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.
유사 서비스, Splunk, Elastic security.

4. 과제 결과물 활용 방안 :

통계