복합시나리오를 이용한 IMP 기반 보안관제 모니터링 수준향상 방안에 관한 연구

권대혁*
*고려대학교 컴퓨터정보통신대학원
e-mail : goofyno7@korea.ac.kr

An Improving the Information Protection Level by IMP(Integrated Management Platform) based Hybrid Scenario

Dae-Hyeok Kwon*
*Dept. of Computer Information and Communication, Korea University

요 약

IT 산업의 발전과 함께 Big-Data 와 보안은 빠른 속도로 발전하고 정보보호를 위해 다양한 시스템을 구축하는 것보다는 이를 연계하고 활용하는 것이 중요한 시대가 도래하였다. 한 기업이 가지고 있는 기업정보유출사고 등 다양한 해킹공격 또한 꾸준하게 증가되고 있다. 더불어 경제적· 사회적인 손실이 증가되면서 국가 및 기업 상위 감사 기관은 정보보호 관련 법· 제도를 제정하고 이를 강화하여 개정 하고 있다. 하지만, 물리적, 관리적, 기술적으로 연계된 통합 보안 관리 체계가 제대로 구현되지 않는다면 다양한 취약점을 통하여 기업 정보는 언제든 유출 될 수 있다. 본 논문에서는 기업에서 기 운영중인 정보보안 솔루션과 물리보안 솔루션이 효과적으로 통합 보안 관제가 가능한 IMP 플랫폼 구성설계 방안과 불법 침입 및 보안 사고 탐지를 위한 복합시나리오 설계 방안을 제시하여 실 적용 효과를 알아보고 향후 연구 방향을 제시하고자 한다.

1. 서론

2012 년 종사자 수 5 인 이상의 네트워크가 구축된 5,000 개 민간기업을 대상으로 정보화 투자 대비 정보보호 지출비율에 대해서 조사한 결과 지출 비율이 1%미만이거나 지출이 없는 경우가 전체의 86.9%로 나타났다. [1,2] 또한 기업의 물리적 보안 설비 구축과 실시간 모니터링을 실시하려는 기업은 매우 드문 것이 현실이다.

상대적으로 규모가 큰 조직의 경우 조직의 정보보안 수준향상을 위해 외부 보안전문 업체를 통해 수준진단을 받거나, 내부적으로 정보보안 전문 인력을 채용하여 “정보보호팀”을 구성하고 사고대응 체계를 마련하고 물리보안 설비 또한 기업 정보보호를 위한 투자가 이루어지는 기업도 존재한다.

하지만, 이렇게 구축된 정보보안 솔루션과 물리보안 솔루션에 대하여 통합 연계 분석 및 실시간 모니터링을 하지 않고 전문 요원의 분석에 의존함으로써 침해사고에 대한 정확한 분석과 완결적 사고 처리가 불가능함으로써 발생하는 비용과 시간이 소요되고 있다. 이러한 문제점을 해결하기 위하여 정보보안 설비와 물리적 보안 설비에서 발생되는 데이터를 수집 분석하는 통합관리플랫폼 즉, IMP(Integrated Management Platform)를 구현하고 수집된 정보보안 · 물리보안 솔루션의 데이터를 복합시나리오 기반으로 구성/분석/대응하는 통합 모니터링 방안에 대하여 연구하였다.

본 논문의 2 장에서는 행위 기반 시나리오 구성 방안과 융합보안관제 환경 구축에 관한 관련 연구를 알아보고 3 장에서는 제안하고자 하는 모델에 대하여 기술한다. 4 장에서는 논문의 결과와 기대효과에 대하여 기술한다.

2. 관련연구

2.1 정보 유출 시나리오 설계 방안 연구

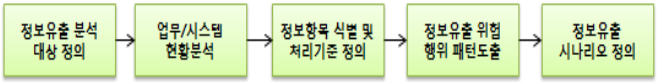
사용자 행위 Modeling 을 이용한 내부정보유출 방지 시나리오 설계방안에 관한 연구[7]에서 제안한 설계 방안은 <표 1>과 같이 4W2H 기준 정보에 의한 사용자 행위 Modeling 기법을 이용하고 있다.

<표 1> 4W2H 에 의한 사용자 행위 Modeling

Who	임직원	계약직	파트너 직원	개인정보 권한자	퇴직자	예정자	휴직자
When	평일 주간	평일 야간	평일 점심	휴일 주간	휴일 야간	접속시간 & 접속 위치	
Where	외부 원격 접속	내부 사내망	DMZ Zone	IP Address	윈도우 접속 계정		
What	개인 정보	고객 정보	영업 정보	기술 정보	매출 현황	인사 정보	원가 정보
How	암호화 해제	다운 로드	열람	이메일 발송	출력	우회 접속	계정 도용
How Much	암호화 해제 횟수	메일 발송 횟수	업로드 Traffic 증가	DB 접근 횟수	DB 쿼리 횟수	USB 복사 횟수	우회 접속 횟수

<표 1>의 4H2W 는 Who, When, Where, What, How, How much 의 각 component 기반으로 시나리오를 설계하는 것이다.

기업의 업무 환경에서 실효성 있는 기업 정보 유출 시나리오 설계 순서는 (그림 1) 과 같다.

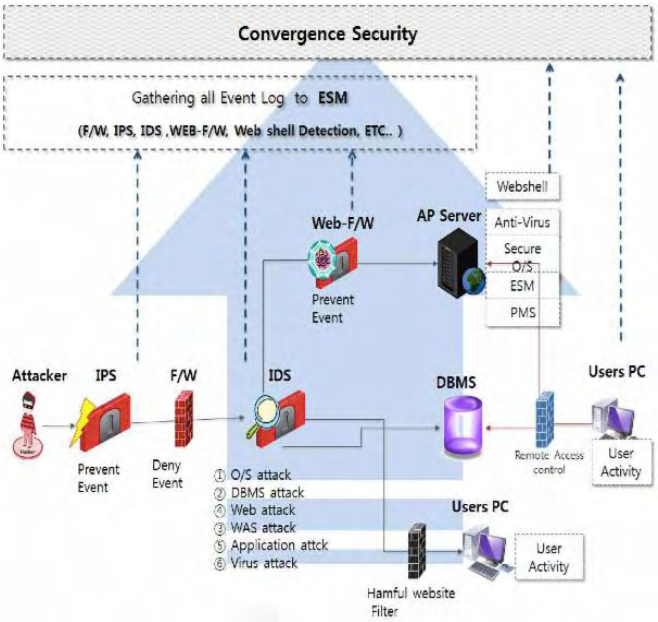


(그림 1) 정보 유출 시나리오 설계 단계

가장먼저 정보유출 분석대상을 정의하고, 업무/시스템 현황분석을 통해 정보항목 식별 및 처리기준을 정의한다. 그리고 정보유출 위험 행위 패턴을 도출하여, 시스템에 적용 가능한지 검증 후, 정보유출 시나리오로 정의 한다. 본 연구의 4W2H 에 의한 사용자 행위 Modeling 이 가능하였고 실효성 있는 정보유출 시나리오 설계 프로세스를 정의함으로써 통합보안 관제를 위한 복합 시나리오 Modeling 으로 확장할 수 있었다.

2.2 융합보안관제환경 구축 및 활용 방안 연구

융합보안관제환경을 위한 아키텍처 구축 및 활용 방안에 대한 연구[8]에서는 수십여 종의 보안솔루션을 융합하고 연관분석하는 방법과, APT 공격을 인지하는 기법과 방법, 정보자산의 정보와 보안이벤트를 통합하고 모니터링하는 방안을 (그림 2)와 같이 구성하였다.



(그림 2) 융합보안 환경 구성

(그림 2)는 네트워크, 원격접속통제, 데이터베이스보안, 호스트보안, 보안감사, 서버 및 사용자 활동정보, 시스템이벤트 로그, 로그관리시스템으로 전사에서 발생되는 정보보안 솔루션의 로그를 수집/분석하고 이를 기반으로 APT 공격 인지 방법을 구현하였다.

3. 시스템 구현

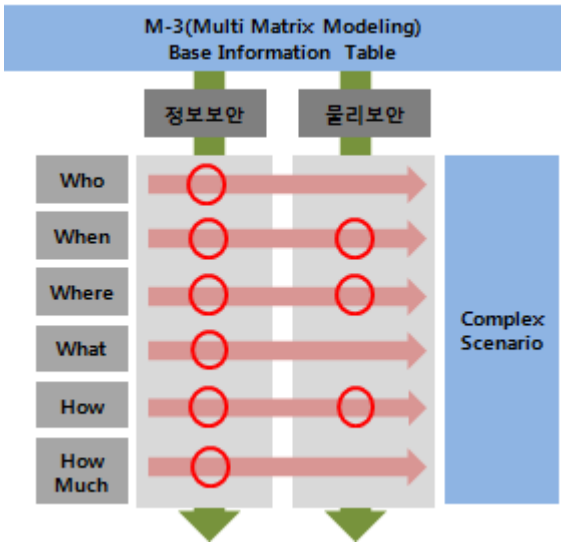
3.1 구현 방법

본 연구에서는 4W2H 에 의한 사용자 행위 Modeling 기법을 기반으로 M-3 (Multi Matrix Modeling)로 확장하여 복합시나리오 모델링 설계 방안을 제시하였다.

또한, 네트워크, 원격접속통제, 데이터베이스보안, 호스트보안, 보안감사, 서버 및 사용자 활동정보, 시스템이벤트의 정보보안 로그만을 수집하고 관리/분석하는 환경 모델에서 CCTV, 출입통제, MDM 등 물리보안 솔루션까지 동시 수용 가능한 IMP(Integrated Management Platform)기반 보안관제 모니터링 플랫폼 모델을 제시하고 구현하였다.

3.2 복합 시나리오 모델 제안

관련 연구와 같이 다양한 정보 유출의 경로를 차단하기 위하여 기업은 복수의 정보보안 솔루션과 물리보안 솔루션을 구축하여 운영 중에 있다.



(그림 3) M-3(Multi Matrix Modeling)설계기법

기업 내부에서 운영중인 정보보안 솔루션과 함께 물리보안 솔루션을 관련연구의 4W2H 로 정의하고 (그림 3)의 M-3 설계 기법을 통하여 정보보안과 물리보안을 연계한 통합 시나리오를 설계하였다.

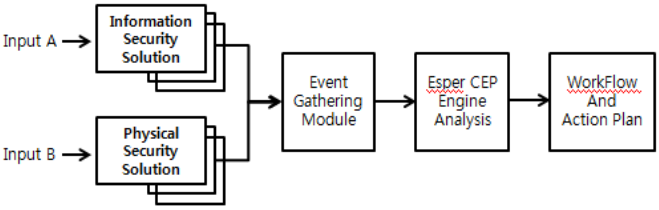
<표 2> M-3 기반 시나리오 설계 예시

Who : 신원 불명의 직원(CCTV) When : 휴식 시간 (CCTV, DLP) Where : 1 층 출입문 스피드게이트를 불법 통과하여 7 층에서 (CCTV, 출입보안) What : 회사 기밀정보를 (DLP,DRM) How : USB 저장매체 복사와 이메일 발송 (DLP) How Much : 5 분동안 100MB 3 회 복사, 5 분동안 100MB 3 회 이상 이메일 발송 (DLP)

예를 들어, “신원 불명의 직원이 휴식 시간을 이용하여 출입문 스피드게이트를 불법 통과한 후 7 층

의 잠금이 해제된 내부 직원 PC 에 접속 한 후 회사 기밀 정보를 외부 USB 저장매체로 5 분 동안 3 회 이상 100MB 이상 파일 복사를 시도하고, e-mail 로 5 분 동안 100MB 이상의 파일을 3 회 이상 파일을 발송 한 경우" 는 <표 2>와 같이 구현되었다.

물리보안 솔루션을 통한 침투 단계의 감시/추적 이벤트와 정보보안 솔루션에서 탐지된 접근/추적/유출 이벤트를 융합한 복합시나리오의 처리 프로세스는 (그림 4)과 같다.

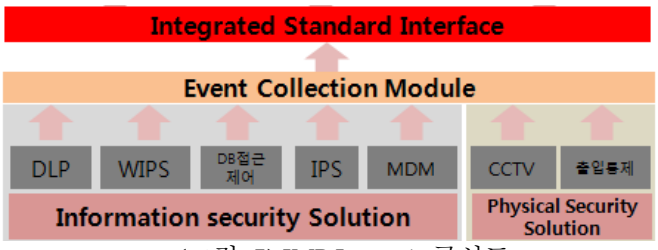


(그림 4) 복합시나리오 프로세스 구성도

복합시나리오는 IMP 플랫폼 기반 분석을 통해 관제요원이 처리 해야 할 세부 워크플로우(Work flow)와 Action Plan 을 제공한다.

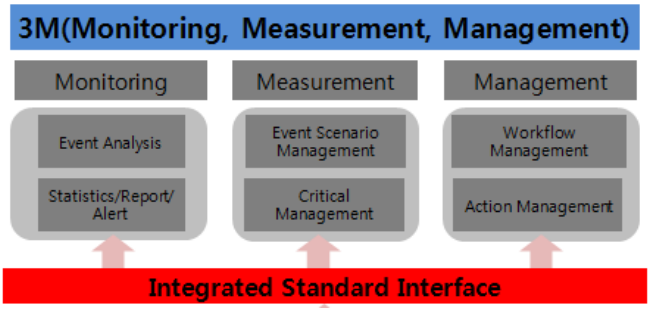
3.3 IMP 플랫폼 모델 구성 제안

IMP 는 정보보안솔루션과 물리보안 솔루션에서 발생되는 모든 이벤트 로그 수집이 가능하도록 구성되어야 한다. 실시간 이벤트 연동 수집을 위해서는 네트워크 보안 장비연동에 사용되는 SNMP, SFlow, Syslog, NTP, 텔넷, Trap 등 다양한 프로토콜을 지원 해야 한다. 또한 물리보안 솔루션에서 발생되는 다양한 Signal, MAC 정보,인증 정보, 위치정보, Time 등 다양한 프로토콜과 다양한 데이터 수집 한다. 이 통합 표준 인터페이스(Integrated Standard Interface) 모듈은 개별 솔루션에서 수집된 자료를 Layer 2 의 분석/관리/통계 모듈로 전달하고, Layer 1 의 표준 구성도는 다음과 같다.



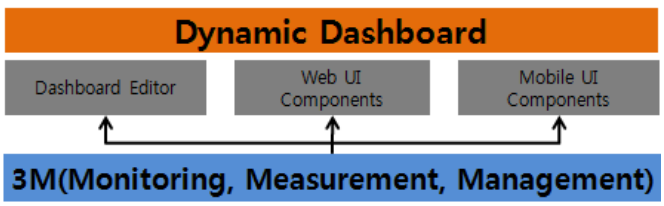
(그림 5) IMP Layer 1 구성도

(그림 5)의 Layer 1 은 정보보안 솔루션과 물리보안 솔루션들이 가지고 있는 사설 Protocol 을 플랫폼으로 연동하기 위하여 ECM(Event Collection Module)이 필요하다. ECM 은 신규로 연동되는 장비(DLP, WIPS, IPS, MDM, DB 접근제어, CCTV)들의 데이터 중 연계 분석에 필요한 데이터를 필터 후 수집하기 위하여 최초 1 회 Base meta-data table 에 기준 Value 를 정의 한다. 이후 개별 장비들의 이벤트를 수집하고 표준화하여 ISI(Integrated Standard Interface)로 전달한다. ISI 는 수집된 데이터를 실시간 분석, 모니터링, 이벤트 관리, 워크플로우 및 활동을 관리하는 Layer 2 로 전달 한다. Layer2 의 표준 구성은 다음과 같다.



(그림 6) IMP Layer 2 구성도

(그림 6)는 ISI 모듈로부터 표준화된 데이터를 3M(Monitoring, Measurement, Management) 모듈에서 사용 될 수 있도록 ISI_Table 에 실시간으로 저장된다. ISI 테이블에 저장된 데이터를 기반으로 Monitoring 모듈에서는 수집된 데이터를 Esper CEP(Complex Event Processing) Engine Query 통하여 "2. 융복합 시나리오 연구" 항목에서 도출된 시나리오를 이 모듈을 통해 연계분석하여 실제 공격으로 판단되는 복수의 이벤트를 복합이벤트를 생성한다. 이렇게 생성된 이벤트는 Complex_Event_table 에 저장되고 리포팅, Alert 등 모니터링에 필요한 항목들로 확장 활용 가능하다. Measurement 모듈에서는 Esper Query 를 추가/수정/저장한다. 이 Esper Query 를 통해 추가되는 복합 시나리오를 이벤트로 발생시키기 위한 작업이 가능하고 임계치 관리(Critical Management)가 가능하다. Management 모듈에서는 저장된 각 복합시나리오에 따라 보안관제 요원의 Workflow 를 정의 할 수 있고 관제요원은 해당 이벤트 발생 시 정의된 Workflow 대로 침해사고 처리 대응을 할 수 있다. 또한 Action Management 를 통해 단일솔루션에 Order 전달이 가능하다. 예를 들어 건물의 특정 층에 이벤트가 발생된 경우 해당 층의 CCTV 를 Control 하여 사고 발생 지역을 감시 할 수 있다. Layer 2 구성 모듈을 통해 통합 관제/관리/통제/대응이 가능하다. Layer 2 모듈을 기반으로 Dynamic Dashboard 가 Layer3 모듈이 다음과 같이 구성된다.



(그림 7) IMP Layer 3 구성도

(그림 7)의 Lay 3 은 3M 모듈에서 분석/저장/표준화 된 데이터를 기반으로 User Interface 를 효과적으로 구성하기 위한 모듈로 구성된다. Dashboard Editor 는 IMP 통합 보안 관제 UI 를 관리자가 능동적으로 편집 구성할 수 있는 기능을 제공한다. Web UI Components 는 인터넷 웹 페이지 접속을 통한 관제 모니터링을 위한

기능을 제공하며 Mobile UI Components 는 Mobile 통합 관제를 위한 기능을 제공하는 모듈로 구성된다.
Layer 4 인 SSM(Standard Service Module)은 Layer 1 에서 Layer3 계층까지의 단계를 통해 분석되어 표준화된 데이터를 기반으로 통합보안관제 모니터링이 가능한 서비스 모듈로 구성된다.

4. 결론 및 기대효과

본 논문에서는 기업의 네트워크 정보보안 침투 경로와 물리적 침투경로를 연계한 M-3 기반 복합시나리오 설계 방안과 IMP 통합보안 관제 플랫폼 모델 구성을 제시하였다.

이렇게 구현된 모델을 K 기업에 적용하여 과거 3 년간 발생 된 정보보안 장비와 물리보안 장비의 운영 비용, 사고처리 시간, 보안성 변동 비율을 비교 분석한 결과 비용은 5.4%, 사고처리시간은 20%, 보안성은 12% 증가될 것으로 분석 되었고, 정보보안 솔루션과 물리보안 솔루션을 각각 관제, 운용하는 것 보다 통합 관제하는 경우에 비용,시간,보안성 측면에서 효과적이라는 결론이다.

향후에는 에너지, 인빌딩 등 기업 정보보안 설비와 건물 에너지 관리 솔루션까지 통합 관리할 경우에 얻어지는 효과에 대해서도 연구가 필요하다.

참고문헌

[1] 한국인터넷진흥원, “2010 정보보호 실태조사(기업편),” 2011 년 5 월
[2] 안전행정부, “2013 국가정보보호백서,” 2013 4 월.
[3] 장항배, “내부정보유출방지 관점에서의 보안수준 평가”, 정보보호 심포지엄, 한국정보보호진흥원, 2009
[4] 박성주, “개인정보 유출방지를 위한 SRI(Security Risk Indicator)기반 모니터링 시스템 개발”,학위논문,2012
[5] 윤인수,”내부자에 의한 정보유출 방지를 위한 보안시스템 구축에 관한 연구”,학위논문,2007
[6] 이대성, 김재성, 김귀남, “정보유출 방지 연구기술 동향”, 정보보호학회 논문지, 제 20 권, 제 1 호, 2010
[7] 한국정보처리학회, “제 40 회 추계학술발표대회 프로그램”, “사용자 행위 Modeling 을 이용한 내부정보유출 방지 시나리오 설계방안에 관한 연구”, 정보처리학회 학술지,
[8] 황동욱, 이상훈, “융합보안관제환경을 위한 아키텍처 구축 및 활용 방안에 대한 연구”, 학위논문, 2014 년 4 월.