Project Proposal

1. 과제명 : Trinity(SIEM using ELK Stack)

2. 과제 목표 및 필요성 : Elastic Stack 을 활용한 중앙 집중식 로깅 시스템 구축 및 대응 서비스 제공

과거부터 현재까지 전 산업분야에 걸쳐 자동화 및 디지털화가 진행되고 있습니다. 이에 따른 개인정보의 보안, 더 나아가 조직 내/외부, 사회 전체에 영향을 미칠 수 있는 침해사고에 대한 대처가 필요합니다. 중요 산업에 대한 사이버 공격, 취약점등에 의한 정보 탈취등의 문제가 발생한다면 개인적인 침해 문제를 넘어 범세계적인 문제가 발생할 수 있습니다. 따라서 사이버 보안에 대한 기술의 요구도는 시간이 지남에 따라 더욱 요구될 것이고 조직에서의 중요성이 커질 것입니다.
조직 내/외부의 사고 요인을 철저하게 인지, 배제, 제거하는 것이 사이버 보안의 그리고 현 프로젝트의 기반입니다. 완전한 취약점과 위협을 제거하는 것은 사실상 불가합니다. 하지만 불가하다는 판단하에 하지 않으면 심각한 침해 사고가 발생 시 대처를 할 수 없으며 조직 운영을 복구하기 까지 상당히 큰 비용이 들어갈 것입니다. 이에 개인 및 조직 내/외부의 위험 요소를 적절하게 판단하고 인지하며 위험 허용 임계 수준을 설정하고, 어떤 위협이 발생했을 때 적절한 대처를 취할 수 있도록 해야합니다. 또한 사고 발생 후 복구 계획을 수립하여 서비스 제공의 연속성을 유지하고 신뢰성을 높이며 조직의 가치를 최대화할 수 있습니다.

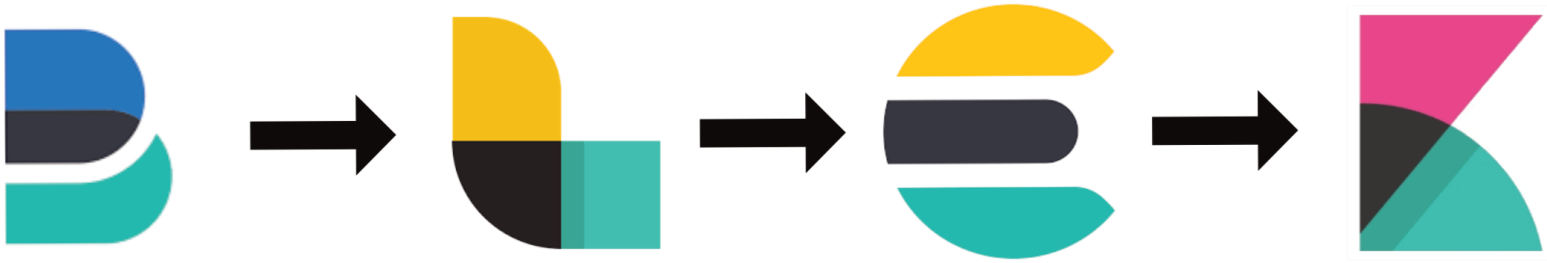
3. 과제 내용 및 적용 기술 :

Elasticsearch, Logstash, Kibana(이하 Elastic Stack)을 사용하여 호스트, 네트워크 로그 기록을 중앙 집중화시스템을 구축하여 의심 징후들을 선제적, 후속 조치를 위한 서비스를 제공합니다.

1. beats, logstash 를 사용하여 클라이언트의 로그를 수집 및 가공, 정제합니다.
2. 전처리된 로그들을 중앙 서버에 전송하여 관리합니다.
3. 중앙 서버에 설치된 엘라스틱 서치를 사용하여 해당 로그를 분석하여 침입, 위협 징후를 파악합니다.
4. 파악된 징후들을 바탕으로 해당 서비스, 연결을 격리, 차단, 복구를 진행합니다.

5. 모니터링 호스트에서 키바나의 데이터 시각화를 통해 서버의 서비스 품질 확인 및 로그 분석 수행합니다.
6. 클라이언트는 실시간 침입 탐지 정보를 웹 서비스를 통해 확인합니다.

SIEM System
Beats, Logstash, Elasticsearch, Kibana 를 사용하여 구성합니다.



Beats - 로그 수집
Logstash - 로그 수집 및 분류, 가공, 정제
Elasticsearch - 제공되는 HTTP RESTful API를 통한 로그 저장, 분석
Kibana - 로그 시각화를 통한 가시성 및 직관적인 분석 가능

Elasticsearch는 Apache Lucene 기반의 검색엔진입니다. HTTP 웹 인터페이스와 JSON 형식으로 비정형 데이터를 인덱스에 저장하고 도큐먼트, 도큐먼트 내 필드 내용에 대한 필터링, 정렬, 통계 등을 통해 분석할 수 있습니다.
Kibana는 Elasticsearch에 저장한 인덱스들을 분석하여 데이터를 시각화하고 UI내 기능을 통해 Elastic Stack의 구성과 관리를 쉽게 할 수 있습니다.

Web Service
AWS, Spring Boot, Maria DB 를 통해 웹서비스를 제공합니다.

4. 과제 결과물 활용 방안 :

ELK Stack을 활용하여 다양하고 대용량의 로그들을 수집, 정제 및 분석하여 나온 데이터를 시각화하여 침해대응을 위한 효율성을 높이고 향후 내/외부 위협에 대한 사전 차단, 사후 대응 및 복구를 통한 조직 내 네트워크 보안성의 향상을 기대할 수 있습니다. SIEM 서비스 제공을 통해 클라이언트에서 발생하는 로그들을 전수 수집하여 분석함으로써 대용량의 로그 분석을 자동화 및 침해 징후 사전, 중도, 사후 파악을 위해 사용할 수 있습니다.
Splunk, IBM의 Qradar 와 같은 기존 시스템은 고비용, 주도적 기술 구현이 어려움에 있습니다. 하지만 Free and Open model을 라이센스를 사용하는 Elastic Stack 을 이용함으로써 비교적 저비용과 최적화된 서비스를 이용할 수 있으며, 필요성을 느끼는 부분에 대한 추가적인 기능을 조직 내 자체적으로 구현하여 Elastic Stack과 연결할 수 있습니다.
로그는 다양하며 현재에는 눈으로만 분석할 수 없는 대용량이라는 특징을 가지고 있습니다. 따라서 빅데이터 분석 기술을 활용하여 사이버 위협에 대한 사전 인지, 차단, 복구를 가능함으로 보안관제에 있어서 신속한 대응을 할 수 있습니다. 또한 백신만으로는 시그니쳐 기반 탐지에 한계가 있으므로 이상 행위 분석을 통해 보완할 수 있습니다.
클라이언트의 정상 서비스에 대한 비정상 위협이 발생할 경우 연관 분석을 통한 사전 징후 발견으로 침해 사고 대응 서비스를 제공할 것입니다.

통계

일정

기간	내용
1주-2주	주제선정 및 과제추진계획서 작성
3주-4주	1차 ELK Stack 기본 파이프라인 및 백엔드 구성
5주-6주	2차 ELK Stack 기본 파이프라인 및 백엔드 구성 및 프론트엔드 대시보드 구현
7주-8주	테스트 로그 수집 및 가공, 분석. 벡엔드 구성, 프론트엔드 대시보드 구현
9주-10주	중간 점검. 2차 로그 분석, 벡엔드 구성, 프론트엔드 구현.
11주-12주	침입 테스트 및 연관 분석을 통한 로그 분석 시각화.
13주-14주	시스템 마지막 테스트 및 점검.