J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버 위협 탐지대응시간 모델링☆

Cyber threat Detection and Response Time Modeling

한 충 희[1] 한 창 희[2*]
Han Choong-Hee Han ChangHee

요 약

보안관제 분야의 실제 업무활동에 대해서는 거의 연구가 없는 실정이다. 이에 본 논문에서는 보안관제의 위협정보 탐지 대응시간 모델링을 통해 적정 투입인력 규모 산정에 기여하고 최신 보안솔루션 투입시의 효과성 분석 등에 활용할 수 있는 실질적인 연구 방법론을 제시하고자 한다. 보안관제센터에서 수행하는 전체 위협정보 탐지대응시간은 TIDRT(Total Intelligence Detection & Response Time)로 정의한다. 전체 위협정보 탐지 대응시간(TIDRT)는 내부 위협정보 탐지대응시간(IIDRT, Internal Intelligence Detection & Response Time)과 외부 위협정보(EIDRT, External Intelligence Detection & Response Time)의 합으로 구성된다. 내부위협정보 탐지대응시간(IIDRT)는 다섯 단계의 소요시간의 합으로 계산할 수 있다. 본 연구의 궁극적인 목표는 보안관제센터의 주요한 업무활동들을 수식으로 모델링하여 보안관제센터의 사이버 위협정보 탐지대응시간 계산식을 산정하는데 있다. 2장에서는 선행연구를 살펴보고, 3장에서는 전체 위협정보 탐지대응시간의 계산식을 모델링한다. 4장에서 결론으로 끝을 맺는다.

☞ 주제어 : 사이버 위협, 위협정보, 보안관제, 탐지 대응, TIDRT, CTI

ABSTRACT

There is little research on actual business activities in the field of security control. Therefore, in this paper, we intend to present a practical research methodology that can contribute to the calculation of the size of the appropriate input personnel through the modeling of the threat information detection response time of the security control and to analyze the effectiveness of the latest security solutions. The total threat information detection response time performed by the security control center is defined as TIDRT (Total Intelligence Detection & Response Time). The total threat information detection response time (TIDRT) is composed of the sum of the internal intelligence detection & response time (IIDRT) and the external intelligence detection & response time (EIDRT). The internal threat information detection response time (IIDRT) can be calculated as the sum of the five steps required. The ultimate goal of this study is to model the major business activities of the security control center with an equation to calculate the cyber threat information detection response time calculation formula of the security control center. In Chapter 2, previous studies are examined, and in Chapter 3, the calculation formula of the total threat information detection response time is modeled. Chapter 4 concludes with a conclusion.

☞ keyword : Cyber threat, threat information, security control, detection response, TIDRT, CTI

1. 서 론

사이버 위협 탐지대응시간 모델링의 목적은 현재의 보안관제 업무 현황을 정확히 규명함으로써 효율적인 보안관제 개선 방안을 도출하기 위함이다. 실제 보안관제 업무 프로세스는 끊임없이 유입되는 사이버 공격들을 자체적으로 보유하고 있는 IPS, IDS로 탐지 분석하여 방화벽 장비에 해당 악성 IP를 차단하거나 외부기관으로부터 수신하는 악성 IP를 방화벽 장비에 차단하는 활동이다. 이러한 보안관제 업무를 모델링하기 위해 1년간의 위협 탐지 데이터들을 엑셀의 피벗 기능을 이용하여 통계적으로 분석하고 보안관제요원들을 대상으로 2018년 12월부터 2019년 1월까지 수행한 설문조사를 통해 도출된 분석결과를 활용하였다.

본 연구를 위해 우선 보안관제센터의 업무활동들 중 가장 큰 부분을 차지하는 사이버 위협에 대한 탐지와 대응활동에 소요되는 업무에 소요되는 세부 업무활동들을 크게 5개의 단계로 구분한다. 그 다음으로, 위의 설문조사를 통해 각 단계에 소요되는 시간들을 상수화하여 악성IP 수량과 등록할 보안장비의 수를 변수로 하는 계산식

1 Information Security Team, Korea Power Exchange, Naju-si, 58321, Korea.
2 Dept. of Computer Science, Korea Military Academy, Seoul, 01805, Korea.
* Corresponding author (chhan46@gmail.com)
[Received 8 March 2021, Reviewed 12 March 2021(R2 20 April 2021), Accepted 20 May 2021]
☆ 본 논문은 2020년도 한국인터넷정보학회 추계학술발표대회 우수논문 추천에 따라 확장및 수정된 논문임.

을 만들어 소요시간을 계산하고자 하였다. 이를 위해, 2장에서는 선행연구를 살펴보고, 3장에서는 전체 위협정보 탐지대응시간의 계산식을 모델링한다. 4장에서 결론으로 끝을 맺는다.

2. 선행연구

2.1 위협 정보(TI, Threat Intelligence)

사이버 위협 인텔리전스(CTI, Cyber Threat Intelligence) 또는 위협 인텔리전스 (TI, Threat Intelligence)는 공격을 방지하기 위한 목적으로 의사 결정을 알릴 수 있는 위협에 대한 증거 기반 지식이다 [1]. TI는 특정 결정을 돕는 대신 위험 환경을 밝히는 데 도움이 되는 정보이다 [2]. TI는 다양한 기술 소스 (예 : 로컬 센서 트래픽) 또는 인적 소스 (예 : 지하 포럼에서 관찰된 토론, 동료와의 커뮤니케이션)에서 수집된 정보이다 [3].

2.2 보안관제센터(Security Operation Center)

Cyril은 보안 관제 센터를 (SOC, Security Operation Center)라고 정의한다. 또한, 보안 관제 센터는 침해 사고를 감지하고 대응하는 플랫폼을 의미한다. 보안 관제 센터는 분석가, 운영자, 관리자 및 기타 직원이 정보 시스템, 인프라 및 서비스를 모니터링 하는 곳이다. 보안 관제 센터 직원은 일련의 프로세스와 절차를 사용하여 사이버 공격, 보안 위반 및 비정상적인 행동을 탐지, 대응 및 복구하는 역할을 수행한다. Cyril은 또한 보안 관제 센터의 가장 중요한 기능은 IPS, IDS 및 Anti-DDoS 장비에서 수집된 보안 이벤트를 모니터링하고 이에 대응하는 활동이다. 보안 관제 대응 활동은 유해하다고 간주되는 보안 이벤트를 선택하고 추가 조사를 수행하는 것에서 시작된다. 추가 조사에는 소스 정보 (소스 IP 주소), 엔티티 정보 (호스트 이름, 도메인 이름), 트래픽 유형 (RDP, SSH, FTP, HTTP, HTTPS, TLS, SSL 등), 프로토콜 정보 (TCP, UDP), 공격 패턴 정보. (서명 정보), 목적지 정보 (목적지 IP), 지역 정보 (출발지) 등을 분석한다[4].

보안관제는 사이버공간의 위협과 침해사고들을 분석하며, 침해사고들에 대응한다는 의미이다[5]. 보안관제의 역할은 내·외부로부터의 위협 요소로부터 정보시스템, 데이터 등의 손상을 막고, 피해 발생을 막는 것을 말한다[6]. 보안관제는 많은 수의 서버 및 네트워크를 모니터링, 분석하여 조치사항을 분석 처리하는 업무이다[7]. 보안관제는 대상기관의 정보시스템 및 다양한 IT자원을 해킹, 바이러스 등과 같은 여러 사이버 공격으로부터 보호하기 위해 각종 보안 이벤트 및 시스템 로그들을 모니터링하고 분석하여 문제점에 대응하는 보안 업무이다[8]. 보안관제시스템은 방화벽(Firewall), 침입차단시스템(IPS), Anti-DDoS장비 등의 보안 이벤트를 하나로 통합하여 관리할 수 있게 해주는 시스템이다. 이기종 장비들에서 생산되는 보안이벤트를 한 곳에서 확인할 수 있도록 해주는 것이 주요 기능이다[9]. 보안관제 업무 중 해외의 악성 IP차단을 위해 여러 가지 활동들을 수행하고 있다. 추가공격여부 확인, 악성 IP의 WHOIS검색, 네트워크별 보안장비에 악성 IP차단 등록, 실무부서에 취약점을 보유한 SW설치 및 변조여부 확인 요청 등의 활동들이 수행된다[10].

2.3 보안관제센터 업무활동

보안관제센터의 주요 업무 활동들은 각종 위협정보들을 수집, 탐지, 대응, 보고 하는 4가지의 단계로 구분할 수 있다. 각 주요 업무 활동의 비율은 보안관제 전문가들의 경험과 의견에 따라 수집 10%, 탐지 40%, 대응 40%, 보고 10%로 정의하였다. 보안관제센터는 365일 24시간 악성 IP, 악성 URL 정보 등 사이버 위협 정보들을 탐지하고 대응하는 활동들을 수행한다. 이러한 탐지, 대응활동들은 전체 보안관제센터의 업무활동 중 약 80%에 해당한다 [11].

악성 IP를 탐지하여 차단하는 과정은 크게 다섯 단계로 구성된다. 첫째, 탐지되는 악성 IP에 의한 추가적인 공격여부를 확인하는 시간 TA(Time for Additional attack checking), 둘째, 악성 IP의 출발지 관련 정보를 확인하기 위한 WHOIS 검색하는 시간 TW(Time for WHOIS checking), 셋째, 방화벽 또는 IPS와 같은 보안장비에 악성 IP정보를 등록하는데 소요되는 시간 TE(Time for Enrollment bad IP), 넷째, 실무부서에 사이버 공격에 의한 피해 여부를 확인 요청하는 시간 TR(Time for Request damage checking), 다섯째, 실무부서의 사이버 공격 피해 여부 확인시간 TC(Time for Checking damage by operation teams)이다. 여기에서 TA, TW, TE는 2018년 12월부터 1월까지 수행한 설문조사를 통해 TA 152초, TW 109초, TE 124초가 평균적으로 소요되는 것으로 분석되었다. TR과 TC는 비주기적 시간으로 분석되었다[12].

3. 전체 위협정보 탐지대응시간 TIDRT 모델링

보안관제센터 업무활동의 핵심은 봉쇄(Blockade), 탐지(Detection), 대응(Response)이다. 봉쇄는 '사이버 위협의 유입경로 구간에서 사이버 위협의 유입을 제한하기 위한 활동'이다. 정보보안 활동은 수많은 보안장비들에 봉쇄정책을 등록하는 것으로부터 시작된다. 사이버 위협이 유입되는 경로에는 이미 사이버 위협을 차단하기 위해 방화벽, IPS, Anti-DDoS 등 수 많은 봉쇄를 위한 보안장비들이 운영되고 있다.

탐지(Detection)는 '사이버 위협을 직접적으로 색출하는 활동'을 의미한다. 봉쇄는 차단 정책에 의해 진행되는 기계적인 과정인 반면, 탐지는 보안관제 분석요원, 바이러스 전문가 등 숙련된 전문가가 수행하는 과정이다. 고위험도의 이벤트인지, 저위험도의 이벤트인지 등을 판단하고 악성 행위를 발생시키는 악성 IP를 추출하는 과정 등이 탐지 활동에 해당된다. 이 밖에 전 직원들의 PC에 Antivirus, EDR 등의 제품을 설치하여 운영하는 것도 탐지 활동에 해당된다.

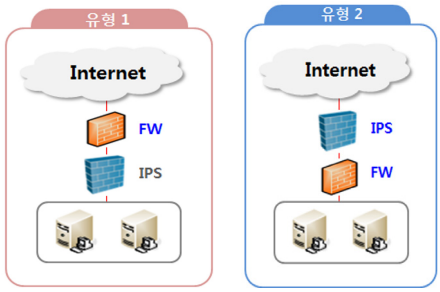
대응(Response)은 '발생된 사이버 위협에 대한 대응활동'이다. 대응 활동에는 사이버 위협이 다시 발생되지 않도록 악성IP 보안장비 등록, 바이러스 치료, 삭제, 악성행위 시도의 제한 등의 활동이 포함된다. 또한 조직내의 구성원들이 정보보안의 목표와 정책들을 충분히 이해할 수 있도록 사이버 위협 사례 등을 교육하는 활동들도 포함된다.

보안관제센터에서 대응하는 전체 위협정보는 자체 보안관제장비를 통해 탐지, 분석되는 내부 위협정보(II, Internal Intelligence)와 외부 정보기관들에 의해 탐지 분석되는 외부 위협정보(EI, External Intelligence)로 구분할 수 있다.

보안관제센터에서 수행하는 전체 위협정보 탐지대응시간은 TIDRT(Total Intelligence Detection & Response Time)로 정의한다. 전체 위협정보 탐지 대응시간(TIDRT)는 내부 위협정보 탐지대응시간(IIDRT, Internal Intelligence Detection & Response Time)과 외부 위협정보(EIDRT, External Intelligence Detection & Response Time)의 합으로 구성된다. 내부위협정보 탐지대응시간(IIDRT)는 다섯 단계의 소요시간의 합으로 계산할 수 있다. TE에는 인터넷 연계 네트워크의 수량 N을 곱해주어야 정확한 시간을 계산할 수 있다. IIDRT(N)을 수식으로 표현하면 <수식1>과 같다.

$$IIDRT(N) = TA + TW + \sum_{i}^{N} TE_{iFW} + TR + TC \quad (1)$$

악성 IP 차단 대응은 그림 1의 유형 1과 같은 구성에서는 IPS 장비에서 탐지되는 사이버 공격 패턴에서 악성 IP를 분석하여 방화벽에 차단 등록하는 것이 일반적인 방법이다.



(그림 1) 네트워크 유형
(Figure 1) Types of Network

그러나 유형 2와 같이 IPS의 위치가 방화벽보다 선행하는 위치에 있는 경우에는 IPS 장비에도 악성IP를 추가적으로 등록해주어야 악성 IP 차단 효과를 구현할 수 있다.

N개의 네트워크에서는 유형 1과 같이 구성하고 있고, M개의 네트워크에서는 유형 2와 같이 각 네트워크별로 구성된 위치가 다른 경우도 있을 수 있다. IIDRT(N,M)의 경우를 수식으로 표현하면 <수식2>와 같다.

$$IIDRT(N,M) = TA + TW + \sum_{i}^{N} TE_{iFW} + \sum_{i}^{M} (TE_{iFW} + TE_{iIPS}) + TR + TC \quad (2)$$

여기에서 방화벽과 IPS장비에 악성 IP를 차단 등록하는 시간은 설문조사 결과 거의 유사한 소요시간을 보인다. 따라서 보안장비별 등록시간을 동일하게 적용하여 수식을 다시 표현하면 <수식3>과 같다.

$$IIDRT(N,M) = TA + TW + \sum_{i}^{N} TE_i + 2\sum_{i}^{M} TE_i + TR + TC \quad (3)$$

위의 수식에서 실무부서와 연관된 소요시간들은 반복적으로 발생되는 시간들이 아니므로 TR과 TC를 제외한다. 여기에 내부 장비들에 의해 망별로 탐지되는 악성 IP들을 II(Internal Intelligence, 내부 위협정보)라 하면 II는 각 네트워크(NW)별로 탐지되는 II들의 합으로 계산할 수

있다. 그림 1의 유형 1과 같은 네트워크가 N개, 유형 2와 같은 네트워크가 M개이면서 자체 보안관제 장비로 탐지 분석되어 얻어지는 II개의 내부 위협정보에 탐지 대응하기 위한 시간 IIDRT(N,M,II)에 대한 수식은 <수식4>와 같이 만들 수 있다.

$$IIDRT(N,M,II) = (TA + TW + \sum_{i}^{(N+2\times M)} TE_i) \times II \quad (4)$$

외부 위협정보 탐지대응시간 EIDRT는 IIDRT에서 TA, TW를 제외한다. II를 대신하여 외부 기관들에 의해 탐지되는 악성 IP들인 EI(External Intelligence, 외부 위협정보)를 곱하여 계산한다. 그림 1의 유형 1처럼 구성된 네트워크가 N개, 유형 2와 같이 구성된 네트워크가 M개이면서 내부 위협정보 II개, 외부 위협정보 EI개에 대응하기 위한 전체 위협정보 탐지대응시간 TIDRT(N,M,II,EI)는 <수식5>와 <수식6>과 같다.

$$TIDRT(N,M,II,EI) = IIDRT + EIDRT \quad (5)$$

$$TIDRT(N,M,II,EI) = (TA + TW + \sum_{i}^{(N+2\times M)} TE_i) \times II + \sum_{i}^{(N+2\times M)} TE_i \times EI \quad (6)$$

등록할 보안장비의 수를 미리 결정할 수 있다면 계산식은 좀더 간단하게 정리될 수 있다. 그림 1의 유형 1처럼 구성된 네트워크가 N개, 유형 2와 같이 구성된 네트워크가 M개인 경우의 등록할 보안장비의 수량 S(N,M)을 구하는 계산식은 <수식7>과 같다.

$$S(N,M) = N + 2\times M \quad (7)$$

등록할 보안장비 수량을 S개, 내부 탐지 위협정보 II개, 외부 탐지 위협정보 EI개일 경우, 내부 위협정보 탐지대응시간 IIDRT(S,II), 외부 위협정보 탐지대응시간 EIDRT(S,EI), 전체 위협정보 탐지대응시간 TIDRT(S,II,EI) 수식은 <수식 8>부터 <수식11>과 같다.

$$IIDRT(S,II) = (TA + TW + TE\times S) \times II \quad (8)$$

$$EIDRT(S,EI) = (TE\times S) \times EI \quad (9)$$

$$TIDRT(S,II,EI) = IIDRT(S,II) + EIDRT(S,EI) \quad (10)$$

$$TIDRT(S,II,EI) = (TA + TW + TE\times S) \times II + (TE\times S) \times EI \quad (11)$$

위의 최종 수식 <수식 11>을 검증한다. TA 152초, TW 109초, TE 124초로 상수처럼 활용한다. 사례기관의 경우 2018년 통계를 활용하면 내부에서 자체적으로 탐지하여 악성 IP로 등록한 1일 평균 내부 위협정보 II 42개와 1일 평균 외부 탐지 위협정보 EI 91개, 등록할 보안장비 수량 S 3개의 상황을 수식에 대입하면 16.79시간이 <수식11>을 통해 계산된다. 16.79시간은 사이버 위협의 탐지와 대응에 해당되는 시간이며 전체 업무시간의 80%이므로 비례식을 이용하여 10%의 수집활동시간(Tcol), 10%의 보고활동시간(Trpt)을 합산한 전체 업무시간 TSOC는 20.99시간으로 계산된다. 4조 2교대하여 3명의 보안관제요원이 24시간동안 침해대응활동을 수행하고 있으므로 1명당 7시간씩 주기적 업무활동을 수행하고 있음을 확인할 수 있다. 나머지 1시간은 비주기적 시간으로 계산식에 포함하지 않았던 실무부서에 사이버 공격에 의한 피해 여부를 확인 요청하는 시간 TR(Time for Request damage checking)과 실무부서의 사이버 공격 피해여부 확인시간 TC(Time for Checking damage by operation teams)에 소요되는 것으로 보안관제센터의 업무활동들을 종합적으로 이해할 수 있다. 이를 통해 본 연구에서 모델링한 최종 <수식11>이 합리적으로 모델링 되었음을 확인할 수 있다.

4. 결 론

보안관제센터 업무활동의 핵심은 봉쇄(Blockade), 탐지(Detection), 대응(Response)이다. 보안관제센터는 자체적으로 탐지 차단하는 위협정보들과 외부 정보기관으로부터 제공받는 위협정보들을 365일 24시간 끊임없이 보안장비에 등록하는 활동들을 수행하는 곳이다. 이러한 활동들에 소요되는 시간들을 측정하는 것은 사이버 위협 탐지 대응활동을 종합적으로 이해하는데 많은 도움이 될 수 있을 것이다.

보안관제센터에서 수행하는 전체 위협정보 탐지대응시간은 내부 위협정보 탐지대응시간과 외부 위협정보의 합으로 구성된다. 본 연구를 통해, 1일 평균 내부 악성 IP 수량, 1일 평균 외부요청 악성IP 수량과 등록할 보안장비 수량 세가지 변수만 확인되면 대응시간을 계산할 수 있게 되었다. 위협정보 탐지 대응시간 모델링을 통해 보안관제센터의 위협정보 탐지대응시간을 추정할 수 있을 것이다. 이를 통해 적정 투입인력 규모 산정과 최신 보안솔루션 투입시의 효과성 분석 등에 활용할 수 있기를 기대한다.

참고문헌(Reference)

[1] McMillan R. Definition: threat intelligence. Gartner; 2013. https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf

[2] Chrismon D, Ruks M. Threat Intelligence: Collecting, analyzing, evaluating, MWR Infosecurity, UK Cert, United Kingdom; 2015. https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

[3] Dalziel H. How to define and build an effective cyber threat intelligence capability. Syngress Publishing of Elsevier; 2014. https://www.sciencedirect.com/book/9780128027301/how-to-define-and-build-an-effective-cyber-threat-intelligence-capability

[4] Cyril Onwobiko, 'Cyber Security Operation Centre: Security Monitoring for protecting Business and supporting Cyber Defense Strategy', Intelligence & Security Assurance, E-Security Group, London, UK. 2018. https://doi.org/10.1109/CyberSA.2015.7166125

[5] Sitaram Kowtha, Laura A. Nolan, Rosemary A. Daley, 'Cyber Security Operation Center Characterization Model and Analysis', Johns Hopkins University, Applied Physics Laboratory, 978-1-4673-2709-1/12, IEEE, 2012. https://doi.org/10.1109/THS.2012.6459894

[6] Eui-yeon Jung, 'A Study on the Integrated Security Monitoring &Control in Financial Investment Industry Computer Networks', Korea Information Processing Society, 19-2, Feb, 2012. https://www.koreascience.or.kr/article/CFKO201221868477405.jsp-kj=SSMHB4&py=2012&vnc=v27n6&sp=588

[7] Gil Sun, Yu, 'A Study on the Cyber Security monitoring Detection and Response', Department of Digital Forensics, The Graduate School of Hanseo University, August, 2018.

[8] Tae-Woong Seo, 'An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control', Journal of Multimedia, 15(1), Jan, 2012.

[9] Kim, MinJun, 'A study on the implementation of white-list intrusion detection system on control networks', Department of Industry Security, Graduate School, Kyonggi Univ, Jun, 2011.

[10] Han Choong-Hee, 'Oversea IP Ranges Blocking for Security Enhancement of Critical Infrastructures with Cyber Threats Analysis in Electric Industry', Journal of the Korea Institute of Information Security and Cryptology 29(2), pp. 401~415, Apr, 2019. https://doi.org/10.13089/JKIISC.2019.29.2.401

[11] Han Choong-Hee, "A Study on Cyber Threat Detection Response Analysis and Blocking Method", Doctor's Thesis, Department of Interdisciplinary Program of Information Security Graduate School of Chonnam National University, pp. 1~121. Aug, 2019.

[12] Han Choong-Hee, "Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system", International Journal of Critical Infrastructure Protection, Volume 26, 100312, Sept. 2019. https://doi.org/10.1016/j.ijcip.2019.100312

◐ 저 자 소 개 ◑

한 충 희(Han Choong-Hee)
1996년 동국대학교 컴퓨터공학(이학사)
2002년 동국대학교 정보보호학과 (이학석사)
2019년 전남대학교 정보보호협동과정 (이학박사)
2002년~현재 전력거래소 정보보안팀 차장
관심분야 : 보안관제, 사이버 위협 탐지 대응, 악성코드 etc.
email : justicehan@kpx.or.kr

한 창 희 (Han ChangHee)
1990년 육군사관학교 물리학과(이학사)
1994년 美 Syracuse 대학교 전산학(이학석사)
2004년 美 Univ. of Southern California 전산학(이학박사)
1994년~현재 육사 컴퓨터과학과 교수
관심분야 : 정보보호, 사이버전, 지능형 탐지, 인공지능
email : chhan46@gmail.com