통합보안관리시스템에 대한 평가항목 도출

김선주*, 이공선*, 신석규*
*한국정보통신기술협회
e-mail : sunjoo, kslee, skshin@tta.or.kr

A Derivation of Evaluation Item about Enterprise Security Management

Seon Joo Kim*, Kong Seon Lee*, Seok Kyoo Shin*
*SQEC, TTA

요 약

통합보안관리시스템(Enterprise Security Management)은 기업의 보안 정책을 기반으로 다수의 보안 시스템을 중앙에서 통합관제, 운영, 관리를 지원하는 시스템이다. 국내의 경우 정보보호시스템에 대한 보안성 평가는 국제공통평가기준을 근거로 평가 및 인증이 이루어지고 있는 반면, SW 품질관점에서의 ESM 에 대한 평가 방안에 대한 연구는 미미한 실정이다. 이에 따라 본 논문에서는 SW 품질관점에서 ESM 에 대한 평가항목을 제안하고자 한다.

1. 서론

현대의 기업들은 인터넷을 기반으로 다양한 IT 서비스를 제공하고 있으며, 각각의 IT 서비스를 위해 최적의 시스템을 도입하여 관리, 운영하고 있다. 또한, 안전한 IT 서비스를 위해 기업은 방화벽(Firewall), 침입탐지 시스템(IDS; Intrusion Detection System), 침입 차단 시스템(IPS; Intrusion Protection System), 백신 프로그램 등을 도입하여 운영하고 있다. 기업의 IT 서비스가 증가함에 따라 기업의 전산 담당자가 관리 부담이 증가하고 있으며, 기업의 보안 정책을 시스템에 효율적으로 적용할 필요성이 대두 되었다. 이러한 보안 장비들을 통합 관리하기 위해 통합보안관리시스템(Enterprise Security Management, 이하 'ESM')이 출현하였다.

ESM 은 보안 관제 분야에서 다양한 이기종 시스템을 통합 관리하고, 운영하기 위해서 매우 중요한 역할을 하고 있다. 국내의 경우 ESM 도입을 위한 한국정보보호진흥원에서 ISO/IEC 15408 에 기반하여 수행하는 정보보호 제품에 대한 보안성 평가가 있지만, 본 논문에서는 소프트웨어 품질과 관련된 국제표준인 ISO/IEC 9126, 12119 를 기반으로 하여 ESM 에 대한 6 개의 품질특성별(기능성, 사용성, 신뢰성, 효율성, 유지보수성, 이식성)로 평가항목을 도출하였다.

2. 통합 보안 관리 시스템(ESM)

ESM 은 기업의 보안 정책을 기반으로 다수의 이기종 시스템을 효율적으로 관리하고, 각종 보안 솔루션, 네트워크 장비와 연동하여 효율적인 시스템 운영 및 관리를 지원하고, 기업의 자산에 대한 기밀성, 무결성, 가용성을 지원하기 위한 통합 보안 솔루션으로 다양한 보안 시스템과 네트워크 장비를 모니터링하고, 다양한 종류의 보안 솔루션을 하나로 통합 관리가 가능하다. 이러한 통합 보안 솔루션은 기업의 보안 정책에 맞도록 전체 IT 시스템을 적절히 통제할 수 있는 고도화된 솔루션에 대한 요구가 높아지고 있으며, 일부 공공기관을 비롯하여 금융기관 등이 ESM 도입에 적극적으로 나서고 있다.

2.1 ESM 구조

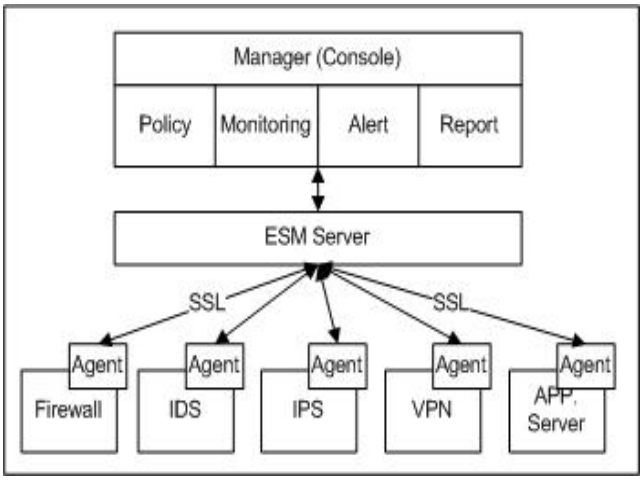
ESM 은 기업의 보안 정책에 따라 네트워크와 시스템을 관리하고 운영하는 시스템이다. ESM 을 구축하는 기업의 IT 시스템 운영 방식이나 보안 정책에 따라 ESM 구조가 다르다. 그러나, 일반적으로 콘솔(Console), ESM 서버(Server), 에이전트(Agent)로 구성되며, 각 구성요소간 관계는 그림 1 과 같다.

콘솔은 이벤트 수집 규칙 설정, 설정에 따른 이벤트 모니터링, ESM 서버에 저장된 이벤트를 분석하여 시스템 관리자에게 경고 메일이나 SMS 메시지를 보내는 경보 기능, 보고서 작성 기능 등을 가진 프로그램이다.

ESM 서버는 콘솔에서 정의한 이벤트 수집 규칙에 의해 각각의 에이전트로부터 데이터를 수집하는 기능을 가진 서버 프로그램이다.

에이전트는 방화벽, 침입 차단 시스템, 침입 방지 시스템, 가상사설통신망(VPN), 일반 응용 프로그램 서버에 설치되고, 각각의 장비에서 발생하는 각종 이벤트 수집 규칙에 따라 이벤트를 ESM 서버로 전달하고, 콘솔의 통제를 받는 프로그램이다.

ESM 서버와 각각의 에이전트, 콘솔간 통신은 데이터의 안전성을 보장하기 위해 일반적으로 SSL(Secure Socket Layer)를 사용한다.



(그림 1) ESM 구조

2.2 ESM 기능 요구사항

ESM 의 기능 요구사항을 기능과 성능으로 구분하여 기술하면 다음과 같다.

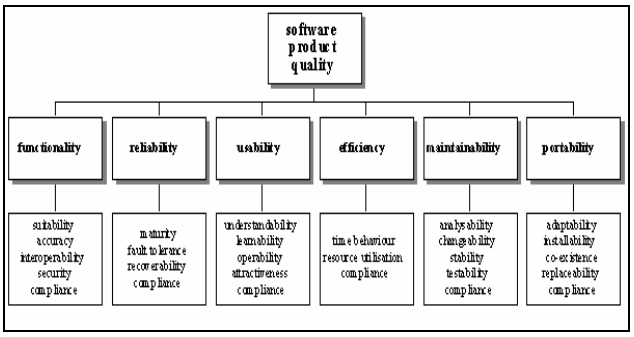
- 기능
  - 자산(관제대상 장비) 관리
  - 자산(관제대상 장비)에 대한 정책 관리
  - 운영자 및 사용자 관리
  - 에이전트(Agent) 관리
  - 보안 이벤트에 따란 위험 레벨 관리
  - 상호연관성 분석
  - 모니터링 규칙 설정 및 모니터링
  - 보안 이벤트에 따른 경보 기능
  - 서버 및 에이전트의 장애 감시
  - 통계 및 보고서 관리
- 성능
  - 이벤트 처리 시 자원 사용률의 적절성
  - 이벤트 수집 및 수집 정책에 따른 반응속도
  - 이벤트 검색시간의 신속성
  - 대량 데이터 처리 시간의 적절성

따라서, ESM 을 평가하기 위해서는 위에 기술한 기능과 성능 측면에서 요구되는 사항을 바탕으로 평가항목을 도출해야 한다. 이를 위해서는 먼저, SW 품질 평가항목을 살펴볼 필요가 있다.

3. ISO/IEC 9126, 12119

3.1 ISO/IEC 9126

현재 국제적인 표준으로 인정받고 있는 품질 평가 모델은 ISO/IEC9126 이다. 본 표준 문서는 SW 품질 특성과 척도에 관한 지침서로 고객 관점에서 SW 에 관한 품질 특성과 부특성을 정의하고 있다(그림 2).



(그림 2) SW 품질특성과 부특성

- 기능성(Functionality): 기능의 존재와 기능 특성과 관련된 특성이다. 예를 들어, 일련의 기능이 정상적으로 동작하고, 정확하게 동작하며, 타 시스템과의 상호연동가능여부 및 중요데이터에 대한 손실을 방지하거나 프로그램과 데이터에 대한 접근 권한 등을 평가한다.
- 신뢰성(Reliability): 명시된 기간 동안 명시된 조건에서 성능 수준을 유지하는 SW 능력과 관련된 특성을 평가한다.
- 효율성(Efficiency): SW 의 성능과 사용되는 자원과 관련된 특성이다. 예를 들어, 기능 수행에 따른 반응시간이나 자원 사용률 등을 정량적으로 측정하여 평가한다.
- 유지보수성(Maintainability): 시스템 사용 중 발생하는 요구사항을 만족하는지에 규정된 속성을 수행하기 위해 필요한 노력과 관련된 집합을 말한다. 예를 들어, 시스템 사용 중 발생하는 문제 해결정보, 시스템 설정 변경 가능여부 등을 평가한다.
- 이식성(Portability): 시스템의 구조 변경 정보 및 설치/제거 가능 여부, 타 응용시스템에 영향이 없는지 여부, 제품의 업그레이드 후 과거 버전의 데이터 호환 여부 등을 평가한다.

3.1 ISO/IEC 12119

ISO/IEC 12119 는 SW 패키지에 대한 요구사항(품질 요구사항)을 정의한 표준문서이다. SW 패키지란 일반적인 어플리케이션 또는 기능을 위해서 몇몇 사용자에게 제공된 완비되고 문서화된 프로그램 집합이다. 이러한 SW 패키지가 갖춰야 할 요구사항을 제품설명서, 사용자 설명서, 프로그램 및 데이터로 나뉘어 각각 요구사항을 기술하고, 시험을 위한 지침(SW 패키지 시험 방법에 대한 지침)이 기술되어 있다.

- 제품 설명서: 사용자나 잠재적 구매자가 그 제품이 합당한지를 스스로 평가할 수 있도록 하기 위한 문서로서 제품의 식별(제품 이름, 버전 또는 날짜), 공급자명, 주소, 수행가능 업무(work task), 요구되는 시스템(HW, SW), 타제품과의 인터페이스, 인도 항목(문서, 데이터 미디어 등), 사용자 설치 가능 여부, 운영을 위한 지원이 제공되고 여부, 유지보수 제공 여부 등이 제공되어야 한다.

- 사용자 설명서: 제품 사용에 필요한 정보, 제품 설명서에서 언급한 모든 기능과 프로그램 내에서 사용자가 호출 가능한 모든 기능은 완전하게 기술되어 있어야 한다. 또한, 프로그램 설치/제거에 관련된 설치 안내서나 유비보수 유형에 대해 필요한 모든 정보를 프로그램 유지보수 안내서를 포함해야 한다.
- 프로그램 및 데이터: 설치/제거를 비롯한 사용자 설명서에 언급된 모든 기능의 존재해야 하고, 기능은 정확히 동작해야 한다. 사용자가 프로그램을 통제할 있어야 하고, 데이터의 훼손이나 손실이 일어나지 않아야 한다. 메시지를 이해하거나, 관련 정보를 이해하기 쉽도록 제공하고, 심각한 결과를 초래하는 기능의 실행은 취소 가능하거나, 프로그램이 그 명령을 실행하기 전에 결과에 대해 분명한 경고를 하고 확인을 요청하도록 해야 한다.

4. ESM 평가 방안

위의 2, 3 장에서 ESM 의 구조와 기능요구사항과 ISO/IEC 9126, 12119 품질특성에 대해 살펴보았다. 본 장에서는 ESM 평가 시 고려사항을 기술하고, 이를 바탕으로 평가항목을 도출한다.

4.1 ESM 평가 시 고려사항

ESM 평가 시 고려사항으로는 2.2 절에서 언급된 기능과 성능 측면의 요구사항을 바탕으로 개발되었는지를 평가해야 한다. 또한, ESM 은 관제대상 장비를 효율적으로 관리하면서 동시에 관제대상 장비의 서비스에 부하를 주지 않아야 한다. 따라서, ESM 평가 시 ESM 자체의 기능뿐만 아니라 관제대상 장비로부터 이벤트 로그를 수집하고, 관리를 효율적으로 하는지 같이 평가해야 할 것이다.

4.2 평가 항목

2.1 절에서 기술한 ESM 구조와 기능요구사항을 바탕으로, ESM 을 평가하기 위한 평가항목을 품질 특성별로 기술하면 다음과 같다.

- 기능성 – 적합성, 정확성
  - 관제대상 장비의 관리 정책 설정 및 관리 기능
  - 정책 백업 및 복구
  - 공격 탐지 기능
  - 사용자 및 운영자 관리 기능
  - 서버 및 에이전트 구동 상태 관리 기능
  - 사용자 및 운영자 접속 이력 및 작업 내용 기록 기능
  - 장애 관리 기능
  - 서버 및 에이전트 성능 임계치 설정 기능
  - 상호연관성 규칙 설정 및 분석 기능
  - 보안 이벤트의 내용에 따른 위험도 관리 기능
  - 보안 이벤트 모니터링 규칙 설정 기능
  - 보안 이벤트에 따른 경보 기능
  - 서버/에이전트 장애 감시
  - 통계 보고서 작성 및 관리
- 기능성 – 상호운영성
  - 관제대상 장비에서 발생하는 이벤트 로그를 별도의 에이전트 설치 없이 수집 기능
- 기능성 – 보안성
  - 서버와 에이전트간 안전한 통신 지원 기능
  - ESM 운영자 및 사용자 접속 시 안전한 통신 지원 기능
- 신뢰성 – 결함 허용성
  - 서버 및 에이전트에서 장애 발생 시 시스템이 정지/다운 여부
  - 장애 발생 시 타 프로그램(예: OS 다운)에 영향 여부
- 신뢰성 – 회복성
  - 서버나 에이전트에서 오류 발생 시, 시스템이 정지/다운되지 않고, 회복 가능 여부
  - 네트워크 단절 시 재시도 여부
- 사용성 – 이해가능성
  - 장애 발생 이벤트 및 자산 관리를 위한 절차를 사용자가 이해 가능 여부
- 사용성 – 학습성
  - 각종 이벤트 관련 메시지를 쉽게 이해하고, 이를 수행 가능 여부
  - 도움말 사용 가능 여부
- 사용성 – 운영성
  - 사용자가 ESM 서버 및 에이전트를 쉽게 운영하고, 제어 가능 여부
- 효율성 – 시간효율성
  - 서버 및 에이전트에 부하발생 시 서버의 처리시간 적절성
  - 자산(관제대상 장비)에서 공격 이벤트의 실시간 탐지
  - 자산(관제대상 장비)에서 장애 발생 시 실시간 탐지
  - 조건에 따른 이벤트 검색 시 서버 반응시간의 적절성
- 효율성 – 자원효율성
  - 서버 및 에이전트에서 부하 발생시 서버의 자원 사용률 적절성
- 유지보수성 – 분석성
  - 서버에 기록된 이벤트 로그를 바탕으로 관제대상 장비에서 발생하는 이벤트를 식별하고, 분석하여 문제 해결 가능 여부
- 유지보수성 – 변경성
  - 환경 설정 변경을 제공하는지 여부
- 이식성 – 설치가능성
  - 다양한 관제대상 장비(UNIX 서버, 윈도우서버, 네트워크 장비 등)에서 에이전트 프로그램을 설치/제거 가능 여부
  - 에이전트 프로그램 업그레이드 시 자동으로 업그레이드 가능 여부
- 이식성 – 공존성
  - 에이전트 프로그램이 설치된 장비에 다른 응용프로그램들과 공존 가능 여부

- 다른 종류의 보안 프로그램과 공존할 때 원활히 동작 가능 여부

위에서 열거된 항목 중 '신뢰성' 요구사항에 해당하는 평가항목을 기술하면 <표 1>과 같다.

<표 1> 품질특성 '신뢰성' 평가항목

품질 부특성	평가항목
결함 허용성	- 서버 프로세스 장애 발생 시 에이전트 정지/다운 여부 - 에이전트 프로세스 장애 발생 시 서버 정지/다운 여부 - 에이전트에서 프로세스 장애 발생 시 다른 에이전트와 정상적인 데이터 송수신 기능 - 서버와 에이전트간 네트워크 장애 발생 시 서버 및 에이전트 동작 기능
회복성	- 서버 재구동 후, 에이전트와 정상적인 데이터 송수신 기능 - 서버 정지 또는 재구동 시간 동안 에이전트에서 발생된 이벤트 데이터의 재전송 - 에이전트 재구동 후 해당 에이전트와 정상적인 데이터 송수신 기능 - 서버와 에이전트간 네트워크 장애 발생 처리 완료 후 서버 및 에이전트 데이터 송수신 기능

5. 결 론

본 논문에서는 ESM 평가항목을 도출하였다. ESM 은 다수의 서버를 관리하거나 보안관제를 하고 있는 분야에서는 필요한 시스템이다. 또한, IT 환경의 발전에 따라 ESM 에 대한 평가항목도 지속적으로 보완되어야 한다.

ESM 을 적절하게 평가하기 위해서는 에이전트가 설치되는 다양한 OS 와 다수의 보안 정비에서도 원활히 동작해야 하므로 시스템의 효율성과 이식성이 매우 중요하다 .또한, 보안측면이 다른 일반 SW 에 비해서 중요하다. 따라서, ESM 을 평가함에 있어서 신뢰성에 가중치를 두고 제품을 평가해야 한다.

마지막으로 ESM 과 연동되는 관제대상 장비가 점차로 증가함에 따라 다수의 장비를 관리하기 위한 효율성을 평가하기 위한 성능 평가 방안도 제안되어야 하며, 향후에는 본 논문에서 제안된 평가항목을 바탕으로 실제 적용 사례에 대한 연구가 필요하다.

참고문헌

[1] TTA 정보통신용어 사전
[2] TTA SW 테스트 전문 기술 자료집
[3] ISO/IEC 9126: Software Engineering- Software Product Quality
[4] ISO/IEC 12119: Information Technology Software Packages Quality Requirements and Testing
[5] 행정안전부 고시 제 2008-26 호, "정보보호시스템 공통 평가기준", 2008.7.16