프로젝트 결과 보고서

목 차

[1. 프로젝트 개요 3](#_Toc74493519)

[1.1 프로젝트 명 및 기간 3](#_Toc74493520)

[1.2 프로젝트 목표 3](#_Toc74493521)

[1.3 프로젝트 범위 4](#_Toc74493522)

[2 프로젝트 조직 5](#_Toc74493523)

[2.1 프로젝트 책임 및 역할 5](#_Toc74493524)

[2.2 프로젝트 환경 6](#_Toc74493525)

[2.3 프로젝트 산출물 8](#_Toc74493526)

[3 보고 및 검토 방안 9](#_Toc74493527)

[3.1 보고 및 검토 계획 9](#_Toc74493528)

[4 프로젝트 관리 11](#_Toc74493529)

[4.1 형상관리 11](#_Toc74493530)

[4.1.1 형상관리 대상 11](#_Toc74493531)

[4.1.2 버전관리 표준 11](#_Toc74493532)

[4.1.3 Base-Line 등록 시점 11](#_Toc74493533)

[4.1.4 형상 라이브러리 11](#_Toc74493542)

[4.2 위험관리 12](#_Toc74493543)

[4.3 의사소통관리 13](#_Toc74493544)

# 프로젝트 개요

## 프로젝트 명 및 기간

* 프로젝트명 : 클라우드 SIEM 서비스
* 프로젝트 기간 : 2021.04.17 ~ 2021.06.14.
* 프로젝트 인원 : 김한진, 공경선, 금소영, 김동관, 김범, 서용석, 최병섭

## 프로젝트 목표

* AWS 환경에서 서비스 운영을 Azure 환경에서는 이벤트 탐지 및 모니터링을 할 수 있도록 구축한다.
* AWS 인프라 서비스에서 개발을 위한 개발환경 및 테스트 환경과 서버 배포 시스템을 구축한다.
* AWS 환경에서의 사용자 활동과 네트워크 활동 log&event를 수집하여 Azure Sentinel 에서 모니터링 한다.
* AWS CloudWatch의 log&event로 보고서를 생성하여 S3에 저장한다.
* 생성된 보고서를 관리자에게 메일을 전송하는 기능을 자동화한다

## 프로젝트 범위

|  |  |  |
| --- | --- | --- |
| **구분** | **구현 범위** | **비고** |
| 클라우드 환경 구축 | AWS WAF, AWS Network FireWall 구축 | - |
| AWS EC2, AutoScaling, Route53 | Web Server 구축 |
| AWS 클라우드와 Azure 클라우드 연동 | -  - |
| 로그 수집 및 저장 | Cloud Watch, Cloud Trail,CloudWatch Agent 적용 | - |
| 자동화를 위한 Lambda 코드 구축 | - |
| AWS S3에 log 저장 | - |
| 이벤트 탐지 | Azure Sentinel 구축 | - |
| AWS WAF와 Network Firewall ruleset 설정 | - |
| 로그 보고서 작성 | - |
| 이벤트 대응 | 악의적 공격 차단 | - |
| IP 탐지 및 차단 | - |
| 비정상 지역 접근 차단 | - |
| AWS SNS알림 서비스 | - |

**[표1-1] 프로젝트 범위**

# 프로젝트 조직

## 프로젝트 책임 및 역할

|  |  |  |
| --- | --- | --- |
| **책임** | **역할** | **담당자명** |
| 아키텍처 설계 / 인프라 | 프로젝트 총괄, 의사 결정 | 김한진 |
| 아키텍처 설계, 인프라 구축(AWS) |
| 인프라 | 인프라 구축(Azure Sentinel) | 공경선 |
| 인프라 | 인프라 구축(Azure Sentinel) | 서용석 |
| 개발 | 로그 보고서 작성 파이썬 개발 | 김동관 |
| 개발 | 로그 보고서 작성 파이썬 개발 | 김범 |
| 개발 | 로그 보고서 작성 파이썬 개발 | 금소영 |
| 개발 | 인프라 구축(AWS) | 최병섭 |

[**표2-1] 책임 및 역할**

## 프로젝트 환경

|  |  |  |
| --- | --- | --- |
| **서비스명** | **수량** | **용도** |
| Amazon EC2 | 3 | 1. 프로젝트용 테스트 서버를 생성한다. 2. WEB 서버, WAS 서버, 보고서 생성 서버를 사용한다 3. 사용 증가 시 Auto Scaling 으로 서버 자동 증설한다 4. CloudWatch Agent 설치 후 log들을 CloudWatch로 전송한다 |
| Amazon Simple Storage Service(S3) | 1 | 1. Lambda와 AWS CLI로 자동화하여 로그 등을 백업한다. 2. 로그 보고서 저장 한다. |
| Elastic Load Balancing | 2 | 1. WEB 서버의 부하 분산 2. WAS 서버의 부하 분산 |
| AWS Web Application Firewall(WAF) | 1 | 1. 웹 애플리케이션의 보안 탐지 및 차단 한다. |
| AWS CloudTrail | 1 | 1. AWS 계정의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 서비스 2. AWS 인프라의 작업과 관련된 계정 활동을 로깅하고 연속적으로 모니터링 한다.. |
| AWS Systems Manager | 1 | 1. AWS의 인프라에 대한 가시성과 제어 기능을 제공한다. 2. 여러 AWS 서비스의 운영 데이터를 볼 수 있음 3. AWS 리소스 전체에서 운영 작업을 자동화할 수 있음. |
| Amazon Virtual Private Cloud(VPC) | 1 | 1. Aws 클라우드의 논리적으로 격리된 섹션을 프로비저닝하여 정의한 가상 네트워크를 통해 그 섹션에서 AWS 리소스를 실행한다. |
| AWS NAT | 1 | 1. 외부망과 사설망 내부를 이어준다. 2. 보안상으로 보면 프로토콜을 숨겨줄 수 있다. |
| Amazon SNS | 1 | 1. 애플리케이션 간 및 애플리케이션과 사용자 간 통신 모두를 위한 완전관리형 메시지 서비스 |
| Amazon Lambda | 1 | 1. 주기적으로 CloudWatch에 있는 로그들을 S3에 년/월/일 별로 저장한다. 2. Amazon SNS와 연동하여 로그 보고서를 S3에 저장 시 관리자 메일 계정으로 알람 메일을 보낸다. |
| AWS | 1 | 1. 회사에서 AWS 내부 시스템에 접근할 때 사용한다. |
| Azure log Analytics | 4 | 1. log Analytics는 Azure Monitor Logs에서 수집된 데이터에서 로그 쿼리를 편집 및 실행하고 그 결과를 대화형으로 분석하는 Azure Portal의 도구 |
| Azure logic apps | 4 | 1. 앱, 데이터, 서비스 및 시스템을 통합하는 자동화된 워크플로를 만들고 실행할 수 있는 클라우드 기반 플랫폼 서비스 |
| Azure Sentinel | 1 | 1. 클라우드 네이티브 SIEM 및 인텔리전트 보안 분석을 적용하여 엔터프라이즈 보호 서비스 |

[표2-2] 사용서비스

## 프로젝트 산출물

|  |  |  |
| --- | --- | --- |
| **단계** | **작업** | **산출물** |
| 프로젝트 계획 | 프로젝트 범위 확정  프로젝트 일정 확정  프로젝트 진행 방향 확정 | 프로젝트 수행 계획서  클라우드 사용계획서 |
| 분석/설계 | 요구사항 분석 / 정의 / 관리  아키텍처 설계  기능 설계 | 요구사항 명세서  아키텍처 설계서 |
| 인프라 구축 및 개발 | 프로그램 설계  업무프로세스 설계  코드 설계  기능 구현 | 프로젝트 ACL  Source Code 정의서 |
| 테스트 및 이행 | 통합테스트 및 미비점 보완  시스템 운영 시 인계 및 필요사항 정의 | 통합 테스트 시나리오 및 결과서  시스템운영 요청서 |
| 완료 | 매뉴얼 작성  프로젝트 완료 | 구성 매뉴얼  프로젝트 완료 보고서 |

**[표2-3] 프로젝트 산출물**

## 보고 및 검토 방안

## 보고 및 검토 계획

* 보고방안

|  |  |  |  |
| --- | --- | --- | --- |
| **보고사항** | **주기/형식** | **주요 보고 및 검토사항** | **보고자** |
| 착수보고 | 2021.04.24(토)  /프로젝트계획서 | -프로젝트 기획 및 주제 선정  -프로젝트의 목표, 수행방안 및 개발 계획  -프로젝트 수행 조직 및 인력투입 계획 | PM |
| 주간보고 | 매주 토요일  /주간 보고서 | -주간 프로젝트 진척 현황  -문제해결 처리 기록  -변경요청 처리 기록 | PM |
| 이슈보고 | 문제, 장애 발생시  /보고서 | -장애 발생 및 기타 문제 사항 발생 보고  -조치계획 및 조치 결과 보고 | PM,  담당PL |
| 중간보고 | 2021.22.(토)  /중간보고서 | -분석/설계 진척 현황 중간 점검  -본 사업 진행 이슈 파악 및 처리 보고  -향후 사업 진행 내용 및 일정 보고 | PM,  발표자 |
| 완료보고 | 2021.06.14(월)  /완료보고서 | -본 사업 요구사항 요약  -본 사업 진행 경과 / 실행 사항  -단계별 계획 대비 실적 분석 | PM |
| 회의록 | 회의록 | -회의 중 협의된 사항에 대한 확인 문서 | 회의진행자 |

[**표3-1] 보고 방안**

* 검토일정

|  |  |  |
| --- | --- | --- |
| **검토 종류** | **차수** | **일정** |
| 산출물 검토 | 1차 | 2021년 4월 24일 ~ 2021년 5월 21일 |
| 2차 | 2021년 5월 24일 ~ 2021년 6월 13일 |
| 클라우드 환경 산출물 검토 | 1차 | 각 단계 완료 후 |
| 2차 | 2021년 5월 24일 ~ 2021년 6월 13일 |

**[표3-2] 산출물 검토 일정**

# 프로젝트 관리

## 형상관리

### 형상관리 대상

* + 형상관리 절차 주요 내용
* 변경 사항 발생 (개발자)
* 형상변경 요청 (github 또는 주간보고 issue사항으로 요청)
* 변경 여부 결정 (반려 시 절차 종료)
* 변경
* 검토 및 테스트 (테스트는 개발 부분 해당)
* 버전 관리

### 버전관리 표준

* 검수 이전의 문서 버전은 1.0으로 시작하여 변경 시 0.1 증가
  + Base-Line 등록 시 2.0버전을 부여하며, 변경 시 0.1씩 증가

### Base-Line 등록 시점

- 문서 산출물: 각 단계 마일스톤 완료 후 또는 문서 생성 즉시

- 프로그램 소스코드: 2021년 5월 11일 (개발자 투입 및 구현단계 시작 이후)



### 형상 라이브러리

* 문서 산출물: GitHub

<https://github.com/gkswls321/SKinfosec>

* 프로그램 소스코드: GitHub

<https://github.com/gkswls321/SKinfosec>

텍스트이(가) 표시된 사진

자동 생성된 설명

**[그림4-1] Github 사용 화면**

## 위험관리

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **단계** | **위험** | **발생가능성** | **영향도** | **대응 방안** |
| 프로젝트 계획 | 일정 계획 오류 | 중 | 중 | WBS관리를 통하여 일정에 대한 꾸준한 모니터링 실시 |
| 분석/설계 | 요구사항 및  분석 오류 | 중 | 중 | 고객과의 지속적인 소통을 통하여 명확한 요구사항을 도출 |
| 구현 | 일정 지연 | 중 | 하 | 팀원들과의 정보공유 및 진척사항 관리, 업무 효율성 및 부하 관리  각 개인의 피로도 파악 대처 |
| 통합테스트/이행 | 테스트 시나리오 오류 | 하 | 중 | 테스트 시나리오 검증 및 오류 발견시 시나리오 재작성 |
| 링크실패/성능 저하 | 중 | 중 | 단위 및 통합테스트 강화 |
| 기타 위험요소 | 산출물 오류 | 중 | 중 | 각 단계별 산출물 검토 및 오류 발견시 즉시 정정 |
| 비즈니스 지식의 부족 | 하 | 중 | 현업과의 상호작용을 증가시키고, 적절한 지식전수 |

**[표4-1] 위험관리 구분**

## 의사소통관리

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **보고체** | **보고자** | **보고 주기** | **보고방법** | **산출물** | **보고 대상** |
| 아키텍처팀 | PM | 매주 토요일 오전 9시30분 | 주간회의 | 주간보고서 | 멘토 |
| 인프라팀 | 인프라 매니저 | 매주 토요일 오전 10시 | 주간회의 | 주간보고서 | 멘토 |
| 개발팀 | 보안매니저 | 매주 토요일 오전 10시 30분 | 주간회의 | 주간보고서 | 멘토 |
| Project committee | 회의록 담당자 | 매일 오후 5시 30분 | 일간회의 | Project Committee 회의록 | PM |

**[표4-1] 회의 구분**

기타 내용 : 첨부파일