



# 분석

Security Fundamentals

© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

보안 수명 주기 - 분석 을 시작하겠습니다.

# 교육 내용

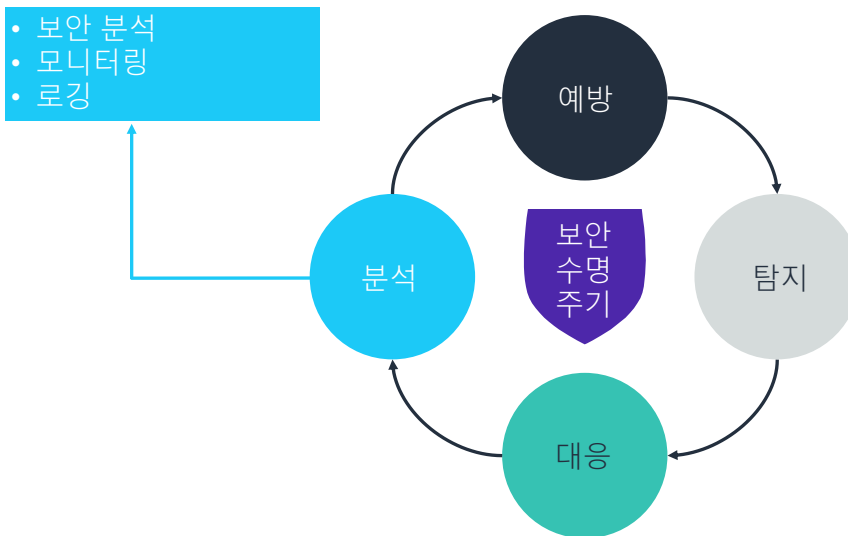
## 이 강의의 핵심

배울 내용은 다음과 같습니다.

- 취약성을 찾을 수 있도록 보안 분석을 위한 도구와 프로세스를 파악합니다.
- 보안 분석을 수행하는 방법에 대한 가이드라인을 나열합니다.
- 다양한 테스트, 모니터링, 로깅 유형이 보안 분석을 어떻게 지원하는지 설명합니다.



## 보안 수명 주기: 분석




3

aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- 예방 - 첫 번째 방어선입니다.
- 탐지 - 예방이 실패했을 때 수행됩니다.
- 대응 - 보안 위협을 탐지했을 때 취해야 할 조치를 설명합니다.
- 분석 - 향후에 인시던트가 다시 발생하지 않도록 예방하는 새로운 조치를 구현하면서 주기가 완료됩니다.

이 강의에서는 보안 수명 주기의 **분석** 단계를 배웁니다. 구체적으로, 보안 모니터링, 로깅, 분석을 수행하는 데 사용하는 도구와 기법을 알아볼 것입니다.



보안 분석

## 분석이란?

보안 침해 후 발생한 상황을 검토하는 작업

효과적인 분석을 위해  
질문해야 할 사항:

- 얼마나 많은 보안 침해를 겪었습니까?
- 발생 이유는 무엇입니까?
- 어떤 영향을 미쳤습니까?
- 이 문제가 다시 일어나지 않게 하려면 어떻게 해야 합니까?

분석은 보안 수명 주기의 마지막 단계입니다. 분석 단계에서는 보안 인시던트의 원인을 검토하고 현재의 보안 제어 조치를 분석하여 취약성을 판단합니다. 목표는 제어 조치를 개선하고 강화하여 네트워크와 시설, 조직을 더 강력하게 보호하는 것입니다.

분석 단계에서 해야 할 질문입니다.

- 얼마나 많은 보안 침해를 겪었습니까?
- 발생 이유는 무엇입니까?
- 데이터 침해가 우발적으로 일어났습니까?
- 얼마나 많은 사람이 영향을 받았습니까?
- 이 문제가 다시 일어나지 않게 하려면 어떻게 해야 합니까?

다음 주제에서는 분석 단계에서 이런 질문에 답하기 위해 활용할 수 있는 가이드라인과 기법을 설명합니다.

## 분석을 위한 일반적인 가이드라인

가장 중요한 부분을 가장 강력하게  
보호합니다.

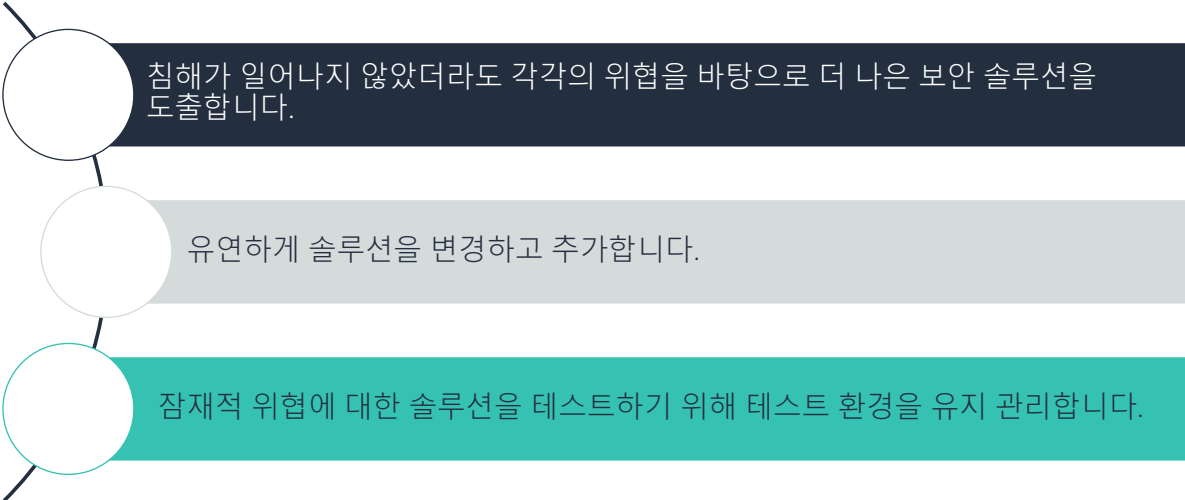
사용할 수 있는 가장 좋은 솔루션을  
구현합니다.

시뮬레이션 공격으로 솔루션의 균형을  
맞춥니다.

시뮬레이션의 결과를 평가한 후  
개선합니다.

분석의 주된 목표는 여러분의 환경에서 기존의 보안을 개선하고 강화하는 것입니다. 이 일반적인 가이드라인은 보안 분석 수행을 위한 것으로, 시뮬레이션 공격을 사용하여 테스트해야 한다는 내용도 있습니다.

## 분석을 위한 일반적인 가이드라인(계속)



침해가 일어나지 않았더라도 각각의 위협을 바탕으로 더 나은 보안 솔루션을 도출합니다.

유연하게 솔루션을 변경하고 추가합니다.

잠재적 위협에 대한 솔루션을 테스트하기 위해 테스트 환경을 유지 관리합니다.

공격을 시뮬레이션하기 위해 테스트할 때는 프로덕션 환경과 동일한 별도의 테스트 환경에서 진행하시기 바랍니다.

## 보안 테스트의 유형



외부 취약성 평가



외부 침투 테스트



애플리케이션과 플랫폼에 대한 내부 검토

분석 단계에서 보안 테스트를 수행하면 됩니다. 테스트 유형은 다음과 같습니다.

- **외부 취약성 평가** - 제3자가 인프라와 구성 요소에 관해 거의 알지 못하는 상태로 시스템 취약성을 평가합니다.
- **외부 침투 테스트** - 제3자가 시스템에 관해 거의 알지 못하는 상태에서 통제된 방식으로 시스템에 침입하려고 적극적으로 시도합니다.
- **애플리케이션과 플랫폼에 대한 내부 검토** - 시스템을 어느 정도 알거나 완전히 아는 테스터가 알려진 취약성에 있어 다음 항목의 효과를 검증합니다.
  - 구현된 제어 조치
  - 애플리케이션 및 플랫폼

AWS 고객은 AWS 클라우드에서 AWS 인프라를 대상으로 보안 평가 또는 침투 테스트를 수행해 보는 것이 좋습니다.



## 스마트한 솔루션 만들기

보안은 경계가 아니라 구조의 집합이어야 합니다.

티어가 있는 솔루션은 유연성과 구축의 잠재력이 더  
큽니다.

각기 다른 보안 솔루션을 티어로 정리합니다.

이전 강의에서 논의한 바와 같이 계층 또는 티어가 있는 보안 솔루션이 일반적으로 가장 효과가 좋습니다.

AWS Well-Architected Framework의 보안 핵심 요소는 스마트한 보안 솔루션을 만드는 청사진의 한 가지 예로, AWS 클라우드 내의 정보와 시스템을 보호하는 가이드와 모범 실무를 제공합니다.

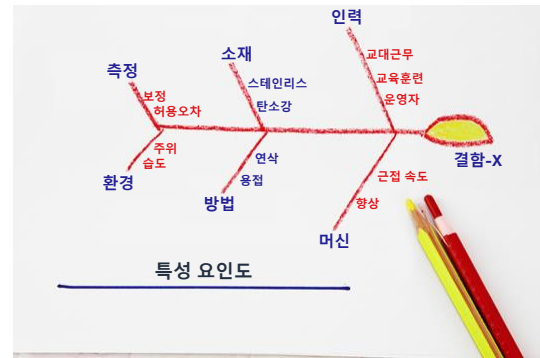
자세한 내용은 AWS Well-Architected Framework 가이드의 [보안 핵심 요소 - AWS Well-Architected Framework](#)를 참조하십시오.

## 근본 원인 분석(RCA)

보안 침해의 근본 원인을 찾는 데 사용됨

### RCA 수행 단계

1. 문제 및 문제와 관련된 이벤트를 정확하게 설명합니다.  
예: 어떻게 일어났는가?, 어디에서 일어났는가?
2. 이벤트를 순서대로 정리하여 이벤트 타임라인을 만듭니다.
3. 이벤트를 분석하여 연결 관계를 파악하고 문제를 유발했을 가능성이 가장 큰 이벤트를 파악합니다. 이것을 이벤트 상관관계라고 합니다.
4. 오리지년부터 최종 문제까지 이벤트의 순서를 시각적으로 표현합니다(다이아그램, 그래프 등).



근본 원인 분석(RCA)은 '침입이 발생한 이유는 무엇입니까?'라는 질문에 명확하고 정확한 답을 제공하는 데 사용되는 방법입니다.

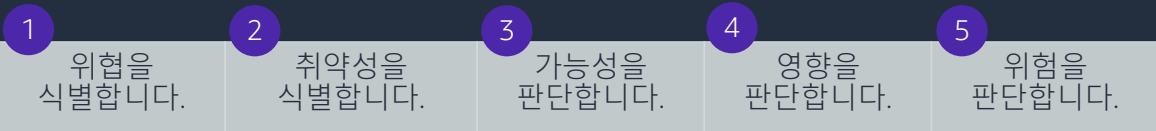
## 위험 평가

위험이란 특정 자산에 발생할 수 있는 위협의 가능성과 위협이 발생할 경우 해당 자산에 미칠 수 있는 영향입니다.

위험 평가를 통해 위험을 식별하고 순위를 매길 수 있습니다.



기본적인 5단계:



가장 강력하게 보호해야 하는 가장 중요한 자산 또는 가장 핵심적인 비즈니스 프로세스는 무엇입니까?

## 위험 대응 전략

### 위험 회피

- 위험을 유발하는 활동을 중단합니다.

### 위험 이전

- 위험에 대한 책임을 다른 주체에 할당합니다.

### 위험 완화

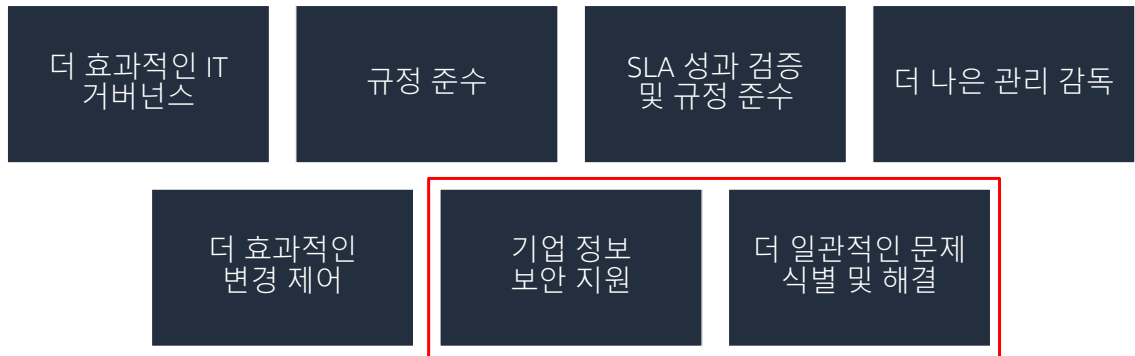
- 위험을 줄일 제어 조치를 구현합니다.

### 위험 수용

- 위험을 줄이기 위한 조치를 취하지 않고, 모니터링하고 대응을 계획합니다.

위험 평가의 결과에 따라 특정 자산 또는 활동에 어떤 보안 대응 전략을 사용할지 결정합니다.

## 모니터링 및 로깅의 이점



모니터링과 로깅은 보안 문제를 식별하고 해결하는 데 사용되는 데이터를 제공하기 때문에 보안 분석에도 도움이 되는 방법입니다.

모니터링 및 로깅의 이점:

- 모니터링과 로깅은 IT 거버넌스를 효과적으로 수행하는 방법을 제공할 수 있습니다.
- 모니터링과 로깅은 법률, 규정, 운영과 관련한 세부 사항을 준수하도록 하여 규정 준수를 보장하는 데 도움이 됩니다.
- 모니터링과 로깅은 SLA 성과 검증을 지원하고 규정 준수를 보장하는 데 도움이 됩니다.
- 모니터링과 로깅은 관리 감독과 제어에 기여할 수 있습니다.

## 모니터링과 로깅 비교

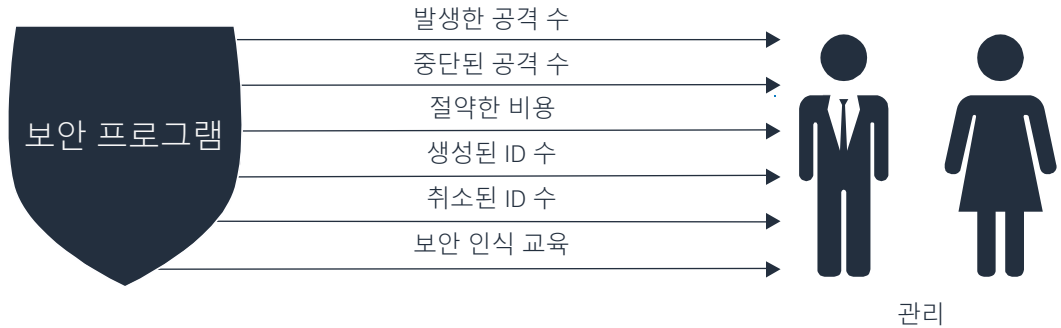
- 로그
  - IT 시스템 및 프로세스를 조사하는 데 필요한 데이터를 제공함
  - 모니터링의 입력일 수도, 출력일 수도 있음
- 로그 모니터링 대상
  - 변경
  - 예외
  - 기타 중대한 이벤트
- 모니터링에서 생성된 레코드는 추가 분석을 위한 로그로 사용됨

모니터링과 로깅은 서로를 보완합니다. 환경에서 모니터링되는 중대한 이벤트를 로그하는 것입니다.

다음 주제에서는 모니터링과 로깅을 더 자세히 살펴봅니다.

## 지표 사용

- 지표는 보안 프로그램의 성과를 측정합니다.
- 보안 프로그램의 지표는 양수일 수도, 음수일 수도 있습니다.



지표를 사용하여 보안 솔루션의 성공을 평가하고 보여줍니다.



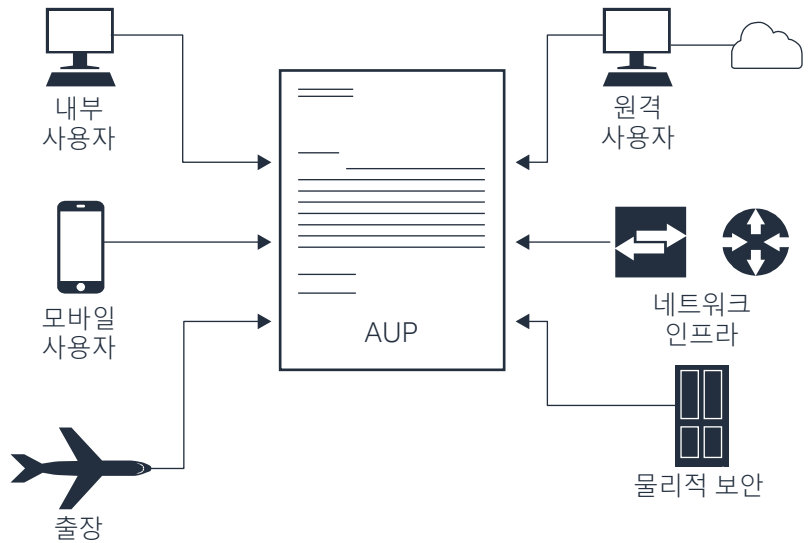
환경 모니터링



## 모니터링

- 기업의 이용 목적 제한 정책 (AUP)에서는 직원 또는 사용자가 다음과 같은 회사의 네트워크에서 모니터링되는 방식을 정의합니다.

- 회사
- 원격
- 모바일 디바이스



기업에서는 이용 목적 제한 정책(AUP) 문서를 만들어 모니터링되는 사람이나 항목을 결정하는 규칙을 정의할 수 있습니다.

## 모니터링의 유형

### 위치

- 현장
- 원격
- 내부 또는 외부
- 아웃소싱

### 리소스

- 시스템
- 네트워크
- 데이터베이스
- 물리적
- 직원

### 사용 현황

- 사용 또는 소비 현황
- 위치
- 이 정보에 액세스할 수 있는 사람

모니터링의 유형은 어디에서 모니터링하는지, 어떤 유형의 리소스나 사용 현황이 모니터링되는지에 따라 달라질 수 있습니다.

## 서비스형 모니터링(MaaS)

- 클라우드 기반 인프라 모니터링
- 인프라 전체가 클라우드에 배포됨
- 언제, 어디서나 정보 모니터링 가능



Amazon CloudWatch

예를 들면, AWS 클라우드에서 Amazon CloudWatch 서비스는 AWS 클라우드 리소스와 AWS에서 실행되는 애플리케이션에 대한 모니터링 서비스를 제공합니다. CloudWatch Logs를 사용하면 로그를 모니터링하고 저장할 수 있어 시스템 및 애플리케이션을 이해하고 운영하는 데 도움이 됩니다.

서비스형 모니터링(MaaS)의 이점은 이런 유형의 서비스가 실시간 애플리케이션 및 시스템 모니터링을 제공할 수 있다는 점입니다. 예를 들어 CloudWatch Logs는 애플리케이션 로그에서 발생하는 오류의 수를 추적하고 오류 비율이 사용자가 지정한 임계값을 초과할 때마다 알림을 발송할 수 있습니다.

## 모니터링될 수 있는 디바이스

라우터	스위치	방화벽	무선 액세스 포인트(AP)
프린터	가상 프라이빗 네트워크(VPN) 접선기	카메라	카드 리더
랩톱	전화	태블릿	차량

네트워크에 연결할 수 있는 디바이스라면 거의 대부분의 디바이스를 모니터링할 수 있습니다.

## 모니터링 정책

모니터링 정책을 수립할 때 질문해야 할 사항:

- 무엇을 모니터링해야 합니까?
- 얼마나 엄밀히 모니터링해야 합니까?
- 얼마나 자주 모니터링해야 합니까?
- 누가 모니터링합니까?
- 모니터링을 아웃소싱합니까?
  - 모니터링 데이터 보존
  - 모니터링 도구 액세스
  - 원격 모니터링
- 모니터링 담당자를 누가 감독합니까?
  - 정책
  - 규정

모니터링 정책을 만들 때는 이런 요소를 고려하시기 바랍니다.

## 모니터링 보존 정책

보존 정책에는 다양한 데이터 유형을 보존하는 기간이 명시됩니다.



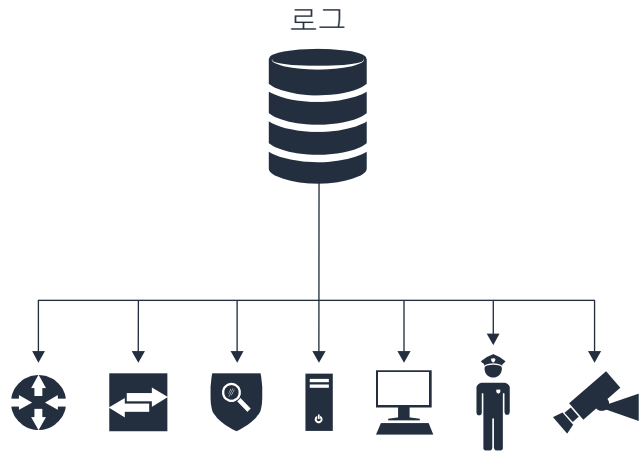
모니터링 정책에는 각기 다른 데이터를 얼마나 오래 보존할지도 명시해야 합니다.



로깅

## 로깅 정책

- 로깅의 대상과 로그 관리 방법이 명시된 로깅 정책을 정의합니다.
- 로깅 정책**과 **인프라** 지원이 서로 긴밀히 연결되고 통합된 기업 솔루션이어야 합니다.



기업의 어떤 리소스와 활동을 로깅해야 하는지 파악합니다. 로깅 정책에 이 정보를 포함합니다. 또한 로그를 관리할 방법도 정의합니다.



## 로그 정보 보호

- 로그를 원래 디바이스, 로그 서버 또는 둘 다에 보관합니다.
- 다음과 같이 로그 서버에 대한 물리적 및 논리적 액세스를 제어합니다.
- 로그 백업 또는 복구 프로세스
- 보존 정책
- 타임스탬프

무단 액세스로부터 로그 정보를 보호하고 정기적으로 로그를 백업하는 것이 중요합니다. 분석 결과가 정확하려면 모든 로그 서버의 시계를 정확히 맞추고 동기화해야 합니다.

## 핵심 사항



© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

26

- 보안 분석의 목적은 보안 제어 조치를 강화하여 네트워크와 시설, 조직을 더 강력하게 보호하는 것입니다.
- 테스트, 모니터링, 로깅은 보안 분석을 뒷받침하는 핵심적인 활동입니다.
- 모니터링 정책은 모니터링을 수행하는 대상, 담당자, 시점, 방식에 관한 세부 정보를 정의합니다.
- 로깅 정책에는 로깅 대상, 로그 관리 방식이 명시됩니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 보안 분석의 목적은 보안 제어 조치를 강화하여 네트워크와 시설, 조직을 더 강력하게 보호하는 것입니다.
- 테스트, 모니터링, 로깅은 보안 분석을 뒷받침하는 핵심적인 활동입니다.
- 모니터링 정책은 모니터링을 수행하는 대상, 담당자, 시점, 방식에 관한 세부 정보를 정의합니다.
- 로깅 정책에는 로깅 대상, 로그 관리 방식이 명시됩니다.