https://doi.org/10.33778/kcsa.2021.21.1.045

망분리 네트워크 상황에서 사이버보안 취약점 실시간 보안관제 평가모델★

이 동 휘*, 김 홍 기**

요 약

망분리 네트워크에서 보안관제를 할 경우 내부망 또는 위험도가 높은 구간에서는 평시 이상징후 탐지가 거의 이루어지지 않는다. 그렇기 때문에 보안 네트워크 구축 후 최적화 된 보안구조를 완성하기 위해서 망분리된 내부망에서의 최신 사이버 위협 이상징후를 평가할 수 있는 모델이 필요하다. 본 연구에서 일반 네트워크와 망분리 네트워크에서 발생하는 사이버 취약점과 악성코드를 데이터셋으로 발생시켜 평가하여, 망분리 내부망 사이버 공격에 위협 분석 및 최신 사이버 취약점을 대비 할 수 있게 하고, 특성에 맞는 사이버 보안 테스트 평가 체계를 구축하였다. 이를 실제 망분리 기관에 적용 가능한 평가모델을 설계 하고, 테스트 망을 각 상황별로 구축하여 실시간 보안관제 평가 모델을 적용하였다.

Real-time security Monitroing assessment model for cybersecurity vulnera bilities in network separation situations

DongHwi Lee*, Hong-Ki Kim**

ABSTRACT

When the security monitoring system is performed in a separation network, there is little normal anomaly detection in internal networks or high-risk sections. Therefore, after the establishment of the security network, a model is needed to evaluate state-of-the-art cyber threat anomalies for internal network in separation network to complete the optimized security structure. In this study, We evaluate it by generating datasets of cyber vulnerabilities and malicious code arising from general and separation networks, It prepare for the latest cyber vulnerabilities in internal network cyber attacks to analyze threats, and established a cyber security test evaluation system that fits the characteristics. The study designed an evaluation model that can be applied to actual separation network institutions, and constructed a test data set for each situation and applied a real-time security assessment model.

Key words : Security Monitroing, Security Monitroing assessment, Network Separation

접수일(2021년 2월 26일), 수정일(1차: 2021년 03월 22일), 게재확정일(2021년 03월 23일)

★ 본 논문은 2020학년도 동신대학교 연구년 교수 연구비지원에 의하여 연구되었음

* 동신대학교/융합정보보안전공 교수(주저자)

** 동신대학교/융합정보보안전공 교수(교신저자)

1. 서 론

인터넷을 통한 보안 위협이 커짐에 따라 인터넷을 기반으로 구축한 환경들이 다양한 보안 위협에 직면하게 되었다. 인터넷망과 업무망이 분리되지 않은 단일망에서 외부의 공격에 노출됨에 따라 악성코드 감염, 내부 자료 유출, 시스템 제어 등의 피해가 발생하고 있다[1]. 이에 대한 보안 대책으로

공공기관을 필두로 하여 망분리 네트워크를 구축하여 사용하고 있지만 망분리 상황에서 보안 전문 인력과 예산 부족으로 인하여[2] 보안관제 구성 및 사이버 위협 훈련이 복잡하고 어려워 지능형 지속공격등 새로운 사이버공격에 취약점이 존재한다. 이러한 네트워크 구조 보안 취약점을 개선하기 위하여 본 연구에서는 사이버위협에 대한 실시간 방어를 위해 단일 망과 망분리 상황에 보안관제 테스트 베드를 구축하여, 각 위협에서 대한 적절한 보안조치를 할 수 있게 방향성을 제시한다.

실시간 사이버 보안 평가모델을 설계하기 위해 각 장비별 최신 및 대표 취약점을 기반으로 위험요소를 식별하게 하고, 또 이를 각 내부구간의 악성코드를 발생시켜 이에 따른 이벤트를 탐지·분석하여구간별·위험별, 가중치를 부여하여 각 장비(네트워크, 시스템, 보안장비)에 대표 취약점 관련 데이터셋을 업데이트하고, 위험 수준을 평가하여 최신 보안 대처 방안을 적용하는 보안관제 탐지 방향성을 제공하여 보안관제 담당자들이 사이버 보안위협에 대한 최신 대비책과 대응이 가능하게 한다.

2. 망분리 네트워크 보안 위협

네트워크에 사이버 보안 위협이 커짐에 따라 인터넷과 직접 연결된 시스템 환경들이 다양한 보안 위협에 직면하게 되었다. 이에 대한 보안 대책으로 공공기관을 필두로 하여 망분리를 통해 업무망과 인터넷망이 분리되는 네트워크가 구축되었다.

그러나 망분리 상황에도 망이 연계되는 PC 예외자(인터넷망/업무망을 동시에 사용 가능한 사람, 무선네트워크를 사용 가능한 사람 등)와 권한/규칙 등에 대한 관리가 부족하여 사고가 빈번하게 발생한다[3].

망간 연계 상황에서 발생하는 사고에 따른 공격 기법과 그에 대한 대응은 <표 1>과 같다. 이러한 상황 속에서 보안관제의 필요성이 높아져, 네트워크 구성별 실시간 보안관제 평가모델을 설계하고자 한다.

<표 1> 보안 위협에 따른 대응방안[4],[5]

	공격 기법	대응방안
초기 정찰 (Initial Reconnaissance)	스캐닝 : 운영 체제 식별, 취약점 조사	스캐닝 탐지 중요 자산 접속 감시 내부 네트워크 감시
초기 침입 (Initial Exploitation)	악성코드 첨부 이메일 발송 웹사이트 접속 유도 감염된 이동식 매체 발송	악성코드 탐지 : 파일 평판
지속성 확보 (Establish Persistence)	추가 백도어 설치 은닉	사용자 행위 감시 악성 사이트 탐지 : 도메인 평판 내부 네트워크 감시
공격 도구 설치 (Install Tools)	추가 공격 도구 다운로드	악성코드 탐지 : 파일 평판
내부망 이동 (Move Laterally)	중요 시스템 또는 중요 데이터베이스로 이동	내부 네트워크 감시 계정 접속 감시
수집 / 유출 (Collect, Exfil, Exploit)	중요 데이터 유출 데이터 손상, 조작 및 파괴	실시간 네트워크 모니터링 해커가 노리는 대상 파악

망분리 상황에서 망연계 시스템의 환경 구성 방식은 DMZ 구간을 통해 내·외부에서 모두 인터넷을 사용할 수 있도록 하였고 보안장비의 통합 로그[6, 7]를 모니터링 할 수 있는 관제 시스템을 네트워크 구성 별로 구축하였다.

망분리에서 구축된 내부망에 취약점, DoS, 악성코드, 네트워크 패킷 등의 데이터셋을 보내어 보안관제 시스템에서 어떤 결과가 나오는지 분석해보고, 이를 통해 평가모델을 제시하고자 한다.

3. 장비별 사이버 보안 취약점 분석

망분리 네트워크 활용이 점차 증가하면서 이에따른 네트워크 및 보안시스템의 사용도와 중요도 또한 변화하고 있는 추세이다. 이러한 변화에 맞게 각 시스

템(네트워크, 보안, 서버) 등의 안정성이 보장되어야 하지만 새로운 환경이 증가함에 따라 또 다른 보안위협이 증가하고 있다. 이러한 상황에서 보안관제시 각 시스템에서 발생할 수 있는 대표 취약점, 최신 취약점 이벤트에 대하여 분석하여 장비별로 생길수 있는 문제와 CVSS 및 이벤트 발생일을 기준으로 연구함.

3.1 네트워크 보안 취약점

네트워크 보안 장비 취약점은 IPv4, IPv6, UDP, DNS, DHCP, TCP, ICMPv4, ARP 등이 적용된 제품에서 비정상 이벤트인 데이터 유출 등의 피해가 발견된 네트워크 취약점이 대다수이다. 대표적으로는 <표2>과 같은 TCP/IP 프로토콜이 적용된 장비들로써 파라미터 처리/입력값 검증이 미흡하여 발생하는 취약점과 기타 메모리 경계값을 벗어난 읽기로 인해 발생하는 정보노출 취약점들이 존재한다. 또한 보편적으로 많이 사용하는 네트워크 장비 취약점을 분석함

<표 2> 네트워크 장비 대표 취약점

분류	취약점 공격
Treck TCP/IP 프로토콜이 적용된 네트워크 장비	CVE-2020-11896 IPv4/UDP 패킷의 매개변수 처리가 미흡하여 발생하는 원격코드 실행 취약점
	CVE-2020-11899 IPv6에서 패킷의 입력값 검증이 미흡하여 메모리 범위를 벗어난 읽기 및 서비스 거부 취약점
	CVE-2020-11903-11905 DHCP/DHCPv6 패킷 처리가 미흡하여 메모리 경계 값을 벗어난 읽기로 인해 발생하는 정보노출 취약점

3.2 시스템 보안 취약점

시스템 보안 취약점은 대표적으로 <표 3>과 같이 Window, Unix, Linux서버 등에서 공격자가 특수하게 제작된 악성 응용프로그램을 실행할 경우 원격코드를 실행하여 정보노출 및 스푸핑, 권한상승 등을 허용하는 취약점이 존재한다. 또한 리눅스 유닉스의 Sudo 결점을 이용하여 제한된 사용자가 루트 권한으로 명령을 실행하도록 허용하여 비정상적인 이벤트를 발생하게 하는 취약점 또한 존재한다. 연계 취약점은 VPN 서버 취약점을 이용하여 서비스 거부 공격 및 DNS 취약점을 이용해 원격코드를 실행시키는 취약점 또한 존재한다.

<표 3> 시스템 대표 취약점

분류	취약점 공격
WINDOW SERVER	CVE-2019-1358,1359 원격 코드 실행 취약점
	CVE-2019-1166 스푸핑 취약점
LINUX SERVER	CVE-2019-16746 버퍼 오버플로우 취약점
LINUX /UNIX SERVER	CVE-2019-14287 SUDO 명령어에서 입력값 검증이 미흡하여 발생하는 권한 상승 취약점
DNS로 운영되는 Windows server	CVE-2020-1350 DNS로 운영되는 Windows 서버에서 요청값에 대한 처리가 미흡하여 발생하는 원격코드실행 취약점
Cisco FTD 소프트웨어 VPN 시스템	CVE-2020-3189 VPN 시스템 로깅 기능의 취약성

3.3 보안 장비 취약점

망분리 환경에서 다양한 네트워크 장비와 시스템을 구축하면서 IDS, IPS, UTM등 보안 장비와 시스템의 중요하고 민감한 정보들에 허가받지 않는 자가 접근하지 못하게 하여 안전성과 신뢰성을 높여주는데 꼭 필요한 필수 불가결한 요소들이다.

이러한 보안장비는 <표4> 와 같이 취약점에 영향받는 시스템 권한 상승 또는 서비스 거부 등의 피해를 발생시킬 수 있으므로 해당 제품을 사용하는 장비는 각 시스템과 연계되는 분석이 필요하다.

<표 4> 보안장비 연계 취약점

분류	취약점 공격
CISCO IPS	CVE-2014-0718 Cisco IPS 분석 엔진 서비스 거부 취약성
	CVE-2014-0719 Cisco IPS Control-Plane MainApp 서비스 거부 취약성
	CVE-2014-0720 Cisco IPS 점보 프레임 서비스 거부 취약성
juno space Firewall	CVE-2017-2310 방화벽 우회 취약점을 통해 특정 제작 된 패킷을 허용하는 취약점이 존재
A10 ACOS 웹 방화벽 (WAF)	CVE-2018-15904 SQL 인젝션 공격 차단하기 위해 구성된 규칙 처리 취약점
Cisco IOS XE 소프트웨어 방화벽	CVE-2020-3421 DOS 취약성
Suricata-IDS	CVE-2019-16411 IPV4 패킷을 보내면 decode-ipv4.c의 OptValidateTimestamp 함수가 할당되지 않은 메모리 영역에 액세스 하려고 하는 취약성이 존재
Cisco Firewall	CVE-2020-3421 DOS 취약성
Huawei IPS 모듈	CVE-2018-7994 메모리 누수 취약점 존재

4. 실시간 보안관제 평가 모델

4.1 각 시스템별 수준측정

보안관제 평가모델은 구성요소 별 취약성을 파악하고 취약성을 이용한 위협의 발생 가능성과 위협 발생 시 시스템에 미치는 영향의 정도를 결정하는 과정인 위험 분석을 통하여 해당 시스템을 평가하고 대상 시스템이 효과적으로 적용되고 있는지 분석 하여야 한다.

분리된 네트워크와 단일 네트워크에 동일한 이벤트를 발생 시켰을때 각 모델의 위험도 평가를 위해 실시간 보안관제 평가 모델을 제시한다. 또한 보안관제의 특성에 맞춰 시스템과 보안장비, 네트워크 장비에 관한 수준 모델 <표 8, 9, 10>을 제시한다. 각 위험 수준을 구분하는 값은 앞에서 제시한 취약점 요소에 대한 데이터 셋을 기반으로 샘플링하여 측정하고, 분석된 값을 사용했다.

<표 5> 시스템 수준별 기준 및 정략적 값

Level	Standard	Value
High	정보 누출이 중요한 시스템 또는 공격자가 모든 정보를 읽거나 수정, 삭제할 수 있으며 권한에 위협을 끼칠 수 있음	SxL2Hi
Low	정보 누출이 중요한 기능에 직접적인 영향을 미치지는 않지만, 중요한 시스템을 지원하는 능력이나 중요 정보의 가독성 수준에 영향을 미칠 수 있음	SxL1Hi
None	정보 누출이 중요한 기능 및 지원 기능의 성능에 영향을 미치지 않는 수준	SxL0Hi

<표 6> 네트워크 장비 수준별 기준 및 정략적 값

Level	Standard	Value
High	공격자가 임의의 파일을 읽거나 수정 및 삭제가 가능할 수 있으며, 루트 권한을 이용해 치명적인 위협을 끼침	NxL2Hi
Low	공격자가 임의의 파일을 읽을 수 있습니다. 또한 외부의 접속으로부터 안전하지는 않으며 작은 영향이 생김	NxL1Hi
None	외부로부터 공격에 안전하며 시스템을 안전하게 운영할 수 있음	NxL0Hi

<표 7> 보안 장비 수준별 기준 및 정략적 값

Level	Standard	Value
High	외부로부터 공격을 막기 힘든 상황이며, 시스템의 운영에 치명적인 피해를 입힐 수 있습니다.	ExL2Hi
Low	외부로부터 공격을 막아내지만, 위협으로 부터 절대적으로 안전하지는 않으며 시스템 운영에 작은 영향이 생길 수 있다.	ExL1Hi
None	외부로부터 공격에 안전하며 시스템을 안전하게 운영할 수 있습니다.	ExL0Hi

4.2 연계 평가

각 시스템, 보안 장비, 네트워크 장비 각각의 시간당 총 이벤트 수, 위험 이벤트, 이벤트 가중치, 구간 가중치를 변수로 두어 해당 장비의 위험도를 실시간으로 평가할 수 있다.

Risk Assessment Model

m = Total Event
v = Risk Event
t = Event Weight
i = Section Weight

$$\sum_{n=1}^{m} \frac{(v_m \cdot t_m \cdot i_m)}{m}$$

각 <표 5, 6, 7>에서 I의 이벤트 검출에 따른 가중치를 다르게 부여하여 위 평가 모델에 t를 대입한다. 이때 t의 값은 <표 8>를 통해 가중치가 정해진다. 또한 보안장비, 네트워크 장비, 시스템 순서로 공격을 받았을 때 더 큰 영향을 미칠 수 있는 곳에 가중치를 더 크게 둔다. 그렇게 산출된 값을 <표 9>을 통해 해당 특성의 보안관제 위험 수준을 평가한다.

<표 8> 중요 네트워크 구간 수준

수준	가치	설명
L5	Very High	내부 네트워크에 큰 피해를 입힐 수 있으며, 서버 운영에 치명적인 부작용을 일으킴
L4	High	내부 네트워크에 피해를 입힐 수 있으며, 서버 운영에 부작용을 적용
L3	Moderate	외부 네트워크에 큰 피해를 입힐 수 있으며, 서비스에 이용이 제한될 수 있고, 내부 네트워크로 피해가 확산
L2	Low	외부 네트워크에 피해를 입힐 수 있으며, 일부 서비스에 이용이 제한
L1	Very Low	외부 네트워크에 적은 피해를 입힐 수 있으며, 일부 서비스에 영향

<표 9> 통합 수준 평가 모델

수준	가치	설명	값
L5	Very High	취약성으로 인해 시스템의 무결성과 가용성이 영향. 그리고 시스템에 여러가지 심각하거나 치명적인 부작용을 일으킴	L5mvit
L4	High	취약성으로 인해 시스템의 무결성과 가용성이 영향. 그리고 시스템에 심각한 악영향을 끼침	L4mvit
L3	Moderate	취약성으로 인해 시스템의 무결성과 가용성이 영향. 그리고 시스템에 심각한 악영향을 미칠 수 있음	L3mvit
L2	Low	취약성으로 인해 시스템의 무결성과 가용성이 영향. 그리고 시스템에 제한적인 악영향을 미칠 것으로 예상	L2mvit
L1	Very Low	취약성으로 인해 시스템의 무결성과 가용성이 영향. 그리고 시스템에 무시할 만한 악영향을 미침	L1mvit

위와 같은 방식을 통해 보안관제 구간에서 사이버 위험 요소가 발생할 가능성과 단계별 보안 수준을 나타내어 통합 수준 평가 위험도에 대해 더 자세하게 나타낼수 있으며, 이에 따라 보안구조 또는 시스템을 보완해야 하는지 점검한다. 그리고 새로운 사이버위협 발생 가능성과 보안위협 영향성에 따른 최종 사이버 보안관제 수준을 나타낸다.

최종적으로 도출된 각종 위험도 수치를 이용하여 분리 네트워크의 내부망에 대한 실시간 보안관제 상황에서 탐지 및 대응 현황을 평가하는 데 사용된다.

5. 평가모델 설계 및 실험

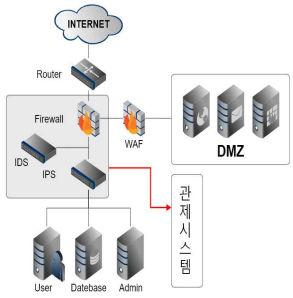
5.1 평가모델 설계

단일 네트워크와 분리 네트워크(망 연계) 상황에서의 내·외부 위협으로 인한 보안관제 탐지 및 대응 현황을 평가하고자, 취약점 데이터셋과 악성코드를 이용하여 다양한 패킷 및 이벤트를 탐지하고 해당 값을 수치화하여 네트워크, 보안장비, 시스템등 각각의 장비

에 대한 사이버 보안관제 탐지 및 대응방안 평가모델을 설계하였다. 위 평가모델은 빠른 대응이 중요시되는 보안관제의 특성에 맞춰 다양한 변수를 지정하였으며, 즉각적으로 대등할 수 있도록 구축되었다. 해당 모델의 적합성을 위해 단일 네트워크, 논리 네트워크, 물리 네트워크에서 각각 동일한 데이터셋을 전송하였다.

5.1.1 단일망 설계

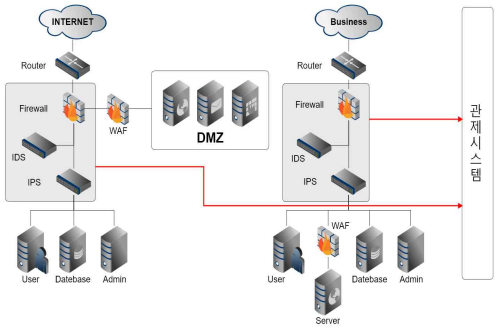
망분리가 되지 않은 단일망에서는 업무망이 외부 공격에 노출되어 다양한 피해가 발생하게 된다. 이러한 환경 속에서 (그림 1)과 같이 보안관제 시스템을 구축하였다.



(그림 1) 단일망 with 보안관제

5.1.2 물리적 망분리 설계

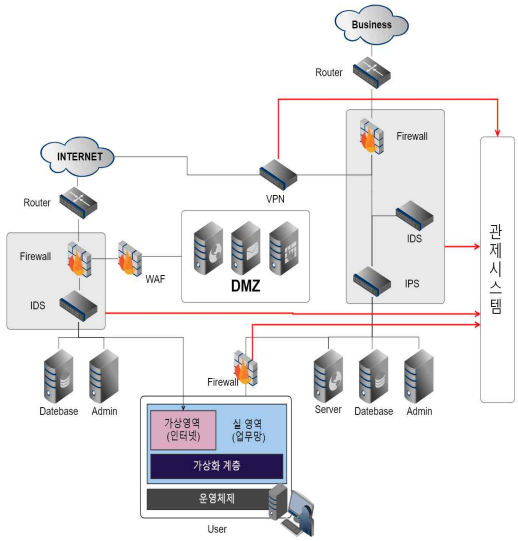
(그림 2)는 인터넷망과 업무망을 물리적으로 분리하고 업무망을 폐쇄망으로 운영하여 외부의 접속을 불가능하게 하는 물리적 망분리 구성이다.



(그림 2) 물리적 망분리 with 보안관제

5.1.3 논리적 망분리 설계

논리적 망분리란 업무용 PC에 가상화 영역을 구성하고 게이트웨이를 사용하여 사전에 구축된 가상 보안 네트워크를 통해 가상화 영역에 인터넷 접속을 가능하게 하여 (그림 3)과 같이 네트워크를 논리적으로 분리하는 방식이다.



(그림 3) 논리적 망분리와 with 보안관제

5.2 평가모델 실험

<표 10> 분리(인터넷)망 클라이언트에서 각 구간별로 패킷을 전송한 값

구분	전체 위협	장비	분리_인터넷망	
			DMZ	그 외
datase t01	1023	有	478	1023
		無	811	811
datase t02	862	有	372	862
		無	676	676
datase t03	900	有	425	900
		無	727	727
datase t04	4820	有	1456	4820
		無	4701	4701

네크워크 구성은 5.1과 같이 구성하였다. 실험은 악성코드가 담긴 PCAP 데이터셋을 공격자, 피해자의 IP에 해당하는 부분만 변경하여 피해 시스템으로 전송하였고, 모든 실험은 각 구간별 클라이언트에서 진행되었다.

<표 10>은 데이터셋을 인터넷망 내부의 클라이언트에서 전송하였을 때 보안관제에서 탐지하지 못한 패킷의 결과 값이다. 패킷을 전송하였을 때, DMZ를 제외한 모든 구간에서 같은 값이 도출되었다. 또한 보안관제의 각 센서 및 보안장비 유무에 따라 분석되었다.

<표 11> 분리(업무)망 클라이언트에서 각 구간별로 데이터 셋을 전송한 값

구분	전체 위협	장비	분리_업무망	
			Server	그 외
dataset01	1023	有	478	1023
		無	811	212
dataset02	862	有	372	862
		無	676	186
dataset03	900	有	425	900
		無	727	173
dataset04	4820	有	1456	4820
		無	4701	4701

<표 12> 외부 공격 실험

구분	전체 위협	장비	단일망
dataset01	1023	有	478
		無	811
dataset02	862	有	372
		無	676
dataset03	900	有	425
		無	727
dataset04	4820	有	1456
		無	4701

그 외 : 인터넷망(PC, DB, Admin), 업무망(PC, Server, DB, Admin) 의 모든 장비를 포함한다.

<표 11>은 업무망 내부 구간에서 데이터셋을 전송하여 탐지 한값을 나타내고, <표 12>는 외부에서 각 구간에 데이터셋을 보내고, 각 네트워크 내부 중요 클라이언트를 중심으로 데이터셋을 보내는 방식으로 실험이 진행 되었다.

<표 13> 외부 공격 분리 인터넷망 분석 결과

구분	장비	분리_인터넷망		
		DMZ	DB	Admin
dataset01	有	0.56	1.32	1.44
	無	0.95	1.04	1.14
dataset02	有	0.52	1.32	1.43
	無	0.94	1.03	1.12
dataset03	有	0.57	1.32	1.43
	無	0.97	1.06	1.15
dataset04	有	0.39	1.44	1.56
	無	1.28	1.4	1.52

<표 13>은 망 분리 인터넷망으로 이를 통해 외부 구간과 인터넷망 구간에서 데이터 셋을 전송하였을 때 각 구간에 나타나는 정량적인 수치는 차이가 없는 것으로 나타났다.

<표 14> 외부 공격 분리 업무망 분석 결과

구분	전체 위협	장비	분리_업무망		
			Server	DB	Admin
dataset01	1023	有	0.71	1.65	1.76
		無	1.20	1.3	1.39
dataset02	862	有	0.66	1.65	1.76
		無	1.20	1.29	1.38
dataset03	900	有	0.72	1.65	1.76
		無	1.24	1.33	1.42
dataset04	4820	有	0.50	1.8	1.92
		無	1.63	1.75	1.87

<표 15> 외부 공격 단일망 분석 결과

구분	위협	장비	단일망		
			DMZ	DB	Admin
dataset01	1023	有	0.56	0.77	0.82
		無	0.95	1.30	1.39
dataset02	862	有	0.52	0.71	0.75
		無	0.94	1.29	1.38
dataset03	900	有	0.57	0.77	0.83
		無	0.97	1.33	1.42
dataset04	4820	有	0.39	0.54	0.57
		無	1.28	1.75	1.87

실험 결과 단일망 보다 망분리 네트워크에서 업무망에서 데이터셋과 위험도가 증가되는 것을 분석하였다.

6. 결 론

최근 다양한 네트워크 구성이 변화하고 이에 따른 각 분야별 특성 있는 보안 모델이 구축되고 있다. 그러나 망분리 되어 있는 내부망의 경우 위협에 대한 빈도가 적다보니 실제 분석 및 경각심이 떨어져 보안 위협에 노출되어 있다.

이러한 이유 때문에 내부망 보안관제를 평가 할 수 있는 방안에 대한 관심이 높아지고 있다. 보안관제 평가 모델은 내·외부에서 최신 취약점을 비롯한 악성코드 데이터셋을 송출하고 보안관제 탐지 및 대응능력 평가 결과를 도출한다.

본 연구의 실시간 보안관제 평가모델은 일정 기간이 소요되며, 그 기간 동안 축적된 정보를 업데이트를 통해 각 특정 시스템 및 구간의 가중치를 분석 해야 한다. 그리고 또 다른 신규 취약점이 생성되면 수시로 업데이트가 필요하다. 그렇기에 주기적으로 실시간 보안관제 평가를 실시하고 보안취약성에 대한 대비를 하기 위해 사이버 위협 및 탐지를 하여 평가하는 방법만이 주의환기를 강화할 수 있으며, 차후에 새로운 위협이 발견되더라도 쉽게 대처가 가능하다. 본 연구에서 신속히 평가하고 시스템을 개선하는 방식의 평가 방법을 제시하였다. 다만 각 업무별, 중요도별 다양한 상황 및 보안 구축 방법이 상이하기 때문에 그에 따른 요소별 점수화가 오류나 문제점을 야기할 가능성이 있다. 이를 해결하기 위해선 특수한 상황이나 보안장비의 연계성을 고려하여 해당 보안관제에 맞게 수정할 필요가 있다.

참고문헌

[1] 이은배, 김기영, “망분리기반의 정보보호에 대한 고찰”, 정보보호학회 논문지, 20권 1호, 2010.

[2] 박지윤, 정윤선, 이재후, “금융권 망분리 현황과 망분리 정책 개선에 대한 고찰”, 정보보호학회지, 26권 3호, pp. 58-63, 2016.6.

[3] 인포섹, “[보안동향] 망분리 구축 이대로 안전한가?,” SK인포섹(주) 공식블로그, 2017년 7월, http://blog.naver.com/skinfosec2000/221061944974

[4] 홍준혁, 이병엽, 인공지능기반 보안관제 구축 및 대응방안. 한국콘텐츠학회논문지, 21(1), pp. 531-540, 2021.

[5] 배재권, 인공지능과 빅데이터 분석 기반 통합보안관제시스템 구축방안에 관한 연구. 로고스경영연구, 18(1), pp. 151-166, 2020.

[6] 김종민, 김동민, 이동휘, "제어시스템의 내부자 위협 탐지를 위한 Event Log 타당성 및 중요도분석에 관한 연구", 융합보안논문지, Vol. 18, No. 3, pp. 77-85, 2018.

[7] 김종민, 이동휘, “XML기반 Windows Event Log Forensic 도구 설계 및 구현”, 융합보안논문지, Vol. 20, No. 5, pp. 27-32, 2018.

〔저자소개〕

이 동 휘 (DongHwi Lee)
2007년 경기대학교 정보보호학과
(이학박사)
2011~2012년 University of Colorado Denver, Dept. of Computer Science and Engineering
현 재 동신대학교 에너지융합대학 에너지응용학부 융합정보보안전공 교수

email : dhclub@dsu.ac.kr

김 홍 기 (Hong-Ki Kim)
1996년 2월 전남대학교 전산통계학과
(이학박사)
현 재 동신대학교 에너지융합대학 에너지응용학부 융합정보보안전공 교수

email : hkkim@dsu.ac.kr