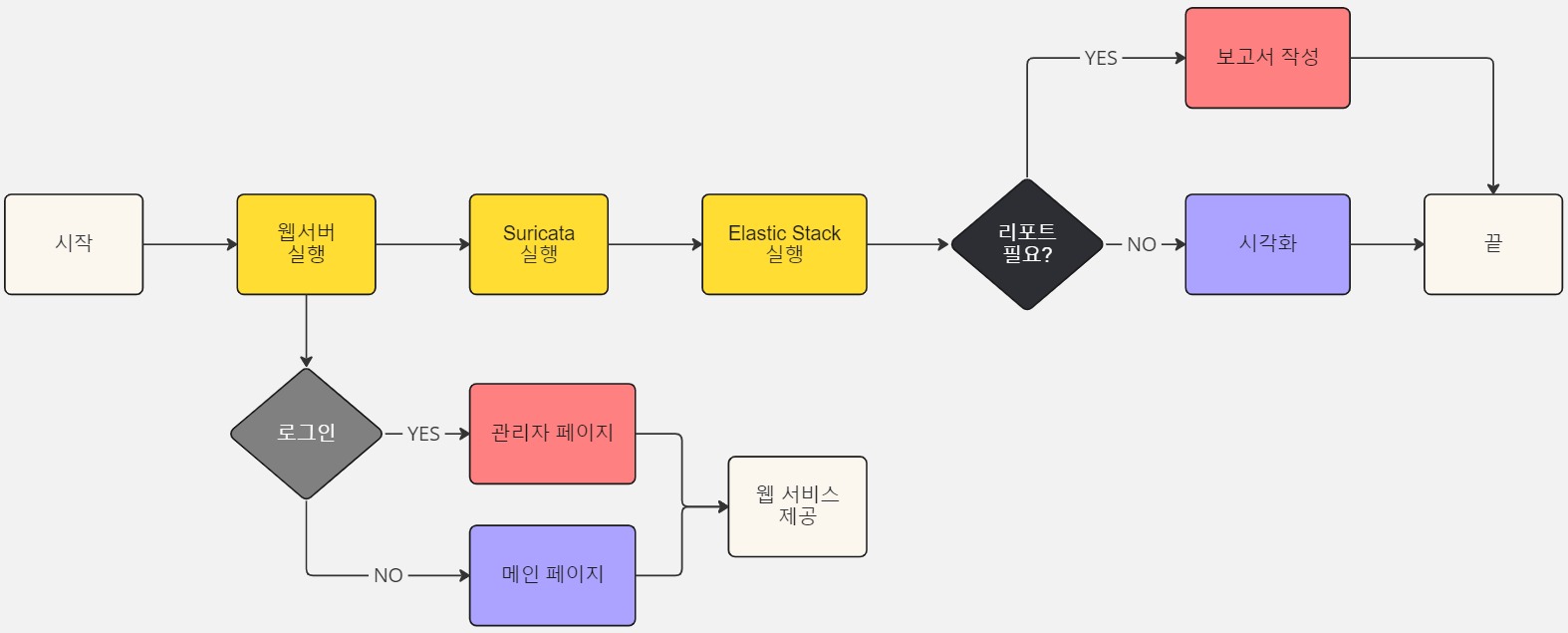
1. Flow Chart



2. 요구사항 명세서 (기능적/비 기능적)

A. 기능적

|  |  |  |  |
| --- | --- | --- | --- |
| **요구사항번호** | 기능-001 | **요구사항 명** | **Suricata 운영** |
| **요구사항설명** | 1. 방화벽 뒤에 Suricata를 설치하고 운영한다.  2. Suricata를 통해 네트워크 로그를 수집한다.  3. Rule을 설정하고 IDS 모드를 실행하여 관련 이벤트 로그를 수집한다. | | |
| **관련요구사항** | Suricata의 IDS 모드를 활용하여 침입 탐지를 우선한다. | | |
| **전제 조건** | 방화벽이 운영중이어야 한다. | **우선순위** | 2 |

|  |  |  |  |
| --- | --- | --- | --- |
| **요구사항번호** | 기능-002 | **요구사항 명** | **Elastic Stack 운영** |
| **요구사항설명** | 1. Suricata와 연동하여 Elastic Stack을 설치하고 운영한다.  2. 수집된 로그 데이터를 Elastic Stack을 활용하여 시각화한다.  3. Elastic Stack을 활용하여 필요한 데이터를 검색하고 분석한다. | | |
| **관련요구사항** | Nginx와 연동하여 웹서버에 Elastic Stack를 구현한다. | | |
| **전제 조건** | 웹서버가 운영중이어야 한다. | **우선순위** | 1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **요구사항번호** | 기능-003 | **요구사항 명** | **Report 작성** |
| **요구사항설명** | 1. Elastic Stack을 활용하여 로그 관련 리포트를 작성한다.  2. 필요한 사항이 포함된 리포트 작성을 자동화 한다.  3. 웹페이지에 요약된 리포트 형식을 구현한다.  4. Elastic Stack의 시각화 데이터를 활용하여 리포트 작성에 추가한다. | | |
| **관련요구사항** | Elastic Stack을 활용한 지속적인 관제를 운영한다. | | |
| **전제 조건** | Elastic Stack 서비스를 제공받고 있다. | **우선순위** | 1 |

B. 비기능적

|  |  |  |  |
| --- | --- | --- | --- |
| **요구사항번호** | 비기능-001 | **요구사항 명** | **작동 환경** |
| **요구사항설명** | 1. Django WAS를 통하여 웹서버를 운영한다.  3. 로그 빅데이터 관제에 Elastic Stack을 이용한다.  2. 해당 플랫폼은 네이버 클라우드 Ubuntu 22.04 64bit에서 작동한다.  4. 해당 플랫폼은 Python 기반으로 하여 개발한다. | | |
| **관련요구사항** |  | | |
| **전제 조건** |  | **우선순위** |  |

3. WBS (work breakdown structure)

|  |  |
| --- | --- |
| **케이스 ID : report-001 웹서버 운영** | |
| **사전조건** | 사용자가 운영중인 웹서비스에 접속한다. |
| 시나리오 | |
| **[주요 이벤트 경로]**  1. 사용자가 제공 중인 웹서비스에 접근한다.  2. 사용자가 원하는 뉴스 기사를 클릭한다.  3. 상세 페이지로 이동하여 관련 기사의 자세한 내용을 제공한다.  4. 사용자가 원하는 뉴스 기사를 검색한다.  5. 검색 결과 페이지로 이동하여 관련 검색 내용을 표시한다.  6. 사용자가 원하는 내용을 클릭하면 관련 상세 페이지로 이동한다.  **[대안 또는 예외 경로]**  1. 로그인을 시도할 경우에 로그인 페이지로 이동한다.  2. DB에 저장된 관리자 계정과 비교하여 로그인 성공/실패 여부를 제공한다. | |
| 사후조건 | 주기적인 업데이트를 통하여 사용자에게 새로운 기사를 제공한다.  검색을 통한 오래된 기사 검색 기능도 제공한다. |

|  |  |
| --- | --- |
| **케이스 ID : report-002 웹서버 로그인** | |
| **사전조건** | 사용자가 운영중인 웹서비스에 로그인을 시도한다. |
| 시나리오 | |
| **[주요 이벤트 경로]**  1. 사용자가 제공 중인 웹서비스 메인 페이지에서 로그인을 클릭한다.  2. 로그인 페이지로 이동한다.  3. 로그인 ID와 Password를 입력하고 로그인을 시도한다.  4. DB에 저장된 관리자 계정과 비교하여 로그인 성공/실패 여부를 제공한다.  A. 로그인 성공 시 관리자 메뉴가 제공되는 메인 페이지로 접속한다.  B. 로그인 실패 시 다음과 같은 메시지를 알려주고 사용자 메인 페이지로 이동한다.  i. 알림 메시지 : “관리자 계정을 입력하세요.”  **[대안 또는 예외 경로]**  1. 메인 페이지에서만 관리자 로그인 접속을 활성화 한다.  2. 차후 제공 예정인 서비스 등을 위하여 사용자 로그인/로그아웃 기능을 구현한다. | |
| 사후조건 | 관리자 메뉴를 통하여 뉴스 기사 올리기, 수정, 삭제가 가능하도록 한다.  관리자 메뉴를 통하여 웹서버 로그 데이터 확인과 리포트 작성이 가능하도록 연결한다. |

|  |  |
| --- | --- |
| **케이스 ID : report-003 Suricata 설치 및 운영** | |
| **사전조건** | 관리자가 Suricata를 실행한다. |
| 시나리오 | |
| **[주요 이벤트 경로]**  1. 웹서버에 Suricata를 설치한다.  2. Suricata의 기본 Rule을 Update 한다.  3. Suricata에 필요한 Custom Rules을 적용한다.  4. Suricata를 IDS 모드로 운영한다.  5. Suricata의 최근 로그를 지속적으로 모니터링 한다.  6. Suricata의 전체 로그 데이터를 수집, 분석한다.  **[대안 또는 예외 경로]**  1. 침입 방지가 필요할 경우 IPS 모드로 Suricata를 운영한다.  2. | |
| 사후조건 | 지속적인 Log 모니터링을 위하여 항상 Suricata 운영을 유지한다.  주기적으로 빅데이터 Log 파일을 DB화 한다. |

|  |  |
| --- | --- |
| **케이스 ID : report-004 Elastic Stack 설치 및 운영** | |
| **사전조건** | 관리자가 Elastic Stack을 실행한다. |
| 시나리오 | |
| **[주요 이벤트 경로]**  1. 웹서버에 순서대로 Elasticsearch, Kibana, Logstash, Filebeat를 설치한다.  2. Filebeat 와 Suricata를 연동한다.  3. Elastic Stack에 설정한 ID/Password로 접속한다.  4. filebeat filter를 선택한다.  5. 실시간으로 Suricata가 수집한 Log 시각화 데이터를 확인한다.  6. Elastic을 활용하여 Log 데이터를 검색, 분석한다.  **[대안 또는 예외 경로]**  1. Kibana 기능을 nginx와 연동하여 접속 가능하게 한다.  2. Elastic Stack이 사용하는 Port들을 관리한다. | |
| 사후조건 | 리포트 작성을 위하여 대시보드 시각화 및 관련 통계 데이터를 공유받는다.  중요한 이벤트 Log는 DB화하여 Elasticsearch를 활용한다. |

|  |  |
| --- | --- |
| **케이스 ID : report-005 웹서버 로그 시각화** | |
| **사전조건** | 관리자가 Elastic Stack을 운영한다. |
| 시나리오 | |
| **[주요 이벤트 경로]**  1. Elastic Stack에 로그인하여 접속한다.  2. Filebeat로 받아온 Suricata Log 데이터를 확인한다.  3. 설정한 시각화 필드를 통해 Log 데이터를 분석, 시각화 한다.  **[대안 또는 예외 경로]**  1. 로그인한 관리자에 한하여 분석한 Log 데이터와 시각화 내용을 제공한다.  2. 필요한 필드를 반영하여 시각화 내용을 구성한다. | |
| 사후조건 | Suricata와 연동하여 관련 Log 데이터를 항상 모니터링 한다.  리포트 작성을 위하여 필요한 시각화 필드와 관련 내용을 공유한다. |

|  |  |
| --- | --- |
| **케이스 ID : report-006 로그 데이터 자동 리포트** | |
| **사전조건** | 관리자가 Elastic Stack을 활용하여 보고서를 작성한다. |
| 시나리오 | |
| **[주요 이벤트 경로]**  1. 관리자가 Elastic Stack에 접속한다.  2. 실시간 수집되고 있는 Log 데이터를 확인하고 리포트 작성을 실행한다.  3. 웹페이지를 통해 자동으로 작성된 보고서 내용을 확인한다.  4. pdf 형식으로 저장을 원하는 경우 ‘리포트 저장’을 클릭한다.  5. 필요한 데이터가 포함된 다양한 보고서를 작성한다.  **[대안 또는 예외 경로]**  1. 로그인한 관리자 정보를 보고서 작성 시 포함한다.  2. Elastic Stack에서 수집, 분석된 구체적인 데이터도 제공 가능하다. | |
| 사후조건 | 필요한 리포트 작성을 위하여 지속적으로 Elastic Stack을 운영한다.  작성된 리포트 자료를 DB화하여 관리한다. |