Journal of The Korea Society of Computer and Information
Vol. 20 No. 8, pp. 35-43, August 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.8.035

Enhancement of Internal Control by expanding Security Information Event Management System

DongSung Im*, Yongmin Kim **

Abstract

Recently, internal information leaks is increasing rapidly by internal employees and authorized outsourcing personnel. In this paper, we propose a method to integrate internal control systems like system access control system and Digital Rights Managements and so on through expansion model of SIEM(Security Information Event Management system). this model performs a analysis step of security event link type and validation process. It develops unit scenarios to react illegal acts for personal information processing system and acts to bypass the internal security system through 5W1H view. It has a feature that derives systematic integration scenarios by integrating unit scenarios. we integrated internal control systems like access control system and Digital Rights Managements and so on through expansion model of Security Information Event Management system to defend leakage of internal information and customer information. We compared existing defense system with the case of the expansion model construction. It shows that expanding SIEM was more effectively.

▸ Keyword : Internal control system, Security Information Event Management, Scenario, Monitoring

I. Introduction

현재 빅 데이터, 사물 인터넷, 전자화폐 등 IT 기술의 눈부신 변화만큼 외부의 공격 및 내부자에 의한 보안 위협도 급격히 늘어나고 있다. 공격 타켓을 정해 고도화된 방법으로 장기간 동안 공격하는 APT공격, 정치적 목적을 달성하기 위해 특정 집단을 공격하는 핵티비즘, 웹사이트를 통해 유포되는 악성 코드 등 다양하고 지능화된 공격들에 노출되어 있다. 과거에는 시스템들의 취약점을 노린 외부 해커에 의해 보안 사고가 주를 이루었으나 최근에는 내부 임직원 및 인가된 외주 용역 인력에 의해 내부 정보 유출 사고가 증가하고 있다. 인가된 내부 직원이 불순한 의도로 내부 정보를 유출하는 행위를 차단하기가 쉽지 않은 것도 현실이다. 하지만 잇따른 개인정보 유출 사고로 개인정보보호법이 더욱 강화되어 내부 정보 유출 방지를 위한 대응이 필요하다. 과거에는 작은 비용의 과태료를 부과였으나, 징벌적 손해 배상, 양벌 규정을 통한 임원 책임 확대 등 제재 수준이 대폭 강화되었다. 또한 SANS의 2012년 로그 수집 설문 조사에 따르면 로그 수집이 중요한 가장 큰 이유는 내부자의 의심스런 행위 감지였다[1]. 따라서 IT 서비스 환경 변화와 내부 정보 유출 대응, 법규 강화 등의 보안 패러다임에 부합하는 보안 기술이 요구된다. 즉 방화벽, IPS 등의 경계 방어 시스템 위주로 통합했던 통합 로그 관리 시스템을 문서 보안, 시스템 접근 제어 등의 단위 내부 통제 시스템들의 로그를 통합하고 행위 중심의 상호 연계 분석이 가능하도록 확장할 필요가 있다[2].

본 논문의 구성은 다음과 같다. 2장에서는 현재 사용되고 있는 통합 로그 관리 시스템에 대한 관련 연구를 기술하고 3장에서는 개인 정보 처리 시스템에 대한 불법 행위와 내부 보안 시스템을 우회하는 행위들을 대응할 수 있는 시나리오 도출 확장 모델에 대해 제안하였다. 4장에서는 내부 정보 및 고객 정보 유

• First Author: DongSung Im, Corresponding Author: Yongmin Kim
*DongSung Im(seaids@naver.com), Interdisciplinary program of Information Security, Chonnam National University
**Yongmin Kim(ymkim@chonnam.ac.kr), Dept. of Electronics Commerce, Chonnam National University
• Received: 2015. 04. 15, Revised: 2015. 05. 07, Accepted: 2015. 06. 24.

출을 대응하기 위해 구축된 문서보안, DB접근 제어 등의 내부 통제 시스템을 중심으로 통합 로그 관리 시스템 확장 모델이 적용된 사례를 살펴보고 기존에 운영되었던 방식과 비교하여 확장 모델의 결과를 평가하였다. 마지막으로 5장에서는 결론 및 향후 연구에 대해 보였다.

II. Security Information Event Management System

산업간 벽이 허물어지고 통합되는 융복합 시대와 내부 정보 유출 사고들이 큰 이슈가 되고 있는 이 시점에 통합 로그 관리 시스템은 다시 주목을 받고 있다. 이에 통합로그 관리 시스템 개요와 특징 및 요구 사항 등에 대해 분석한다.

1. Security Information Event Management System Characteristic

초기에는 각각의 보안 시스템들에서 발생하고 있는 이벤트 로그들과 중요 업무 시스템의 액티비티 로그들을 수집하고 컴플라이언스에 요구하는 데이터 무결성을 보장하기 위한 로그 수집/저장 중심의 시스템이었다[3]. 그리고 방화벽, IPS/IDS ,DDoS 등의 외부 경계선 방어를 목적으로 하는 경계 방어 시스템(Perimeter Defense System)들의 로그들을 단순 분석하는 ESM(Enterprise Security Management)솔루션으로 확장되었다[4]. 현재에는 내부 통제를 수행하는 보안 시스템들의 이벤트와 장기간 동안 수집된 저장 로그를 기반으로 기초적인 분석이 아니라 입체적 관점으로 상관 분석하는 형태로 변화하고 있다[5]. 따라서 통합 로그 관리 시스템은 보안 시스템과 IT 시스템들에서 발생되는 이벤트들을 장기간 수집/저장하고 통합적으로 분석하여 의미 있는 위협을 사전에 탐지 및 모니터링하는 시스템으로 정의할 수 있다.

통합 로그 관리 시스템은 주로 이기종간 보안시스템들의 보안 로그를 수집하고, 위협에 대응하기 위해 이를 상관 분석하여 시각화하는 특징을 가지고 있다[6][7]. 좀더 살펴보면 경계 방어 시스템 및 내부 정보를 취급하는 업무 시스템 등 다양한 장치로부터 정형/비정형의 다양한 로그들을 고속으로 수집한다[8]. 이후 수집된 원시 데이터는 파싱 기술을 통해 공통된 포맷으로 정규화와 카테로그화된 공격 유형 등으로 범주화되어 저장 관리된다. 정규화된 다양한 이벤트들은 실시간 상관 관계 분석을 통해 예측할 수 있는 위협들을 탐지·모니터링 한다[9][10]. 그리고 리포팅, 데시보드 형식의 시각화를 통해 보안의 가시성을 확보하는 형태로 구성되어 있다. 그리고 로그 수집 대상은 경계 방어 시스템 중심이며 DB와 syslog, snmp 등의 형태로 수집된다.

그림 1과 같이 IPS/IDS는 syslog 혹은 DB Query로 이벤트 로그를 연동하고 악성 코드를 발생시키는 IP, Port등의 로그들을 수집한다. 또한 VPN은 주로 해당 서버에서 syslog로 설정하여 통합 로그 관리 시스템으로 이벤트를 전송하는데 주로 해외에서 들어 오는 불법 IP 정보 등이 해당 될 수 있다.

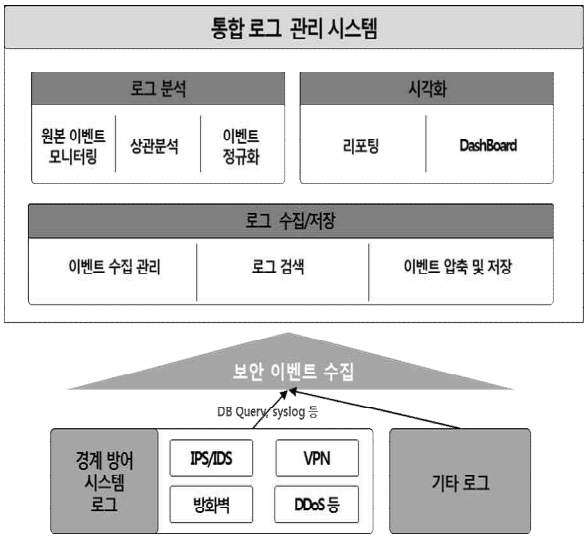


Fig. 1. SIEM concept graphic

2. Requirements of expanding Security Information Event Management System

더욱 지능화되고 있는 사이버 공격과 은행, 카드사 등의 금융권 내부 정보 유출 사고들을 능동적으로 대응하기 위해서는 보다 지능화되고 정교화된 방어 시스템들이 필요한 실정이다. 이에 통합 로그 관리 시스템 기술은 내부망 보안 시스템들의 이벤트를 수집하고 분석하는 등의 내부 위협 행위 감시 기술로써 연구가 활성화되고 있다[11]. 또한 APT 공격과 같은 알려지지 않은 치명적인 공격에 대응하기 위해 방화벽, IDS/IPS, DDoS, VPN 등의 기존 보안장비와 서버, 네트워크 장비 등으로부터 통계 정보, 보안 이벤트 로그 정보를 함께 가져와서 이들 정보들 간의 상호 연관성 분석을 수행하는 콘텍스트 기반의 분석 기술로 확장되고 있다[12][13].

기존 관련 연구들을 분석해 보면 내부 정보 유출 징후 분석을 통한 유출방지체계 구축에 관련 연구[2]는 국내외 compliance 준거 요건으로 구성된 고객 보안 정책, 기업 내부 정보 유출 통제정책 기반 하에 집중 관리가 필요한 인력, 내부 정보 취급 업무 시 내부정보 취급자의 악의적 또는 부주의 등으로 인해 유발될 수 있는 프로세스상의 내부 정보 유출 위험들을 기반으로 회사 구성원들이 어떤 내부 정보를 어떻게 취급하고, 통제되고 있는지 등에 대한 세부 내부 정보 유출 위협 내역들을 분석·수립하였다. 이를 통해 탐지·분석 정책을 개발·적용·검증하여 내부 정보가 외부로 유출되는 위협들을 방지할 수 있는 체계를 효과적으로 구축할 수 있도록 연구하였다. 그러나 내부 정보 유출, APT 등의 복합 공격을 상호 연계 분석하여 능동적으로 대응하는 통합 시나리오 발굴에 대해서는 체계적인 발굴 방법이 없어 통합 시나리오 발굴 및 적용에 한계가 있었다. 그리고 시나리오 기법을 활용한 기업 정보보호 방법론에

관한 연구[4] 관련 주요 내용은 개별 보안 시스템들에 대해 내부 정보 유출 모니터링 측면에서 임직원의 기업 내부 정보 유출 사례와 관리적·기술적 한계에 대해 분석하였다. 또한 단위 보안 시스템들의 패턴 설계, 행위 패턴 기반의 시나리오 설계 등의 시나리오 기법을 통한 통합 보안 모니터링 방법을 제시하여 고도화되고 있는 내부 임직원에 의한 내부·고객 정보 유출 위협에 대해 기업의 정보보호 활동을 강화할 수 있도록 하였다. 그러나 고객 정보를 처리하는 개인 정보 처리 시스템들에 대한 보안 이벤트 수집이 없어 고객의 개인 정보 유출 징후를 입체적으로 상호 연계하여 탐지하는데 한계가 있다. 또한 해당 연구에는 통합 시나리오가 일부 있으나 통합 시나리오를 만드는 방법이 체계적이지 않아 이에 대한 개선 사항으로 체계적인 통합 시나리오 발굴 모델이 필요한 상황이다.

이와 같이 트랜드 및 기존 관련 연구 분석을 통해 통합 로그 관리 시스템의 확장 요구 사항을 분류해 보면 다음과 같다.

첫째, USB, 메일, 프린터 등의 내부 정보 유출 경로가 확대되고 있으며 이것들이 서로 유기적으로 연관되어 내부 정보가 유출되고 있다. 이에 통합 로그 관리 시스템에서는 내부 보안 솔루션의 단위 로그 수집이 아니라 산재되어 있는 다양한 보안 시스템들의 로그들을 통합적으로 수집할 필요가 있다.

둘째, APT과 같이 장기적으로 고도의 해킹 기술로 내부를 공격하는 복합 공격에 대해 대처할 수 있는 개별적 보안 솔루션의 단순 시나리오가 아닌 여러 주요 보안 인프라가 연계된 통합 시나리오들을 도출하여 이에 대응할 필요가 있다.

셋째, 해킹기술 및 정보유출의 방법이 다양화됨에 따라 이에 대응하는 보안시스템도 계속적으로 증가하고 있다. 따라서 다수 보안 솔루션들을 통합적으로 운영하고 대응할 수 있는 통합 로그 관리 시스템 확장 측면의 체계적인 시나리오 발굴 방법이 요구된다.

III. SIEM expansion Model

APT, 악성 코드 등 다양한 위협에 의해 내부 정보 및 개인정보가 유출되는 상황에서 특정 정보 유출 대응 영역에 분산되어 개별적으로 운영되는 보안 시스템은 한계가 있어 이를 유기적으로 연계하여 통합 대응할 수 있는 방안이 필요하다. 이에 본 연구에서는 내부 정보 유출을 효과적으로 탐지·대응할 수 있게 5W1H를 활용한 시나리오 중심의 통합 로그 모니터링 시스템 확장을 제안하고자 한다. 본 연구 확장 모델은 분석 단계, 개인정보보호 시스템과 보안 시스템 우회 대응 단위 시나리오 도출 단계, 해당 단위 시나리오를 통합 구성하는 통합 시나리오 도출 단계, 그리고 보안 가시성 확보를 위한 모니터링 단계로 구성된다.

1. Analysis Step

1.1 Analysis of targeted System

기업에는 PC, 서버, 보안 장비, 네트워크 장비 등의 다양한 시스템들이 운영되고 있다. 다양한 인프라 중에서 내부 통제를 위한 중요 자산들을 식별하고 연동에 필요한 중요 정보들을 수집·분석할 필요가 있다.

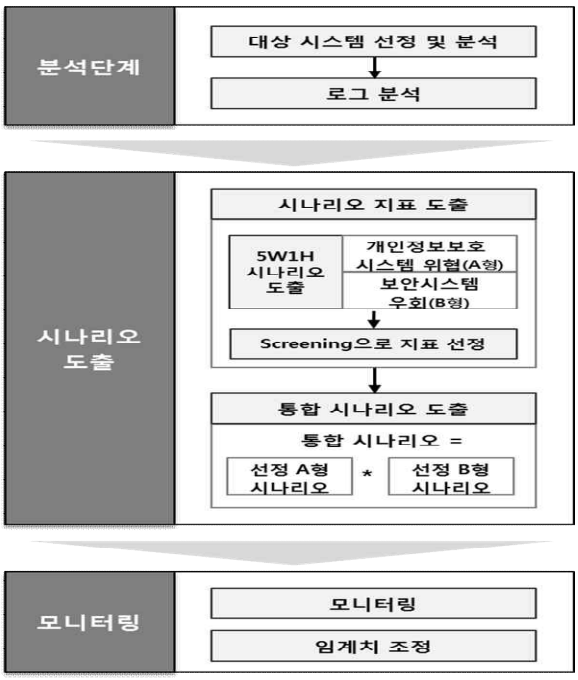


Fig. 2. SIEM expansion model

유효한 로그 수집을 위해 DRM, 접근 통제, PC 보안 등의 보안시스템과 고객 정보를 가지고 있는 고객정보시스템, 채용 시스템 등의 개인정보처리시스템으로 분류하고 식별할 수 있다. 선정된 시스템들은 로그 수집을 위해 IP, 연동 주기, 연동 방식을 결정하여야 한다. 특히 DB, syslog, File 등의 어떤 연동 방식을 선택할 것인지에 따라 식별되어야 할 정보가 추가 될 수 있다. 예를 들어 DB 연동 방식인 경우 DBMS 종류, DB Port, DB명 및 연동 테이블 등이 될 수 있다. 그리고 보안성을 고려할 경우 기존 DB 계정을 사용하지 않고 조회 권한만 갖는 DB 계정을 별도 만들어 보안 로그를 수집할 필요가 있다. 그리고 주요 보안 사고 사례들을 분석하여 취약점과 이를 통해 확장 모델 시나리오들을 도출할 수 있다. IT 센터 외주 개발 업체 직원이 10만 4천 건을 USB로 유출한 S사와 카드 3사 회사 전산망에 접근하여 개인 정보 1억 580만 건을 유출한 카드사 등의 개인 정보 유출 사고들은 중요 시스템의 불법 접근 행위와 USB로 개인 정보를 유출하는 행위 등을 연계하여 통합하는 시나리오들이 필요하다.

1.2 Analysis of collected logs

연동할 시스템의 정보가 파악된 경우에는 연동 시스템들의 로그들을 상세 분석할 필요가 있다. 어떤 로그들을 저장하고 어떤 로그들이 실제 내부 통제와 개인정보보호 대응을 위해 필요한지를 분석하여 파악하여야 한다.

제목	A개인정보시스템		작성자	홍길동
시스템	A개인정보시스템		고객승인	IT관리 김철수
로그구분	DB		연동방식	DB 쿼리
파일명 (테이블)	· LST_MANAGER_LOGIN : 관리자 로그인 이력			
연동정보요약			연동주기	10분
피일 / 테이블 상세				
테이블 명	LST_MANAGER_LOGIN (관리자 로그인 이력)			
Colum ID	타입	설명	이벤트 필드	비고
LOGIN_IP	VARCHAR2(20)	로그인IP 정보	Source Address	
LOGIN_DT				

Fig. 3. example of the analysis on the collected logs

특정 내부 통제 시나리오가 도출되었으나 해당 로그들이 수집이 되지 않으면, 해당 시나리오는 실제 운영시에 이벤트가 발생하지 않아 유효하지 않을 수 있다. 특히 DB 연동 방식인 경우 중요 내부 정보를 보유한 테이블명과 해당 테이블의 컬럼명, 타입, 크기 등의 스키마 구조를 파악하여야 한다. 이러한 정보들을 통해 시스템 연동 및 유효한 로그들을 정확히 수집할 수 있다. 그림 3은 특정 개인정보시스템으로 관리자 로그인 이력 테이블에 대한 분석이다. 개인정보시스템으로 접속하는 IP 정보는 이 특정 테이블의 20byte varchar2 Login_IP 칼럼에 저장된다. 따라서 운영자들은 접속 로그인 정보를 내부 통제를 위한 중요한 정보로 활용할 수 있다.

2. Unit Scenario

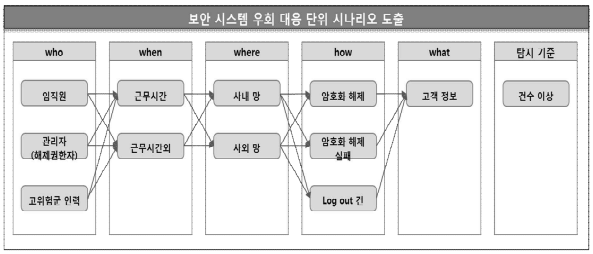
2.1 Personal information processing system scenario

개인 정보 처리 시스템에 대해 불법 접속하여 중요 정보를 유출할 수 있는 위협에 대응하기 위해 5W 1H 관점에서 단위 시나리오를 생성할 수 있다. 5WIH는 Who, When, Where, What, Why, How을 기준으로 정보 유출 위협을 분석하는 것이다. 시나리오 관점의 5W1H(육하원칙)를 좀더 살펴보면 일반 임직원, 퇴직 예정자, DB 운영자, DB 개발자, 개인정보 취급자, 계약직, Blacklist 등의 누가(Who) 측면과 근무 시간, 근무외 시간, 공휴일, 휴가 등의 언제(When)측면이 있을 수 있고 본사망, 해외망, 인터넷, C&C IP 등의 언제(Where)가 있을 수 있다. 그리고 개인정보 처리 시스템에서의 개인 정보 문서, 중요 문서 등의 무엇을(what)과 해당 중요 정보를 조회, 다운로드, 인쇄 등의 어떻게(How) 행위를 했느냐로 구분할 수 있다. 또 그 해당 행위가 실수, 업무, 고의 등의 왜(Why)로 분류할 수 있을 것이다.

여기에 임계치를 통해 단위 시나리오를 탐지 기준 이상시 탐지할 수 있을 것이다. 1천 건수이상의 건수와 상위 5%이상, 기존 정규 패턴 일탈 등의 기준을 통해 임계치를 측정할 수 있다. 예를 들어 고객 정보를 가지고 있는 CRM 시스템에 개인정보 취급자인 퇴직예정자가 토요일 오후 9시에 회사에서 고객 정보가 있는 DB table에 Query를 평소보다 과다하게 1만건 이상 수행하는 행위를 탐지할 수 있는 단위 시나리오를 도출할 수 있다. 해당 위협 시나리오는 업무가 아닌 고객 정보 유출 가능성으로 판단 할 수 있다.

2.2 Scenario of bypassing security system

내부 통제를 위해 운영되고 있는 보안 시스템들에 대해 누가(who), 무엇을(What), 어떻게(How)중심으로 내부 중요 정보 유출 대응 시나리오를 도출할 수 있다. 개인정보 취급자, 권한이 있는 사용자, blacklist, 퇴직예정자 등의 누가(who)측면, 중요 문서, 고객 개인정보 등의 무엇(What)을 암호 문서 해제, 웹메일로 외부 유출 등의 어떻게(How)를 중심으로 보안 솔루션 우회 통제 단위 시나리오를 생성할 수 있다. 그림 4는 일반적인 문서 보안 시스템 우회를 시도하는 행위들을 탐지하는 시나리오 도출 모델이며 이를 통해 얻어진 상세 시나리오 사례들이다.



보안시스템	who	when	where	How	what	탐지기준	도출 단위 시나리오
문서 보안	임직원	근무시간	사내망	암호화 해지 건	고객 정보 문서	1건 이상	임직원이 근무시간에 암호화 해제 건수 탐지 기준 초과
	임직원	근무시간	사내망	암호화 해지 실패 건	고객 정보 문서	50건 이상	임직원이 근무시간에 암호화 해제 실패 건수 탐지 기준 초과
	임직원	근무시간외 시간	사외망	암호화 해지 실패 건	고객 정보 문서	1건 이상	임직원이 근무시간외 사외에서 암호화 해제 실패 건수 탐지 기준 초과
	임직원	근무시간	사내망	Log out 건	고객 정보 문서	10회 이상	임직원이 근무시간에 Log out 건수 탐지 기준 초과
	관리자(해제권한자)	근무시간	사내망	암호화 해지 건	고객 정보 문서	50건 이상	관리자가 근무시간에 암호화 해제 건수 탐지 기준 초과
	관리자(해제권한자)	근무시간외 시간	사내망	암호화 해지 건	고객 정보 문서	30건 이상	관리자가 근무시간외 암호화 해제 건수 탐지 기준 초과
	Blacklist	근무시간	사내망	암호화 해지 실패 건	고객 정보 문서	1건 이상	Blacklist가 근무시간에 암호화 해제 실패 건수 탐지 기준 초과
	Blacklist	근무시간외 시간	사내망	암호화 해지 실패 건	고객 정보 문서	1건 이상	Blacklist가 근무시간외 암호화 해제 실패 건수 탐지 기준 초과

Fig. 4. Scenario derivation of security system

특히 보안 시스템 우회 대응 시나리오에서 어떻게(How)는 각 보안 시스템의 예방 통제의 주요 기능에 해당 될 수 있다. 예를 들어 문서 보안 시스템인 DRM에서 개인정보 취급자가 업무시간외에 다수 고객 개인 정보가 있는 문서들을 전체 암호화 해제하는 경우의 우회 시나리오들을 도출할 수 있다. 문서 보안 시스템의 주요 통제 기능인 암·복호화 기능의 How을 중심으로 시나리오를 구성할 수 있다.

2.3 Key threat scenario selection

개인정보 처리 시스템의 위협과 보안 시스템 우회에서 도출된 시나리오들을 가지고 유효성, 위험과의 연관성 등으로 평가하여 주요 위험 시나리오들을 선정할 수 있다. 핵심 위험 시나리오 Screening 요소인 유효성, 위험과의 연관성, 산출 용이성, 자동화 정도에 따라 High(3), middle(2), Low(1)로 점수를 주어 10점 이상을 핵심 위험시나리오로 선정·분류한다.

Table 1. Scenario selection calculation

산출 방법		
*총합 = 유효성 + 위험과의 연관성 + 산출용이성 + 자동화정도 *시나리오 선정: 총합 >= 10		
선정 항목 내용		
선정 항목	항목 상세 설명	점수 구분
유효성	시나리오로 이용할 수 있는지에 대한 가치를 평가함	H:3, M:2, L:1
위험과의 연관성	내부 정보 및 개인 정보와 연관된 위험의 수준을 나타냄	H:3, M:2, L:1
산출용이성	시나리오가 반복적으로 발생할 수 있는 수준을 나타냄	H:3, M:2, L:1
자동화 정도	자동으로 측정할 수 있는 수준을 나타냄	H:3, M:2, L:1

선정 항목 관련 유효성과 위험과의 연관성은 조직의 보안 관리 지침 및 특성에 따라 수치화하고 산출용이성, 자동화 정도는 일정기간 동안 모니터링을 실시한 후 평균값을 중심으로 산정·보정한다. 예를 들어 특정 회사의 보안 지침관련 일반 직원이 암호화 해제 권한이 없는 경우 중요 문서를 유출하는 시나리오는 유효성 점수가 Low이고, 암호화 해제 건수를 일정 기간 모니터링한 결과 평균 50건이라면 발생 빈도와 자동화관련 High는 평균값의 110%, Low는 90%이하로 점수화할 수 있다.

3. Integration scenario

통합 시나리오는 개인정보처리 시스템 위협 시나리오와 보안 시스템 우회 대응 시나리오를 통합하여 도출할 수 있다.

Table 2. Integration scenario derivation method

통합 시나리오 =
개인정보 처리 시스템 위협 시나리오 * 보안 시스템 우회 대응 시나리오

표 3은 고객 정보를 암호화 해제 후 USB로 유출하는 통합 시나리오로 연관 단위 시나리오들을 통합하여 도출 할 수 있다. CRM시스템의 고객 정보를 1일 100건이상 다운로드한 사람이 해당 문서를 100건 이상 해제하는 DRM 우회와 USB 쓰기 PC 보안 시스템을 우회한 단위 시나리오들의 통합으로 내부 정보 유출 위협 통합 시나리오를 만들 수 있다.

4. Monitoring

모니터링 단계에서는 시나리오에서 탐지된 개인 정보 유출 등의 이상 행위에 대한 징후를 알려 준다. 개인별, 조직별 내부 통제 위반 요약 정보와 상세 정보를 보여주고 이를 통해 일간, 주간, 월간 등의 기간별 Top 5, 10 통계 정보를 제공한다.

Table 3. Example of Integration scenario

통합 시나리오	연관 단위 시나리오					
	개인정보처리시스템위협 시나리오			보안시스템 우회 대응 시나리오		
	설명	시스템	탐지기준	설명	시스템	탐지기준
고객 정보 과다 다운로드 하여 암호화 해제후 USB로 고객 정보 유출	고객 정보 다운로드 건수	CRM 시스템	1일/100건 이상	중요 문서 해제 건수	DRM	1일/100건
				USB 쓰기 건수	PC 보안	1일/100건

정상 업무로 판단되는 Alert들을 분석하여 해당 시나리오들의 임계치 조정을 수행한다. 이를 통해 고객에 맞는 최적화된 시나리오를 유지·운영할 수 있다. 그리고 전사 차원의 모니터링 가시성을 확보하여 개인정보 유출 위협 탐지 및 대응에 대한 효율성을 증대 시킬 수 있다.

IV. Evaluation SIEM expansion Model

1. Environment of integrating internal control system

내부 직원은 공통망과 외부 인터넷 비지니스를 수행하는 쇼핑몰망으로 구분되어 네트워크를 분리하여 이용하고 있다. 이를 보호하기 위하여 각각의 망에 방화벽, IPS, DDoS와 외부 원격 접속을 위한 공통망용 VPN을 운영하고 있었다. 이후 단말 보안으로 문서 암/복호화를 수행하는 문서 보안과 USB등의 매체를 제어하는 통합 PC 보안등이 구축되었고, 주요 서버의 접근을 통제하는 서버 접근 제어와 DB 보호를 위한 DB 접근제어 시스템, 내부 정보 유출 모니터링을 위한 네트워크 DLP(Data Loss Protection) 등의 다양한 보안 시스템들이 운영 되고 있다. 다음 그림 5는 통합 로그 관리 시스템 확장 모델을 적용하여 구축한 사례의 구성도이다. 즉 다수 보안 솔루션이 산재되어 있고 통합적으로 관리되지 않고 있는 고객 사이트에 실제 해당 모델을 구축하였다.

구축시 본 확장 모델을 로그 수집·분석 모듈, 통합시나리오 모듈, 모니터링으로 구성하였다. 로그 수집·분석 모듈에서 수집된 로그들은 통합시나리오 모듈 DB로 전송된다. 또한 임계치 비교 모듈에서 설정된 임계값과 비교하여 이때 초과되는 룰들은 분석 모듈에서 상관 분석되어 불법 행위들을 탐지하였다. 예를 들어 CRM 다운로드 초과와 DRM 문서 해제, PC보안 USB 쓰기 건수들은 임계치를 비교하여 초과할 경우 각 룰과 관련된 테이블의 공통화된 IP_Address들을 join하여 같다면 해당 IP 주소에서 개인정보를 암호화 해제후 USB로 유출하는 불법 행위로 탐지할 수 있다.

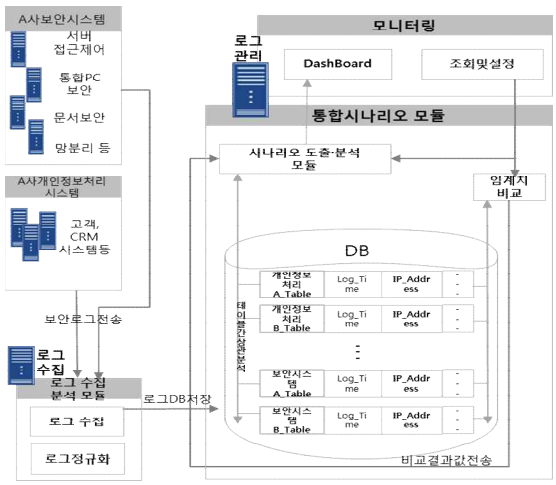


Fig. 5. Deployment of the expansion model environment

2. Example of implementing SIEM expansion Model

내부 보안 시스템 연동을 위해 먼저 운영중인 단위 내부 통제 시스템들의 기능과 적용된 보안 정책에 의해 발생되는 이벤트 등의 수집 로그 분석을 수행하는 현황 분석을 진행하였다. 특히 내부 정보 유출 위협 탐지를 위해 각 단위 내부 보안 시스템의 상호 연관성을 고려하여 시나리오 룰을 설계한 후 통합 로그 관리 시스템에 적용시 단위 내부 통제 시스템들의 로그 수집 분석을 제대로 수행하지 않는 경우 시나리오와 관련된 이벤트 로그들이 발생하지 않을 수 있다.

대상 선정 및 연동 방식 분석관련 각 내부 통제 시스템에서 발생되어 저장되는 이벤트들을 통합 로그 관리 시스템으로 수집하기 위해 각 해당 시스템들이 자신들의 이벤트 로그를 어떻게 저장하는지 확인하고 가장 효율적인 방법을 찾아 연동 방식을 결정했다. 이벤트가 DB 테이블에 저장되는 경우 해당 table의 뷰(view)를 만들고 일정 시간에 배치(batch) 형태로 검색하여 통합 로그 관리 시스템으로 가져 온다. 이를 통해 테이블 접근에 대한 보안성 및 업무 가용성을 확보할 수 있다. DB 검색으로 가져오지 못하는 경우에는 syslog ,ftp 등의 형태로 이벤트를 수집하는 것이 가장 효과적인 연동 방식인 것으로 확인하였다.

표 4에서는 선정된 연동 대상 시스템과 해당 시스템에서 수집되는 주요 정보와 해당 로그들을 어떻게 연동했는지를 확인할 수 있다. 그리고 유효한 로그를 수집하기 위한 수집 로그 분석에서는 각 선정 시스템의 설정과 로그 생성을 확인하였다. 표 5은 유효한 시나리오 도출을 위해 주요 연동 대상 시스템들의 각 보안 정책 설정 여부를 검증한 내용이다.

Table 4. Selecting System and analysis of the integration method

대상 시스템	주요 로그 수집정보	연동 방식
문서 보안	·문서 복호화 이력 ·화면 캡쳐 이벤트	DB
통합 PC 보안	·USB write 이벤트 ·출력물 출력 이력	DB
POS보안	·PE 파일 변경 이력 ·악성코드 삭제 이벤트	syslog
v3/patch 관리	·백신 데몬 off ·Patch Deploy 이력	DB
망분리	·망분리 로그인 이력 ·영역간 파일 이동 이력	syslog
시스템 접근 제어	·telnet,ftp 등 접속 이력 이벤트 ·금지 명령 수행 이벤트	DB
DB접근 제어	·DB 접속 이력 이벤트 ·주요 table 검색 등 명령 수행	ftp
DLP	·외부 메일 다수 발송 내용/이력 ·외부 불법 메신져 내용/이력	DB
무선 인증	·무선 접속 이력 정보	syslog
인사 시스템	·관리자 접속 이력 정보 ·관리자 수행 명령 이력	DB

Table 5. analysis of the collected logs

구분	보안 정책	로그생성여부
문서 보안	생성자 읽기/편집/해제/반출 권한부여	○
	저장/종료 시 강제 암호화	○
	복사/붙여 넣기 차단	○
	출력물에 대한 워터마킹 설정	×
	문서 열람 횟수 제어	○
통합 PC 보안	USB Read/Write 제어	○
	휴대폰 테더링 제어	○
	웹사이트 접속 모니터링	×
	출력물 워터마킹 및 이력 관리	○
	메신저 대화 내역 모니터링	×
시스템 접근 제어	계정 잠김 설정	○
	요일별 접근 시간 설정	×
	금지 명령어 설정	○
	접속 IP/MAC 설정	○
	telnet,ssh,ftp 등 접근 서비스 통제	○
DLP	음란물,해팅 사이트 통제	○
	특정 그룹에 대한 웹하드 허용	○
	메신저 대화 내역 모니터링	○
	외부 전송 메일 모니터링	○
	원격 제어 서비스 통제	○

이에 따르면 일요일 새벽에 중요 시스템에 접근하여 중요 문서를 PC로 가져와 해당 문서를 암호화 해제하는 위협 대응 시나리오를 만들어 적용할 경우 시스템 접근 제어에 요일별 접근 시간 설정이 안 되어 있어 해당 시나리오 이벤트가 발생하지 않는다. 또한 문서 보안의 출력물에 대한 이력 로그와 주요 시스템 접근 제어의 주요 서버 접근 이력을 가지고 통합 시나리오를 만들 경우 해당 이벤트가 발생하지 않는다. 왜냐하면 문서 보안에서는 해당 정책이 적용되지 않았고 통합 PC보안에 적용

되어 있어 단위 대응 시나리오를 재조정하여야 한다. 즉 해당 통합 시나리오를 통합 PC보안과 시스템 접근 제어와의 조합으로 변경하여야 한다. 이와 같이 각 단위 내부 통제 시스템들에 대한 로그 수집 분석은 매우 중요한 의미를 갖는다.

둘째 개인 정보 보호 처리 시스템인 인사 시스템에서 5W1H 중심으로 도출할 수 있는 단위 시나리오를 생성하였고 또한 DRM, DB 접근 제어 등 내부 보안 시스템들을 우회할 수 있는 위협 시나리오들을 도출하였다. 개인정보 처리 시스템인 인사 시스템에서 계좌 번호 등의 금융 정보를 포함하는 고객 정보에 대해 개인정보 취급자, 시스템 운영자, Blacklist기준과 사내망, 사외망의 where 관점, DB query, 다운로드, 변경, 인쇄의 How 관점 등 5W1H 중심으로 다양한 단위 시나리오를 도출하였다.

대상시스템	who	when	where	How	what	탐지기준	도출 단위 시나리오	비고
인사시스템	개인정보취급자	근무시간	사내망	Query	고객 정보	1000건 이상	개인정보 취급자가 근무시간에 DB Query 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사내망	Query	고객 정보	100건 이상	개인정보 취급자가 근무시간외 DB Query 탐지 기준 초과	
	개인정보취급자	근무시간	사외망	Query	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간에 DB Query 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사외망	Query	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간외 DB Query 탐지 기준 초과	
	개인정보취급자	근무시간	사내망	다운로드	고객 정보	500건 이상	개인정보 취급자가 근무시간에 다운로드 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사내망	다운로드	고객 정보	50건 이상	개인정보 취급자가 근무시간외 다운로드 탐지 기준 초과	
	개인정보취급자	근무시간	사외망	다운로드	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간에 다운로드 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사외망	다운로드	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간외 다운로드 탐지 기준 초과	
	개인정보취급자	근무시간	사내망	변경	고객 정보	500건 이상	개인정보 취급자가 근무시간에 변경 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사내망	변경	고객 정보	50건 이상	개인정보 취급자가 근무시간외 변경 탐지 기준 초과	
	개인정보취급자	근무시간	사외망	변경	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간에 변경 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사외망	변경	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간외 변경 탐지 기준 초과	
	개인정보취급자	근무시간	사내망	인쇄	고객 정보	1000건 이상	개인정보 취급자가 근무시간에 인쇄 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사내망	인쇄	고객 정보	100건 이상	개인정보 취급자가 근무시간외 인쇄 탐지 기준 초과	
	개인정보취급자	근무시간	사외망	인쇄	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간에 인쇄 탐지 기준 초과	
	개인정보취급자	근무시간외 시간	사외망	인쇄	고객 정보	1건 이상	개인정보 취급자가 사외에서 근무시간외 인쇄 탐지 기준 초과	
	시스템 운영자	근무시간	사내망	DB Query	고객 정보	1000건 이상	시스템 운영자가 근무시간에 DB Query 탐지 기준 초과	
	시스템 운영자	근무시간외 시간	사내망	DB Query	고객 정보	100건 이상	시스템 운영자가 근무시간외 DB Query 탐지 기준 초과	
	시스템 운영자	근무시간	사외망	DB Query	고객 정보	1건 이상	시스템 운영자가 사외에서 근무시간에 DB Query 탐지 기준 초과	

Fig. 6. Scenario derivation of personal system

특히 그림 6은 개인정보 취급자가 개인정보 처리 시스템인 인사 시스템에서 근무시간내 고객 정보를 500건 이상 다운로드하는 위협 등 다양한 행위들을 도출 할 수 있었다. 또한 중요 문서를 보호하기 위해 운영중인 DRM 보안 시스템의 경우 해제 권한자, 암호화 해제 건수, 암호화 해제 실패 건수, Logout 건수, 근무 시간 등의 5W1H중심으로 보안 시스템 우회 단위 시나리오들을 도출하였다.

그리고 선정 항목에 의해 적용 가능한 시나리오들을 선별하였다.

시나리오 구분		핵심 시나리오 선정					탐지기준
		유효성	위험연관성	산출용이성	자동화	선정 결과	
인사시스템 위협	개인정보 취급자가 근무시간에 다운로드 탐지 기준 초과	3	3	3	3	o	500건 이상
	개인정보 취급자가 사외에서 근무시간외 DB Query 탐지 기준 초과	0	3	3	3	x	1건 이상
	시스템 운영자가 근무시간에 다운로드 탐지 기준 초과	3	3	2	3	o	10건 이상
DRM 보안 시스템 우회	관리자가 근무시간에 암호화 해제 건수 탐지 기준 초과	3	3	3	2	o	50건 이상
	관리자가 근무시간외 암호화 해제 건수 탐지 기준 초과	3	3	3	2	o	10건 이상
	일반 임직원이 근무시간에 사외에서 암호화 해제 건수 탐지 기준 초과	0	3	2	2	x	1건이상

Fig. 7. Case of Scenario selection

그림 7은 선정된 핵심 시나리오들 예이다. 개인정보 취급자가 사외에서 근무시간외 DB Query 탐지 기준을 초과하는 시나리오인 경우 개인정보 취급자는 사외에서 접근하는 것이 원칙적으로 허용되지 않아 즉 고객 환경 유효성을 고려하여 선정에서 제외되었다.

선정된 핵심 시나리오들 중에서 개인정보 처리 시스템 위협 시나리오와 보안 시스템 우회 대응 시나리오를 통합하여 최적의 통합 시나리오들을 도출 적용하였다.

종합 시나리오	연관 단위 시나리오					
	개인정보처리시스템 위협 시나리오			보안 시스템 우회 대응 시나리오		
	설명	관련시스템	탐지기준	설명	관련시스템	탐지기준
개인 정보 취급자가 근무 시간에 인사시스템의 개인 정보를 다운로드하여 암호화 해제후 USB로 유출	개인 정보 취급자가 사내에서 근무 시간에 인사시스템의 개인 정보를 다운로드	인사시스템	500건 이상	관리자가 근무 시간에 암호화 해제 건수 탐지 기준 초과	DRM	50건 이상
				관리자가 근무 시간에 USB 쓰기 건수 탐지 기준 초과	PC 보안	50건 이상
개인 정보 취급자가 근무 시간 외에 인사시스템의 개인 정보를 다운로드하여 암호화 해제후 USB로 유출	개인 정보 취급자가 사내에서 근무 시간 외에 인사시스템의 개인 정보를 다운로드	인사시스템	50건 이상	관리자가 근무 시간외에 암호화 해제 건수 탐지 기준 초과	DRM	10건 이상
				관리자가 근무 시간외에 USB 쓰기 건수 탐지 기준 초과	PC 보안	10건 이상
개인 정보 취급자가 근무 시간에 인사시스템의 개인 정보를 조회하여 암호화 해제후 USB로 유출	개인 정보 취급자가 사내에서 근무 시간에 인사시스템의 개인 정보를 조회	인사시스템	1000건 이상	관리자가 근무 시간에 암호화 해제 건수 탐지 기준 초과	DRM	50건 이상
				관리자가 근무 시간에 USB 쓰기 건수 탐지 기준 초과	PC 보안	50건 이상
개인 정보 취급자가 근무 시간 외에 인사시스템의 개인 정보를 조회하여 암호화 해제후 USB로 유출	개인 정보 취급자가 사내에서 근무 시간 외에 인사시스템의 개인 정보를 조회	인사시스템	100건 이상	관리자가 근무 시간외에 암호화 해제 건수 탐지 기준 초과	DRM	10건 이상
				관리자가 근무 시간외에 USB 쓰기 건수 탐지 기준 초과	PC 보안	10건 이상
개인 정보 취급자가 근무 시간에 인사시스템의 개인 정보를 다운로드하여 암호화 해제후 메신저로 유출	개인 정보 취급자가 사내에서 근무 시간에 인사시스템의 개인 정보를 다운로드	인사시스템	500건 이상	관리자가 근무 시간에 암호화 해제 건수 탐지 기준 초과	DRM	50건 이상
				관리자가 근무 시간에 메신저로 파일 첨부 시도 탐지 기준 초과	DLP	1건 이상
개인 정보 취급자가 근무 시간 외에 인사시스템의 개인 정보를 다운로드하여 암호화 해제후 메신저로 유출	개인 정보 취급자가 사내에서 근무 시간 외에 인사시스템의 개인 정보를 다운로드	인사시스템	50건 이상	관리자가 근무 시간외에 암호화 해제 건수 탐지 기준 초과	DRM	10건 이상
				관리자가 근무 시간외에 메신저로 파일 첨부 시도 탐지 기준 초과	DLP	1건 이상
개인 정보 취급자가 근무 시간에 인사시스템의 개인 정보를 조회하여 암호화 해제후 메신저로 유출	개인 정보 취급자가 사내에서 근무 시간에 인사시스템의 개인 정보를 조회	인사시스템	1000건 이상	관리자가 근무 시간에 암호화 해제 건수 탐지 기준 초과	DRM	50건 이상
				관리자가 근무 시간에 메신저로 파일 첨부 시도 탐지 기준 초과	DLP	1건 이상
개인 정보 취급자가 근무 시간 외에 인사시스템의 개인 정보를 조회하여 암호화 해제후 메신저로 유출	개인 정보 취급자가 사내에서 근무 시간 외에 인사시스템의 개인 정보를 조회	인사시스템	100건 이상	관리자가 근무 시간외에 암호화 해제 건수 탐지 기준 초과	DRM	10건 이상
				관리자가 근무 시간외에 메신저로 파일 첨부 시도 탐지 기준 초과	DLP	1건 이상

Fig. 8. Example of Integration scenario derived

그림 8은 통합 로그 관리 시스템 확장 모델에서 도출된 통합 시나리오 사례들이다. 그리고 추가적으로 APT 등의 최신 공격 대응, 일반적인 내부 정보 유출 패턴과 고객 IT 문화를 반영하여 시나리오를 분석했다. 예를 들면 내부직원은 업종 특성상 이직율이 높은 상황이었다. 타 산업대비 잦은 임직원 퇴직으로 인원에 대한 통제가 필요했다. 그래서 퇴직예정자들을 중점 관리 대상으로 좀더 상세 관리할 수 있는 시나리오를 생성하여 내부 정보 유출 위협에 대응 하였다.

3. Evaluation by Comparing existing defense system with the expansion model

11년 4월 N사 전산망 마비, 14년 1월 카드사 개인 정보 유출 사고 등 주요 공격 사례들의 위협들을 기반으로 기존 대응 시스템과 확장 모델을 평가하여 통합 로그 관리 시스템 확장 모델의 우수성을 평가하였다. 표 6 N사의 경우 유지 보수 업체 직원의 노트북이 악성 코드에 감염되어 다수 시스템들의 etc 등 중요 파일들이 삭제되는 위협들이 발생했다. 기존 대응 시스템에서는 중요 파일 삭제 행위와 연결 행위 공격을 탐지할 수 없었다. 그러나 본 확장 모델에서는 특정 사용자의 rm, dd 등

금지 명령 수행 대응 시나리오를 적용하여 탐지할 수 있고 또한 악성코드가 감염된 사용자를 탐지하는 백신 감지 시나리오와 해당 감염 사용자가 주요 서버에서 삭제 등의 금지 명령어를 수행하는 것을 탐지할 수 있는 시스템 접근 제어 금지 명령 시나리오를 상호 연계 통합하여 연결 행위 공격을 탐지 할 수 있다.

Table 6. Comparison existing defense system with the expansion model by cases of main security attacks

주요 보안 공격 사례		위협	기존	확장 모델
11년 4월 N사 전산망 마비	악성 코드에 감염된 관리자 PC로 내부망 접근하여 주요 서버 파괴	주요 서버들 운영에 필요한 중요 파일 삭제 행위	파일 삭제 행위 인지 못함	rm, dd 등 금지 명령 수행 행위 대응 시나리오 적용으로 탐지
		악성 코드감염 후 주요 서버 접속하여 파일을 삭제하는 연결 행위 공격	상호 연계성 탐지 불가	악성 코드에 감염되어 주요 서버에 금지 명령을 수행하는 연결 행위 공격의 사용자를 통합 시나리오를 적용하여 탐지(백신 감지 시나리오와 시스템 접근 제어 금지 명령 시나리오 통합)
12년 2월 S사 개인정보 유출 사고	IT 센터 외주 개발 업체 직원이 개인정보 10만 4천건 USB로 불법 유출	개인 정보를 USB로 유출하는 불법 행위	USB 불법 행위 통제 미흡	주민번호, 성명 등 개인 정보를 포함한 중요 문서를 1일 임계치 이상 USB로 불법 유출하는 행위를 PC 보안 시스템 시나리오에 적용하여 탐지
		중요 시스템 접근 후 개인 정보를 USB로 유출하는 복합 공격 위협	복합 공격 탐지 불가	외주 직원이 중요 시스템에 불법 접근 하는 행위를 탐지하는 시스템 접근 제어 시나리오와 중요 문서 1일 임계치를 초과하여 USB 사용시 탐지하는 PC보안 시스템 시나리오를 통합하여 복합 공격 대응
14년 1월 카드사 개인정보 유출 사고	외주 직원이 각각의 회사 전산망에 접근 개인정보 1억 580만건 대량 유출	개인 정보 처리 시스템 불법 접근	비허가자 개인정보 처리 시스템 접근 탐지 미흡	허용되지 않은 사용자 IP에서 불법 접근하여 다운로드하는 행위를 탐지하는 단위 시나리오를 적용하여 탐지 가능
		개인 정보 처리 시스템 접근후 개인 정보를 USB로 유출하는 불법 연계 행위 위협	불법 연계 행위 탐지 불가	계좌 번호,카드 번호 등 개인 신용 정보를 불법 다운로드하는 행위를 탐지하는 개인정보 처리 시스템 위협 시나리오와 해당 개인 정보 파일을 USB 로 1일 임계치를 초과하여 과다 사용하는 사용자를 탐지하는 PC 보안 시스템 우회 시나리오를 통합하여 탐지

마지막으로 표 7의 기존 관련 선행 연구와 구축 사례 비교를 통해 기존 대비 본 모델의 우수성을 평가하였다. 이전에는 방화벽, IPS 등의 경계 방어 시스템만 운영되면서 개별적으로 이벤트들만 관리한다. 내부 중요 정보가 유출되는 경우 사고와 관련된 이벤트가 없거나, 사고이후에도 담당자가 인지하지 못할 수 있다. 복합 공격에 대한 연결 고리를 찾을 수 없는 단순·격리된 저장이며 사용자 행위 중심의 상호 연계 분석이 아니라 OSI 3~4 계층 네트워크 패킷 중심의 탐지이기 때문이다. 한편 통합 로그 관리 시스템 확장 모델을 통한 통합 시나리오 분석은 다수 계층에 걸쳐 컨텐츠와 행위 중심으로 상호 연계 분석을 수행하기 때문에 내부 정보 유출과 APT 등의 알려지지 않은 공격에 능동적으로 대응할 수 있다. 그리고 개인정보 처리 시스템 공격 대응 시나리오와 체계적인 통합 시나리오 발굴 방법이 없었던 기존의 관련 연구 대비 5W1H 기준으로 개인 정보 처리 시스템 위협 대응 시나리오를 도출하고 보안 시스템 우회 시나리오와 상호 연계하여 체계적으로 통합 시나리오를 도출하는 본 모델은 APT, 내부 정보 유출 등의 복합 공격 탐지에 보다 더 효과적으로 대응할 수 있다.

Table 7. Evaluation by cases and previous related studies

평가 항목			기존	확장 모델
구축 사례	수집 로그 분석	대상 로그	OSI 3~4계층 시그니쳐 로그	OSI 3~7계층 시그니쳐/컨텐츠 로그
		로그 수집	네트웍 중심 정형 데이터 수집	사용자 행위 중심 비정형/정형 데이터 수집
	시나리오 도출		단순 시나리오로 복합공격에 취약	개인정보 처리 시스템과 보안 시스템 우회에 대응할 수 있는 체계적인 통합 시나리오 도출
	탐지 대응	APT 공격	경계방어 시스템 중심으로 APT에 취약	사용자 행위 중심의 상호 통합 분석이어 APT 탐지
		내부 정보 암호화 해제 후 유출	개별 보안 이벤트 수집으로 상호 연계 탐지 불가	문서보안 1일 50건이상 암호화 해제후 관련 파일들을 50건이상 USB로 유출하는 통합 시나리오로 탐지
기존 관련 연구 비교			개인정보 처리 시스템위협 시나리오 없음	5W1H기준으로 개인정보 처리 시스템 위협 대응 시나리오 도출 가능
			보안 이벤트 수집시 유효성 검증 미흡	보안 로그 수집시 분석 단계에서 로그 유효성 검증 수행
			체계적인 통합 시나리오 발굴 방법 없음	보안 시스템 우회와 개인정보 처리 시스템 위협 시나리오를 상호 연계하여 체계적으로 통합 시나리오 도출

V. Conclusions

다양한 유무선 매체와 사물인터넷의 출현은 고객의 IT 비지니스를 더욱 확대하고, 그로 인해 발생되는 보안 위협을 통하여 해커의 공격 기술은 날로 고도화, 지능화 되고 있다. 또한 은행, 카드사 등의 금융권 보안 사고들은 내부자의 고객 정보 및 내부 정보 유출로 통합적인 내부 통제의 필요성을 다시 한번 요구하고 있다. 이와 같이 통합 로그 관리 시스템 확장 모델은 내부 정보 유출 위협 감지와 알려지지 않은 공격에 능동적으로 대응할 수 있다.

본 연구에서는 융·복합 환경에 적합한 통합 로그 관리 시스템의 특징 및 구성과 동향에 대해 분석하고 이를 토대로 통합 로그 관리 시스템 확장 모델을 설계하였다. 또한 기존 관련 선행 연구와 구축 사례 비교를 통해 통합 로그 관리 시스템 확장 모델의 효과를 평가할 수 있었다.

향후 전자 금융 거래시 사용자의 단말기 정보, 접속 정보, 거래 내용, 거래 패턴 등의 정보들을 종합적으로 판단하여 불법 거래를 탐지하는 이상 금융 거래 탐지 시스템(Fraud Detection System)구축시 통합 로그 관리 시스템 확장이 어떻게 활용될 수 있는지 연구할 필요가 있다. 또한 다양한 사이트에 사례 기반의 적용 평가를 확장하여 효과성 입증관련 통계적인 연구를 수행해 보는 것도 필요할 것이다.

REFERENCES

[1] Jerry Shenk, “Learning from Logs: SANS Eighth Annual 2012 Log and Event Management Survey Results”, SANS, pp. 2-3, May 2012.

[2] GiHyouk Lee, “A Study on the implementation of leak prevention system through internal information leaks symptom analysis”, Journal of The Korea Institute of Information Security & Cryptology, Vol. 19, No. 3, pp. 70-73, June 2009.

[3] NIST FIPS PUB 800-92, Guide to Computer Security Log Management, pp. 2-32, Sep. 2006.

[4] Jae Chan Yoo, “A Study on the Protection for Corporation Information Using Scenario Technique,” The Graduate of SungKyunkwan University, pp. 14-16, August 2012.

[5] Kelly M, Mark Nicolett, Oliver Rockford, “Magic Quadrant for Security Information and Event Management”, Gartner Group, pp. 2-8, June 2014.

[6] Donghan Kim, “SIEM Trend to the intelligent Log management platform in the Big Data Environment ”, National IT Industry Promotion Agency, Weekly Technology Trends, pp. 5-8, Aug. 2013.

[7] mcafee, *http://www.mcafee.com/us/resources/reports/rp-when-minutes-count.pdf*

[8] Soondeok Yu, “Security response technology in the Big Data Environment ”, National IT Industry Promotion Agency, Weekly Technology Trends, pp. 9-11, Sep. 2013.

[9] EMC, *http://www.emc.com/security*

[10] IBM, *http://www-03.ibm.com/software/products/en/qradar-siem*

[11] Ki-Soon Yu, and Sul-Hwa Im, “Development directions and technology trends of SIEM”, Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 6, pp. 91-93, Dec. 2013.

[12] Gartner, *http://blogs.gartner.com/ramon-krikken/2012/05/22/siem-future-would-you-like-some-context-with-that/*

[13] Jong-Hyun Kim, and SeonHee Lim, “Technical Trends of Cyber Security with Big Data”, Electronics and Telecommunications Research Institute, 2013 Electronics and Telecommunications Trends, pp. 20-23, June 2013.

Authors

DongSung Im received the B.S. degree in Electronics Engineering from INha University, Korea, in 1996.

He received the M.S. degree in Interdisciplinary program of Information Security from Chonnam National University, Korea, in 2015.

Mr. Im is currently a Security Engineer in AhnLab. He is interested in information security consulting, system and network security.

Yongmin Kim received the Ph.D. degree in Computer Science and statistics from Chonnam National University, Korea, in 2002,

Dr. Kim is currently a Professor in the Department of Electronic Commerce, Chonnam National University.

He is interested in electronic commerce security, system and network security.