Journal of the Korea Industrial Information Systems Research Vol.26 No.5, Oct. 2021 :69-77
http://dx.doi.org/10.9723/jksiis.2021.26.5.006 ISSN:1229-3741

효과적인 보안관제를 위한 위협정보 우선순위 도출+

(Analysis of Threat Information Priorities for Effective Security Monitoring & Control)

강 다 연[1)]
(DaYeon Kang)

요 약 본 논문에서는 기업의 IT시스템에 대한 위협에 대응하고자 하는 기업의 자산을 지켜주는데 매우 중요한 영역인 보안관제 위협정보를 확인하고자 한다. 보안관제는 보안 장비에서 발생한 이벤트, 로그를 중심으로 실시간 분석하여 위협을 판정하고 대응한다. 보안관제 업무에 있어서 우선적으로 위협정보를 평판정보와 분석정보로 구분하여 우선순위를 도출하고자 한다. 평판정보는 Hash, URL, IP, Domain으로 구성하였으며, 분석정보는 E-mail, CMD-Line, CVE, 공격동향정보로 구성하여 분석하였다. 연구결과, 평판정보의 우선순위가 상대적으로 높았으며 위협정보에 대한 정확성과 대응성을 높이는 것에 의의가 있다.

핵심주제어: 보안관제, 위협정보, 평판정보, 분석정보, 우선순위, 중요도

Abstract This study aims to identify security-based threat information for an organization. This is because protecting the threat for IT systems plays an important role for an corporate's intangible assets. Security monitoring systems determine and consequently respond threats by analyzing them in a real time situation, focusing on events and logs generated by security protection programs. The security monitoring task derives priority by dividing threat information into reputation information and analysis information. Reputation information consisted of Hash, URL, IP, and Domain, while, analysis information consisted of E-mail, CMD-Line, CVE, and attack trend information. As a result, the priority of reputation information was relatively high, and it is meaningful to increase accuracy and responsiveness to the threat information.

Keywords: Security Monitoring Control, Threat Information, Reputation Information, Analysis Information, priority, importance

1. 서 론

기업을 경영하는데 필수적인 중요 정보는 IT 시스템 상에 존재하고 있다. 많은 기업들의 주요 사업 자산이 해킹에 의해 유출되거나 또는 랜섬웨어에 감염되거나 하는 이유로 시스템의 파괴 또는 서비스 마비 등이 일어나는 경우가 발생하기도 한다. 이로 인해 기업이 영속성에 직접적인 영향을 받기도 하며 기업이 가지게 될

* Corresponding Author: kang@dau.ac.kr
+ 이 논문은 동아대학교 교내연구비 지원에 의하여 연구되었음.
Manuscript received April 14, 2021 / revised May 06, 2021 / accepted June 09, 2021
1) 동아대학교 경영정보학과, 제1저자

불이익에 또한 악영향을 미치기에 여러 힘든 상황에 직면하게 된다. 그렇기에 많은 기업이 보안솔루션을 도입하고 운영하고 있는 실정이며, 위협 탐지 및 대응에 필요로 하는 보안관제 서비스의 24시간 365일 기업 보안을 더욱더 강화하고 있다.

보안관제는 보안 장비에서 발생한 이벤트, 로그를 중심으로 실시간 분석하여 위협을 판정하고 대응한다. 이는 기업의 IT시스템에 대한 위협에 대응하고자 하는 기업의 자산을 지켜주는 부분에서 무엇보다 중요한 업무의 역할이다.

보안관제는 언제 발생할지 예측할 수 없기에 사전에 대응하기가 쉽지 않은 부분이다. 정보기술이 발달하면서 해킹에 대한 범죄가 보다 지능적으로 변화해가면서 다양한 악의적인 수법이 많이 발생하고 있기에 기업의 정보보안에 관한 보안관제는 더욱더 필요하고 매우 중요하다.

기업에서 위협이 발생하기 이전에 정보보안 사고에 대한 대비를 위한 방안을 마련하는 것이 중요하다. 특히, 기업의 데이터를 안전하게 보호하기 위해서는 사이버 침해 및 해킹의 위협으로부터 차단하고자 사전에 대비하는 것이 우선적이다.

KISA(2020)의 2021년 사이버 위협 전망 자료에 따르면 2020년의 랜섬웨어는 코로나-19 대유행에 따른 위장형 공격과 원격근무 시스템을 노린 이메일 그리고 원격접속에 의한 악의적인 공격이 유행하였기에 발생하는 피해가 더욱 증가하였다. 특히 소디노키비 (Sodinokibi)랜섬웨어의 경우를 보면 결재용 포스기기를 검색하고 카드정보를 수집하는 형태의 변종이 보고되었으며, 최근 공격자들은 협박 수단을 강화하기 위하여 피해자의 민감한 정보를 유출하고 2차 범죄수익을 발생시키기 위한 다양한 시도를 수행하고 있어, 랜섬웨어의 피해규모가 확대 될 것이라고 전망하였다. 또한 고도화된 표적 맞춤형 악성 이메일과 대량 피싱이 결합한 매스피어링이 등장하면서 Emotet 악성코드를 활용하여 스팸 메일을 생성하고 배포가 증가하였으며, 다크웹 시장에서의 거래와 이에 따른 사이버 범죄조직 규모의 확대가 공격 기법 및 방식을 더욱 강화하면서 많은 피해를 우려하고 있다.

기업의 보안 관련 연구로는 금융보안 분야의 연구동향을 비교 분석한 연구를 통해 향후 연구분야 도출의 방향성을 제시한 연구가 있으며(Chae et al.,, 2021), 금융회사의 정보보호 보안업무 자신감에 영향을 미치는 요인들에 관한 관계를 분석한 연구가 있다(So and Kim, 2017). 또한 시스템 개발적인 부분에서는 비밀번호의 보안성을 향상시키기 위한 인식시스템을 개발하여 기업들의 보안매체와 투자에 관한 관심을 높이는 연구가 진행되었다(Choi et al., 2017).

기업의 효과적인 보안을 위한 연구로 보안관제와 관련된 업무개선 방안에 관한 연구 및 보안관제 측면에서의 제도적인 개선에 관한 연구들 중 Hong and Lee(2021)의 연구에서는 인공지능기반 보안관제 플랫폼 개방 방안을 신규 보안 기술 대응 모델 연구를 통한 적용 범위 확대를 통한 공격 동향 수집과 분석, 데이터 생성 기법을 통한 대응모델을 통해 분석 자동화를 지속적으로 관리하고, 유해 IP관리, 보안이벤트 탐지정책 관리, 보안업무 법제도 관리 하는 통합관제 체계를 구축해야 할 필요성을 언급하였다. Oh and Jo(2019)는 인공지능기술을 통합보안관제 기술에 적용하는 방안으로 비 정상행위 위협에 대응력을 강화하는 학습방법으로 데이터의 수립처리부터 머신러닝기술을 도입하여 인공지능 처리 능력을 강화하는 방안을 제시하였다. 또한 Jo and Shin(2019)은 보안관제조직의 특성에 맞는 사이버보안 프레임워크를 제시하기 위해 보안관제센터의 환경에 맞도록 NIST CFS에서 구현된 dentify-Protect-Detect-Respond-Recover 5개 기능을 기반으로 management 기능을 추가하였다. Pi and Park(2019)은 다크웹 환경에서 크롤러와 엘라스틱서치를 이용한 산업보안을 위한 보안관제 모델을 제시하였다 하지만 위에서 분석한 기존연구들을 살펴보면 인공지능기술 기반연구와 기술기반 보안관제 프레임워크를 제시한 연구는 있었지만(Hong and Lee, 2021; Oh and Jo, 2019; Jo and Shin,2019), 보안관제 위협정보 요인을 평판정보와 분석정보로 구분하여 보안관제의 위협 정보의 우선순위를 도출하는 보안관제 연구는 없었다.

따라서 본 연구는 이러한 많은 피해를 발생시

키는 수많은 보안 위협 중 보다 효과적으로 대응하기 위한 보안관제의 위협정보 요인을 도출하여 그 중요성에 대한 우선순위를 살펴보고 보안관제에 대한 업무 항목을 평가하는 데 그 목적이 있다.

2. 선행연구

2.1 보안관제 개념과 중요성

보안 관제란 '조직의 정보기술 자원 및 보안 시스템을 안전하게 운영하기 위해 사이버 공격 정보를 탐지 및 분석하여 즉시 대응하는 일련의 업무'이다. 보안관제의 행위가 이루어질 때 정부와 기업에서는 보안 위협을 식별하고 사용자 인식강화 및 대응체계 점검을 위한 예방 활동을 수행하고 보안 시스템에서 발생하는 이벤트를 수집하여 상관분석 결과를 토대로 대응하고자 하는 목표가 있다(Kim et al., 2009).

기존의 보안관제에서 이루어지는 전산 자산 취약점의 진단이 먼저 국내에 사전에 규정된 진단 항목으로 이뤄졌다. 즉, 표준화된 취약점 항목들에 대한 점검이었다(Jo and Shin, 2019). 취약성은 외부의 위협이 목표로 하는 시스템에 악의적인 영향을 미칠 수 있는 사이버 공격이다. 해커들의 지능적인 공격을 대처하는 방안으로 보안 위협이 되는 정보를 체계적으로 분석하는 연구가 필요하다.

디지털 전환의 발 빠른 움직임의 변화에 따라 클라우드 중심의 비즈니스 환경을 구축하려는 대다수 금융기관과 공공분야의 기관들의 관심이 많은 편이다. 이에 혁신을 추구하는 디지털 환경에 적합한 보안 환경의 영향도 매우 높아지고 있다. 전통적인 보안 환경에서는 통합보안 관제센터를 토대로 침해 대응을 위한 정보보호 체계와 개인정보보호 체계를 구축해 왔다. 그리고 이를 토대로 보안 관제를 수행했지만, 혁신적 기술을 기반으로 한 서비스의 개념에서는 자동화된 보안 체계도 클라우드 환경 기반으로 운영되고 제공될 것이다.

최근 정부 및 공공기관과 기업들은 사이버 침해사고 대응을 위해 보안관제 업무를 보다 강화하고 있다. 더군다나 신종 사이버 위협에 대한 탐지와 대응 역량이 정보시스템과 데이터를 보호하는데 핵심 요소임이 확인되었기에 보안관제 업무의 중요성은 더욱 높아지고 있다(Yonhapnews, 2021)

또한 IT 환경의 급변화는 다양한 IT 인프라 활용에 따라 기업의 중요정보 즉, 자산에 접근하는 경로와 방식이 다양해지며 새로운 보안 위협의 등장에 대한 두려움이 더욱더 심각해지고 있다. 이전의 수동적인 관제 중심에서의 전환이 시급히 필요하며 능동적인 보안 관제를 위한 변화에 중점을 두는 것이 무엇보다 중요하다. 인공지능을 정보보안 분야에 접목하여 차세대 보안 관제를 기대하는 방향의 긍정적인 전략이 필요할 것이다. 하지만 고성능 인공지능 기반 융합보안의 영역도 결국 인간의 직관력을 기반으로 평가하여 운영하고 관리하는 것이기에 보안관제 전문가를 위한 인력양성을 위한 방안의 중요성은 더욱 높아질 것이다.

2.2 보안관제 관련 연구

최근 보안관제 연구로 4차 산업 기술 중 관심이 높은 인공지능 기반과 융합한 분야의 적용이라는 부분의 연구가 많다. 보안관제 구축 및 대응 방안을 인공지능기반의 플랫폼 개발 방안을 제시한 연구(Hong and Lee, 2021)는 차세대 보안체계를 운영하여 신규위협에 대한 처리범위와 속도향상을 높이면서 기존의 수동적인 이벤트 처리 방식의 한계를 보완하고자 연구하였다. 또한 인공지능 기술기반의 통합보안관제 서비스모델을 제시하고자 개발한 연구에서는 정상 행위 기반의 학습모델을 개발하였으며 이는 식별되지 않는 비 정상행위 위협에 대응력을 강화하기 위한 방안이었다(Oh and Jo, 2019). 다중 검색엔진을 이용해 자산의 취약점을 사전에 점검하여 특수한 취약점을 보호하고자 하는 관점에서 보안관제 모델을 제한하는 연구도 있었다(Lee and Jo, 2021). 이는 해킹 관련 다중 검색엔진을 활용하여 보호 자산의 사전 취약점 대응 기능을 추가한 보안 관제모델을 제안하였다. 이외 침해

위협에 대한 대용량 보안이벤트 데이터를 동적으로 상관 분석하여 보안관제 시스템 설계를 위한 연구가 있다(Jeong and Park, 2011). 이는 탐지효율성과 신속성을 향상시킬 수 있는 방안에서 보안관제 시스템 설계를 제안하였다.

2.3 보안관제 업무

보안관제 업무에 대한 프로세스는 5단계로 구성되어 있다. 순환구조의 프로세스 형태로 예방, 모니터링, 분석, 대응 및 조치, 보고 단계이다.
가트너에 의하면 보안 위협이 급증하고 있으며, 대응하기 위한 보안 솔루션도 급속하게 늘고 있는데 이는 보안관제 업무가 복잡해지고 있어서 SOAR(Security Orchestration, Automation and Response)의 필요성에 대해 언급하였다. 지능화된 사이버 위협에 대응하기 위해서 기업에서 도입하는 다양한 해결책의 도입이 이뤄지고 있지만, 보안 담당 기관이나 담당자의 역할은 업무의 과중으로 이어지고 있는 현실이다. 이를 해결하고자 하는 대응 방안이 SOAR 자동화된 보안 전략임을 강조하고 있다. 지능화된 사이버 위협에 대응하기 위해서 기업에서 도입하는 다양한 해결책의 도입이 이뤄지고 있지만, 보안 담당 기관이나 담당자의 역할은 업무의 과중으로 이어지고 있는 현실이다.

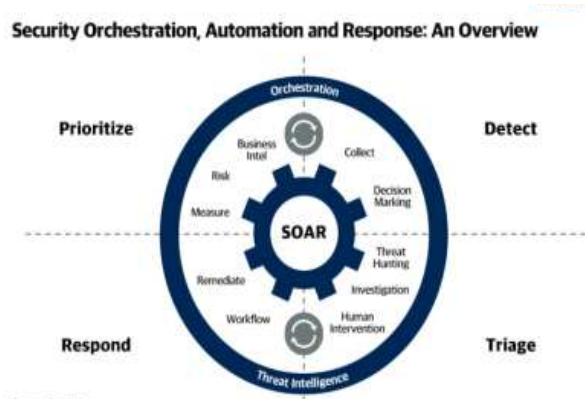

Fig. 1 SOAR
(source: Gartnet(2017), Innovation Insight for Security Orchestration, Automation and Response, White paper, 30 November.)

지능화된 사이버 위협에 대응하기 위해서 기업에서 도입하는 다양한 해결책의 도입이 이뤄지고 있지만, 보안 담당 기관이나 담당자의 역할은 업무의 과중으로 이어지고 있는 현실이다. 이를 해결하고자 하는 대응 방안이 SOAR 자동화된 보안 전략임을 강조하고 있다. SOAR은 자동화 (SOA, Security Orchestration and Automation), 보안사고 대응 플랫폼(SIRP, Security Incident Response Platform), 위협 인텔리전스 플랫폼 (TIP, Threat Intelligence Platform)의 세 가지 보안 대응 영역을 제공한다. SOA는 다양한 보안시스템과 상호작용을 통해 연동을 지원하고, 이를 기반으로 자동화 할 수 있어야 하는 역량이다. SIRP는 보안사고 대응의 전반적인 과정을 하나의 플랫폼에서 정의된 사고대응 워크플로를 기반으로 퍼리할 수 있어야 하는 역량이다. 그리고 TIP는 조직에 위협이 되는 사이버보안위협 정보, 인텔리전스들을 통합하고 활용 할 수 있는 역량을 말한다.

이에 조직은 SOAR을 도입하면서 기대 할 수 있는 효과로는 기업의 입장에서는 보안 영역 투자 대비 효율을 추구하는 것이 가능하고 실무자의 입장에서는 즉시 대응 프로세스 조치를 취할 수 있기에 단순 반복적으로 수행하는 업무 시간의 절감과 대응에 집중할 수 있다는 부분이 있다. 또한 관리자의 입장에서는 사고 대응에 대한 파악의 속도가 빠르게 최적화된 프로세스 기반의 보안 역량을 기대할 수 있는 환경의 구축이 가능하다는 부분이 Fig. 1과 같다(Gartner, 2018).

차세대 보안관제 진화를 돕는 방안으로 SOAR의 관심도가 높으며, 보안 위협을 수집한 분석 시스템으로 이를 분석하고, 그 결과 차단 시스템에서 차단하도록 만들어 위협 대응 정책을 업데이트하면서 유사 위협에 대해 대응을 하기 위한 전략이라는 부분에서 기대하는 바가 크다.

하지만 프로세스에 대한 표준화 및 보안사용사례에 대한 대응 자동화에 관한 제도적 기술적 향상에 대한 지원이 원활하게 이루어지고 있지 않다. 보안관제 센터에서 각종 보안 위협을 실시간으로 감시 및 분석하고 대응하는 보안관제

업무에서 무엇보다 중요한 것은 보안 위협정보를 분류하는 것부터 추가 제공되는 각종 정보를 종합적으로 최신 위협에 방어할 수 있어야 하는 사항까지 포괄하여 업무를 수행해야 한다. 즉, 효과적인 보안 관제를 위해서 중요한 위협정보를 평판 정보, 분석정보로 구분하여 위협정보에 대한 중요도를 분석하여 중요도가 높은 정보의 관리를 위한 보호 및 예방방안에 대한 조치가 먼저 이뤄질 수 있도록 관심을 가지는 것이 중요하다. 결과적으로 신뢰를 기반을 둔 안전한 IT 자산 보호를 가능하게 해주는 것에 큰 영향을 미치는 것 중 가장 중요한 부분이 보안관제이다. 본 연구를 위해 평판정보와 분석정보를 선정한 기준은 평판정보와 분석정보의 요소들을 활용함으로써 사이버 위협정보에 대한 정확성을 높이고, 신속한 대응력을 도출해 낼 수 있기 때문이며, 결과적으로는 보안솔루션에 적용될 수 있는 정책을 개발해낼 수 있기 때문이다(Kim, 2019, Partk et al. 2018)

3. 연구 설계

3.1 연구모형

본 연구는 효과적인 보안관제 위협정보를 도출하기 위하여 금융업에서 사이버 위협정보를 분석하는 화이트해커와 취약점진단 전문가들에게 주로 활용하는 위협정보의 요소에 대해 델파이기법을 통한 2차에 걸친 인터뷰와 검토를 통해 선정되었다. 보안관제 정보를 평판정보과 분석정보 분류하여 평가항목들에 대한 정보요인들을 선정되었으며, 상대적 정보의 하위항목의 상대적 중요도 우선순위를 AHP(Analytic Hierarchy Process)를 적용하여 쌍대비교를 통해 도출하고자 한다(Lin and Hsieh, 2004). 본 연구수행을 위한 연구모형의 설계는 Fig. 2와 같다.

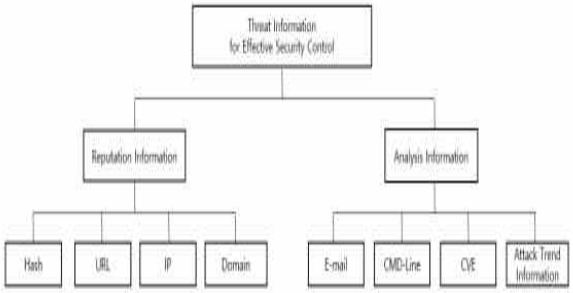

Fig. 2 Research Model

3.2 연구모형의 항목

본 연구모형에 포함된 평가기준과 항목에 대한 1계층, 2계층에 관한 내용은 Table 1과 같다.

Table 1 Demographics of Experts Characteristic

Evaluation criteria	Evaluation item	explanation
Reputation Information	Hash	Hash function
	URL	Uniform Resource Locator
	IP	Internet Protocol address
Analysis Information	Domain	Domain Information
	E-mail	E-mail Information
	CMD-Line	Command-Line
	CVE	CommonVulnerabilities and Exposures
	Attack trend Information	Information that reflects attack trend

4. 실증분석

4.1 연구 도구 및 자료수집

본 연구는 보안관제 관련 보안전문가를 대상으로 설문하여 Satty의 AHP(Analytic Hierarchy Process)를 활용하여 계층 분석적 의사결정을 평가하기 위해 실증 분석하였다(Satty, 1990). AHP는 의사결정의 전 과정을 여러 단계로 나

눈 후 이를 단계별로 분석 해결함으로써 합리적이고 최종적인 의사결정에 이를 수 있도록 지원해 주는 방법으로 의사 결정방법 중 복잡한 상황의 구조화, 합리적 그룹의사결정 도출 등을 위한 과학적이고 강력한 의사결정 방법이라고 할 수 있다(Chanm and Kumar, 2007). 본 연구는 효과적인 보안 관제를 위한 위협정보를 평가하기 위한 연구이며, 이에 보안전문가들의 의견사항을 수렴하기 위해 일차적으로 보안관제와 관련하여 위협정보라고 인식하는 평판 정보와 분석정보에 대한 연구모형을 설계하기 위한 인터뷰 및 설문이 이뤄졌다. 이를 기반으로 최종 연구모형을 설계하였으며, 전문가들의 의견을 수렴하여 평가항목에 대한 근간을 구성하였다. 또한 보안관제 위협정보의 우선순위를 도출하는데 충분히 평가항목들에 대한 이해도가 높고 보안관제 위협정보에 대한 상대적 중요도를 측정할 수 있는 보안 분야에 종사한 경력이 최소 10년 이상 20년 이하의 현직에 종사하고 있는 전문가들을 대상으로 설문을 수행하였다. 총 10인의 전문가들에게 설문지를 배부하여 최종 10부 회수하였으며, AHP 분석을 위해 Expert Choice2000을 활용하여 분석하였다. 전문가들의 인구 통계적 분석 결과는 SPSS 20.0을 사용하여 결과를 도출하였다. 설문의 응답자에 관한 일관성을 확인하기 위해 AHP의 일관성 지수(CI; Consistency Index)가 0.1 이하인 응답의 결과로 신뢰할 수 있는 설문으로 판단하여 분석을 진행하였으며, 회수한 설문지 모두 일관성 지수가 양호하여 최종분석에 활용되었다(Harker, and Vargas, 1987).

최종분석을 위한 설문 응답자의 특성으로 Table 2에 제시된 설문 응답자인 보안관제 위협정보를 평가하기 위한 관련 전문적인 경험은 10년에서 20년 이상이었으며, 보안 분야의 전문가가 현재 소속된 산업 분야로는 정보통신업이 1명(10%), 금융보험이 1명(10%), 정보기술업이 8명(80%)으로 나타났다.

그리고 위협정보 DB 활용이 필요한가에 대한 응답으로 DB 활용이 필요하다가 9명(90%), 필요 없다가 1명(10%)으로 분석되었다.

Table 2 Demographics of Experts Characteristic

Experts Characteristic	Remark	People
professional experience	10-20 (Year)	10
financial insurance	industry	1
Inforamtion Communication	industry	1
Information Technology	industry	8
Threat Information DB	Yes	9
	No	1
Total	100%	

4.2 분석 결과

본 연구의 목표인 효과적인 보안관제 위협정보의 우선순위의 중요도를 평가한 결과 Table 3과 같다. 우선 1계층의 우선순위 분석의 결과는 평판 정보 항목이 중요도 0.677로 가장 높게 나타났으며, 그다음으로 분석정보가 0.323으로 나타났다. 중요도 수치에 대한 차이가 있는 결과를 확인하였다.

Table 3 Results of the Layer 1

Layer 1	Weighting	Priority
Reputation Information	0.677	1
Analysis Information	0.323	2
CI	0.00	

Table 4는 연구모형에서 제2계층 항목에 포함되는 요인들에 관한 결과를 제시하였다. 첫 번째 평판 정보 항목에서 가장 수치가 높게 나타난 항목은 Hash로 중요도 0.468로 나타났으며, 1순위를 차지하였다. 다음으로 0.241의 IP 항목, 0.182의 URL이 3순위, 마지막 도메인이 4순위로 중요도 수치가 0.111로 나타났다.

두 번째 분석정보 항목에서의 결과에서는 0.378의 수치로 1순위를 차지한 항목은 CVE이었으며, 다음으로 0.266의 중요도를 나타낸 CMD-Line이 2순위, 다음으로 공격 동향 정보

의 수치가 0.264로 나타나 3순위를 차지하였으며, 끝으로 0.092로 나타난 E-mail 항목 순으로 결과가 나타났다.

Table 4 Resuls of the Layer 2

Layer 1	Layer 2	Weighting	CI	Priority
Reputation Information	Hash	0.467	0.06	1
	URL	0.182		3
	IP	0.241		2
	Domain	0.111		4
Analysis Information	E-mail	0.092	0.03	4
	CMD-Line	0.266		2
	CVE	0.378		1
	Attack trend Information	0.264		3

Table 5는 계층별 평가항목에 대한 중요도 결과를 나타낸 것이다. 최종적으로 평판 정보의 Hash가 가장 위협한 정보임을 나타낸 중요도 수치 0.316으로 1순위 결과로 분석되었으며, 다음으로 평판 정보의 IP 위협이 0.163으로 2순위, 역시 평판 정보의 URL아 3순위로 중요도 수치가 0.123으로 나타났다. 다음으로 4순위는 분석정보의 항목에 포함된 CVE로 0.122의 수치를 확인할 수 있었으며 5순위는 분석정보의 CMD-Line으로 0.086의 수치를 차지하였다. 다음으로 분석정보 항목인 공격 동향 정보가 6순위, 평판 정보의 도메인이 7순위, 마지막으로 분석정보의 E-Mail이 8순위로 가장 낮은 중요도를 차지하는 것을 확인할 수 있다.

Table 5 Results of Priority Layer2

Layer 1	Layer 2	Weighting	Priority
Reputation Information	Hash	0.316	1
	URL	0.123	3
	IP	0.163	2
	Domain	0.075	7
Analysis Information	E-mail	0.030	8
	CMD-Line	0.086	5
	CVE	0.122	4
	Attack trend Information	0.085	6

Table 6에서는 최종분석 결과에 대한 순위를 제시한 것이다. 총 1순위부터 8순위에 해당하는 항목을 제시하고 각 항목에 포함된 1계층의 정보 항목 유형을 제시하였다.

Table 6 Final Analysis Result

Final Rank		Information
Rank 1.	Hash	Reputation
Rank 2.	IP	Reputation
Rank 3.	URL	Reputation
Rank 4.	CVE	Analysis
Rank 5.	CMD-Line	Analysis
Rank 6.	Attack trend Information	Analysis
Rank 7.	Domain	Reputation
Rank 8.	E-mail	Analysis

5. 결 론

최근 보안 위협에 대한 정보를 파악하여 분석하는 위협 인텔리전스에 대한 필요성을 많이 언급하고 있다. 즉, 다양한 경로에서 발생하여 수집하게 된 위협정보를 사전에 입수하게 된다면, 고도화된 보안 위협에 대한 대응이 보다 신속하게 이뤄질 수 있을 것임이 분명하기 때문이다. 보안관제 센터에서는 위협 인텔리전스와 같은 과정을 통해 보안관제 대상과 연관성이 있는 정보를 선별하기도 하며, 공격자의 의도된 취약점에 대해서 정보를 파악하고 분석하고 검토하기도 한다. 하지만 보안관제의 효율성을 높이기 위한 위협 인텔리전스 활용 방안이 있음에도 불구하고, 발생하게 될 위협에 대한 대처를 잘하려는 방안으로 보안관제의 위협정보에 대한 구분을 평판 정보와 분석정보로 구분하여 위협중요도를 평가한 연구가 없었기에 본 연구에서 보안관제 위협정보를 평가할 수 있는 전문가를 대상으로 위협정보에 대한 중요도를 평가하여 우선순위에 대해 알아보았다.

분석 결과, 평판 정보가 0.677, 분석정보가 0.323의 가중치로 나타나서 평판 정보의 위협정

보 중요도가 더욱 높다는 것을 확인할 수 있었다. 또한 평판 정보의 하위계층 항목에서는 Hash, IP, URL, Domain 순으로 위협정보에 대한 중요도 순으로 나타났으며. 분석정보의 하위계층 항목에서는 CVE, CMD-Line, Attack trend Information, E-mail 순위로 중요도가 높게 나타났다.

최종적인 위협정보에 대한 순위로 총 1위부터 8위까지 분석되었다. 1위부터 3위까지는 3계층 중요도 분석 결과와 같은 Hash, IP, URL이었으며, 4위는 CVE, 5위는 CMD-Line, 6위는 Attack trend Information, 7위는 Domain, 8위는 E-mail 으로 확인되었다. 평판정보의 우선순위가 높게 나타난 결과는 위협정보가 생성, 배포될 때 악성 IP, 파일 Hash, Domain정보 및 연관된 공격이 발생하기 때문이다. 이는 악성 위협임을 확인하는데 중요한 역할을 한다. 분석정보는 이미 분석된 정보에 대해 정확히 방어가 가능하고 차단할 수 있도록 하기에 분석정보에 대한 대응으로 인해 서비스에 대한 영향도를 작게 가져갈 수 있는 특징이 있는 것으로 판단한다. 따라서 주로 오픈소스 형태의 평판정보의 지속적인 운영과 관리가 무엇보다 중요하다고 할 수 있다.

본 연구의 의의는 보안 관제를 위한 위협정보 중요도 우선순위 순으로 위협정보를 위한 관제 중요 지침이나 정책이 보다 강화되면 보안관제의 효율적인 운영 및 관리가 보다 더 잘 이뤄질 것이라 기대하기에 실무적으로 활용방안을 제시하는 바에 있다.

본 연구의 한계점으로는 보안관제의 위협정보를 평판 정보, 분석정보로 국한하여 실증 분석하여 연구를 진행하였기에, 추후 연구에서는 더 다양한 관점에서 위협정보를 구분하여 비교· 분석하는 실증연구가 필요할 것이다. 또한 보안관제의 업무에 대한 신뢰성을 높이는데 영향을 주는 요인들을 분석하는 연구가 추후 진행되어 보안관제 업무를 수행하는 담당 기관이나 담당자의 업무의 효율성 향상 증대에 이바지할 수 있도록 할 필요성이 있다.

References

Chae, H. G., Lee, G. H. and Lee, J. Y.(2021). Analysis of Domestic and Foreign Financial Security Research Activities and Trends through Topic Modeling Analysis, *Journal of the Korea Industrial Information Systems Research*, 26(1), 83-95.

Chanm, F. T. S. and Kumar, N. (2007). Global Supplier Development Considering Risk Factors using Fuzzy Extended AHP-based Approach, Omega, 35(4), 417-431.

Choi, Y. B., Kim, J. H., Kim, J. W. and Moon, B. H.(2017). Implementation of OTP Detection System using Imaging Processing, *Journal of the Korea Industrial Information Systems Research*, 22(6), 17-22.

Gartnet(2017), Innovation Insight for Security Orchestration, Automation and Response, White paper, 30 November.

Harker, D. T. and Vargas, L. G.(1987) The theory of ratio scale estimation: Satty's analytic hierarchy process, *Management Science*. 33(11), 1383-1403.

Hong, J. H. and Lee, B. Y. (2021). Artificial Intelligence-based Security Control Construction and Countermeasures, *The Korea Contents Society*, 21(1), 531-540.

Jeong, K. M. and Park, H. S. (2011). Design of a Security Monitoring System based on correlation analysis. *KSCI review Conference*, 335-338.

Jo, C. S. and Shin, Y. T. (2019). A Study on Improvement of Cyber Security Framework for Security Operations Center, *Convergence security journal*, 19(1), 111-120.

KISA (2020), *KrCERT/CC publishes the trends of cyber threat for 2021 with AusCERT, CERT-In, and Sri Lanka*

CERT/CC, 07 Dec.

Kim, B. I. (2019). Automatic collection and analysis of cyber threat information, ICT R&D Trend, 31-37.

Kim, Y. J., Lee, S. H., Kwon, H. Y. and Lim, J. I. (2009). A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services, *Journal of the Korea Institute of Information Security and Cryptology*, 19(1), 103-111.

Lee, J. K. and Jo, I. J. (2021), Improvement Mechanism of Security Monitoring and Control Model Using Multiple Search Engines, T*he Korea Contents Society*, 21(1), 284-291.

Lin, C. and Hsieh, P. J. (2004). A Fuzzy Decision Support System for Strategic Portfolio Management. *Decision Support Systems*, 38, 383-398.

Oh, Y. T. and Jo, I. J. (2019) Development of Integrated Security Control Service Model based on Artificial Intelligence Technology, *Korea Contents Society*, 19(1), 108-116.

Park, J. B., Choi, B. H. and Jo, H. S. (2018), A Study on the Activation of Cyber Threat Information Sharing, Journal of The Korean Institute of Communication Sciences, 35(7), 41-48.

Pi, D. K, Park, W. H. (2019). A study on Security Control & Monitoring Model of Industrial Security Threat in the Darkweb Environment, The Korea Association for Industrial Security, 9(1), 117-140.

Satty, T. L. (1990). How to Make a Decision: The Analytic Hierarchy Process, European Iournal of Operation Research, 48(1), 9-26.

So, H. C. and Kim, J. K.(2017). Influence of Information Security Activities of Financial Companies on Information Security Awareness and Information Security Self Confidence : Focusing on the Mediating Effect of Information Security Awareness, *Journal of the Korea Industrial Information Systems Research*, 22(4), 45-64.

Yonhapnews. (2021). *Strengthening the prevention of cyber threats such as hacking,* https://www.yna.co.kr(Accessed on Feb, 18th, 2021).

강 다 연 (DaYeon Kang)

- 정회원
- 한국해양대학교 해운경영학과 경영학사
- 부산대학교 경영학과 경영학석사
- 한국해양대학교 해운경영학과 경영학박사
- (현재) 동아대학교 경영대학 경영정보학과 조교수
- 관심분야: 정보시스템 보안, 보안정책, 클라우드 컴퓨팅, 경영전략