[별첨 5]

분산 환경기반 대용량 보안 이벤트 처리 및 연관성 분석 기술

이종훈 (mine@etri.re.kr)
지능보안연구그룹

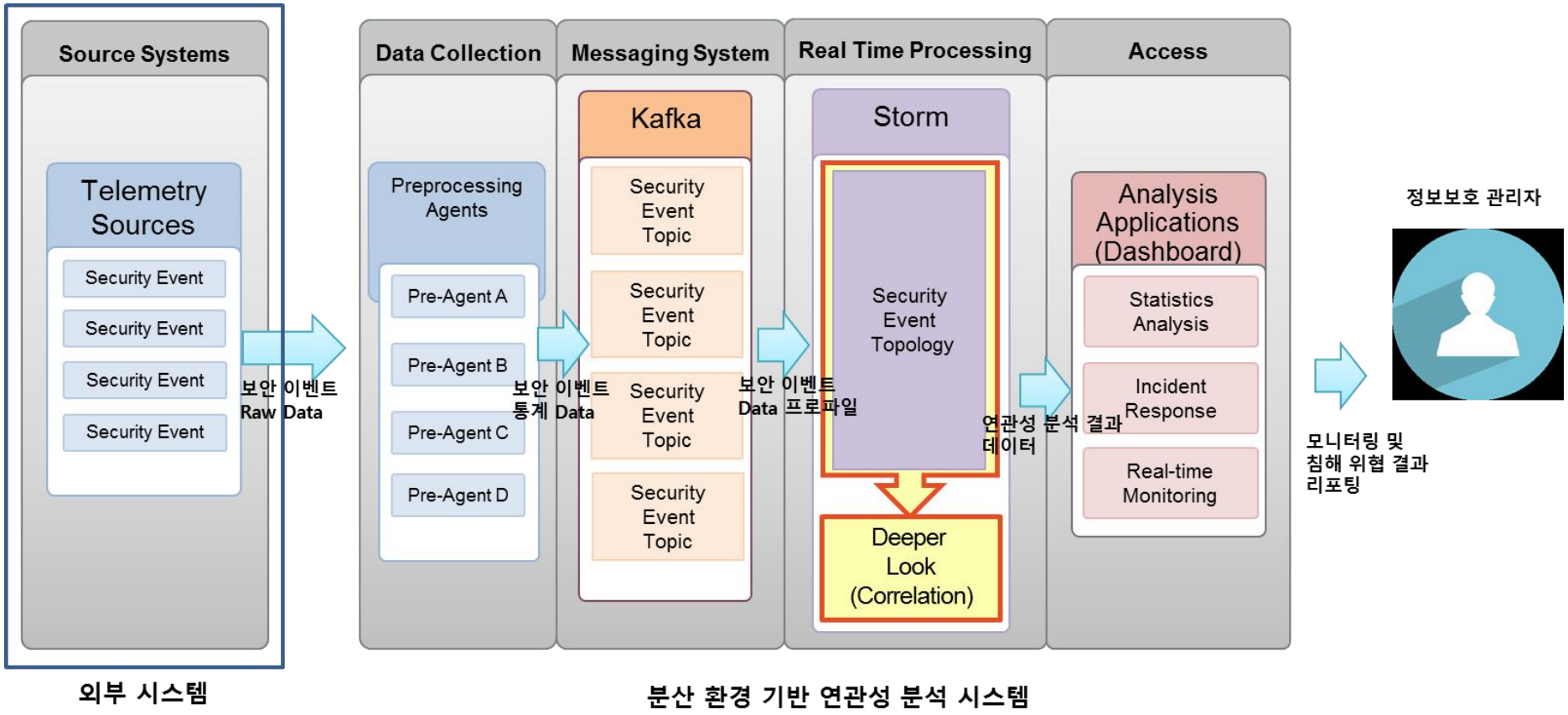
ETRI 한국전자통신연구원
www.etri.re.kr
초연결통신연구소 정보보호연구본부

1. 기술의 개요
2. 기술이전 내용 및 범위
3. 경쟁기술과 비교
4. 기술의 사업성
 - 활용분야 및 기대효과
5. 국내외 시장 동향

▣ 필요성

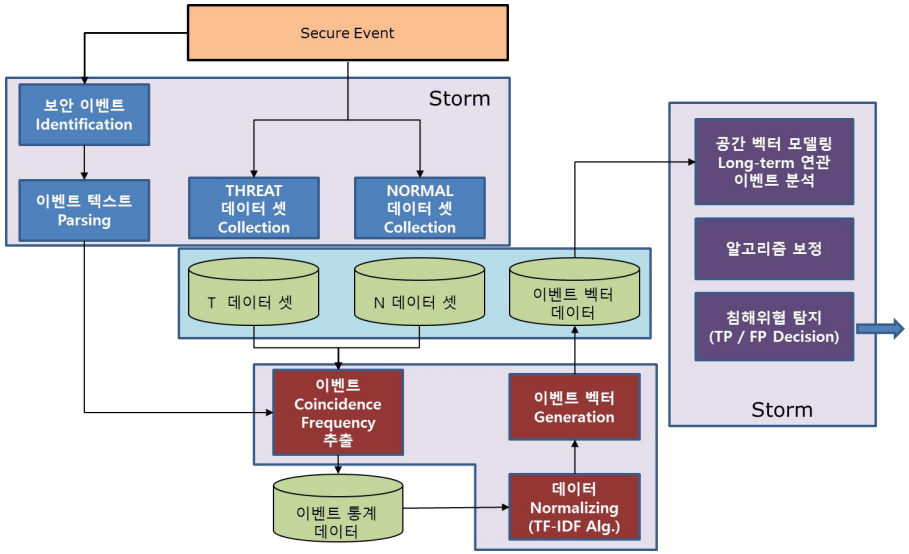
- 3.20 사이버테러 등 최근 보안 사고들은 점차 규모가 커지고 있으며, 지능형 지속 위협(APT)과 같이 고도화/지능화된 공격이 등장하고 있음
- 각종 보안 위협이 날이 갈수록 증가하고 있고, 해킹의 위협은 더 정교해지고 치밀해져 가고 있고, 이를 위한 모든 사이버 위협의 실시간 탐지, 예측 및 대응을 위한 솔루션이 요구되고 있음.
- 따라서, IT기반 시설의 사용자, 네트워크, 시스템, 응용서비스 등으로부터 발생하는 데이터 및 보안이벤트를 수집 저장 관리하고, 연관성을 분석하여 보안 인텔리젼스를 향상시키는 지능형 보안 위협 탐지를 위한 대용량 데이터 연관성 분석 기술 필요함

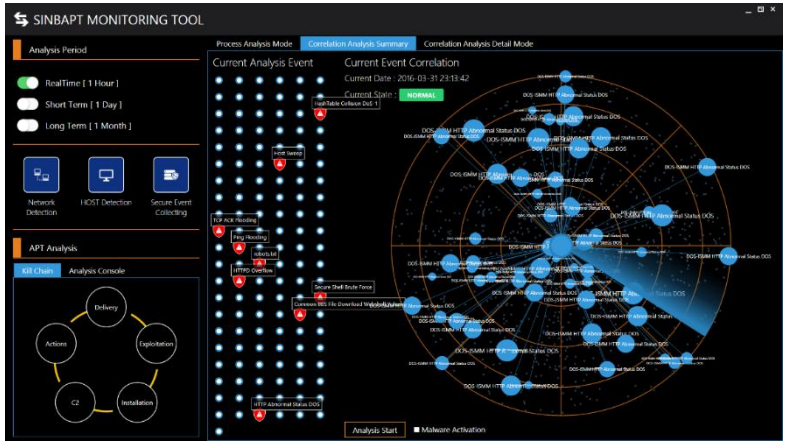
▣ 분산 환경기반 대용량 보안 이벤트 처리 및 연관성 분석 기술



▣ 기술의 특징

- 네트워크 보안 장비에서 발생하는 보안 이벤트 로그를 수집한 후, 이를 파싱하여 데이터 통계화를 수행
- 과거 발생한 침해 위협 사고(Threat) 과의 이벤트 발생 패턴, 접속 IP와의 연관성을 분석함
- 실시간 침해 위협을 인지하고 탐지
- TF-IDF알고리즘과 공간 벡터 모델링 방법을 통한 분석을 수행





▣ 기술명 : 분산 환경기반 대용량 보안 이벤트 수집 처리 기술

A. 내용

- KAFKA 기반 다중 소스 보안 이벤트 수집 및 데이터 파서 기능
- 수집 이벤트 실시간 통계 데이터 추출을 위한 데이터 처리(Storm Bolt) 기능

B. 범위

- 분산 환경 기반 보안 이벤트 수집 및 처리 프로그램,
- vSIEM 연관성 분석 요구사항정의서/시험 절차 및 결과서/사용자 매뉴얼
  * 단, 문서중 수집 및 처리 기술에 해당되는 문서 내용만 이전 대상에 포함됨.
- 특허: PR20160642KR / PR20160602KR / PR20160626KR

▣ 기술명 : 분산 환경기반 보안 이벤트 연관성 분석 기술

A. 내용

- TF-IDF 알고리즘을 이용한 이벤트 벡터화 및 학습 기능
- 공간 벡터 모델링을 통한 Long-term 연관 이벤트 분석 및 침해 위협 탐지 기능
- 보안 이벤트별 단위시간 발생 Statistics 및 실시간 모니터링 뷰
- 보안 이벤트 Long-term 연관성 분석 시각화 뷰

B. 범위

- 침해 위협 탐지를 위한 보안 이벤트 연관성 분석 프로그램, 대용량 보안 이벤트 연관성 분석을 위한 사용자 도구 프로그램
- vSIEM 연관성 분석 요구사항정의서/시험 절차 및 결과서/사용자 매뉴얼
- 특허: PR20160642KR / PR20160602KR /PR20160626KR

▣ 기술 개발 현황

❖ **기술성숙도**(TRL : Technology Readiness Level) **단계 : (5)단계**

구 분	단계	정 의	세 부 설 명
기초 연구 단계	1	기초 이론/실험	▫기초이론 정립 단계
	2	실용 목적의 아이디어 특허 등 개념정립	▫기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	▫실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 ▫개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	▫시험샘플을 제작하여 핵심성능에 대한 평가가 완료된 단계 ▫3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 ▫컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/시스템 시작품 제작 및 성능 평가	▫확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 ▫개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 ▫경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일롯 규모 시작품 제작 및 성능 평가	▫파일롯 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 ▫파일롯 규모 생산품에 대해 생산량, 생산용량, 불량률 등 제시 ▫파일롯 생산을 위한 대규모 투자가 동반되는 단계 ▫생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 ▫성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	▫실제 환경에서 성능 검증이 이루어지는 단계 ▫부품 및 소재개발의 경우 수요업체에서 직접 파일롯 시작품을 현장 평가(성능 및 신뢰성 평가) ▫가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	▫표준화 및 인허가 취득 단계
사업화	9	사업화	▫본격적인 양산 및 사업화 단계 ▫6-시그마 등 품질관리가 중요한 단계

▣대용량 보안이벤트 처리 및 연관성 분석 기술

- 기존 SIEM 솔루션이나 SOC 센터에서 사이버 침해 위협 탐지 및 분석을 위해 수집된 보안 이벤트에 대해 공격 룰 기반으로 분석을 해왔으나, 본 기술은 룰 없이 데이터 마이닝을 기반으로 과거 Long-term 데이터와의 연관성을 분석하여 침해 위협을 인지하기 위한 분석 기술임
- 본 기술은 다양한 보안이벤트를 수집하여 저장 → 연관성을 분석 및 검색 → 공격 징후에 판단하기 위한 시스템을 제공
- 대용량 데이터 수용을 위한 분산 환경 기반으로 데이터마이닝 기술을 적용하여 사이버 침해 위협의 분석이 가능한 지능형 보안 위협 분석 기술을 제공함
- 데이터 마이닝을 이용한 머신 러닝을 통한 인공지능 기반 침해 위협 탐지 솔루션 개발 분야에 활용이 가능

▣ 사업성

예상 제품 /서비스	예상단가 (천원)	이전기술의 비중(%)	잠재적/현재적 경쟁자와 가격,시장 등에서 경쟁상 유리한 점	판매 가능 시기
지능형 보안 분석 분야의 SIEM 솔루션	100,000 / 데이터 분석 플랫폼 및 서비스 (중소기업기준)	90%	a. 가격경쟁력면: 기존 외산제품에 비해 저렴하며 기능 요구사항에 따라 변동 가능 b. 시장환경면: DDoS 및 해킹 공격에 대한 실시간 탐지 및 분석 기술에 대한 시장의 급속한 요구 및 구매력 증가 c. 기타: 기능면에서 경쟁력 있음 (기존 룰 기반 방식의 한계를 극복함)	2019

- ❖가격 경쟁력: 상용제품의 기능 요구사항에 따라 변동가능
- ❖상용화를 위한 생산설비 등 추가비용: S/W 이므로 생산 설비 등 추가비용 없음
- ❖상용화를 위한 추가적인 기술개발 내용: 해당 없음

▣ 국내외 시장 동향

- 최근 인공지능 및 빅데이터 분석 등의 기술이 발전하면서, 방대한 보안 로그, 네트워크 정보, 응용 트랜잭션 등 대용량 데이터를 통합하여 분석할 수 있는 지능형 보안 분석과 관련된 시장의 수요가 증가되고 있음.
- 데이터마이닝 및 머신러닝 기반의 통합 로그 분석은 현재 제한적으로 연구/개발되고 있으나, 빅데이터 분석과 같은 대용량, 이종데이터 분석을 위한 인프라 제공시 향후 해당 분야의 연구가 활성화 될 것으로 전망됨
- 지능형 사이버 해킹 공격이 증가하면서 시장에서 SIEM 보안 솔루션 및 서비스에 대한 수요가 증가 되고 있음.

(단위 : 백만불, 억원)

관련 제품 /서비스	시장	1차년도 (2017)	2차년도 (2018)	3차년도 (2019)	4차년도 (2020)	5차년도 (2021)	합계
네트워크 보안 관리 솔루션	해외 (백만불)	1,573.5	2,311.5	3,395.6	4,988.1	7,327.5	19,596.2
	국내 (억원)	314.7	462.3	679.12	997.62	1,465.5	3,919.24

* TechNavio Analysis, Inc사의 Global Virtualization Security Management Solutions자료의 2011~2015년도 예측치를 기반으로 관련 CAGR을 적용하여 2017~2021년도 시장규모를 추
* 국내 시장규모는 전체 세계 시장규모(CAGR 46.9%)의 2%(아시아환태평양 지역의 약 20%)로 추정
* 지역별 세계시장 점유율: 아메리카 57%, 유럽 및 중동 32%, 아시아환태평양 11%

www.etri.re.kr

※ 하단의 문의처 소개후, 발표후 개별기술 상담이 가능함을 다시 한 번 안내함

♣ 연락처 : ㅇㅇㅇ연구부문(본부), 홍길동 선·연 (042-860-0000, hkd@etri.re.kr)