공하면 팀은 학습을 리더십으로 높일 수 있습니다. 이러한 가시성을 통해 노력은 목표 기반 단계로 전환됩니다. 조직은 리소스 및 광범위한 구현 지원을 기반으로 복원력 및 복구를 위한 공식 목표를 설정합니다.

마지막으로 카오스 엔지니어링은 사이버 보안과 마찬가지로 지속적인 ROI 정당화를 필요로 하는 것 이상으로 성숙합니다. 이 단계에서 카오스 엔지니어링은 조직 프로세스에 완전히 통합됩니다. 구현은 단기 지표가 아닌 장기 복원력에 중점을 둡니다. 카오스 엔지니어링은 경쟁 우위와 고객 신뢰를 유지하는 데 필수적인 핵심 기능으로 취급됩니다.

카오스 엔지니어링을 조직에 통합

카오스 엔지니어링을 보안과 동일한 중요도로 높이려면 다음 제안을 고려하세요.

- 카오스 엔지니어링을 협상할 수 없는 관행으로 설정 - 사이버 보안이 조직의 기본 요구 사항으로 간주되는 것처럼 카오스 엔지니어링을 시스템 복원력과 신뢰성을 보장하기 위한 필수 관행으로 간주합니다. 카오스 엔지니어링을 선택적 또는 임의 활동으로 사용하는 것이 아니라 조직의 프로세스, 도구 및 문화에 통합합니다. 자세한 내용은 [복원력 수명 주기 프레임워크](#) 가이드를 참조하세요.
- 경영진 수준의 보안 동의 및 지원 - 보안 이니셔티브와 마찬가지로 카오스 엔지니어링 노력에는 경영진의 동의와 적극적인 지원이 있어야 합니다. 여기에는 조직 전체에서 카오스 엔지니어링 관행을 구현하고 유지하기 위한 전용 리소스, 예산 및 인력 할당이 포함됩니다.
- 거버넌스 및 감독 구현 - CISO 및 보안 거버넌스 프레임워크와 마찬가지로 전담 카오스 엔지니어링 팀 또는 최고 복원력 책임자를 설정합니다. 이 팀 또는 역할은 다양한 팀과 사업부에서 카오스 엔지니어링 작업을 감독하고 조정할 책임이 있습니다.
- 카오스 엔지니어링을 개발 및 운영 주기에 통합 - 보안 관행이 소프트웨어 개발 및 배포 프로세스에 통합되는 것처럼 카오스 엔지니어링을 소프트웨어 개발 및 제공 수명 주기의 원활한 일부로 만듭니다.
- 정기적인 카오스 엔지니어링 드릴 및 시뮬레이션 수행 - 보안 침해 시뮬레이션 및 인시던트 대응 드릴과 마찬가지로 정기적인 카오스 엔지니어링 실험을 수행하여 인시던트 대응 기능을 검증하고 잠재적 사각 지대를 사전에 식별합니다.
- 카오스 엔지니어링을 사용하여 런북 유지 관리 - 보안 검토 수행과 마찬가지로 카오스 엔지니어링 실험을 사용하여 인시던트 대응 및 복구를 위한 런북의 효과와 정확성을 검증합니다. 또한 카오스 엔지니어링 실험은 대기 중인 엔지니어가 런북 절차 실행을 연습할 수 있는 사실적인 시뮬레이션 역할을 할 수 있습니다. 시뮬레이션을 통해 엔지니어는 실제 인시던트를 처리할 수 있도록 운영 중인 메모리와 준비 상태를 유지할 수 있습니다.

- 복원력 문화 조성 - 보안 인식 훈련과 마찬가지로 카오스 엔지니어링 교육 및 지식 공유 이니셔티브에 투자하여 복원력 문화를 조성합니다. 카오스 엔지니어링 관행을 채택하는 팀을 위한 훈련 프로그램, 부서 간 협업 및 인센티브를 포함합니다.
- 복원력 지표 측정 및 보고 - 복원력 지표를 정기적으로 모니터링하고 이해관계자에게 보고합니다. 이 문서에서 설명하는 정량적 및 정성적 지표를 시작점으로 사용합니다.
- 복원력을 경쟁 우위로 취급 - 사이버 보안 조치는 경쟁 우위를 제공할 수 있습니다. 마찬가지로 카오스 엔지니어링 및 복원력 기능을 고객에게 더 안정적이고 신뢰할 수 있는 서비스를 제공하는 데 도움이 되는 차별화 요소로 봅니다.

경영진 동의 받기

카오스 엔지니어링은 C-suite의 기존 책임 내에 명확한 소유자가 없는 경우가 많습니다. CEO는 성장, 수익성 및 시장 리더십을 중시합니다. CFO는 재무 성과, 비용 제어 및 위험 관리에 중점을 둡니다. CTO는 기술 전략, 제품 로드맵 및 엔지니어링 우수성을 우선시합니다. CISO는 보안 및 규정 준수를 감독합니다.

단일 경영진이 실제로 복원력을 소유하지 않기 때문에 동의와 지원을 얻기 어려운 경우가 많습니다. 하지만 시스템 장애는 수익, 고객 만족도 및 브랜드 평판에 영향을 미치며, 이는 CEO와 CFO의 관심사입니다. CTO와 CISO는 복원력 조치를 구현해야 하지만 조직의 명령이 부족할 수 있습니다. 이러한 모호성은 전략적 투자를 하고 조직을 일반적인 복원력 전략에 맞추는 데 방해가 될 수 있습니다.

또한 이러한 모호함으로 인해 카오스 엔지니어링과 같은 복원력 이니셔티브를 위해 경영진의 동의를 얻기가 어렵습니다. 결국 C레벨 리더는 성장, 혁신, 고객 경험, 규정 준수 등 다양한 전략적 우선 순위를 정하고 있습니다.

C레벨 경영진에게 카오스 엔지니어링의 가치를 효과적으로 전달하려면 다음 접근 방식을 고려하세요.

- C-suite 경영진의 주요 우려 사항과 결정 동인을 결정합니다.

예를 들어 최고 경영진이 고객 이탈, 규정 준수, 비용 절감 또는 경쟁 압력에 대해 걱정하고 있습니까? 카오스 엔지니어링을 회사의 고유한 과제와 목표에 맞는 포스 승수로 배치합니다.

- 공유된 목표와 전략적 결과를 식별합니다.

카오스 엔지니어링 전략은 전체 조직의 성장 전략, 고객 경험, 시장 기회 및 운영 효율성을 어떻게 지원하나요? 목표, 비즈니스 영향, ROI 및 이니셔티브를 수행하지 않을 경우의 위험에 따라 이니셔티브의 우선순위를 정합니다.

- 주요 복원력 지표를 사용하여 카오스 엔지니어링 전략의 효과를 정량화 가능한 용어로 전달합니다.

가용성, 탐지 시간, 대응 시간 및 복구 시간이라는 네 가지 주요 복원력 지표로 시작합니다. 수익, 비용 절감, 브랜드 평판과 같은 비즈니스 성과와 직접 연계합니다.

- 기술 세부 정보를 잃어버리지 마세요.

전반적인 감정과 측정 가능한 비즈니스 영향에 집중합니다. C-suite는 성장을 주도하고, 고객 신뢰를 높이고, 혁신을 촉진하는 결과에 신경을 씁니다.

예방 역설

장애가 발생하기 전에 성공적으로 완화되면 이해관계자에게 취해진 예방 조치의 가치 및 필요성을 설득하기가 어려워집니다. 이러한 현상을 예방 역설이라고 합니다. 예방 역설은 카오스 엔지니어링을 전략적 필수 요소로 통합하는 데 가장 큰 장애물이며 인간의 인식에 내재된 편향에서 비롯됩니다.

Y2K 버그는이 역설을 잘 보여줍니다. 전 세계 컴퓨터 시스템을 업데이트하는 데 수년간의 준비와 수십억 달러가 투자되었습니다. 그러나 2000년으로의 원활한 전환은 많은 사람들이 Y2K 우려 사항의 과도한 특성에 대한 증거로 해석되었습니다. 수행된 예방 노력의 성공은 거의 인식되지 않았습니다.

이러한 방지 역설은 오늘날 카오스 엔지니어링에 투자하는 조직에 계속 도전하고 있습니다. 사전 예방 조치를 통해 잠재적 중단이 성공적으로 방지되면 재해가 매우 없기 때문에 예방에 소비되는 리소스를 정당화하기가 역설적으로 어려울 수 있습니다.

이 현상의 근본 원인은 정보를 처리하기 위해 마음이 연결된 방식에 있습니다. 인간의 인지 프로세스는 실제 이벤트와 가시적인 결과에 대응하고 기억하는 데 중점을 둡니다. 재해가 방지되면 보유하거나 공유할 획기적인 서술이 없습니다. 예방 역설의 또 다른 측면은 뒷모습 편향입니다. 이벤트가 발생한 후 개인은 아무 일도 발생하지 않았다고 결론을 내리는 경향이 있으므로 실제로 문제가 되지 않았습니다. 적절한 예방 조치로 인해 실제 문제가 방지될 가능성은 인식되지 않습니다. 이 심리적 사각 지대는 조직에 영구적인 문제를 일으킵니다. 예방 및 복원력이 높을수록 역방향에서 더 많은 노력이 필요하지 않은 것처럼 보입니다.

예방 역설을 해결하기 위해 조직은 특정 단계를 수행하여 보이지 않는 예방 작업을 가시화하고 측정 가능하며 가치 있게 만들 수 있습니다. 잠재적 단계는 다음과 같습니다.

- 예방 조치 없이 발생할 수 있는 일을 문서화하고 시뮬레이션합니다.
- 예방 조치가 회피된 잠재적 재해를 측정하는 이벤트에 대한 스토리를 공유합니다.
- 준비하지 않았고 결과적으로 결과를 겪은 피어 조직을 가리킵니다.
- 잠재적 영향의 맥락에서 예방 비용을 제시합니다.
- 예방 노력을 눈에 보이는 마일스톤과 업적으로 나눕니다.

- 예방 조치가 존재하는 이유와 과거 중요도에 대한 제도적 메모리를 구축합니다.
- 이해관계자에게 복원력 및 카오스 엔지니어링 관행의 가치에 대해 정기적으로 교육합니다.

결론

카오스 엔지니어링은 조직의 전략적 필수 요소입니다. 채택 여정은 오해, 문화적 저항 및 리소스 제약과 같은 문제에 직면할 수 있지만 명확한 리더십 기반 목표를 설정하면 프로세스를 촉진할 수 있습니다. 관행이 성숙해지면 정량적 운영 개선과 질적 조직적 이점을 모두 포착하는 전체적인 접근 방식을 통해 투자 수익을 정량화합니다. 전체적인 접근 방식은 경제적 압박이 있을 때 특히 중요합니다.

이러한 전략적 필요성을 현실로 전환하려면 먼저 조직의 현재 성숙도를 평가합니다. 조직은 폴루트 실험 단계, 목표 기반 단계 또는 그 사이의 어느 곳에 있습니까? 이 평가를 기반으로 맞춤형 로드맵을 생성하여 다음을 수행합니다.

- 카오스 엔지니어링 거버넌스를 수립합니다(예: 최고 복원력 책임자 지정).
- 카오스 사례를 개발 워크플로에 통합합니다.
- 정기적인 훈련 프로그램을 구현합니다.
- 포괄적인 복원력 지표를 개발합니다.

이 변환은 하룻밤 사이에 수행되지 않습니다. 그러나 이러한 구체적인 단계를 수행하면서 지속적인 경영진 지원을 확보하면 카오스 엔지니어링을 사이버 보안과 동일한 전략적 수준으로 높이는 데 도움이 됩니다. 사이버 보안과 마찬가지로 카오스 엔지니어링은 조직의 운영 DNA 및 프로세스의 필수적인 부분이 될 수 있습니다.

리소스

- [ITIC 2021 글로벌 서버 하드웨어, 서버 OS 신뢰성 설문 조사 결과](#)
- [카오스 엔지니어링의 비즈니스 사례](#)
- [전략적 투자로서의 사이버 보안: ROI 최적화가 더 안전한 미래로 이어지는 방법](#)
- [카오스 엔지니어링에 대한 I&O 리더 가이드](#)
- [AWS Resilience Hub 점수를 사용하는 방법](#)
- [AWS Resilience Hub 콘솔을 사용하여 권장 실험 구현](#)

부록 A – 카오스 엔지니어링을 위한 목표 유형

목표 유형에 대한 다음 설명에는 Amazon 및 기타 조직이 카오스 엔지니어링 목표를 설계한 방법에 대한 실제 예제가 포함됩니다.

탄력적 아키텍처 목표

카오스 엔지니어링을 채택하기 위한 초기 동인 중 하나는 시스템 및 인프라 전반에서 단일 장애 지점(SPOF)을 식별하고 줄이는 것입니다. 목표는 중요한 시스템 및 아키텍처, 특히 새로운 서비스 또는 애플리케이션의 복원력을 검증하기 위해 설정됩니다.

탄력적 아키텍처 목표에는 서비스 종속성의 장애를 시뮬레이션하는 카오스 실험 실행이 포함됩니다. 실험은 제한 시간, 재시도, 캐싱 동작 및 회로 차단기 구성이 올바르게 작동하는지 확인합니다. 이러한 실험은 해결 문제를 발견하여 고객에게 영향을 미치는 인시던트를 방지하는 데 도움이 됩니다. 예를 들어 [카오스 엔지니어링을 사용하여 Prime Video에서 복원력 있는 서비스 구축](#)을 참조하세요.

서비스 복구 목표

서비스 복구 목표는 운영 중단 또는 인프라 장애로부터 복구하는 능력을 개선하는 데 중점을 둡니다. 예를 들어, 운영 중단 시 조직은 핵심 서비스에 대한 특정 복구 시간 목표(RTO)를 달성하는 것을 목표로 할 수 있습니다. 팀은 카오스 실험을 설계하여 대피 전략, 장애 조치 메커니즘 및 자동화된 복구 프로세스를 검증하고 최적화할 수 있습니다. 최적화는 궁극적으로 서비스 복원에 필요한 시간을 줄입니다. 예제는 [AWS Lambda: Resilience under-the-hood](#)를 참조하세요.

사용자 경험 목표

특히 트래픽이 많은 기간이나 중요한 이벤트 발생 시 일관되고 안정적인 사용자 경험을 유지하는 것이 중요합니다. 이러한 경우 특정 서비스 수준 목표(SLOs) 충족을 중심으로 목표를 설정합니다. 이 고객 중심 접근 방식을 사용하면 장애 또는 성능 저하된 조건에서도 복원력 노력이 우수한 사용자 경험을 제공하는 것과 직접 연계됩니다. 예제는 [엔지니어링 복원력: Amazon Search의 카오스 엔지니어링 여정에서 얻은 교훈을 참조하세요](#).

지표 기반 목표

검증된 복원력 모범 사례를 채택한 서비스에 점수를 부여하여 계산된 복원력 점수와 같은 정량적 지표를 기반으로 목표를 설정할 수 있습니다. 그런 다음 특정 카오스 실험을 사용하여 복원력 점수를 결정

할 수 있습니다. 이 점수는 팀이 알려진 가용성 위험을 완화하고 권장 복원력 조치를 구현하는 진행 상황을 추적할 수 있는 조치 역할을 할 수 있습니다. 그러나 이러한 점수를 신중하게 해석하고 더 광범위한 복원력 목표를 희생하면서 단일 지표를 과도하게 강조하지 않는 것이 중요합니다. 예제는 [복원력 점수 이해를](#) 참조하세요.

규정 준수 목표

금융 서비스 산업은 강력한 복원력 기능을 요구하는 엄격한 규제 요구 사항에 따라 주로 카오스 엔지니어링을 수용하는 최전선 러너로 부상했습니다. 규정에 따라 금융 기관은 중요한 시스템 및 프로세스의 취약성을 사전에 식별, 테스트 및 해결해야 합니다. 이러한 규정에는 다음이 포함됩니다.

- 미국 연방 기관에서 발행한 운영 복원력을 강화하기 위한 사운드 프랙티스에 대한 기관 간 논문
- 운영 복원력에 대한 유럽 중앙 은행의 지침
- 디지털 운영 복원력법(DORA)에 대한 유럽위원회의 제안

조직이 금융 기관인 경우 포괄적인 테스트 및 검증 전략을 통해 운영 복원력을 입증하기 위한 명시적 목표를 설정하여 이러한 규정을 준수합니다. 예를 들어 [London Stock Exchange Group은에서 카오스 엔지니어링 AWS 을 사용하여 복원력을 개선](#)합니다를 참조하세요.

부록 B – 정량적 및 정성적 측정

이 섹션에서는 운영 개선을 추적하는 정량적 지표와 카오스 엔지니어링 관행에서 더 광범위한 조직 결과를 평가하는 정성적 측정치를 간략하게 설명합니다.

양적 측정

다음 정량적 측정은 카오스 엔지니어링 사례를 통해 달성된 직접적인 인시던트 및 운영 개선을 입증할 수 있는 주요 지표를 추적하기 위한 프레임워크를 제공합니다.

- 인시던트:
 - 인시던트 빈도 – 인시던트 분류 프레임워크 내의 인시던트 수를 추적하고 일정 기간 동안 중요도 (심각, 메이저, 마이너)로 분류합니다. 인시던트 분류 프레임워크에 대한 자세한 내용은 [부록 C](#)를 참조하세요.
 - 가동 중지 및 성능 저하 - 각 인시던트 분류에 대한 총 가동 중지 또는 서비스 성능 저하 기간을 측정합니다.
 - 인시던트 대응 지표 – 인시던트를 이해하려면 각 인시던트 분류에 대해 탐지 시간, 식별 시간, 완화 시간, 복구 시간, 에스컬레이션 시간 및 기타 관련 지표를 측정합니다.
 - 고객에게 영향을 미치는 인시던트 – 고객에게 영향을 미치는 인시던트 수 또는 고객에게 영향을 미치기 전에 포함된 인시던트의 비율을 추적합니다.
 - 런북 변경 – 카오스 실험을 통해 얻은 인사이트에서 얻은 런북 업데이트 또는 개정 수를 추적합니다. 실행서는 특정 유형의 인시던트에서 복구하기 위해 특정 작업 또는 절차를 수행하기 위한 자세한 지침을 제공합니다.
- 비용:
 - 인프라 비용 – 복원력을 개선하기 위해 취한 조치에 필요한 클라우드 컴퓨팅 리소스 및 중복 조치를 포함하여 인프라 비용에 대한 데이터를 수집합니다.
 - 고객 영향 – 시스템 장애 또는 가동 중지와 관련된 고객 경험, 이탈률 및 수익 손실에 미치는 영향을 측정합니다.
 - 직원 생산성 – 엔지니어링 및 운영 팀이 인시던트 대응, 소방, 사후 작성 및 시스템 장애와 관련된 기타 대응 작업에 소요한 시간을 추적합니다.
 - 지속적인 시스템 개선 – 카오스 실험의 인사이트의 직접적인 결과로 구현된 프로세스 개선, 아키텍처 변경 또는 자동화된 복구 메커니즘의 수를 계산합니다.
 - 규정 준수 – 비용을 추적하고 운영 복원력과 관련된 규제 요구 사항 또는 업계 표준을 충족하기 위해 노력합니다.

- 채택 – 조직 전반의 카오스 관행 채택률을 추적합니다.
- 고객 만족도 – 고객 만족도 지표의 변화를 측정하여 시스템 신뢰성 개선이 비즈니스에 미치는 영향을 측정합니다.

정성적 측정

다음 정성적 측정은 카오스 엔지니어링 사례를 통해 달성된 광범위한 조직 결과를 추적하기 위한 프레임워크를 제공합니다.

- 직원 신뢰도 및 준비 상태:
 - 조사 팀은 주기적으로 실제 인시던트를 처리하는 데 대한 신뢰도 수준과 대기 교체에 대한 인식된 준비 상태를 측정합니다.
 - 훈련의 일환으로 카오스 실험에 참여한 대기 중인 엔지니어의 비율을 추적합니다.
- 문화 전환:
 - 설문조사, 피드백 세션 또는 감사를 통해 복원력 사고방식이 조직에 침투한 정도를 평가합니다.
 - 카오스 엔지니어링 관행을 적극적으로 지지하고 지지하는 팀의 수를 추적합니다.
- 부서 간 협업 및 지식 공유:
 - 카오스 엔지니어링 학습과 관련된 팀 간 지식 공유 세션 또는 워크숍의 빈도와 참석을 추적합니다.
 - 여러 팀 또는 부서가 참여하는 공동 카오스 엔지니어링 이니셔티브의 수를 추적합니다.
- 훈련 효과:
 - 훈련 후 설문 조사 또는 평가를 수행하여 카오스 엔지니어링 훈련 프로그램의 효과를 평가합니다.
 - 카오스 엔지니어링 훈련 프로그램에 참여하고 포스트모템을 읽는 엔지니어 수를 추적합니다.
- 인재 유치 및 유지:
 - 카오스 엔지니어링 프로그램이 중단 수정에 소요되는 시간과 노력을 줄여 최고의 엔지니어링 인재를 유치하고 유지하는 데 도움이 되는지 평가합니다.
- 브랜드 평판:
 - 운영 복원력에 대한 조직의 입증된 약속과 관련된 브랜드 인식 또는 평판의 변화를 추적합니다.
- 경쟁 우위:
 - 시스템 가용성 측면에서 동종 업계에 비해 경쟁 우위를 추적합니다.

부록 C – 인시던트 분류

프레임워크는 시스템에 영향을 미치는 장애 유형 및 문제에 대한 전체적인 보기를 제공하므로 분류 프레임워크 내에서 인시던트를 추적하는 것이 중요합니다. 조직이 인프라 장애와 같은 단일 클래스 내에서만 인시던트를 추적하는 경우 인사이트와 다른 영역의 개선 기회를 놓칠 수 있습니다. 여러 클래스에서 인시던트를 추적하면 수행할 다양한 카오스 실험을 더 잘 이해할 수 있습니다. 이러한 관점은 잠재적 사각 지대를 식별하는 데 도움이 되며 엔지니어링 범위 확장을 지원하여 복원력이 뛰어나고 내결함성이 뛰어난 시스템을 만듭니다.

제안된 인시던트 분류 프레임워크는 인시던트의 특성과 잠재적 영향을 기반으로 인시던트를 분류하는 데 도움이 되도록 설계되었습니다. 인시던트를 8가지 주요 범주로 그룹화하는 상위 수준 분류를 사용합니다.

- 배포 문제:
 - 실패한 배포
 - 롤백 실패
 - 배포 중 구성 문제
- 소프트웨어 버그 및 회귀:
 - 기능적 버그
 - 통합 문제
 - 성능 문제
 - 할당량 문제
 - 복원력 메커니즘 문제(재시도 횟수, 제한 시간)
 - 데이터 무결성 문제
- 테스트 문제:
 - 누락된 테스트
 - 비효율적인 테스트
 - 급증 테스트
- 인프라 장애:
 - 하드웨어 장애(서버, 네트워크 디바이스, 스토리지)
 - 조정 문제
 - 종속성 실패(타사 서비스, APIs)
 - 네트워크 연결 문제

- 운영 문제:
 - 인적 오류(잘못 구성, 우발적인 변경)
 - 실패 모니터링 및 알림
 - 용량 계획 문제
 - 백업 및 복원 실패
- 보안 인시던트:
 - 무단 액세스 시도
 - 데이터 침해
 - 서비스 거부(DoS) 공격
- 타사 서비스 중단:
 - 클라우드 공급자 중단
 - DNS 실패
 - 외부 API 및 서비스 중단
- 환경적 요인:
 - 자연 재해(지진, 화재, 홍수, 정전)
 - 날씨 관련 문제

이는 특정 요구 사항과 조직에 맞게 조정할 수 있는 비결정적 예제 분류 프레임워크입니다. 시스템이 발전하거나 새로운 유형의 인시던트가 발생하면 분류 프레임워크를 정기적으로 검토하고 업데이트하는 것이 좋습니다.

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 [RSS 피드](#)를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2025년 1월 28일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 버전으로 마이그레이션합니다.
- 리플랫폼(리프트 앤드 리세이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예:에서 온프레미스 Oracle 데이터베이스를 Oracle용 Amazon Relational Database Service(RDS)로 마이그레이션합니다 AWS 클라우드.
- 재구매(드롭 앤드 슝) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예:의 EC2 인스턴스에서 온프레미스 Oracle 데이터베이스를 Oracle로 마이그레이션합니다 AWS 클라우드.
- 재배포(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중에 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

ABAC

[속성 기반 액세스 제어를](#) 참조하세요.

추상화된 서비스

[관리형 서비스를](#) 참조하세요.

ACID

[원자성, 일관성, 격리, 내구성](#)을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 더 유연하지만 [액티브-패시브 마이그레이션](#)보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 작동하고 그룹의 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로는 SUM 및 MAX가 있습니다.

AI

[인공 지능](#)을 참조하세요.

AIOps

[인공 지능 작업을](#) 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용할 수 있는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 [포트폴리오 검색 및 분석 프로세스](#)의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 [What is Artificial Intelligence?](#)를 참조하십시오.

인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 [운영 통합 가이드](#)를 참조하십시오.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서의 [용 ABAC AWS](#)를 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환 AWS 하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 [AWS CAF 웹 사이트](#)와 [AWS CAF 백서](#)를 참조하십시오.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 견적을 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

잘못된 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 [봇](#)입니다.

BCP

[비즈니스 연속성 계획](#)을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그인 시도, 의심스러운 API 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 [Data in a behavior graph](#)를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. [Endianness](#)도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, ‘이 제품은 책인가요, 자동차인가요?’ 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

별개의 동일한 두 환경을 생성하는 배포 전략입니다. 현재 애플리케이션 버전은 한 환경(파란색)에서 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 빠르게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 작업을 실행하고 인적 활동 또는 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 잘못된 봇이라고 하는 일부 다른 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 것입니다.

봇넷

[맬웨어](#)에 감염되어 [있고 봇](#) 셰이더 또는 봇 운영자라고 하는 단일 당사자가 제어하는 봇 네트워크입니다. Botnet은 봇과 봇의 영향을 확장하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 [About branches](#)(GitHub 설명서)를 참조하십시오.

브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는데 액세스할 수 있는 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 Well-Architected 지침의 [깨진 절차 구현](#) 표시기를 AWS 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 [그린필드](#) 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 [AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화](#) 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

C

CAF

[AWS 클라우드 채택 프레임워크](#)를 참조하세요.

canary 배포

최종 사용자에게 버전의 느린 증분 릴리스입니다. 확신이 드는 경우 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

[Cloud Center of Excellence](#)를 참조하세요.

CDC

[변경 데이터 캡처](#)를 참조하세요.

변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

카오스 엔지니어링

시스템의 복원력을 테스트하기 위해 의도적으로 장애 또는 중단 이벤트를 도입합니다. [AWS Fault Injection Service \(AWS FIS\)](#)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

[지속적 통합 및 지속적 전달](#)을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

클라이언트측 암호화

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 [CCoE 게시물](#)을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 [엣지 컴퓨팅](#) 기술과 연결됩니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 [클라우드 운영 모델 구축](#)을 참조하십시오.

클라우드 채택 단계

조직이 로 마이그레이션할 때 일반적으로 거치는 4단계 AWS 클라우드:

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 - 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 [The Journey Toward Cloud-First and the Stages of Adoption](#) on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 [마이그레이션 준비 가이드](#)를 참조하세요.

CMDB

[구성 관리 데이터베이스](#)를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리에는 GitHub 또는 Bitbucket Cloud. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 [AI](#) 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정 미준수가 될 수 있으며 일반적으로 점진적이고 의도하지 않습니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 검색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 [적합성 팩](#)을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 [지속적 전달의 이점](#)을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 [지속적 전달\(Continuous Delivery\)](#)과 [지속적인 개발](#)을 참조하십시오.

CV

[컴퓨터 비전을](#) 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework의 보안 원칙 구성 요소입니다. 자세한 내용은 [데이터 분류](#)를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 분산된 데이터 소유권을 제공하는 아키텍처 프레임 워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 [데이터 경계 구축을 참조하세요 AWS](#).

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 일반적으로 많은 양의 기록 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

[데이터베이스 정의 언어](#)를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 컨트롤을 AWS 추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations 호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 [AWS Organizations와 함께 사용할 수 있는 AWS 서비스](#)를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

[환경](#)을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 [Detective controls](#)를 참조하십시오.

개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

[스타 스키마](#)에서는 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트 필드 또는 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 일반적으로 쿼리 제약, 필터링 및 결과 집합 레이블 지정에 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

[재해](#)로 인한 가동 중지 시간과 데이터 손실을 최소화하는 데 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 [Disaster Recovery of Workloads on AWS: Recovery in the Cloud](#)를 참조하세요.

DML

[데이터베이스 조작 언어](#)를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 [컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET\(ASMX\) 웹 서비스를 점진적으로 현대화하는 방법](#)을 참조하십시오.

DR

[재해 복구](#)를 참조하세요.

드리프트 감지

기존 구성과의 편차 추적. 예를 들어 AWS CloudFormation 를 사용하여 [시스템 리소스의 드리프트를 감지](#)하거나 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 [랜딩 존의 변경 사항을 감지](#)할 수 있습니다.

DVSM

[개발 값 스트림 매핑](#)을 참조하세요.

E

EDA

[탐색 데이터 분석](#)을 참조하세요.

EDI

[전자 데이터 교환](#)을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 [클라우드 컴퓨팅](#)과 비교할 때 엣지 컴퓨팅은 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간의 비즈니스 문서 자동 교환. 자세한 내용은 [전자 데이터 교환이란 무엇입니까?](#)를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

[서비스 엔드포인트](#)를 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 [엔드포인트 서비스 생성](#)을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, [MES](#), 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 [봉투 암호화](#)를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마 이그레이션 전략의 에픽에 대한 자세한 내용은 [프로그램 구현 가이드](#)를 참조하십시오.

ERP

[엔터프라이즈 리소스 계획을](#) 참조하세요.

탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

F

팩트 테이블

[스타 스키마](#)의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블에 대한 외래 키가 포함된 열의 두 가지 유형이 포함됩니다.

빠른 실패

개발 수명 주기를 줄이기 위해 자주 중분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 중요한 부분입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 [AWS 장애 격리 경계를 참조하세요](#).

기능 브랜치

[브랜치를](#) 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그래디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 [기계 학습 모델 해석 가능성을 참조하세요 AWS](#).

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용

할 수 있습니다. 예를 들어, 날짜 ‘2021-05-27 00:15:37’을 ‘2021년’, ‘5월’, ‘목’, ‘15일’로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

몇 장의 샷 프롬프트

유사한 작업을 수행하도록 요청하기 전에 작업과 원하는 출력을 보여주는 몇 가지 예제를 [LLM](#)에 제공합니다. 이 기법은 컨텍스트 내 학습을 적용하여 모델이 프롬프트에 포함된 예제(샷)에서 학습합니다. 퓨샷 프롬프트는 특정 형식 지정, 추론 또는 도메인 지식이 필요한 작업에 효과적일 수 있습니다. [제로샷 프롬프트도 참조하세요.](#)

FGAC

[세분화된 액세스 제어를 참조하세요.](#)

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 [변경 데이터 캡처](#)를 통해 연속 데이터 복제를 사용하여 최대한 짧은 시간 내에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

[파운데이션 모델을 참조하세요.](#)

파운데이션 모델(FM)

일반화 및 레이블 지정되지 않은 데이터의 대규모 데이터 세트에 대해 훈련된 대규모 딥 러닝 신경망입니다. FMs은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 작업을 수행할 수 있습니다. 자세한 내용은 [파운데이션 모델이란 무엇입니까?](#)를 참조하세요.

G

생성형 AI

대량의 데이터에 대해 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트 및 오디오와 같은 새 콘텐츠 및 아티팩트를 생성할 수 있는 [AI](#) 모델의 하위 집합입니다. 자세한 내용은 [생성형 AI란 무엇입니까?](#)를 참조하세요.

지리적 차단

[지리적 제한을 참조하세요.](#)

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 [콘텐츠의 지리적 배포 제한](#)을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 [트렁크 기반 워크플로](#)는 현대적이고 선호하는 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조업에서는 골든 이미지를 사용하여 여러 디바이스에 소프트웨어를 프로비저닝할 수 있으며 디바이스 제조 작업의 속도, 확장성 및 생산성을 개선하는 데 도움이 됩니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 [브라운필드](#)라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

HA

[고가용성](#)을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스

키마를 변환하는 것은 복잡한 작업일 수 있습니다. AWS 는 스키마 변환에 도움이 되는 [AWS SCT를](#) [제공](#)합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

홀드아웃 데이터

[기계 학습](#) 모델을 훈련하는 데 사용되는 데이터 세트에서 보류된 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교하여 모델 성능을 평가할 수 있습니다.

동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫폼 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

정보

IaC

[코드형 인프라를 참조하세요.](#)

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

[산업용 사물 인터넷을 참조하십시오.](#)

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 적용 또는 수정하는 대신 프로덕션 워크로드를 위한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 [변경 가능한 인프라](#)보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 [변경 불가능한 인프라를 사용한 배포](#) 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. [AWS Security Reference Architecture](#)에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 참조하기 위해 2016년에 [Klaus Schwab](#)에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 [산업용 사물 인터넷\(IoT\) 디지털 트랜스포메이션 전략 구축](#)을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs. [AWS Security Reference Architecture](#)에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 [IoT란?](#)을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 [기계 학습 모델 해석 가능성을 참조하세요 AWS](#).

IoT

[사물 인터넷](#)을 참조하세요.

IT 정보 라이브러리(TIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

IT 서비스 관리(TSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 [운영 통합 가이드](#)를 참조하십시오.

ITIL

[IT 정보 라이브러리](#)를 참조하세요.

ITSM

[IT 서비스 관리](#)를 참조하세요.

L

레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 [안전하고 확장 가능한 다중 계정 AWS 환경 설정](#)을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터를 기반으로 사전 훈련된 딥 러닝 [AI](#) 모델입니다. LLM은 질문 답변, 문서 요약, 텍스트를 다른 언어로 변환, 문장 완성과 같은 여러 작업을 수행할 수 있습니다. 자세한 내용은 [LLMs](#) 참조하십시오.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

[레이블 기반 액세스 제어](#)를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 [최소 권한 적용](#)을 참조하십시오.

리프트 앤드 시프트

[7R](#)을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. [Endianness](#)도 참조하세요.

LLM

[대규모 언어 모델을](#) 참조하세요.

하위 환경

[환경을](#) 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공지능의 한 유형입니다. ML은 사물 인터넷 (IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 [기계 학습](#)을 참조하십시오.

기본 브랜치

[브랜치를](#) 참조하세요.

맬웨어

컴퓨터 보안 또는 개인 정보 보호를 손상하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 중단하거나, 민감한 정보를 유출하거나, 무단 액세스를 가져올 수 있습니다. 맬웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB는 관리형 서비스의 예입니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원재료를 작업 현장의 완성된 제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

[마이그레이션 가속화 프로그램을](#) 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 결과를 검사하여 조정하는 전체 프로세스입니다. 메커니즘은 작동 시 자체를 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 [메커니즘 구축](#)을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations 하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

[제조 실행 시스템](#)을 참조하세요.

메시지 대기열 원격 측정 전송(MQTT)

리소스가 제한된 [IoT](#) 디바이스에 대한 [게시/구독](#) 패턴을 기반으로 하는 경량 M2M(machine-to-machine) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 [AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요](#).

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로 서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 [에서 마이크로서비스 구현을 참조하세요 AWS](#).

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 [AWS 마이그레이션 전략](#)의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 [클라우드 마이그레이션 팩토리 가이드](#)와 [마이그레이션 팩토리에 대한 설명](#)을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

로 마이그레이션하기 위한 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다 AWS 클라우드. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. [MPA 도구](#)(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 실행 계획을 수립하는 프로세스입니다. 자세한 내용은 [마이그레이션 준비 가이드](#)를 참조하십시오. MRA는 [AWS 마이그레이션 전략](#)의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 로 마이그레이션하는 데 사용되는 접근 방식입니다 AWS 클라우드. 자세한 내용은 이 용어집의 [7R 항목](#)을 참조하고 [대규모 마이그레이션을 가속화하기 위해 조직 동원을 참조하세요](#).

ML

[기계 학습](#)을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 [의 애플리케이션 현대화 전략을 참조하세요 AWS 클라우드](#).

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 [의 애플리케이션에 대한 현대화 준비 상태 평가를 참조하세요 AWS 클라우드](#).

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 [마이크로서비스로 모놀리식 유형 분해](#)를 참조하십시오.

MPA

[마이그레이션 포트폴리오 평가](#)를 참조하세요.

MQTT

[메시지 대기열 원격 측정 전송](#)을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드를 위해 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework는 [변경 불가능한 인프라](#)를 모범 사례로 사용할 것을 권장합니다.

O

OAC

[오리진 액세스 제어를](#) 참조하세요.

OAI

[오리진 액세스 ID](#)를 참조하세요.

OCM

[조직 변경 관리](#)를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

[작업 통합](#)을 참조하세요.

OLA

[운영 수준 계약을](#) 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC-UA

[Open Process Communications - Unified Architecture](#)를 참조하세요.

Open Process Communications - 통합 아키텍처(OPC-UA)

산업 자동화를 위한 M2M(Machinemachine-to-machine) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 상호 운용성 표준을 제공합니다.

운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

운영 준비 상태 검토(ORR)

인시던트 및 가능한 장애의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 및 관련 모범 사례 체크리스트입니다. 자세한 내용은 AWS Well-Architected Framework의 [운영 준비 검토\(ORR\)](#)를 참조하세요.

운영 기술(OT)

물리적 환경과 함께 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조에서 OT 및 정보 기술(IT) 시스템의 통합은 [Industry 4.0](#) 혁신의 핵심 초점입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 [운영 통합 가이드](#)를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 [Creating a trail for an organization](#)을 참조하십시오.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 [사용 가이드](#)를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특

정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 [OAC](#)도 참조하십시오.

ORR

[운영 준비 상태 검토](#)를 참조하세요.

OT

[운영 기술](#)을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. [AWS Security Reference Architecture](#)에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

P

권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 [권한 경계](#)를 참조하십시오.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

PII

[개인 식별 정보](#)를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

[프로그래밍 가능한 로직 컨트롤러](#)를 참조하세요.

PLM

[제품 수명 주기 관리](#)를 참조하세요.

정책

권한을 정의하거나(자격 [증명 기반 정책](#) 참조), 액세스 조건을 지정하거나([리소스 기반 정책](#) 참조), 조직의 모든 계정에 대한 최대 권한을 정의할 수 있는 객체 AWS Organizations 입니다([서비스 제어 정책](#) 참조).

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 스토어를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다. 자세한 내용은 [마이크로서비스에서 데이터 지속성 활성화](#)를 참조하십시오.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 [마이그레이션 준비 상태 평가](#)를 참조하십시오.

조건자

false 일반적으로 WHERE 절에 있는 true 또는를 반환하는 쿼리 조건입니다.

조건자 푸시다운

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄어들고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 [Preventative controls](#)를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 있는 AWS 있는의 엔티티입니다. 이 엔티티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 [역할 용어 및 개념](#)의 보안 주체를 참조하십시오.

설계에 따른 개인 정보 보호

전체 개발 프로세스를 통해 개인 정보를 고려하는 시스템 엔지니어링 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 [프라이빗 호스팅 영역 작업](#)을 참조하십시오.

사전 예방적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 [보안 제어](#)입니다. 이러한 제어는 리소스가 프로비저닝되기 전에 리소스를 스캔합니다. 리소스가 컨트롤을 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 [제어 참조 가이드](#)를 참조하고 보안 [제어 구현의 사전](#) 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도, 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리.

프로덕션 환경

[환경](#)을 참조하세요.

프로그래밍 가능한 로직 컨트롤러(PLC)

제조 분야에서는 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체인

한 [LLM](#) 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 작업을 하위 작업으로 나누거나 예비 응답을 반복적으로 구체화하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

마이크로서비스 간의 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 [MES](#)에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 지침과 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

R

RACI 매트릭스

[책임, 책임, 상담, 정보 제공\(RACI\)을 참조하세요.](#)

RAG

[Retrieval Augmented Generation](#)을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

[책임, 책임, 상담, 정보 제공\(RACI\)을 참조하세요.](#)

RCAC

[행 및 열 액세스 제어를](#) 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의로드를 줄일 수 있습니다.

재설계

[7R을 참조하세요.](#)

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

[7R을 참조하세요.](#)

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전은 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 [계정에서 사용할 수 있는 지정을 참조 AWS 리전 하세요.](#)

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

[7R을 참조하세요.](#)

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

[7R을 참조하세요.](#)

리플랫폼

[7R을 참조하세요.](#)

재구매

[7R을 참조하세요.](#)

복원력

중단에 저항하거나 복구할 수 있는 애플리케이션의 기능입니다. 에서 복원력을 계획할 때 [고가용성](#) 및 [재해 복구](#)가 일반적인 고려 사항입니다 AWS 클라우드. 자세한 내용은 [AWS 클라우드 복원력을 참조하세요.](#)

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조연자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 Implementing security controls on AWS의 [Responsive controls](#)를 참조하십시오.

retain

[7R을 참조하세요.](#)

사용 중지

[7R을 참조하세요.](#)

검색 증강 세대(RAG)

응답을 생성하기 전에 [LLM](#)이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 [생성형 AI](#) 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대한 의미 검색을 수행할 수 있습니다. 자세한 내용은 [RAG란 무엇입니까?](#)를 참조하십시오.

교체

공격자가 보안 인증 정보에 액세스하는 것을 더 어렵게 만들기 위해 [보안 암호](#)를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적인 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

RPO

[복구 시점 목표를](#) 참조하세요.

RTO

[복구 시간 목표를](#) 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

S

SAML 2.0

많은 ID 제공업체(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 [SAML 2.0 기반 페더레이션 정보](#)를 참조하십시오.

SCADA

[감독 제어 및 데이터 획득](#)을 참조하세요.

SCP

[서비스 제어 정책](#)을 참조하세요.

secret

에는 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 AWS Secrets Manager 기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 [Secrets Manager 설명서의 Secrets Manager 보안 암호에 무엇이 있습니까?](#)를 참조하세요.

설계별 보안

전체 개발 프로세스에서 보안을 고려하는 시스템 엔지니어링 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어에는 [예방](#), [탐지](#), [대응](#) 및 [사전](#) 예방의 네 가지 주요 유형이 있습니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 [탐지](#) 또는 [대응](#) AWS 보안 제어 역할을 합니다. 자동 응답 작업의 예로는 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

데이터를 AWS 서비스 수신하는가 대상에서 데이터를 암호화합니다.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 [서비스 제어 정책](#)을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 [AWS 서비스 엔드포인트](#)를 참조하십시오.

서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 지표(SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정입니다.

서비스 수준 목표(SLO)

서비스 [수준 지표](#)로 측정되는 서비스의 상태를 나타내는 대상 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 담당하는 반면, 사용자는 클라우드의 보안을 담당합니다. 자세한 내용은 [공동 책임 모델](#)을 참조하십시오.

SIEM

[보안 정보 및 이벤트 관리 시스템](#)을 참조하세요.

단일 장애 지점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에서 장애가 발생한 경우.

SLA

[서비스 수준 계약을 참조하세요.](#)

SLI

[서비스 수준 표시기를 참조하세요.](#)

SLO

[서비스 수준 목표를 참조하세요.](#)

분할 앤 시드 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 [에서 애플리케이션 현대화에 대한 단계별 접근 방식을 참조하세요 AWS 클라우드.](#)

SPOF

[단일 장애 지점을 참조하세요.](#)

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 [데이터 웨어하우스](#) 또는 비즈니스 인텔리전스용으로 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도

하고 대체하는 것과 비슷합니다. [Martin Fowler](#)가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 [컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET\(ASMX\) 웹 서비스를 점진적으로 현대화하는 방법](#)을 참조하십시오.

서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 획득(SCADA)

제조에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 시스템을 테스트합니다. [Amazon CloudWatch Synthetics](#)를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

[LLM](#)에 컨텍스트, 지침 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다. 자세한 내용은 [AWS 리소스에 태그 지정](#)을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

[환경을](#) 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

전송 게이트웨이

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 [전송 게이트웨이란 무엇입니까?](#)를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 [다른 AWS 서비스와 AWS Organizations 함께 사용을](#) 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

피자 두 판이면 충분한 소규모 DevOps 팀. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 [Quantifying uncertainty in deep learning systems](#) 가이드를 참조하십시오.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

[환경](#)을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수행하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 [VPC 피어링이란?](#)을 참조하십시오.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에 대해 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대 위치를 기반으로 행 값에 액세스하는 등의 작업을 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

[쓰기를 한 번, 많이 읽기를 참조하세요.](#)

WQF

[AWS 워크로드 검증 프레임워크](#)를 참조하세요.

한 번 쓰기, 많이 읽기(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 데이터를 읽을 수 있지만 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 [변경할 수 없는](#) 것으로 간주됩니다.

Z

제로데이 익스플로잇

[제로데이 취약성](#)을 활용하는 공격, 일반적으로 맬웨어입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

제로샷 프롬프트

[LLM](#)에 작업 수행에 대한 지침을 제공하지만 작업에 도움이 될 수 있는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 작업을 처리해야 합니다. 제로샷 프롬프트의 효과는 작업의 복잡성과 프롬프트의 품질에 따라 달라집니다. [스크린샷이 거의 없는 프롬프트도 참조하세요.](#)

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.