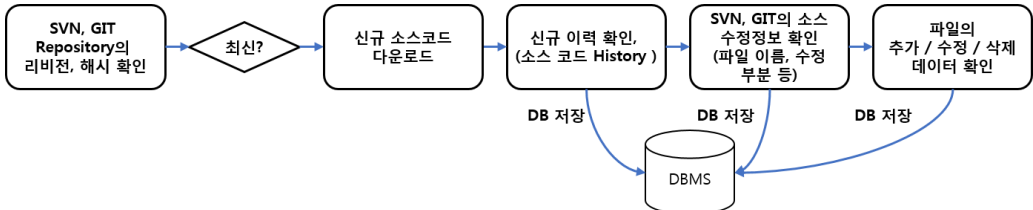
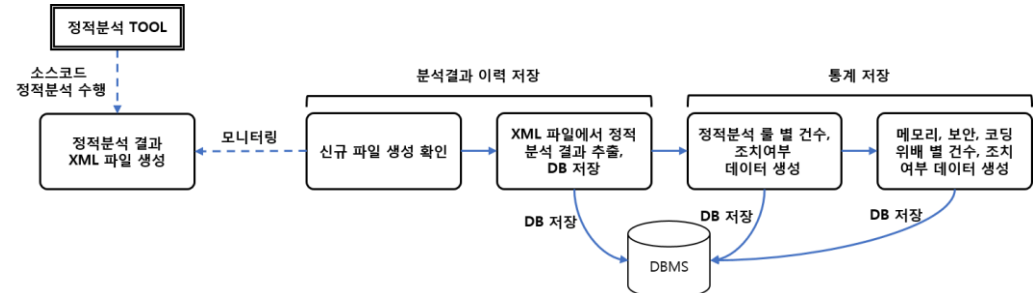


# 경 력 기 술 서

성명 : 김인수

| 직 장 명<br>/ 근무기간 | 근무부서명<br>/ 직책/직급                 | <ol style="list-style-type: none"> <li>회사소개 (근무 당시 인원수)</li> <li>담당업무 및 업무 실적 (수행 프로젝트 위주)</li> <li>퇴사 사유</li> </ol>  |
|-----------------|----------------------------------|---|
| 모비젠             | BDS연구소<br>ES연구1팀 /<br>팀원 /<br>선임 | <ol style="list-style-type: none"> <li>회사소개<br/>빅데이터 SI개발 회사 / 직원수 - 약 140명 / 매출액 - 약 190억</li> <li>담당업무, 프로젝트<br/>◎ 주요 업무 <ul style="list-style-type: none"> <li>SI 프로젝트 개발 (Java 프로세스 개발, 시스템 테스트, 화면설계/DB 스키마 설계 참여)</li> <li>서버에서 실행되는 Back-end 프로세스 개발</li> <li>제안서, 중간보고서, 완료보고서 등 문서 산출물 작업 참여</li> </ul> </li> </ol> <p><b>프로젝트 명 : 한국전력연구원 내부자보안 - Kepco Insider Threat Detection and Indicator</b></p> <p>○기간 : 2017.02 ~ 진행 중</p> <p>○프로젝트 성격 : 고객사 시스템 개발(SI, 연구과제)</p> <p>○개발 환경 및 개발 언어 : Linux / Java / MariaDB / Git</p> <p>○프로젝트 소개</p> <ul style="list-style-type: none"> <li>전력연구원 내부 시스템의 소스코드를 임의로 수정하여 발생할 수 있는 불법행위를 방지하기 위하여 SVN, Git와 같은 버전관리시스템과 정적분석 툴의 데이터를 수집, 분석하여 전력연구원 내부 시스템의 소스의 변경을 추적, 확인하는 연구과제</li> </ul> <p>○담당업무</p> <ul style="list-style-type: none"> <li>SVN, Git 저장소의 소스코드 저장 이력 수집하여 알맞은 형식으로 가공하여 DB 저장<br/>SVNKit, JGit 라이브러리 사용</li> <li>저장 정보 : SVN REVISION, GIT HASH, 커밋 날짜, Author, 디렉토리 경로, 파일 이름, 확장자, 추가/수정/삭제/대체, 메시지(코멘트), 파일 크기</li> </ul>  <pre> graph LR     A[SVN, GIT Repository의 리비전, 해시 확인] --&gt; B{최신?}     B --&gt; C[신규 소스코드 다운로드]     C --&gt; D[신규 이력 확인, 소스 코드 History]     D -- DB 저장 --&gt; E[(DBMS)]     E -- DB 저장 --&gt; F[SVN, GIT의 소스 수정정보 확인 파일 이름, 수정 부분 등]     F -- DB 저장 --&gt; G[파일의 추가 / 수정 / 삭제 데이터 확인]     </pre> <ul style="list-style-type: none"> <li>소스코드의 정적분석 결과 수집하여 알맞은 형식으로 가공하여 DB 저장<br/>빌드 결과로 생성된 XML 파일을 읽어 데이터 수집.</li> <li>저장 정보 : 프로젝트 빌드 번호, 입력시간, 메시지, 체크된 코드의 라인 수, 모듈 이름, 패키지 이름, 파일 이름, 카테고리, 타입, 출처, 탐지/조치 여부</li> </ul>  <pre> graph LR     A[정적분석 TOOL] -- 소스코드 정적분석 수행 --&gt; B[정적분석 결과 XML 파일 생성]     B -- 모니터링 --&gt; C[신규 파일 생성 확인]     C -- 분석결과와 이력 저장 --&gt; D[XML 파일에서 정적 분석 결과 추출, DB 저장]     D -- DB 저장 --&gt; E[(DBMS)]     E -- DB 저장 --&gt; F[정적분석 물 별 건수, 조치여부 데이터 생성]     F -- DB 저장 --&gt; G[메모리, 보안, 코딩 위해 별 건수, 조치 여부 데이터 생성]     </pre> <ul style="list-style-type: none"> <li>실시간으로 시스템에서 사용하는 method, 기능을 확인하기 위하여 사용한 method, 기능의 로그 생성기능 추가, 생성한 로그를 DB에 저장</li> <li>웹UI에서 확인, 차트 사용하는 추가 데이터 생성하여 DB 테이블에 저장</li> <li>DB 테이블 설계, 구성<br/>논리, 물리 스키마 구성<br/>테이블 생성, 저장/조회 쿼리 작성, 테스트</li> </ul> <p>○성과</p> <ol style="list-style-type: none"> <li>SVN, GIT의 파일 수정 이력 수집하여 프로젝트의 이력 추적 기능 제공</li> </ol> |

2) 정적분석 결과를 수집, 분석하여 프로젝트 소스코드의 버전 별 취약점 확인, 취약점 탐지 정보와 조치 여부의 통계와 추적 기능 제공

**프로젝트 명 : SK텔레콤 3D N/W Visualization Mgmt. Platform 분석서버 구축 및 Streaming App. 개발 (SKT 3DVS)**

○기간 : 2016.5 ~ 2016.12

○프로젝트 성격 : 고객사 시스템 개발(SI, 연구과제)

○개발 환경 및 개발 언어 : Linux / Java / Apache Kafka / Spark Streaming / MariaDB / Git

○프로젝트 소개

- SNMP, Monasca, N/W flow, IDS 이벤트 데이터 등을 Apache Kafka로 수집 후 Spark streaming을 사용하여 배치 분석 후 N/W flow 관계, 각 종류별 TOP N 데이터를 생성하여 결과를 GUI 서버로 전송하는 프로젝트

○담당업무

- 데이터 수집 : Apache Kafka 사용

SNMP, N/W flow, Monasca, IDS 이벤트 등의 데이터 수집 기능 개발

SNMP, Monasca, IDS 이벤트, Switch, Link 구성정보 등 : JSON 문자열로 수집

N/W flow : 5초 마다 50만건의 데이터를 binary(byte 배열)로 수집

각 데이터 종류별로 별도의 Topic 사용하여 수신. (수집처에서 별도의 Kafka 사용하는 경우 있음)

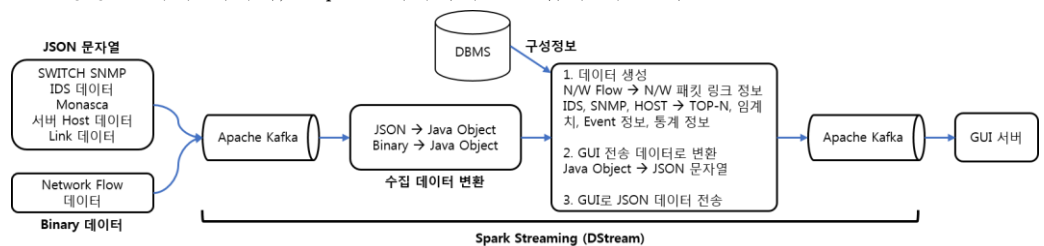
분석 결과, 통계 데이터의 GUI 서버 전송 기능 개발

- 수집 데이터 분석 : Spark streaming 사용

수집한 데이터의 파싱, 분석, 통계 생성 기능 개발(수집한 JSON, binary 데이터의 Java object 변환)

수집한 데이터를 구성정보와 비교하여 패킷의 링크정보 생성

생성된 이력 데이터, Top-N 데이터의 DB 입력 기능 개발



- 수집-생성 데이터 검증, 성능 테스트

○성과

- 1) 수집 데이터의 실시간 처리/저장/전송
- 2) 5초 내 50만 건 데이터 처리(연구 과제에서 서버 2대로 클러스터 구성)
- 3) 수집, 가공 데이터의 검증을 통한 데이터 무결성 보장

**프로젝트 명 : KISA 사이버 위협정보 수집검증 및 종합 정보공유 기능 개발 (C-TAS, CShare)**

○기간 : 2015.09 ~ 2016.01

○프로젝트 성격 : 고객사 시스템 고도화(SI)

○개발 환경 및 개발 언어 : Linux / Java / Spring framework / Tibero / Git

○프로젝트 소개

- 기존 C-TAS, CShare 시스템 수집되는 위협정보의 정제/보완/검증 작업을 통하여 더욱 개선된 위협정보를 제공하고 기존 시스템을 고도화 하는 프로젝트

○담당업무

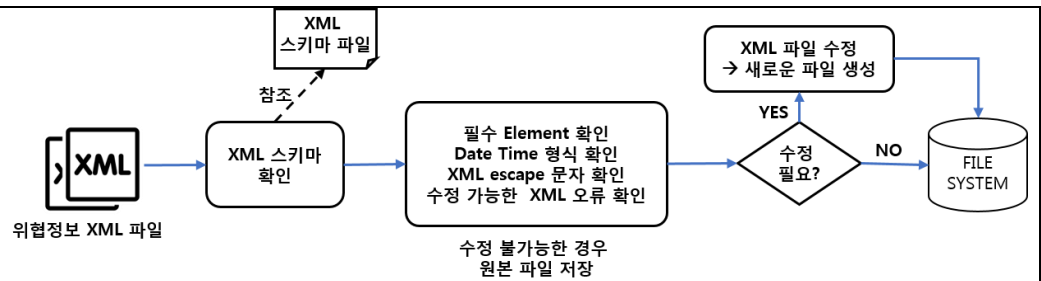
- 외부 수집 데이터(XML)의 정해진 규격에 따른 정제, 보완 기능 개발

수집 대상인 위협정보를 XML 형식의 파일로 수집.

- 위협정보 정제 기능

수집된 위협정보 XML 데이터의 오류 수정 기능으로 오류 수정이 가능한 것만 처리.

주로 발생하는 오류 위주의 수정(날짜, 시간 Format 통일, XML Escape 처리, 필수 element 확인)

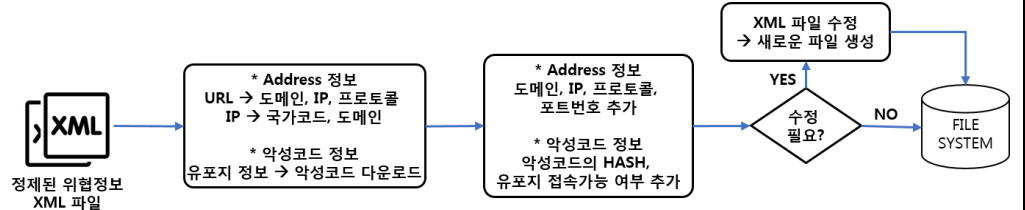


#### - 위협정보 보완 기능

정제된 위협정보 XML 데이터 사용하여 추가 정보 보완.

URL 사용한 추가 데이터 : 프로토콜, 도메인, IP, IP의 국가코드

악성코드 유포지 URL : 악성코드 다운로드 가능 여부, 악성코드의 MD5 해시 추출



#### - CShare 사이트 속도개선 작업 (유지보수 프로젝트와 함께 진행)

개선 대상 메뉴와 기능 확인, 해당 쿼리 추출하여 사례에 따라 처리.

이력 데이터 테이블 사용하여 속도가 느린 경우 : 통계 데이터 테이블 사용으로 변경.

테이블에 파티션이 없는 경우 : 데이터 크기에 맞게 테이블 파티션 사용.

인덱스를 사용하지 않는 경우 : 대부분 order by 절. 인덱스 생성이 부담되어 고객과의 협의 후 쿼리에서 order by 절 삭제.

서브 쿼리가 문제인 경우 : 서브 쿼리에서 너무 많은 데이터를 조회하지 않도록 수정, hint 사용.

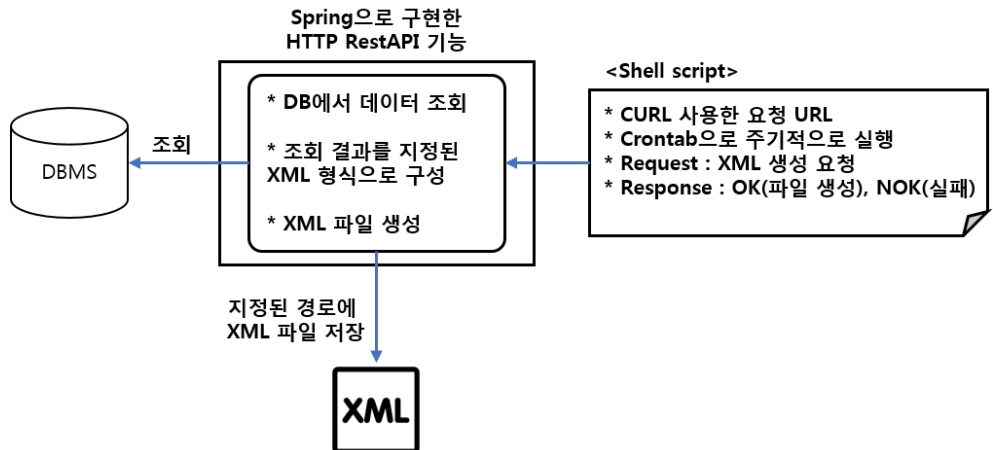
수정된 쿼리 테스트, 수정된 쿼리 적용

#### - 회원 이력, 관리자 이력 관련 테이블 및 기능 설계/정리

#### - KISA 시연용 UI 프로그램에 C-TAS 시스템의 실제 데이터 연동

어도비 AIR로 만들어진 시연 프로그램이 실제 데이터로 만들어진 XML 파일 제공

HTTP RestAPI 기능으로 상용 DB에 저장된 데이터를 조회하여 XML 파일 생성



#### ○성과

- 1) CShare 웹사이트(<https://cshare.krcert.or.kr:8443/>) 조회속도 개선
- 2) 수집된 위협정보의 정제, 보완 단계 추가로 위협정보의 오류발생 감소
- 3) 정보가 추가, 보완된 위협정보의 공유 제공으로 공유되는 위협정보의 품질 향상
- 4) KISA 시연 UI 프로그램용 실제 데이터 제공

**프로젝트 명 : KISA 사이버 위협정보 분석 공유 시스템 보안 및 운영 관리 (C-TAS 운영)**

○기간 : 2015.06 ~ 2015.12

○프로젝트 성격 : 고객사 시스템 유지보수(SM)

○개발, 운영 환경 및 개발 언어 : Linux / Java / Spring framework / Tibero

○담당업무

- DB 조회 쿼리 분석 및 속도 저하부분 분석

- DB 조회 속도 개선 위한 DB 스키마, 쿼리 수정 (테이블 파티셔닝 적용, 이력 데이터의 통계화, 쿼리 수정 등)
- C-TAS, CShare 사이트 메뉴별로 자동으로 접속하여 메뉴 별 조회속도를 자동 측정하는 프로세스 개발
- 시스템 OS 패치(OpenSSL 등) 시 서버, 프로세스 모니터링과 재기동
- 전반적인 시스템 운영업무 (서버 상태 확인 및 시스템 유지관리)

#### ○성과

- 1) 하루 2 차례 시스템 점검 후 메일 발송 적용으로 시스템의 점검과 보고의 자동화
- 2) C-TAS, CShare 사이트의 조회 속도 개선
- 3) C-TAS, CShare 웹UI의 조회속도 확인 자동화
- 4) 시스템OS, 보안의 최신상태 유지/관리

#### 프로젝트 명 : KISA 사이버위협 및 침해사고 정보 종합분석공유 시스템 고도화 (C-TAS, CShare)

○기간 : 2014.10 ~ 2015.03

○프로젝트 성격 : 고객사 시스템 고도화(SI)

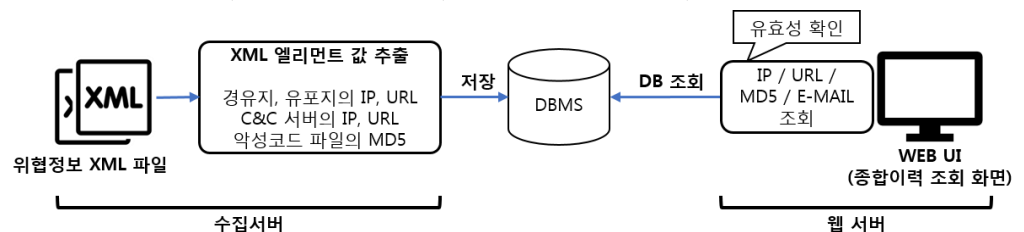
○개발 환경 및 개발 언어 : Linux / Java / Tiberio / Git

○프로젝트 소개

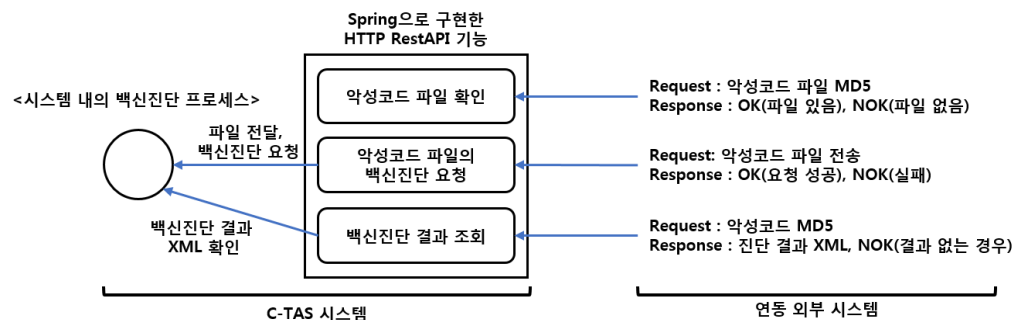
- C-TAS, CShare 시스템의 기능 보완과 추가를 통한 시스템 고도화 프로젝트

○담당 업무

- 수집 위협 정보의 종합이력 기능 개발  
수집된 위협정보에서 미리 지정된 elements 추출. 종류별 테이블에 저장.  
DB 테이블 설계, 대상 정보의 분류, 저장/조회 부분 설계, 개발.



- 정보공유 모듈(ExportAPI)의 HTTPS 통신 기능 적용 (Java key store 동적생성)
- 악성코드 백신 분석 데이터 연동위한 HTTP REST API 기능 개발  
백신분석 대상 악성코드의 파일 업로드, 백신분석의 결과 제공 API



- CShare 웹 사이트의 정보공유의 수집/제공 통계 생성 쿼리 등 작업, 통계 생성 모듈 개발
- DB 테이블 튜닝으로 인한 웹 속도 개선 작업 (이력 데이터의 통계화, 테이블의 파티셔닝 적용 등)

#### ○성과

- 1) 위협정보 공유 시 HTTPS 적용으로 보안기능 향상.
- 2) 통계 생성으로 다양한 정보공유 상태, 현황 정보 제공

#### 프로젝트 명 : SKT Mobile Botnet Sinkhole (MBS)

○기간 : 2014.04~2014.09

○프로젝트 성격 : 고객사 신규 구축(SI)

○개발 환경 및 개발 언어 : Linux / Java / Spring framework / Quagga / MariaDB / SVN

○프로젝트 소개

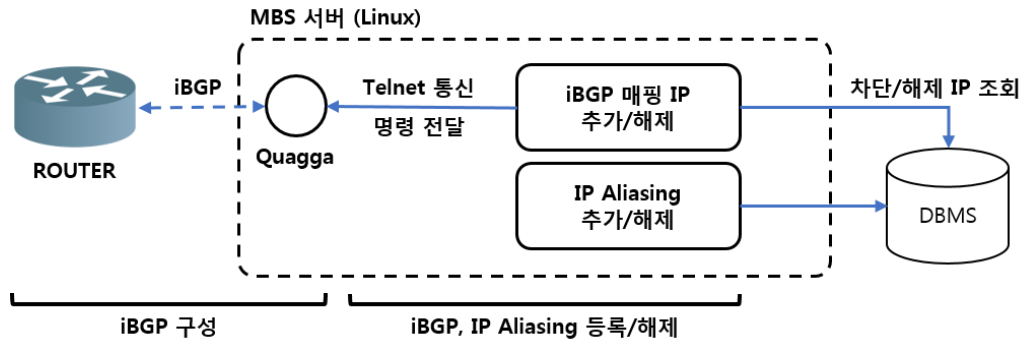
- iBGP, IP aliasing을 사용하여 리눅스 서버를 악성코드 C&C 서버로 위장하여 악성코드에 감염된 스마트폰에서 전송한 패킷을 리눅스 서버로 수신하여 망부하 감소, 가입자 보호를 위한 프로젝트

○담당 업무

- iBGP/IP Aliasing 설정, 차단 프로세스 개발

Quagga 라우터로 패킷 수신을 위한 iBGP 명령 전달, IP 주소 aliasing 모듈 개발(iBGP 설정/해제, IP aliasing 설정 해제 기능)

Quagga 사용한 리눅스 서버에서의 iBGP 라우팅 구성



- DB 저장, 통계 기능 개발

수집한 패킷 로그 데이터 저장하는 DB 로더 모듈 개발 (5초 단위 데이터 저장)

C&C 서버 IP, 차단 패턴에 따른 통계 생성 모듈 개발 (Hourly, Daily 통계)

이메일 통한 일일보고 생성 및 발송 모듈 개발 (일별 차단 IP, 차단 건수의 일일 보고서 발송)

○성과

- 1) 악성코드에 감염된 스마트폰에서 C&C 서버로의 통신 차단
- 2) C&C 서버로의 악성코드 통신 차단으로 가입자보호
- 3) C&C 통계/차단 통계 제공
- 4) 매일 아침 일일보고서 형식으로 차단 통계제공

**프로젝트 명 : KISA 사이버위협 및 침해사고 정보 종합분석공유 시스템 (C-TAS, CShare)**

○기간 : 2013.09 ~ 2014.03

○프로젝트 성격 : 고객사 신규 구축(SI)

○개발 환경 및 개발 언어 : Linux / Java / Hadoop / Tibero / Git

○프로젝트 소개

- 수집, 공유된 위협정보, 악성코드를 분석하여 프로파일링 된 위협정보를 생성하여 KISA 내 분석가 회원사에게 공유하는 시스템 개발 프로젝트

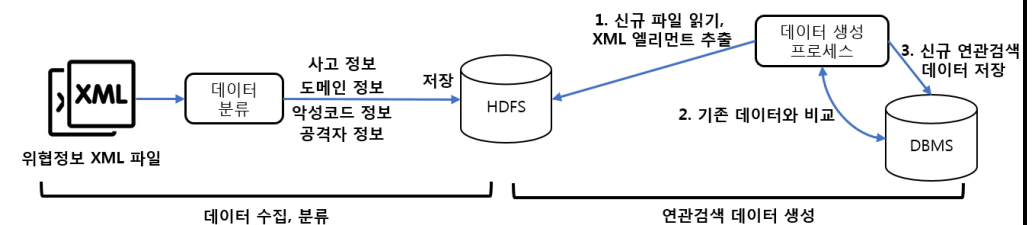
○담당 업무

- 악성코드의 행위분석

Fireeye 장비로의 행위분석 요청 모듈 개발(FTP 통한 malware 파일 다운로드, 행위분석 요청)

행위분석 결과 조회 및 저장 기능 개발(Java 기반의 Https 통신 통한 분석 결과 조회, 다운로드)

- 프로파일링 된 악성코드 위협정보 간의 연관검색 모듈 개발 (XML 파일 간의 연관성 조회)



○성과

- 1) 악성코드의 행위분석 결과 제공
- 2) 연관검색 메뉴의 정상기능 제공

**프로젝트 명 : 삼성전자 VD-HA3.0 Big Data 시스템 구축**

○기간 : 2013.04 ~ 2013.06

○프로젝트 성격 : 고객사 신규 구축(SI)

○개발 환경 및 개발 언어 : Linux / Java / Hadoop / Hive / SVN

○프로젝트 소개

|       |               |  |
|-------|---------------|--|
|       |               | <p>- 전세계의 삼성 스마트 TV에서 로그를 수집하여 수집한 로그를 분석하는 빅데이터 프로젝트</p> <p>○담당 업무</p> <ul style="list-style-type: none"> <li>- 수집한 스마트TV 로그의 익명화 작업<br/> 평문 개인정보를 보관할 수 없어 수집한 로그의 개인정보의 익명화 처리<br/> 실시간 익명화 기능 개발전까지 일단위로 로그의 익명화 처리 수행</li> <li>- 전처리된 CSV 형식의 로그 파일을 Hadoop MapReduce 기능을 사용하여 통계 메타 데이터 생성</li> <li>- Daily 통계 데이터 생성하는 Hive 모듈 개발(Hiveql)</li> <li>- 아마존 EMR 사용한 Daily 통계 모듈 실행 환경 구성</li> </ul> <div data-bbox="462 448 1452 672"> <pre> graph LR     A[수집로그] --&gt; B[전처리된 CSV 파일]     B --&gt; C[Meta 데이터 생성<br/>Map-Reduce]     C --&gt; D[Meta-data]     D --&gt; E[통계 데이터 생성<br/>HIVE]     E --&gt; F[저장<br/>S3(HDFS)]     subgraph 전처리         A         B     end     subgraph "통계 데이터 생성<br/>Hourly, Daily, Monthly"         C         D         E     end </pre> </div> <p>- 프로젝트 완료 전 프로젝트 종료(삼성전자에서 프로젝트 중단)</p> <p>○성과</p> <ol style="list-style-type: none"> <li>1) 스마트TV 로그를 Hadoop MapReduce와 Hive 통하여 일간 통계 생성</li> <li>2) 시간 당 기가 단위의 데이터 처리</li> </ol> <p>3. 퇴사사유<br/>근무환경, 자기발전</p>   |
| 제이컴정보 | 보안기술연구소/팀원/선임 | <ol style="list-style-type: none"> <li>1. 회사소개<br/>보안솔루션 개발 회사 / 직원수 - 약20명 / 매출액 - 약20억</li> <li>2. 담당업무, 프로젝트</li> </ol> <p>◎ 주요 업무</p> <ul style="list-style-type: none"> <li>▪ ESM 등, 회사 제품 개발 등 보안 솔루션 개발</li> <li>▪ Restful API 등 Java를 사용한 Back-end 서버 프로세스 개발, 구축 시스템 테스트</li> </ul> <p><b>프로젝트 명 : Mobile Device Lock</b></p> <p>○기간 : 2012.10 ~ 2013.04</p> <p>○프로젝트 성격 : 솔루션 개발 프로젝트</p> <p>○개발 환경 및 개발 언어 : Linux / Java / Android / Spring framework / Oracle</p> <p>○담당 업무</p> <ul style="list-style-type: none"> <li>- 스마트폰에 APP을 설치하여 데이터 통신이 안 되는 곳에서 SMS를 사용한 통신으로 카메라, 통화, APP 등의 사용을 제한하는 솔루션 개발, Push 메시지와 HTTP RestAPI 사용한 버전도 별도 개발</li> <li>- 스마트 폰 간의 SMS(문자) 사용한 통신 시의 데이터 변환 모듈 개발</li> <li>- 관리자 WEB : 대시보드 중 사용자 현황 차트, 정책 관리 및 정책 수정 페이지 부분 개발</li> <li>- Android App의 서버와 통신 기능 개발</li> <li>- REST API 기반의 Android APP과 통신하는 서버 개발</li> <li>- Android 폰과 서버의 정책 적용 통신(푸시/WEB)의 적용과 테스트</li> </ul> <p>○성과</p> <ol style="list-style-type: none"> <li>1) APP 사이의 통신 기능, APP과 WAS의 통신(Rest API) 개발로 신뢰성있는 통신 제공</li> <li>2) 통신기능 테스트로 신뢰성 있는 통신 보장</li> </ol> <p><b>프로젝트 명 : ESM pentagon 5.0</b></p> <p>○기간 : 2011.09 ~ 2012.06</p> <p>○프로젝트 성격 : 솔루션 개발 프로젝트</p> <p>○개발 환경 및 개발 언어 : Linux / Java / Oracle</p> <p>○담당 업무</p> |

|      |                   |  |
|------|-------------------|--|
|      |                   | <ul style="list-style-type: none"> <li>- 매니저 모듈 개발 : 에이전트에서 전송한 데이터 취합, 권한에 따른 처리 및 알람 발생 등</li> <li>- 통신 라이브러리 개발 참여</li> <li>- Spring, Apache MINA 기반의 통신 서버 개발(데이터 중계 전담)</li> </ul> <p>○성과</p> <ol style="list-style-type: none"> <li>1) ESM의 통신 기능 제공</li> <li>2) 통신전담 모듈의 개발로 ESM 각 모듈(프로세스)의 통신부하 감소</li> </ol> <p><b>프로젝트 명 : 증거력을 갖는 서버 및 네트워크 실시간 보안 감시 솔루션 개발</b></p> <p>○기간 : 2011.02 ~ 2011.08</p> <p>○프로젝트 성격 : 한국산업단지공단 연구과제</p> <p>○개발 환경 및 개발 언어 : Linux / Java / Oracle</p> <p>○담당 업무</p> <ul style="list-style-type: none"> <li>- 기존 제품인 e-Pentagon ESM을 수정하여 기능 추가하여 개발</li> <li>- 에이전트 : 시스템 로그 수집(Linux/Solaris/AIX), 수집 로그의 인증 데이터 생성</li> <li>- 매니저 : 에이전트가 수집한 데이터 취합, DB 저장, 인증 서버와 통신 연결, 수집 로그 검증 기능 개발</li> <li>- 클라이언트 : 수집 로그 검색, 매니저로 검증 요청</li> <li>- 인증 서버 : 인증 데이터 추가 생성 후 저장, 요청 인증 데이터 검색 후 매니저로 전송</li> </ul> <p>○성과</p> <ol style="list-style-type: none"> <li>1) 신뢰성 있는 수집 로그의 검증 기능 제공</li> <li>2) 한국산업단지공단 연구과제 완료</li> </ol> <p>3. 퇴사사유<br/>급여 미지급</p>                                      |
| 케이사인 | 통합인증사업<br>부/팀원/주임 | <ol style="list-style-type: none"> <li>1. 회사소개<br/>보안솔루션 개발 회사 / 직원수 - 약100명 / 매출액 - 약320억</li> <li>2. 담당업무, 프로젝트 <ul style="list-style-type: none"> <li>◎ 주요 업무 <ul style="list-style-type: none"> <li>▪ 통합인증솔루션 개발, 유지보수</li> <li>▪ 투입된 프로젝트에서 통합인증솔루션 구축</li> </ul> </li> </ul> </li> </ol> <p><b>프로젝트 명 : 인천공항 통합인증 구축/연계</b></p> <p>○기간 : 2010.02 ~ 2010.03</p> <p>○프로젝트 성격 : 고객사 신규 구축(SI)</p> <p>○담당 업무</p> <ul style="list-style-type: none"> <li>- 인천공항 설치 사이트 특성에 맞도록 통합인증 에이전트 모듈의 변경</li> <li>- 인천공항 내 시스템에 통합인증 에이전트 모듈의 설치</li> </ul> <p>○ 성과</p> <ol style="list-style-type: none"> <li>1) 인천공항 통합인증 구축</li> </ol> <p><b>프로젝트 명 : 국가대표포털 통합인증 구축/연계</b></p> <p>○기간 : 2009.10 ~ 2010.02</p> <p>○프로젝트 성격 : 고객사 신규 구축(SI)</p> <p>○담당 업무</p> <ul style="list-style-type: none"> <li>- 통합인증 서버 및 에이전트 수정 및 테스트</li> <li>- 통합인증 에이전트 상태 확인 위한 헬스체크 프로그램 개발</li> <li>- 국가대표포털과 연계 기관들의 통합인증 연계 작업</li> </ul> <p>○ 성과</p> <ol style="list-style-type: none"> <li>1) 국가대표포털과 연계기관의 통합인증 연동</li> </ol> <p>3. 퇴사사유<br/>근무환경 악화</p> |