Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.175

웹 서비스 특성 기반 효율적인 보안관제 모델 연구

이 재 헌,[1†] 이 상 진[2‡]
[1]한국전력거래소, [2]고려대학교 정보보호대학원

A Study on Effective Security Control Model Based on Characteristic of Web Service

Jae-heon Lee,[1†] Sang-Jin Lee[2‡]
[1]Korea Power Exchange, [2]Korea Graduate School of Information Security

요 약

보안관제는 여러 정보를 수집하고 그 정보를 분석하는 과정에서 유효한 결과 값을 도출함으로써 사이버 침해로부터 IT시스템을 지켜내는 것이다. 현재 보안관제는 단편적인 정보만을 가지고 사이버 위협 정보를 분석하는 것에서 벗어나, 많은 데이터를 바탕으로 체계적이고 종합적인 관점의 분석을 가능케 하는 SIEM(Security Information Event Management) 장비 사용으로 매우 효과적으로 수행하고 있다. 하지만, 이런 보안관제도 보안 인력의 수작업으로 사이버 공격을 분석하여 대응하고 있다. 따라서 뛰어난 보안장비가 있더라도, 사용자에 따라 결과가 달라질 수 있게 된다.

본 연구는 정보제공을 포함하면서도 특성 있는 웹 서비스를 운영하는 사이트인 경우, 특성 정보 분석을 통해 보안관제의 기준점을 제시하고, 이를 바탕으로 단계적인 분석과 효과적인 필터링이 가능한 유형 발굴 및 적용을 통해 집중 보안관제할 수 있는 모델을 제안한다. 이 모델을 사용한다면 효과적으로 공격을 탐지하고, 분석 및 차단 방안을 마련할 수 있을 것이다.

ABSTRACT

The security control is to protect IT system from cyber infringement by deriving valid result values in the process of gathering and analyzing various information. Currently, security control is very effective by using SIEM equipment which enables analysis of systematic and comprehensive viewpoint based on a lot of data, away from analyzing cyber threat information with only fragmentary information. However, It can also be said that cyber attacks are analyzed and coped with the manual work of security personnel. This means that even if there is excellent security equipment, the results will vary depending on the user using.

In case of operating a characteristic web service including information provision, This study suggests the basic point of security control through characteristics information analysis, and proposes a model for intensive security control through the type discovery and application which enable a step-wise analysis and an effective filtering. Using this model would effectively detect, analyze and block attacks.

Keywords: Security Control, Intensive security control, Characteristic Web Service

Received(10. 16. 2018), Modified(12. 28. 2018), Accepted(01. 07. 2019)

† 주저자, seasonleader@naver.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

I. 서 론

현대 사회는 거의 모든 분야에서 IT시스템을 활용하여 업무를 수행하고 있으며, 회사의 핵심 기능 혹은 인터넷 사용자에게 공개되어야 하는 기능들을 구현할 때도 IT시스템을 활용하는 시대이다. 이와 같이 인터넷과 연결된 IT시스템으로 외부의 불특정 다수에게 웹 서비스를 제공하는 기업은 외부 침입에 대응하기 위해 보안 인력에 의존하여 보안 관제를 하고 있다. 좀 더 상세하게는 각종 보안장비들의 로그를 종합하여 분석하고 대응하는 통합보안관제시스템을 활용하고 있다.

한편, 인터넷 환경의 빠르고 급격한 변화는 여러 디바이스들로부터 엄청나고 다양한 형식의 정보들이 유통되면서, 단 시간 내 파악하기 힘든 사이버 공격 발생과 랜섬웨어 같이 사용자의 중요한 정보가 순식간에 유실될 수 있는 가능성이 상존하게 되었다. 이러한 사이버 공격에 대응하기 위해 기존과는 다른 종합적이고 체계적인 관점의 보안관제 시스템이 필요하게 되었고, 최근 SIEM이라는 용어로 재탄생되어 빅데이터 처리 기반의 보안관제 시스템을 활용하는 수준까지 오게 되었다[1].

기존의 보안관제 활동과 빅데이터를 분석하여 처리하는 최근의 SIEM 장비 활용은 분명 사이버 공격을 방어하는데 많은 도움을 주고 있다. 하지만, 다양한 시스템을 활용하여 사이버 보안을 관리하려면 보안 인력이 필요하고, 수작업에 의존하는 보안관제의 특성으로 인해 사람에 의한 차이가 발생한다.

본 연구는 현재의 보안관제에서 벗어나, 좀 더 개선된 보안관제 결과를 만들 수 있는 효과적인 모델을 제안하고자 한다. 인터넷 기반 웹 서비스를 제공하는 시스템 중 일반적인 정보 제공 서비스가 아닌, 기업의 특성을 반영하여 외부의 사용자에게 제공하는 웹 서비스 환경인 경우, 환경 내 보안 위협을 추출하고, 종합적인 분석을 통해 가장 특징적인 정보를 기반으로 한 보안관제 모델을 제안한다.

기업의 특성을 반영하여 웹 서비스를 하는 시스템들 중 특수 목적을 가지고 웹 서비스를 제공하는 전력거래시스템에 적용하였고, 이 보안관제 모델의 효과성을 검증하기 위해 운영 중인 시스템 네트워크 내의 통합 보안 관리 시스템을 활용했다. 전력거래시스템은 일반적으로 양방향 정보 제공 등의 웹 서비스와는 달리, 전력 인프라에서 전력 생산을 통해 수익을 창출하고자 하는 특수 목적을 가진 사용자들이 전력거래를 위해 웹 서비스를 받고자 하는 시스템이기 때문에, 이 특성이 반영된 특수성을 활용하였다. 특수 목적 혹은 특성이 일반적인 웹 서비스와 다를 경우를 분석하여 특성 추출을 통한 효율적인 보안관제의 모델을 만드는 것이, 이 논문의 목적이다.

또한, 이 과정 중 많은 데이터를 분석하면서, 특성 추출 후 체계적이고 단계적인 보안관제의 기반이 될 수 있는, 가장 일반적이고 평균적인 기준분석 방법을 제시하여, 보안관제 업무의 분석 범위를 줄일 수 있도록 하겠다.

II. 최근까지의 보안관제

2.1 단일 보안 시스템과 ESM

보통의 통신 네트워크를 보안하기 위해 운영되고 있는 보안장비는 DDoS 방어 장비, IDS/IPS, Web Fire Wall, Fire Wall 등이 있으며, 보다 확장되고 강화된 네트워크에서는 NAC(Network Access Control), 단말접근제어, 서버접근제어 등 상세 보안 강화를 목적으로 한 장비까지 운영되고 있다. 개별 장비들은 저마다의 목적을 가지고 있기에 특성에 맞는 시스템 운용이 필요하다. 또한, 침입자의 공격시도를 규명하고 이 과정에서 분석된 내용을 토대로 불분명한 침입시도를 규명하는 보안관제는 개별 보안 시스템에서 수집하고 있는 정보를 토대로 수행한다[2].

일반적으로 단일 보안 시스템을 운영하며 개별 정보들을 가지고 보안관제를 한다는 것은 개별 장비들에 저장되는 각종 공격 정보들을 수작업으로 일일이 확인하고, 그 정보들을 종합적으로 분석하는 것이다. 이와 같은 방법은 빠른 시간 안에 정보를 확인하고 분석하여 신속히 대응하는데 한계가 있다.

이를 극복하고자 각종 보안 시스템의 정보를 수집하여 체계적으로 저장하고 종합적인 분석을 편리하게 해주는 ESM(Enterprise Security Management)이 출시되었다. 이 시스템은 일반적으로 이기종 보안 시스템의 보안 로그 정보들을 수집한다. 최근에는 네트워크 자원 관리 시스템(NMS) 및 시스템 자원 관리 시스템(SMS) 등의 로그 정보와 웹 서버의 웹로그(Web Log)까지 다양한 로그 정보를 수집하는 형태로 개발되었다[3]. ESM이 수집하는 로그 정보들은, 개별 보안 시스템이 모두 독자적인 기능을 하면서, 각 기기의 로그 정보들을 저장한다. 이런 정보들이

ESM과 연동을 통해 기본 데이터로 쓰인다. 이 시스템의 동작 방식을 간략히 살펴보면 다음과 같다[4].

- 정보 수집 : 단일 보안 시스템의 보안 로그를 ESM과 연동할 수 있는 형식으로 수집
- 수집 정보 가공 : 저장된 보안 로그를 보안 관제 정책과 부합하는 형식으로 필터링하고, 분석 가능한 형식으로 변환하는 정규화 과정을 통해 분류
- 분석 : 수집 및 가공된 정보에서 위협 여부를 판단할 수 있도록 상이한 보안 로그간의 실시간 연관 분석
- 종합 표출 : 수집되는 단일 보안 시스템의 각종 정보 중 보안관제 정책에 부합되는 보안 이벤트를 직관적으로 확인할 수 있도록 결과를 표출

일반적인 ESM 활용 방법은 종합 로그의 연관 분석을 통해 결과를 추출하고, 이 값을 통해 단일 보안 시스템 내 규칙의 설정을 수정해 가며 적절한 보안 정책을 만들어 가는 것이다. 또한, 이 과정 중 ESM은 적용된 보안 정책을 추가로 분석하고 감시할 수 있도록 한다.

그렇지만 나날이 발달하는 IT시스템으로 인해, 취급해야 하는 정보의 양이 매우 많아져서, 정보를 수집하고 가공 및 분석하는 ESM은 처리속도에 한계를 보이게 되었다. 속도의 제한은 급변하는 사이버 위협의 상황을 인지하고 처리하는데 있어, 취약한 보안 요소 중 하나라 할 수 있다.

2.2 SIEM과 현재의 보안관제

IT기술의 발달로 개별 시스템의 처리 속도가 올라갔으며, 이로 인해 생성되는 데이터의 양도 방대해졌다. 그로 인해 기존 데이터베이스 관리도구의 능력을 넘어서, 수십 테라바이트의 데이터로부터 가치를 추출하고 결과를 분석해야 할 필요성이 대두되었다[5]. 정보보안 분야에서도 기존의 방식으로는 관리 및 분석이 어려워 빅데이터 처리 기술 접목이 필요하게 되었다. 그 결과, 나타난 개념이 SIEM (Security Information Event Management)이다. SIEM은 빅데이터 처리 기술이 접목되어 다양한 형태와 일정하지 않은 형식의 보안 데이터를 빠르고 효과적으로 분석할 수 있는 기술이다.

SIEM은 앞서 살펴본 ESM의 개선판이라 할 수 있다. 각종 로그의 분석 결과를 활용하여 단계적인 설정을 통해 연관되는 결과만을 도출해주는 시나리오 보안 경보 이벤트를 생성할 수 있는데, 기존의 ESM과는 대비되는 특징이다. 다음은 SIEM과 ESM의 주요 기능과 차이점을 확인할 수 있다[6].

〈SIEM(a) / ESM(b)〉

- 분석 대상
  - (a): 보안시스템, 서버시스템, 네트워크 장비, 어플리케이션 로그, 시스템 감사정보, 네트워크 흐름 등
  - (b): 보안시스템, 서버시스템 로그
- 수집 & 저장
  - (a): 정형 & 비정형 데이터, 원본 로그 보관
  - (b): 정형 데이터, 원본 로그 미보관
- 수집 & 분석 아키텍처
  - (a): Indexing, MapReduce 등 빅데이터 처리 기반, 초당 3~5만건 이상 수집 및 분석
  - (b): RDBMS 기반, 초당 3천건 내외 수집 및 분석
- 분석 특징
  - (a): 다양한 룰 및 시나리오 기반 탐지, 비정상 공격 연관성 분석, 수개월 단위 분석 용이, 정·오탐 분석 정확도 높음
  - (b): 단순 패턴 기반 탐지, 알려진 공격 위주 탐지, 단 시간 범위 분석, 정오탐 분석 정확도 낮음

SIEM이 도입되었다고 해서 보안관제 업무가 크게 달라지지는 않았다. 다만, 좀 더 많은 데이터를 분석하고, 빠른 속도로 결과를 보여주며, 여러 결과 값을 연관되게 분석하여 의미 있는 결과 값을 확인할 수 있는 정도이다. 또한, SIEM을 사용하는 사용자의 활용 능력에 따라 개별적인 차이가 드러날 수 있다.

현재도 많은 기업과 공공기관은 다양한 공격과 빠르게 변화하는 사이버 공간 상의 위협에 대응하기 위해 기본적인 단일 보안 시스템뿐만 아니라, ESM과 SIEM을 이용하여 보안관제를 하고 있다. 보안관제 인력의 능력에 따라 정·오탐을 분석하여 처리하는 건수가 보통 적게는 5~10건, 많게는 20~30건이기에 장비의 활용도는 매우 중요한 지표가 될 수 있다. SIEM을 활용하는 곳에서도 장비의 성능이 뛰어나도, 보안 인력에 따라 결과가 달라질 수 있는 건 마찬가지이다.

III. 웹 서비스 특성 기반 보안관제

3.1 보안관제와 웹 서비스 특성

앞서, 살펴본 현재의 보안관제를 볼 때, 통합 보안 관리 시스템을 활용하여 보안관제 업무를 하면서도, 사용자에 따라 달라지는 결과의 편차를 개선할 수 있는 보안관제 모델이 필요하다.

일반적인 보안관제의 분석 및 대응 절차는 아래와 같다.

① 공격 정보 탐지 내용 확인 (통합 보안 관리 시스템)
② 단일 보안 시스템으로 개별적 탐지 내용 확인
③ 관련 공격 대상 장비 단의 공격 정보 확인
④ 공격의 성공 여부 확인 (정·오탐 식별시 개별 대조 확인 필요)
⑤ 분석 결과를 반영하여 보안장비 최적화 및 공격 대상 장비 보완

위 절차에서 공격 정보 탐지 내용을 확인할 때, 연관 보안장비들의 분석과정에서 분석에 특화된 보안 인력이 아닌 이상, 일정한 기준을 가지고 분석하는 것이 아닌, 상황에 맞는 대응 양상을 보이는 것이 일반적이다. 또한, 실시간으로 유입되는 수십, 수백만 건의 공격 정보에서 정·오탐을 효율적인 방법으로 가려내는 것은 쉬운 일이 아니다. 따라서 상황에 따라 접근하는 방법이 아닌, 시스템의 특성을 분석한 상태에서 일반적이지 않은 주요 요소를 찾아내어 이를 기반으로 보안관제를 하는 방법이 효율적일 수 있다.

보안관제를 한다는 것은 외부의 공격이 들어오는 접점이 있다는 것이고, 이런 환경은 웹 서비스를 제공하는 시스템을 운영하고 있는 사이트라 할 수 있다. 웹 서비스는 주로 외부의 사용자들이 접근하여 정보를 조회하거나, 입력하는 등의 일반적인 행위가 일어나는 것이 보통이며, 이 중 악의를 가지고 OWASP TOP10과 같이 알려진 공격 혹은 알려지지 않은 공격 등의 행위도 일어나게 된다.

공격 행위와는 달리, 세금을 내거나, 공식 문서를 출력하거나, 주식을 거래하거나, 물건을 거래하는 등 실명이 인증된 후 특수 목적을 위해 정상적으로 웹 서비스를 이용하는 사용자들의 접근성을 고려하여, 보통 80포트(HTTP), 443포트(HTTPS)로 웹서비스를 운영하고 있다. 또한, 사용자가 유동 IP를 사용할 수도 있기 때문에 방화벽으로 IP를 차단할 수 없다.

이런 운영 방식에서 공격자와 실제 사용자를 가려낼 수 있는 효율적인 방법이 바로 특성 기능 파라미터를 활용한 화이트리스트 추출 방법이다. 특수한 웹 서비스를 제공하는 시스템에서는 사용자들이 필수적으로 사용할 수밖에 없는 기능에 버튼을 클릭하거나 정보를 입력하도록 구현되어 있다. 특수한 웹 서비스를 사용하면서 접하게 되는 기능들은 일반적인 웹 서비스 사용할 때의 기능과 다르지 않으며, 크게 보았을 때 2가지 주요 기능으로 구현된다. 기본적으로 사용자의 필요에 의해 ID/PW나 공인 인증과 같은 인증과정을 거친 후에 사용되는 기능이다.

- 사용자 정보 조회 기능 : 사용자의 필요에 의해 개인적인 정보들을 확인할 때 사용되는 기능
  - 예시 : 세금 정보 조회, 세금 납부 내역 조회, 증명서 발급 내역 조회, 주식 거래 내역 조회, 물품 거래 내역 조회, 계좌 조회, 거래 수익 조회 등
- 요청 기능 : 사용자의 필요에 의해 사이트별로 제공되어 처리되는 기능으로 각종 신청, 승인 요청 등이 일어나도록 한다.
  - 예시 : 세금 납부, 납부 확인증 출력, 증명서 발급, 매수 및 매도 접수, 계좌 이체 등

위에서 살펴본 주요 기능들은 보통 웹 서비스 내에서, 보다 세분화된 유형으로서 기능하고 있으며, 세부 기능들을 확인하면 사용되는 파라미터 정보까지도 확인할 수 있다. 특성 있는 웹 서비스의 주요 기능들로부터 정보 확인이 되는지 알아보고 이에 기반한 보안 관제가 가능한지 검증하기 위해, 본 논문에서는 전력거래 시장을 운영하는 전력거래시스템을 대상으로 웹 서비스 특성을 확인해 보았다. 조사 대상으로 하는 전력거래시스템은 사이버 공간에서 우리나라 전력 거래의 모든 과정이 원활히 돌아가도록 해주는 시스템이다.

주요 기능들 중 사용자가 필수적으로 사용할 수밖에 없는 기능들 위주로 시스템 소스코드를 확인해 보았으며, 그 목록과 파라미터 정보는 아래 목록과 같다. 여기서 파라미터 정보는 소스코드 내 정보이므로 보안을 위해 일부를 '*'으로 대체하였다.

〈전력거래시스템 내 사용자가 활용하는 주요 필수 기능〉

(1) 전력거래 시장 - 송전단 변경 입찰 기능

☞ 파라미터 정보 : *id*e*id*e*a*l.****

(2) 전력거래 시장 - 발전단 변경 입찰 제출 기능
☞ 파라미터 정보 : *en*e*id*e*a*l.****

(3) 전력거래 시장 - 초기 입찰 기능
☞ 파라미터 정보 : *id*n*t*i*e*ai*_D.****

(4) 전력거래 시장 - 거래 후 전자세금 계산 승인
☞ 파라미터 정보 : *C*B*0*0*F

(5) 회원사의 나의 사업정보 바로가기
☞ 파라미터 정보 : *ci*a*ic*i*t.*o

(6) 양방향 REC 계약시장 - 회원사 계정의 My Rec의 매도 현황 조회
☞ 파라미터 정보 : *o*d*e*is*.*o

(7) 양방향 REC 계약시장 - 회원사 계정의 My Rec의 매수 현황 조회
☞ 파라미터 정보 : *u**e**is*.*o

(8) 양방향 REC 계약시장 - 계약시장 등록버튼
☞ 파라미터 정보 : *o*t*a*t*n*.*o

(9) 양방향 REC 계약시장 - 계약 등록 입력 페이지 버튼
☞ 파라미터 정보 : *o*t*a*t*e*i*i*n*i*w.*o

(10) 양양방향 REC 현물시장 경로 버튼
- 거래시스템 웹페이지 상
- 모든 거래 회원사가 클릭하는 버튼
☞ 파라미터 정보 : *e*l*i*e*a*e.*o

(11) 양방향 REC 현물시장 주문접수 - 매도 주문접수 호출 시
☞ 파라미터 정보 : *e*l*e*u*s**a*e*r*c.*o

(12) 양방향 REC 현물시장 주문접수 - 매수 주문접수 호출 시
☞ 파라미터 정보 : *r*d**u*_*_N_*u*m*t.*o

위 12가지 기능 목록에서 보듯이 사용자가 필수적으로 사용할 수밖에 없는 기능들은 앞서 언급한 주요 2가지 기능으로 조회(매도 및 매수 현황)와 요청(입찰, 제출, 승인, 접수 및 등록 등) 기능들로 이루어져 있다. 특히 전력을 생산하여 거래하는 사용자들을 위한 시장시스템에서의 기능들로 구성되어 있기 때문에 주로 사용자들이 입찰(Bid), 정보제출(Submission) 등의 기능을 사용하며, 그 결과 거래의 현황을 확인하여 자신들의 정보를 확인하는 특정 정보(Sell & Buy Status) 조회(Inquiry) 기능 파라미터임을 볼 수 있다.

3.2 보안관제 모델과 특성 분석 결과 활용 검증

본 절에서는 위에서 살펴본 주요 세부 기능들을 활용하여 보안관제를 효율적으로 할 수 있는 방법을 제시하고 이에 대한 검증을 한다.

일반적인 보안관제의 절차와 유사하지만 3.1절에서 확인한 특성 있는 웹 서비스일 경우의 보안관제 방법은 Fig. 1.과 같은 절차를 제안한다. 기존의 일반적인 보안관제와는 다른 관제를 하기 위해, 관제의 기준점을 제시하고 그로부터 활용되는 요소들을 추출하는 전반적인 방법론이다.

제안하는 위의 보안관제 프로세스를 수행하기 위해 3.1절에서는 웹 서비스 특성 분석과 특성 파라미터를 확인하였다. 이후 과정인 특성 파라미터를 통한 화이트리스트 IP 추출 및 검증은 다음과 같이 확인하였다.

앞서 나열한 12가지 주요 기능별 파라미터 값을 활용하기 위해 단일 보안 장비 및 이들의 로그를 검색할 수 있는 통합 보안 관리 시스템(SIEM : 이글루시큐리티 사의 SPiDER TM 5.0)을 사용하였으며, 그 내용은 다음과 같다.

① 수집된 웹 로그 내 파라미터 정보 검색
② 정보 파악
③ 파악된 정보를 바탕으로 웹 서버 앞에 있는 IPS (침입방지시스템)에 정책 생성 및 등록
- 예시) 4번 필수 기능 정책명 :
test1_*C*B*0*0*F@security
④ 사용자들의 시도 시 IPS에 탐지되었는지 확인

사용자들이 사용한 필수 기능 정보 유무를 웹 서버로부터 수집된 웹 로그 정보가 저장되어 있는

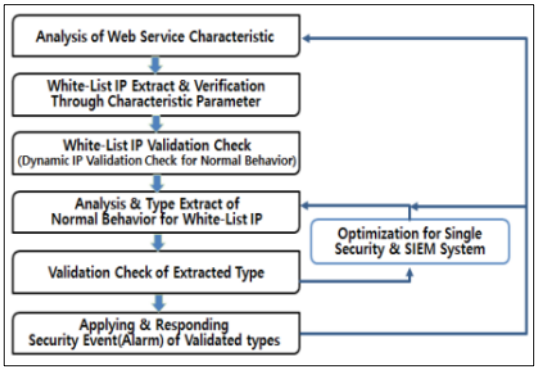


Fig. 1. Propossed Security Monitoring Process

SIEM 시스템에서 검색하여 확인하고, 그 후 웹 서버 앞에 위치한 IPS에 필수 기능 시도가 탐지되도록 파라미터 정보를 시그니처로 만들어 등록하였다. 이때, IPS에 시그니처를 만들어 '탐지'정책으로 운영되게 하였는데, 이는 보통의 웹 서버가 클라이언트와 통신하는 최종 포인트이기 때문에 공격 정보를 먼저 파악할 수 있는 단일 보안 시스템인 IPS에서 탐지되도록 하였다. IPS에서 탐지된 사용자들의 필수 기능 시도 정보는 해당 장비가 알아보기 쉽도록 구분된(Parsing) 영역(Field) 정보에 따라 더 많은 정보가 담겨져 있다. 대표적인 정보로는 공격 시도 문자열이 담겨져 있는 공격명(Attack) 정보와 출발지 IP 및 웹 요청 시도의 상세 정보가 있는 페이로드(Payload) 정보이다.

IPS에 탐지된 정보 중 파라미터(문자열) 정보가 담긴 공격명(Attack) 정보와 출발지 IP는 외부의 사용자들이 필수 기능을 사용할 때의 정보라고 할 수 있으므로, 이 때의 시도는 특수한 웹 서비스를 사용하기 위한 인증된 사용자라고 볼 수 있다. 따라서 그 때의 정보 중 출발지 IP 정보는 정상 사용자라고 판단할 수 있는 화이트리스트 IP로 활용 가능하다. 사용자가 필수 기능을 사용할 때 IPS에서 탐지되는 로그는 SIEM 장비에 누적되므로 이 데이터를 가지고 다음과 같이 화이트리스트 IP를 목록화 해보았다.

- IPS에 탐지된 영역(Field)정보 중 공격명(Attack)이 위의 12가지 필수 기능 파라미터 일 때 출발지 IP 영역(Field) 정보를 중복 제거한 후 SIEM DB에 누적되도록 목록화 기능 사용 (이 해당 설명은 순차적인 화이트리스트 IP의 목록화 절차이며, Fig. 2.로 도식화하였다)

화이트리스트 IP 목록화 결과는 그 자체로도 의미있는 값이지만, 필수 기능을 사용하는 사용자들의 IP가 유동 IP이기 때문에 이를 고려한 목록화 검증 단계도 필요하다. 이를 고려한 화이트리스트 IP의 간단한 유효성 검증 방법은 아래와 같다.

- IP의 평균 변경 주기 설정(분석에 따른 값)
- 최초 IP 누적 후 변경 주기 이후의 특성 파라미터 시도 여부 점검
- IP의 평균 변경 주기에 따른 검증 횟수 설정 후 목록화

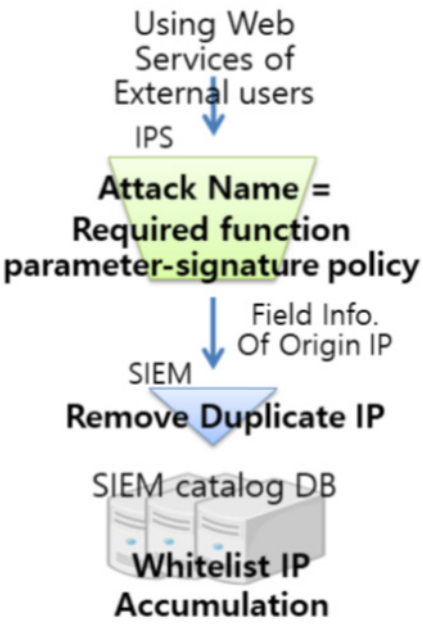


Fig. 2. Whitelist IP accumulation using SIEM

Table 1.은 약 20일간 SIEM 시스템으로 검색하여 IPS 탐지 정보로부터 탐지된 파라미터별 화이트리스트 누적건수와 동일한 IP는 중복 제거한 결과

Table 1. Number of Whitelist IPs by detection parameter

Search period : `18.07.20 ~ 08.08 (20days)	
Parameter info.	Whitelist IP Cumulative count (including duplicates)
*id*e*id*e*a*l.****	41
*en*e*id*e*a*l.****	41
*id*n*t*i*e*ai*_D.****	22
*C*B*0*0*F	763
*ci*a*ic*i*t.*o	12
*o*d*e*is*.*o	576
*u**e**is*.*o	192
*o*t*a*t*n*.*o	538
*o*t*a*t*e*i*i*n*i*w.*o	8
*e*l*i*e*a*e.*o	3,873
*e*l*e*u*s**a*e*r*c.*o	2,527
*r*d**u*_*_N_*u*m*t.*o	5
Total cumulative count	8,598
Whitelist IP number after removing duplicated IPs	4,789

로 누적된 화이트리스트 IP 총 개수를 보여준다.

다음으로 누적된 IP를 활용하여, 탐지되는 전체 시도 중 정·오탐 건수를 판별해보고자 IPS에 탐지되는 전체 건수를 기준으로 정상 사용자 시도인 화이트리스트 IP 건수를 제외해보았다. 단일 보안 시스템 중 방화벽의 경우에는 외부 사용자에게 제공하는 웹 서비스 정책을 불특정 다수에게 열어주고 있으므로 공격 정보를 식별할 수 있는 IPS를 활용하여 확인하였으며, 그 결과는 Table 2.와 같다.

Table 2.는 누적된 화이트리스트 IP를 활용하여 정·오탐 식별에 대한 효과 유무를 확인하기 위해 테스트 하였으며, 위 결과는 20일간 누적된 4,789개 화이트리스트 IP와 2일간의 전체 공격에서의 결과 데이터이므로 추가적인 데이터 테스트가 필요하다. 전력거래시스템을 사용하는 실제 사용자들의 총 IP 개수는 실험 시 확인하기 어려웠지만, 등록 및 인증된 약 2만개 이상의 사용회원들이 있었기 때문에 이 정보를 바탕으로 추가적인 화이트리스트 IP 누적은 가능하다고 판단하였다. 이를 바탕으로 목록화 실험해본 결과로, 약 45일간 누적된 화이트리스트 IP는 8,794개, 약 52일간 누적된 IP는 10,139개가 됨을 SIEM의 누적된 목록화 DB에서 확인할 수 있었고, 각각 늘어난 IP를 활용하여 추가로 2번에 걸쳐 전체 공격 건수 대비 정·오탐을 식별하는 과정을 통해 향상된 결과를 확인할 수 있었다.

Table 2. The result of the false-positives & true-positives identified by the whitelist IP

Search period	`18.08.14 ~ 08.16 (2days)
Search requirement	**4,879 Whitelist IP Usage**
Total number of external attacks	92,005
Removal count of false-positives - Whitelist IP count	540
True-positives count - Attack count excluding whitelist IPs identified as parameters	91,465
Percentage of true positive against all external attacks	99.41%

위 결과는 웹 서비스 특성에서 화이트리스트 IP라는 기준 정보를 통해 확인할 수 있는 의미 있는 데이터 추출이 가능하다는 것을 보여준다. 하지만 단순히 누적된 화이트리스트 IP만으로는 복잡하게 얽혀있는 공격들을 의미있게 판별하였다고 할 수 없다. 제안한 보안관제 프로세스의 단계 중 화이트리스트의 정상 행위 분석을 통해 추가적으로 정제된 과정을 통해 면밀한 보안관제를 할 수 있는 방법을 확인해보았다.

3.3 집중 보안관제 유형 확인, 검증

특성을 통해 추출된 누적 화이트리스트 IP를 가지고 정상 사용자들이 시도하는 유형(공격 및 정상 시도 등)을 웹 서비스 전단에 있는 단일 보안시스템을 통해 분석하였다. IP의 누적 개수에 따라 시도 유형을 검색할 때 더 정제된 결과 값을 가져올 수 있기 때문에, IP 개수를 달리하고 검색 기간을 늘리며 3차례의 결과 추출을 통해 유형을 분석하였다. 최초 시도에는 장비별로 의미있는 유형을 추출하고자 4개 종류의 장비에서 확인하였으며, 이후에는 방화벽과 IPS 에서 의미있는 유형을 확인할 수 있었다. Table 3.은 확인된 유형이다.

Table 3. Type analysis result in communication with White list IP

Item		
Primary Type Analysis	**Secondary type analysis**	**Tertiary type analysis**
Cumulative IP count		
5,246	8,954	10,139
IP accumulation period		
`18.08.14~ 08.22 (9days)	`18.08.14~ 09.03 (22days)	`18.08.14~ 09.13 (32days)
Type search period		
`18.07.23~ 08.22 (34days)	`18.08.09~ 09.06 (32days)	`18.08.12~ 09.13 (36days)
System		
FW,IPS, WAF,DDoS	FW,IPS ※ Multiple feature identification was easy to identify with	FW,IPS ※ Only with FW and IPS

	FW and IPS	
Extraction type		
Drop type	Identify attacks and drop types in normal attempts - Identified some with Attempts for network check and false-positives	Identify attacks and drop types in normal attempts - Identified some with Attempts for network check and false-positives (Reconfirmation)
Type of attempt by origin country	Identified the major time zone used by each country -Identified time zones similar to the first analysis	Identified the major time zone used by each country -Identified time zones similar to the second analysis
Whitelist verification based on departure frequency	Whitelist verification based on departure frequency - Can be used for static IP verification and IP management in security control	No specific info.
Uniqueness by Destination IP	Uniqueness by Destination IP - No specific info. other than secondary server	No specific info.
Unauthorized port identification and uniqueness	No specific info.	No specific info.
Packet size type per parameter	Packet size type per parameter - Identify packet ranges by parameters	Packet size type per parameter - Identify packet ranges and packet for request & reply with web server

분석 결과에서 보듯이 특성 있는 웹 서비스를 하는 시스템인 전력거래시스템에서는 셀에 음영표기한 것과 같이 크게 3종류의 유형이 확인되었다. 하지만 여기서 확인하는 모든 유형이 다른 특성 있는 웹 서비스 시스템에도 100% 적용 가능한 것은 아니다. 유형을 확인하는 과정에서 유효한 항목을 발견할 수 있으며, 이런 과정 및 항목들이 보안관제의 프로세스로 적용될 때 유효한 방법론이 될 수 있을 것이다.

전력거래시스템에서 확인한 첫 번째 유형은 나라별 사용 시간대로서, 각 나라에서 사용자들이 사용하는 시간대의 범위를 확인할 수 있었으며, 이를 통해 사용 시간대 이외의 시간대를 집중적으로 관제할 수 있을 것으로 판단하였다.

두 번째 유형은 특성 파라미터별 패킷 사이즈이다. 파라미터별로 웹 서버 로그와 IPS 탐지 로그를 확인하였다. 파라미터별 페이로드 정보에서는 응답 패킷의 길이는 요청 패킷보다 더 다양했기 때문에, 여기서는 요청 패킷으로만 분석하여 진행했다. 파라미터별 요청 정보를 분석한 결과 일정한 패킷 사이즈의 범위를 확인할 수 있었다. 응답 정보도 같은 방식으로 분석하였지만 사용자가 요청한 기능별로 응답하는 WAS 데이터의 패킷 사이즈가 무작위로 달라져 요청 패킷 사이즈와 비교했을 때 상대적으로 활용 면에서는 의미가 없음을 확인하였다.

세 번째 유형은 오탐 식별 유형이다. 화이트리스트 사용자들이 시도하는 유형 중 80% 이상이 정상 시도가 아닌, 웹 공격 유형에서 HTTPD overflow와 같이 버퍼 오버 플로우 공격 시도였다. 시도의 전후 관계, 대상 및 횟수 등을 확인했을 때 해당 시도들은 공격이 아닌 정상 시도임을 확인하였다. 따라서 80% 이상 화이트리스트가 시도하는 건수에 대해서는 단일 보안 시스템에서 운영하는 정책 값을 조정하여 오탐을 줄여가는 과정이 필요하다. 그리고 나머지 유형을 집중적으로 관제할 수 있을 것으로 판단하였다.

위에서 확인한 3종류의 유형으로 집중 보안관제의 유효성을 확인하기 위해 44일간 누적된 IP 12,241개를 활용하고, SIEM에 저장된 로그를 누적된 IP 기간이 포함된 2, 4, 6주 단위로 검색하여 확인하였다. 여기서, 검색 기간은 각기 다른 2주 단위가 아닌 개별 주차를 모두 포함하는 누적 기간으로 하여 산출 데이터의 결과 질을 높이고자 하였다. 그 결과는 Table 4,5,6,과 같다.

첫 번째 유형인 클라이언트의 주요 사용 시간대

Table 4. Results of validation of major time zones by country

Attempt on country	Philippines		Singapore		Hongkong	
Time range	10~15H		10~18H		10~18H	
Search period	In	Out	In	Out	In	Out
	Attempt count					
`18.08.14 ~ 08.28	2,730	0	2,282	6	1,932	82
`18.08.14 ~ 09.11	4,338	0	2,282	6	1,932	82
`18.08.14 ~ 09.25	6,078	52	3,036	6	2,102	82

유형에서는 실험 대상 특징에 따라 평균 16개 나라에서의 시도가 확인되었으며, 그 중 3개 나라의 사용 시간대에 대해 확인한 결과가 Table 4.이 다. 표에서 보듯, 주로 사용하는 시간대 범위의 시도 건수가 높고, 시간범위 이외에 시도 건수가 현저히 낮음을 볼 수 있다. 따라서 주요 시간대 시도는 제외시키고, 주요 시간대 이외에 시도만을 집중 관제하는 것이 효과적이다.

Table 5.은 두 번째 유형 결과를 보여준다. 앞서 살펴본 실험 대상 시스템의 확인된 특성 파라미터 12 종류 중 사용 빈도수가 가장 높았던 3가지 종류만 선택해서 확인한 결과이다. 특성 파라미터별 패킷 사이즈에서는 사용자의 웹 서비스 정상 시도 시 패킷 사이즈의 범위를 기간 별로 확인

Table 5. Verification of packet size range validity by parameter

Parameter type	*e*l*i*e*a*e.*o		*C*B*0*0*F		*e*l*e*u*s **a*e*r*c.*o	
Time range	235 ~ 1,163 bytes		275 ~ 1,514 bytes		494 ~ 1,094 bytes	
Search period	Range					
	In	Out	In	Out	In	Out
	Attempt count					
`18.08.14 ~ 08.28	20,423	0	13,076	0	27,842	0
`18.08.14 ~ 09.11	44,949	0	25,786	0	62,710	0
`18.08.14 ~ 09.25	68,751	0	36,373	0	97,277	0

하였으며, 이 범위도 6주 동안의 추출 데이터에서 범위의 정제된 값을 확인할 수 있었다. 파라미터별로 검색된 총 건수 대비 패킷 사이즈 범위와 추출된 통계치의 건수 대비 패킷 사이즈의 범위를 상대적으로 비교했을 때, 정상 시도 패킷 사이즈의 범위를 명확히 확인할 수 있었다.

Table 5.의 결과는 패킷 사이즈 범위 이외에 범위가 나오지 않아야 함을 실험적으로 확인한 것이며, 조사된 패킷의 사이즈와 다른 패킷이 나온다면 이는 명확한 공격일 수 있으므로, 이를 집중 관제해야 함을 알려준다. 또한, 검색 기간을 충분히 두어 확인한 패킷 범위 결과는 파라미터별 패킷 범위 결과 중 최대 패킷 사이즈(Max)만으로도 단순 필터 값으로 활용이 가능했다. 파라미터별 최대 패킷 사이즈는 인증된 사용자 중에서 필수 기능 사용 시 패킷 사이즈가 추가될 수 있는 시도가 일어날 때, 예를 들면 인젝션 공격과 같은 시도 등이 일어날 때, 집중적으로 관제할 수 있다.

마지막으로 세 번째 유형은 오탐 식별 유형이며,이에 대해 검증한 결과가 Table 6.이다. 검증을 위해 실험 시 화이트리스트 IP 개수별로 시도

Table 6. The result of the defined attack type validation in the whitelist

Item	Search period		
	`18.08.14 ~ 08.23	`18.08.14 ~ 09.03	`18.08.14 ~ 09.25
Whitelist IP number	6,045	8,964	12,241
Whitelist type count	75,738	135,518	253,665
Excluding normal whitelist types in whitelist type (Attack type) (A)	1,443	2,731	4,967
False-posititves identification (B) (Threshold adjustment Type)	1,271	2,588	4,876
Attack type (True-positives count :A-B)	172	143	91

하는 유형을 추출하였다.

누적된 화이트리스트 IP 개수가 많을수록 운영 시스템으로 유입되는 패킷 전체 중 화이트리스트가 시도한 유형을 제외하였을 경우 90% 이상이 실공격임을 확인하였다. 또한, Table 8.의 결과에서 보듯이 화이트리스트가 시도하는 전체 유형 중에서도 80% 이상의 건수가 오탐 식별을 가능하게 한 유형이었다. 이들은 단일 보안 시스템 보안 정책의 임계치를 조정할 수 있는 유형이다. 앞서 언급한 대로, 80% 이상의 검증은 특성 파라미터 기능을 사용하는 화이트리스트들의 시도를 시간의 전후 관계 및 횟수 분석을 확인한 결과이다. 임계치 조정이 가능하다 함은 보통 클라이언트가 시도하는 공격 혹은 정상 시도 중 단일 보안 시스템의 정책(시그니처)에서 사용자 정의로 수치를 변경하여 공격의 탐지 범위를 조정할 수 있도록 만든 정책에서 확인할 수 있다.

시스템으로 유입되는 전체 패킷 중 화이트리스트 IP의 정상 시도를 제외하여 나머지인 공격을 식별하고, 화이트리스트의 정상 시도 내에서도 오탐을 식별한 결과, 실제 공격 유형(A-B)인 나머지 건수가 정상적으로 공격을 시도한 수치이기 때문에, 이 건수들을 집중적으로 분석하는 것이 다른 시도 건수를 분석하는 것보다 매우 효율적인 방법이다.

추가적으로, 오탐 식별 건수가 많을수록 단일 보안 시스템의 정책 조정 값을 보다 명확히 할 수 있기 때문에, 보안관제 업무 프로세스에서 이를 반영한다면, 보다 정제된 결과 값을 얻을 수 있다.

3.1~3.3절까지의 검증 결과에서 알 수 있듯이 웹 서비스 특성을 반영하여 보안관제할 수 있는 방법이 가능함을 확인하였다. 여기서 확인된 각각의 요소들은 실제 보안관제에도 적용하여 필터링 해볼 수 있으며, 제외된 이후에 나머지만을 집중 관제하는 방법이 일반적인 보안관제 방법과 비교할 때 효과적이다. 집중 관제를 하기 위해 추출된 요소들이 검증되면 그 결과만으로도 매우 의미 있는 피드백 값이기 때문에 그 때 그 때 단일 보안 시스템 및 각종 보안 정책을 변경 및 최적화 하는 단계가 필요하다. 집중 관제 유형 이외의 시도들로만 필터링 되어 관제될 수 있도록 개별적인 집중 관제 요소들은 SIEM 장비 등에 보안 알람 이벤트로 적용하여 상시 보안관제에 적용할 수 있다.

IV. 결 론

본 논문에서는 특수한 웹 서비스를 하는 경우, 필수 기능을 분석하여 특성 파라미터를 추출하고 이를 기반으로 화이트리스트 IP를 추출하여 정상 시도 패킷 분석 후, 확인되는 유형을 이용하여 정상 패킷 이외의 나머지를 집중 관제하는 전반적인 보안관제 프로세스 운영 방안을 제안하였다. 전력거래라는 입찰, 매도, 매수 및 거래 현황 정보 조회 등의 특성 기능이 반영된 전력거래시스템을 실험 대상으로 하여 제안 방법의 효과성을 확인 및 검증하였다.

화이트리스트 IP의 누적 데이터가 많을수록 정상 시도 패킷의 유형 값은 보다 정확해진다. 또한, 그 유형 값을 토대로 집중 보안관제를 했을 때의 비교 수치가, 오탐을 판별하고 정탐을 집중 관제하는데 매우 효율적인 방법임을 확인하였다. 지금까지의 일반적인 보안관제 방법은 보안 인력의 분석 능력 및 상황에 따라 운영의 결과가 달라지는 것이 일반적이나, 제안 방안을 적용한다면, 기준점 제시 후 단계적인 분석 및 필터링이 가능한 유형 적용 등 집중 관제할 수 있기 때문에, 보안관제 인력의 평균 능력을 통해서도 매우 효과적인 관제 결과를 가져올 수 있다.

향후 과제로는 사용자가 사용하는 IP가 유동 IP인 경우 화이트리스트 IP 추출의 추가적인 유효성 검증 절차가 필요하다. 또한, 추출된 유형 중 정의된 공격 유형에서 확인된 결과 값을 통해, 반복적으로 단일 보안 시스템의 정책을 조정함으로써 유형 결과 값을 보다 명확히 하는 과정이 필요하다. 마지막으로, 화이트리스트 패킷 기반의 유형 추출 시 세부적인 조건 값을 활용하여 보다 정밀한 데이터를 만들 수 있다는 점을 고려하여, 추가적인 유형 발굴이 필요하다.

본 논문에서 검증한 보안관제 모델로서도 충분히 집중적으로 공격 패킷을 관제할 수 있다는 점은 의의가 매우 크다. 몇 가지 추가 과제를 활용하여 적용한다면 더욱 정제된 보안관제 데이터를 얻을 수 있을 것이다.

References

[1] Gil-Heon Song and Soo-Woong Kim, "A Study on Enhancing Enterprise

Security through Big Data-based Security Control," Korea Management Information System Society Spring Conference, Vol.2016, No.06, pp. 286-299

〔2〕 JinGuk-Um, "Model Proposal for Detection Method of Cyber Attack using SIEM," Thesis of Master's degree, The graduate of Korea University, pp. 5, Dec. 2016.

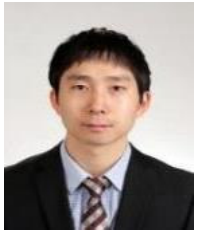
〔3〕 Kyung-Shin Kim, "Security Analysis and Improvement of Integrated Security Management System," The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), 15(1), pp. 17, Feb. 2015

〔4〕 Hyun-Chul Chang, "A Study on Integrated Security Management Method of Heterogeneous Security Systems," Thesis of Master's degree, The Graduate of Konkuk University, pp. 23, Dec. 2015

〔5〕 Byung-chul Kim, "Big Data Security Technology and Response Study," The Journal of Digital Policy & Management, 11(10), pp. 447, Oct. 2013

〔6〕 Seung-Yong Kang, "A Derivation of Log Analysis Scenario for Effective Security Monitoring," Thesis of Master's degree, The graduate of Jeonnam National University, pp. 25, Aug. 2016

〈저자소개〉



이 재 헌 (Jae-heon Lee) 정회원
2008년 2월: 숭실대학교 정보통신전자공학부 졸업
2013년 3월~현재: 한국전력거래소 정보보안팀
2017년 9월~현재: 고려대학교 정보보호대학원 사이버보안학과 석사 졸업 예정
〈관심분야〉 인공지능 보안관제, 비정상 행위 탐지, CPS 보안

이 상 진 (Sang-jin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학 대학 조교수
2008년 3월~현재: 고려대 정보보호연구원 디지털포렌식연구센터장
2017년 3월~현재: 고려대학교(정보보호대학원) 원장
〈관심분야〉 대칭키 암호, 정보은닉이론, 컴퓨터 포렌식