Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1167

취약점 데이터베이스 기반 개선된 보안관제 모델의 효과성 연구*

현 석 우,† 권 태 경‡
연세대학교 정보대학원 정보보호연구실

A Study of Effectiveness of the Improved Security Operation Model Based on Vulnerability Database*

Suk-woo Hyun,† Taekyoung Kwon‡
Information Security Lab., Graduation School of Information, Yonsei University

요 약

본 논문에서는 기존 보안관제의 한계점을 살펴보고, 효율적인 모니터링을 위한 취약점 데이터베이스 기반의 새로운 보안관제 모델과 그 효과성을 연구한다. 제안한 모델은 로그 탐지를 위한 정보보호 장비, 취약점 데이터베이스, 탐지 로그와의 연동 결과를 시각화하여 제공하는 대시보드로 구성하였다. 모델의 평가는 사전에 구축한 가상 인프라에서 모의공격 시나리오를 설정하여 효과를 분석하였으며, 기존의 방식과 달리 자산이 가지고 있는 보안 취약점에 특화된 공격 위협에 신속히 대응할 수 있고 취약점 데이터베이스와 연계한 보안관제로 탐지 규칙 간의 중복을 발견하여 최적의 탐지 규칙을 작성할 수 있음을 확인하였다.

ABSTRACT

In this paper, the improved security operation model based on the vulnerability database is studied. The proposed model consists of information protection equipment, vulnerability database, and a dashboard that visualizes and provides the results of interworking with detected logs. The evaluation of the model is analyzed by setting up a simulated attack scenario in a virtual infrastructure. In contrast to the traditional method , it is possible to respond quickly to threats of attacks specific to the security vulnerabilities that the asset has, and to find redundancy between detection rules with a secure agent, thereby creating an optimal detection rule.

Keywords: Vulnerability Database, Security Vulnerability, Security Operation, Infringement Accident, Cyber Threat

I. 서 론

모든 정보가 데이터화되는 빅데이터 시대 흐름에 맞춰 많은 기관이 공공, 민간의 다양한 분야에서 데이터를 활용해 새로운 가치를 창출하기 위한 여러 시도를 하고 있다. 이에 각 기관에서는 엄청난 양의 정보를 저장, 활용하기 위하여 정보시스템을 운영하고 시스템의 안전성을 확보하기 위하여 사이버보안팀, 침해사고대응팀(CERT) 등 현장대응 조직을 강화하고 있다. 그뿐만 아니라 조직의 대응능력 향상을 위해 정기적인 취약점 진단, 침해사고 대응훈련 등

Received(07. 11. 2019), Modified(1st: 08. 16. 2019, 2nd: 09. 05. 2019), Accepted(09. 05. 2019)
* 본 연구는 2019년도 정보(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2017-0-00380, 차세대 인증 기술 개발)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 지원을 받아 수행된 연구임(IITP-2019-2016-0-00304).
† 주저자, 2017521142@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

많은 노력을 기울이고 있다.

하지만 취약점 분석 결과는 서비스 가용성 또는 시스템 호환성 등의 문제로 소프트웨어 패치, 업그레이드와 같은 조치가 적시에 이루어지고 있지 않다. 침해사고 대응훈련의 경우 단기 효과는 있겠지만, 장기적인 관점에서는 효과가 미비한 것이 사실이다. 보안관제의 경우 IDS, IPS, 방화벽 등 수많은 정보보호 장비에서 발생하는 로그 전체에 대응해야 하는 관제 요원의 업무가 과중되고 있고, 자산의 취약점과 연계한 모니터링이 부족해 과탐의 빈도가 높고 효과적인 관제 업무의 수행이 제한된다.

이에 본 논문에서는 기존 보안관제의 한계점은 무엇이며, 취약점 데이터베이스에 기반한 개선된 보안관제 모델의 효과에 관하여 연구한다. 연구 범위는 다음과 같다. 첫째, 취약점 데이터베이스를 모델링하고 설계한다. 취약점 데이터베이스는 정보자산 현황, 취약점 분석 결과, 공개 취약점 정보 등을 저장, 관리한다. 둘째, 웹 크롤링을 통하여 CVE(Common Vulnerabilities and Exposures), CVSS(Common Vulnerability Scoring System)와 같은 공개 취약점 정보를 수집하는 모듈을 개발한다. 이는 취약점에 대한 상세내용, 참고자료 등 객관적인 정보를 제시한다. 셋째, 모델 구현을 위한 개발환경, 가상 인프라를 구축한다. 모의환경은 VMware를 통해 구축하며 오픈소스 소프트웨어를 활용하여 비용과 모델의 자유도를 고려하였다. 넷째, 정보보호 장비의 로그와 취약점 데이터베이스, 취약점 분석 결과를 연계한 위협 탐지 모델을 구현한다. 제안한 모델은 자산이 가지고 있는 보안 취약점을 이용한 위협에 해당하는 로그에 우선순위를 부여해 보안관제의 효율성을 높인다.

II. 관련 연구

2.1 취약점 데이터베이스

김동진 등은 미국, 일본, 중국 등의 보안 취약점 관리체계를 조사 및 분석하여 국내 환경에 적합한 취약점 관리체계 구축방안을 제안하였으며, 취약점 데이터베이스를 보안성 평가 및 보증에 활용하는 방안에 관한 연구가 필요함을 주장하였다[1].

류한얼 등은 구성모의 환경에서 사이버 공격의 유효성 확인을 위해 취약점 데이터베이스로부터 보안 취약점 정보를 확인하여 CVE, CWE 등 표준 데이터 간 관련성 높은 정보를 제공하고 누적된 분석 결과를 제시함으로써 유용한 정보를 제공할 뿐만 아니라 악성 행위 시도의 성공 여부를 판단할 수 있는 방안을 제시하였다[2].

Gu Yun-hua 등은 취약점 데이터베이스가 다양한 종류의 취약점에 대한 정보를 제공하는 것뿐만 아니라 취약점 정보를 관리하는 데에도 유용하므로 사이버 위협으로부터 시스템을 보호하는 중요한 역할을 한다고 주장하였다. 또한, CVE, IBM의 X-Force, NVD(National Vulnerability Database)를 활용한 취약점 데이터베이스를 제안하였다. 제안한 취약점 데이터베이스는 공신력 있고 객관성이 확보된 3가지 데이터베이스의 정보를 통합하여 사용자에게 필요한 정보를 제공한다[3].

김유경 등은 소스코드 보안 취약점 자동진단 시스템의 일부인 취약점 데이터베이스의 전체 구조에 관하여 연구하였고, 전 세계적으로 다양하게 수행되고 있는 보안 취약점 관련 연구 동향을 제시하였다[4].

Yung-Yu Chang 등은 NVD에 포함되어 있는 CVE 정보를 바탕으로 발생빈도, 위험도 등 보안 취약점의 트렌드를 분석하였다. 그뿐만 아니라 CVSS 범위에 따라 위험도를 3단계로 구분하여 고위험군 취약점의 발생빈도, 위험도 등을 함께 분석하였다[5].

Su Zhang 등은 NVD 정보를 활용한 취약점 트렌드 분석은 소프트웨어 결함에 대비하는 데 중요한 역할을 한다고 주장하였고, NVD 정보의 데이터마이닝을 통해 각 벤더별로 알려지지 않은 소프트웨어 취약점의 발생 가능성을 예측하는 모델을 제안하였다[6].

2.2 보안관제 모델

현정훈 등은 침해대응 관제를 위한 빅데이터 분석 기법에 관한 연구와 함께 정보보호 시스템에서 발생하는 이벤트 로그와 단말 및 서버에서 발생하는 로그 데이터들의 시계열 연관성 분석을 통해 이상 행위를 탐지하는 보안관제 모델을 구현하였다[7].

엄진국 등은 초창기 관제 시스템부터 지금의 SIEM을 이용한 관제 시스템까지 다양한 사례를 분석하여 효과적인 침해위협의 탐지방법에 관한 연구를 수행하였고, 과거 단순 위협 탐지가 아닌 시나리오 기반의 관제체계를 소개하고 상관분석 정책의 제작 및 검증 방법을 제시하였다[8].

조상덕은 보안관제에서 최신 보안 취약점 공격에 체계적으로 대응하기 위하여 ESM을 활용한 보안관제와 패턴 기반 보안관제의 문제점을 알아보고, 이러한 문제들을 해결하기 위해 보안 취약점 진단 방법론 중 모의해킹 진단 방법을 활용하여 최신 보안 취약점 공격에 효율적으로 대처할 수 있는 보안관제 고도화 방안을 제안하였다[9].

전인석 등은 SIEM의 빅데이터 분석 기법을 활용하여 소프트웨어 취약점에 대한 위협을 효과적으로 탐지하고 대응할 수 있는 모델을 제안하고 제안한 탐지 모델의 일부를 실제 서비스에 적용하고 구체적인 수치를 제시함으로써 모델의 효과를 입증하였다[10].

이재헌 등은 사용자들이 필수적으로 사용하는 특성 기능의 파라미터 정보 분석을 통해 보안관제의 기준점을 제시하였으며, 특수 목적의 기능을 하는 전력거래시스템을 대상으로 제안한 모델의 유효성을 검증하였다[11].

2.3 기존 연구와의 차이점

취약점 데이터베이스는 사이버 위협에 대한 대응능력을 향상시킬 수 있는 정보보안의 기초자산으로 자산에 대한 정기적 취약점 분석, 공개 취약점 정보의 주기적 수집, 정확한 자산현황 관리 등이 뒷받침되어야 한다. 이를 통해 기관은 식별된 보안 취약점을 적시에 전파하고 보안대책의 적용결과와 후속조치 등을 효과적으로 관리할 수 있다.

지금까지의 취약점 데이터베이스 관련 연구는 단순히 데이터베이스의 정보를 통합하여 제공하는 것으로 운영환경과 연계하여 적용하기 어렵다. 그뿐만 아니라 보안 취약점 진단 결과의 적용을 자동화할 수 있는 보안관제 프로세스와 소관체계 자산정보의 이력관리에 관한 연구가 필요하다.

이에 본 논문에서는 취약점 데이터베이스 구축의 핵심 요소인 자산 관리와 취약점 진단에 관한 연구를 수행하며, 관리대상 취약점 정보 확인부터 식별된 취약점 후속조치 완료 시까지의 이력관리가 가능하다는 점에서 차이점을 가진다. 그뿐만 아니라 보안관제의 정탐률 향상을 위하여 고위험 취약점에 대한 가중치를 부여하는 보안관제 모델을 제안하였다.

III. 보안관제 모델

3.1 모델 개요

취약점 데이터베이스에 기반한 보안관제 모델은 Fig. 1과 같이 로그 탐지를 위한 정보보호 장비, 공개 취약점 정보와 취약점 진단 결과가 저장되는 취약점 데이터베이스, 탐지 로그와 취약점 데이터베이스 연동 결과를 시각화하여 제공하는 대시보드(dashboard)로 구성한다. 이를 통하여 보안관제 인력에게는 위협 우선순위를 고려한 경고 메시지를 제공하며, 자산 관리자는 자산 정보를 등록, 수정하

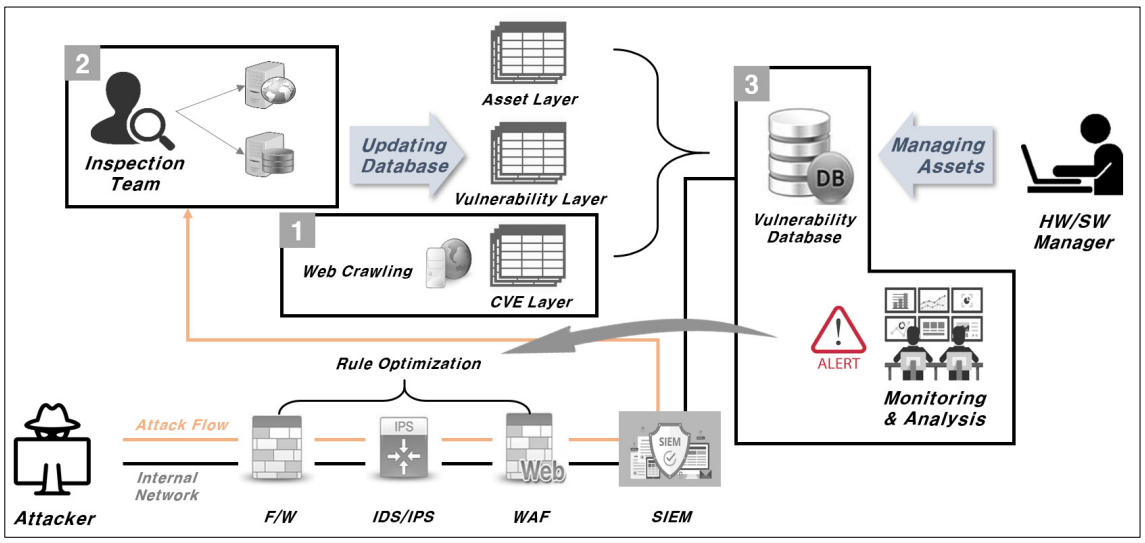


Fig. 1. Security Operation Model

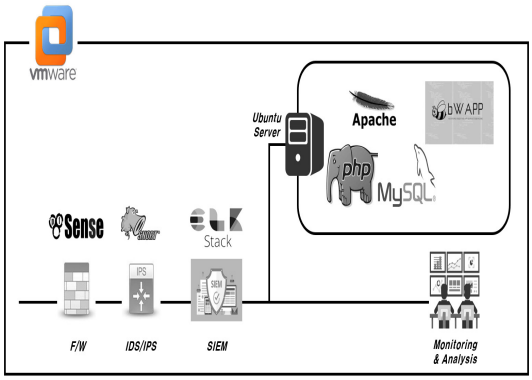


Fig. 2. Building a Virtual Infrastructure

고 취약점 진단 결과와 후속조치 결과를 등록하여 이력관리 및 조치 추적이 가능하도록 한다.

모델을 구현하고 검증하기 위해 가상환경의 인프라를 구축하며 가상화 솔루션인 VMware Wortkstation을 이용한다. Fig. 2와 같이 모의공격과 효과분석의 효용성을 높이기 위해 Ubuntu 서버를 구축하며, 취약점 진단의 대상이 될 APM(Apache struts2, Php, Mysql) 패키지와 bWAPP 애플리케이션을 서버에 구성한다.

가상 인프라 구축에 사용되는 소프트웨어는 모두 오픈소스로 모델 적용 시 비용을 절감할 수 있고, 라이센스의 제약 없이 기능을 사용할 수 있다는 장점이 있다. 그뿐만 아니라 필요한 기능을 자체적으로 개발할 수 있다는 점에서 개발 단계의 의존성을 줄이고 모델의 자유도를 확보하였다.

3.2 취약점 데이터베이스 설계

취약점 데이터베이스를 개체-관계 모델을 이용해 개념적으로 모델링한 결과는 Fig. 3과 같다. 총 3개의 레이어(layer)로 구성되며, 각 레이어를 구성하는 테이블과 속성에 대한 설명은 다음과 같다.

3.2.1 취약점 레이어(vulnerability layer)

취약점 레이어는 자산에 대한 보안 취약점 정보, 분석 결과, 조치 이력을 통합 관리하는 테이블이다.

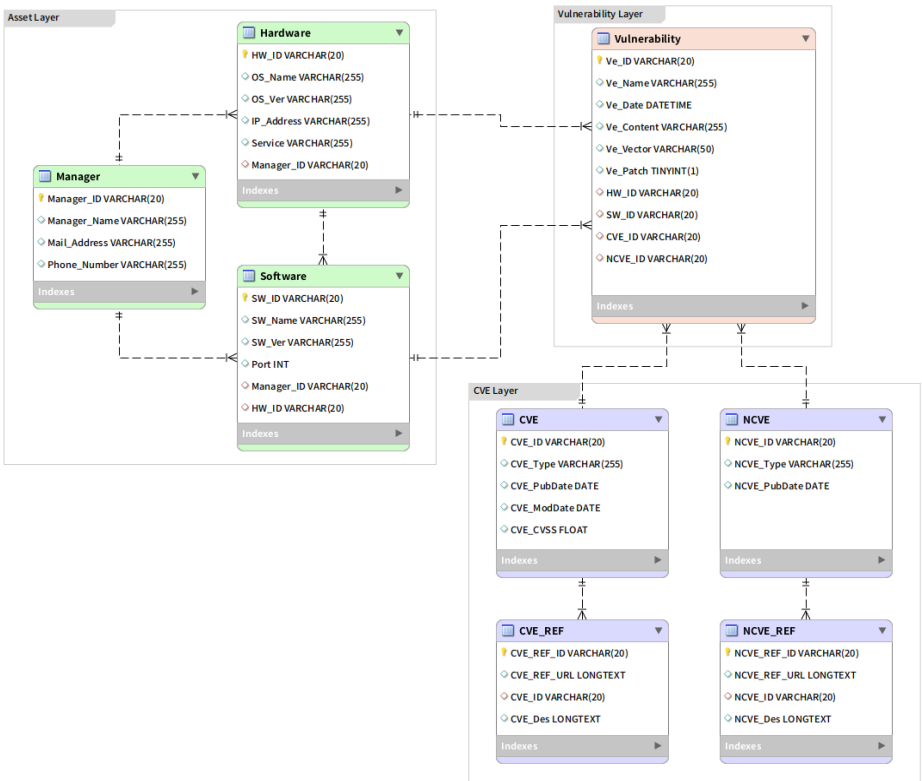


Fig. 3. E-R Diagram of Vulnerability Database

보안 취약점 진단 보고서를 항목별로 자동으로 테이블에 개체 인스턴스(entity instance)로 입력하며, 각 인스턴스는 연동 결과를 대시보드에 시각화하는 데 활용된다.

Ve_Vector 속성은 보안 취약점에 대한 access vector로 network, local, adjacent와 같은 도메인으로 구성된다. 탐지 로그와의 연동에 활용되는 Ve_Patch 속성은 취약점 패치 여부를 담고 있다. 또한, 다른 레이어 정보를 제공하기 위해 각 테이블의 ID 속성을 외래키로 참조한다.

Table 1. Description of Vulnerability Layer

Column	Type	Contents
Ve_ID	varchar	vulnerability id
Ve_Name	varchar	name of the vulnerability
Ve_Date	date	registering date
Ve_Vector	varchar	access vector of the vulnerability
Ve_Patch	tinyint	indicator of whether to patch

3.1.1 자산 레이어(asset layer)

자산정보 레이어는 Manager, Hardware, Software 3개의 테이블로 취약점 레이어와의 연동성을 고려하여 구성한다. 주요 수집 정보는 정보시스템을 구성하는 하드웨어, 소프트웨어, 관리자 정보로 취약점 조치대상 자산을 식별하는 데 활용된다.

Table 2. Description of Asset Layer

Column	Type	Contents
Manager_ID	varchar	asset manger id
HW_ID	varchar	hardware id
OS_Ver	varchar	operation version of hardware
Service	varchar	service name provided by hardware
SW_Ver	varchar	version of software
Port	int	port number of the service

Manager 테이블은 자산 관리자에 대한 정보를 담고 있으며, Hardware, Software 테이블은 서버 시스템 운영 정보, 네트워크 정보, 정보보호 시스템 정보를 포함한다.

3.2.2 CVE 레이어(CVE layer)

보안 취약점은 CVE ID가 부여된 공개 취약점과 부여되지 않은 알려지지 않은 취약점으로 분류하며, CVE 레이어는 외부 사이트로부터 웹 크롤링(web crawling)한 정보를 포함하는 CVE 테이블과 그 외 알려지지 않은 취약점 정보를 포함하는 Non-CVE 테이블로 구성된다. 또한, 각 취약점에 대한 상세정보를 제공하기 위한 테이블을 포함한다.

CVE_ID, NCVE_ID 속성은 각 테이블의 기본키이며 Vulnerability 테이블에 참조된다. CVE_Type 속성은 취약점의 타입을 나타내며 DoS, overflow, XSS 등의 도메인을 갖는다.

Table 3. Description of CVE Layer

Column	Type	Contents
CVE_Type	varchar	types of the vulnerability
CVE_PubDate	date	publishing date of the vulnerability
CVE_CVSS	float	CVSS score of the vulnerability
CVE_REF_URL	longtext	URL of the known vulnerability references
NCVE_Des	longtext	description of the vulnerability
NCVE_REF_URL	longtext	URL of the unknown vulnerability references

3.3 보안관제 모델 설계

3.3.1 취약점 데이터베이스 연동

Fig. 4는 취약점 데이터베이스와의 연동 프로세스를 나타낸다. 취약점 데이터베이스와의 연동은 정보보호 장비에서 탐지된 로그 중 조직의 자산이 가지고 있는 보안 취약점을 이용한 위협에 선제적으로 대

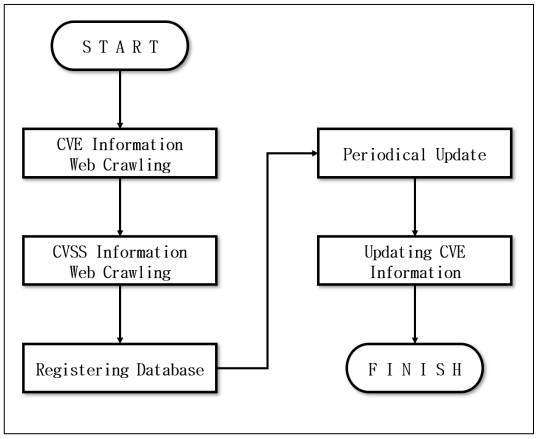


Fig. 4. CVE Information Crawling Process

응하기 위함이다. 이외에도 웹 애플리케이션의 access log와 error log도 수집하여 정보보호 장비의 로그와 연계한 분석이 가능토록 하였으며, 각각의 로그를 대시보드를 통해 시각화하기 위하여 파싱(parsing)하는 작업이 필요하다.

필드별로 파싱된 로그들은 취약점 데이터베이스의 Vulnerability 테이블과 비교하는 과정을 거친다. Vulnerability 테이블에 등록되어 있는 데이터는 조직의 자산에 해당하는 보안 취약점으로 해당 취약점의 패치 유무와 CVE ID 존재 여부에 따라 Fig. 5와 같이 우선순위를 부여한다. 취약점 패치 유무는 취약점 데이터베이스에서 탐지된 로그 메시지에 해당하는 보안 취약점을 조회하여 ve_patch 값을 리턴하도록 한다.

우선순위 1순위는 취약점 패치가 되지 않은 보안 위협에 해당하는 로그로 CVE ID를 갖는 경우와 갖지 않는 경우(NCVE ID)로 분류할 수 있다. 취약점 패치가 적용된 경우는 자산에 위협이 되지 않는 로그로 판정하여 3순위를 부여하며 마찬가지로 CVE ID, NCVE ID를 각각 갖는 경우로 분류한다. 그 외에 정보보호 장비의 기본 탐지 규칙에 따라 탐지된 로그는 2순위를 부여한다. 이 경우 자산의 취약점에 해당하는지 바로 판정될 수는 없고 관제 인력에 의한 로그 분석을 통해 위협을 식별해야 한다. 이처럼 탐지 로그와 취약점 데이터베이스를 연동하여 자산의 취약점에 해당하는 경우 위협 우선순위를 고려하여 경고 메시지를 제공할 수 있다.

A : Correspond to CVE_ID	
• Not Patched Vulnerability with CVE_ID	Priority : 1st
• Patched Vulnerability with CVE_ID	Priority : 3rd
B : Correspond to NCVE_ID	
• Not Patched Vulnerability with NCVE_ID	Priority : 1st
• Patched Vulnerability with NCVE_ID	Priority : 3rd
C : Corresponding to Default Rules of Firewall / IDS	
• Not Relevant to Asset's Vulnerability	Priority : 2nd

Fig. 5. Classification of Alert Log

3.3.2 시각화 모듈

ELK Stack은 지속적으로 누적되는 데이터를 실시간으로 분석하기 위한 오픈소스 솔루션이다. 이는 elasticsearch, logstash, kibana로 구성되어 있는 로그 수집서버로써 SIEM과 같은 역할을 한다. 단순한 로그 처리 작업은 데이터베이스를 통해서도 수행할 수 있지만, 보안관제에서는 로그를 저장하면서 분석하는 작업이 필수적이다. 또한, 경우에 따라 통합된 정보에서 원하는 결과를 얻을 수 있어야 하므로 ELK Stack을 활용한다.

시각화 모듈은 취약점 데이터베이스와 취약점 패치 유무를 비교하여 결정한 우선순위를 포함한 결과를 대시보드로 제공하는 역할을 한다. 시각화 모듈의 작동 프로세스는 Fig. 6과 같다.

Logstatsh의 input plugin에서는 탐지 로그가 저장되어 있는 데이터베이스로부터 데이터를 전달하기 위하여 jdbc 라이브러리를 사용하며, 데이터를

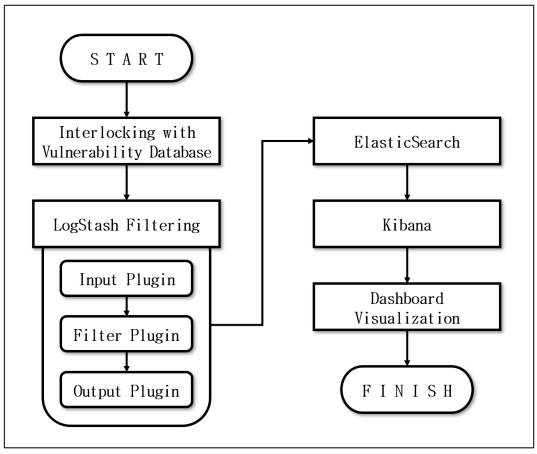


Fig. 6. ELK Stack Visualizing Process

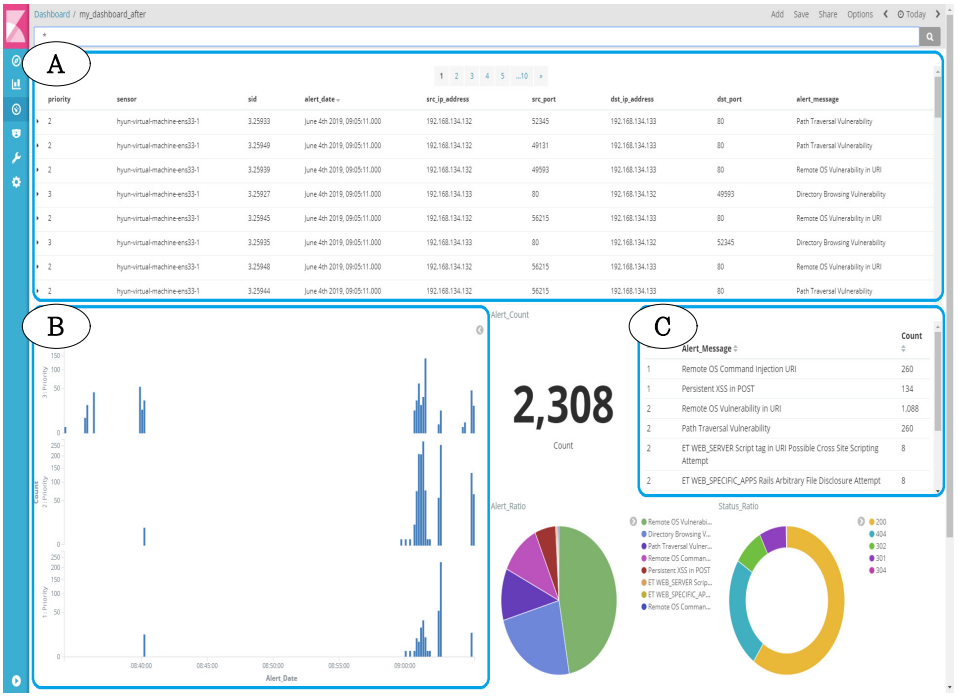


Fig. 7. Dashboard Configuration using Kibana

불러오는 데 필요한 구문, 페이징 처리에 관한 설정을 해주었다. 또한, 지속적으로 발생하는 로그 데이터를 전달받아야 하므로 리눅스의 cron 서비스를 통해 매분 입력 작업 스케줄에 맞춰 파이프라인 작업이 실행될 수 있도록 하였다. Output plugin에서는 입력받은 로그 데이터를 전송할 목적지인 elasticsearch로 전송하고 데이터 조회에 필요한 index를 설정한다.

Elasticsearch는 실시간 분석이 가능한 검색엔진으로 logstash로부터 데이터를 전달받는다. Kibana는 elasticsearch에 수집된 데이터를 시각적으로 탐색하고 실시간으로 분석할 수 있도록 Fig. 7과 같이 대시보드 형태로 보여준다.

A 영역(alert list)은 보안관제 시 로그 분석을 위한 데이터 테이블이다. IDS 장비에서 발생한 탐지 로그를 시간 순서에 따라 나타내며, 분석하고자 하는 로그 데이터를 클릭하면 상세정보를 확인할 수 있다.

B 영역(priority chart with date)은 시간에 따른 경고 메시지 개수를 나타내는 그래프이다. 우선순위를 고려하지 않은 단순한 그래프로는 발생하는 로그 전체에 대응해야하기 때문에 효율적인 관제 업무 수행이 제한된다. 이러한 점을 개선하기 위하여 우선순위별로 그래프를 분리하여 조직의 자산이 가지고 있는 보안 취약점과 연계한 관제가 가능하도록 하였다.

C 영역(priority count with alert message)은 우선순위와 탐지명에 따라 분류한 경고 메시지 개수를 나타내는 데이터 테이블이다. 전체 경고 메시지 개수를 세분화한 것으로 발생 빈도가 높은 보안 취약점을 직관적으로 확인할 수 있도록 하였으며, 이외에도 파이 차트를 통해 대응에 필요한 데이터들을 명확하고 직관적으로 제공한다.

IV. 모델평가 및 분석

이 장에서는 사전에 구축한 가상 인프라에서 모의공격 시나리오를 설정하여 제안한 보안관제 모델의 효과를 분석한다.

4.1 모의공격 시나리오

4.1.1 디렉터리 탐색 공격

디렉터리 탐색 공격은 클라이언트가 특정 디렉터리를 요청할 때 서버 내의 디렉터리 리스트와 파일

목록이 보이는 취약점을 이용한 공격이다. 디렉터리 안에 포함된 중요 정보가 노출될 수 있는 심각한 취약점으로 소스 파일, 백업 파일 등을 디렉터리 탐색 공격으로 다운로드 할 수 있다.

4.1.2 크로스 사이트 스크립팅 공격

크로스 사이트 스크립팅 공격은 웹 애플리케이션을 이용하여 다른 클라이언트에게 악성코드를 보내는데 사용하는 공격으로 입력 값의 검증이 제대로 이루어지지 않아 발생한다. 악성 스크립트는 브라우저의 쿠키, 세션 토큰에 접근할 수 있으며, HTML 페이지의 내용도 조작할 수 있다.

공격을 탐지하기 위해서는 서버로 향하는 TCP 패킷의 클라이언트 바디에서 문자열 일치 여부를 확인해야 한다. 이때, URL 인코딩을 통해 서버에 전달되므로 '〉' 문자는 '%3E'로 변환하여 'script%3E'와 같이 탐지 시그니처를 작성하였다.

4.1.3 원격명령 삽입 공격

원격명령 삽입 공격은 클라이언트가 실행하고자 하는 명령어를 취약한 서버에게 요청하여 악의적인 행위를 수행하는 공격 방법이다. 해당 취약점은 입력받는 변수 값을 서버에서 제대로 검증하지 않아 발생하는 것으로 권한이 없는 클라이언트가 시스템, 데이터베이스 등의 중요 정보를 획득할 수 있다.

취약한 서버에 시스템 명령어를 삽입하기 위하여 '|', '&'와 같은 메타 문자를 사용하고, 이를 탐지하기 위해 명령어 내에서 사용되는 '/', '\'와 같은 문자를 pcre 정규표현식으로 표현하여 탐지 시그니처를 작성하였다.

4.2 효과분석

가상 인프라에서 모의공격 시나리오를 바탕으로 제안한 보안관제 모델의 효과를 분석한다. 디렉터리 탐색 공격의 경우 취약점 패치를 완료하였고, 나머지 취약점들은 패치가 되지 않은 상태이다.

4.2.1 로그 가독성

Fig. 8은 snort IDS에서 탐지한 로그를 sguil 분석 도구를 통해서 모니터링한 결과이다. 이 경우

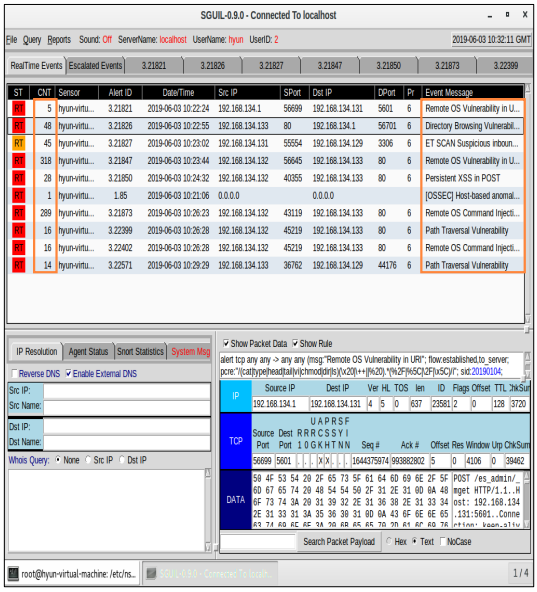


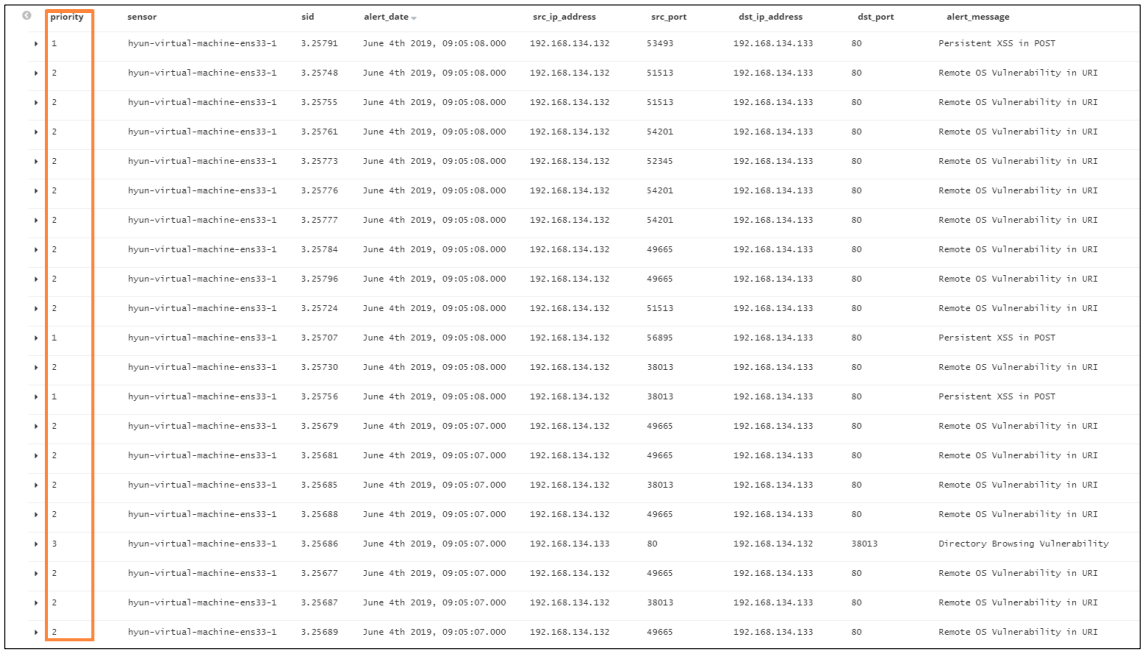
Fig. 8. Monitoring Alert Log with Sguil

각 위협의 탐지 건수를 탐지명을 기준으로 나타내고 있다. 3가지 공격을 탐지하는 시그니처에 의해 취약점의 패치 여부와는 관계없이 탐지 로그가 모두 발생한다. 즉, 기존의 모니터링 방식으로 위협에 대응하기 위해서는 디렉터리 탐색 공격을 포함한 탐지 로그를 차례대로 모두 분석해야 하며 이로 인해 실제로 취약성을 가지고 있는 위협에 대해서는 조치가 지연될 수밖에 없다.

Fig. 9는 제안한 보안관제 모델을 적용하여 모니터링한 결과이다. 이 경우 자산이 가지고 있는 보안 취약점과 취약점을 데이터베이스를 연동하여 보안 위협에 대한 우선순위를 고려한 탐지 로그가 발생한다. 이를 통하여 디렉터리 탐색 공격이 먼저 탐지되었다고 하더라도 패치가 완료되어 취약성을 갖지 않는 위협으로 판단할 수 있으며, 우선순위가 높은 크로스 사이트 스크립팅 공격과 원격명령 삽입 공격에 선제적으로 대응할 수 있을 것이다.

4.2.2 분석 업무 효율성

탐지 로그가 발생한 시간을 09:05:05부터 09:05:10까지 필터링하여 분석해보면, 총 117건의 탐지 로그가 발생하였으며 각 우선순위에 따른 탐지 로그는 각각 12건(1순위), 78건(2순위), 27건(3순위)이었다. 기존의 모니터링 방식으로는 시간 순서에



priority	sensor	sid	alert_date	src_ip_address	src_port	dst_ip_address	dst_port	alert_message
1	hyun-virtual-machine-ens33-1	3.25791	June 4th 2019, 09:05:08.000	192.168.134.132	53493	192.168.134.133	80	Persistent XSS in POST
2	hyun-virtual-machine-ens33-1	3.25748	June 4th 2019, 09:05:08.000	192.168.134.132	51513	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25755	June 4th 2019, 09:05:08.000	192.168.134.132	51513	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25761	June 4th 2019, 09:05:08.000	192.168.134.132	54201	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25773	June 4th 2019, 09:05:08.000	192.168.134.132	52345	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25776	June 4th 2019, 09:05:08.000	192.168.134.132	54201	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25777	June 4th 2019, 09:05:08.000	192.168.134.132	54201	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25784	June 4th 2019, 09:05:08.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25796	June 4th 2019, 09:05:08.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25724	June 4th 2019, 09:05:08.000	192.168.134.132	51513	192.168.134.133	80	Remote OS Vulnerability in URI
1	hyun-virtual-machine-ens33-1	3.25707	June 4th 2019, 09:05:08.000	192.168.134.132	56895	192.168.134.133	80	Persistent XSS in POST
2	hyun-virtual-machine-ens33-1	3.25730	June 4th 2019, 09:05:08.000	192.168.134.132	38013	192.168.134.133	80	Remote OS Vulnerability in URI
1	hyun-virtual-machine-ens33-1	3.25756	June 4th 2019, 09:05:08.000	192.168.134.132	38013	192.168.134.133	80	Persistent XSS in POST
2	hyun-virtual-machine-ens33-1	3.25679	June 4th 2019, 09:05:07.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25681	June 4th 2019, 09:05:07.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25685	June 4th 2019, 09:05:07.000	192.168.134.132	38013	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25688	June 4th 2019, 09:05:07.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI
3	hyun-virtual-machine-ens33-1	3.25686	June 4th 2019, 09:05:07.000	192.168.134.133	80	192.168.134.132	38013	Directory Browsing Vulnerability
2	hyun-virtual-machine-ens33-1	3.25677	June 4th 2019, 09:05:07.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25687	June 4th 2019, 09:05:07.000	192.168.134.132	38013	192.168.134.133	80	Remote OS Vulnerability in URI
2	hyun-virtual-machine-ens33-1	3.25689	June 4th 2019, 09:05:07.000	192.168.134.132	49665	192.168.134.133	80	Remote OS Vulnerability in URI

Fig. 9. Monitoring with Improved Model

따라 발생한 로그 117건을 차례대로 분석해야 할 것이며, 이는 과탐의 빈도 또한 높아 효율적인 보안관제가 되지 못한다. 반면에, 개선된 방식으로는 자산의 취약점에 특화된 공격 징후에 즉시 대응할 수 있다. 3순위에 해당하는 탐지 로그는 패치가 완료된 보안 취약점으로 자산에 영향을 미치지 않는 위협으로 판단할 수 있다.

보안관제 인력이 로그 1건을 분석하는 데 걸리는 시간이 최소 3분에서 최대 5분이라고 가정하면 기존의 방식으로는 117건의 로그를 분석하는데 최소 351분에서 최대 585분이 소요된다. 개선된 방식을 적용하면 분석해야 할 로그는 90건으로 줄어들게 되고 분석하는데 최소 270분에서 최대 450분이 소요되어 약 23.1%의 개선 효과를 보였다. 모델의 효율성은 수식(1)과 같이 나타낼 수 있다.

$$\frac{Total\ \ Log-(1^{st}priority+2^{nd}priority)}{Total\ \ Log} \quad (1)$$

4.2.3 탐지 규칙 최적화

크로스 사이트 스크립팅 공격의 경우 취약점 데이터베이스를 통해 발생한 1순위 탐지 로그와 IDS의 기본 탐지 규칙에서 발생하는 2순위 탐지 로그가 각각 발생하는 것을 확인할 수 있었다. 2순위 탐지로그는 직접 로그를 분석하여 자산의 취약점에 해당하는 위협인지를 판단해야 한다. 하지만 취약점 데이터베이스와 연계하여 자산이 가지고 있는 보안 취약점에 대한 탐지 규칙을 작성할 수 있었고 이를 적용한 결과, 탐지 규칙 간의 중복을 발견하여 최적의 탐지 규칙을 작성할 수 있었다.

V. 결 론

사이버 경계영역인 보안관제 분야에서는 신속한 대응이 절실하다. 이를 위해선 발생하는 전체의 로그를 분석하는 것이 아니라 정보자산이 갖는 취약성에 해당하는 위협에 선제 대응할 수 있는 역량과 식별된 취약점을 적시에 전파하고 보안대책 적용결과 및 후속조치 등을 통합 관리하는 체계의 구축이 필요하다.

본 논문에서는 조직의 정보자산이 가지고 있는 보안 취약점을 통합 관리할 수 있는 취약점 데이터베이스를 구축하고 이에 기반한 보안관제 모델을 연구하였다. 단순히 정보를 통합하여 제공하는 기존의 취약점 데이터베이스와 달리 조직의 운영환경과 연계한 활용방안에 관한 연구를 진행하여 자산의 가치, 위협의 중요도를 고려한 보안관제 모델을 구현하였다.

모델 구현을 위하여 가상 인프라 구성, 취약점 데

이터베이스 모델링, 공개 취약점 정보수집 모듈 개발, 취약점 데이터베이스 연동 개발 등을 수행하였으며, 모의공격 시나리오를 설정하여 제안한 모델의 효과를 분석하였다. 모의실험 결과 탐지 로그를 차례대로 분석하는 기존의 방식과 달리 자산이 가지고 있는 보안 취약점에 특화된 공격 위협에 신속히 대응할 수 있었다. 그뿐만 아니라 취약점 데이터베이스와 연계한 보안관제로 탐지 규칙 간의 중복을 발견하여 최적의 탐지 규칙을 작성할 수 있었다.

본 연구를 실제 운영환경에 적용하여 정보자산에 대한 정기적 취약점 분석과 결과에 대한 이력관리, 공개 취약점 정보의 정기적 수집, 정확한 자산 현황 관리 등을 수행할 수 있으며, 취약점 데이터베이스의 최적화를 통하여 사이버 위협 징후에 대한 적시적인 관제로 조직의 위협 대응능력이 향상될 것이다.

References

[1] Dong-jin Kim, Sung-je Cho, "An Analysis of Domestic and Foreign Security Vulnerability Management Systems based on a National Vulnerability Database," Internet and Information Security, vol. 1, no. 2, pp. 130-147, Nov. 2010.

[2] Han-eul Ryu, Tae-kyu Kim, Wan-soo Cho, "Method of Standard Dataset based Vulnerability Database Design for Constructive Modeling & Simulation," Proceedings of Symposium of the Korean Institute of Communications and Information Sciences, pp. 1346-1347, Jun. 2017.

[3] Gu Yun-hua, Li Pei, "Design and Research on Vulnerability Database," 2010 Third International Conference on Information and Computing, vol. 2, pp. 209-212, Jun. 2010.

[4] Yu-kyong Kim, Seung-cheol Shin, Joon-seon Ahn, Ouk-seh Lee, Eun-young Lee, Hwan-soo Han, "Analysis and Documentation of Korean Common Weakness Enumeration for Software Security," Communications of the Korean Institute of Information Scientists and Engineers, vol. 28, no. 2, pp. 20-31, Feb. 2010.

[5] Yung-Yu Chang, Pavol Zavarsky, Ron Ruhl, Dale Lindskog, "Trend Analysis of the CVE for Software Vulnerability Management," 2011 IEEE Third International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, pp. 1290-1293, Oct. 2011.

[6] Su Zhang, Xlnmlng OU, Dolna Caragea, "Predicting Cyber Risks through National Vulnerability Database," Information Security Journal : A Global Perspective, pp. 194-206, Nov. 2015.

[7] Jeong-hoon Hyun, Hyoung-joong Kim, "Security Operation Implementation through Big Data Analysis by Using Open Source ELK Stack," Journal of Digital Contents Society, vol. 19, no. 1, pp. 181-191, Jan. 2018.

[8] Jin-guk Um, Hun-yeong Kwon, "Model Proposal for Detection Method of Cyber Attack using SIEM," The Journal of The Institute of Internet, Broadcasting and Communication, vol. 16, no. 6, pp. 43-54, Dec. 2016.

[9] Sang-duck Cho, "A Study of Security Monitoring Enhancement by Using Security Vulnerability diagnosis," Konkuk University, Feb. 2014.

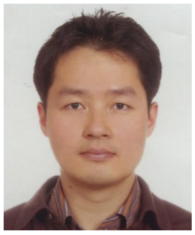
[10] In-seok Jeon, Keun-hee Han, Dong-won Kim, Jin-yung Choi, "Using the SIEM Software vulnerability detection model proposed," Journal of the Korea Institute of Information Security & Cryptology, vol. 25, no. 4, pp. 961-974, Aug. 2015.

[11] Jae-heon Lee, Sang-jin Lee, "A Study on Effective Security Control Model Based on Characteristic of Web

Service," Journal of the Korea Institute of Information Security & Cryptology, vol. 29, no. 1, pp. 175-185, Feb. 2019.

〈저자소개〉

현 석 우 (Sukwoo Hyun) 학생회원
2016년 2월: 한국항공대학교 전자 및 항공전자공학 졸업
2017년 3월~현재: 연세대학교 정보보호 연구실 석사 과정
〈관심분야〉 정보보호, 사이버보안, 가상화 기술, 소프트웨어 보안, 정보보호 교육 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환 교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, 인증, 유저블 시큐리티, 사물인터넷 보안, 소프트웨어 보안, 펌웨어 보안 등